BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

İNTERNET DEĞİŞİM NOKTASI VE VERİ MERKEZLERİNİN BİLGİ GÜVENLİĞİ PERSPEKTİFİNDEN İNCELENMESİ; DÜNYADAKİ DURUM VE ÜLKEMİZ İÇİN ÖNERİLER

Lebibe YALÇINTAŞ

Teknik Uzmanlık Tezi

Eylül 2013

İstanbul

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.

BTK ISBN 978-605-345-088-7

BTK Yayın No T 0199

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

İNTERNET DEĞİŞİM NOKTASI VE VERİ MERKEZLERİNİN BİLGİ GÜVENLİĞİ PERSPEKTİFİNDEN İNCELENMESİ; DÜNYADAKİ DURUM VE ÜLKEMİZ İÇİN ÖNERİLER

Lebibe YALÇINTAŞ

Teknik Uzmanlık Tezi

Eylül 2013

İstanbul

Lebibe YALÇINTAŞ tarafından hazırlanan **İnternet Değişim Noktası Ve Veri Merkezlerinin Bilgi Güvenliği Perspektifinden İncelenmesi; Dünyadaki Durum Ve Ülkemiz İçin Öneriler** adlı bu tezin Teknik Uzmanlık tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Aktül KAVAS
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Teknik Uzmanlık tezi olarak kabul edilmiştir.

Başkan : _____

Üye : _____

Üye : _____

Üye : _____

Üye : _____

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	İnternet Değişim Noktası ve Veri Merkezlerinin Bilgi Güvenliği Perspektifinden İncelenmesi; Dünyadaki Durum Ve Ülkemiz İçin Öneriler
Türü	Teknik Uzmanlık Tezi
Yazar	Lebibe YALÇINTAŞ
Teslim Tarihi	Eylül 2013
Anahtar Kelimeler	Bilgi güvenliği, Standart, Siber saldırı, İnternet Değişim Noktası ve Veri Merkezi.
Tez danışmanı	Yrd. Doç. Dr. Aktül KAVAS
Sayfa Adedi	ix + 116

Global dünyada teknoloji kullanımının dolayısıyla bilgisayar kullanımının yaygınlaşmasıyla, insanlar ve toplum birçok bakımdan bu teknolojiye bağımlı hale gelmiştir. Bu durum beraberinde bireyleri, toplumsal yaşamı ve uluslararası ilişkileri etkisi altına alan çok önemli zararları da getirmiştir.

Hayatın her alanına giren bilgisayarların kullanılmasıyla internet ortamında bir dünya daha oluşmuştur. Siber alan dediğimiz bu dünya insanlara sağladığı yararlar ve kolaylıklar yanında, amaç dışı ya da kötü niyetli eller tarafından kullanılmasıyla da bazı zarar ve dezavantajlarla da karşı karşıya kalınmıştır. Terörün bu alanda da boy göstermesi saldırganların amaçlarını internet üzerinden gerçekleştirmek için siber saldırılar düzenlemesi içinde bulunduğumuz dünyayı da etkilemektedir.

Çalışmada; internet ve siber saldırıların uluslararası bilgi güvenliğine yönelik risk ve tehditlerine dikkat çekilerek, internet değişim noktası ve veri merkezleri bilgi güvenliği perspektifinden incelenecektir. Sonuç olarak ülkemizdeki mevcut durum ve çözüm önerileri ile bu konuda yeni bir bakış açısı oluşturulmaya çalışılacaktır.

ABSTRACT

INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY	
Thesis	Point of Information Security Perspective Analysis of Changes in Internet Data Centers, The World Situation and Suggestions for Our Country
Type	Technical Expert Thesis
Author	Lebibe YALÇINTAŞ
Submission Date	September 2013
Key Words	Information securtiy, Standard, Cyber attacks, Internet exchange point, data center
Advisor	Assoc. Prof. Aktül KAVAS
Total Page	ix + 116

Therefore the widespread use of computer technology, the use of a global world, people have become dependent on this technology, and society in many ways. This is the case with individuals under the influence of international relations, social life and also has a very significant losses.

The use of computers in all areas of life which consists of a world out there on the internet. The benefits of the people in this world we call cyberspace and amenities as well as unintended or malicious damage by the hands and disadvantages to the use of some of the faces will be kept. Terrorism to show up in this area on the internet to carry out the objectives of the attackers were in the world affects the regulation of cyber attacks.

In this study, the Internet and the risks and threats of cyber attacks, by drawing attention to the international information security, internet exchange point will be examined from the perspective of information security and data centers. As a result, the current situation in the country and solutions to create a new perspective on this issue will be studied.

TEŞEKKÜR

Tez çalışmam süresince yapmış olduğu katkı ve desteklerinden dolayı danışmanım Yrd. Doç. Dr. Aktül KAVAS'a, Kurum Başkanlarıma, Bölge Müdürümüz Sayın İsmail KARAYILAN'a, tezimin tüm süreçlerinde yardımlarını esirgemeyen TİB İletişim Uzman Sayın Mustafa DEMİREL'e, anlayış ve yardımlarını esirgemeyen değerli çalışma arkadaşlarıma, benden sabır ve desteğini esirgemeyen eşime teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AB	Avrupa Birliği (European Union (EU))
AMS-IX	Amsterdam İnternet Değişim Noktası (The Amsterdam Internet Exchange)
AS	Otonom Sistemler (Autonomous Systems)
AT&T	Amerikan Telefon ve Telgraf Şirketi (American Telephone and Telegraph Company)
BCM	İş Sürekliliği Yönetim Sistemi (Business Continuity Management)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGP	Sınır Geçiş Protokolü (Border Gateway Protocol)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIX.BG	Bulgaristan İnternet Değişim Noktası (Bulgarian Internet Exchange)
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BSI	İngiliz Standartlar Enstitüsü (British Standards Institute)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CDN	Küresel İçerik Sağlayıcı (Content Delivery Networks)
COBIT	Bilgi Teknolojisi ve İlgili Teknolojilere İlişkin Kontrol Hedefleri (The Control Objectives for Information and related Technology)
DAE	Avrupa için Sayısal Gündem (Digital Agenda for Europe)
DDoS	Dağıtık Servis Engelleme Saldırısı (Distributed Denial of Service Attack)
DE-CIX	Frankfurt İnternet Değişim Noktası (German Internet Exchange)
DoS	Servis Aksatma (Denial of Service)
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency)
GZFT	Güçlü yanlar, Zayıf yanlar, Fırsatlar, Tehditler

HLEG	ITU Yüksek Seviyeli Uzmanlar Grubu (High Level Experts Group)
ISO/IEC	Uluslararası Standardizasyon Kuruluşu (International Organization for Standardization)/ve Uluslar arası Elektroteknik Komisyonu (International Electrotechnical Commission)
ISP	İnternet Servis Sağlayıcı (Internet Service Provider)
IT	Bilgi Teknolojileri (Information Technologies)
ITIL	Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technology Infrastructure Library)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
ITU-IMPACT	ITU Siber Saldırılara Karşı Uluslararası Çok Taraflı Ortaklık (International Multilateral Partnership Aganist Cyber Threats)
ITU-T	ITU Telekomünikasyon Standartlaştırma Birimi (ITU Telecommunication Standardization Sector)
IXP	İnternet Değişim Noktası (Internet Exchange Point)
İDN	İnternet Değişim Noktası
İSS	İnternet Servis Sağlayıcı
İSYS	İş Sürekliliği Yönetim Sistemi
KKP	Kurumsal Kaynak Planlama
LINX	Londra İnternet Değişim Noktası (London Internet Exchange)
MTPoD	Maksimum kabul edilebilir kesinti süresi (Maximum Tolerable Period of Disruption)
OECD	Ekonomik Kalkınma ve İşbirliği Örgütü (The Organisation for Economic Co-operation and Development)
PNS	Sınır Ağ Güvenliği (Perimeter Network Security)
PP	Tam Yetkili Temsilciler Konferansı (Plenipotentiary Conference)
PUKÖ	Planlama-Karar verme- Uygulama-Önlem alma
RPO	Kabul edilebilir veri kaybı (Recovery Point Objective)
RTO	Hedeflenen kurtarma süresi (Recovery Time Objective)
SOME	Siber Olaylara Müdahale Ekipleri

TADOC	Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı (Turkish International Academy against Drugs and Organized Crime)
TNAP	Türkiye Network Altyapı Platformu
TÜRKAK	Türk Akreditasyon Kurumu
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
UKAS	Birleşik Krallık Akreditasyon Hizmetleri
US-CERT	Amerikan Bilgisayar Acil Durum Hazırlık Takımı (United States-Computer Readiness Team)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
WSIS	Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society)
WTDC	Dünya Telekomünikasyon Kalkınma Konferansı (World Telecommunication Development Conference)
WTSA	Dünya Telekomünikasyon Standardizasyon Genel Kurulu (World Telecommunication Standardization Assembly)

GİRİŞ

Bilgi Teknolojileri ve iletişim alanında son yıllarda yaşanan gelişmeler, birçok teknolojinin bir arada kullanılmasını ve ortak altyapılar üzerinden bilgi teknolojileri ve haberleşme hizmetlerinin sunulması gerekliliğini gündeme getirmektedir.

Küresel rekabetin oluşmasında kullanımı yaygınlaştıkça belirleyici unsurlardan biri olan Bilgi ve İletişim Teknolojileri (BİT) altyapısı; alternatif yapı ve hizmetlerin sunumu ile bilgiye uygun maliyetli, hızlı, etkin, yaygın ve en önemlisi de güvenli bir şekilde ulaşılması ile gerçekleşmektedir.

Çağımızda ülkelerin Bilgi ve İletişim Teknolojilerini benimseyip üretir hale gelmesi vazgeçilmez bir şart olmaktadır. Ancak BİT sektörünün bu kadar hızlı büyümesi, yaşamımızın ayrılmaz bir parçası olması, bu sektör üzerinden yapılan saldırı, risk ve tehditler önem kazanmaktadır. BİT sektöründe Bilgi Güvenliği kavramı ve bunun için yapılması gereken faaliyetler öne çıkan önemli bir konu haline gelmiştir. Tüm dünyada BİT gelişimi ve güvenliği konusunda bir dizi tedbirler, önlemler ve planlamalar yapılmaktadır.

Bu kapsamda 2010 yılında hazırlanan Avrupa 2020 Strateji Planında yer alan yedi temel girişiminden biri olan Avrupa Sayısal Gündemi (Digital Agenda for Europe, (DAE)) kapsamında Avrupa'nın arzu edilen hedefe ulaşmasını engelleyen sorunların içerisinde "*Artan siber suçlar ve internette tüketici güvenliğinin düşüklüğü ile fiber internet altyapısına yönelik yatırımın eksikliği*" hususları yer almaktadır (EC.EUROPA, 2013).

Bu sorunların çözümü Avrupa Sayısal Gündeminin ana hedefini oluşturmaktadır.

Ülkemizin 2007-2013 yıllarını içeren Dokuzuncu Kalkınma Planı'nın vizyonu "*İstikrar içinde büyüyen, gelirini adil paylaşan, küresel ölçekte rekabet gücüne sahip, bilgi toplumuna dönüşen ve AB'ye üyelik için uyum sürecini tamamlamış bir Türkiye*" olarak tanımlanmaktadır (EKUTUP, 2013).

Dokuzuncu Kalkınma planı içerisinde belirlenen "Bilgi ve İletişim Teknolojilerinin Yaygınlaştırılması" hedefi Bilgi Teknolojileri ve İletişim Kurumu (BTK)'nin faaliyetleri içerisinde de yer almaktadır.

Ayrıca Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)'nın yayınladığı 2009-2013 Stratejik planında, BİT sektörü için belirlenen stratejik amaç ve hedeflerin gerçekleştirilmesinde, BTK ilgili kurum olarak yer almaktadır (BTK, 2013, s.24).

Ulaştırma, Denizcilik ve Haberleşme Bakanlığınca düzenlenen 10. ve 11. şuralarda 2023 yılına kadar öncelik kazanacak projelerde ve BTK'nin 2013-2015 Stratejik Planı'nda da yer alan başlıklarda "*Ülke genelinde fiber optik ağların kurulması ve Türkiye'nin bölge ülkeler arasında fiber kesişim noktası olması*" ve "*Kişisel verilerin yasa dışı ve kötü amaçlı kullanımını önleyecek düzenlemelerin geliştirilmesi*" bulunmaktadır (BTK, 2013, s.25,27).

Türkiye BİT sektörü için yapılan Güçlü yanlar, Zayıf yanlar, Fırsatlar ve Tehditler (GZFT[1]) analizinde fırsatlarımız olarak, "*ülkemizin coğrafi yapısından kaynaklanan güneyinde ve doğusunda yeni gelişmekte olan dış pazarların olması, BİT sektöründe başta fiber altyapı olmak üzere altyapı yatırımlarına yoğun ilginin bulunması*" görülürken, "*siber tehditlerin giderek artması ve güvenlik sorunları*" tehditlerimiz içerisinde yer almaktadır (BTK, 2013a, s.32, 33).

Ülkemizde uluslararası ölçekte bir İnternet Değişim Noktası (Internet Exchange Point (IXP/İDN)) ve Veri Merkezi altyapısının kurulmasının; bilgi güvenliği ve siber tehditler açısından öneminden bahsedilmektedir. BİT sektörünün hızlı gelişimi, gerek kişisel gerekse kurumsal iş süreçlerinde internetin yoğun kullanımından kaynaklanan trafik ve veri artışı önümüzdeki süreçte bu alt yapıları daha da önemli hale getirecektir. Dünyadaki siber tehditlere karşı daha etkin bir koruma sağlamak bu alt yapıların kurulumunu gerekli kılacaktır.

[1] GZFT Analizi: Bir projede ya da bir ticari girişimde kurumun, tekniğin, sürecin, durumun veya kişinin güçlü ve zayıf yönlerinin belirlemekte, iç ve dış çevreden kaynaklanan ve fırsatları saptamak için kullanılan stratejik bir tekniktir.

Ulusal bir İDN'nin kurulması ile ülke adına, başta siber güvenliğin sağlanması olmak üzere, internet altyapısının gelişmesi, bağlantı hızının artması, maliyetlerin azalması ve hizmet kalitesinin artması yönünde önemli katkı sağlayacaktır. Bununla birlikte küresel içerik sağlayıcılar (Content Delivery Network, (CDN)) ve bölgesel İnternet Servis Sağlayıcı (Internet Service Provider, (ISP/İSS))'ler için alternatif bir bağlantı noktası oluşturması gibi kısa ve uzun vadede çeşitli avantajlarıda beraberinde getirecektir.

Bu tez çalışmasında internet değişim noktaları ve veri merkezlerinin kurulumunun siber güvenliği sağlanmasındaki rolü ve öneminden bahsedilmekte, ayrıca ülkemizde ulusal bir İDN altyapısı oluşturulmasının sağlayacağı katkıların neler olduğu açıklanmaktadır. İDN ve veri merkezleri arasındaki ilişki, Dünyadaki internet değişim noktaları ve veri merkezleri anlatılmaktadır. Bu konuda ülkemizde yapılan çalışmalardan ve mevcut durumdan yola çıkılarak ulusal bir İDN altyapısının oluşturulması için önerilerde bulunulmaktadır. Bu çalışmanın, ülkemizde kurulacak büyük ölçekli İDN alt yapısına dair sağlıklı bilgiler içermesi için bilimsel kaynaklar, tezler, makaleler, uluslararası kuruluşların resmi internet siteleri, UDHB'nın raporları, BTK'nin veri tabanı ve yayınlaşmış uzmanlık tezleri, 2013-2015 Stratejik Planı, kanun ve yönetmelikler esas alınmıştır.

Girişi takiben tezin birinci bölümünde; bilgi güvenliğinin öneminden ve temel unsurlarından bahsedilmektedir. Bilgi güvenliği sürekliliği açısından kullanılan uluslararası standartlar anlatılmakta, ayrıca Bilgi Güvenliği Yönetim Sistemi (BGYS) hakkında bilgi verilmektedir.

İkinci bölümde; siber riskler ve siber güvenlikten yola çıkılarak, siber saldırı çeşitleri ve yöntemleri hakkında bilgi verilmektedir. Bilgi güvenliği açısından siber riskler ve ülkemizdeki mevcut durum anlatılmaktadır. Bu bölümde ayrıca siber güvenlikte uluslararası kuruluşların kararları ve ülkemizdeki mevcut mevzuattan bahsedilmektedir.

Üçüncü bölümde; internet değişim noktası ve veri merkezi kavramları, aralarındaki ilişki ve internet değişim noktası altyapısı anlatılmaktadır. İnternet değişim noktası ve veri merkezine sahip olmanın bilgi güvenliği açısından önemi ve sağladığı diğer avantajlardan da bahsedilmektedir.

Dördüncü bölümde; dünyadaki önemli internet değişim noktalarından örnekler ile Ülkemizdeki internet değişim noktası, veri merkezi uygulamaları ve bu konuda yapılan çalışmalar ile bundan sonraki süreçte yapılması gerekenler hakkında bilgi verilmektedir.

Tezin son bölümü olan sonuç ve öneriler kısmında; daha önceki bölümlerde anlatılan konulardan yola çıkılarak, Türkiye'de oluşturulacak internet değişim noktası altyapısı için bir model önerisinde bulunulmaktadır.

1. BİLGİ GÜVENLİĞİ KAVRAMI

Bilginin korunması ve gizliliği kurum ve işletmeler için her geçen gün daha önemli hale gelmektedir. Bu bağlamda güven ortamının yaratılması stratejik açıdan önem taşımaktadır. Güvenlik problemleri, iş devamlılığını engelleyerek kurumların itibar kaybetmesine, pazar kaybına, müşteriler ve iş ortakları karşısında güven yitirmesine neden olmaktadır (Çetinkaya, 2008, s.10). Bilgi güvenliğinin sağlanması için gerekli tedbirleri almayan, güvenlik ihlalleri konusunda çalışanlarında farkındalık oluşturmayan kurum ve işletmelerde oluşabilecek itibar kaybı ve maddi kayıplar, yapılacak yatırımlardan daha da büyük olmaktadır (Doğantimur, 2009, s. 7,8).

1.1. Bilgi Güvenliğinin Önemi

Kurumlar, verimlilik ve etkinliklerini arttırmak üzere bilgisayar teknolojileri ve iletişim ağları kullanımına ağırlık vermektedir. Bu durum da bilgi güvenliğinin önemini gündeme getirmekle birlikte pek çok güvenlik sorununu da beraberinde getirmektedir (Demir, 2005, s.147,156).

Kurum faaliyetlerinin elektronik ortama taşınmasıyla Kurumsal Kaynak Planlama (KKP) ve e-iş fonksiyonlarını bir araya getirmekte ancak bu gelişmelerle birlikte güvenlik teknolojilerinin önemi gündeme gelmektedir (Demir, 2005, s.147,156).

Bilgi güvenliği; bilginin tehlike ile karşılaşıldığı durumlarda kaybın en aza indirilmesi, firmaların kaynaklarının her koşulda gizliliğinin, ulaşılabilirliğinin ve bütünlüğünün korunmasını amaçlamaktadır. ISO/IEC 27002 standardı bilgi güvenliği bakış açısıyla hazırlanmış bir standarttır.

Bir kurumun ISO/IEC 27001 sertifikasına sahip olması; %100 seviyesinde bilgi güvenliğinin sağlanması anlamına gelmemekte olup kurumun kritik bilgi varlıklarını tanımladığı, güvenlik risklerini bildiği ve çalışanlarının bilgi güvenliği farkındalığı içerisinde olduğu anlamına gelmektedir. Bu standardı

edinemeyecek kadar pahalı bulan kurum ve işletmeler, beraberinde bir takım güvenlik risklerini de göze almışlar demektir (Çetinkaya, 2008, s.11).

Kurumların etkin bilgi güvenliği sağlamak adına kendi risk yönetimi metodolojilerini belirlemeleri gerekmektedir. Kurumsal değerlerin korunması, etkinlik ve verimliliğin sağlanabilmesi için yapılan yatırımların denetlenmesi ve kontrol edilmesi gerekmektedir. Bir kurumun güvenlik standartları kapsamında; bilgi güvenliği politikası ve diğer güvenlik ile ilgili süreçlerini oluşturması ve işletmesi gibi sorumlulukları bulunmaktadır. Bunlar; risk yönetimi ve risk işleme planları, görev ve sorumlulukları, iş devamlılığı planları, acil durum olay yönetimi süreçleri ve uygulamada bunların kayıtlarından oluşmaktadır. Kurumun yukarıda bahsedilen bilgi güvenliği misyonunu içeren bir bilgi güvenliği politikasına ve bu politikayı destekleyen süreç tanımlarına sahip olması gerekmektedir.

Kurum personelinin bilgi güvenliği ve siber tehditler konusunda eğitilmesi ve maksimum düzeyde bilgi güvenliği farkındalığına sahip olması sağlanmalıdır. Kurulacak Bilgi Güvenliği Yönetim Sistemi içerisinde ölçülebilir kontrol hedeflerinin belirlenmesi, belirlenen amaca uygunluğunun kontrol edilmesi ve kurumun üst yönetimine periyodik olarak raporlanması gerekmektedir. Kurulan Bilgi Güvenliği Yönetim Sistemi kurum için belirlenen süreç ilişkisine göre yaşatılması ve performansının sürekli takibinin yapılması gereklidir. Bu da ancak yönetimin aktif desteği ile olabilmektedir (Çetinkaya, 2008, s.13).

Bilgi teknolojileri kullanımıyla yaşanan bilgi güvenliği sorunları zamanla kullanılan ağ ve sistemler üzerinde diğer sistemleri ve kullanıcıları olumsuz yönde etkilemeye başlamıştır. Kurum çalışanlarının bilgisayar ve BİT ile yeniliklere, yeni yazılımlara, değişik işleri kolaylaştıran programlara ayak uydurmaya çalışması, güvenlik açıklarını da beraberinde getirmektedir. Bu durum bilgi güvenliği tedbirlerinin alınmasını ve yazılım güvenliği merkezinin devreye girmesini gerektirmektedir. Ağ ortamlarında çalışan kişiler ve diğer uygulamalar tarafından ulaşılan uygulama yazılımlarındaki güvenlik açıkları, kurumlarda kurumsal bilgi güvenliği tehditlerinde ilk sırayı almaktadır.

Özellikle internet ortamında çalışan yazılımlar güvenlik açısından daha çok tedbir alınmasını gerektirmektedir. Buna rağmen esneklik ve kullanım kolaylığı altında birçok eklentiler yapılmakta ve güvenlik göz ardı edilmektedir. Ağ ve sistem güvenliğinin sağlanması için geliştirilen yöntemleri başarı ile uygulayan kurumlarda Sınır Ağ Güvenliği (Perimeter Network Security, (PNS)[1]) kavramının önemi çok iyi anlaşılmıştır.
Başlıca yazılım güvenliği tehditleri şöyledir:

- Çevresel değişkenler,
- Bellek taşmaları,
- Enjeksiyonlar,
- Güvensiz ağ ve haberleşme ortamları,
- Varsayılan sistem ayarları,
- Programcı arka kapıları

Amerikan Bilgisayar Acil Durum Hazırlık Takımı (United States-Computer Readiness Team, (US-CERT)) tarafından açıklanan güvenlik açıklarına göre;

2004 yılında 3.780
2005 yılında 5.990
2006 yılında 8.064
2007 yılında 3.907 adet saldırı rapor edilmiştir (Vural ve Sağıroğlu, 2007, s.507,522).

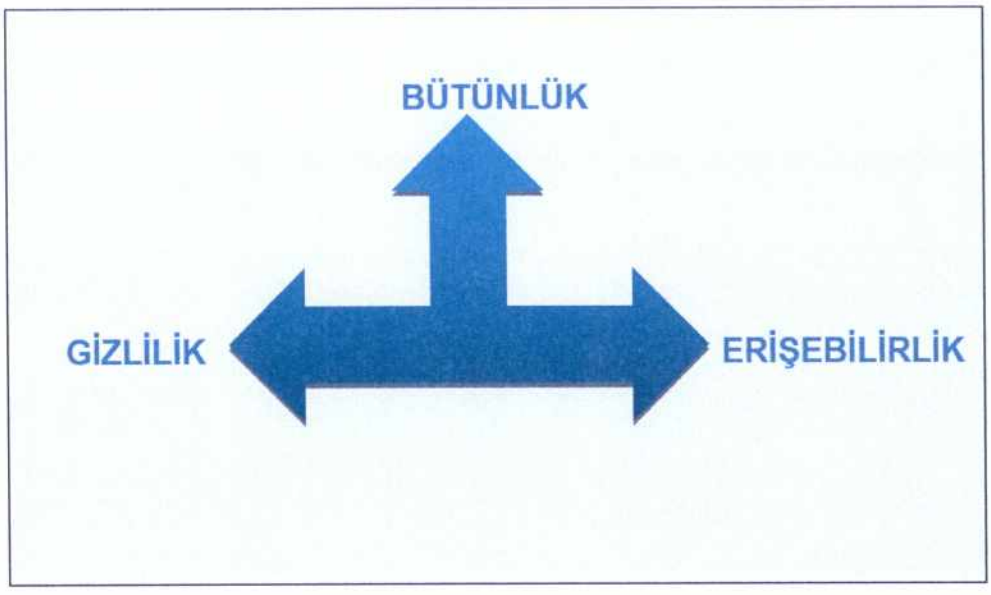
1.2. Bilgi Güvenliği Unsurları

Bilgi güvenlik politikaları ve bilgi güvenliği süreçleri her kuruma göre değişiklik göstermektedir. Her kurum kendi hedeflerine uygun bilgi güvenliği politikasını oluşturmaktadır. İzlenecek politikanın kuruma özgü ve kurumun ihtiyaçlarına göre oluşturulması gerekmektedir (Doğantimur, 2009, s.28). Buna göre bilgi güvenliği temel unsurları aşağıdaki gibi sınıflandırılabilmektedir;

[1] PNS (Perimeter Network Security): Güvenlik politikasında tanımlanan iletişim kuralları ile ağa ve kaynaklara erişim, tüm giriş-çıkış noktalarında kontrol edilerek saldırılardan korunma sağlanır

- Gizlilik
- Bütünlük
- Erişebilirlik

Şekil 1.1 Bilgi güvenliği temel unsurları



Kaynak: Doğantimur, 2009

1.2.1. Gizlilik

Gizlilik;

> *"Bilgi ve iletişim şebekeleri üzerinden yapılan haberleşmenin ya da bilgi ve iletişim sistemlerinde saklanan verilerin yetkisiz erişime karşı korunmasıdır"*

Buna göre; gizlilik açısından, güvenlik politikası yetkisi olmayanlara bilgi sızmasının ne zaman olabileceğini açıklamaktadır (Doğantimur, 2009, s.28). Kişisel verilerin iletilmesi ve işlenmesi işlemleri de güvenlik konusunda açıklığa sebep olmaktadır. Bu doğrultuda haberleşmenin gizliliğinin sağlanması da üzerinde durulması gereken ayrı bir konu olmaktadır. Bu

alanlarda bilgilerin gizliliğine ihtiyaç duyulmaktadır (Turhan, 2009, s.6). Hassas bilginin yetkisiz erişime karşı korunmasını, bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmek, gizlilik politikasının kapsamına girmektedir (Kayrak, 2012, s.155,163).

1.2.2. Bütünlük

Bütünlük; verilerin düzgün bir şekilde eksilmeden, bozulmadan muhafaza edilmesidir. Bütünlük kritik hassasiyete sahip alanlarda büyük önem arz etmektedir. Verilerin doğruluğunun hayati önem taşıdığı sağlık alanında, sanayi tasarımları ya da kimlik doğruluğunun önemli olduğu kurumlarda üzerinde önemle durulan bir konu olmaktadır (Turhan, 2009, s. 6).

Bütünlük açısından,

> *"güvenlik politikası bilginin hangi durumda, hangi yolla ve/veya kimler tarafından değiştirebileceğini tanımlar"* (Doğantimur, 2009, s.28).

Kayrak'a göre bilginin, tam, doğru ve kurumsal değerler ve beklentiler çerçevesinde geçerli olmasını, bilginin ve işleme yöntemlerinin doğruluğunu ve tamlığını temin etmek bilginin bütünlük politikası kapsamına girmektedir (Kayrak, 2012, s.155,163).

1.2.3. Erişebilirlik

Erişilebilirlik; verilere her durumda ulaşılabilmenin sağlanmasıdır. Enerji kesintileri, doğal afetler, kazalar, sistem kesintileri ya da saldırılar gibi olağanüstü durumlarda bile verilerin erişilebilir olması ve hizmetlerin aksaklığa uğramadan sunulmaya devam edilmesi gerekmektedir. Bunu sağlayacak araç ve kaynakların korunması, yetkili kullanıcıların gerek duyulan bilgi ve ilişkili kaynaklara ulaşabilmesinin garanti edilmesi "Erişebilirlik" politikasının kapsamına girmektedir (Kayrak, 2012, s.155,163). Örneğin haberleşme şebekelerinde yaşanan problemler hava taşımacılığı gibi önemli hizmet alanlarında telafi edilemeyecek zararlara yol

açabilmektedir. Bu gibi durumlarda verilere erişebilirliğin de önemi ortaya çıkmaktadır (Turhan, 2009, s.6).

1.3. Bilgi Güvenliği Standartları

Bilgi güvenliği süreçlerinin uygulanma ve yönetilme sürecinde, kurumsal plan ve uygulamaların geliştirilmesinde uluslararası kabul görmüş yöntemlerin kullanılması gerekmektedir (UDHB, 2013, s.16).

Kurumsal bir kimliğe sahip olmak isteyen kuruluşlar için, faaliyet gösterdikleri alanların her biri ile ilgili, o alandaki uluslararası standartların belirlemiş olduğu kurallara uyumlu olmak çok önemlidir (Şahinaslan, 2011, s.569).

Mevcut bulunan uluslararası bilgi güvenliği standartları incelendiğinde *"ISO/ IEC 9001, ISO/IEC 27001, ISO/IEC 27005, RISK IT, ISO/IEC 31000, AS/NZS 4360:2004, FISMA, NIST SP 800–53, PCI, PMI, CMMI, SPICE, ITIL, COBIT gibi standartlar mevcuttur. Bunların bir kısmı doğrudan bir risk yönetim standardı iken ISO/IEC 9001, PCI, CMMI, SPICE, PMI, ITIL, COBIT, HIPAA"* standartların kendisi bir risk yönetim standardı olmamakla birlikte risk yönetimi ile de ilgilidir (Şahinaslan, 2011, s.569).

Bilişim sistemleri stratejisinde, bilişim sistemleri yönetimi, teknoloji, veri ve uygulamaya ilişkin durumlar, dünyada ve Ülkemizde de genel kabul görmüş standartlara uygun olarak düzenlenmiştir. COBIT çerçevesi ile uyumlu bir şekilde inşa edilen stratejinin bilgi güvenliği ve hizmet yönetimine ilişkin kısımlarında diğer standartlardan yararlanılmıştır (Kayrak, 2012, s.204).

1.3.1. Bilgi Güvenliği Yönetimi ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı

İletişim ortamlarının yaygınlaşması ve kullanımının artmasına paralel olarak bilgi güvenliğinin önemi de artmıştır. Güvenlik duvarları, saldırı tespit sistemleri, anti virüs yazılımları, şifreleme, vb. teknik önlemler kurumsal bilgi güvenliğinin sağlanması için yeterli olmamaya başlamıştır. Bu sebeple

kurumların üst yönetimleri tarafından kritik bilgi varlıklarını ve çalışanlarını içerecek bilgi güvenliği yönetim sistemlerinin olması gerekliliği ortaya çıkmıştır. Oluşturacak BGYS kurum veya kuruluşların bilgi güvenliği, iş sürekliliği gereksinimlerini karşılamalı ve üst yönetim tarafından destelenecek hedeflere uygun olarak kurulması gerekmektedir (Doğantimur, 2009, s.11,12).

Önel ve Dinçkan'na göre;

> *"Bilgi Güvenliği Yönetim Sistemi BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır."*

temel amacın, kurum için önemli olan bilginin korunması olduğu belirtilmiştir. (Önel ve Dinçkan, 2007, s.6).

Bilgi Güvenliği Yönetim Sistemi (BGYS), bilgi güvenliğinin en önemli bölümüdür. Bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanmasına yönelik standartları belirlemektedir. Bu bakış açısıyla siber güvenlik ile ilgili uygulamalara bir standart getirmektedir.

Bilgi güvenliği standardı ilk defa 1995 yılında İngiliz Standartlar Enstitüsü (British Standards Institute, (BSI)) tarafından çıkarılmış ve BS 7799 standardına dayanmaktadır. Söz konusu standart 2000 yılında Uluslararası Standardizasyon Kuruluşu (International Organization for Standardization, (ISO)) tarafından ISO/IEC 17799 olarak yayımlanmıştır. ISO/IEC 17799 en son 2005 yılında güncellenmiş ve 2007 yılında da ISO/IEC 27002 adını almıştır.

BGYS'nin uygulanmasına ilişkin hususları kapsayan standart "BS 7799-2" 1999 yılında yayımlanmıştır. Söz konusu standart ISO tarafından 2005 yılında ISO/IEC 27001 standardı olarak kabul edilmiştir (UDHB, 2013, s.13,19).

ISO/IEC 27001, BGYS için gereklilikleri belirleyen bir standarttır. Bilgi ihlallerinin tanımlanıp, yönetilmesini ve bunların minimize edilmesini sağlamaktadır. Bu standart; ISO 9001, ISO 14001 yönetim standartlarıyla uyumlu olarak geliştirilmektedir. Dolayısıyla yönetim standartlarının gereklerini de yerine getirmektedir (Vural ve Sağıroğlu, 2007, s.507,522).

TS ISO/IEC 27001 standardına göre oluşturulmuş BGYS,

> *"bilgi sistemlerini, bilgi ağları ve bilgi sahiplerini bilgisayar destekli sahtekârlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi çok geniş kaynaklardan gelen tehdit ve tehlikelerden korumayı amaçlamaktadır"* (UDHB, 2013, s.13,19).

Bu standart bilginin gizliliği ve güvenilirliği ile birlikte, ilgili kurum ve işletmeleri rekabet gücü, kârlılık gibi konularda da olumlu yönde etkileyerek, yasal yükümlülüklerin ve ticari prestijin korunması ve sürdürülmesini sağlamaktadır (UHD, 2013, s.13,19). ISO/IEC 27001 yalnızca bilgisayar, bilişim güvenliği ve süreçlerin güvenliği olarak algılanmamalıdır, aynı zamanda basılı dokümanların güvenliği ile uygulanan süreçlerin de güvenliğini kapsamaktadır.

> *"Bilgi Güvenliği Yönetim Sistemi" (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanan ISO/IEC 27001 standardı süreçlerinin güvenliğini sağlamayı hedefleyen bir bilgi güvenliği standardıdır"* (Doğantimur, 2009, s.12,15).

Tüm kuruluş türlerini kapsayan BGYS,

> *"ihtiyaca göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtmektedir"* (Doğantimur, 2009, s.12,15, Çetinkaya, 2008, s.15).

ISO/IEC 27001 ve ISO/IEC 27002 standartları doğrudan bilgi güvenliği konusu ile ilgilenmektedir. Ayrıca çok teknik ve teknolojik bir standart değildir.

Belli bir ürün veya bilgi teknolojisi ile ilgilenmez, sadece bilgi güvenliği ile ilgilenir (Önel ve Dinçkan, 2007, s.6).

BGYS'nin tasarımı ve gerçekleştirmesi, kuruluşun ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan süreçler, kuruluşun büyüklüğü ve yapısına göre şekillenmektedir. BGYS'de girdilerden çıktı elde edimine kadar süren her faaliyet süreç olarak kabul edilmekte, yani süreç yaklaşımı hâkim olmaktadır. (Doğantimur, 2009, s.15).

Bu standart, kullanıcılarını şu konularda bilgilendirmektedir:

- Bilgi güvenliği ihtiyaçlarını ve bilgi güvenliği için politika ve hedeflerin belirlenmesi ihtiyacını anlamak,
- Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
- BGYS'nin performans ve etkinliğini izlemek ve gözden geçirmek,
- Nesnel ölçmeye dayalı olarak sürekli iyileştirmek (Doğantimur, 2009, s.15,18).

BGYS'nin yaşayan bir süreç olması için Planla-Uygula-Kontrol et-Önlem al (PUKÖ) döngüsünün olması gerekmektedir. ISO/IEC 27001 standardının PUKÖ modeli aşamaları şu şekilde özetlenelebilmektedir:

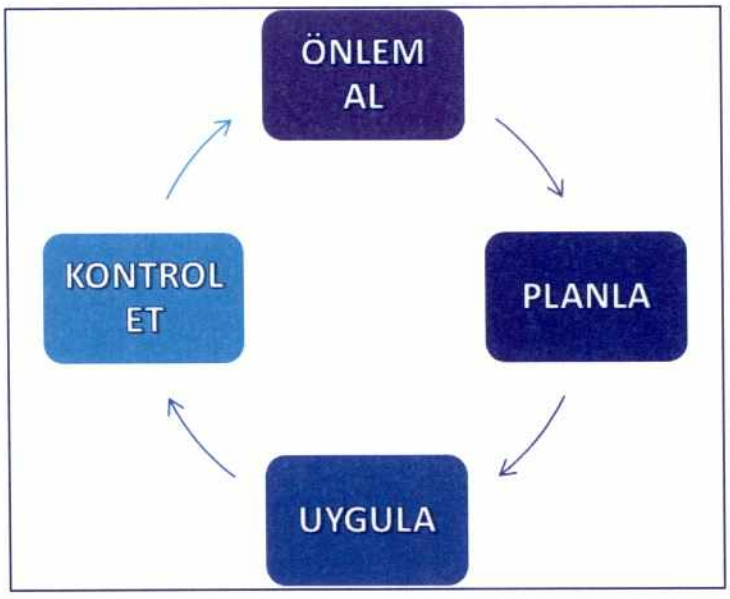
Planlama; Bu aşamada BGYS kurularak, sistemin politikası, amaçları, hedefleri, süreçleri ve prosedürleri oluşturulmaktadır.

Uygulama; BGYS'nin gerçekleştirilmesi ve işletilmesini yani, BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesini kapsamaktadır.

Kontrol et; BGYS'nin izlenmesi ve gözden geçirilmesini kapsamaktadır. Kullanım deneyimlerine göre süreç performansının değerlendirilmesini, uygulama sonuçlarının ölçülmesini ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesini ifade etmektedir.

Önlem al; sürekliliğin sağlanması ve sistemin iyileştirilmesi açısından, yönetimin kontrolleri sonrasında gelen sonuçlar doğrultusunda, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesini sağlamaktadır (Doğantimur, 2009, s.15,18). Yaşanabilecek olumsuzluklara engel olmak için değişen riskler göz önünde bulundurularak önleyici tedbirler alınmakta, karşılaşılabilecek sorunlara karşı önceden hazırlıklı olunmaktadır. Bunun yanı sıra BGYS olumsuzlukları gidermek üzere düzeltici tedbirleri de içermektedir. Önleyici tedbirler için gerçekleştirilen faaliyetler çoğunlukla düzeltici tedbirler için gerçekleştirilen faaliyetlerden daha az maliyetli olmaktadır (Vural ve Sağıroğlu, 2007, s.507,522).

Şekil 1.2. ISO/IEC 27001 PUKÖ döngüsü



BGYS'nin kurulması ile kurumlarda varlık envanteri belirlenmekte, belirlenen varlıklara karşı olası risk ve tehditler tespit edilerek güvenlik politikaları ve süreç prosedürleri oluşturulmaktadır. Uygulama ve birbirini tamamlayan denetimler sonrasında sistemin iyileştirilmesine yönelik olarak, uygun çözümlerin geliştirilmesi, düzeltici-önleyici-iyileştirici faaliyetlerin gerçekleştirilmesi sağlanmaktadır (Doğantimur, 2009, s.15,18).

ISO/IEC 27001 standardı ile kurulan BGYS, kurumların risklerini belirleyip yönetmesini, iş sürekliliği ve önemli bilgilerini korumasını sağlamaktadır. Kurumun kendisinde motivasyon duygusunu kuvvetlendirirken, kurumun iç ve dış paydaşlarında da bir güven duygusu oluşturmaktadır. Daha verimli ve güvenli bir çalışma ortamı oluşturularak, bilgilerin sistematik bir yaklaşım içerisinde güvenliği sağlanmış olmaktadır (Doğantimur, 2009, s. 12,15).

ISO/IEC 27001 standardına göre BGYS kurulum adımları ve sistem belgelendirmesine sahip olmak isteyen kuruluşların izlemesi gereken süreç;

- Kurumsal bilgi güvenlik politikalarının oluşturulması,
- BGYS kapsamının belirlenmesi,
- İnsan kaynağı ve stratejinin belirlenmesi,
- Eğitim ihtiyacının belirlenmesi ve farkındalık eğitimlerinin verilmesi,
- Bilgi varlıklarının saptanması,
- Bilgi varlıklarının gizlilik-bütünlük-erişim değerlerinin belirlenmesi,
- Risklerin belirlenmesi ve oluşturulacak risk yönetimi sürecine göre değerlendirilmesi,
- Sızma/ Entegrasyon/Teknik Uyum Testleri,
- Yüksek seviyede bulunan riskler için önleyici faaliyetlerin belirlenmesi,
- Kontrollerden istenen güvence derecesinin belirlenmesi,
- Kontrol hedeflerinin ve kontrollerin saptanması,
- Dokümantasyonun hazırlanması, onaylanması ve tüm çalışanlara yayınlanması,
- Prosedürler ve dokümanların uygulamaya alınması,
- İç Denetimlerin yapılması,
- Yönetimin kontrolüne sunulması,
- Belgelendirme için başvuru ve
- Belgelendirmenin gerçekleşmesi

olarak sıralanmaktadır (UDHB Şurası, 2013, s.16,19,), (Vural ve Sağıroğlu, 2007, s.507,522).

Şekil 1.3. BGYS'de kritik süreç çıktıları

ISO/IEC 27001 standardı kapsamında belgelendirme hizmeti veren kuruluşlar Türk Akreditasyon Kurumu (TÜRKAK), Birleşik Krallık Akreditasyon Hizmetleri (UKAS)'dir ve verdikleri belgeler uluslararası geçerliliğe sahiptir.

Belgelendirilmiş ISO/IEC 27001 BGYS standardının en önemli yaklaşımlarından biri belgenin üç yıl için verilmesi ve her yıl bu belgenin denetimle doğrulanmasıdır (UDHB Şurası, 2013, s.16,19).

1.3.2. BS 25999 İş Sürekliği Yönetim Sistemi standardı

BS 25999 standardı, doğal afet, sistem kesintisi ya da kaza gibi aksaklıkların yaşanması durumunda kurumlarda iş sürekliliğinin nasıl sağlanacağı konusunda oluşturulmuş bir yönetim sistemidir. BS 25999 İş Sürekliliği Yönetim Sistemi (Business Continuity Management, (BCM)) standardı, en iyi uygulamayı temel alan ve tüm "İş Sürekliliği Yönetim Sistemi" yaşam döngüsünü içine alan bir denetim kümesini kapsamaktadır.

İş sürekliliği çalışmaları; işletmenin iş süreçlerinde meydana gelen kesintiye ne kadar tahammül edebildiği ve kesintiye uğrayan süreç veya sistemleri bu süre içerisinde tekrar çalışır hale getirmek için yapılması gereken işlemlerden oluşmaktadır. İş Sürekliliği Yönetim Sistemi (İSYS) gerekliliklerini tarif eden BS 25999 standardı;

> *"İş süreçlerinin önceden tanımlanmış, kabul edilebilir bir düzeyde sürekliliğini sağlamak amacıyla, kuruluşun, olaylara ve iş kesintilerine karşı planlama ve müdahale etme konusundaki stratejik ve taktik kapasitesidir."*

şeklinde tanımlanmaktadır (Artıbel, 2013).

İşletmeler genellikle iş süreçlerindeki kesintileri engellemek, rekabet avantajı sağlamak, yasal yükümlülüklerini yerine getirmek, müşteri kayıplarını engellemek, kurum itibarını korumak, pazar payı kayıplarını engellemek için iş sürekliliği ile ilgilenmektedir. BSI'nin, 2006 yılında BS 25999 İSYS için Uygulama Prensipleri ve 2007 yılında BS 25999-2:2007 İSYS için gereklilikler standartlarını yayınlamış olması iş sürekliliği bilincinin arttığını göstermektedir. BS 25999 sayesinde, iş sürekliliğini anlama, geliştirme ve uygulama kolaylaşırken diğer kuruluş veya müşterilerle olan ilişkilerde de güven artışı olmaktadır (Artıbel, 2013).

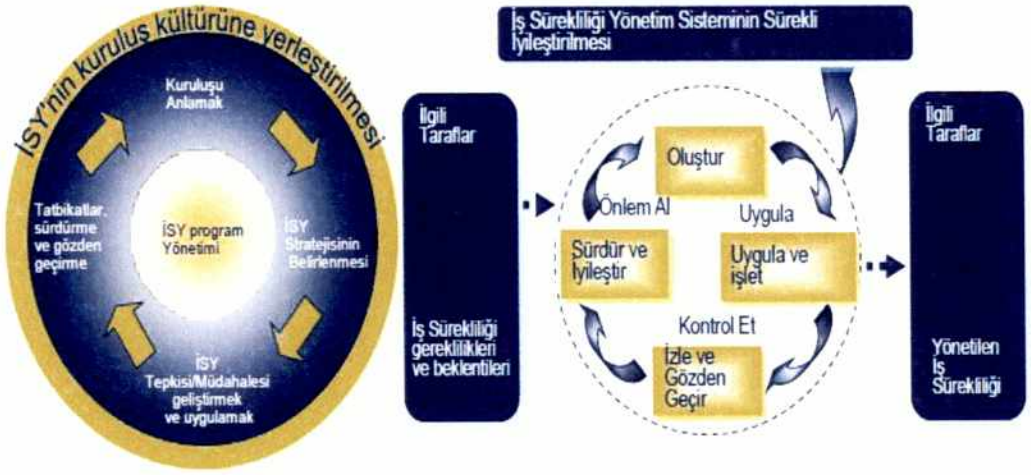
BS 25999, finans, telekomünikasyon, ulaşım ve kamu sektörü gibi yüksek risk içeren ortamlarda kullanılmaktadır (Artıbel, 2013).

BS 25999 standardının sağladığı faydalar aşağıda sıralanmıştır.

- Uluslararası kabul gören en iyi uygulamaları temel alan, ortak bir çerçeve sağlamakta,
- Karşılaşılabilecek iş kesintilerine karşı proaktif bir direnç kazandırmakta,
- Her hangi bir kesinti durumunda, kritik ürün ve hizmetlerin, tanımlı zaman aralıklarında, önceden kabul edilebilir olarak belirlenen seviyelerde kazanılması için bir geri çekme metodolojisi sunmakta,

- Kuruluşun iş kesintilerini yönettiğini kanıtlamakta,
- Saygınlık ve markayı korumakta,
- Yeni pazarlara açılma ve yeni müşteriler kazanılmasını sağlamakta,
- İlgili kanun ve yönetmeliklerin dikkate alındığını göstermekte,
- Denetimler sayesinde iş kesintisi ve sigorta primlerini düşürmektedir (Yıldırım, 2009, s.6,26).

Şekil 1.4. İş sürekliliği hayat çevrimi



Kaynak: Yıldırım, 2009, s.14

BS 25999 İSYS'nin başarıya ulaşabilmesi için üzerinde önemle durulması gereken konular 10 ana başlık altında ele alınmıştır.

- Üst Yönetim Desteği

İş sürekliliği çalışmaları için en yüksek seviyede yönetim onayı ve desteğinin alınması gerekmektedir. Üst yönetimin iş sürekliliği sürecine katılımının doğru olarak anlaşılması, desteklenmesi ve çalışanlar tarafından bu desteğin hissedilmesi ve organizasyon kültürüne adaptasyonu için önemlidir. Üst yönetim desteği sadece politika ve benzeri dokümantasyonun onaylanmasının yanı sıra; çalışmaların gözden geçirildiği toplantılara

katılmak, tatbikat sonuçlarını incelemek, yatırım kararı vermek bazı bilgilendirme notlarının veya çalışma sonuçlarının bizzat yönetim tarafından bildirilmesi şeklinde olmalıdır. Üst yönetim desteği ayrıca gerekli iş gücünün ayrılması, ihtiyaç duyulan bütçenin tahsis edilmesi gibi konular içinde oldukça önemli olmaktadır (Artıbel, 2013).

- Stratejik İş Planın Parçası Olma

BS 25999 iş sürekliliği kurumun stratejik hedefleri için gereklidir. Kurumun işlevini gerçekleştirmesi veya yasal yükümlülüklerini yerine getirebilmesi için her zaman güncel ve ihtiyaca yanıt verebilir durumda hazır olmak gerekmektedir. Aksi halde iş süreçlerinde kesintiler yaşanabilmektedir. Kuruluşun herhangi bir kesintinin ardından normal operasyonuna geri dönerek hizmetlerini eksiksiz verebilmesi ve bunu sağlayabilecek önlemleri önceden geliştirebilmesi gerekmektedir (Yıldırım, 2009, s.6,26).

- Eylem planları / görev listeleri,
- Kaynak gereksinimleri,
- Sorumlu kişi veya kişiler,
- Formlar ve Ekler (Yıldırım, 2009, s.6,26).

- İş Sürekliliği Organizasyonu

BS 25999 standardını yerleştirme çalışmalarında kurumun birçok bölümü ve birçok çalışanı çeşitli görevler almaktadır. Son kullanıcıların bile yapması gereken görev ve sorumluluklar bulunmaktadır. Bazı kurumlarda iş sürekliliği yönetimi için ayrı gruplar kurulmuştur. İSYS'nin kurum içinde yaşayabilmesi için gerekli personel gücü ve koordinasyonu sağlamak, olağan üstü durumlarda beklenen faydayı sağlaması açısından kritik olmaktadır. Bu konuda bir kurum kültürünün oluşturulması sürecin doğru işletilmesi açısından gerekmektedir.

- Risk Analizi ve İş Etki Analizi

Doğru bir İş Sürekliliği Yönetim Sistemi oluştururken, Risk ve İş Etki Analizi çalışmalarının çıktılarını kullanmak gerekmektedir. İş etki analizi çalışması sonucunda, kurum süreçlerinin kritikliği, süreçler için Hedeflenen Kurtarma Süresi (Recovery Time Objective, (RTO)[2]), Kabul Edilebilir Veri Kaybı (Recovery Point Objective, (RPO)[3]) ve Maksimum Kabul Edilebilir Kesinti Süresi (Maximum Tolerable Period of Disruption, (MTPoD)[4]) belirlenmektedir. Ayrıca risk analizi kullanılarak süreçlerde kesintiye neden olabilecek riskler belirlenmektedir.

- Yeterli Bütçe Ayrılması

İSYS'nin kurulumu ve işletimi sırasında bir takım giderler için bütçe ayrılması gerekmektedir. Kurulum aşamasında danışmanlık, eğitim ve benzeri hizmetlerin satın alınması, işletme sırasında gerekli insan kaynağının sağlanması bu giderlere örnektir. Bu sebeple iş etki analizinde belirlenen kabul edilebilir kesinti sürelerinin sağlanması açısından gerekli bütçenin ayrılması veya planlanması gerekmektedir (Artıbel, 2013).

- Yeterli Bilgi Teknolojileri Altyapısı

İş gereklilikleri nedeni ile birçok iş sürecinin bilgi teknolojileri ile doğrudan ilişkisi bulunmaktadır. Bilgi teknolojileri altyapısının süreklilik ihtiyaçlarına uygun olması, süreklilik ihtiyaçlarının karşılanması için oldukça önemlidir. Sunucuların, haberleşme hatlarının, enerji altyapısının yedekli yapıda alışması bilgi teknolojileri altyapısının sürekli hizmet verebilmesi açısından çok önem arz etmektedir (Artıbel, 2013).

---

[2] RTO: Hedeflenen Kurtarma Süresi: Kesintiye uğrayan iş sürecinin ne kadar süre sonra çalışır hale getirileceğine dair hedef süredir.

[3] RPO: Kabul Edilebilir Veri Kaybı: İş sürecinin ne kadar veri kaybı ile eski haline getirileceğine dair hedef süredir.

[4] MTPoD: Maksimum kabul edilebilir kesinti süresi; bir iş süreci veya bilgi teknolojileri bileşeni için kurumun kabul edebileceği maksimum kesinti süresini ifade etmektedir (http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/.../download, TÜBİTAK, UEKAE, İş Sürekliliği Yönetim Sistemi Kurulumu, s.6).

- Dokümantasyon

Her yönetim sisteminde olduğu gibi İSYS için de dokümantasyon önemlidir. İş sürekliliği planının, olağanüstü durum yönetim planının ve bu planlarla ilgili diğer talimat ve süreçlerin hazır, güncel ve ilgili çalışanların her zaman ulaşabileceği ortamda saklanması gerekmektedir. Dokümantasyon sade, kolay uygulanabilir olmalıdır (Artıbel, 2013).

- Periyodik tatbikatlar

Olağanüstü durumlar için hazır olunması ve çeşitli senaryolar üzerinde periyodik tatbikatlar yapılması yönetim sisteminin eksikliklerinin belirlenmesi açısından çok önemlidir. Tatbikat planlarının senelik olarak hazırlanması ve periyodik olarak yapılması, kurumun olası acil durum senaryoları için hazır olmasını sağlamaktadır. Tatbikatlar hazırlanan planların kısmi veya tamamının test edilmesi şeklinde olabilmektedir. Tatbikat sonrası değerlendirme raporu hazırlanarak, iş sürekliliği olgunluk seviyesinin arttırılması için gerekli adımlar belirlenmekte ve kurumun üst yönetimine raporlanmaktadır (Artıbel, 2013).

- Eğitim ve bilinçlendirme

BS 25999 standardı çerçevesinde; İş sürekliliği çalışmalarının benimsenmesi ve kurum farkındalığının artırılması açısından, tüm çalışanlara ve iş sürekliliği organizasyonunda bulunan takımlara eğitim verilmesi gerekmektedir. İş sürekliliği planı içerisinde eğitim konusunda izlenecek yöntemler belirlenir ve plan içerisinde yer alır. Eğitim faaliyetlerini yürütmek üzere bir organizasyon oluşturulması ve belirlenen zamanlarda eğitim faaliyetlerinin yürütülmesi sağlanır (Artıbel, 2013).

- Plan bakım ve güncelleme

Kurumun süreçlerinde meydana gelen değişiklikler iş sürekliliği planını doğrudan etkilemektedir. Süreç değişiklikleri plan güncellemesini beraberinde

getirmektedir. Zamanla ortaya çıkan değişikliklerin iş sürekliliği planına uyarlanması için periyodik olarak gözden geçirilmesi ve gerekli güncellemelerin yapılması gerekmektedir. Kurum süreçlerindeki kritik seviyelerin ve dolayısıyla hizmet veren sistemlerin önceliklerinin değişmesi, alınması gereken önlemleri de değiştirebilmektedir. Bunun sonucunda yeni yatırım gereksinimleri ortaya çıkabilmektedir. Sistem değişikliği gerektiren bu gibi durumlarda, bütçe ve zaman planının önceden öngörülerek hazırlanması gerekmektedir (Artıbel, 2013).

1.3.3. COBIT, ITIL ve diğer standartlar

COBIT, Bilgi ve İlgili Teknolojilere İlişkin Kontrol Hedefleri (The Control Objectives for Information and Related Technology) yaygın şekilde kullanılan bir modeldir. Bilgi teknolojilerinin süreçlerine dair çözüm önerilerine değil esas olarak kontrol hedeflerine ve yönetilmesine odaklanarak süreç içerisinde sağlanması gereken en iyi uygulamaları açıklamaktadır. Kontrol hedefinin her birinin beş ayrı olgunluk düzeyinde değerlendirildiği COBIT, etkinlik, verimlilik, bütünlük, devamlılık, uyumluluk ve güvenirlilik unsurlarını ön plana çıkarmaktadır (Kayrak, 2012, s,204).

COBIT hem bir denetim aracı, hem de yönetişim aracıdır. Bu nedenle yönetimden bilgi teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlamaktadır (UDHB Şurası, 2013, s.13,19).

1996 yılında yayımlanan COBIT, bilgi teknolojileri sistemlerini tanıma, anlama bilgi teknolojileri yönetişim modeline göre gerekli olan güvenlik ve kontrol seviyelerini belirlemekte kullanılmaktadır.
COBIT yöneticilere, denetçilere ve Bilgi Teknolojileri (BT) kullanıcılarına; iş hedeflerinin bilgi işlem hedeflerine dönüşümünü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirirken, aynı zamanda bilgi teknolojileri alt yapılarının da etkin kullanımını sağlamaktadır. İçerdiği stratejik bilgi teknolojileri planı, bilgi mimarisi, stratejiyi işletmek için

gerekli bilgi teknolojileri donanım ve yazılımları, sürekli hizmet sağlaması ve bilgi teknolojileri performansını izleme sistemi ile karar vermeyi kolaylaştırdığı için tercih edilmektedir. Kontrol, güvenlik ve süreç yönetimi güvencesi sağlaması ile bilgi teknolojileri kullanıcılarına, bilgi teknolojileri altyapısı içindeki sorunların belirlenmesinde de denetçilere yardımcı olmaktadır (UDHB Şurası, 2013, s.13,19).

COBIT, 34 adet üst düzey sürece sahiptir. Bunların kapsadığı 210 adet kontrol hedefi aşağıda verilen dört ana başlık içinde yer almaktadır.

- *Planlama ve Organizasyon*: Bu süreç kuruluşun temel sistem bileşenlerinin belirlenmesi, politikaların ve genel kuralların oluşturulmasını içermektedir. Bilgi teknolojileri süreç ve ilişkilerinin tanımlanması, yatırım, insan kaynakları, kalite, risk ve proje yönetimi süreçlerini kapsamaktadır (UDHB Şurası, 2013, s.13,19).

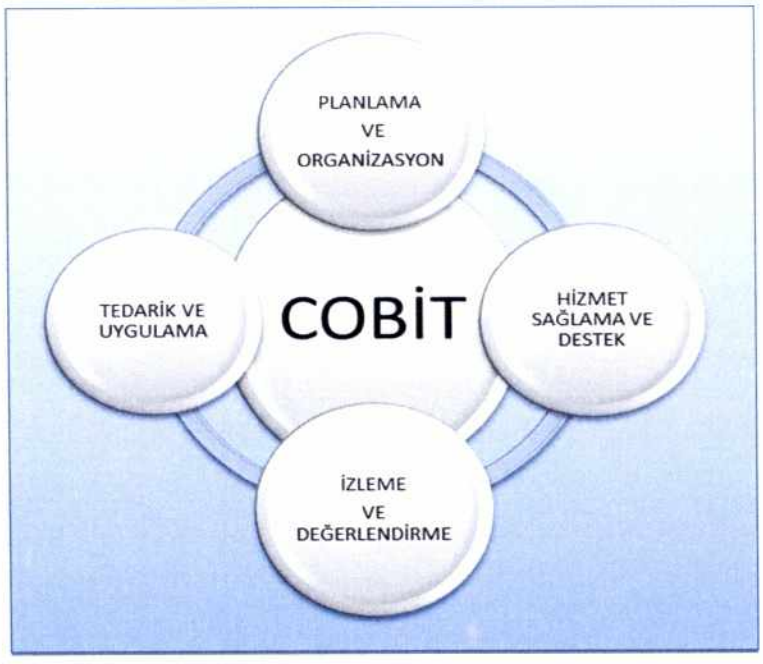
- *Tedarik ve Uygulama:* Tedarik ve uygulama süreç alanı, bilgi teknolojileri gereksinimlerini belirler, teknolojiyi tedarik eder ve kuruluşun mevcut iş süreçleri içinde uygulamasını yapar. Ayrıca, kuruluşun bilgi teknolojileri sistemi ve bileşenlerinin ömrünü uzatmak için bir bakım planı oluşturmaktadır (UDHB Şurası, 2013, s.13,19).

- *Hizmet Sağlama ve Destek:* Alınan hizmetlerin tanımlanması ve yönetimi kapsamında, performans ve kapasite yönetimi ile birlikte hizmet sürekliliği ve maliyetlerin belirlenmesini sağlamaktadır. Uygulamaların bilgi teknolojileri sistemi içinde yürütülmesi ve sonuçlarıyla olduğu kadar, sistemlerin etkili ve yeterli işletilmesine olanak sağlayan destek süreçlerini de kapsar. Destek süreçleri, kullanıcıların eğitimi, problem ve veri yönetimi ve sistem güvenliği konularını içermektedir (UDHB Şurası, 2013, s.13,19).

- *İzleme ve Değerlendirme:* Bu süreç alanı, bilgi teknolojileri sistemi tasarlanırken, belirlenen stratejilere göre kurum ihtiyaçlarının karşılanıp

karşılanmadığını ele almaktadır. Ayrıca bilgi teknolojileri sisteminin performansı izlenerek iç ve dış denetçiler tarafından etkinliğinin değerlendirilmesi ve gerekli mevzuat uyum çalışmalarının yapılmasını kapsamaktadır (UDHB Şurası, 2013, s.13,19).

Şekil 1.5. COBIT süreç alanları



ITIL, hizmet sunumu ve desteği süreçlerinden oluşan yönlendirici sekiz kitaptan oluşmaktadır. Süreç odaklı olup, bilgi işlem süreçlerini birbirleriyle ilişkilerinde uyum sağlatan özelliktedir. Prensipte kullanıcı memnuniyeti ön plandadır. Her türlü ölçekteki kurumda ve sektörde kullanılabilmesi ITIL'in avantajlı olan boyutudur (ITIL, 2008).

İş süreç yaklaşımı sayesinde ITIL, müşteri, tedarikçi, BT bölümü ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını sağlamaktadır. "En iyi uygulamalar / deneyimler" üzerine yapılandırılmış olan ITIL BT Servis Yönetimi ve dağıtımı süreçleri ile dünyada yaygın olarak kullanılmakta ve kabul görmüş bir standart olarak benimsenmektedir. ITIL, servis yönetimi ve sağlama süreçleri için en uygun başvuru kaynağıdır. Servis yönetimini en iyi

şekilde sürdürmek için yol gösteren ve kullanıcılarına servis sağlama süreçlerini ayrıntılı şekilde gösteren bir kitap kümesi olmaktan çıkmış, dünyaca kabul gören yöntemler dizisine dönüşmüştür (ITIL, 2008).

- *Uluslararası ISO 17799 (BS7799–1) ve ISO 27001 (BS7799–2)* standartları ve Türk Standartları Enstitüsü tarafından hazırlanan ve ulusal standart olarak kabul edilen *TS ISO/IEC 17799* ve *TS 17799-2* standartları, kamu sektöründe oldukça yaygın kullanılmaktadır (Kayrak, 2012, s.204). ISO 17999 standardı bilginin gizliliği ve bütünlüğünün nasıl korunacağı ve bilgiye sürekli erişimin nasıl sağlanacağı konusunda rehberlik eden uluslararası kabul görmüş bilgi güvenliği yönetim standardıdır (Özbilgin, 2003).

2. SİBER ORTAMDA BİLGİ GÜVENLİĞİ

Siber güvenlik siber ortamda, kurum, kuruluş ve bireysel kullanıcıların varlıklarını korumak için kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama ve teknolojileri içine alan bir kavramdır (Ünver ve Canbay, 2010, s.99).

Bilginin her türlü atağa ve tehdide karşı genel olarak korunmasını içeren siber güvenlik; kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır (Filiz, 2012, s.1). Bununla birlikte, gizlilik, bütünlük, erişilebilirlik, inkâr edilmezlik ve kimlik doğrulama sağlamak da siber güvenliğin diğer unsurları olmaktadır (Ünver ve Canbay, 2010, s.99).

Siber güvenlik alanında birçok çalışma ve özellikle kritik altyapının olduğu alanlarda ciddi yatırımlar yapılmaktadır. Ancak;

> *"Bilgi sistemleri doğrultusunda, elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinlikler"* (Filiz, 2012, s.1,6).

olarak ifade edilen siber terörizm ve siber saldırı sorununa, gerek iletişim sektöründeki tüm aktörler ve yerel hükümetler tarafından gerekse devletlerarası işbirliği açısından, henüz yeteri kadar önem gösterilmemektedir. Ancak her geçen gün artan tehdit ve saldırılar karşısında 1990'ların sonlarında başlayan siber güvenlik çalışmalarına son yıllarda hız verilmiştir (Ünver ve Canbay, 2010, s.100).

2.1. Bilgi Güvenliği Riskleri

Teknolojinin hayatımıza getirdiği birçok gelişmenin yanı sıra, siber ortamın kötü niyetli kişiler tarafından saldırı ve zarar verme gibi amaçlarla kullanılması ve en büyük değer olan bilginin hedef alınması sonucunda ortaya çıkan zararlar her geçen gün büyük boyutlara ulaşmaktadır (Filiz, 2012, s.4). Bununla birlikte bireysel ve kurumsal kullanıcılar bilgilerini elektronik ortamlara açtıkça, elektronik ortamlarda yapılan iş ve işlemler artmakta, karşılaşılan güncel tehdit ve risklerde de doğal olarak artışlar gözlenmektedir (Vural ve Sağıroğlu, 2008, s.520).

Kurum ya da kuruluşların, asli görevlerini kısmen veya tamamen yerine getiremez duruma getirebilecek olası bilgi güvenliği riskleri aşağıda verilmektedir.

• *İnsan Kaynaklı Riskler:* Kullanıcıların sistemi bilinçsiz ve yeterli eğitime sahip olmadan kullanması sonucu sistemde oluşabilecek aksaklıklardan kaynaklanan, görevin yerine getirilmesini etkileyen, engelleyen veya geciktiren sorunlar şeklindeki kötü niyetli olmayan girişimler olabileceği gibi sisteme kasıtlı olarak zarar verme amaçlı, güvenlik boşluklarından yararlanılarak yapılan saldırılar şeklindeki kötü niyetli tehditler de olabilmektedir (Tekerek, 2007, s.33).

• *Fiziksel Riskler:* Genellikle önceden tahmin edilemeyen deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi gibi doğal olaylar bu tür tehditlerdendir (Tekerek, 2007, s.133). Doğal afetlerin ortaya çıkması engellenemez ancak oluşabilecek hasarları en az seviyeye indirgemek için tedbirler almak mümkündür (Uslu, 2007, s.70,72).

• *Sabotaj, Terörist Saldırılar, Siber Saldırılar:* Stratejik öneme sahip kurum ve kuruluşlarla, çevrimiçi alışveriş sitelerine sahip firmalar her zaman sabotaj, siber terör veya saldırı riski altındadır. Siber saldırılar bilgi güvenliği

açısından ele alınabilecek en önemli risk grubundadır (Vural ve Sağıroğlu, 2008, s.520).

• *Yazılım ve Donanım Riskleri:* Yazılımlardaki değişiklikler kolayca fark edilemez, her zaman kötü amaçlı olarak tahrip edilebilme, değiştirilebilme, silinebilme gibi riskler altındadır (Tekerek, 2007, s.133). Yazılım geliştirici firmalar piyasa sundukları programlar için garantiyi ancak, belli bir süre içinde oluşabilecek hatalı kodları düzeltme şeklinde vermektedirler. Donanım tarafında ise üretici firmalar, en az bir en fazla üç yıl garanti vermektedir. Bu durumda üretimden kaynaklanan hatalar her zaman için bir risk unsuru oluşturmaktadır (Vural ve Sağıroğlu, 2008, s.520).

• *Korunmasızlık:* Yazılım veya donanımdan kaynaklanan güvenlik açıkları sebebiyle, her zaman için sistemdeki bilgisayarlara veya bilgisayar ağı üzerindeki kaynaklara izinsiz olarak erişebilme riski bulunmaktadır (Tekerek, 2007, s.134). Güvenlik açıkları yazılım-donanım bazında alınması gereken teknik tedbirlerin yetersizliğinden kaynaklanabileceği gibi, fiziki güvenliğin zayıflığından veya kullanıcıların bilinçsizliğinden de kaynaklanabilmektedir. Bu tür saldırılara maruz kalan işletmeler maddi ve itibar kaybına uğramakta ve hizmetleri aksayabilmektedir (Vural, 2008, s.520).

Verilerin saklandığı, işlendiği, üzerinde uygulamaların çalıştığı sistemler ve manyetik ortamlar da benzer saldırılar karşısında zarar görebilmekte, kısmen veya tamamen kullanılamaz hale gelebilmektedir. Bu durum işletmenin, kurum ya da kuruluşun görevlerini yerine getirmesine engel olabilmektedir (Vural, 2008, s.520).

2.2. Siber Saldırı Kavramı

Siber Saldırı kavramı ile ilgili yapılan birçok tanımdan bazıları aşağıda verilmektedir.

Cep telefonu, sosyal medya ve iletişim ortamları, web siteleri, online oyunlar, elektronik posta aracılığıyla bir kişi veya bir grup tarafından başka bir bireyi karalayıcı, küçük düşürücü yayın ve duyurular yapılarak kişilik haklarına saldırılması siber saldırıdır.

Pollitt'e göre;

> *"Siber saldırı, bilgisayar ve bilgi sistemlerine, bilgisayar programları ve verilerine önceden tasarlanmış politik saldırılardır"* (Pollitt, 2004, aktaran Topal, 2004, s.20,21).

Siber saldırı; siber alanın terörist faaliyetler için kullanılması sonucu ortaya çıkmıştır. Bununla birlikte siber terör saldırısı, bilgisayar ağ sistemlerini kullanarak kritik önemi olan özel ve kamusal altyapılara (enerji, ulaşım, sağlık, bankacılık, e-devlet platformu vs.) zarar vermek ya da tamamen kullanılamaz hale getirmeyi amaçlayan saldırılar şeklinde de ortaya çıkmaktadır (İren ve Gürkaynak 2011, s.267).

Diğer taraftan siber saldırı; siyasal bir amaç için toplum ya da devlete zarar vermek adına devlet tarafından iyi korunan alanlardaki (ulusal güvenlik ağları vs.) bilgileri elde etmek, değiştirmek veya terörist amaçlar için kullanmaktır. Bununla birlikte sanayi, finans ve bankacılık gibi sektörlerde kritik bilgilerin maddi çıkarlar sağlamak amacıyla elde edilmesidir (İren ve Gürkaynak 2011, s.267).

Siber saldırı, teröristlerin dinsel, politik ve sosyal hedeflerine ulaşmak amacıyla, toplum veya devletleri yıldırmak ve baskı altına almak için dijital mülkiyete yasa dışı zarar vermesidir (Topal, 2004, s.20,21).

İngiltere çıkardığı Terörizm Yasası 2000'de siber saldırıyı;

> *"Hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlerin içine izinsiz girmek veya bu sistemleri bozmak"*

olarak tanımlamaktadır.

Collin'e göre;

> *"Siber dünyayla terörizm birleşmesi sonucunda siber saldırılar ortaya çıkmıştır"* (Topal, 2004, s.20,21).

Siber saldırı faaliyetleri siyasi tansiyonun arttığı veya taraflar arasında çatışmaların yaşandığı ortamlarda da meydana gelebilmektedir (İren ve Gürkaynak, 2011, s.267).

Son dönemde siber saldırı olaylarında artış görülmektedir. Siber saldırıların yükselişe geçmesinin en önemli sebebi olarak, insanların ve hayati öneme sahip altyapı hizmetlerinin iletişim ve bilgisayar ağlarına gittikçe bağımlı hale gelmesi sonrasında, bu sistemlerin dışarıdan müdahaleye açık alanlarının ortaya çıkması ve kötü niyetli kişiler tarafından kullanılması şeklinde görülmektedir (İren ve Gürkaynak, 2011, s.267).

2.3. Siber Suçların Sınıflandırılması

Siber suçlarda kullanılan saldırılar; çoğunlukla zevk ve çıkar amaçlı basit ve kurgulanmamış saldırılar şeklinde olabileceği gibi, bilişim altyapılarını hedef alacak şekilde çok iyi planlanmış ve koordine edilmiş de olabilmektedir (Filiz, 2012, s.9).

Belirli bir tarifi olmamakla birlikte Birleşmiş Milletler (BM) siber suçları aşağıdaki başlıklar altında sınıflandırmaktadır.

2.3.1. İzinsiz erişim

Bilgisayar sistem ve servislerine izinsiz erişim en çok işlenen suçların başında gelmektedir (Filiz, 2012, s.9). İletişimin birçok alanda bilgisayar ve bilgi teknolojileri kullanılarak yapılmakta olduğu günümüzde, birçok önemli bilgi bu ortamda iletilmektedir (Güneş, 2004, s.3). Bireysel bilgiler ile birlikte artık hemen hemen tüm kamu ve özel sektöre ait bilgiler, güvenlik ve

istihbarat birimlerinin tutmuş olduğu bilgiler, bilgisayar ve veri merkezlerinde muhafaza edilirken yine bu hassas bilgilere ulaşmak da bilgisayar yoluyla olmaktadır. Bu noktada gizlilik gerektiren bilgilere yetkili kişiler haricinde yapılan erişimler izinsiz erişim olarak nitelendirilmektedir (Topal, 2004, s.24).

İzinsiz erişim, bir bilgisayar sistemine yetkisiz olarak erişmek suretiyle bilgilerin güvenliğine yönelik tehditler ve saldırılar şeklinde ortaya çıkar. Bu tür saldırılar genellikle bilgisayar sistemine virüs, solucan, truva atları gibi zararlı yazılımlar yüklenerek yapılmaktadır (Turhan, 2010, s.46). Bunlar bilgi sistemlerinin mantıksal yapısını değiştirerek, sistem de gecikme ve belirsizlikler oluşturmaktadır.

2.3.2. Engelleme ve zarar verme

Bilişim sistemlerine yapılan saldırılardan biri olan engelleme ve zarar verme hedef bilişim sistemine fiziksel zarar verme ya da fiziksel erişim sağlayarak zarar verme şeklinde meydana gelmektedir. Bu tür saldırılarda asıl hedef, maddi zarardan ziyade bilginin kaybı ve kullanılamaz hale gelmesidir (Filiz, 2012, s.9).

Hedef alınan sisteme uzaktan erişim yoluyla fiziksel olarak ya da doğrudan sisteme müdahale etmek suretiyle bilgileri silmek, yok etmek veya değiştirmek, engelleme ve zarar verme olarak nitelendirilmektedir. Servis aksatma (Denial of Service, (DoS)) veya dağıtık servis engelleme saldırısı (Distributed Denial of Service Attack, (DDoS)) yöntemleriyle yapılan saldırılar engelleme ve zarar vermeye yönelik saldırılardır (Turhan, 2010, s.47).

DoS saldırıları tek bir bilgisayar veya üzerinden ağ üzerinden yapılır. Saldırganlar sisteme yetkisiz giriş sağlayamazlar ise sistemin erişilebilirliğini engellemeye yönelik DoS saldırılarında bulunur. Bu saldırılarda amaç kullanıcıların erişimlerini engelleyerek hizmet akışının durmasını sağlamaktadır. Eski teknoloji ya da donanımlar (eski model bilgisayar ya da modem vs.) kullanmak suretiyle bile yeni teknoloji kullanan ağlar bu

saldırılarda zarar görebilmektedir. Ucuz maliyetli girişimler olması, saldırganın zor tespit edilmesi ve çok fazla yetkinlik gerektirmemesi gibi sebepler, DoS saldırılarının siber saldırılarda yaygın olarak kullanılmasına neden olmaktadır (Turhan, 2010, s.47).

DDoS saldırıları birçok bilgisayar veya ağ üzerinden yapılır. Etki altına alınmış yüzlerce bilgisayar hedef olarak seçilmiş tek bir veya birkaç bilgisayar sistemine ya da ağ'a saldırarak hedefi etkisiz hale getirebilmektedir (İren ve Gürkaynak, 2011).

Bu saldırılarda, virüs, solucan, zombi gibi zararlı yazılımlar kullanılarak kullanıcının bant genişliği, sunucu ya da ağ'da bulunan modem, yönlendirici gibi cihazları hedef alınır. Böylece kullanıcıların tüm kaynaklarını tüketmeye yönelik bu saldırılar, hedef sistemin erişilemez hale gelmesi, alınan servisin engellenmesi veya yavaşlaması ile sonuçlanır.

2.3.3. Değişiklik yapma

Bu saldırılar sistem kullanıcısının haberi olmadan sisteme girilmesi ve gizli bilgilerine ulaşarak değiştirilmesi şeklinde ortaya çıkmaktadır (Topal, 2004, s.45).

Bilgisayarda değişiklik yapılması bir tür dolandırıcılık olarak nitelendirilmektedir. Bu tür saldırılar genellikle insanların banka bilgilerinin ele geçirilmesi ya da değişik senaryolar ile suçu işleyenlerin kendi hesaplarına para transferi şeklinde gerçekleşebilmektedir (Filiz, 2012, s.9).

Bu saldırı türü bilgisayar veri ve programlarının kullanımına, bütünlüğüne ve işleyişine zarar veren saldırılardır. Bu şekilde bilgilere yetkisiz erişim elde edenler, eriştikleri bilgileri sadece kopyalama veya incelemekle kalmaz, bu bilgileri değiştirip silebilmektedir. Veri kayıplarına yol açan bu tür saldırıların en bilinen örneklerinden birisi bilgisayar virüsleridir (Turhan, 2010, s.47).

2.4. Siber Saldırı Yöntemleri

Siber alanda gerçekleşen saldırıların kendine özgü yöntemleri bulunmaktadır. Bu saldırı yöntemleri ile ulusal haberleşme veya elektrik şebekeleri gibi kamusal hizmetlere erişim engellenebilmekte ya da internet erişimi devre dışı bırakılarak tüm toplumda günlük yaşantıyı olumsuz etkileyen sonuçlar ortaya çıkarılabilmektedir (İren ve Gürkaynak, s.270).

Siber saldırılarda yaygın olarak kullanılan yöntemler aşağıdaki başlıklar altında verilmiştir.

2.4.1. Oltalama (Phishing)

Oltalama; internet kullanıcılarının ikna edilmesi yöntemiyle ya da kandırılarak kişisel bilgilerini, banka bilgilerini, kredi kartı bilgilerini ele geçirmeyi hedefleyen bir dolandırıcılık yöntemi olarak tanımlanmaktadır (Turhan, 2006, s.100).

Resmi bir mesaj gibi gözüken e-postalarla insanlardan önemli bilgiler elde edilmektedir. Sahte e-postalar ile kandırılan kullanıcılar, istenilen hayati bilgileri gönderebilmekte, bu bilgilerin kötü niyetli şahısların eline geçmesiyle de büyük zararlara uğramaktadırlar (Canbek, 2006, s.165,174).

En sık oltalama yöntemi, bankacılık işlemlerinde görülmektedir. İnternet bankacılığında internet sayfasının bir kopyası yapılarak söz konusu kullanıcının hesap bilgileri oltalama yöntemi ile çalınabilmektedir (Turhan, 2010, s.34). ABD'de en fazla müşteriye sahip Lloyds, Citibank, PayPal ve Bank of America gibi bankalar en çok oltalama saldırısına uğrayan bankalar arasındadır (Turhan, 2010, s.34). Ayrıca Facebook, Myspace, Twitter gibi sosyal paylaşım siteleri de oltalama saldırılarından etkilenmektedir (Antiphishing, 2013).

2.4.2. İstek dışı elektronik postalar (SPAM)

Spam mailler, pazarlama, reklâm veya sosyal içerikli mesajların, kullanıcılara istekleri dışında internet ya da cep telefonu gibi teknolojiler aracılığı ile yollanması şeklinde görülmektedir (UDHB Raporu, 2005, s.23).
Spam ciddi bir siber güvenlik problemidir. Bu tür girişimler bilgisayar yoluyla dolandırıcılık için kullanılabileceği gibi, zararlı yazılım türlerinin yayılmasına da bir düzenek oluşturmaktadır. Özellikle teknolojinin gelişmesiyle cep telefonları ve anlık mesajlaşma hizmetleri Spam'lerin yayılmasını hızlandırmaktadır (Turhan, 2010, s.34).

"Günümüzde ticari e-posta'ların %97'si istek dışı elektronik postadır"

2.4.3. Zararlı yazılımlar

Zararlı yazılım; sahibinin bilgisi dışında bilgisayar veya ağlara zarar vermek, kötü niyetli girişimlere ulaşmak üzere tasarlanmış yazılımlardır (Turhan, 2010, s.34). En yaygın zararlı yazılımlar, virüsler, solucanlar, Truva atları, zombi, casus yazılımlar olarak karşımıza çıkmaktadır.

2.4.3.1. Virüsler

Virüsler; bilgisayar belleğine yerleşmek suretiyle, çalışan programlara kendilerini kopyalayan, yerleştiği programların yapısını değiştirebilen ve çoğalabilen programlardır. Bu şekilde bir bilgisayardan diğerine diskler ve ağlar arasında kendilerini kopyalayarak hızla yayılabilmektedirler. Bu tür yazılımlar bazı dosyaları silerken bazılarını da hiç kullanılamaz hale getirebilmektedir. Siber saldırıda kullanılan virüsler, hedef bilgisayarı zararlı yazılımları kullanacak şekilde yeniden programlayabilmekte böylece ele geçirdikleri bilgileri değiştirmekte veya yok etmektedirler (İren ve Gürkaynak, 2011).

Virüsler en tehlikeli ve en eski zararlı yazılımlar olup, kısa süreliğine çalışmayı bloke edebilen veya ekrana mesajlar gönderebilen zararsız

sayılabilecek türlerinin yanında, çoğu virüs yazılımın, önemli dosyaları silmek veya sistemi tamamen çalışmaz hale getirmek gibi yıkıcı etkileri olmaktadır. Virüsler, kendini üzerine kopyaladığı bir dosyanın açılması, bir e-postanın okunması veya virüs bulaşmış bir programın çalıştırılması gibi yöntemlerle yayılabilmektedir (Turhan, 2010, s. 34).

2.4.3.2. Solucanlar

Solucanlar; bilgisayar ağları arasında herhangi bir donanım veya yazılıma zarar vermeden dolaşabilen, kullanıcı müdahalesine gerek kalmadan kendi kendini aktif hale getirebilen ve bir kopyasını ağa bağlı olan diğer bilgisayarlara bulaştırabilen programlardır. Solucanlar da virüsler gibi sisteme zarar vermeden sistemin içinde hareket edebilmektedir (Turhan, 2010, s. 34).

Solucanlar, hedef sistemin korunmasız olduğu anlarda güvenlik açıklarını tespit ederek yayılmaktadır (Turhan, 2009, s. 34). Kendilerini sayısız kez kopyalama özellikleri sayesinde bir bilgisayardan yüz binlerce solucan başka bilgisayarlara gönderilebilmektedir (İren ve Gürkaynak, 2011, s.263,275).

Solucanların kontrol dışı çoğalmaları, ancak sistem kaynaklarının aşırı kullanılması veya diğer çalışan programların yavaşlaması ya da çalışmakta olan diğer görevlerin sonlanmasına neden olması halinde fark edilebilmektedir (Turhan, 2010, s.34).

2.4.3.3. Truva Atları (Trojan)

Truva Atı, zararsız ve faydalı olarak bilinen programların içine gizlenmiş yazılımlardır (İren ve Gürkaynak, 2011, s.263,275).

İçinde bulundukları programları kontrol edebildikleri gibi onlara zarar verebilmekte ve aynı anda birçok işlevi yerine getirebilmektedir. Bazı Truva atları yerleştikleri bilgisayar içinde farklı özel kelimeleri arayabilmekte ve o kelimelerin geçtiği dosyaları kopyalayarak başka bir bilgisayara otomatik olarak gönderebilmektedir (İren ve Gürkaynak, 2011, s.263,275).

Truva atları zararsız gibi görünse de bilişim güvenliğine zarar verebilen zararlı yazılımlardandır. Virüs ve solucanlar gibi kendi başlarına işlem yapamazlar, bu programlar arka planda çalışarak kullanıcının sistemine uzaktan erişim imkânı sağlamaktadır. Bilgisayarları uzaktan yönetmek için arka kapı açan Truva atları, lisanslı programların yasa dışı kopyalarının veya aktivasyon kodlarının yayınlandığı sitelere, mp3, oyun veya yetişkin içerik dağıtan sitelere ziyaret sırasında bilgisayarlara indirilmektedir. Truva atlarıyla sisteme arka kapıdan (backdoor) ulaşan bilgisayar korsanları, bilgisayarın sistem yapılanmasını değiştirerek, kullanıcı şifre ve diğer kişisel bilgilere ulaşabilmektedir (Turhan, 2010, s. 33).

Truva atlarının virüs gibi diğer zararlı yazılımlara göre tespiti çok daha zor olmaktadır. Herhangi bir şekilde bulaşmadıkları ve bir etkide bulunmadıkları için, ancak etkisi görüldükten sonra anlaşılabilmektedirler. Yerleştikleri sistemi kullanarak ağ'ın geri kalanına yayılmak suretiyle dosyalara ulaşıp, üzerinde değişiklikler yapabilmekte veya dosyaları tamamen silebilmektedir (İren ve Gürkaynak, 2011, s.263,275).

Hedef bilgisayar veya ağlara uzaktan erişim sağlayarak, tüm şifreleri çözer ve özel bir e-posta adresine gönderir. Ayrıca klavye girişlerini kaydetme ve güvenlik programlarını devre dışı bırakma gibi zararlı işlevleri bulunmaktadır. Bu yazılımların tek amacı dosyaları silmek ya da tamamen yok etmektir (Uslu, 2007, s.34).

2.4.3.4. Zombiler

SPAM gibi istek dışı elektronik postalar vasıtasıyla zararlı yazılımların bilgisayara bulaşması ve bilgisayarların kontrolünün habersizce ele geçirilmesidir. Bu bilgisayarlar kullanılarak kişilere ait özel bilgiler ele geçirilmektedir (Ünver ve Canbay, 2010, s.94). Bu tür zararlı yazılımlar güvensiz girilen sitelerden, indirilen programlardan veya tıklanan linklerden sisteme bulaşabilmektedir (OGM, 2013).

Zombi bilgisayarlar bir araya getirilerek botnet[5] adı verilen yapılar oluşturulmaktadır. Botnetlerce kontrol altında tutulan bilgisayar sayısı artarak Dünya çapında birçok yerdeki bilgisayarları kontrol altına alabilmektedir. Bu tür yazılımlar zombi bilgisayar ve botnetleri kontrol eden kişiler tarafından, birçok ülkede yasaklanan ve suç olarak belirlenen istek dışı elektronik posta gönderme amacıyla kullanılmaktadır (Ünver ve Canbay, 2010, s.94).

2.4.3.5. Casus yazılımlar

Casus yazılım; virüs ve solucanlardan farklı olarak, sistemlere bir kez bulaştıktan sonra kendi kopyasını oluşturarak kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılımlardır (Turhan, 2010, s.35).

2.5. Siber Güvenlik ve Türkiye

Bilgi güvenliği bir ürün veya hizmet değildir. İnsan faktörü, teknoloji ve eğitim üçgeninde, ulusal ve uluslararası güvenlik standartlarına bağlı olarak yaşayan canlı bir süreçtir. Bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsetmek de mümkün olmayacaktır (Vural ve Sağıroğlu, 2008, s.520).

Türkiye'de en fazla güvenlik açıklarına web uygulamalarında rastlanmaktadır. Kurumlar genelde sınır ağ güvenliğinin sağlanmasına yönelik çözümlere (güvenlik duvarı, saldırı tespit sistemleri, antivirüs programları, vb.) önem gösterirken, web uygulama güvenliği kavramına yeterince özen göstermemektedir.

---

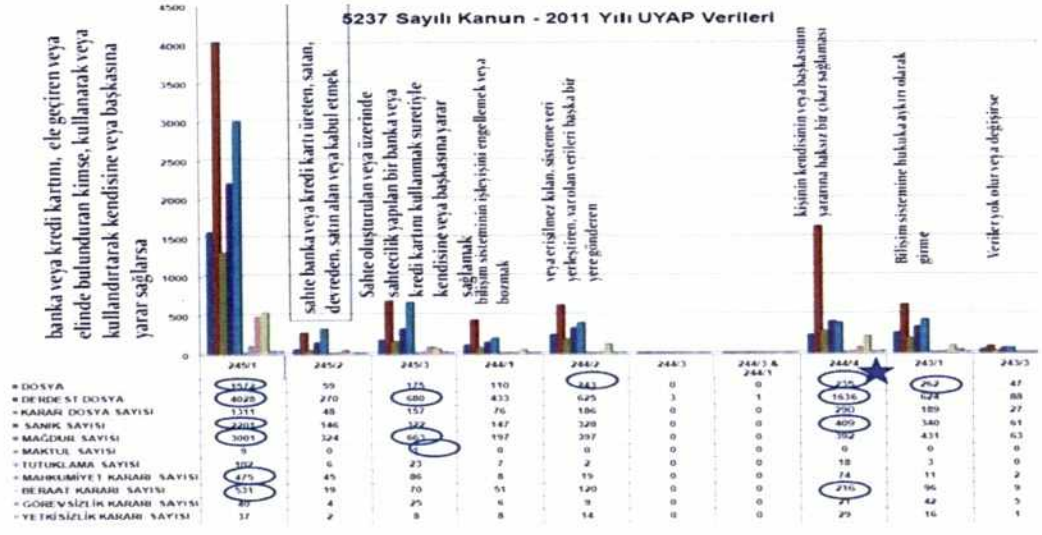
[5] Botnet; bot robotun kısaltmasıdır. İstenmeyen e-posta mesajları göndermek, virüs yaymak, bilgisayar ve sunuculara saldırmak veya sahtekârlıklarda bulunmak amacıyla kullanılır. Bilgisayarların kullanıcıların haberi olmadan internet üzerinde bir takım görevleri otomatik olarak gerçekleştirmesine yol açan kötü amaçlı yazılımlardır. http://www.microsoft.com/tr-tr/security/resources/botnet-whatis.aspx

2.5.1. Ülkemizin siber suçlardaki mevcut durumu

Türkiye'de internet ortamındaki saldırılar, özel ve kamu kesimlerindeki bilgi işlem ve veri merkezi yapılarına, özellikle Bakanlıklar, PTT-TT, Emniyet Genel Müdürlüğü gibi kamu kurum ve kuruluşlarına, Türk Silahlı Kuvvetlerinin bilgi işlem sistemlerine yönelik olarak, genellikle bu sistemleri çökertmek bazen de teröristler tarafından propaganda amaçlı olarak gerçekleştirilmektedir (Özcan, 2004, s.318,319). Emniyet Genel Müdürlüğü kayıtlarına göre 150'si aktif olmak üzere Türkiye aleyhine faaliyet gösteren zararlı internet site sayısı 8000 civarındadır. Bu siteler başta Amerika, Almanya, Hollanda olmak üzere diğer Batı Avrupa ülkeleri üzerinden de yayın yapmaktadır.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığının her yıl yayınladığı raporda bilişim suçları da yer almaktadır. Bugüne kadar raporlanan bilişim suçları çok fazla olmamakla beraber son yıllarda ortaya çıkarılan bilişim suçlarının hem nitelik kazandığı hem de sayılarının oldukça arttığı görülmektedir (Dijle ve Doğan, 2011, s.43).

Şekil 2.1. 2011 yılı Türkiye'de bilişim suçları



Kaynak:Uyap, 2011

Ülkemizin siber tehdit ve saldırı araçlarına kaynaklık etmesi, ülkemizdeki bilişim suçlarının artışına da yol açmaktadır. Bunun sonucu olarak, 2003 yılında kayıtlı bir bilişim suçu ve dolandırıcılığı olmamasına rağmen, 2008 yılında 560 olay gerçekleşmiş ve şüpheli kişi sayısının 842'ye çıktığı görülmüştür (Özkan, 2006, s.318,319). Türk Ceza Kanunu'nu 243, 244 ve 245. bilişim suçlarını düzenleyen maddelerinden açılan dava sayısının artması da ülkemizde bilişim suçlarının hızla arttığını ortaya koymaktadır (Özkan, 2006, s.318,319).

1990-2011 yılları arasını kapsayan "Türkiye'de Bilişim Suçları" adlı araştırma raporuna göre suç türlerine bakıldığında "Bilişim Sistemi" (Sistemlere izinsiz giriş) suçlarında ilk üç sırayı, Batman, İstanbul ve Muğla almaktadır (Yenişafak, 2013).

2.5.2. Siber risklere karşı mücadele

Son yıllarda dünya genelinde ortaya çıkan siber tehdit ve saldırıların artması, bu girişimlerin büyük maddi zararlara yol açmasının yanında kamu düzeni ve güvenliğini etkileyecek noktaya gelinmesi konunun ülkeler ve uluslararası kurum ve kuruluşlarca ele alınmasını gerektirmiştir (Ünver ve Canbay, 2010, s.99).

Siber suçlar genellikle maddi çıkarlar elde etmek amacıyla organize suç örgütleri tarafından işlenmektedir. Bilgi ve iletişim şebekeleri sayesinde farklı ülkelerdeki ve kıtalardaki siber saldırganlar birbirleriyle iletişim kurup, bilgi paylaşma, propaganda yapma, yeni üyeler kazanma gibi etkinlikler yapabilmektedir (Turhan, 2010, s.33).

Siber suçların pek çok ülke mevzuatında suç olarak tanımlanmamış olması saldırganların izlerini bırakmadan başka ülkelerde suç işlemesine ortam oluşturmaktadır. Mevzuatlarda boşlukların olması suç ve suçlulara yönelik soruşturma ve yargılamaları da güçleştirmektedir. Bu suçların çoğunun uluslararası niteliğinin bulunması uluslararası alanda yapılacak çalışmaları

zorunlu hale getirmektedir. Bu amaçla BM, AB, OECD, Avrupa Konseyi gibi kuruluşlarca Avrupa Konseyi Siber Suçlar Sözleşmesi imzalanmıştır (Turhan, 2010, s.33).

Türkiye'de ise siber suçlarla mücadele için 1997 yılında Emniyet Genel Müdürlüğü bünyesinde Bilgi İşlem Daire Başkanlığı altında "İnternet ve Bilişim Suçları Bürosu" kurulmuştur. Bilgisayar suçlarının önüne geçilmesi ve bilgi güvenliğinin sağlanması için oluşturulan bu kuruluşta; Asayiş, Bilgi İşlem, Interpol, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Terörle Mücadele ve Hareket Daire Başkanlıkları ile Hukuk Müşavirliği'nden bilişim suçlarıyla ilgili hizmet verebilecek kişiler yer almaktadır (Özkan, 2006, s.83).

Emniyet Genel Müdürlüğü'ne bağlı Bilişim Suçları Araştırma Merkezi Başkanlığı (Turkish International Academy against Drugs and Organized Crime, (TADOC))'da siber terör ve diğer suçlarla ilgili çalışmalar yapmaktadır. Bu birim, bilişim suçları konusundaki gelişmeleri takip ederek bilgisayar sistemlerine izinsiz giriş ve zarar yöntemlerine karşı alınacak tedbirleri araştırmakta, bilişim suçları konusunda yetiştirilecek personelin eğitim standartlarını tespit etmekte ve bilişim suçları konusunda çalışma yapan yerli ve yabancı kuruluşlarla iletişime geçmektedir. Ayrıca Emniyet Teşkilatı bünyesinde sadece siber suçlarla mücadele için "siber polis" ekipleri oluşturulmuştur (Özkan, 2006, s.83).

Siber Güvenlik ile ilgili yapılması gerekenler;

Siber güvenlik konusunda yapılacak çalışmalardan istenilen sonuçların alınabilmesi ve bu çalışmaların başarılı olabilmesi amacıyla ulusal politika ve stratejilerin geliştirilmesi ve bu çerçevede yasal mevzuatın oluşturulması gerekmektedir. Ayrıca teknolojik gelişmelere paralel olarak siber saldırı araç ve yöntemlerinin de değişebileceği ve gelişebileceği göz önünde bulundurularak, mevcut mevzuatlar gözden geçirilmesi ve tespit edilen ve öngörülen eksikliklerin giderilmesi gerekmektedir (Ünver ve Canbay 2010, s.100,103).

Siber güvenliğin sağlanmasında hukuki tedbirler yanında yazılım, donanım ve iş süreçlerinin kalitesinin artırılarak daha güvenli hale getirilmesi gerekmektedir. Bunun için TS ISO/IEC 27001, BS 25999, COBIT ve ITIL gibi güvenlik standartlarının, benzer nitelikteki teknik rehber ve kılavuzların geliştirilmesi, uygulanması ve kullanılması sağlanmalıdır (Ünver ve Canbay, 2010, s.100,103).

Siber tehdit, araç ve yöntemlere karşı yeni politikalar, yasalar, standartlar, ürün ve çözümler konusunda birçok çalışma yapılmaktadır. Bu çalışmalarda politika belirleyicileri, yazılım, donanım ve uygulama geliştiricilerinin de kapasitelerinin geliştirilerek yeni ve olası güvenlik sorunlarına yönelik yeni çözümler geliştirmeleri gerekmektedir. Bu suçlar üzerinde çalışan, soruşturma yapan, delil toplayan kolluk güçlerinin de verilecek eğitimlerle teknik ve idari kapasiteleri geliştirilmesi bu suçların tespitini hızlandıracaktır.

Teknolojik gelişmeler yanında siber saldırı araç ve yöntemleri de gelişmektedir. Bu bakımdan son kullanıcıları, siber tehdit ve riskler, saldırı ve güvenlik önlemleri konusunda bilgilendirmek ve bu konuda farkındalığın artırılması için eğitim faaliyetlerini yaygınlaştırmak büyük önem taşımaktadır.

Siber saldırıları araştırma, tespit ve önleme çalışmalarında ülkeler arası işbirliğinin önemi her geçen gün artmaktadır. İşbirliği çerçevesinde mevzuatların, suç soruşturma ve kovuşturma usullerinin uyumlu hale getirilmesi, bilgi paylaşım mekanizmalarının oluşturulması gibi çalışmaların yapılması gerekmektedir (Ünver ve Canbay, 2010, s.100,103).

Ulusal Internet Değişim Noktası ve Veri Merkezi altyapıları oluşturmak bilgi güvenliğinin sağlanması ve siber suçların mücadelesinde en önemli teknolojik uygulamalar olmaktadır (Akan, 2013, s.14).

Kısaca, siber risklere karşı mücadelede alınacak tedbirleri aşağıdaki maddeler şeklinde sıralamak mümkündür.

- Ulusal politika ve stratejinin geliştirilmesi,

- Yasal mevzuatın oluşturulması,
- Teknik tedbirlerin geliştirilmesi,
- Kurumsal yapılanmanın belirlenmesi,
- Ulusal işbirliği ve koordinasyonun sağlanması,
- Kapasitenin geliştirilmesi,
- Farkındalığın artırılması,
- Uluslar arası standartlara uyum ve işbirliğinin sağlanmasıdır (Ünver ve Canbay, 2010, s.100,103).

2.6. Siber Güvenlikte Uluslararası Yaklaşımlar ve Ülkemizdeki Düzenlemeler

Dünyada internet ortamında bilgi alış verişinin artışına paralel olarak siber güvenliği sağlamaya yönelik alınacak tedbirler de giderek önem kazanmaktadır. Siber güvenlik konusunda birçok uluslararası kuruluş ve örgüt yasal mevzuatlar konusunda çalışmalar yapmakta, bu doğrultuda yasal düzenlemeler yapılmaktadır. Ülkemizde de bu uluslararası karar ve tavsiyeler dikkate alınarak, paralel düzenlemeler yapılmaktadır. Aşağıda siber güvenlik alanında uluslararası ilgili kuruluşların aldığı kararlar ve ülkemizdeki düzenlemeler ele alınmaktadır.

2.6.1. Uluslararası kuruluş kararları ve yaklaşımlar

Bu bölümde ülkemizin de üyesi olduğu ve aldığı kararlar ve yaptığı çalışmalarla siber güvenlik konusunda öne çıkan Uluslararası Telekomünikasyon Birliği (International Telecommunication Union, (ITU)) ve Avrupa Birliği (Europan Union, (EU))'nin yaptığı çalışmalar anlatılmaktadır.

2.6.1.1. Uluslararası Telekomünikasyon Birliği (ITU) kararları

Ülkemizin de üyesi olduğu ITU, Dünya Bilgi Toplumu Zirvesi sürecinde siber güvenlik konusunda aktif bir şekilde çalışmaktadır.

2001 yılında, ITU Konseyi, Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society, (WSIS)) adıyla uluslararası bir toplantı düzenlenmesini kararlaştırmıştır. İlk aşaması Aralık 2003'te Cenevre'de, ikinci aşaması Kasım 2005'te Tunus'ta yapılan zirvenin WSIS ilkeler bildirgesinde;

- *Bilgi ve şebeke güvenliği,*
- *Kimlik doğrulama,*
- *Tüketici haklarını ve kişisel mahremiyetin korunması,*
- *Küresel bir siber güvenlik kültürü*

konuları görüşülmüştür.

Cenevre Eylem Planında yapılacak çalışmalardan C5 kararı olan "*Bilgi ve İletişim Teknolojilerinin Kullanımında Güven ve Güvenliğin Tesis Edilmesi*" konusunun sorumluluğu ITU'ya verilmiştir. Söz konusu C5 kararı;

- *İstem dışı elektronik haberleşme ile mücadele,*
- *Siber güvenlik konusunda işbirliğinin geliştirilmesi,*
- *Siber güvenlik konusunda fikir alışverişinde bulunmak üzere üye ülke temsilcilerinin ve sektör temsilcilerinin katılımıyla toplantılar düzenlenmesi,*
- *Bir mutabakat zaptı oluşturulmasını*

önermektedir (ITU, 2013).

2008'de Johannesburg Dünya Telekomünikasyon Standardizasyon Genel Kurulu (World Telecommunication Standardization Assembly, (WTSA))'unda alınan 50, 52 ve 58 sayılı kararları WSIS Eylem Planının C5 numaralı başlığı ile ilgilidir:

50 sayılı karar,

> *"Uluslararası Telekomünikasyon Birliği Telekomünikasyon Standartlaştırma Biriminin (*International Telecommunications Union

> Telecommunication Standardization Sector, (ITU-T)) *WSIS siber güvenlik faaliyetleri ve ITU Genel Sekreterliğinin siber güvenliğe ilişkin olarak başlattığı girişimler konusunda ilgili taraflarla işbirliğini sürdürmesi ve siber tehditlere karşı savunmaya duyulan ihtiyaç hakkında genel farkındalık düzeyini arttırması*"

konularına değinmektedir" (Ünver, Canbay ve Mirzaoğlu, 2009, s.8,9).

52 sayılı karar:

> *"ITU-T'nin spam ile mücadeleye ilişkin uluslararası girişimler hakkında bir rapor hazırlamasını, üye ülkelerin ve sektör temsilcilerinin bu çalışmalara katkıda bulunmalarını ve üye ülkelerin ulusal mevzuatlarını spam ile mücadele konusunda gerekli tedbirleri alacak şekilde iyileştirmelerini talep etmektedir"* (Ünver, Canbay ve Mirzaoğlu, 2009, s.8,9).

58 sayılı kararda, siber ağlardaki güvenlik önlemlerinin az olduğu gelişmekte olan ülkeler üzerinden diğer ülke ağlarına saldırıların olabileceğine değinilmekte, üye ülkelere ulusal bilgisayar olaylarına müdahale ekiplerinin kurulmasını önermektedir (UDHB Şura, 2013 s.19,20).

2010 yılında Haydarabad'da yapılan "Dünya Telekomünikasyon Kalkınma Konferansı" (World Telecommunication Development Conference, (WTDC)) kapsamında alınan 45 sayılı kararda, uluslararası işbirliğinin artırılarak istenmeyen elektronik e-posta, siber güvenlik ile mücadelede gizlilik ve ifade özgürlüğünün de göz önünde bulundurulması gerektiği bildirilmektedir. 69 sayılı kararda ise yine ulusal bilgisayar ekipleri arasında işbirliği yapılmasına yönelik ITU'da yapılacak çalışmalara yer verilmektedir (UDHB Şura, 2013 s.19, 20).

Guadalajara'da 2010 yılında düzenlenen "ITU Tam Yetkili Temsilciler Konferansında" (Plenipotentiary Conference –PP 2010) alınan 130-174-181 sayılı kararlar, bilgi iletişim teknolojisinde; güvenlik için ITU bünyesindeki görevler, farkındalığın artırılması ve yasa dışı kullanımın engellenmesi için

yapılması gerekenler, kavramlar ve bu konuda ortak dilin oluşturulmasını içermektedir. Çocukların İnternet kullanımındaki güvenlik konusunu 179 sayılı karar ele almaktadır (UDHB Şura, 2013 s.20, 21).

ITU 2011 yılında ülkelerin çalışmalarında örnek alabilecekleri 10 ana başlıktan oluşan "ITU Ulusal Siber Güvenlik Strateji Rehberi"ni yayınlamıştır. Rehber özellikle ülkelerin oluşturacağı stratejilerin temelinde ulusal kültürün dikkate alınmasının, ülkedeki siber güvenlik algısının oluşması ve kalıcılığın sağlanması konularında önemli olduğunu belirtmektedir (UDHB Şura, 2013 s.21, 22).

ITU Genel Sekreterliği, WSIS sonrasında bilgi toplumunda güven ve güvenliğin sağlanmasına yönelik "Küresel Siber Güvenlik Gündemi"ni yayınlamıştır (Ünver, Canbay ve Mirzaoğlu, 2009, s.10).

Tüm bu çalışmaların yapılmasında ITU Genel Sekreterliğine destek olmak üzere, siber güvenlik ile ilgili konularda bilgi düzeyi çok üst seviyede uzmanlardan oluşan bir "Yüksek Seviyeli Uzmanlar Grubu" (High Level Experts Group, (HLEG)) kurulmuştur. Küresel Stratejik Raporu (2008)'unda siber güvenliğin beş ana unsuru aşağıdaki şekilde gösterilmektedir (UDHB Şura, 2013 s.9).

Şekil 2.2. HLEG ve küresel siber güvenliğin ana unsurları

Kaynak: UDHB Şura, 2013 s.9

Operasyonel olarak siber güvenliğin sağlanması için Uluslararası Siber Tehditlere Karşı Çok taraflı Ortaklık (International Multilateral Partnership Against Cyber Threats, (ITU-IMPACT)) kurulmuştur. ITU-IMPACT, ITU üyesi ülkelerin operasyonel süreçleri konusunda birçok kurum ve kuruluşla işbirliği yaparak bilgi aktarımı ve eğitim faaliyetlerini tarafsız olarak yürütmektedir (UDHB Şura, 2013 s.9).

ITU bünyesinde kurulan Siber Güvenlik Birimi tarafından bu alanda olumlu gelişmelere yol açan;

- Gelişmekte olan ülkeler için Siber Güvenlik Rehberi (2006, 2007),
- Gelişmekte olan ülkeleri Destekleyici Siber Güvenlik Çalışma Programı (2007, 2009),
- Ulusal Siber Güvenlik/Kritik Bilgi Altyapılarının Korunması Kendini Değerlendirme Kılavuzu (2008),
- Siber Suç Mevzuatı Hazırlama Rehberi (2009),

Siber Suçları Anlamak: Gelişmekte Olan Ülkeler için Rehber (2009) gibi dokümanlar hazırlanmıştır (Ünver, Canbay ve Mirzaoğlu, 2009, s.12).

ITU-T bünyesinde, güvenlik ile ilgili faaliyetleri yürüten çeşitli çalışma grupları ise bu konudaki standardizasyonları belirlemektedir. Bu çalışma grubu, güvenlik çalışmalarının koordinasyonu ve önceliklendirilmesi, güvenlik konusunda farkındalığın arttırılması, temel güvenlik tavsiye kararlarının geliştirilmesi, gibi şu ana kadar 100'ün üzerinde karar almıştır (UDHB Şura, 2013 s.21, Ünver, Canbay ve Mirzaoğlu, 2009, s.12).

2.6.1.2. Avrupa Birliği (AB) kararları

AB, siber güvenlik konusunda öne çıkan konuları, Avrupa 2020 Stratejisi Planında yer alan Avrupa Dijital Ajandası (DAE) belgesinde aşağıdaki beş madde olarak vermektedir (İKV, 2013).

- *Siber dayanıklılığın sağlanması,*
- *Siber suçların büyük ölçüde azaltılması,*
- *Siber savunma politikası ve bu alandaki kabiliyetin Ortak Güvenlik ve Savunma Politikası kapsamında geliştirilmesi,*
- *Siber güvenlik için gerekli endüstriyel ve teknolojik kaynakların geliştirilmesi,*
- *AB'nin temel değerlerini yansıtan tutarlı bir AB uluslararası siber mekân politikası oluşturulması.*

AB'nin siber saldırılarla mücadele alanındaki düşüncelerini yansıtan "*Açık, Güvenli ve Emniyetli bir Siber Mekân*" başlıklı strateji belgesinde belirlenen plana göre bilişim sistemlerinin dayanıklılığının artırılması, siber suçların azaltılması ve AB'nin uluslararası siber güvenlik ve savunma politikalarını güçlendirilmeyi amaçlayan "Güven ve Güvenilirlik" tedbirleri ile ilgili maddeler aşağıda verilmektedir.

> ➢ *Avrupa Ağ ve Bilgi Güvenliği Ajansı* (European Network and Information Security Agency, *(ENISA))'nı modernize etmek ve AB kurumları için Bilgisayar Acil Müdahale Ekipleri (Computer Readiness Team, (CERT)) oluşturmak için yasa teklifi hazırlamak* (Yaşa, 2011, s.24).

- *Kişisel verilerin korunmasına ilişkin mevzuatın güncellenmesi çalışmaları kapsamında, güvenlik ihlali bildirimi hükümlerinin genişletilmesini incelemek* (Yaşa, 2011, s.24).
- *Siber ataklarla mücadele edecek yasal altyapı için teklif hazırlamak* (Yaşa, 2011, s.24).
- *Avrupa düzeyinde ve uluslararası düzeyde siber uzayda yargısal kurallara ilişkin yasal teklifler hazırlamak* (Yaşa, 2011, s. 24).
- *Takviyeli ağ ve bilgi güvenliği politikası oluşturmak* (EC.EUROPA, 2013).
- *Avrupa Siber Suçlar platformu kurmak (*EC.EUROPA, 2013).
- *Avrupa siber suç merkezi oluşturmanın yararını analiz etmek* (EC.EUROPA, 2013).
- *Siber suç ve saldırılara karşı uluslararası düzeyde mücadeleyi güçlendirmek* (EC.EUROPA, 2013).
- *AB çapında siber güvenlik hazırlığını yapmak, stratejisini ve direktifini hazırlamak* (EC.EUROPA, 2013).
- *Bilgisayar acil müdahale ekipleri kurmak* (EC.EUROPA, 2013).

Yine bu belge kapsamında ağ ve bilgi güvenliği (Network and Information Security, (NIS)) yönerge taslağı ile üye devletlerin, e-Ticaret platformları ve sosyal ağlar için güvenli bir dijital ortam sağlamakla yükümlü olması kararlaştırılmıştır (İKV, 2013).

2.6.2. Ülkemizdeki düzenlemeler

Ülkemizde siber güvenlikle ilgili düzenlemeler ve yapılan çalışmalar;

- **Siber Güvenlik Kurulu:**

"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 20.10.2012 tarih ve 28447 sayı ile resmi gazetede yayınlanmıştır. 6 maddelik karara göre bir "Siber Güvenlik Kurulu" kurulacaktır. Bu kurulun görevleri; siber güvenlikle ilgili alınacak önlemleri

belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak, bunların uygulanmasını ve koordinasyonunu sağlamaktır. Ayrıca bu belgelerin muhafaza edildiği sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirleri almakla yükümlü bulunmaktadır (Resmi Gazete, 2012).

- **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı:**

Ulusal siber güvenliğin temini için bütün sorumluluk Bakanlar Kurulu kararı ile Başkanlık görevi UDHB'na verilmiştir. Buna göre siber güvenlik ile ilgili politika, strateji ve eylem planlarını UDHB hazırlayacak ve diğer bakanlıkların, müsteşarlıkların ve kamu kuruluşlarının yapacağı işleri koordine edip onlara başkanlık edecektir. Bu kurumlar "Siber Güvenlik Kurulu" tarafından belirlenen politika, strateji ve eylem planları doğrultusunda verilen görevleri yapmak zorundadır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı;

> *"Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğini, kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasını, siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesini ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasına yönelik kamu ya da özel sektör tarafından işletilen bilişim sistemlerinin altyapılarının oluşturulmasını kapsar"* (Resmi Gazete, 2013a).

Bu eylem planında gerçekleştirilecek 29 eylem maddesi içinde yer alan Ulusal siber olaylarla müdahale merkezinin (USOM), sektörel ve kurumsal siber olaylara müdahale ekiplerinin (SOME) kurulması ve siber tehditleri

önleme projesinin gerçekleştirilmesi ile son kullanıcıların eğitimi ve bilinçlendirilmesi görevleri BTK'ya verilmiştir (UDHB Şurası, 2013, s.39).

- **Ulaştırma, Denizcilik ve Haberleşme Bakanlığı – TÜBİTAK İşbirliği Protokolleri:**

UDHB, TÜBİTAK, Bilim Sanayi ve Teknoloji Bakanlığı arasında işbirliği protokolü yapılmıştır. Bu protokolle "Elektronik Haberleşme Altyapısı - Üstyapısı, Siber Güvenlik, E-Devlet Hizmetleri, Bulut Bilişim ile Ar-Ge Projeleri" hizmetlerinin TÜBİTAK'tan alınmasına karar verilmiştir. Daha sonra Haberleşme Genel Müdürlüğü ile TÜBİTAK arasında;

"Ulusal Siber Güvenlik Teknoloji Geliştirme Programı Konusunda Danışmanlık Hizmetleri Alımı Sözleşmesi"

yapılmıştır. Buna göre;

" -Güvenlik Duvarı Yönetim Sistemi Geliştirilmesi,
-Siber Tehdit Tespit ve Önleme Sistemi Geliştirilmesi ve İşletilmesi,
-Gelişmiş Siber Casusluk Tehdit (APT) Analizi,
-Zararlı Yazılım ve Mücadele Analiz Merkezi,
-Ulusal İnternet Sürekliliği Planlanması Projesi"

bu kapsamda yapılmak üzere anlaşılmıştır (UDHB, 2013, s.39).

- **Ulusal Siber Güvenlik Tatbikatı 2011:**

BTK ve TÜBİTAK'ın koordinesinde yapılan Ulusal Siber Güvenlik Tatbikatı 2011'de 41 kamu kurumundan, özel sektörden ve sivil toplum kuruluşundan 200 'e yakın çalışan yer almıştır. Katılımcıların teknik becerilerinin artırılması için gerçek ve yazılı senaryolar üzerinden tatbikat gerçekleştirilmiştir (UDHB, 2013, s.40).

- **Siber Kalkan Tatbikatı 2012:**

BTK'nın koordinasyonunda haberleşme sektöründe faaliyet gösteren 12 işletmecinin katılımı ile 2012 yılında gerçekleştirilmiştir. Yurtiçi ve

yurtdışından İSS'lerin test sistemlerine 150 farklı kaynaktan DDoS saldırılar gerçekleştirilmiş ve erişim sağlayıcılarının DDoS saldırıları engelleme konusundaki kabiliyetleri test edilmiş, katılımcılar arasında bilgi ve tecrübe paylaşılması sağlanmıştır (UDHB, 2013, s.41).

- **Ulusal Siber Güvenlik Tatbikatı 2013:**

2013 yılında bu kez UDHB koordinasyonunda siber saldırılara karşı hazırlıklı olmak amacıyla "Ulusal Siber Güvenlik Tatbikatı 2013" yapılmıştır. BTK ve TÜBİTAK tarafından yürütülen bu tatbikat, 61 kamu ve elektronik haberleşme, enerji, savunma, finans ve sağlık gibi önemli alanlarda altyapıları olan kurum ve kuruluşların katılımı ile yapılmıştır. Siber saldırganların saldırı yöntemlerini tecrübe etme imkânı sağlanmıştır (BTK, 2013b).

- **SPAM'larla Mücadele Projesi:**

BTK başkanlığında, İSS ve yer sağlayıcı kuruluşlar 2009 yılında yeni bir proje başlatmıştır. SPAM'ların engellenmesine yönelik bu proje 3 faz olarak uygulanmış ve alınan sonuçlara göre istem dışı e-posta sayısının % 99 oranında azaldığı görülmüştür (UDHB Şurası, 2013, s.42).

- **Siber Tehditleri Önleme Projesi (STOP):**

Bu projede;

  - Bal küpü sistemi kurulması[6] (Siber tehditleri tespit etmek için)
  - Siber Güvenlik ve Eylem Planına göre işleyen raporlama sisteminin kurulması ve geliştirilmesi (Siber tehditlerle ilgili veri üretilmesi ve siber tehditlerin önlenmesi için gerekli yapıların oluşması)

ele alınmaktadır (BTK, 2013c).

---

[6] Bal küpü, bilişim sistemlerine karşı gerçekleştirilen saldırıların tespit edilmesi için kurulmuş tuzaklardır.

- **Elektronik Haberleşme Güvenliği Yönetmeliği:**

Resmi Gazete'de yayınlanan "Elektronik Haberleşme Güvenliği Yönetmeliği" (20.07.2008 tarih ve 26942 sayılı) ile sektörde yetkilendirilmiş işletmecilere yükümlülükler getirilmiştir. Bu yönetmelik 2009 ve 2013 yıllarında güncellenmiştir. Buna göre:

> *"Risk analizinde tespit edilen tehdit ve zafiyetler ile bunların yüksek, orta veya düşük şeklinde tasnifi ile gerçekleşme olasılıkları ve önlemleri, bir tehdit ve/veya zafiyetin gerçekleşmesi durumunda yürütülecek faaliyetleri ve bu faaliyetlerde görev alacak personel ile bunların yetki ve sorumluluklarının neler olacağını içeren iş akış diyagramları ve acil eylem planlarını, donanım-yazılım bileşenlerinin kurulumu, kullanımı ve işletimi ile bakım ve onarımı sırasında ortaya çıkan ve raporlanan problem ile uygunsuzlukları, 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 azaltılması"* ile ilgili alınacak önlemler belirtilmiştir. (Resmi Gazete, 2012b).

Bu yönetmelik ile işletmecilere "TS ISO/IEC 27001 veya ISO/IEC 27001" BGYS standardına uyum sağlanma zorunluluğu getirilmiştir.

Ayrıca 15.10.2010 tarihli "Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulanmasına İlişkin Tebliği", 24.07.2013 yürürlüğe giren "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkındaki Yönetmelik", 5070 sayılı "Elektronik İmza Kanunu", 6112 sayılı Türk Ticaret Kanunu ve e-imza ve kayıtlı elektronik posta düzenlemeleri ile bilgi güvenliği ve siber güvenlikle ilgili yasal mevzuatlar oluşturulmuştur (UDHB, 2013).

TÜBİTAK Siber Güvenlik Enstitüsü (SGE), Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Dairesi Başkanlığı, Türk Silahlı Kuvvetleri Siber Savunma Merkezi Başkanlığı, siber güvenlik hedeflerinin gerçekleşmesine destek olan Sivil Toplum Örgütleri, ülkemizde siber güvenlikle mücadele eden ve düzenlemeler yapan kurumların başında gelmektedir (UDHB, 2013).

3. İNTERNET DEĞİŞİM NOKTASI VE VERİ MERKEZLERİ

Bu bölümde öncelikle internet altyapısı ve internette veri iletiminde kullanılan yönlendirme protokolleri ve trafik değişimi anlatılmaktadır. İnternet değişim noktası ve veri merkezlerinin topolojik yapısı hakkında bilgi verildikten sonra internet değişim noktası ve veri merkezlerinin ekonomik ve stratejik önemi ve bilgi güvenliğini sağlamada rolü ele alınmaktadır.

3.1. İnternet Altyapısı ve Trafik Değişimi

İnternet farklı lokasyonlarda bulunan bilgisayar sistemlerinin iletişim kurabilme temeline dayalı bir altyapıdır. Ortak bir İnternet protokolü (TCP/IP)[1] kullanarak her birinin müşterileri ile trafik paylaşmasını kabul eden geniş, bağımsız bir ağlar grubudur (Jensen, 2009).

Bu ağın merkezinde birbirine yüksek hızlı bağlantılarla bağlı, sürekli çalışır haldeki bilgisayarlar bulunmaktadır. Bilgisayarlar arası iletişimin kurulabilmesi için bilgisayarımızın bu hizmeti sunan İSS ile bağlantı kurması gerekmektedir. Gerek bireysel gerekse kurumsal bütün tüketiciler internete erişmek üzere İSS'lerden hizmet almaktadır.

İSS'ler kullanıcıları internet ortamına taşıyabilmek için hizmet sunucularından oluşan bilgisayar donanımları, yönlendirme ve anahtarlama teknolojilerinin kullanıldığı transmisyon ekipmanları, bakır ve/veya fiber optik kablo erişim şebekesinden oluşan bir internet altyapısı kurmaktadır (Güngör ve Evren, 2002, s.16).

Büyük çaplı internet ağ işletmecileri genel olarak "Omurga Sağlayıcı" olarak adlandırılmaktadır. Omurga sağlayıcılar farklı coğrafyalarda ve kıtalarda altyapıları bulunan diğer İSS'lere trafik taşıma hizmetleri veren uluslararası

[1] TCP/IP(Transmission Control Protocol/Internet Protocol), Bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır. (http://tr.wikipedia.org)

işletmelerdir. Trafik taşıma hizmetlerinden dolayı, fiber, ATM[2], Çerçeve Röle (Frame Relay)[3], uydu gibi yüksek hızlarda çalışan altyapılara ihtiyaç duymaktadırlar (Güngör ve Evren, 2002, s.17).

İlk haberleşme altyapılarında iletim hattı olarak kullanılan bakır kablolar, gerek dayanaklılık gerekse bant genişliği kısıtlarından dolayı bugün yerini, üzerinden ışık hızında veri taşıma imkânı sunan, çevresel faktörlerden minimum etkilenen, günümüzde haberleşmenin başlıca altyapısını oluşturan fiber optik kablolara bırakmaktadır. Fiber optik kabloların uzak mesafelerde kullanılan tek modlu (single mode)[4] ve yakın mesafelerde kullanılan çok modlu (multi mode)[5] olmak üzere iki farklı tipi bulunmaktadır.

İnternet omurgalarının altyapılarında tek modlu kablolar kullanılmaktadır. Günümüz haberleşme teknolojileri olanakları ile bir çift fiber devre üzerinden 8 Tbps veri taşımak mümkün olmaktadır.

İnternet birçok farklı işletme, servis sağlayıcı, omurga sağlayıcı ve tüketicilerin oluşturduğu ağların birleşiminden oluşan bir platformdur. Omurga ağlar bu yapı içinde trafik taşıyan altyapılardır. Bugün servis sağlayıcılar arasında yapılan ara bağlantı anlaşmaları ile taşınan trafik hacmi baz alınarak, tarifeler belirlenmektedir (Güngör ve Evren, 2002, s.19).

Bu anlamda ara bağlantı yapan işletmeler arasındaki trafik akışını belirlemek ve yönetmek üzere yüksek kademeli protokol ve yönlendiriciler, çok önemli yer tutmaktadır.

---

[2]ATM (Asynchronous Transfer Mode) Genişbant ISDN (2Mbps ve üzeri hızlarda çalışmak üzere geliştirilen ISDN) şebekesinde kullanılan anahtarlama teknolojisidir,

[3]Çerçeve Röle, Yerel alan ağları ve geniş alan ağlarının uç noktaları arasında sürekli olmayan veri akışı için kullanılan bir haberleşme teknolojisidir (Güngör ve Evren, 2002).

[4]Tek Modlu, Sadece tek bir modu destekleyen fiberdir. (www.supernet.web.tr/fiber_optik_kablolama.asp)

[5]Çok Modlu, Ses, veri ve video sinyallerini içeren yüksek transmisyon oranları için yerel alan ağı kablolarıdır (www.supernet.web.tr/fiber_optik_kablolama.asp)

3.1.1. Yönlendirme protokolleri

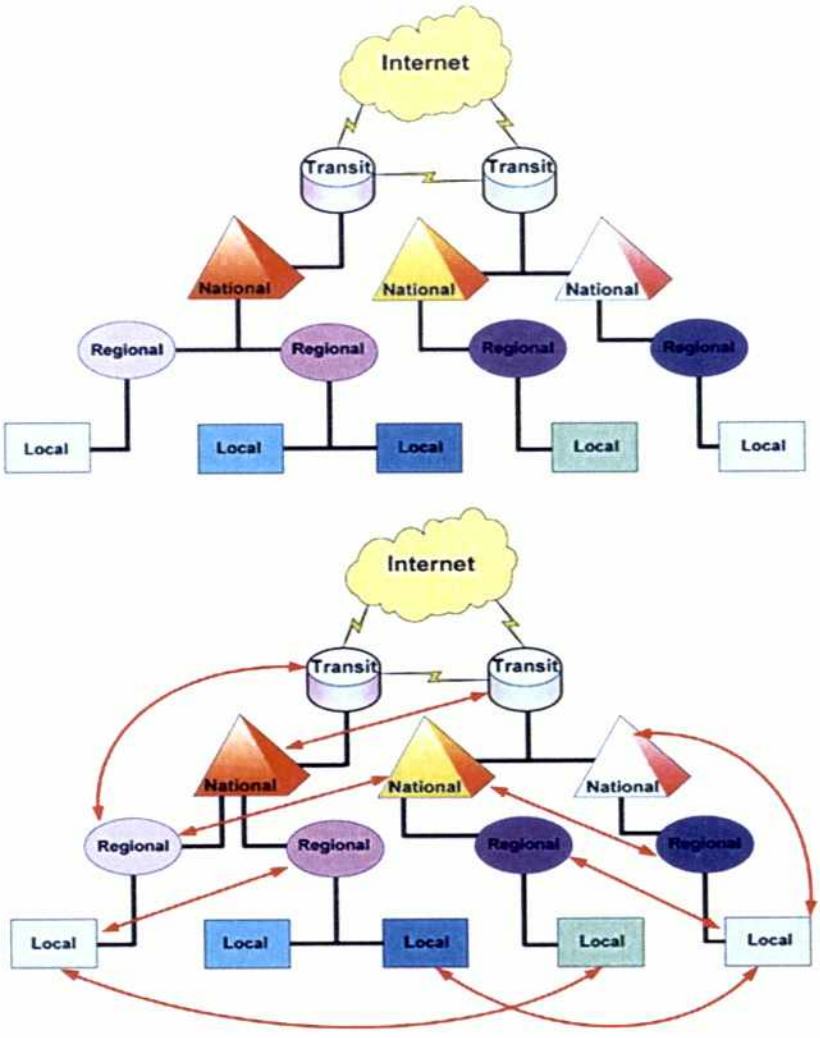
Bilgisayar sistemleriyle oluşturulan her bir veri paketlere ayrılarak altyapı üzerinden IP adresleri ile taşınmaktadır. IP adres paketleri, gönderen ve alacak adres olarak sınıflandırılmaktadır. İnternet altyapısında çalışan yönlendirme cihazları üzerinden geçen her paket hedef adresine göre yönlendirilmektedir. Yönlendirici cihazlar, gelen her pakete bakarak, hedef adresine göre gitmesi gereken istikamete paketi yönlendirmektedir (Docstore, 2013).

İnternet altyapısı işletme modeli, birbirinden bağımsız İSS'ler ve sahip oldukları havuz sistemler (Otonom sistemler, Autonomous Systems, (AS))'den oluşmaktadır.

AS, birden fazla yönlendirme cihazının fiziksel ve mantıksal olarak birbirleri ile irtibatlandırılması sonucunda oluşturulan IP ağ havuzlarıdır. AS ile IP ağlar, coğrafi konumlarına göre gruplara bölünerek sınırları çizilmekte ve bu şekilde daha kolay yönetilmektedir.

Değişik büyüklüklerdeki İSS'lerin internete erişim yöntemleri farklı olmaktadır. İnternetteki bir veriye ulaşmak isteyen bir İSS abonesinin veri trafiği, bu karmaşık yapı yüzünden bir çok İSS şebeke üzerinden geçmesi gerekebilmektedir. Şebeke sağlayıcıların birbirleri ile yapacakları her bağlantı, karmaşıklığı artırmakta, verimsizlik ve güvenlik açıkları ortaya çıkarmaktadır. Aşağıdaki şekilde, internet topolojisinin son yıllarda nasıl daha karmaşık bir hiyerarşiye dönüştüğü gösterilmektedir.

Şekil 3.1. İnternet topolojisinin karmaşık hiyerarşisi



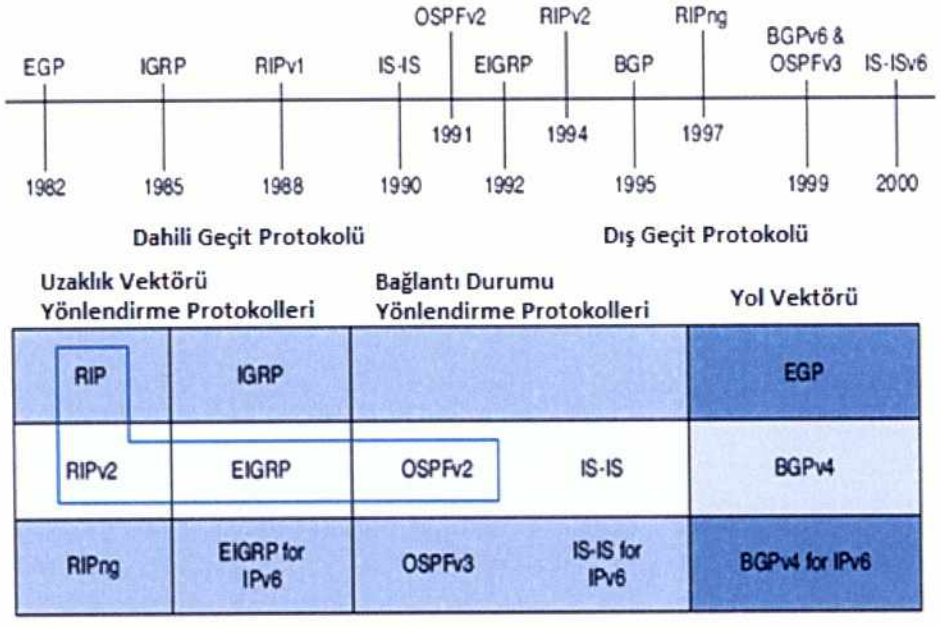
Kaynak: Cavalcanti, 2010

IP paketlerinin istenilen doğru adrese ulaşımı, yönlendiriciler tarafından yapılmaktadır. Hedef IP adresi, ağ geçidi (Gateway), hat durumunu gösteren işaret (Flag), yönlendiricinin bir sonraki sekmesine ulaşılan arayüz (Interface) gibi hedef adres bilgileri Yönlendirme Tablosu (Routing Table) adı verilen tablolarda tutulmaktadır. Yönlendirici, gelen paketlerin başlığında bulunan IP adreslerini yönlendirme tablosundaki bilgiler ile karşılaştırarak doğruluğu kanıtlanan paketleri hedefe yönlendirilmektedir. Her bir paketi yönlendirmek için sıradaki aygıtı araştırıp yönlendirme yapmaya bir atlama denilmektedir.

Her yönlendirici atlama sayısını, kendisine paket gönderen yönlendiriciden almaktadır.

Yönlendirme protokolleri, yönlendiricilerin birbirleriyle haberleşmesini ve gerekli yönlendirme bilgilerini birbirleriyle paylaşmalarını temel alan protokollerdir. 1980'li yıllardan günümüze ağlarda kullanılan bu protokollerin sınıflandırması ve evrimi aşağıdaki şekilde gösterilmektedir. (Cisco, 2009)

Şekil 3.2 1982-2000 arasında protokollerin sınıflandırılması



Kaynak: PTG, 2013

Yönlendirme işlemi, ağ topolojisi ve ihtiyaçlar göz önünde bulundurularak genellikle statik ve dinamik olmak üzere iki farklı şekilde yapılmaktadır.

3.1.1.1. Statik yönlendirme

Bu yönlendirme metodu küçük ağlarda kullanılmaktadır. Bu metot da yönlendirme yapılacak her bir cihazda hangi paketin nereye gideceğine karar veren mekanizma, cihazın yöneticisi tarafından el ile yapılan yapılandırma marifeti ile gerçekleşmektedir. Cihaz yöneticisi tarafından hangi paketin

nereye gitmesi gerektiği bilgisi statik olarak el ile tanımlanmaktadır. Hedef ağ ile bu paketi hedefine taşıyacak bir sonraki yönlendiricinin adresinin bilinmesi gerekmektedir.

Bu yönlendirme metodu cihaza yük getirmeyen, maliyeti düşük, ancak işletmesi oldukça zor olan bir metot olmaktadır(BTK, 2013d).

3.1.1.2. Dinamik yönlendirme

Dinamik yönlendirmede, aynı otonom sistem içerisinde yer alan yönlendirme cihazları, gelen paketleri gitmesi gereken yöne otomatik olarak karar vererek göndermektedir. Yönlendirme cihazlarının ilk yapılandırılması sırasında yapılan ayarlamalar ile otomatik olarak yönlendirme kabiliyetini kullanan bu yönlendirme metodu dinamik yönlendirme olarak adlandırılmaktadır.

Dinamik yönlendirme protokolü tanımlanırken öncelikle yönlendirme protokolünün türü seçilmeli, daha sonra da duyurulacak IP adresleri belirtilmelidir. Dinamik yönlendirme protokolleri yeteneklerine ve ihtiyaçlara göre çeşitlilik göstermekte olup yoğun olarak kullanılan protokoller aşağıda belirtilmiştir

Aynı otonom sistem içerisinde yer alan yönlendirme cihazları dinamik yönlendirme metotlarından Yönlendirici Bilgi Protokolü (Router Information Protocol, (RIP)), Dâhili Ağ Geçidi Yönlendirme Protokolü (Interior Gateway Routing Protocol, (IGRP)), Artırılmış Dâhili Ağ Geçidi Yönlendirme Protokolü (Enhanced Interior Gateway Routing Protocol, (EIGRP)) ve İlk Açık Yöne Öncelik (Open Shortest Path First, (OSPF)) gibi protokolleri kullanmaktadır. Yönlendirme protokolleri ile her cihazın kendisinden sonra gelecek yani paketin gönderileceği cihazları tanıması sağlanır (Cisco, 2009)

Farklı otonom sistemleri ile konuşma ihtiyacı olan yönlendirme cihazlarında ise Sınır Geçiş Protokolü (Border Gateway Protocol, (BGP)) kullanılmaktadır.

RIP Protokolü:

Bir TCP/IP ağındaki yönlendiricilerin birbirini otomatik olarak tanımasında kullanılan bir iç yönlendirme protokolüdür. İlk geliştirilen yol belirleme protokolüdür. Uzaklık (distance)-doğrultu (vector) algoritmasını kullanarak yönlendirme tablosunu oluşturmak üzere bilgi toplar ve bu bilgileri tablo halinde IP protokolünün kullanımına sunar. Uzaklık atlama sayısını, doğrultu bir sonraki atlamaya çıkış arayüzünü ifade etmektedir. En iyi yol seçimini yaparken tek kriter olarak atlama sayısına bakar ve maksimum 15 atlamayı kabul eder, ancak 15 atlamadan uzaktaki sistemler erişilemez olarak tanımlanır. Dolayısıyla küçük ağlarda kullanılan bir yönlendirme protokolüdür (Cisco, 2009).

IGRP Protokolü:

IGRP Cisco sistem tarafından 1980'lerin başlarında tasarlanan ve otonom sistemlerde kullanılan güçlü bir protokoldür. Ağ'ın bant genişliği, gecikme süresi, güvenilirlik, yük vb. gibi değerlerine bakarak en iyi yolu bulmaya çalışır. RIP'e göre daha geniş ağlarda çalışabilir. RIP'de basamak sayısı (paketin ulaştığı yönlendirici sayısı) 15 iken IGRP'de bu değer 255'dir (Cisco, 2009).

EIGRP Protokolü:

EIGRP, IGRP protokolünün yetersiz kalmaya başlamasıyla Cisco tarafından yeni bir sürüm olarak geliştirilmiştir. Maksimum basamak sayısı 224'dür. Alternatif yollar arasında çok yüksek geçiş hızı sunar. Yönlendirme tablosunda bir değişiklik olduğunda tüm tabloyu değil, sadece güncellenen kısmı göndermektedir. Böylece yönlendiriciye getirdiği ek yük de çok düşüktür ve ağ trafiğini de optimum kullandırır ve trafiği hızlandırır. Ayrıca EIGRP; IP, IPX, AppleTalk protokollerini de desteklemektedir. Bu nedenlerle Cisco yönlendiricilerde çok tercih edilen bir protokoldür (Cisco, 2009).

OSPF Protokolü:

OSPF, IP ağlarında kullanılmak üzere Internet Engineering Task Force (IETF) tarafından tasarlanmıştır. Açık standartlara sahip bir protokoldür. OSPF, dahili gateway protokol ailesindendir. Hattın durumuna göre iletişim kurarak, hat yoğunluğuna göre güncelleme yapar, hedefe gidecek en kısa yolu seçerek efektif çalışmayı öngörür (Cisco, 2009).

BGP Protokolü:

BGP protokolü günümüzde İnternet bağlantılarının kurulmasında ve genişletilmesinde kullanılan en temel protokollerin başında gelmektedir. BGP protokolü yapısı gereği daha karmaşık olmasına karşın internet omurgalarının temelini oluşturan bir protokoldür (PTG, 2013).

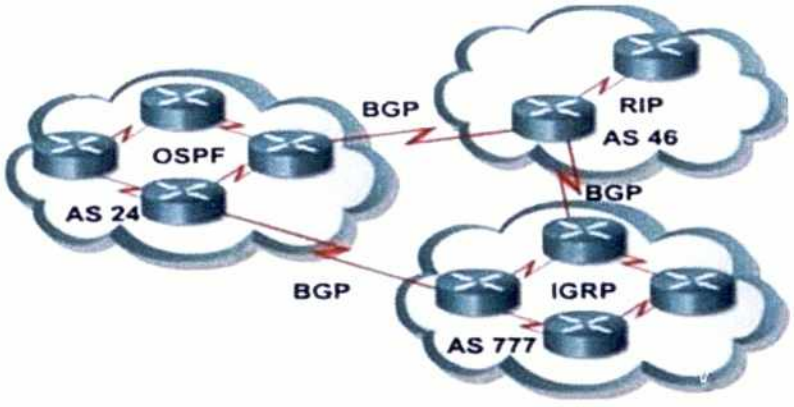
BGP ilk kez 1989 yılında bir internet standardı haline gelmiş ve RFC 1105 olarak tanımlanmıştır. Geçerli sürüm, BGP4 1995 yılında kabul edilmiş ve RFC 4271 olarak tanımlanmaktadır.

BGP'nin; ölçeklenebilir, kararlı ve karmaşık yönlendirme politikalarını desteklemek için gerekli mekanizmaları sağladığı kanıtlamıştır.

Bugün "BGP" den bahsederken, aslında BGP4 anlamına gelen 4. sürüm ifade edilmektedir. Çok az sayıda üretici eski versiyonlara destek verdiğinden önceki sürümler artık kullanılmamaktadır.

BGP kullanım alanı çok yaygın olan bir protokoldür. Ancak küçük ve orta boy ölçekli işletmeler, network tasarımı yaparken çok kapsamlı olmasından dolayı tercih etmezler. Genel olarak internet servis sağlayıcılarının, internet servislerini kullanıcılara sunmak, işletmeleri internet servisi ile buluşturmak, başka servis sağlayıcı ile iletişim kurmak gibi ciddi deneyim gerektiren operasyonlarda ve veri merkezi yönlendirici seviyesindeki cihazların üzerinde kullandıkları protokoldür (Çözümpark, 2013).

Şekil 3.3. BGP protokolünün büyük AS kullanım topoloji



Kaynak: (Çözümpark, 2013)

BGP Kullanmayı Gerektiren Durumlar;

- AS'den bir başka AS'e paket iletimini gerektiren durumlarda,
- Kullandığımız AS'in birden fazla AS'e bağlantısı olduğunda,
- AS üzerindeki trafiğin farklı rotalara yönlendirilmesi,

gerektiren durumlarda kullanılmaktadır.

BGP Kullanmayı Gerektirmeyen Durumlar;

- İnternet bağlantısında yalnıza tek bir network veri hattı ile bağlantı olduğunda,
- Rota yazmak, rota filtreleme yapmak gibi konularda deneyim veya detaylı bilgi olmadığında,
- BGP protokolünü aktif edeceğiniz yönlendiricilerimizde, BGP detaylarını kullanabilecek kadar kapasite ve işlemciye sahip olunmadığında BGP kullanmaya ihtiyaç bulunmamaktadır (Çözümpark, 2013).

BGP Komşuluk İlişkisi: İki cihaz arasında internet (TCP/IP) bağlantısı kurularak BGP konuşması sağlanır ve bu şekilde komşuluk kurulur. BGP komşularına "peer" adı verilmektedir. Komşulukların sınıflandırılması IBGP ve EBGP olarak incelenmektedir.

IBGP (Internal BGP): Aynı AS içerisindeki yönlendiricilerin komşuluk ilişkisi kurduğu durumda kullanılmaktadır.

EBGP (External BGP): Farklı AS'ler arasında yapılan bağlantılar EBGP sayesinde kurulmaktadır. EBGP komşuluğunda direkt bağlantı gerekmektedir.

BGP konuşan cihazlar, dış otonom sistemlerdeki, tüm cihazlar ile komşuluk kuramazlar. İnternet üzerinde 21.000 den fazla AS bulunduğu ve binlerce BGP çalışan yönlendiriciler olduğu göz önünde bulundurulursa bu durumun imkânsıza yakın olduğu anlaşılmaktadır (Çözümpark, 2013).

3.1.2. Trafik değişimi

Önceleri internet servisi sağlayan işletmeler arasında, şebeke kullanımına ya da trafiğe bağlı bir ücret olmaksızın trafik geçirilmesi benimsenmiştir. Ancak büyük piyasa oyuncuları bu düzenlemeleri zamanla iptal etmiş; şebeke kullanımına ve oluşturulan trafik miktarına dayalı ücretlendirme eğilimine gitmişlerdir. Bugün internet arabağlantı düzenlemeleri aracılığıyla trafik hacmine bağlı olarak yapılan ücretlendirme ve denklik anlaşmaları doğrultusunda yürütülen trafik politikaları bulunmaktadır (Güngör ve Evren, 2002, s.18).

İSS'ler arasında şebekelerin kullanımı ve kullanıcıların hizmet aldığı İSS'de erişmek istediği servislerin yer almaması durumunda İSS'ler arasında bir trafik değişimi ihtiyacı olmaktadır. Bu trafik değişimi, aşağıdaki başlıklar altında verilen Transit aktarma ve Denklik (Peering) anlaşmaları yoluyla yapılmaktadır (PCH, 2006).

3.1.2.1. Transit trafik

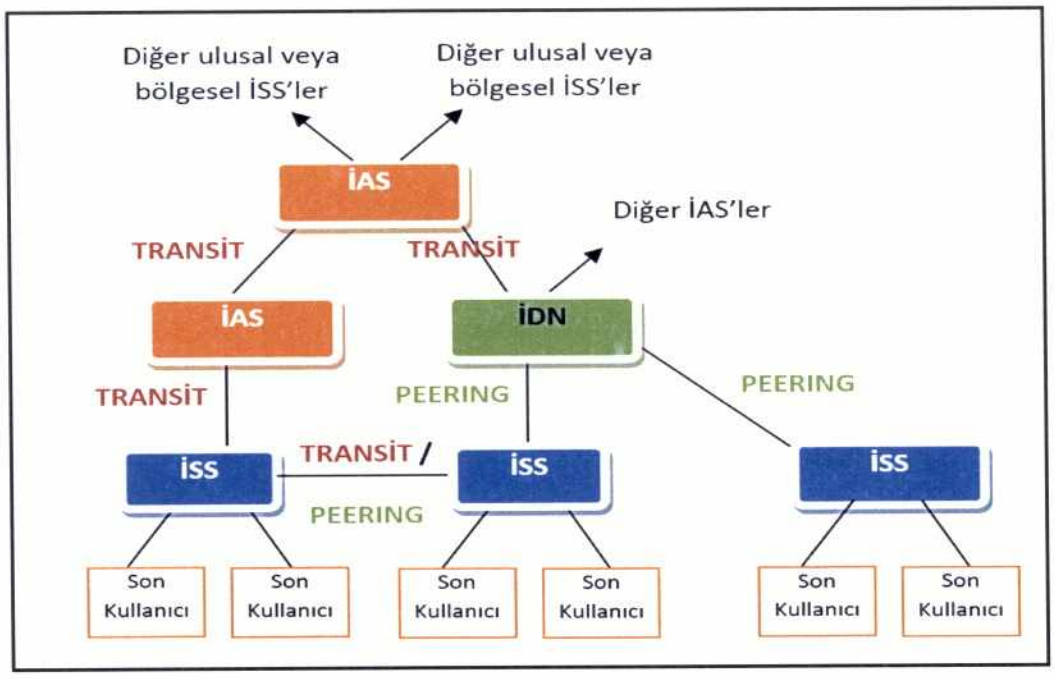
Genellikle büyük omurga sağlayıcı İSS'ler tarafından verilir. Transit taşıma, iki şebeke arasında doğrudan bağlantının olmadığı durumda şebekeler

arasındaki geçişin sağlanabilmesi için trafiğin üçüncü bir şebekeden geçirilmesi anlamına gelmektedir (Güngör ve Evren, 2002, s.19).
"Transit trafik değişimi", uluslararası trafik taşıyan ve omurga sağlayıcı olarak adlandırılan "büyük çaplı internet ağ işletmeci" şebekelerine erişim sağlayan İSS'ler ve yurt içindeki omurga sağlayıcılara erişim sağlayan İSS'ler olmak üzere görülmektedir (Güngör ve Evren, 2002, s.6).

Uluslararası transit trafik değişiminde İSS'ler küresel internet omurgalarına erişim sağlamaktadır. Tier-1 olarak adlandırılan yaklaşık 20 küresel ana omurga sağlayıcı bulunmakta olup hiyerarşik internet yapısının en üstünde yer alan bu işletmecilerin internetteki tüm şebekelere erişimi bulunmaktadır. Trafiğin uçtan uca (peering) kısmı direkt olarak değiştirilmekte böylece transit sağlayıcılar tarafından iletilmesi gereken toplam trafik azaltılmaktadır (ACORN-REDECOM, 2010).

Transit taşıma anlaşması olan bir ağ işletmecisi diğerine ara bağlantı için ödeme yapmakta ve böylece diğer ağın toptan müşterisi olmaktadır. Taşınan trafiğin hacmine ve aradaki bağlantının kapasitesine göre trafiği taşınan işletmeci trafiği taşıyan işletmeciye belirlenen tarifeler üzerinden ücret ödemektedir. Denklik (peering) ilişkisinin tersine, transit taşıma servisi satan ağ, trafiği transit müşterisinden denklik ortağına doğru yönlendirmektedir (Cavalcanti, 2010).

Şekil 3.4. İnternette trafik değişimi

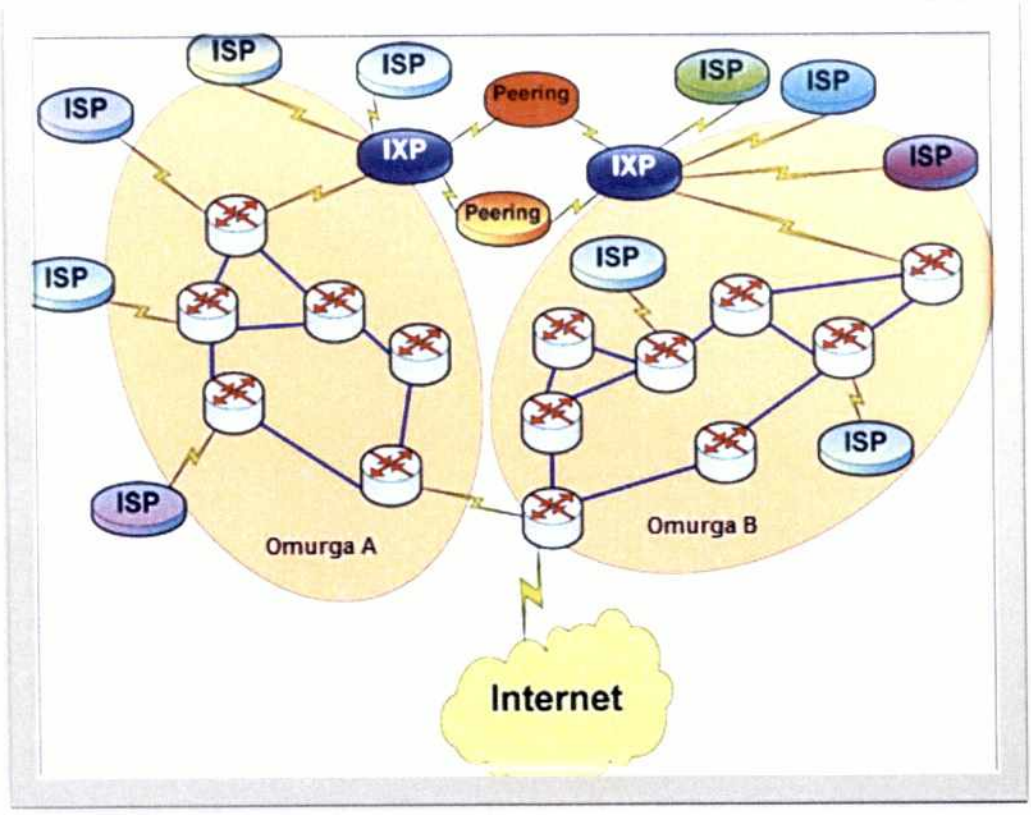


Kaynak: BTK, 2013d,

3.1.2.2. Denklik (Peering)

Değişik İSS'lerin kendi içindeki veri trafiğini, arada başka herhangi bir transit taşıyıcı ve herhangi bir ücret olmaksızın birbirlerine aktarmalarıdır. Denklik (Peering) trafik değişimi genellikle abone sayısı, şebeke büyüklüğü ve trafik hacmi bakımından eşdeğer şebekeler arasında gerçekleştirilmektedir (BTK, 2013d

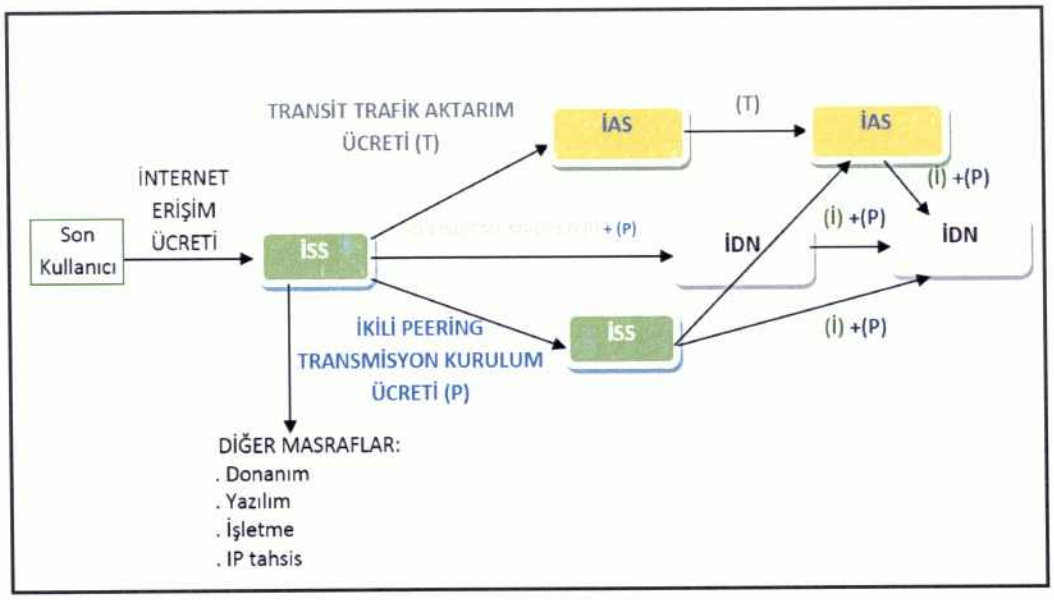
Şekil 3.5. Denklik (Peering) Topolojisi



Kaynak: Cavalcanti, 2010, s.3

Şebekelerin birinde oluşan trafik denklik anlaşması yapılmış olan diğer bir şebekede sonlandırılır, anlaşması olmayan 3. bir şebekede sonlanması söz konusu olmamaktadır. Şebekeler arasındaki trafik geçişi veya şebeke kullanımdan doğan bir ücretlendirme yapılmaması esasına dayanmaktadır (Güngör ve Evren, 2002, s.16).

Şekil 3.6 Trafik aktarım ücretlendirme metodolijisi



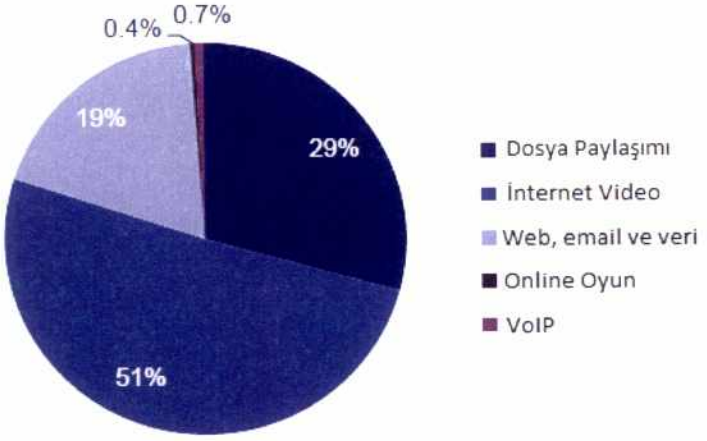
Kaynak: BTK, 2013d

3.2. İnternet Değişim Noktası ve Veri Merkezi Kavramları

Şebeke sağlayıcıların birbirleri ile yaptıkları her bağlantı, karmaşıklığı artırmakta, şebeke performansını olumsuz etkilemekte ve güvenlik açıklarını ortaya çıkarmaktadır. Servis sağlayıcılar, bu karmaşayı ve gereksiz veri trafiğini ortadan kaldırmak üzere İnternet Değişim Noktası (İDN) denilen yüksek hızlı anahtarlama teknolojilerini kullanmaktadır (KENDE, 2012).

Cisco'ya göre, 2011'den itibaren Son Kullanıcı İnternet trafiğinin %98'inden fazlası; özellikle video içerikleri, veri, web uygulamaları ve dosya paylaşımlarından oluşmuştur. Video yayını gibi en fazla bant genişliği gereksinimi olan içeriğin birçoğu temelde tek bir yerde meydana gelen, ama içeriğin son kullanıcılara ulaştırma maliyetini düşürmek için birden fazla yerde depolanan duruk (statik) içeriktir. Bu trafiği kaynaktan her bir hedefe (varış noktasına) ulaştırmak, büyük ölçüde kapasite gerektirir ve bütün kullanıcıları etkileyecek bir tıkanıklık (congestion, yığılma, sıkışıklık) yaratmaktadır (Cisco, 2013).

Şekil 3.7 İnternet trafik dağılımı



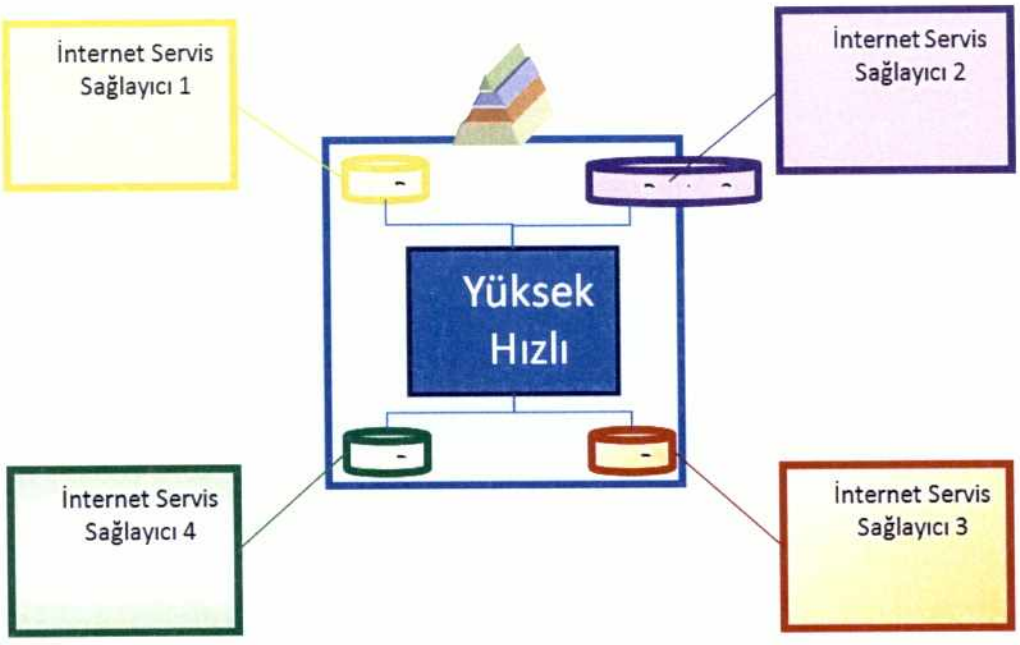
Kaynak: Cisco, 2013

Taşınan trafik artışı ve tüketicilerin farklı içeriklere erişme eğilimlerindeki artış daha hızlı bant genişliklerine olan ihtiyacı artırmaktadır. Bu artışa bağlı olarak İDN'ler ve veri merkezleri yaygınlaşmakta ve daha önemli hale gelmektedir (KENDE, 2012).

3.2.1. İnternet değişim noktası topolojisi

İDN, internet trafiğinin buluştuğu ve değiştirildiği noktalardır (Peering point). Bu sayede ortak bir noktada buluşan servis sağlayıcılar birbirlerine doğrudan trafik gönderebilmektedir. İDN birbirleri ile arabağlantı anlaşması yapan tüm İSS'lerin trafiklerinin bire bir buluşması ve değiştirilmesi anlamına gelmektedir (Türk-internet, 2013).

Şekil 3.8 Basit İDN yapısı



İDN'ler ikiden fazla İSS arasında denklik (peering) prensibine dayalı trafik değiş tokuşu yapılmasını sağlamak üzere belirlenen ortak bir noktada oluşturulan tesislerdir (BTK, 2013d, s.9). Servis sağlayıcı ve hizmet tabanlı ağ operatörlerinin arasındaki trafiğin, otonom sistemler arasında transit bir taşıyıcı olmadan değiştirilmesini sağlayan fiziksel bir altyapıdır (Cavalcanti, 2010, s.1,5).

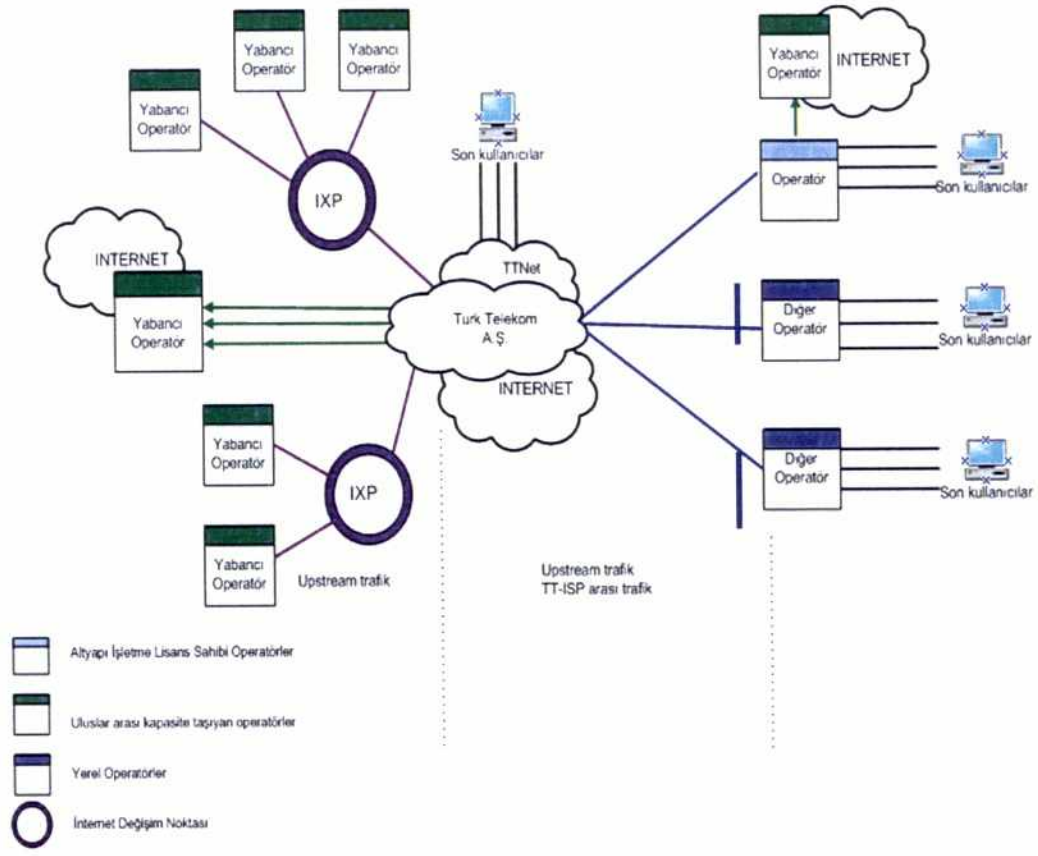
İDN'ler bölgenin en güçlü veri merkezinde kurulur yerleşik olduğu ülkeye, komşu ve bölge ülkelere hizmet sunar. İSS, kendisine ait donanım altyapısı ve yerel şebekeden kiraladığı hatlar aracılığı ile kullanıcıları yerel ve uluslararası internet omurgalarına taşımaktadır (Güngör ve Evren, 2002, s.6).

Cavalcanti'ye göre,

> *"Bir İDN, her birinin diğerine bağlandığı bir ya da daha fazla ağ anahtar / yönlendiriciden (router) oluşmaktadır. Trafiğin bir kısmını peering üzerinden değiştirmek suretiyle, transit taşıma sağlayıcıları*

tarafından iletilmesi gereken toplam trafiği azaltır. Böylece hizmet maliyeti azalır ve ağ performansı artar" (Cavalcanti, 2010, s.1,5).

Şekil 3.9 İnternet alt yapısı içinde İDN (IXP)



Kaynak: BTK, 2013d, s.9

İDN'ler, erişim talebinde bulunan taraf ile erişilen içeriği barındıran tarafın aynı sınırlar içerisinde yer aldığı durumda uluslararası bağlantıların kullanılmamasını sağlamakta böylece trafiğin dolaşmasından kaynaklanabilecek gecikmelerin azalması, hizmet kalitesini artırmaktadır. Diğer taraftan bağlantı maliyetlerinin düşmesi İSS'lerin kârlılığını artırarak bu gelirlerin altyapı güçlendirme faaliyetleri için kullanılmasına olanak sağlayabilmektedir (BTK, 2013d, s.7,10).

Şekil 3.10 Dünya'da internet değişim noktaları

Kaynak: Telegeography, 2013

İDN'lerin yaygınlaşması servis sağlayıcılar, işletmeler, akademik topluluk ve hükümetlerin işbirliği çabalarıyla gerçekleşebilmektedir. İDN kullanımının artmasına paralel olarak internet topolojisi gelişmekte, bağlantı hızı, gecikme ve trafik değişim maliyeti gibi performansların iyileşmesine yol açmaktadır (Cavalcanti, 2010, s.1,5).

Değişim noktasında mevcut bulunan ağ sayısı ile doğru orantılı olan İDN, büyük omurgalı ağ sağlayıcılarla bağlantı kurma eğilimindedir (Çiftçi, 2008, s.20, Cavalcanti, 2010, s.1,5).

3.2.2. Veri merkezleri

Veri merkezleri kamu, özel kurum ve işletmelerin kritik bilgilerinin yönetildiği, depolama ve yedekleme ünitelerini barındıran, uygulama ve sistem sunucularını, ağ katmanlarını bulunduran fiziksel ortamlardır. Daha genel anlamda veri saklama ve yedekleme, web, elektronik posta, alan adı hizmetleri, donanım, yazılım yönetim ve denetim hizmetleri, güvenlik, felaket kurtarma hizmeti, danışmanlık, tasarım, sistem entegrasyonu, kurulum hizmetleri veren büyük altyapılardır (İVMUEY, 2005).

Kurum ve işletmeler, verilerini dolayısıyla bilgi teknolojileri ekipmanlarını, güvenlik konusundaki çekinceleri, kontrolü elinde bulundurma alışkanlığı, başka bir lokasyonda verilere başkaları tarafından müdahale edilebileceği şüphesi gibi sebepler yüzünden kendi bünyelerinde tutmak istemektedir. Güvenlik alanındaki teknolojik gelişmeler, işletmelerin bilişim altyapısı ve uygulamalarını kendi bünyesinde barındırma yerine, bu hizmetler için çözüm sunan kuruluşlara yönelmelerine yol açmaktadır. Günümüzde iş dünyası ve kamu hizmetlerinde, süreklilik, yerel veritabanlarını merkezi veritabanında birleştirme ve kaynakları merkezi olarak yönetme büyük önem taşımaktadır (Bilgi Toplumu, 2013).

Bu merkezler yüksek düzeyli güvenliğin sağlandığı, sürekli hizmetin alındığı, ölçeklenebilir ve yönetilebilir bir ekosistem olmaktadır. Bulut bilişimin[6] kullanımındaki artışa paralel olarak, iş dünyası ve devlet kurumları veri merkezlerine güvenlik, çevresel etkiler ve standartlara bağlılık kriterleri açısından daha çok odaklanmaktadır.

Müşteri ihtiyaçları ve verilen hizmetlerdeki büyüme potansiyelini önceden belirleyerek gerekli önlemleri almak; enerji, soğutma, telekomünikasyon ve ağ ekipmanları için gerekli altyapı donanımları ve güvenlik önlemlerini tesis etmek, veri merkezlerinin başlıca fonksiyonlarındandır (İVMUEY, 2005).

Veri Merkezlerinde ölçek büyüdükçe bu yatırımlar açısından verimlilik de artmaktadır (UDHB Raporu, 2010, s.9). Aşağıdaki tabloda, 2008 yılında ABD'de gerçekleştirilen Çalıştay (LADIS)[7]'da orta büyüklükteki bir veri merkezi ile büyük ölçekteki veri merkezinin değişik parametreler açısından maliyetleri gösterilmektedir. Genel olarak dünyanın birçok bölgesinde veri merkezlerinde tüketilen enerji maliyetleri genel maliyetlerin büyük oranını teşkil etmektedir.

---

[6] Bulut bilişim, düşük yönetim çabası veya servis sağlayıcı etkileşimi ile hızlı alınıp salıverilebilen ayarlanabilir bilişim kaynaklarının paylaşılır havuzuna, istendiğinde ve uygun bir şekilde ağ erişimi sağlayan bir modeldir (www.tubitak.gov.tr/tubitak_content_files/.../Korkmaz_Bulut_Bilisim.ppt, s.11)

[7] LADIS:Large-Scale Distributed Systems (Büyük Ölçekli Dağıtık Sistemler)

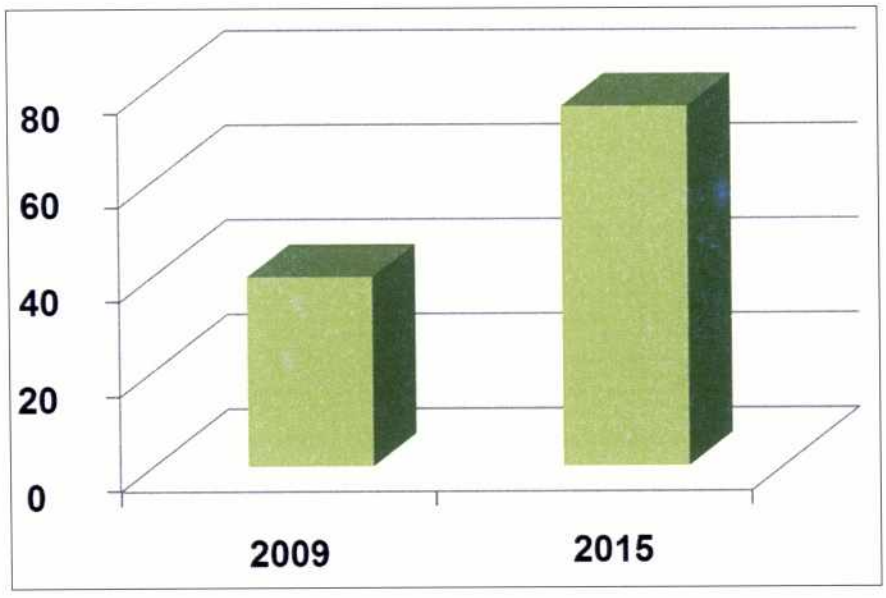
2009 -2015 yılları arasında dünyadaki sunucu sayısında yaklaşık iki kat artış öngörülmektedir (UDHB Raporu, 2010, s.9).

Tablo 3.1.Farklı büyüklüklerdeki veri merkezi işletme maliyetleri

Teknoloji	Maliyet orta ölçekte veri merkezi (1000sunucu)	Maliyet büyük ölçekte veri merkezi (50.000sunucu)	Oran
Ağ	$ 95 Mbit/sn/ay	$ 13 Mbit/sn/ay	7.1
Depolama	$ 2,20 Gbyte/ay	$ 0.40 Gbyte/ay	5.7
Yönetim	Yaklaşık 140 sunucu/yönetici	Yaklaşık 1000 sunucu/yönetici	7.1

Kaynak: Hamilton, 2008

Şekil 3.11 Dünyadaki sunucu sayısında artış oranı



Kaynak: UDHB, 2010, s.10

Sunulan hizmete göre temel olarak yer paylaşımı (co-location)[8] ve barındırma (hosting)[9] olmak üzere iki farklı hizmet modeli sunulmaktadır (İVMUEY, 2005).

Şekil 3.12 Taşınabilir Veri Merkezi

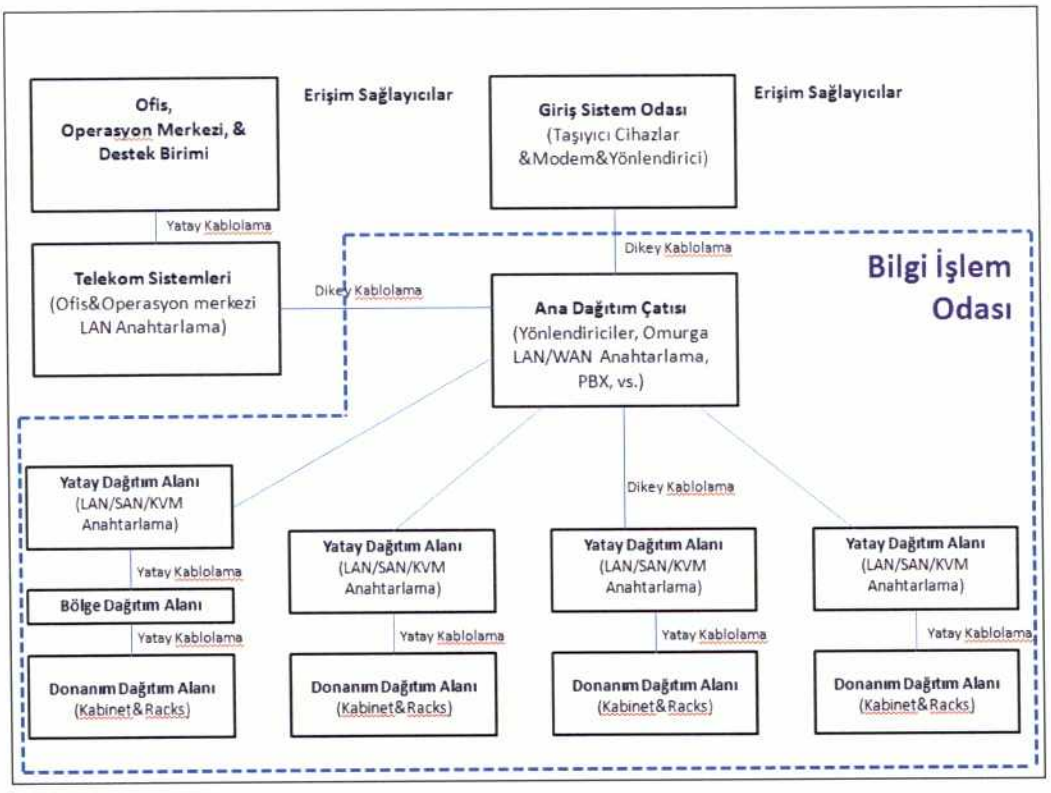
İnternet veri merkezi yapısında uygulama sunucuları, erişim sunucuları, müşterilerin sunucuları (co-located server), depolama birimleri, yönlendiriciler (router), güvenlik sistemleri ve yönetim araçları gibi donanımlar yer almaktadır. Ayrıca enerji birimleri (güç kaynağı bağlantı ve dağıtım elemanları, kesintisiz güç kaynağı, jeneratör), klima, yangın uyarı ve söndürme sistemleri, güvenli giriş sistemleri, telekomünikasyon şebekesine bağlantı birimleri gibi altyapı elemanları da internet veri merkezini oluşturan temel fiziksel bileşenlerdir (İVMUEY, 2005).

---

[8] Yer paylaşımı hizmeti; veri merkezlerinden kendi BT sistemlerini internet veri merkezi alanına kurmak için hizmet alan kuruluşların, internet veri merkezinin temel altyapı olanaklarını ve ağ altyapısını kullanması ayrıca eğer isterse yönetim hizmetini kullanmasıdır.(İnternet Veri Merkezi Uygulamalarının Ekonomisi ve Yapılabilirliği, 2005, s.9)

[9] İnternet uygulamalarının elektronik ortamda iletilebilmesi için gerekli uç birim görevini gören her bilgisayara barındırıcı "host", bu hizmetin sunulmasına ise barındırma "hosting" denir". Barındırıcıların alan adları vardır (domain name). Bu alan adları IP ile ilişkilendirilmiş şekildedir (Güngör ve Evren, 2002, s.8)

Şekil 3.13 Veri merkezi fiziksel bileşenleri



Kaynak: TIA, 2006

3.3. İnternet Değişim Noktası ve Veri Merkezlerinin Önemi

Türkiye'de telekomünikasyon alanındaki ilerlemelerle internet kullanıcı sayısının artmasıyla doğru orantılı olarak veri merkezi alanında da büyük gelişmeler yaşanmıştır. Kullanıcı sayısındaki artış, telekomünikasyon alanındaki yoğun rekabet ve Bankacılık ve Denetleme Kurulu (BDDK)'nın bankalara ait veri merkezlerinin Türkiye'de inşa edilmesi için getirdiği zorunluluklar üzerine Türkiye veri merkezi alanında %60'lık büyüme göstermiştir (İVMUEY, 2005).

Kamu kurumlarında e-devlet ve vatandaşa sunulan hizmetlerin internet ortamına geçirilmesi projeleri bilgi teknolojileri harcamalarını artırmıştır. Türkiye yapılaşma çalışmaları bünyesinde kamu kurumlarının hizmet kalitesini geliştirmek amaçlı bilgi teknolojileri ve veri merkezi alanlarında

yoğun yatırımlar yapmıştır (İnternet Veri Merkezi Uygulamalarının Ekonomisi ve Yapılabilirliği, 2005, s.9,15). Özellikle büyük projelerde (Türkiye'de e-Dönüşüm gibi), bilişim teknolojisi kullanılan her alanda birleştirme, paylaşma ve dış kaynak kullanımına gidilmesi ihtiyacı internet veri merkezi hizmetlerinin kullanılması gereğini ve önemini artırmıştır (İVMUEY, 2005).

Ülkemizde içerik yurtiçi ve yurtdışındaki birçok veri merkezinden yayınlanmaktadır. Türkiye'deki veri merkezi endüstrisinin son dönemlerdeki gelişimine karşın talebi karşılamada yeterli olmaması ve İDN yapısının bulunmaması içeriğin büyük kısmının yurtdışına çıkmasına yol açmaktadır. Tahmini olarak %55-65 gibi içerik yurt dışında depolanmaktadır (UDHB, 2010, s.19).

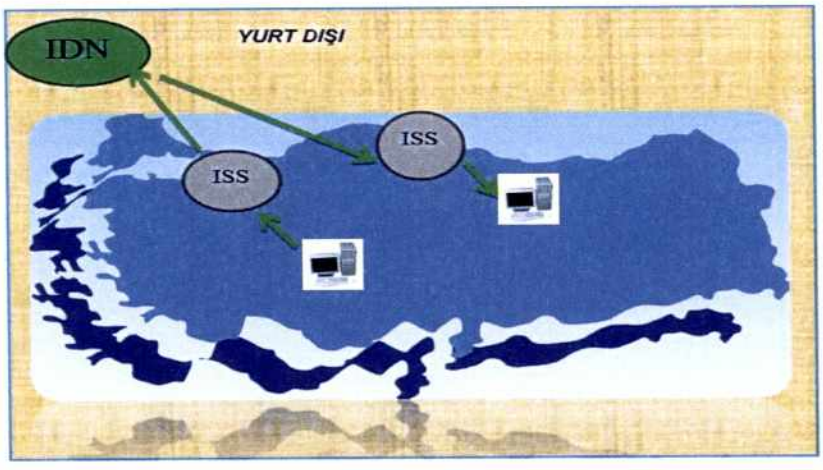
Almanya'daki kullanıcıların ülke dışına giden trafiği 600 Gigabit/sn iken Türkiye'nin yurtdışına giden trafiği 400-500 Gigabit/sn olduğu görülmektedir. Bu noktada bir değerlendirme yapacak olursak internet penetrasyonu Türkiye'ye oranla daha yüksek olan Almanya'nın trafiğinin yine Türkiye'nin yurtdışına giden trafiğine oranla daha düşük olması, Almanya'nın güçlü veri merkezlerine ve İDN'lere gösterdiği önemi ortaya koymaktadır. Bu yapılar sayesinde ülke kendi içeriğini kendi sınırları içinde tutabilmektedir. Bunun yanı sıra "Google, MSN, YouTube, Facebook" gibi globalleşmiş büyük şirketler tüketicilerine ulaşabilmek için altyapı olarak Alman Veri Merkezlerini kullanmaktadır. Bu düşünceyle veri merkezlerini güçlendirip, İDN'lerin artırılması bilgi güvenliği, uluslararası ekonomik istihbarat, vergi ve işletmelerin rekabet gücü açısından büyük avantajlar sağlamaktadır (Akan, 2013, s.19,22).

Özetle İDN 'lerinin önemli etkileri şu şekilde sıralanabilir;

- Siber güvenliğin sağlanması,
- Ağ performansının artması,
- Servis kalitesinin artması,

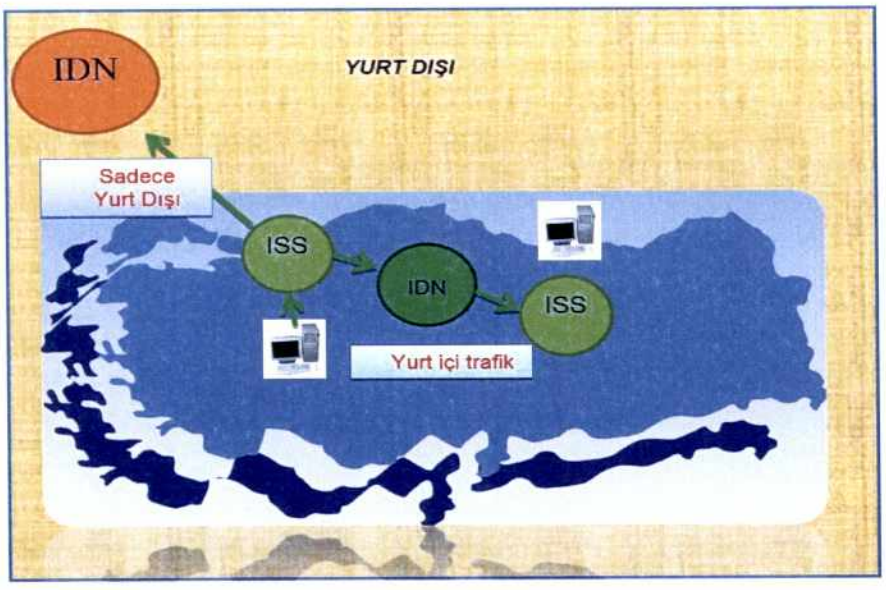
- Global içerik sağlayıcılar ve bölgesel İSS'ler için alternatif bir bağlantı noktası olması (BTK, 2013d)
- Uzun mesafe bağlantı maliyetlerini ortadan kaldırması,
- Ulusal kapasitenin daha düşük maliyette olması ve bu alanda yatırım yapılması ve yerel kullanıcılar için bant genişliği sağlanması,
- Yerel bağlantılarda yaklaşık 10 kat daha hız artışı sağlanması,
- Daha yüksek hız ve daha ucuz bağlantı sayesinde, yeni ulusal içerik sağlayıcılar ve servislerin oluşması,
- Trafik yoğunluğunun azalması ve ters yöndeki trafik için işletmelere daha fazla seçenek sunulması daha yumuşak ve daha rekabetçi piyasa koşullarının oluşmasını sağlamaktadır (Internetsociety, 2013).

Şekil 3.14 Ülke içindeki trafiğin yurtdışından dolaşması



Kaynak: BTK, 2013d, s.9-15

Şekil 3.15 Ülke içindeki trafiğin ülke içinde kalması



Kaynak: BTK, 2013d, s.9-15

3.3.1. Stratejik ve ekonomik önemi

İDN'ları ve veri merkezleri altyapıları sayesinde Jeopolitik açıdan önemli bir konuma sahip Türkiye, Avrupa, Balkanlar, Ortadoğu ve Kafkasların kavşak noktası olma imkânına sahip olmaktadır. Böylece dünyanın uzak köşesindeki birçok ülkenin ve özellikle Avrupa'nın bu bölgelerdeki üssü haline gelecektir (Akan, 2013, s.12).

İlerleyen yıllarda Çin ve Hindistan'ı Avrupa'ya bağlayan fiber altyapıların Rusya ve Süveyş-Hint Okyanusu yolu yerine Türkiye üzerinden geçişi için gerekli altyapıyı oluşturmak, ülkemizin Asya ve Avrupa'yı bilişim anlamında da birbirine bağlayan vazgeçilmez bir köprü olmasını sağlayacaktır. Bunun sonucu olarak Türkiye'nin bilişim hizmetleri sağlayan dış kaynak (outsourcing) ülkesi olması çok kolaylaşacaktır (Akan, 2013, s. 12,13).

MSN, Facebook, YouTube, Google gibi dünya çapında teknoloji devlerinin Türkiye'de altyapı kurmaları, yeni teknolojilerin gelişmesine ve nitelikli

işgücünün artmasına olanak tanımaktadır. Doğu'ya ve Avrupa'ya yönelik bilişim hizmeti üretmek için işbirliği fırsatı doğmasıyla, Türkçe içeriklerin bölgedeki diğer ülkelerde yaşayan insanlara daha kolay ulaşması mümkün olabilecektir (UDHB raporu, 2010, s.15, Akan, 2013, s.13).

Global veri merkezlerinin artması ülkenin bölgesel bir İDN'ye dönüşmesi açısından önemli olup, bölgedeki diğer ülkelerin İSS'leri ve içerik sağlayıcıları içinde ilgi odağı olabilmektedir (BTK, 2013d, s.9,15).

İDN'ye sahip olmak beraberinde pek çok avantaj getirmektedir. İşletmeler açısından; başlangıçta pazar payı küçük İSS'lerin lehine olması piyasanın gelişmesine katkı sağlayacaktır. Diğer taraftan küçük işletmeciler, uluslararası ve yurtiçindeki diğer İSS'lere bağlantı maliyetlerinin düşmesi ile altyapılarına daha fazla yatırım yapma imkânı bulabileceklerdir (BTK, 2013d, s.10,15).

Ulusal İDN ile çevrimiçi hizmetlere eşit olarak tüm ulusal kullanıcılar erişilebilmektedir. İDN, rekabet fırsatları yaratarak internet hizmetlerinin makul bir fiyatta sunulmasını ve kalitesinin artmasını sağlamaktadır (Internetsociety, 2013).

İşletmecilerimizin, ulusal bir İDN'ye katılımı ülkemizin sosyo-ekonomik yapısını ve ticari faaliyetlerini geliştirmek açısından son derece önemlidir (Ulaştırma, 2010). Ulusal bir İDN ve veri merkezi altyapısı, birçok sektördeki uluslararası firmaların Türkiye'ye daha fazla yatırım yapmalarına imkân yaratabilmektedir (UDHB raporu, 2010, s.16).

3.3.2. Operasyonel önemi

İDN yapısı; gelişmiş yönlendirme verimliliği ve daha az hata toleransı, gecikme ve bant genişliği gereksinimleri açısından da avantaj sağlamaktadır. Bir İDN'de direkt olarak denklik (peering) prensibine dayanarak aktarılan trafik faturalandırılmamaktadır (Cavalcanti, 2010, s.1,5).

İDN'ler ile alternatif yollar oluşturularak veri akışında çökme, kesinti ya da yavaşlama olma ihtimali ortadan kaldırılabilmektedir. Trafiğin tek bir omurga yerine alternatif omurgadan geçmesi trafiği rahatlatmakta ve hız kazandırmaktadır (Turk-İnternet, 2013).

3.3.3. Veri güvenliği açısından önemi

Veriye ulaşmada izlenilen güzergâhtaki her fazladan nokta geçişi, bilgi güvenliği açısından tehdit oluşturmaktadır. Güçlü bir İDN'nin varlığı güzergâh yolunun kısalmasını sağladığından bu tehditler en aza inmektedir (BTK, 2013d, s.11)

Güçlü bir İDN'nin varlığı, o bölgede internet trafik akışı açısından bir ağırlık merkezi oluşturacağından, bilgi güvenliği ve gizliliğinin korunmasında Türkiye'ye büyük avantaj sağlayacaktır (Akan, 2013, s.13).

Ayrıca gerektiğinde, İDN'deki internet servis sağlayıcıları arasında güvenlikli ve direk arabağlantı imkânı, bu iki İSS arasındaki trafiğin dinlenebilirliğini azaltmaktadır.

Ülkenin kendine ait bir İDN'i olması sayesinde, trafik akışının yurtdışındaki bir İDN'nin ya da transit geçişin kullanılmasını gerektirmemesi, yurt dışı kaynaklı siber tehditlerin ihtimalini de azaltmaktadır. Kamu kurumlarının birbiri ile haberleşmesindeki trafik değişiminin yurtdışından gerçekleşmesi siber güvenlik açısından zafiyetin doğmasına neden olmakta ve İDN altyapısının önemini ortaya çıkarmaktadır (BTK, 2013d, s.11).

4. DÜNYADA VE TÜRKİYE'DE İNTERNET DEĞİŞİM NOKTASI VE VERİ MERKEZİ UYGULAMALARI

Bu bölümde Avrupadaki önemli İnternet Değişim noktaları incelenmiş ve ülkemizdeki durumdan bahsedilecektir.

4.1. Dünyadaki Önemli Değişim Noktaları ve Veri Merkezleri

İDN'ler, Londra, Amsterdam, Frankfurt, Hong Kong, Singapur gibi Dünyanın en büyük finans merkezleri haline gelmiş ve büyük veri merkezleri bulunan şehirler etrafında yoğunlaşmışlardır. Bu ülkelerin İDN'leri kamu kurumları, ticari işletmeler veya İSS'lerden oluşan birlikler tarafından işletilmekte ve işletim maliyetleri katılımcı İSS'ler arasında paylaşılmaktadır (Jensen, 2009, s.12).

Kasım 2009'da Avrupa'da 33 ülke ve 115 şehre dağılmış olarak toplam 389 İDN mevcuttur (Cavalcanti, 2010, s.1,5). Londra'da LINX, Frankfurt'ta DE-CIX, Amsterdam'da AMS-IX bölgenin 3 dev İDN'si konumundadır (UDHB Raporu 2010, s.20). Romanya'da NXData ise 120 üyeli bir İDN'ye sahiptir.

İDN bulunmayan ülkeler ise Arnavutluk, Bosna Hersek, Sırbistan, Lichtenstein gibi küçük veya serbestleşmemiş ülkeler ve Türkiye'dir (UDHB Raporu 2010, s.20).

Güçlü veri merkezleri ve İDN'si olan ülkelerin bulunduğu yerler bilişim sektörü için de önemlidir. Cisco gibi firmalar Avrupa'daki en önemli noktasını AMS-IX'in civarına kurmuştur.

Türk Telekom, LINX, AMS-IX, ve DE-CIX'e doğrudan bağlıdır. Ancak Türkiye'de 7 servis sağlayıcının birlikte kurmakta olduğu TNAP adlı İDN henüz başlangıç safhasındadır (UDHB Raporu 2010, s.20).

Nüfus yoğunluğu, coğrafi özellikler, ekonomik gelişmişlik düzeyi gibi faktörlerden kaynaklanan değişiklikler İDN sayılarını etkilemektedir. (BTK, 2013d, s. 12,17).

Tablo 4.1. İDN'lerin bölgelere göre dağılımı

Bölgeler	Nisan 2006	Ekim 2012	Değişim (%)
Afrika	18	22	+22
Asya-Pasifik	60	76	+27
Avrupa	85	137	+61
Güney Amerika	20	34	+70
Kuzey Amerika	76	88	+16
Toplam	259	357	+27

Kaynak: BTK, 2013d, s.12

İDN'si bulunmayan ülkeler, internet bant genişliğini diğer ülkelerden ithal etmektedirler. İDN'si olup ta ihtiyaç fazlası bant genişliği üreten ülkeler (Örneğin: Hollanda) diğer ülkelere bant genişliği ihraç edebilmektedir. Ek-1 de dünyadaki İDN'ler ile ilgili daha detaylı bir liste verilmektedir.

Tablo 4.2. Ülkelerde yer alan İDN sayıları

İDN Sayısı	Ülkeler
1	Angola, Arjantin, Bahreyn, Botsvana, Kamboçya, Şili, Kolombiya, Kongo, Fildişi, Hırvatistan, Küba, Kıbrıs, Danimarka, Dominik Cumhuriyeti, Gana, Yunanistan, Macaristan, Haiti, İzlanda, İsrail, Kenya, Laos, Lübnan, Litvanya, Malavi, Malezya, Malta, Moritus, Moğolistan, Mozambik, Nepal, Nikaragua, Pakistan, Panama, Paraguay, Portekiz, Porto Riko, Suudi Arabistan, Slovenya, Sri Lanka, Svaziland, Tayland, **Türkiye**, Uganda, Zambiya, Zimbabve
2	Avusturya, Bangladeş, Belçika, Bulgaristan, Kanada, Ekvator, Mısır, Estonya, Finlandiya, Lüksemburg, Hollanda Antilleri, Nijerya, Norveç, Peru, Filipinler, Romanya, Slovakya, Tanzanya, Vietnam
3	Çek Cumhuriyeti, Singapur, Güney Afrika, İsviçre, İrlanda
4	Kore, Tayvan,
5	Hollanda, Polonya, Ukrayna
6	İspanya
7	Hindistan, Endonezya, İtalya, Yeni Zelanda
10 ve üzeri	**Avustralya, Brezilya, Fransa, Almanya, Japonya, Rusya, İsveç, İngiltere, ABD**

Kaynak: BTK, 2013d

"İnternet Trafik Değişimi" raporuna göre, tek İDN kurularak tüm trafiğin buraya yönlendirilmesindense daha fazla noktaya özellikle nüfusun yoğun olduğu bölgelere İDN'ler kurulması ekonomik avantaj sağlamaktadır (OECD, 2012) .

Şekil 4.1.Ülkemize yakın bölgelerde bulunan İDN'ler

Kaynak: Telegeography, 2013

İDN-İSS arası uzaklık bakımından Avrupa ve Amerika kıtaları farklılık göstermektedir. Amerika'daki İDN'lere bağlantı sağlayan İSS'ler altyapılarını genişletmek durumunda kalmaktadır. Avrupa'daki İDN'lere bağlantısı olan İSS'ler genellikle aynı bölgede yer almaktadır (BTK, 2013d, s.12,17).

İSS'ler arası internet trafiği değişimi ticari anlaşmalarla yapılmaktadır. Ancak 1997 yılında Avustralya regülasyon kurumu, en büyük İSS'in diğer üç büyük İSS ile denklik anlaşması yapmasını zorunlu hale getiren kararı bu anlayışa farklı bir yaklaşım getirmiştir (BTK, 2013d, s.12,17).

Aşağıdaki başlıklar altında, dünyadaki önemli değişim noktası ve veri merkezleri hakkında daha detaylı bilgiler verilmektedir.

4.1.1. Frankfurt (DE-CIX)

Frankfurt DE-CIX dünyanın en büyük İDN'sidir. 55'den fazla ülkede İDN durumundadır. DE-CIX doğrudan IP bağlantısı için altyapı sağlar (de-cix, 2013). 1995 yılında kurulan DE-CIX trafik hacmi ve üye sayısı bakımından Avrupa'nın en büyük İDN'lerinden birisi olmuştur. DE-CIX Frankfurt

Telegeography' de 1. sırada yer almıştır. Frankfurt DE-CIX'in arasında Türk Telekom'unda olduğu 480'in üzerinde üyesi bulunmaktadır. Frankfurt, Equinix, Interxion ve Telecity Group vb. olmak üzere 18 veri merkezinde DE-CIX'in bulunuşu bölge de değişilmez bir internet değişim merkezi olmasını sağlamıştır (BTK, 2013d, s.12,17).

Şekil 4.2.Frankfurt DE-CIX

Kaynak: Datacenterdynamics, 2013

DE-CIX, kar amacı olmayan üyelerden bağımsız bir birlik tarafından işletilmektedir. Frankfurt'un 11 farklı noktasında toplanan yedekli hatlar üzerinden hizmet veren DE-CIX'in 2007 yılından bu yana %100 erişilebilirlik sağlamaktadır (BTK, 2013d, s.12,17). DE-CIX endüstrinin en güçlü ve gelişmiş peering platformlarında çalışmaktadır. DE-CIX, İSS geniş bant sağlayıcıları, içerik dağıtım ağları, web barındırma ve diğer işletmelerin her türlü IP performanslarını geliştirmekte ve onların IP taşıma maliyetlerini düşürmektedir (De-Cix, 2013). DE-CIX'ten en yoğun zamanlarda saniyede 1,7 terabitten fazla elektronik veri aktarımı gerçekleşmektedir. Dünyanın en büyük veri değişim noktası, Almanya'daki veri trafiğinin yaklaşık yüzde 90'ını ve tüm Avrupa'nın veri trafiğinin yarısına yakın veriyi taşımaktadır (Investinhessen, 2013).

4.1.2. Londra (LINX)

İngiliz İnternet Servis Sağlayıcısı olan LİNX PIPEX, BT Internet Services, Demon Internet, EUnet GB ve UKERNA/JANET öncülüğünde 1994 yılında kurulmuştur. İngiltere'de faaliyet gösteren dünyanın en büyük ve en eski İDN'lerinden biri olan LINX transatlantik bağlantı maliyetlerini azaltmayı amaçlamaktadır (BTK, 2013d, s.12,17). %75'i Avrupa'dan ve geri kalanı Orta Doğu, Asya Pasifik, ABD ve Afrika bölgesinde yer alan 56 farklı ülkeden olmak üzere toplam 448 üyesi olan LİNX'in bu üyeleri arasında İngiltere'nin, Avrupa'nın ve Amerika'nın belli başlı tüm İnternet Servis Sağlayıcıları bulunmaktadır. Türk Telekom'da LINX'in üyesidir. LINX Londra'da bulunan 8 noktası sayesinde bağlantı yapmakta ve trafik değişmelerini gerçekleştirmektedir. İngiltere'nin trafiğinin %90'ı LINX üzerinden geçmektedir (Türk-internet, 2013).

Şekil 4.3. Londra Docklands'da LINX'in bulunduğu veri merkezlerinden biri

Kaynak: Türk-internet, 2013

Dünya'da 150 kadar noktada değişim yapan LINX, Avrupa trafiğini, Amerika'ya taşımaktadır. LINX, PIPEX tarafından verilen ve 8 tane 10 megabit'lik port olan Catalyst 1200 ile bu işe başlamıştır. Bu switch başka bir Catalyst 1200 ve bir Cisco 1100 ile bağlıydı. 1996 yazında kurulan ikinci

switch ise bir internet değişim noktasına kurulan ve dünyanın ilk 100 megabit kapasiteli switch'i olan Catalyst 5000'dü. LİNX bugün, en yoğun olduğu dönemde bile 65 gigabit'lik bir trafiği yönetebilmektedir (Türk-internet, 2013).

Üye temsilcilerinin katılımıyla belirli aralıklarla düzenlenen toplantılarda alınan kararlara göre yönetilen LINX kar amacı taşımamaktadır. Çok çeşitli türde şebeke LINX üzerinden peering yapmaktadır. Google, Akamai, Yahoo ve BBC gibi büyük içerik sağlayıcıların da içinde bulunduğu oyun, video, DDoS engelleme, yazılım ve reklam hizmeti gibi pek çok farklı hizmet sağlayıcı grup LINX'in üyesidir (Jensen, 2009).

Şekil 4.4. Londra internet değişim noktası

Kaynak: Turk-İnternet, 2013

4.1.3. Amsterdam (AMS-IX)

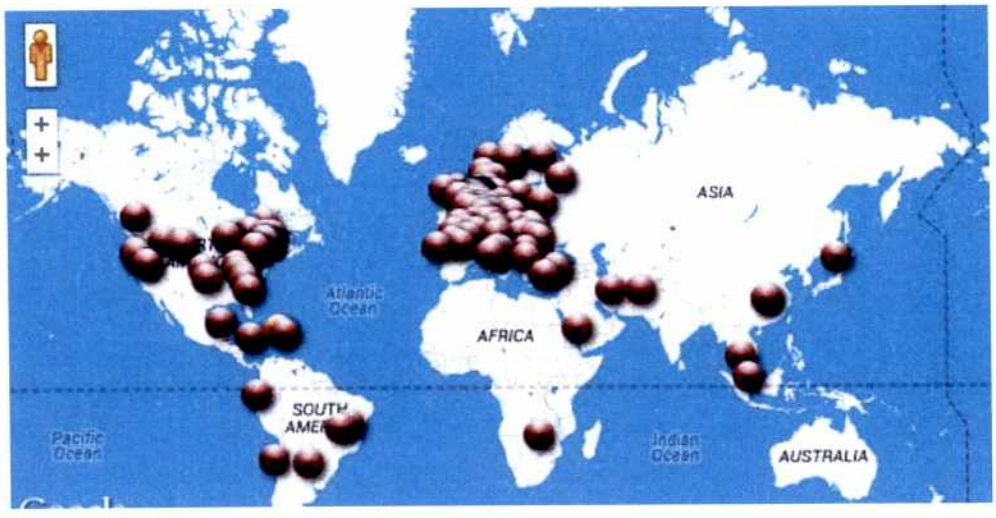
AMS-IX 1990'lı yıllarda kurulmuştur. Herhangi bir kar amacı olmayan kuruluş, bugün 1171 port üzerinden 613 üyeye hizmet sunmaktadır. AMS-IX'in üyeleri Akamai, Amazon, AOL, AT&T, Balkan IX, BBC, Belgacom, Belnet, BT, Deutsche Telekom, Facebook, Invitel, Korea Telecom Corp., Magyar Telekom plc., Portugal Telecom, Qatar Telecom, Ripe NCC, Russian Institute for Public Networks (RIPN), Superonline İletişim Hizmetleri A.Ş, Telecom

Italia Netherlands B.V., Telekom Austria, Telekom Malaysia Berhad, Türk Telekomünikasyon A.Ş., Verizon Business, Vodafone, Yahoo Europe, Yandex Europe bulunmaktadır (AMS-IX, 2013).

Şekil 4.5. AMS-IX veri merkezi

Kaynak: (Ams-ix, 2013)

Şekil 4.6. AMS-IX'in üyesi olan ülkeler



Kaynak: (Ams-ix, 2013)

AMS-IX'e bağlı ağların çoğu AMX-IX birliğine üye ve AMX-IX BV şirketinin %100 hissedarlarıdır. Bağlı ağların %25'i KPN, Ziggo ve UPC gibi erişim sağlayıcı ve NPO, Surfnet, TMG ve Leaseweb gibi Hollanda'lı yerel

yayıncılardan oluşmaktadır. Diğer %75'i ise Google, Microsoft, Facebook, Netflix ve Amazon gibi Amerikan teknoloji şirketleri ile Deutsche Telekom, Orange, BT, Vodafone, Etisalat, Korea Telecom,Yandex ve Avustralyalı Internode gibi dünyanın dört bir yanındaki işletmecilerden oluşmaktadır. Anlık trafik değişimi yaklaşık 2,25 Tbps (Terabit per second)[1] olmak üzere günlük trafik hacmi 15 PetaByte (PB)[2]'ı bulmaktadır (AMS-IX, 2013).

4.1.4. Bulgaristan (BIX.BG)

Bulgar İnternet Değişim Noktası (BIX.BG) ülkenin ilk internet değişim noktasıdır. 2009 yılında ilk başta şirketler arası peering için kurulmuştur. Şu an 52 üyesi olan BIX.BG değişim noktasında anlık ortalama 45-50 Gbps'lik bir trafiğin değişimi gerçekleşmektedir. Ocak 2013 itibariyle üyelerine sağladığı toplam band genişliği kapasitesi ise 307 Gbps'dir. BIX.BG'nin ana amacı her üyesine kaliteli ve en düşük maliyetli trafik imkânı sağlamaktır (BIX.BG, 2013).

Ülkemizden Superonline'ın da (2 Gbps) bulunduğu BIX.BG'in diğer üyelerinden bazıları, Akamai, Macar Telekom ve Yahoo'dur (BTK, 2013d, s.12,17).

4.2. Türkiye İnternet Değişim Noktası ve Veri Merkezi Uygulamaları

Bilindiği üzere İnternet Değişim Noktalarının, internet üzerinden yayınlanan içeriğe erişim sürelerinin iyileştirilmesi, erişim hizmetlerinde maliyetlerin azaltılması, internet üzerinden gerçekleştirilebilecek siber olaylara kolay müdahale edilebilmesi gibi faydaları bulunmaktadır. Bu faydalarından bir kısmı internet servis sağlayıcılarını ve internet üzerinden tüm dünyaya içerik sunan içerik sağlayıcılarını doğrudan etkilemektedir.

---

[1] Terabit : 10^{12} bit'dir

[2] PetaByte (PT) : 10^{15} Byte'dır.

Ülkemizde yukarıda sıralanan kaygılar ile kurulmuş bazı ağ yapıları mevcuttur. Bu ağlara, 7 farklı büyük İSS'yi bünyesinde barındıran Türkiye Network Altyapı Platformu (TNAP) ve global bir şirket olan Terremark tarafından kurulan ağlar örnek verilebilir.

4.2.1. Terremark internet değişim noktası ve veri merkezi

Ülkemizde 2009 yılından bugüne kadar hizmet veren Terremark, dünyanın farklı bölgelerinde bulunan 13 erişim noktası ile veri saklama, ara bağlantı, barındırma, güvenlik, yedekleme, yönetilebilen alan adı yayınlama hizmeti ve bulut hizmetleri gibi hizmetler sunmaktadır. Bu hizmetleri kaliteli sunabilmesi için de bir İDN'e ihtiyaç duymaktadır. Ülkemizde bir İDN bulunmamasından dolayı, farklı İSS'lerden hizmet alarak kendi bünyesinde bir İDN kurmuştur (Terremark, 2013).

Terramark tarafından ülkemizde kurulan merkez, İstanbul internet değişim noktası anlamına gelen İST-IX olarak adlandırılmaktadır. Ancak Terremark tarafından ülkemizde kurulan model Amerika'da da tercih edilen Network Access Point (NAP) olarak da adlandırılan ticari internet değişim noktalarına daha yakın bir örnektir (Terremark, 2013).

Terremark ülkemiz İSS şirketlerinden Süperonline, Türk Telekom, Vodafone'dan internet erişim hizmeti almaktadır. Bu İSS'lerin dışında da uluslararası bağlantılar için Telecom Italia'dan erişim hizmeti almaktadır. Tüm bu İSS'ler ile Terremark yönlendirme cihazları arasında BGP dinamik yönlendirme protokolü kullanılmakta olup IP seviyede bir trafik değişimi söz konusudur. Böyle bir altyapı ile Renesys gibi küresel içerik hizmeti sunan Terremark müşterileri, hangi İSS'nin müşterisi olursa olsun Terramark müşterilerinin içeriğine hızlı bir şekilde erişmeleri sağlanmaktadır (Menog, 2013).

4.2.2. TNAP internet değişim noktası

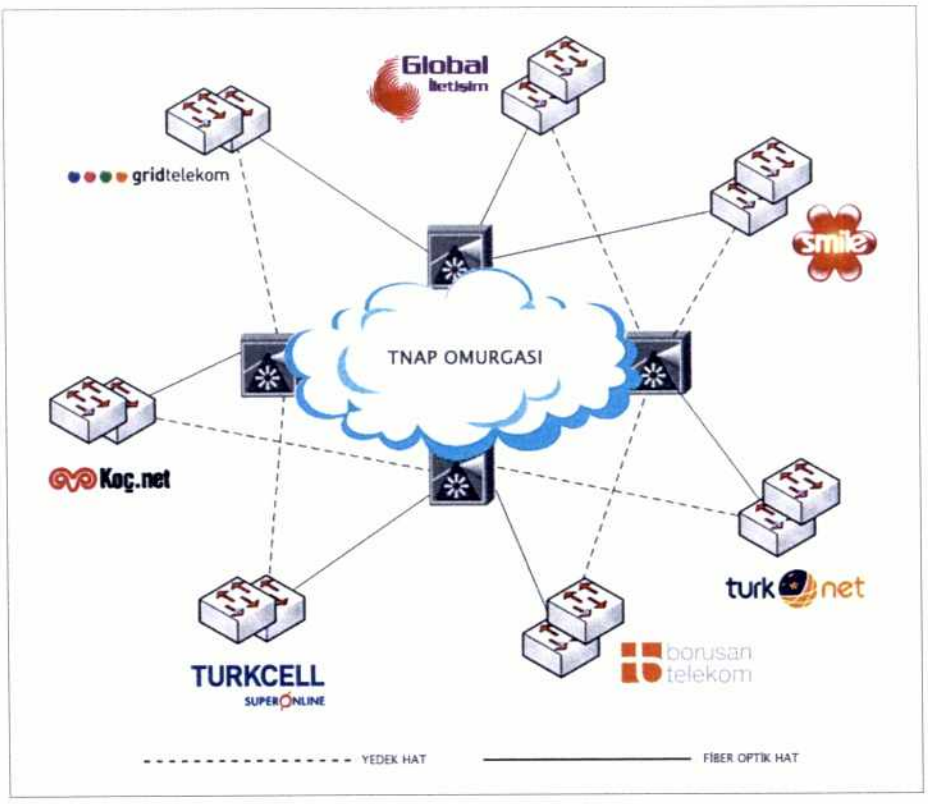
Bilindiği üzere ülkemizde uluslararası standartlarda bir İDN bulunmamaktadır. Ancak internet üzerinden hizmet sunan farklı şirketler tarafından oluşturulmuş, temelinde internet trafiğinin değişim felsefesi bulunan, katılım gösteren her işletmecinin ortak menfaatlerinin barındırıldığı modeller oluşturulmuştur. TNAP'de bu modellerin ilklerindendir (TNAP, 2013).

İnternet altyapıları için önemli bir maliyet kalemi olan transmisyon maliyetlerini azaltmak, internet erişim altyapılarında büyük aktör olan TT'ye alternatif olabilmek gibi amaçlar için 7 büyük işletmeci tarafından kar amacı gütmeden, masrafların paylaşımı temel felsefesi ile TNAP kurulmuştur (TNAP, 2013).

TNAP, Borusan Telekom, Smile, Global İletişim, Gridtelekom, KoçNet, Süperonline ve TürkNet gibi BTK tarafından yetkilendirilmiş 7 büyük İSS'nin oluşturduğu bir platformdur (TNAP, 2013).

Bahse konu bu platform ile 7 farklı İSS'nin sistemleri birbirine 10 Gbps kapasiteli devreler ile bağlanmaktadır. TNAP olarak adlandırılan platformun çizimi Şekil 4.7'de görülmektedir (TNAP, 2013).

Şekil 4.7. TNAP Platformu



Kaynak: TNAP, 2013

Şekil 4.7 'de görülen topoloji marifeti ile İSS'ler Terramark altyapısında olduğu gibi dinamik yönlendirme protokolü olan BGP kullanmaktadır. Bu sayede IP tabanlı bir trafik değişimi söz konusudur. Bu da işletmecilerin trafikleri arasındaki değişim için kolay politika belirleme ve kolay yönetim imkânı sunmaktadır (TNAP, 2013).

4.2.3. Ülkemizde internet değişim noktası ve veri merkezi çalışmaları

Ülkemizde internetin kullanılmaya başlandığı 1993'lü yıllarda internet altyapılarında meydana gelen haftalık kesintiler olağan karşılanmaktayken, 2000'li yıllarda bu hassasiyet saatlere, 2003 yılından sonra bu hassasiyet dakikalara kadar düşmüştür. Günümüzde bu hassasiyet değişim göstermiş,

artık internet üzerinden yayınlanan bir içeriğe milisaniyeler mertebesindeki erişimin hızı konuşulur hale gelmiştir (Demirel, 2013, sözlü görüşme).

Diğer taraftan ilk broadband denemelerinin yapıldığı 2000'li yıllarda internet erişim hizmetlerinde haftanın her günü yaşanma olasılığı olan ve saatlerce süren internet erişim hizmeti kesintileri, BTK tarafından gerçekleştirilen düzenlemeler ve İSS'lerin altyapılarında yaptığı iyileştirmeler sayesinde çok kısa sürelere indirilmiştir (Demirel, 2013, sözlü görüşme).

İşte tam da böyle bir ortamda BTK tarafından internet altyapılarının kalitesinin artırılması, iyileştirme süreçlerine destek sağlanması gibi kaygılar ile İDN kurulması için analiz çalışmaları başlatılmıştır (Demirel, 2013).

Bu analiz çalışmalarında, kurulacak bir İDN'nin internet erişim kalitesini artıracağı, erişim maliyetlerini düşüreceği, serbestleşmenin önünü açacağı, ülkemiz siber güvenlik çalışmalarına katkı sağlayacağı değerlendirilmektedir (Demirel, 2013, sözlü görüşme).

Bu itibarla TNAP, TT gibi ülkemiz internet kullanıcılarının % 95 'ni kapsayan işletmecilerle, gerekse DE-CIX ve Google gibi küresel aktörlerle toplantılar zinciri gerçekleştirilmiştir (Demirel, 2013, sözlü görüşme).

Bu toplantılar neticesinde ülkemizde birkaç farklı ilde, küresel içeriğin ülkemize gelebilmesi için cazibe oluşturabilecek, ticari bir hedefi ve amacı bulunmayan bir İDN kurulmasının faydalı olacağı görüşü hâkim olmuştur. (Demirel, 2013, sözlü görüşme).

SONUÇ VE ÖNERİLER

Ülkemizde ilk kullanıldığı yıllarda, eğlence aracı olarak düşünülen internet, tüm dünyada olduğu gibi günümüzün en etkin iletişim araçlarının başında yer almaktadır. İnternet, birçok kritik verinin erişilebildiği, kamu hizmetlerinin çevrim içi ortamlarda sunulduğu, kritik yönetim toplantılarının yapıldığı bir ortam olmaktadır.

İnternet'in gerek dünya ölçeğinde gerekse ülkemizde göstermiş olduğu bu hızlı gelişim, idari ve teknik olarak internet altyapılarında bir dizi iyileştirmelerin yapılmasını da zorunlu hale getirmektedir.

İnternet ortamında yapılan yayınlara ilişkin düzenlemeler ve internet altyapısında yapılan iyileştirmeler ile kullanıcıların istenilen içeriğe güvenli ve kesintisiz bir şekilde erişebilmesi sağlanmaktadır.

İnternet doğası gereği tüm bileşenleri ile birlikte büyümekte ve gelişmektedir. İyileşmenin bir süreç olması ve bu sürecin insanın var olduğu sürece devam edeceği ilkesinden yola çıkarak, internet altyapılarında yapılması gereken iyileştirmelerin tamamlandığını söylemek çok doğru bir yaklaşım olmayacaktır. Günümüzde saniyelik erişim kesintileri bile hoş karşılanmamakta, hatta internet üzerinde yayınlanan içeriğe erişimin birkaç milisaniyeden uzun sürmesi dahi rahatsızlığa yol açabilmektedir. Bu hızlı değişimi karşılayabilmek ve internetin doğasından kaynaklanan sorunların önüne geçmek için farklı modeller ve altyapılar kullanılmaktadır.

İnternet Değişim Noktaları, erişim zamanında ciddi iyileştirmeler sağlamaktadır. İnternet üzerinde erişilmek istenen içeriğe ulaşmak için geçilen her bir cihaz erişim süresini uzatmakta bu da erişim kalitesini düşürmektedir. İDN'ler trafiğin erişim şebekeleri üzerinden gereksiz olarak dolaşmasına gerek kalmadan bu sürelerin ve maliyetlerin azalması için en uygun çözümleri oluşturmaktadır.

İDN'ler sayesinde ülke içinde bulunan içerik trafiğinin yurtdışına çıkmasının önüne geçilmektedir. Bu sayede yurtdışı bağlantı kaynaklarının verimliliği artmaktadır.

İDN bulunan ülkelerde, uluslararası içerik hizmeti sunan şirketler, İDN'ler üzerinden erişim kalitesini artırmak için veri merkezlerini bu noktalarda bulundurmayı tercih etmekte, böylece İDN'ler bulundukları ülkelere hem ticari hem de teknolojik faydalar sağlamaktadır.

Veri merkezlerine erişim büyük oranda iletişim şebekeleri üzerinden gerçekleşmektedir. Veri merkezlerine dolayısı ile buradaki içeriğe, hızlı ve güvenli erişimin en iyi çözümü, veri merkezlerinin İDN'lere konuşlandırıldığı durumdur. Ülkemizde ticari kaygılar ile kurulmuş İDN özelliği taşıyan İST-IX ve TNAP örnekleri mevcuttur. İST-IX, bünyesinde global veri merkezi şirketi olan Terremark'ı da barındırmaktadır.

Bu iki örnek İDN tecrübeleri açısından ülkemiz için çok önemlidir. Ancak bu iki örnek ülke genelindeki toplam interne trafiğinin çok az kısmını taşıdığı için ususal bir İDN yapısında bulunmamaktadır.

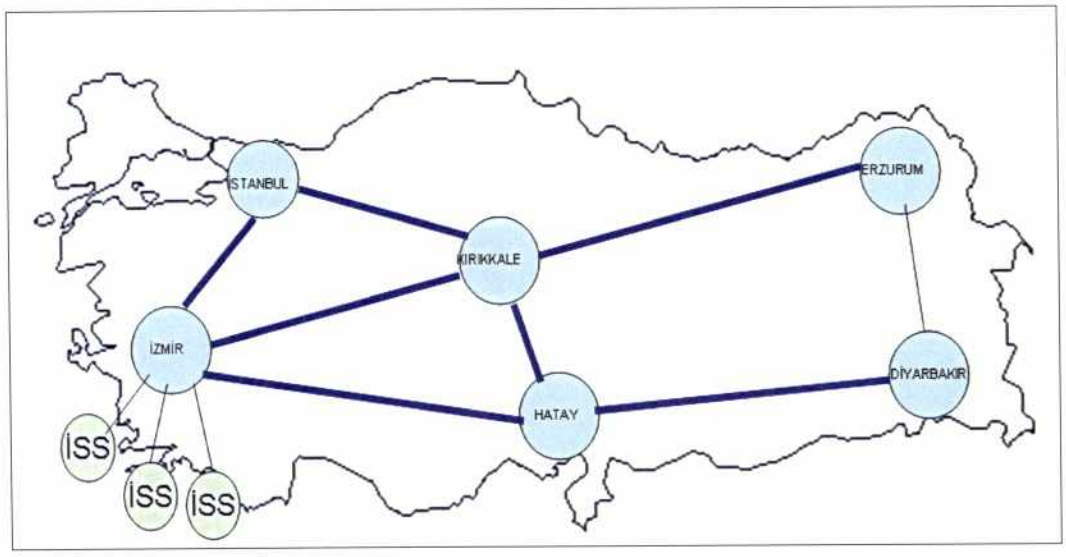
Bilindiği üzere UDHB'nın önderliğinde Siber Güvenlik Kurul'u göreve başlamıştır. Bu Kurul ilk olarak Siber Güvenlik Eylem Planını hazırlamıştır. Siber güvenliğin tesis ettirilmesi internet altyapıları üzerinde yapılacak iyileştirmeler ile mümkündür. İDN'ler siber ve bilgi güvenliğinin tesis ettirilebilmesi için imkânlar sunmaktadır.

Bu itibarla ülkemizde, dünya uygulamalarının örnek alındığı, siber ve bilgi güvenliğinin tesis edildiği, ülke kullanıcılarına fayda sağlarken bölgedeki diğer ülkelerin de internet ve BİT çalışmalarına katkı sağlayabilecek, dünya ile bütünleşmiş, bünyesinde veri merkezlerini barındıran bir İDN'nin kurulmasının önemli olduğu değerlendirilmektedir.

Ülkemizde oluşturulacak Ulusal bir İDN altyapısı için aşağıda öneriler sunulmaktadır;

Aşağıdaki şekilde gösterildiği üzere kurulması önerilen muhtemel teknik altyapının; farklı illeri kapsayacak, yedekli çalışabilecek, mümkün olduğu kadar sınıra ve fiber optik kablo güzergâhlarına yakın ve birbirleri ile uyum içerisinde çalışabilecek bir model olabileceği değerlendirilmektedir. EK-2 de Türkiye'deki mevcut fiber altyapısı konusunda bilgi verilmektedir.

Türkiye'de kurulacak İDN'lerin bulunması önerilen lokasyonlar

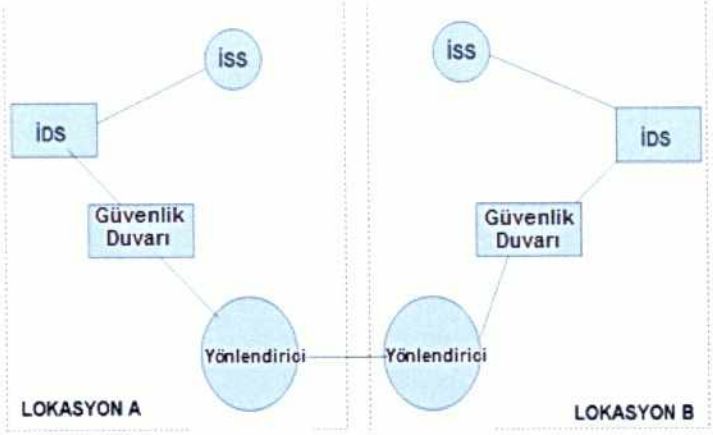


İDN'lerin lokasyonlarının belirlenmesi önemli bir husustur, bunun için mevcut İSS'lerin altyapılarının kuvvetli olduğu, fiber optik kablo geçiş güzergâhlarının mümkün olduğu kadar kesişim kümesi olan, komşu ülke İSS'lerin sistemleri ile kolay bir şekilde irtibat sağlanabilecek noktaların belirlenmesi önemli olmaktadır.

Bu kapsamda ülkemizde kritik yedeklilik merkezleri şemsiyesi altında toplanan İzmir'e, birçok İSS'lerin merkezi olan İstanbul'a, Doğu, Güneydoğu ve Karadeniz fiber optik kablo güzergâhlarının kesişim noktası olan Kırıkkale'ye ve komşu ülkeler ile kolay bir şekilde irtibat sağlanabilecek, Erzurum, Diyarbakır ve Hatay'a konuşlandırılacak cihazlar ile oluşturulacak

bir topolojinin, ülke gereksinimlerine hizmet edebilecek bir İDN'in omurgasını oluşturacağı değerlendirilmektedir.

Siber güvenliği sağlamak için İSS'lerin irtibatlandırılması



Yukarıdaki şekilde iki lokasyon arasındaki irtibatlandırmanın siber ve bilgi güvenliğinin tesis ettirilmesi için nasıl bir topoloji oluşturulması gerektiği gösterilmiştir. Şekilde görüldüğü üzere iki farklı İSS'nin değiştirilmesi muhtemel trafiği, önce internet üzerinden yapılacak ataklara karşı altyapıyı koruyan Saldırı Tespit Sistemleri (Intrusion Detection Systems (IDS)) üzerinden, ardından İDN erişim politikalarının oluşturulduğu güvenlik duvarından geçirilerek farklı lokasyondaki İSS'lere iletilmek üzere yönlendiricilere gönderilmektedir.

Ülkemizin siber tehditler karşısında gerçek bir risk analizinin yapılabilmesi, çok katılımcı bir İDN yapısındaki sistemlerden alınan raporlar sayesinde mümkün olabilecektir. Bugün karşı karşıya olduğumuz bu olgunun gerçek büyüklüğü konusundaki veriler kesin ve yeterli değildir.

Bu saldırıların kamuoyu ile paylaşılması, siber riskler konusunda toplum bilincinin oluşmasını ve verilecek eğitimlerle bu konuda en zayıf halka olan kullanıcı zafiyetinin önüne geçilmesini mümkün hale getirecektir.

Kurulması planlanan İDN'ler için oluşturulacak bu modelde;

- İkinci ve üçüncü katman trafiklerin değişimine imkân sağlayacak geniş katılımlı ve kar amacı taşımayan bir yapıda olması önemlidir.

- Ulusal bir İDN altyapısı gerçekleştirebilmenin, ancak ana omurga sağlayıcısı ve servis sağlayıcıların bu yapı içerisinde yer alması ile mümkün olacağı düşünülmektedir. Türk Telekom A.Ş. ve TTNet'in İDN yapı içinde ticari kaygılar nedeni ile bulunmak istemeyişindeki çekincesine çözüm olabilecek alternatif modeller oluşturmak gerekmektedir.

- Türk Telekom A.Ş. ve TTNet'in internet trafiğinin bir anda tamamı ile katılımı beklenilmemelidir. Başlangıçta bu yapıda yer almak isteyen diğer yerel ve daha küçük trafik kapasiteli İSS'lerin oluşturacağı toplam trafiğe eşdeğer bir katılım ilk adım için yeterli görülmelidir. Bundan sonraki süreçte belirlenen takvime ve yapılan düzenlemelere göre bant genişliğinin kademeli olarak artırılması yönünde bir model üzerinde çalışmalar yapılmalıdır.

- Bu noktada, BTK olarak ülke dışına aktarılan kaynakların yurtiçinde kalması, bu kaynakların geniş bandın yaygınlaşmasına yönelik yatırımlar için kullanılmasını sağlamak üzere, tarafların görüşlerini eşit paydaşlar olarak şeffaf bir şekilde sunabileceği, etkin ve süreklilik arz eden bir platform oluşturulması yönünde çaba sarf edilmesi gerekliliği değerlendirilmektedir.

- Ayrıca ulusal İDN altyapısı içinde, küresel içerik sağlayıcıların, ulusal İSS'lerin, kamu kurum ve kuruluşların, üniversitelerin, bankacılık ve finans sektörünün vb. yer alması yapılacak düzenlemelerle desteklenmelidir. Bu yapıda yer alacak kurum ve işletmeler için konuyu cazip hale getirecek teşvik (enerji gibi girdilerde uygun tarifeler, arazi tahsisi, kamu fonlarından istifade, vergi muafiyetleri vb.) mekanizmalarının oluşturulması yönünde yapılacak düzenlemeler için, ilgili taraflara BTK koordinasyonunda teknik bilgilendirme desteği sağlanabileceği değerlendirilmektedir.

- Kurulacak İDN'lerin kritik altyapı kapsamında düşünülerek, bu platformun ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı yükümlülüklerini yerine getirmesi gerekliliği değerlendirilmiştir.

- İlk İDN yapısının İstanbul'da kurulması, bundan sonra kurulacak olan İDN'ler açısından da teşvik edici bir yapı oluşturacağı değerlendirilmektedir.

- Dünya geneline baktığımızda böyle bir yapının oluşturulmasında geç kalmış olmamıza rağmen önümüzdeki sürecin iyi değerlendirilmesi gerektiği, gerekli girişim ve düzenlemelerin bir an evvel yapılması ile Ülkemizin bulunduğu coğrafya içinde küresel bir İDN ve veri merkezi olmasının kaçınılmaz hale geleceği düşünülmektedir.

- Son dönemde UDHB, Kalkınma Bakanlığı ve BTK'nin organize ettiği uluslararası toplantı ve paneller sonrasında önemli girişimler başlatılmıştır. Küresel içerik sağlayıcılarının da böyle bir yapıda yer alması için yapılan görüşmeler olumlu gelişmeler sağlamış olmakla birlikte ulusal bir İDN yapısının realize edilebilmesi için zaman kaybetmeden söz konusu platformun bir araya gelmesi ve gerekli yasal düzenlemelerin yapılmasının uygun olacağı düşünülmektedir.

KAYNAKLAR

ACORN-REDECOM, 2010
Proceedings of the 4th ACORN-REDECOM Conference Brasilia, D.F., (May 14-15th, 2010)

AKAN Hakan, 2013
Siber Riskler, Siber Suç, Siber Casusluk, Siber Savaş, Grid Teknoloji Sunumu

AMS-IX, 2013
https://www.ams-ix.net/connect-to-ams-ix/benefits-of-connecting

ANTIPISHING, 2013
http://www.antiphishing.org, (28.08.2013)

APWG, 2008
Phishing Activity Trends Report,
http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf, (16.11.2009)

ARTIBEL, 2013
http://www.artibel.com.tr/ISO9001-C74/kalitebelgesi-P1.html, (14.09.2013)

BIX.BG, 2013
http://www.bix.bg/en/en_aboutus/en_about-us.html

BİLGİ TOPLUMU, 2008
http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/.../download,
TÜBİTAK,UEKAE, İş Sürekliliği Yönetim Sistemi Kurulumu, s.6

BİLGİ TOPLUMU, 2013
http://www.bilgitoplumu.gov.tr/Documents/1/KDEP/050200_Eylem07.pdf

BTK, 2013a
BTK Strateji Planı, 2013, s.32, 33, (27.09.2013)

BTK, 2013b
http://www.btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2013.php

BTK, 2013c
http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/mevzuat.php

BTK, 2013d
İDN RAPORU, İnternet Değişim Noktaları, Dünyada Ve Türkiye'de İnternet Değişim Noktalarının Teknik ve Ekonomik Açıdan Değerlendirilmesi, Ankara: Bilgi Teknolojileri Dairesi Başkanlığı,

CANBEK Gürol, SAĞIROĞLU Şeref, (2006)
Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt:9, Sayı:3, s.165,174

CAVALCANTI Daniel, 2010
The Role of Internet Exchange Points in Broadband Policy and Proceedings of the 4th ACORN-REDECOM Conference, Brasilia

CISCO, 2009
http://www.ciscotr.com/yonlendirme-routing-protokolleri.html

CISCO, 2013
Cisco Visual Networking Index: Forecast and Methodology, 2011–2016

CLOUD, 2013
http://cloud.net.tr/?p=253)

COLLIN Barry, 2004
The Future of Cyber Terrorism:Wliere the Physical and Virtual Worlds Converge http://afgen.com/terrorisml.html, (15.05.2004)

COMPUTERWORLD, 2008
ÜSAME İldar Özdemir, Phishing dolandırıcıları taktik değiştiriyor, http://www.computerworld.com.tr/phishing- dolandiricilari-taktik-degistiriyor-detay_2035.html, (18.12.2009)

ÇETİNKAYA Mehtap, 2008
Kurumlarda Bilgi Güvenliği Sistemlerinin Uygulanması, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale.

ÇİFTÇİ Erdem, 2008
İnternet Servis Sağlayıcıları, Yüksek Lisans Tezi, İstanbul: Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü

ÇÖZÜMPARK, 2013
http://www.cozumpark.com/blogs/network/archive/2013/03/24/bgp-protokol-temelleri-b-l-m-1.aspx

DASHORA Kamini, 2011
Cyber Crime in the Society: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences ,3 (1), s. 240,259

DATACENTER, 2012
http://www.datacenterdynamics.com/focus/archive/2012/01/telehouse-opens-frankfurt-data-center

DATACENTERDYNAMİCS, 2013
http://www.datacenterdynamics.com/focus/archive/2012/01/telehou se-opens-frankfurt-data-center

DE-CIX, 2013
http://www.de-cix.net

DEMİR, Berna 2005
Muhasebe Bilgi Sistemlerinde Bilgi Güvenliği. Muhasebe ve Finansman Dergisi, Sayı: 26, 147,156

DEMİREL Mustafa, 2013, BTK İletişim Uzmanı,mdemirel@btk.gov.tr
Sözlü görüşme

DENNING Dorothy, 2001
"Is Cyber Terror Next?" http://essays.ssrc.org/ sept11/essays/denning.htm, (15.04.2011)

DİJLE Hikmet, DOĞAN Nurettin, 2011, Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı, BTK Dergisi, Cilt 4, Sayı 2, s. 43

DİNÇKAN Ali, 2008
TÜBİTAK,UEKAE, BS 25999 İş Sürekliliği Yönetim Sistemi Standardı,s.6

DOCSTORE, 2013
http://docstore.mik.ua

DOĞANTİMUR Fulya, 2009
ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Mesleki Yeterlilik Tezi, Ankara: s.7,8

DPT, 2013
BTK Strateji Planı, 2013, s.16, ekutup.dpt.gov.tr/plan/plan9.pdf

EC.EUROPA, 2013
http://ec.europa.eu/digital-agenda

EKUTUP, 2013
ekutup.dpt.gov.tr/plan/plan9.pdf aktaran BTK Strateji Planı, 2013, s.18

FİLİZ Süleyman, 2012
Güvenlikte Biometrik Sistemler ve Yüz Tanıma, Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi, Bilişim Enstitüsü, Bilgisayar Bilimleri

GÜNEŞ İsmail, 2004
İnternette Güvenlik ve Denetim: Masumiyet Yitiriliyor mu?
http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=243,08

GÜNGÖR Müberra, EVREN Gökhan, 2002
İnternet Sektörü ve Türkiye İncelemeleri Ankara: Telekominikasyon Kurumu Tarifeler Dairesi Başkanlığı

HAMILTON James, 2008
Internet Scale Servise Efficiency (Ladis) Workshop,
HÜRRİYET, 2013 http://webarsiv.hurriyet.com.tr/2001/10/07/37854.asp (2013)

ITU, 2013a
(http://www.itu.int/), (27.08.2013)

ITU, 2013b
http://www.itu.int/ITU-T/wtsa/resolutions04/Res50E.pdf, (27.08.2013)

ITU, 2013c
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf, (27.08.2013)

ITU, 2013d
http://www.itu.int/ITU-T/wtsa/resolutions04/Res51E.pdf, (27.08.2013)

İKV, 2013a
http://www.ikv.org.tr, (28.08.2013)

İKV, 2013b
http://www.ikv.org.tr/images/upload/data/files/ikv_e-bulten_7-13_subat_2013.pdf, (28.08.2013)

INTERNETSOCIETY, 2013
http://www.internetsociety.org/promoting-use-internet-exchange-points-guide-policy-management-and-technical-issues

INVEST-IN-HESSEN, 2013
Avrupa'nın Kalbinde Uluslararası Bir Yatırım ve Ticaret Merkezi,
http://www.invest-in-hessen.de/mm/Hessen_GuteGruende_Tuerkei.pdf

İREN Adem Ali, GÜRKAYNAK Muharrem, 2011
Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler, Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Dergisi, Sayı:16, No:2, s.263,275

İVMUEY, 2004
İnternet Veri Merkezi Uygulamalarının Ekonomisi ve Yapılabilirliği, 2005, E-Dönüşüm Türkiye KDEP-2004 7 NUMARALI EYLEM Raporu, s. 9,15
Ankara: Teknik Altyapı ve Bilgi Güvenliği Çalışma Grubu

İVMUEY, 2005
İnternet Veri Merkezi Uygulamalarının Ekonomisi ve Yapılabilirliği, 2005, s.9,15

JENSEN Mike, 2009
Promoting the Use of Internet Exchange Points: A Guide to Policy, Management and Technical Issues

KAYRAK Musa, 2012
Bilgi Kriterleri Çerçevesinde Bilişim Teknolojileri Denetimi, Sayıştay Dergisi, Sayı: 87, s.155,163.

KENDE Michael, 2012
Report for the Internet Society
How the Internet continues to sustain growth and innovation Ref: 35128-362

KORKMAZ Yakup, 2013
"Bulut Bilişim", Türkiye İçin Fırsatlar, TUBİTAK UEKAE, Ankara

KÖKNAR Ali, 2001, "Sanal Ortamda Terörizm", TC İçişleri Bakanlığı Bilişim ve İnternet Teknolojilerinin Ceza Hukuku açısından Doğurduğu Yeni Sorunlar Semineri'ne sunulan bildiri, Bursa

KRASAVIN Serge, 2004
"What is Cyber-terrorism?" http://www.crimeresearch. org/library/Cyber-terrorism.htm, (04.05.2011)

KÜÇÜKER Mustafa Can, 2012
OECD Ülkelerinde Genişband İnternet Talebi: Panel Veri Uygulaması, Yüksek Lisans Tezi, Ankara: Atılım Üniversitesi, Sosyal Bilimler Enstitüsü, Uygulamalı İktisat Anabilimdalı

MENOG, 2013
http://www.menog.org

NEWAVENERGY, 2011
http://newavenergy.com/blog/2011/09/data-center-industry-beats-the-global-recession-%E2%80%93%C2%A0scalabilty-is-one-of-the-key-concerns-for-growth/#.UkSf6strPIU

OECD, 2006
Task Force On Spam, http://www.oecd.org/dataoecd/63/28/36494147.pdf,s. 6,17, (18.12.2009)

OECD, 2012
http://oecdinsights.org/2012/10/22/internet-traffic-exchange-2-billion-users-and-its-done-on-a-handshake/

OGM, 2013
Bilgi Güvenliği, Zombi Bilgisayarlara Dikkat http://web.ogm.gov.tr

OLOVSSON Tomas, 1992
A Structured Approach to Computer Security", Department of Computer Engineering Chalmers University of Technology S-412, Gothenburg, Sweden

ÖNEL Dinçer, DİNÇKAN Ali, 2007
Bilgi Güvenliği Yönetim Sistemi Kurulumu, Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

ÖZBİLGİN Gökhan, 2003
www.sayistay.gov.tr/dergi/icerik/der49m7.pdf

ÖZKAN Tezcan, 2006
Siber Terör Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi, Yüksek Lisans Tezi Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü

PCEXTRA, 2011
http://pcextra.com.tr/kurumsal/2011/12/terremark-bulutlarin-ustunde-ucuyor/#more-12003

PCH, 2013
http://www.pch.net. Packet Clearing House, Analysys Mason estimates "How the internet continues to sustain growth and innovation"

POLLITT Mark, (2004)
Cyber Terrorism - Fact or Fancy?
http://www.cs.georgetown.edu/%7Edenning/infosec/pollitt.html

PTG, 2013
http://ptgmedia.pearsoncmg.com/images/9781587132063/samplechapter/1587132060_03.pdf

RESMİ GAZETE, 2012
(http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf)

RESMİ GAZETE, 2013a
(http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf)

RESMİ GAZETE, 2013b
(http://www.resmigazete.gov.tr/eskiler/2013/02/20130209-5.htm)

SACCO, P, 2007
Always Availible Data Centers, PTS datacenter solutions whitepapers database, 2007

SAVAŞ Emre, 2011
Türkiye Network Altyapı Platformu (TNAP)
http://www.emresavas.com/turkiye-network-altyapi-platformu-tnap.html

SECURITY THREAT REPORT, 2009
http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf, s.4,9.

SHEPHARD, B. 2002
Information security-who cares?, Power System Management and Control, Fifth International Conference on (Conf. Publ. No. 488), s.126

SİBER GÜVENLİK RAPORU, 2012
İstanbul: İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Hukuku Enstitüsü.

SUPERNET, 2013
http:// www.supernet.web.tr/fiber_optik_kablolama.asp

SYMANTEC, 2009
Global Internet Security Threat Report Trends for 2008, s.10,59

ŞAHİNASLAN Ender, 2011
Bilgi ve Bilgi Teknolojilerine Ait Risklerin Yönetilmesinde Arayış, Yöntem ve Çözüm Önerileri. Akademik Bilişim'11, XIII. Akademik Bilişim Konferansı Bildirileri. Malatya: İnönü Üniversitesi, s.569

TBD, 2008
Bilgi Teknolojisi Alt Yapı Kütüphanesi ITIL, Ankara: Türkiye Bilişim Derneği

TEKEREK Mehmet, 2007, Bilgi Güvenliği Yönetimi, KSÜ, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, s. 132,135

TELEGEOGRAPHY, 2013
http://www.telegeography.com/telecom-resources/internet-exchange-map/index.html, (18.09.2013)

TELEPATİ, 2013
http://www.telepati.com.tr/temmuz11/konu14.htm

TERREMARK, 2013 http://www.terremark.com/services/infrastructure-cloud-services/network-conne

TIA,2006
TIA-942, 2006, http://www.ieee802.org

TNAP, 2013a
http://tnap.net.tr/#page-network

TNAP, 2013b
http://tnap.net.tr/#page-about

TOPAL Hikmet, (2004)
Siber Terör, Yüksek Lisans Tezi, İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı

TURHAN Meltem, 2010
Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri, Uzmanlık Tezi, Ankara: Bilgi Teknolojieri ve İletişim Kurumu

TURHAN Oğuz, 2006
Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), Planlama Uzmanlığı Tezi, s. 1,108, Ankara, Türkiye

TURK-İNTERNET, 2013
(http://www.turk-internet.com/portal/yazigoster.php?yaziid=11420)

TÜRKİYE, 2013
https://www.turkiye.gov.tr/bilgi-teknolojileri-ve-iletisim-kurumu,(27.09.2013)

UDHB, 2005
Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2005), Spam Bildiri Raporu, Ankara, (27.09.2013)

UDHB, 2010
Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2010), 2023 Yılına Kadar Internet ve Bilişim Sektörünü Şekillendirirken İstanbul Veri ve Erişim Başkenti Projesi, Ankara, (27.09.2013)

UDHB, 2013
Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2013), Siber Güvenlik, Ankara, (27.09.2013)

USLU Tolga, 2007
İnternet Güvenliği ve Risk Yönetimi, İstanbul: İstanbul Üniversitesi, Fen Bilimleri Enstitüsü

UYAP, 2011
http://www.turk-internet.com/portal/yazigoster.php?yaziid=33166

ÜNVER Mustafa, CANBAY Cafer, Mirzaoğlu Ayşe Gül,
Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, Ekim 2009

ÜNVER Mustafa, CANBAY Cafer, 2010, Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, Elektrik Mühendisliği Dergisi 438. sayı, s. 92,104

VERİZON, 2013
http://www.verizon.com/jobs/ms/terremark/home.htm

VURAL Yılmaz, SAĞIROĞLU Şeref, 2007
Kurumsal Bilgi Güvenliği, Güncel Gelişmeler, Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, s. 192,199, Ankara

VURAL Yılmaz, SAĞIROĞLU Şeref, 2008
Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi Dergisi, Cilt 23, No:2, s.507,522.

WEAVER Nicholas, PAXSON Vern, STANIFORD Stuart, ve UNNINGHAM Robert, 2003
"A Taxonomy of Computer Worms", Proceedings of the 2003 ACM workshop on Rapid malcode, s. 11,18

WEINMANN Gabriel, 2005, "Cyberterrorism: The Sum of All Fears?", Studies in Conflict & Terrorism, 28, s. 129,149

WELLER Dennis and WOODCOCK Bill, 2012
"Internet Traffic Exchange: Market Developments and Policy Challenges", OECD Digital Economy Papers, No. 207, OECD Publishing (27.09.2013)

YENİŞAFAK, 2013
http://yenisafak.com, (27.09.2013)

YILDIRIM Reyhan, 2009
İş Yönetiminde Başarı Faktörü, İş Sürekliliği Yönetimi, BS 25999 İş Sürekliliği Yönetimi Standart Yapısı ve Gelişimi. İstanbul: İstanbul Teknik Üniversitesi

EKLER

EK-1 Dünya'daki İDN noktalarına ait liste

Tablo Ek-1. 1. Dünya'daki İDN noktalarına ait liste

İsim	Tanım	Kuruluş Yılı	URL	Şehir	Ülke
AIXP	Luanda, Angola (Angola AIP)	2006	http://www.angola-ixp.ao/	Luanda	Angola
BINX	Gaborone, Botswana	2006	http://www.binx.org.bw/,http://www.info.bw/bispa/binx.html	Gaborone	Botswana
KINIX	Kinshasa, Democratic Republic of the Congo	Sep 2002	http://www.ispa-drc.cd/kinix.htm	Kinshasa	Democratic Republic of the Congo
CR-IX	Cairo, Egypt	Dec 2002	http://www.nsrc.org/db/lookup/operation=lookup-report/ID=1100200161570:488991867/fromP age=EG	Cairo	Egypt
CAIX	Cairo, Egypt	2004	http://www.caix.net.eg/	Cairo	Egypt
MEIX	Cairo, Egypt NAP / provider	2007	http://www.gpxglobal.net/	Cairo	Egypt
GIXP	Accra, Ghana (GIX, AIX) :[K			Accra	Ghana
CI-IXP	Abidjan, Cote Ivoire	Jun 2007	http://nsrc.org/AFRICA/CI/Report-IXP-CI-2007.pdf	Abidjan	Ivory Coast
MSIXP / KIXP-MSA	Mombasa, Kenya	2	http://www.tespok.co.ke/index.php/msixp.html	Mombasa	Kenya
KIXP	Nairobi, Kenya	Nov 2000	http://www.kixp.or.ke/	Nairobi	Kenya
LIXP	Maseru, Lesotho	Aug 26, 2011		Maseru	Lesotho
MIX	Blantyre, Malawi	Dec 2008	http://www.mispa.org.mw/mix.html	Blantyre	Malawi
MIXP	Ebene Cybercity, Mauritiu s	Jun 2006	http://www.gov.mu/portal/sites/mixp/index.htm	Quatre Bornes	Mauritius
Moz-IX	Maputo, Mozambique	May 2002	http://www.mozix.org.mz/, http://nsrc.org/AFRICA/ixp-pics/MZ-IXP.png	Maputo	Mozambique
IXPN	Internet Exchange Point of	Jul 2011/12 ?	http://www.nixp.net/	Abuja	NG

İsim	Tanım	Kuruluş Yılı	URL	Şehir	Ülke
	Nigeria				
IXPN	Internet Exchange Point of Nigeria	2006	http://www.nixp.net/	Lagos	NG
IXPN-PH	Internet Exchange Point of Nigeria	July 2012	http://www.nixp.net/	Port Harcourt	NG
RINEX	Kigali, Rwanda	Jul 2004	http://www.rinex.org.rw/	Kigali	Rwanda
SLIX	Freetown, Sierra Leone	2009	http://www.slix.sl/	Freetown	Sierra Leone
CINX	Cape Town, South Africa	2009	http://ispa.org.za/inx/cinx-information/,http://stats.cinx.net.za/	Cape Town	South Africa
NeutrINX	Centurion, South Africa	Sep 2011	http://www.neutrinx.org.za/	Centurion	South Africa
DINX	Durban, South Africa	Sep 2012	http://stats.dinx.net.za/	Durban	South Africa
GINX	Grahamstown, South Africa	Mar 2005	http://ginx.org.za/	Grahamstown	South Africa
JINX	Johannesburg, South Afric a	Dec.1996	http://www.jinx.net.za/	Johannesburg	South Africa
SIXP	Khartoum, Sudan	2011	http://sixp.sd/	Khartoum	Sudan
SZIXP	Mbabane, Swaziland	Jun 2004	http://www.nsrc.org/db/lookup/operation=lookup-report/ID=1090612703142:488719200/fromP age=SZ	Mbabane	Swaziland
AIXP	Arusha, Tanzania	2007	http://www.aixp.or.tz/, http://nsrc.org/AFRICA/ixp-pics/tz-aixp.png	Arusha	Tanzania
TIX	Dar es Salaam, Tanzania	Jan 2004	http://www.tix.or.tz/, http://nsrc.org/AFRICA/ixp-pics/tz-tix.jpg	Dar es Salaam	Tanzania
UIXP	Kampala, Uganda	May 2003	http://www.uixp.co.ug/	Kampala	Uganda
ZAIXP	Lusaka, Zambia	Jun 2006	http://ispa.org.zm/	Lusaka	Zambia
ZINX	Harare, Zimbabwe	July 2001	http://www.zispa.org.zw/zinx.html	Harare	Zimbabwe

EK-2 Türkiye'de bazı kurumlara ait fiber optik altyapısı

Ülkemiz fiber optik kablo altyapısı kamu ve özel olmak üzere farklı tüzel kişilik mülkiyetinde bulunmaktadır. Kamunun mülkiyetinde bulunan fiber optik kablo altyapısının büyük bir kısmı da BTK tarafından yetkilendirilmiştir ancak işletmeciler tarafından kullanılmaktadır. Ülkemizde en büyük fiber optik kablo altyapısı Türk Telekomünikasyon A.Ş.'ye aittir. İkinci sırada Süperonline gelmektedir. Ülkemiz'de BOTAŞ'ın, TCDD'nin ve TEİAŞ'ın fiber optik kablo güzergahları ve bu güzergahlarda kullanılan kabloları mevcuttur. Kamu'nun mülkiyetinde olan ve Ülkenin tamamını kapsayacak mesafelere sahip kamu kuruluşlarının fiber optik kablo altyapı bilgileri Tablo'da özetlenmiştir.

Tablo Ek-2. 1. Fiberoptik Kablo Altyapı bilgileri

Kurum	Toplam Uzunluk
KGM	109 km
BOTAŞ	5.200 km 48/24 elyaf
TCDD	80 km 12 Damarlı 85 km 48 Damarlı 255 km. 48 Damarlı *220 km. 2 adet 48 damarlı *420 km. 48 damarlı
TEİAŞ	5825,2km *1501,5 km 1501,5 km

Kaynak: BTK, 2010

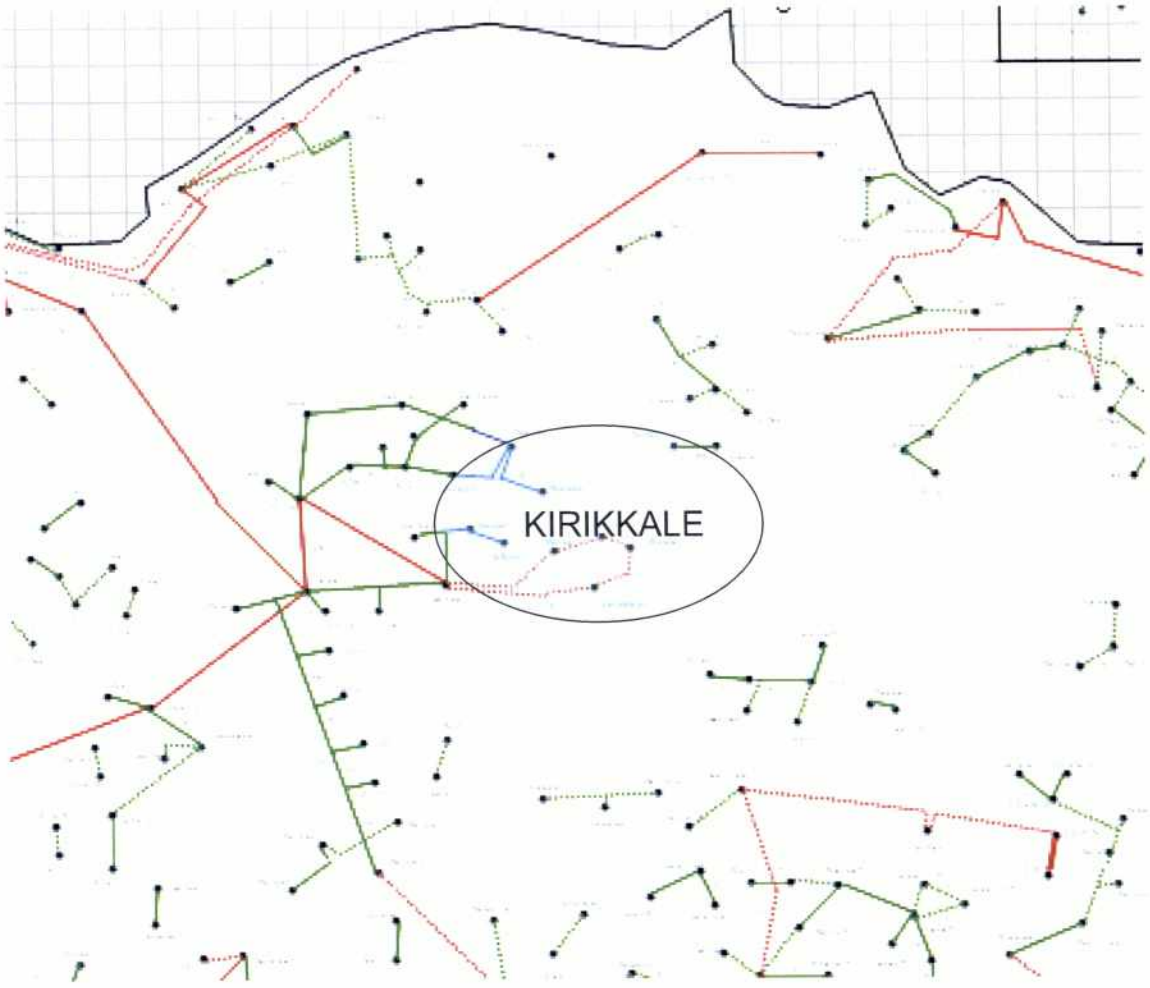
Bahse konu tablodaki kamu kurum ve kuruluşlarından mülkiyeti BOTAŞ'a ait olup Süperonline 15 yıllığına kiralanmış fiber optik kablo altyapı haritası aşağıdaki şekilde gösterilmiştir.

Şekil Ek-2. 1. Fiberoptik Kablo Altyapı Haritası

Kaynak:www.botas.gov.tr

Elektrik iletim hatları üzerinden tesis ettirilen fiber optik kablo altyapısı bulunan TEİAŞ'ın altyapısının bir kısmını gösterir Şekil aşağıda gösterilmiştir.

Şekil Ek-2. 2. TEİAŞ Fiberoptik Kablo Haritası



Kaynak:www.teias.gov.tr

Ayrıca Sivas-Ankara hızlı tren hattının Ankara-Kayseri arasında çalışacak hattın fiber optik kablo hattı tesis etmiştir. Bu hattı gösterir çizim aşağıdaki şekilde görülmektedir.

Şekil Ek-2. 3. Hızlı Tren Hattı Fiberoptik Kablo altyapısı

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 Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu 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.

Lebibe YALÇINTAŞ
30/09/2013

ÖZGEÇMİŞ

1964 yılında Ankara'da doğdu. İlköğrenimi ve orta ve öğrenimini Konya Seydişehir'de tamamladı. Lise öğrenimini Ankara Kız Lisesi'nde bitirdi. Ankara Üniversitesi Fen Fakültesi Fizik Mühendisliği bölümünden Fizik Mühendisi olarak mezun oldu. Telsiz Genel Müdürlüğü'nde mühendis olarak göreve başladı. Halen Bilgi Teknolojileri ve İletişim Kurumu İstanbul Bölge Müdürlüğünde Teknik Bölge Müdür Yardımcısı olarak çalışmaktadır. Evli ve iki çocuk annesidir.