SİBER GÜVENLİĞİN SAĞLANMASI:

TÜRKİYE'DEKİ MEVCUT DURUM VE ALINMASI GEREKEN TEDBİRLER

Hazırlayanlar

Mustafa ÜNVER	Daire Başkanı
Cafer CANBAY	Bilişim Uzmanı
Ayşe Gül MİRZAOĞLU	Bilişim Uzman Yardımcısı

Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı

Mayıs 2009

İÇİNDEKİLER

KISALTMALAR

AB	Avrupa Birliği
AK	Avrupa Konseyi
APEC	Asia Pasific Economic Cooperation Asya Pasifik Ekonomik İşbirliği Teşkilatı
ASEAN	Association of Southeast Asian Nations Güneydoğu Asya Ülkeleri Birliği
BM	Birleşmiş Milletler
BİS	Bilgi ve İletişim Sistemleri
BİŞ	Bilgi ve İletişim Şebekeleri
BİT	Bilgi ve İletişim Teknolojileri
BOME	Bilgisayar Olaylarına Müdahale Ekibi
DBTZ	Dünya Bilgi Toplumu Zirvesi
ITU	International Telecommunication Union Uluslararası Telekomünikasyon Birliği
OECD	Organization for Economic Cooperation and Development Ekonomik İşbirliği ve Kalkınma Teşkilatı
STK	Sivil Toplum Kuruluşu
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi
USD	United States Dollars Amerika Birleşik Devletleri Doları
USGO	Ulusal Siber Güvenlik Otoritesi

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

1 GİRİŞ

19. yüzyılda hüküm süren Sanayi Çağı; 20. yüzyılın son çeyreği ile birlikte yerini Bilgi Çağına bırakmıştır. Sanayi Çağında gücü temsil eden sermaye, hammadde ve işgücünün yerini Bilgi Çağında "bilgi" almıştır. Francis Bacon tarafından da "güç" olarak nitelenen "bilgi" bir üretim faktörü haline gelmiş ve her türlü sosyoekonomik faaliyete önemli bir girdi teşkil etmeye başlamıştır [1].

Bilgi Çağı, her türlü bilginin (veri, görüntü, ses vb.) sayısal olarak ifade edilebilmesine, bir başka deyişle elektronik, optik veya manyetik ortamlar üzerinde saklanabilmesi, işlenebilmesi ve iletilebilmesine imkan tanıyan bilgi ve iletişim teknolojilerinin (BİT) gelişimini temsil etmektedir. Bilginin sayısallaşması, üzerinde bulunduğu fiziksel ortamın sınırlarından bağımsız hale gelmesine, kolaylıkla farklı ortamlara aktarılabilmesine, sonsuz defa çoğaltılabilmesine, değiştirilebilmesine veya yok edilebilmesine imkan tanımaktadır [2]. Her geçen gün hızla gelişen, çeşitlenen ve yaygınlaşan BİT, Bilgi Toplumuna küresel dönüşümün temel öğeleridir.

Elektronik haberleşme şebekeleri ve altyapıları[3] ile bilgi ve iletişim sistemlerini (BİS) birbirine bağlayan, dolayısıyla sayısal bilginin kolaylıkla farklı sistemlere iletilmesine ve dağıtılmasına imkân veren, bu yönüyle küresel ve sınır tanımayan bir yapıya sahip olan İnternet ise söz konusu teknolojilerin başını çekmektedir.

Bilgi Çağı, hayatın pek çok alanında önemli değişikliklerin yaşanmasına sebep olmuş, kurumsal yapılanma, yönetim, operasyonel faaliyetler gibi alanlarda pek çok uygulamayı değiştirmekle kalmamış; finans, elektronik haberleşme, ulaşım, enerji,

---

[1] Canbay, C. Beydoğan, T. A., "Siber Güvenliğin Sağlanması ve Kritik Bilgi ve Altyapıların Korunması: Gelişmekte Olan Ülkeler için Yol Haritası", 17. ITS Konferansı, Montreal – Kanada, 2008

[2] ITU, "Gelişmekte Olan Ülkeler için Siber Güvenlik Rehberi", 2007, http://www.itu.int/osg/csd/cybersecurity/gca/docs/brochure.pdf

[3] 5809 sayılı Elektronik Haberleşme Kanununun 3. maddesinin 1. fıkrasının (h) ve (k) bentlerinde;

- Elektronik haberleşme alt yapısı: Elektronik haberleşmenin, üzerinden veya aracılığıyla gerçekleştirildiği anahtarlama ekipmanları, donanım ve yazılımlar, terminaller ve hatlar da dahil olmak üzere her türlü şebeke birimlerini, ilgili tesisleri ve bunların bütünleyici parçalarını,
- Elektronik haberleşme şebekesi: Bir veya daha fazla nokta arasında elektronik haberleşmeyi sağlamak için bu noktalar arası bağlantıyı teşkil eden anahtarlama ekipmanları ve hatlar da dahil olmak üzere her türlü iletim sistemleri ağını ifade edecek şekilde tanımlanmaktadır.

sağlık, eğitim gibi pek çok kritik altyapının da BİT'e bağımlı hale gelmesine yol açmıştır [4].

Gerek sayısal bilginin kolaylıkla üzerinde bulunduğu fiziksel ortamdan bağımsız hale getirilerek orijinalliğini yitirebilmesi ve İnternet aracılığıyla hızla küresel çapta dağıtılabilmesi, gerekse BİT'e bağımlı hale gelen altyapıların ve sistemlerin günden güne çoğalması, pek çok güvenlik riskini de beraberinde getirmektedir. BİT'e bağımlı olma durumu, bu teknolojilerin siber saldırganlar ve siber suçluların siber ortamda yasadışı amaçlarını gerçekleştirebilecekleri pek çok açıklığa sahip olması dolayısıyla, dünyanın sosyal, politik, ekonomik ve askeri güvenliğini ve istikrarını tehdit eden ciddi bir risk unsurudur [5]. Söz konusu risklerin ciddiyeti ve yol açabileceği olası zararların büyüklüğü, bunlarla baş edebilmek için uygulamaya konması gereken mekanizmaları gündeme getirmiş, Siber Güvenliğin Sağlanması ve Kritik Bilgi ve Altyapıların Korunması hususları gündemin önde gelen konuları arasına girmiştir.

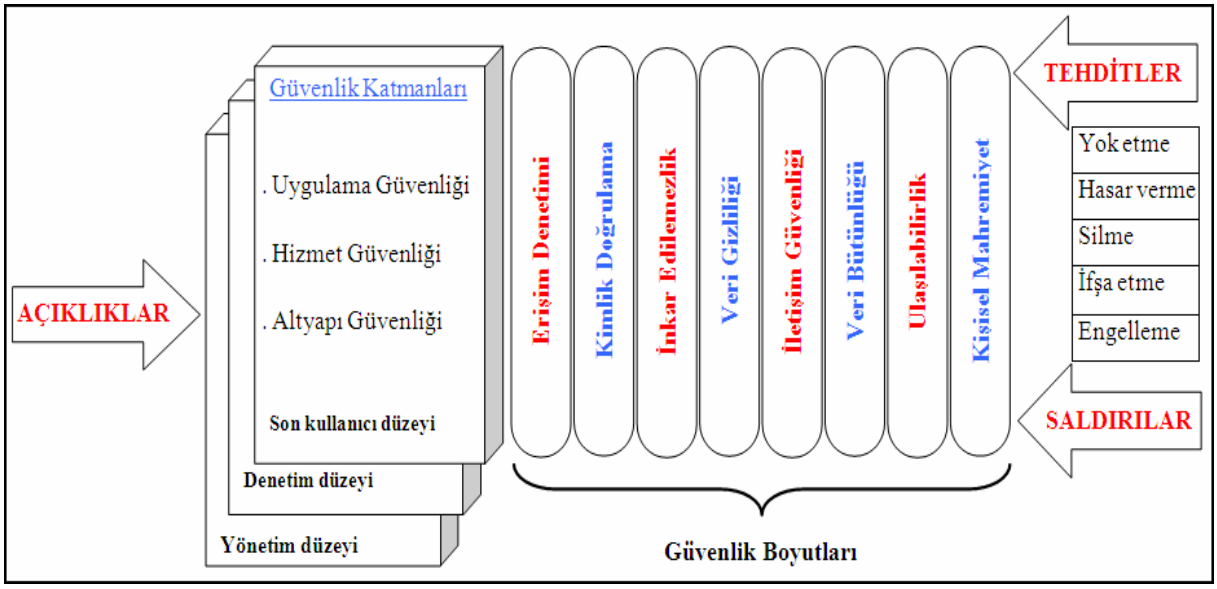
Bu çalışmada, siber güvenliğin sağlanması ve kritik bilgi ve altyapıların korunmasının giderek artan önemi göz önüne alınarak, ülkemizde yapılacak çalışmalara katkıda bulunmak üzere bazı tespitlerde bulunulmaktadır. İkinci bölümde, siber güvenliğin sağlanması ve kritik bilgi ve altyapı kavramları özetlenmektedir. Üçüncü bölümde siber ortamda en fazla gözlenen siber tehditler ve amaçları ile bunlara ilişkin istatistikî veriler özetlenmektedir. Dördüncü bölümde ülkemizde ulusal siber güvenliğin sağlanması konusunda kritik öneme sahip olduğu değerlendirilen temel ilkeler, yöntemler ve adımlara yer verilmektedir.

[4] Canbay, C. Beydoğan, T. A., a.g.e.
[5] Canbay, C. Beydoğan, T. A., a.g.e.

2 SİBER GÜVENLİĞİN SAĞLANMASI VE KRİTİK BİLGİ VE ALTYAPILARIN KORUNMASI

Siber güvenlik, siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü olarak tanımlanmaktadır. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, elektronik haberleşme sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri bilginin erişilebilirliğini, aslına uygunluğu ve inkâr edilemezliği de dahil olmak üzere bütünlüğünü ve gizliliğini sağlamaktır [6]. (Şekil 2.1) Siber güvenlik, siber tehditler ve siber saldırılar ile mücadelenin yanı sıra, BİS'de yer alan açıklıkları en aza indirmeyi de amaçlamaktadır.

Şekil 2.1. Siber Güvenlik



Kaynak: ITU, "ITU_T X.1205 sayılı Tavsiye Kararı, Siber Güvenliğe Genel Bakış", 2008

[6] ITU, "ITU_T X.1205 sayılı Tavsiye Kararı, Siber Güvenliğe Genel Bakış", 2008

ITU – T X.1205 sayılı tavsiye kararında tanımlanan siber güvenliğin temel hedefleri, bilginin;

- Erişilebilirlik,
- Bütünlük,
- Gizlilik

unsurlarını güvence altına almaktır.

Erişilebilirlik: Bilginin, sistemlerin ve hizmetlerin; enerji kesintileri, doğal afetler, sistem hataları, beklenmeyen olaylar ve kötücül saldırılar gibi olası durumlara rağmen, her ihtiyaç duyulduğunda erişilebilir, kullanıma hazır ve tam işlevsel halde bulunmalarını ifade eder. BİŞ'te yaşanabilecek arızaların diğer kritik altyapıların işleyişinde aksaklıklara yol açabileceği durumlarda, erişilebilirliğin korunması hayati önem taşımaktadır [7].

Bütünlük: BİŞ üzerinden gönderilen, alınan veya BİS'de saklanan verilerin eksiksiz ve değiştirilmemiş halde bulunmalarını ifade eder. Paylaşılan verilerin doğruluğuna karşı çok hassas olan sağlık, endüstriyel tasarım gibi sektörler için veri bütünlüğünün sağlanması büyük önem taşımaktadır [8].

Gizlilik: BİŞ üzerinden yapılan haberleşmenin veya BİS'de saklanan verilerin yetkili olmayan taraflarca ele geçirilmekten korunmasını ifade eder. Hassas verilerin iletimi ve haberleşme esnasında kişisel mahremiyetin korunmasında gizlilik esastır [9]. Avrupa Komisyonu tarafından yayınlanan "Şebeke ve Bilgi Güvenliği: Avrupa Politik Yaklaşımı Tasarısı" konulu Tebliğde, erişilebilirlik, bütünlük ve gizlilik, BİŞ'in ve BİS'in güvenlik koşullarında bulunması gereken birbirine bağlı unsurlar olarak sıralanmakta ve bir başka unsur olarak da kimlik doğrulamadan bahsedilmektedir.

[7] Avrupa Komisyonu, "Şebeke ve Bilgi Güvenliği: Avrupa Politik Yaklaşımı Tasarısı, Tebliğ", s. 5, http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf

[8] y.a.g.e.

[9] y.a.g.e.

Kimlik doğrulama: BİS'i kullanan gerçek veya tüzel kişiler tarafından beyan edilen kimlik bilgilerinin teyit edilmesini ifade eder. İnternet bankacılığı gibi uygulamalarda kimlik doğrulamanın güvenliğe katkısı yadsınamaz. Kimlik doğrulama, kimlik bilgilerine ihtiyaç duyulmayan durumlarda, kimliğin anonim hale getirilmesine de imkân tanımalıdır [10]. ITU tarafından 2007 yılında yayınlanan "Gelişmekte Olan Ülkeler için Siber Güvenlik Rehberi" belgesinde ise erişilebilirlik, bütünlük, gizlilik ve kimlik doğrulamaya ek olarak inkâr edilemezlik de siber güvenlik çözümlerinin sağlaması gereken temel güvenlik unsurları arasında sayılmaktadır.

İnkâr edilemezlik: Herhangi bir iş ve işlemin gerçekleştirilmiş olduğunun ispatlanmasını ifade eder ve hesap verilebilirlik, izlenebilirlik ve bazı durumlarda da denetlenebilirlik kavramları ile ilişkilendirilebilir [11].

Kritik altyapılar, Avrupa Komisyonu tarafından, zarar görmesi veya yok olması halinde, vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya kamu hizmetlerinin etkin ve verimli işleyişine ciddi boyutta olumsuz etki edebilecek fiziksel ve teknolojik tesisler, şebekeler, hizmetler ve varlıklar olarak tanımlanmaktadır [12]. Kritik altyapıların hangileri olduğu konusunda genel geçer bir tanım olmamakla ve kritik altyapılar ülkeden ülkeye değişmekle birlikte, çoğunlukla finans, enerji, ulaşım, elektronik haberleşme, sağlık ve temel kamu hizmetleri gibi sektörler ve bunlara ait altyapılar kritik altyapılar olarak ele alınmaktadır [13]. Örneğin, Amerika Birleşik Devletlerinde ve Avrupa Birliği ülkelerinde kritik altyapılar olarak tespit edilen sektörler Tablo 2.1' de listelenmektedir.

---

[10] y.a.g.e.

[11] ITU, 2007, a.g.e. s.23

[12] Avrupa Komisyonu, "Terörle Mücadelede Kritik Altyapıların Korunması", 20.01.2004, Brüksel, s. 3 http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf

[13] ITU, "Siber Güvenliğe Ulusal Yaklaşım üzerine En İyi Uygulamalar Taslak Raporu, Ulusal Siber Güvenlik Çalışmalarının Organize Edilmesi için bir Yönetim Çerçeve Modeli", Ocak 2008, s. 6

Tablo 2.1. ABD ve AB'de Kritik Altyapılar

ABD	AB
Su	Su
Gıda	Enerji
Sağlık	Ulaşım
Enerji	Tarım ve gıda
Finans	Kolluk hizmetleri
Ulaşım	**Bilgi ve iletişim**
Sivil yönetim	Bankacılık ve finans
Bilgi ve iletişim	Bayındırlık hizmetleri
Uzay ve araştırmaları	Federal ve yerel hizmetler
Kimyasal ve nükleer endüstri	Acil hizmetler (sağlık, itfaiye, vb.)
Kamu düzeni ve güvenlik alanı	

Kaynak: Brunner, E. M., Suter, M. , "Uluslararası Kritik Bilgi ve Altyapıların Korunması El Kitabı 2008-2009", Güvenlik Çalışmaları Merkezi, İsviçre

Günümüzde, kritik altyapılar, hızla ve giderek artan bir şekilde BİT'e ve elektronik haberleşme altyapılarına bağlı hale gelmektedir (Şekil 2.2).

Şekil 2.2. Kritik Altyapıların BİT' e Bağlılığı

Kritik bilgi ve altyapıların korunması ise, Avrupa Komisyonu tarafından, olası arızalar, saldırılar veya beklenmedik durumlar karşısında, kritik bilgi ve altyapıların performanslarının belirli bir kalite düzeyinin üzerinde kalmasını ve zararların asgari düzeyde tutulmasını sağlamak için altyapı sahiplerinin, işletmecilerin, üreticilerin, kullanıcıların ve düzenleyici otoritelerin yürüttükleri programlar ve faaliyetler bütünü

olarak tanımlanmaktadır [14]. Dolayısıyla, kritik bilgi ve altyapıların korunması sektörler arası bir kavramdır ve bütüncül bir yaklaşımla ele alınarak kritik altyapıların korunması ile ilişkilendirilmelidir [15].

Kritik bilgi ve altyapıların korunmasını hedefleyen ulusal politikalar;

- Önleme ve erken uyarı,
- Tespit,
- Müdahale,
- Kriz yönetimi

hususlarını ele alan bir çerçeve model üzerine bina edilmelidir [16].

[14] Avrupa Komisyonu, "Kritik Altyapıların Korunması Avrupa Programına İlişkin Rapor", 17.11.2005, Brüksel, s. 19

[15] y.a.g.e.

[16] Suter, M., "Kritik Bilgi ve Altyapıların Korunması üzerine bir Ulusal Çerçeve Model", 2007, Güvenlik Çalışmaları Merkezi, Zürih

3 SİBER TEHDİTLER VE AMAÇLARI

Siber tehditler, BİT olanaklarından faydalanılarak türetilmiş, tamamen yeni suç tanımları doğuran siber saldırıların yanı sıra; BİT olanaklarının araç olarak kullanıldığı, klasik suçların siber ortama uyarlanmış hallerini de kapsamaktadır. Örneğin bilgisayar virüsleri, Bilgi Çağının beraberinde getirdiği tamamen yeni bir suç teşkil eden siber tehditlerdendir. Öte yandan, internet bankacılığı kullanıcılarının maruz kaldıkları dolandırıcılık, gerçek dünyada işlenen dolandırıcılık suçunun bir benzeridir. Bu bölümde, ilk grupta yer alan siber tehditler ve amaçları ile bunlara ilişkin istatistikî veriler özetlenmektedir.

3.1 Siber Tehditler

Siber tehditler esas itibarıyla 5 gruba ayrılabilir:

- Hizmetin engellenmesi ("DoS – Denial of Service" ya da "DDoS – Distributed Denial of Service") saldırıları
- Kötücül yazılımlar
- Yemleme ("phishing")
- İstemdışı elektronik posta ("spam")
- Şebeke trafiğinin dinlenmesi ("sniffing" ve "monitoring")

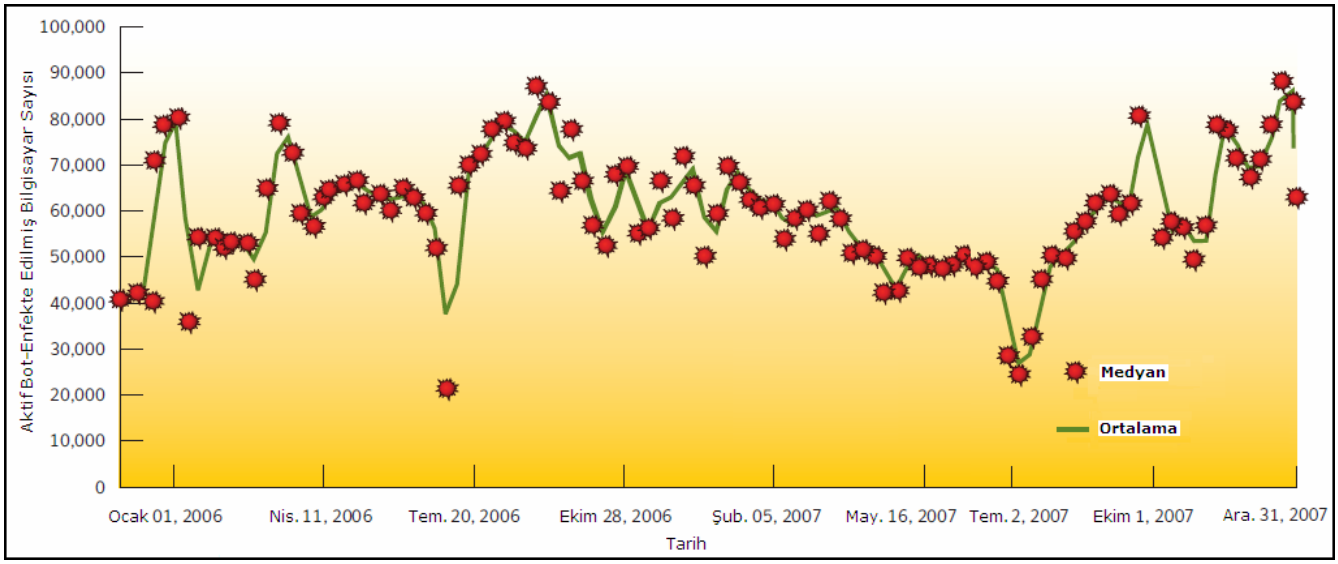
3.1.1 Hizmetin engellenmesi saldırıları

Hizmetin engellenmesi saldırıları, BİŞ'i gereksiz veri trafiği ile meşgul ederek, nihayetinde bunları hizmet sunamaz hale getirmek amacıyla yapılan saldırılardır. Şebekelerde iletilen veriler kimlik doğrulaması yapılamadığı için BİS'e erişemese de,

veri trafiğinin büyüklüğü ve sıklığı BİS'de sunulan hizmetleri yönetilemez hale getirmektedir [17].

DoS ve DDoS saldırıları, güvenlik açıklarından faydalanılarak ele geçirilen ve haberleri dışında başka bir kullanıcı tarafından uzaktan yönetilen "zombi" veya "bot" olarak adlandırılan bilgisayarlar aracı olarak kullanılarak gerçekleştirilmektedir. Dünya çapında bu şekilde yönetilen ve kontrol altında tutulan bilgisayarların yer aldığı "bot network (botnet)" adı verilen ağlar bulunmaktadır ve her gün binlerce bilgisayar bu ağlara dahil olmaktadır. (Şekil 3.1)

Şekil 3.1. Aktif Bot-Enfekte Edilmiş Bilgisayarlar (Günlük)



Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-1 ve 2007-2

Bot olarak nitelenen bilgisayarları kontrol eden sunucularının bulunduğu ülkeler incelendiğinde, ülkemizin, 2007 verilerine göre %2'lik bir pay ile 10. sırada olduğu görülmektedir. (Tablo 3.1)

[17] Hann, R. W., Layne-Farrar, A., "Yazılım Güvenliği Hukuku ve Ekonomisi", Harvard Hukuk ve Kamu Siyaseti Dergisi, Güz 2006, s. 289

Tablo 3.1. Bot Bilgisayarları Kontrol Eden Sunucuların Bulunduğu Ülkeler

Sıra	Ülke	Yüzde
1	ABD	%43
2	Almanya	%7
3	Kanada	%7
4	Güney Kore	%6
5	Çin	%3
6	İngiltere	%3
7	Tayvan	%3
8	İtalya	%2
9	İsveç	%2
10	Türkiye	%2

Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-1

3.1.2 Kötücül yazılımlar

Kötücül yazılımlar;

- Bilgisayar virüsleri
- Kurtçuk (“worm”)
- Truva atı (“trojan”)
- Klavye izleme (“key logger”) yazılımları
- İstem dışı olarak gönderilen ticari tanıtım (“adware”) yazılımları
- Bilgi toplayan casus / köstebek (“spyware”) yazılımlar

olarak sınıflandırılabilir [18].

Bilgisayar virüsleri, kullanıcıların haberi olmaksızın bilgisayarlarına yerleşen, kendi kendilerine hızla çoğalabilen, kendilerini yerleştikleri bilgisayarlarda bulunan programlara iliştirerek kullanıcıların iletişim kurdukları diğer bilgisayarlara da bulaşabilen ve bu bilgisayarlarda saklanan verilerin gizlilik, bütünlük ve

[18] ITU, 2007, a.g.e.

erişilebilirliğine zarar veren kodlar içeren yazılımlardır [19]. En tanınmış bilgisayar virüsleri Melissa, Çernobil, I Love You, Stoned-Marijuana ve Michelangelo olup[20], I Love You virüsünün dünya çapında yaklaşık 45 milyon bilgisayara bulaştığı ve yaklaşık 10 milyar USD' lik maddi kayba yol açtığı ifade edilmektedir [21].

Kurtçuk olarak adlandırılan yazılımlar da tıpkı virüsler gibi kendi kendilerine çoğalarak internette dolaşan kötücül yazılımlardır. Ancak bunların internette dolaşabilmeleri için virüsler gibi kendilerini mevcut bir programa iliştirmelerine gerek yoktur [22]. Kurtçuklar bellek, bant genişliği gibi sistem kaynaklarını meşgul etmek suretiyle BİS'in ulaşılabilirliğine zarar vermeyi ve onları uzaktan kontrol etmeyi amaçlamaktadırlar. En bilinen kurtçuklar Nimda, Love Bug ve Blaster olup, Nimda kurtçuğunun dünya çapında yaklaşık 3 milyar USD' lik, Love Bug'ın ise 10 milyar USD' lik maddi kayba yol açtığı tahmin edilmektedir. [23]

Truva atı olarak bilinen kötücül yazılımlar genellikle sıradan programlar veya yardım dosyalarının içine gizlenip oradan sistemlerin içine sızarak, işlemcileri meşgul etmekte, verileri veya programları kurcalamakta veya yok etmekte, sistemleri çökertmekte veya ileride gerçekleştirilmesi planlanan saldırılar için pasif olarak bekletilmektedirler [24]. En bilinen truva atları NetBus, Back Orifice, SubSeven ve MyDoom'dur. MyDoom adlı truva atının yol açtığı maddi zararın 4,8 milyar USD civarında olduğu öngörülmektedir. [25]

---

[19] y.a.g.e.

[20] Nagpal, R., "Küreselleşme Bağlamında Siber Güvenlik", 2. Dünya Bilişim ve Hukuk Kongresi, Madrid, İspanya, Eylül 2002, s. 6

[21] Schjølberg, S., Hubbard, A. M., "Siber Güvenlik üzerine Ulusal Hukuki Yaklaşımların Harmonize Edilmesi" ITU WSIS Siber Güvenlik Konulu Toplantı, Cenevre, 28 Haziran – 1 Temmuz 2005, s. 12

[22] y.a.g.e.

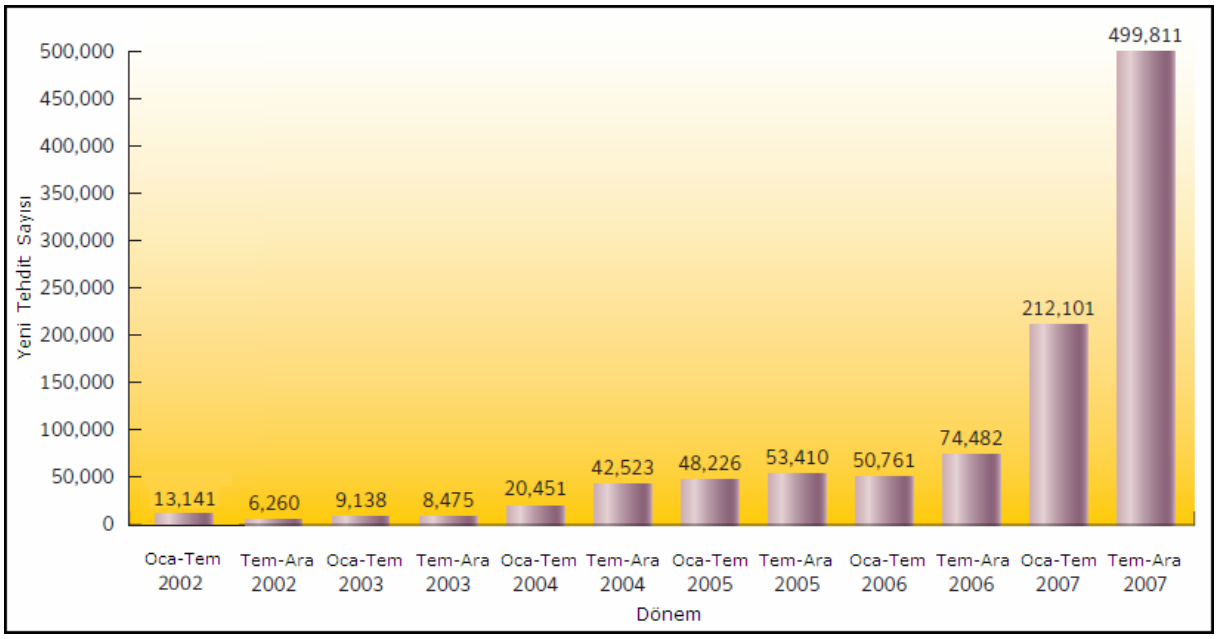
[23] Lemos, R. "Altyapı Riskinin Değerlendirilmesi", CNET News.com, Ağustos 2002, http://builder-news.com/2009-1001-954780.html

[24] ITU, 2007, a.g.e.

[25] Hahn, R.W., Layne-Farrar, A., a.g.e.

Virüs, kurtçuk, Truva atı gibi yazılımlar genellikle bir elektronik posta eki olarak internet kullanıcılarına gönderilir ve bu eki çalıştıran kullanıcıların bilgisayarlarına bulaşırlar. Daha sonra bu yazılımlar kendi kendini çoğaltarak bu bilgisayarların iletişim kurduğu sistem ve şebekelere salgın gibi yayılır. Bunlar ve diğer kötücül yazılımlar genelde ücretsiz veya tanıtım amaçlı yazılımlar, pornografik internet siteleri, oyunlar, tartışma grupları aracılığıyla yayılmaktadır.[26] Günden güne artan ve çeşitlenen kötücül yazılımların Ocak 2002 – Temmuz 2007 arasındaki gelişimi Şekil 3.2' de görülmektedir.

Şekil 3.2. Kötücül Yazılım İçeren Yeni Tehditler

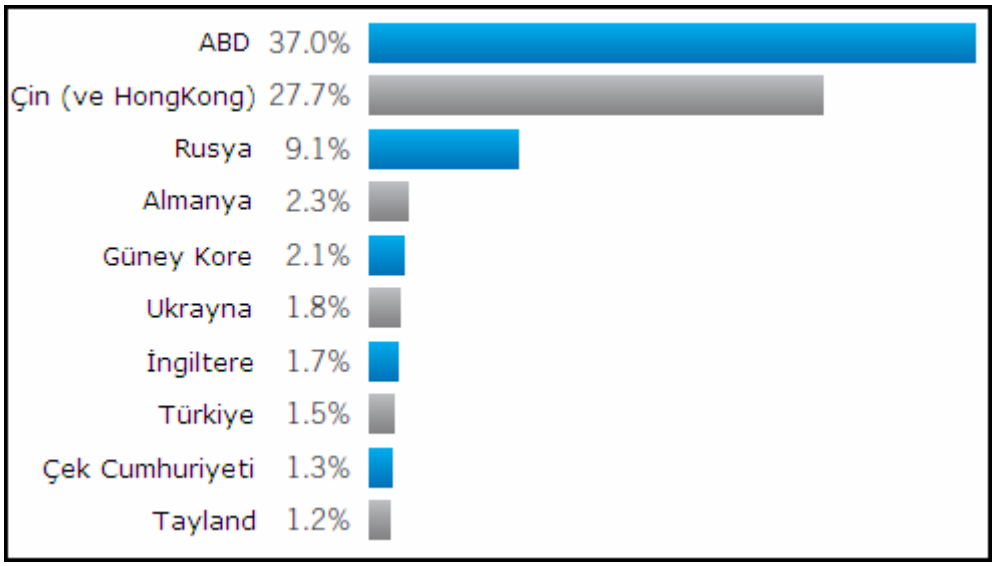


Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-1 ve 2007-2

Ülkemiz, en fazla kötücül yazılım barındıran ülkelerden olup, 2008 verilerine göre %1,5' lik bir pay ile dünya sıralamasında 8. sırada yer almaktadır. (Şekil 3.3)

[26] y.a.g.e.

Şekil 3.3. En Fazla Kötücül Yazılım Barındıran Ülkeler



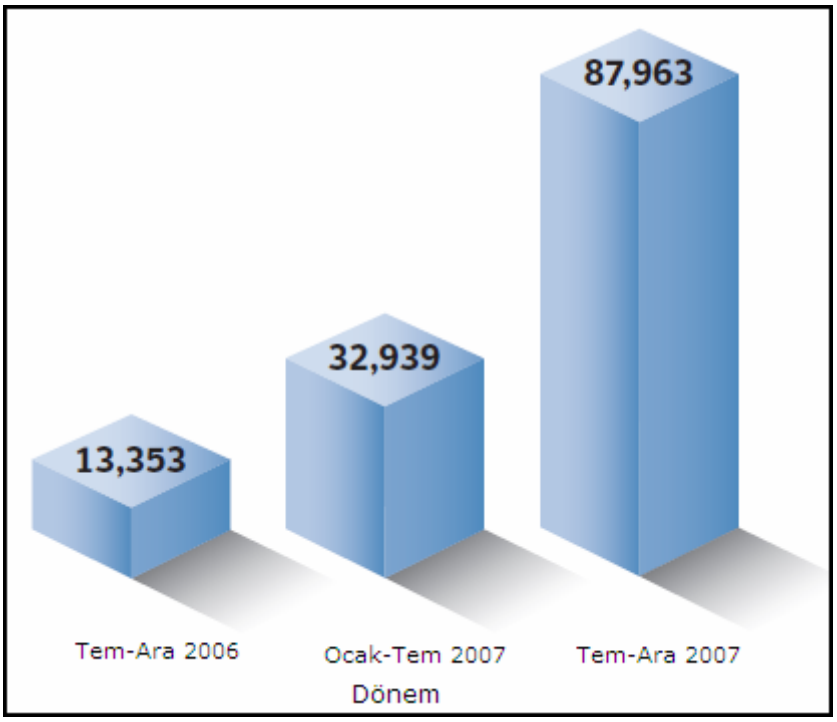
Kaynak: Sophos Güvenlik Tehditleri Raporu 2009

3.1.3 Yemleme

Yemleme, internet kullanıcılarının kandırılarak veya ikna edilerek, ileride yasadışı amaçlarla kullanmak üzere, kişisel veriler, şifre gibi kritik bilgilerinin ele geçirilmesidir [27]. Yemlemede en çok kullanılan yöntem, bankacılık veya elektronik ticaret hizmeti sunan İnternet sitelerinin tıpatıp benzerlerini oluşturmak ve kullanıcılara oluşturulan sahte sitelerin bağlantılarını içeren elektronik postalar göndermek suretiyle kişileri bu sahte sitelere yönlendirmektir. Güvenilir bir kaynaktan geldiğine inandıkları elektronik postaların içindeki bağlantılara giren kullanıcılar, sahte sitelere yönlendirilmekte, bu sitelerdeki belli formları doldurmaları sağlanmakta ve verdikleri bilgiler siber saldırganlarca ele geçirilmektedir. Yemleme, kurum, kuruluş ve ticari markaların itibar kaybetmesine neden olabilmektedir. Symantec tarafından yapılan bir araştırmada, 2006 yılının 2. yarısında 13353 adet olan yemleme sitesi sunucularının 2007 yılının 2. yarısında 87963'e ulaştığı görülmektedir. (Şekil 3.4)

[27] y.a.g.e.

Şekil 3.4. Yemleme (Phishing) İnternet Sitesi Sunucuları



Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-2

Aynı araştırmanın sonuçları, 2007 yılında yemleme saldırılarına maruz kalan markalardan %80' inin finans sektöründe yer aldığını göstermektedir.

3.1.4 İstemdışı elektronik posta

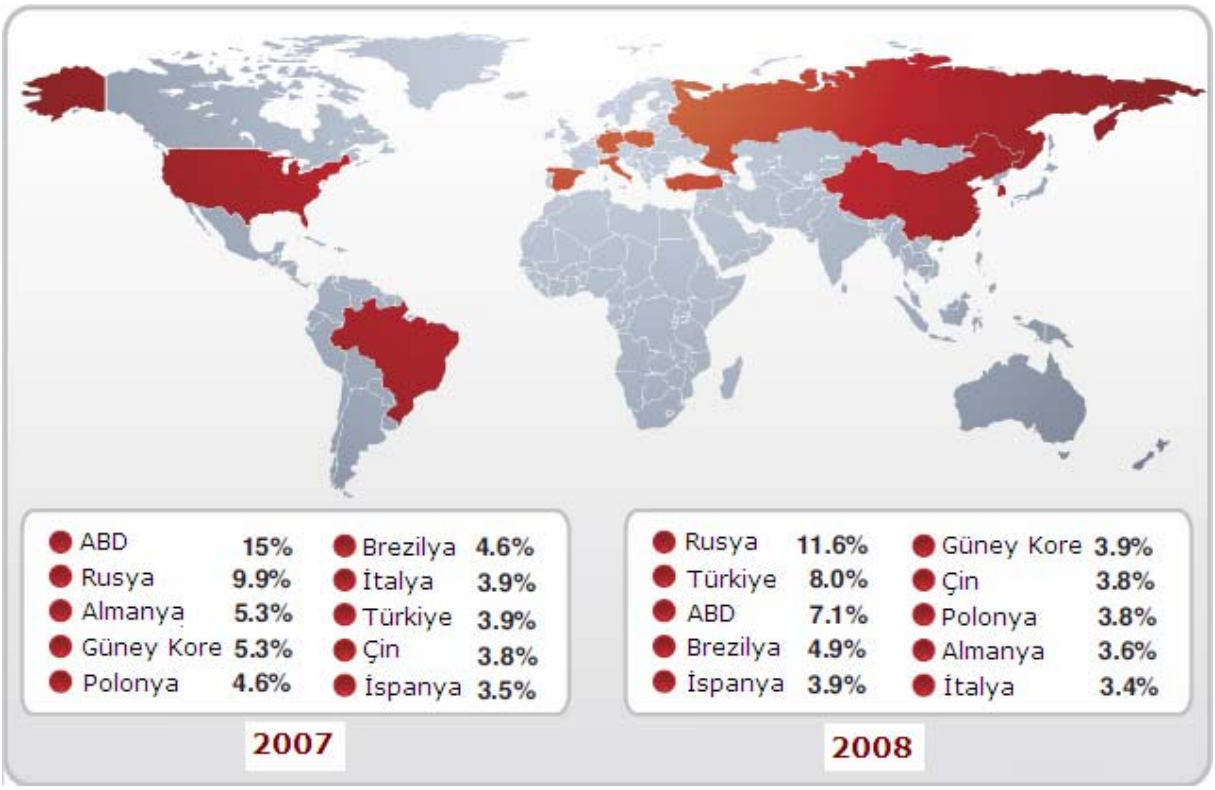
İstemdışı elektronik postalar, istenilmediği halde toplu olarak internet kullanıcılarına gönderilen ve genellikle tanıtım veya propaganda amacı taşıyan elektronik postalardır [28]. İnternet servis sağlayıcıların önemli ölçüde teknik ve mali kaynağı bunları engellemeye tahsis etmelerine ve kamu otoritelerinin bunlarla savaşmaya niyetli olduklarını sürekli ifade etmelerine rağmen, istemdışı elektronik postalar hala yaygın olarak gönderilmektedir. İstemdışı elektronik postalar, e-posta sunucularını ve kullanıcıların posta kutularını gereksiz yere işgal ederek hoşnutsuzluk yaratmakta, aynı zamanda kötücül yazılımların yayılmasına da yardımcı olmaktadırlar. Ayrıca,

[28] Canbay, C. Beydoğan, T. A., a.g.e.

istemdışı elektronik postalar, internet servis sağlayıcıların işletmekte oldukları şebekeleri meşgul etmekte ve şebeke kapasitelerini doldurmaktadırlar.

Ülkemiz, en fazla istemdışı elektronik posta yayan ülkelerdendir. 2007 yılında dünya sıralamasında %3,9'luk pay ile 8. sırada bulunan ülkemiz, 2008 yılında ise %8'lik pay ile 2. sıraya yükselmiştir. (Şekil 3.5)

Şekil 3.5. En Fazla İstemdışı Elektronik Posta Yayan Ülkeler



Kaynak: IBM X-Force Trend İstatistikleri 2007 ve 2008

3.1.5 Şebeke trafiğinin dinlenmesi

BİŞ üzerinden iletilen şifrelenmemiş veya şifreleri çözülebilen verilerin siber saldırganlarca dinlenerek yetkili kullanıcıların bağlantı parametrelerinin ele

geçirilmesidir. Aktif dinleme izleme (“monitoring”), pasif dinleme ise koklama (“sniffing”) olarak nitelendirilir [29].

3.2 Siber Tehditlerin Amaçları

Siber tehditler ile ulaşılmak istenen amaçlar 3 ana başlıkta ele alınabilir:

- BİS’e yetkisiz erişim
- Verilerin değiştirilmesi, yok edilmesi, ifşa edilmesi veya üçüncü taraflara verilmesi
- Hizmetin engellenmesi

3.2.1 BİS’e yetkisiz erişim

Yetkisiz erişim, BİS’e erişme yetkisi olmayan kişilerin şifre gibi sistemlere giriş parametrelerini ele geçirerek veya sistemlerdeki açıklıkları kullanarak BİS’e erişmeleridir. Yetkili kullanıcıların parametreleri, sosyal mühendislik, şebeke trafiğinin dinlenmesi, kötücül yazılımlar kullanarak parametrelerin saklandığı dosyalara erişilmesi, şifrelenmiş parametrelerin kırılması, çevrebirimleri aracılığıyla casusluk yapılması gibi yollarla ele geçirilmekte ve sistemlere nüfuz etmek için kullanılmaktadır [30]. Yetkisiz erişim, kişisel mahremiyetin ve haberleşmenin gizliliğinin ihlal edilmesine zemin hazırlamaktadır.

3.2.2 Verilerin değiştirilmesi, yok edilmesi, ifşa edilmesi veya üçüncü taraflara verilmesi

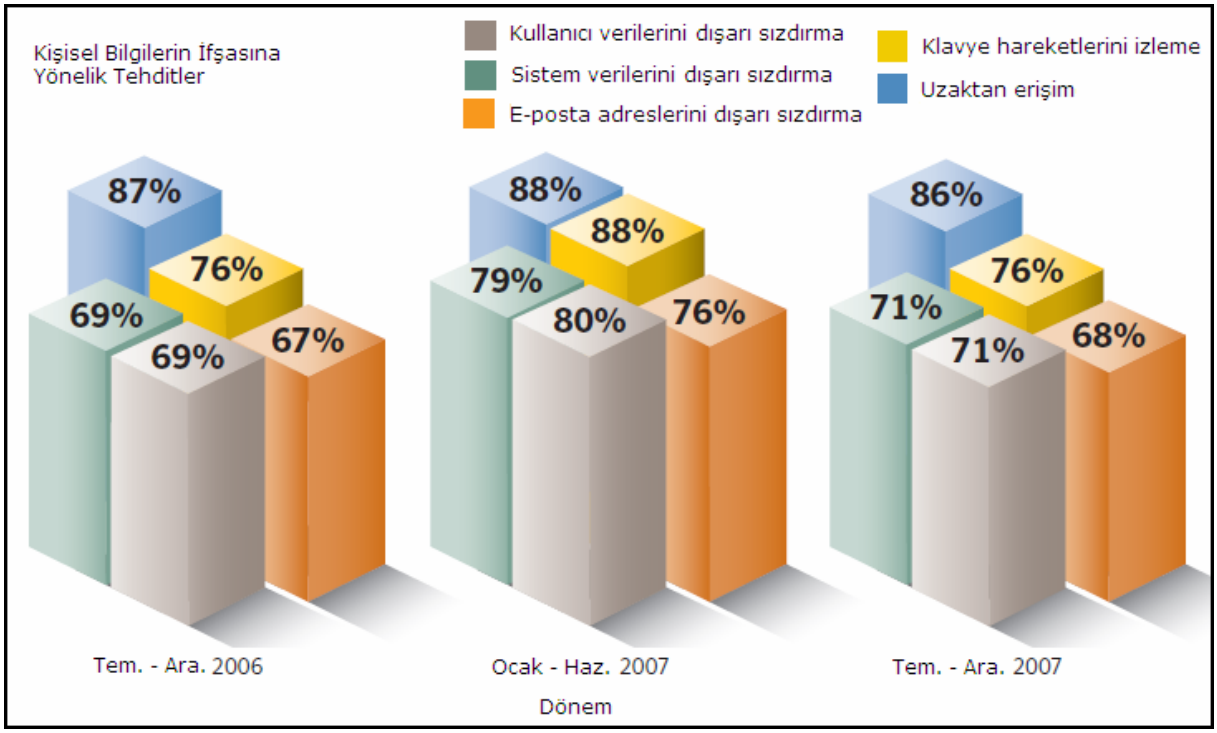
BİS üzerinde saklanan, işlenen ve/veya iletilen veriler, sistemlere dışarıdan yetkisiz erişim, verilerin sistem içinden dışarıya sızdırılması veya yetkisiz erişim ya da

[29] ITU, 2007, a.g.e.
[30] ITU, a.g.e.

sızdırma olmaksızın klavye izlerinin izlenmesi gibi yollarla ele geçirilebilmektedir. Ele geçirilen veriler, sayısal ortamlar üzerinde bulunduklarından, elektronik, optik ve manyetik donanımlar veya özel yazılımlar kullanılarak kolaylıkla değiştirilebilmekte veya yok edilebilmektedir.

Ayrıca, söz konusu veriler, itibarı zedeleme, kamuoyunu yanıltma, şantaj gibi amaçlarla ifşa edilebilmekte; dolandırıcılık, hırsızlık gibi klasik suçlar için kullanılabilmekte veya maddi menfaat elde etmek amacıyla üçüncü taraflara verilebilmektedir. 2006 ve 2007 yıllarında BİS'de saklanan, işlenen ve iletilen kişisel verilerin ele geçirilerek ifşasına yönelik tehditlerin boyutları aşağıdaki şekilde özetlenmektedir.

Şekil 3.6. Kişisel Verilerin İfşasına Yönelik Tehdit Türleri



Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-1 ve 2007-2

BİS'de ele geçirilen kişisel verilerin pazarlandığı yasadışı ekonomiler bile oluşmuştur. Bu ekonomilerde en fazla pazarlanan veriler Tablo 3.2' de listelenmektedir.

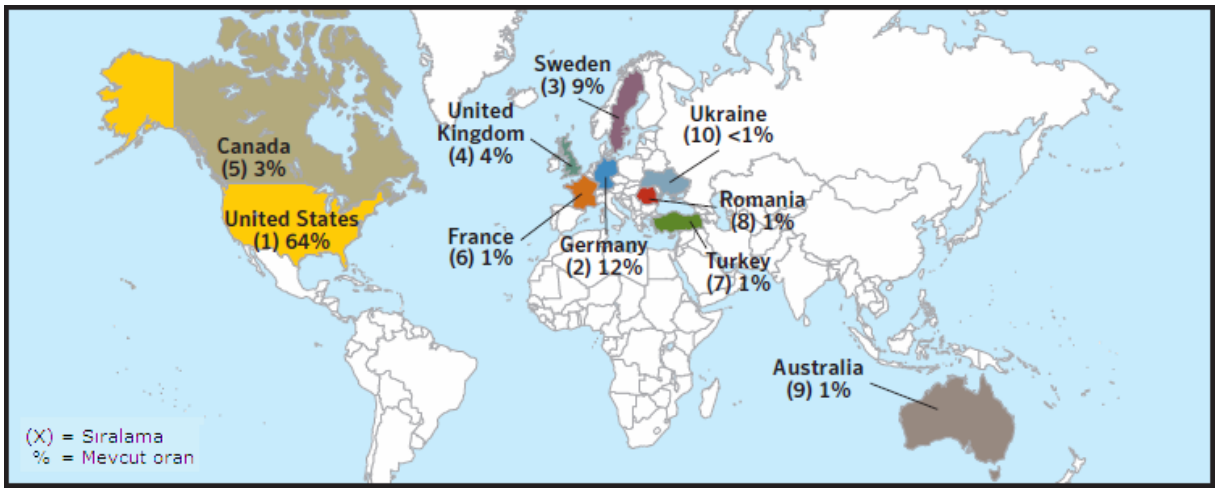
Tablo 3.2. Yasadışı Ekonomilerde En Fazla Pazarlanan Verilerin Analizi

Sıra	Nesne	Yüzde	Fiyat Aralığı
1	Kredi kartı numaraları	%22	0,50 – 5 USD
2	Banka hesapları	%21	30 – 400 USD
3	E-posta şifreleri	%8	1- 350 USD
4	E-posta yazılımları	%8	8 – 10 USD
5	E-posta adresleri	%6	2 – 4 USD/MB
6	Proxy adresleri	%6	0,50 – 3 USD
7	Tüm Kimlik Bilgileri	%6	10 – 150 USD
8	Sahte Kimlikler	%6	10 USD/hafta
9	Vatandaşlık numaraları	%3	5 – 7 USD

Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-1

Yasadışı ekonomi sunucularının bulunduğu ülkeler incelendiğinde ise, 2007 verilerine göre, ülkemizin %1'lik bir pay ile dünya sıralamasında 7. sırada olduğu görülmektedir. (Şekil 3.7)

Şekil 3.7. Yasadışı Ekonomi Sunucularının Bulunduğu Ülkeler

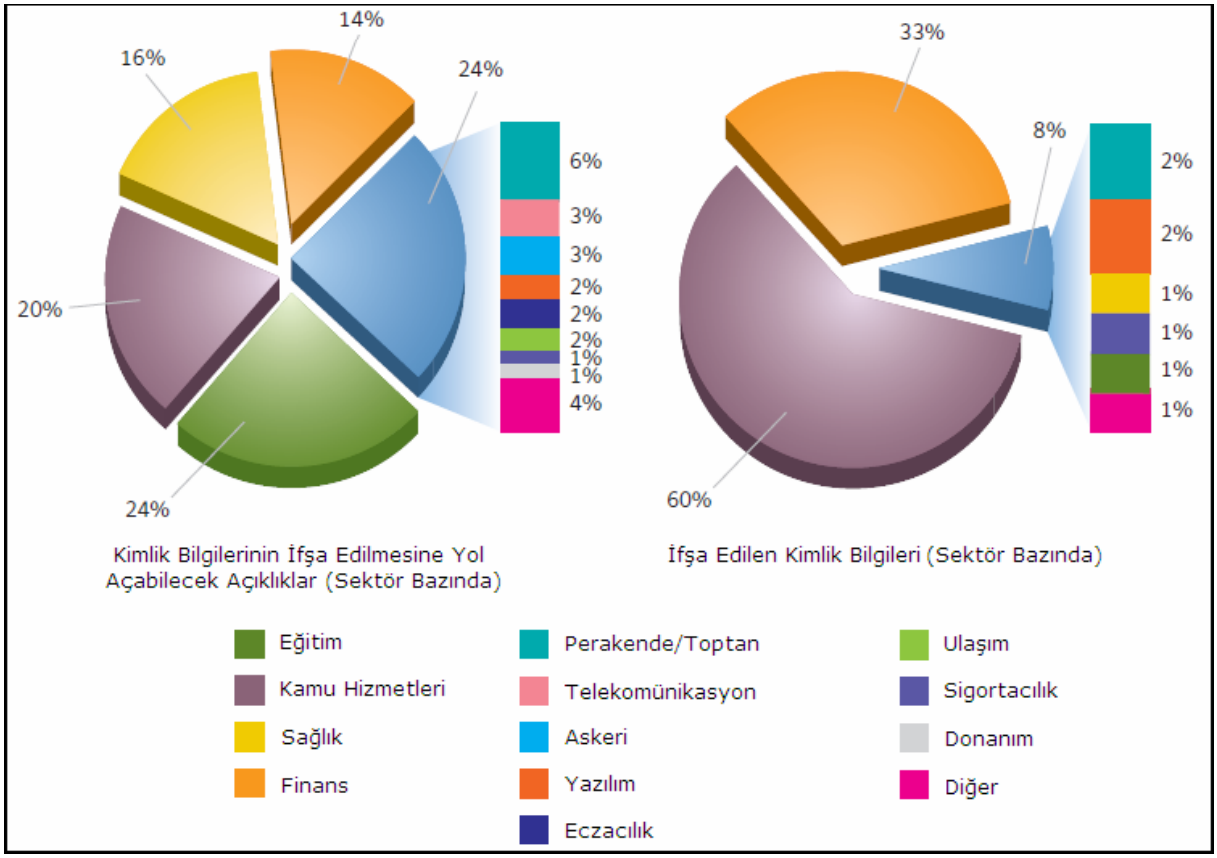


Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-1

Kişisel verilerin bir alt kümesi olan ve yasadışı ekonomilerde en sık pazarlanan veriler kimlik bilgileridir. Kimlik bilgilerinin büyük ölçüde saklandığı ve işlendiği, eğitim, kamu hizmetleri, sağlık, finans gibi sektörlerde kullanılan BİS, bu bilgilerin ifşasına

zemin hazırlayabilecek pek çok açıklıklar içermektedir. Söz konusu bilgilerin en fazla ifşa edildiği sektörlerin başında ise kamu hizmetleri ve finans sektörleri gelmektedir. (Şekil 3.8)

Şekil 3.8. Kimlik Bilgilerinin İfşası



Kaynak: Symantec İnternet Güvenlik Tehditleri Raporu 2007-2

Ülkemizde, 2008 yılında yapılan Konut Edindirme Yardımı ödemeleri sırasında 8,5 milyon kişinin TC kimlik ve sosyal güvenlik numaraları Resmi Gazete yoluyla internette yayımlanmıştır. Türkiye'de İnternet üzerinden işlem yapmak için adeta anahtar konumunda olan TC kimlik ve sosyal güvenlik numaraları kullanılarak herhangi bir kişinin maaş, son çalıştığı kurum, sağlık bilgileri, doğum yeri, anne ve baba adı, kızlık soyadı, ikamet ettiği adres gibi pek çok kişisel verisine kolaylıkla

ulaşılabileceği düşünüldüğünde, bu durumun siber güvenlik açısından son derece önemli sorunları beraberinde getirdiği anlaşılmaktadır [31].

3.2.3 Hizmetin engellenmesi

BİŞ, DoS, DDoS veya elektronik posta bombardımanı gibi saldırılar sonucunda üzerlerinden iletilen veri trafiğini taşıyamaz hale gelebilmektedir. Bu gibi durumlarda, BİS, söz konusu şebekeler aracılığıyla erişilen sistemlere erişilememekte ve bu sistemlerden hizmet alınamamaktadır. Ağ trafiğini farklı hedeflere yönlendirmeyi amaçlayan kötücül yazılımlar da şebekelerin işlerliğini tehdit etmektedirler. Söz konusu tehditler, BİS' i yetkili kullanıcılarına hizmet sunamaz hale getirmekte, saldırılara hedef olan tarafların büyük itibar kaybı ve maddi kayıp yaşamalarına sebep olmaktadırlar [32].

Yukarıda özetlenen siber tehditler ve sonuçlarının yanı sıra; doğal felaketler, kullanıcı hataları, yazılım veya donanımlarda meydana gelebilecek aksaklıklar, enerji kesintileri gibi hususlar da güvenlik riskleri doğurmaktadır [33]. Bu tür durumlar şebekelerin erişilebilirliğini zedeleyebilmekte, şebekelerin çökmesine veya siber saldırganlarca zarara uğratılmasına yol açabilecek ciddi açıklıklar oluşturabilmekte ve elektronik haberleşme altyapılarını yavaşlatabilecek veya çökertebilecek ölçüde trafik oluşturabilmektedirler.

Son yıllarda siber ortamda yaşanan bazı güvenlik olayları, dikkatleri siber güvenliğe çekmiştir. Örneğin, 2007 yılının Nisan ayında, kamu hizmetlerinin yoğun olarak İnternet üzerinden sunulduğu ve büyük bir siber ekonomiye sahip olan Estonya'nın, Rusya'ya ait bir savaş anıtını kaldırmasının ardından, Rus siber saldırganlar

---

[31] Üstün, G., "e-Devlet Skandalı", Milliyet Gazetesi, 30.07.2008, http://www.milliyet.com.tr/Ekonomi/HaberDetay.aspx?aType=HaberDetay&Kategori=ekonomi&ArticleID=972537&Date=30.07.2008&b=KEY%20skandalı&ver=79

[32] Avrupa Komisyonu, "Şebeke ve Bilgi Güvenliği: Avrupa Politik Yaklaşımı Tasarısı, Tebliğ", http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf, s. 9

[33] Canbay, C. Beydoğan, T. A., a.g.e.

tarafından ülkedeki birçok internet sitesi hizmet sunamaz hale getirilmiş, bu sitelerde işlenen veriler silinmiş, 6 bakanlığın internet sitesinin sistemleri çökertilmiş ve pek çok elektronik para transferinin gerçekleşmesi de engellendiği için ekonomide aksaklıklar yaşanmıştır. Estonya siber güvenlik birimlerinin yaptığı incelemelerde öncü saldırıların bizzat Rusya'daki kamu bilişim sistemlerinden geldiği tespit edilmiş, ayrıca, saldırılarda sahiplerinin haberi bile olmadan kontrol altına alınan yüz binlerce zombi bilgisayardan oluşan botnetlerin kullanıldığı ortaya çıkmıştır [34].

[34] Radikal Gazetesi, 4 Haziran 2007 tarihli baskı, http://www.radikal.com.tr/ek_haber.php?ek=sa&haberno=3522

4 ULUSAL SİBER GÜVENLİĞİN SAĞLANMASI

Gerek son yıllarda BİT'de yaşanan gelişmeler ve ülkelerin bu teknolojilere olan giderek artan bağlılığı, gerekse bu teknolojilerin başında gelen internette bulunan siber tehditler ile bunlara ve olası sonuçlarına ilişkin istatistikî verilerle desteklenen gelişmeler, siber güvenliği ve kritik bilgi ve altyapıların korunmasını, ulusal politikalarda öncelikle ele alınması gereken hususlar haline getirmiştir.

Siber güvenlik; siber tehditlere karşı, BİS üzerinde saklanan, işlenen ve/veya iletilen bilginin/verilerin erişilebilirlik, bütünlük, gizlilik unsurları ile bu sistemler üzerinde gerçekleştirilen iş ve işlemlerde bulunması gereken kimlik doğrulama ve inkâr edilemezlik unsurlarının korunmasını amaçlamaktadır. Bu unsurlardan bir veya birden fazlasının korunamaması halinde doğacak sorunlar, bireysel ve kurumsal çapta kayıplarla sınırlı kalmaz; ulusal, hatta küresel çapta ekonomik, siyasi, sosyal vb. pek çok alanda kayıplar yaşanmasına sebep olur. Aynı zamanda BİT'in kullanımında güven ve güvenliği zedeleyerek ulusal ve küresel çapta bilgi toplumuna ulaşma hedeflerinin de başarısızlıkla sonuçlanmasına yol açar.

Bu bağlamda, siber güvenliğin, gerek ulusal güvenliğimizin sağlanmasında, gerekse "e-Dönüşüm Türkiye" projesi kapsamında gerçekleştirilmesi hedeflenen ulusal bilgi toplumuna dönüşüm yolunda öncelik verilmesi gereken bir husus olduğu değerlendirilmektedir. Bu bölümde, ülkemizde ulusal siber güvenliğin sağlanması konusunda kritik öneme sahip olduğu değerlendirilen temel ilkeler, yöntemler ve adımlara yer verilmiştir.

4.1 Temel İlkeler

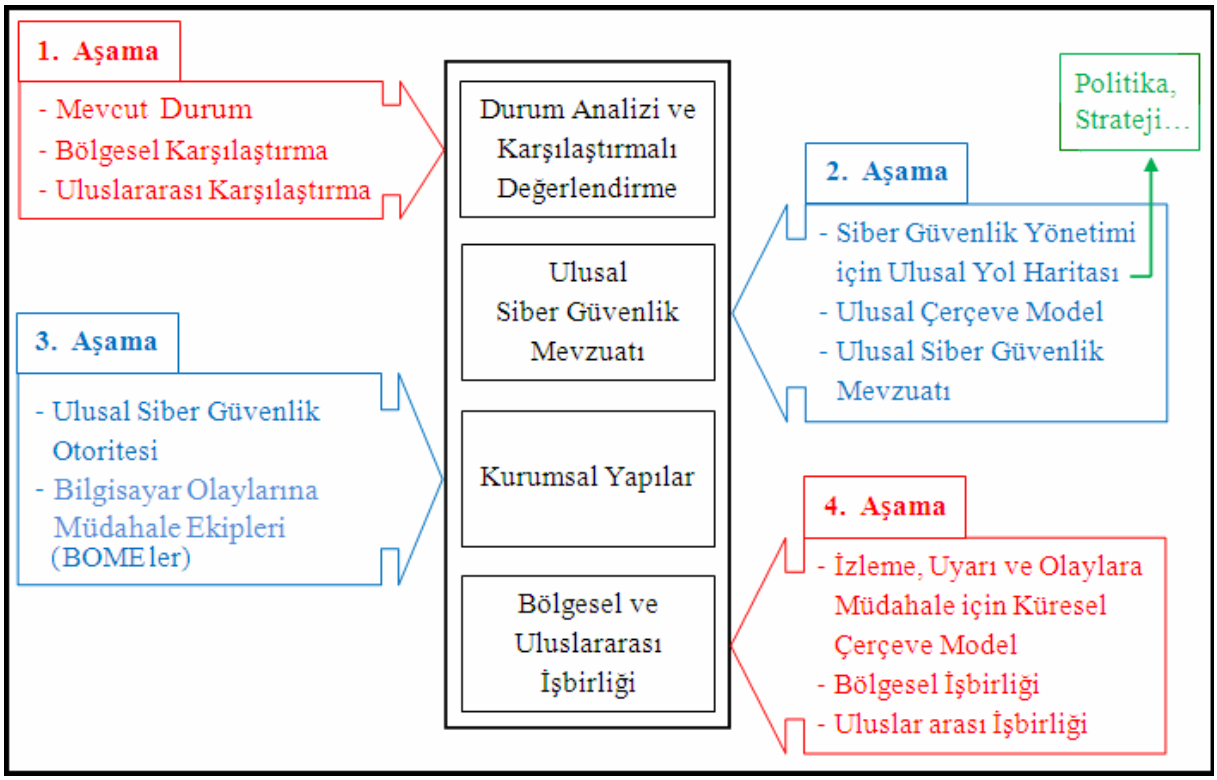
Ulusal siber güvenliğin sağlanmasına yönelik olarak yürütülecek çalışmalarda esas alınması gereken temel ilkeler şunlardır:

1. Uluslararası sözleşmelerle teminat altına alınmış temel insan hak ve hürriyetlerinin korunması,
2. Demokratik toplum düzeninin gereklerine uyulması,
3. Alınacak tedbirlerin Ölçülülük İlkesine göre belirlenmesi,
4. Karar alma süreçlerine tüm paydaşların katılımını sağlayacak kapsayıcı bir yaklaşımın benimsenmesi,
5. Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi,
6. Geliştirilecek çözümlerde güvenlik ile kullanılabilirlik arasında denge kurulması,
7. Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması,
8. Uluslar arası işbirliğinin sağlanması.

4.2 Yöntem

Ulusal siber güvenliğin sağlanmasını hedefleyen çalışmalarda Şekil 4.1'de özetlenen 4 aşamalı yaklaşımın izlenmesi ITU tarafından önerilmektedir.

Şekil 4.1. Siber Güvenliğin Sağlanması Üzerine Bir Yaklaşım



Kaynak: ITU, "Küresel Siber Güvenlik Gündemi – Küresel Stratejik Rapor", 2008

1. Aşamada; ülkemizin siber güvenlik konusundaki mevcut durumu farklı ülkelerin mevzuatları ile ve bölgesel ve uluslar arası çalışmalar ile karşılaştırılarak analiz edilmeli ve siber güvenlik konusunda başarılı ulusal planlar, programlar ve mevzuat geliştirmiş olan ülke örneklerinden yararlanılmalıdır. Bu aşamada önemli olan nokta mer'i mevzuatımızdaki eksiklikleri ve bu eksikliklerin nasıl giderilebileceğine ilişkin olabildiğince çok alternatif yol ve yöntem tespit edebilmektir.

2. Aşamada; siber güvenlik konusunda ulusal yol haritamız (politika ve strateji) ve ulusal çerçeve model oluşturulmalı ve ulusal siber güvenlik mevzuatımız geliştirilmelidir. Ulusal çerçeve model;

- Ulusal siber güvenlik politikası ve stratejisinin etkin bir şekilde uygulanması,
- Mevcut güvenlik yasalarının siber ortama uyarlanması için gereken çalışmaların yapılması,
- BİS'i hedef alan saldırıların önlenmesi, tespit edilmesi, bunlara müdahale edilmesi ve en az hasarla geri dönüşün sağlanması için gereken usul ve esasların belirlenmesi,
- Ulusal siber güvenlik kültürünün benimsenmesinin sağlanması,
- Temel paydaşların belirlenmesi,
- Ulusal siber güvenlik programının denetlenmesi, değerlendirilmesi, doğrulanması ve etkinliğinin arttırılması

gibi hususları ele almalıdır.

Ülkemizde, siber savunma / sanal ortam güvenliği politika esaslarını belirlemek üzere TÜBİTAK UEKAE'nin koordinatörlüğünde çeşitli kamu kurum ve kuruluşlarının temsilcilerinden oluşan bir çalışma grubu oluşturulmuştur. Çalışma grubu faaliyetlerini 30 Ocak 2009 tarihinde tamamlamış ve "Ulusal Sanal Ortam Güvenlik Politikası" belgesini hazırlamıştır. Söz konusu çalışma grubunda yer alan kurum ve kuruluşlar şunlardır:

- Cumhurbaşkanlığı
- Başbakanlık
- Dışişleri Bakanlığı
- Adalet Bakanlığı
- Milli Savunma Bakanlığı
- Maliye Bakanlığı

- Ulaştırma Bakanlığı
- İçişleri Bakanlığı
- Genelkurmay Başkanlığı
- Devlet Planlama Teşkilatı Müsteşarlığı
- Dış Ticaret Müsteşarlığı
- Hazine Müsteşarlığı
- Türkiye Cumhuriyet Merkez Bankası
- Milli Güvenlik Kurulu Genel Sekreterliği
- Milli İstihbarat Teşkilatı Müsteşarlığı
- Bankacılık Düzenleme ve Denetleme Kurumu
- Emniyet Genel Müdürlüğü
- Bilgi Teknolojileri ve İletişim Kurumu
- TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

Mezkûr politika belgesinin ana başlıkları Tehditler ve Açıklıklar, Temel İlkeler ve Sanal Ortam Güvenlik Adımları'dır. Bununla birlikte, politika belgesinde yer alan hususların uygulama adımlarını belirleyen bir strateji ve/veya eylem planı bulunmamaktadır.

3. Aşamada; ulusal siber güvenlik çalışmalarını yürütecek olan kurumsal yapı oluşturulmalıdır. Bu yapının görev ve sorumlulukları ile diğer paydaşlarla ilişkileri belirlenmelidir.

4. Aşamada; İnternet başta olmak üzere BİT'in sınır tanımayan küresel yapısı göz önünde bulundurulmalı ve küresel çapta ele alınmaması halinde siber tehditlerin ve saldırıların sonlandırılamayacağı bilinmelidir. Bu itibarla uluslar arası bir işbirliği modeli geliştirilmelidir.

4.3 Siber Güvenlik Adımları

Önceki bölümlerde tanımlanan temel ilkeler ışığında ve önerilen yöntem doğrultusunda, ülkemizde mevcut bulunan siber güvenlik çalışmaları ile bölgesel ve uluslar arası örneklerin karşılaştırılması suretiyle tespit edilen eksiklikler ve bu eksikliklerin giderilerek ulusal siber güvenlik çalışmalarının etkinliğinin arttırılması için atılması gereken somut adımlar bu bölümde özetlenmektedir. Bu adımları 5 başlık altında toplamak mümkündür:

1. Ulusal siber güvenlik mevzuatının geliştirilmesi
2. Teknik ve işlevsel tedbirlerin alınması
3. Kurumsal yapılanmanın oluşturulması
4. Ulusal kapasitenin geliştirilmesi ve farkındalığın arttırılması
5. Uluslararası işbirliğinin sağlanması

4.3.1 Ulusal siber güvenlik mevzuatının geliştirilmesi

4.3.1.1. Mevcut durum

Günümüzde, BİT'de yaşanan hızlı gelişmeler siber suçluların çıkar amaçlı kullanabilecekleri yeni fırsatlar yaratırken, siber suçlarla mücadeleyi de oldukça karmaşık hale getirmekte; geçmişte sadece fiziksel varlıklara veya kişilere yönelik suçlarla mücadele alanında görev yapmakta olan kolluk kuvvetlerinin ve adli personelin işlerini güçleştirmektedir. Siber suçlarla mücadelede yaşanan belli başlı güçlükler şunlardır:

1. Yasal boşlukların bulunması

Yasalardaki yetersizlikler dolayısıyla bir ülkede suç olarak kabul edilen bir fiilin, başka bir ülkede suç sayılmaması veya o ülkede söz konusu fiile ilişkin herhangi bir mevzuat bulunmaması, siber saldırganlar için "güvenli sığınaklar" oluşturmaktadır [35].

Ülkemizde, 10 yıldır gündemde olan Ulusal Bilgi Güvenliği Kanunu ve Kişisel Verilerin Korunması Kanunu tasarıları halen yasalaştırılamamıştır. Ayrıca, siber ortamın zemin hazırladığı hizmetin engellenmesi, kötücül yazılımlar, yemleme gibi fiilleri kapsayacak mevzuat çalışmalarına da ihtiyaç duyulmaktadır.

2. Usule ilişkin mevzuatın yetersizliği

Siber saldırılar arttıkça ve çeşitlendikçe, mağdurları ve zanlıları tespit etme, delil toplama gibi temel soruşturma aşamaları değişmese de bu aşamalarda kullanılan usullerin değişmesi gerekmektedir. Siber ortamda mağdur ve saldırganı tespit etmenin ve delil toplamanın kendine has zorlukları ve yöntemleri bulunmaktadır. Örneğin, BİT kullanıcıları arasında elektronik posta ve dosya transferini yetkisiz erişimlerden korumak gibi amaçlarla kullanılan şifreleme ve benzeri yöntemler, siber saldırganlar tarafından da elektronik delilleri ulaşılamaz hale getirmek için kullanılmaktadır. Bunun yanı sıra, elektronik deliller kolaylıkla silinebilmekte, tahrip edilebilmekte ve karartılabilmektedir. Ayrıca, karşılıklı yasal yardım antlaşmaları, çok taraflı sözleşmeler veya yetki verme yazıları gibi diğer ülkelerden suça ait delil talep etmeyi sağlayan yazışmalar ve diğer prosedürler gecikmeye sebep olarak elektronik delillerin suçlular tarafından tamamen yok edilmesine yol açabilmektedir. Dolayısıyla, siber saldırıların nasıl araştırılıp soruşturulacağına, delillerin nasıl toplanıp değerlendirileceğine ve ülkeler arasında izlenecek usule ilişkin mevzuata ihtiyaç duyulmaktadır [36].

Çeşitli ülkelerin mevzuatlarında yer alan ve siber güvenlik ile ilişkilendirilebileceği değerlendirilen düzenlemeler EK-1'de listelenmektedir.

---

[35] ITU, "Küresel Siber Güvenlik Gündemi – Küresel Stratejik Rapor", 2008
[36] y.a.g.e.

3. Siber ortamda kolluk kuvvetlerinin yetkilerinin belirsizliği

Gerçek dünyada, her kolluk kuvvetinin gözetmekle sorumlu olduğu bölge coğrafi sınırlarla belirlenmiş durumdadır. İnternet ortamının gözetilmesi sorumluluğu ise tek bir kolluk kuvvetine verilemeyecek kadar kapsamlı olup, bu durum siber saldırganlara sunulan güvenli sığınakları arttırmakta, kolluk kuvvetlerinin işini güçleştirmektedir.

4. Teknik uzmanlık eksikliği

Yüksek teknoloji kullanılarak işlenen suçların soruşturulmasında, iyi yetişmiş insan kaynağına ve elektronik delilleri analiz edebilecek yazılım ve donanıma ihtiyaç duyulmaktadır. Gerek kolluk kuvvetleri, gerekse adli personel arasında, siber suçların ve delillerin teknik altyapıları hakkında uzmanlaşmış yeterli sayıda uzman bulunmamaktadır.

5. Siber ortamda yargılama yetkilerinin belirsizliği

Gerçek dünyada, her adli makamın yargılama yetkisi dâhilinde olan bölge coğrafi sınırlarla belirlenmiş durumdadır. İnternet ortamının sınır tanımayan küresel yapısı gereği, siber suçlar yargılama yetkileri birbirinden farklı alanlarla sınırlı olan pek çok adli makamı ilgilendirebilmektedir. Bu tür durumlarda, suçu oluşturan eylemleri hangi adli makamın soruşturacağı ve cezalandıracağı hususunda belirsizlik ve karmaşa yaşanmaktadır.

6. Siber saldırganların iadesinde yaşanan güçlükler

Yurtdışında bulunan herhangi bir suçlunun ülkesine iadesi için;

1. İşlenen fiilin, her iki ülkenin ceza mevzuatında da suç olarak kabul edilmiş olması (Doctrine of Dual Criminality) ve
2. İşlenen fiilin, iki ülke arasında suçluların iadesine yönelik olarak kabul edilmiş olan bir anlaşmada suç olarak kabul edilmiş olması

gerekmektedir.

Günümüzde, birçok ülke siber suçlara ilişkin yasal düzenlemelerini tamamlamamış olduğu için 1. şartı, ülkeler arasındaki suçluların iadesine yönelik anlaşmalar siber suçların gelişiminden çok önce imzalanmış olduğu için de 2. şartı sağlamak çok güçtür [37].

4.3.1.2. Hedefler

Siber güvenliğin yasal boyutunda yaşanan güçlüklerin azaltılması, soruşturma ve kovuşturmanın etkinliğinin sağlanabilmesi amacıyla yapılması gereken çalışmalar aşağıda belirtilmektedir.

1. Yasal boşluklar giderilmelidir.
2. Usule ilişkin yasal eksiklikler ortadan kaldırılmalıdır.
3. Siber ortamda koruma ve gözetme yetkileri belirlenmelidir.
4. Kolluk kuvvetlerinin ve adli personelin teknik uzmanlığı arttırılmalıdır.
5. Siber ortamda yargılama yetkileri belirlenmelidir.
6. Ülkemiz ve diğer ülkeler arasında siber saldırganların iadesine ilişkin uzlaşma usulleri belirlenmelidir.

4.3.2. Teknik ve işlevsel tedbirlerin alınması

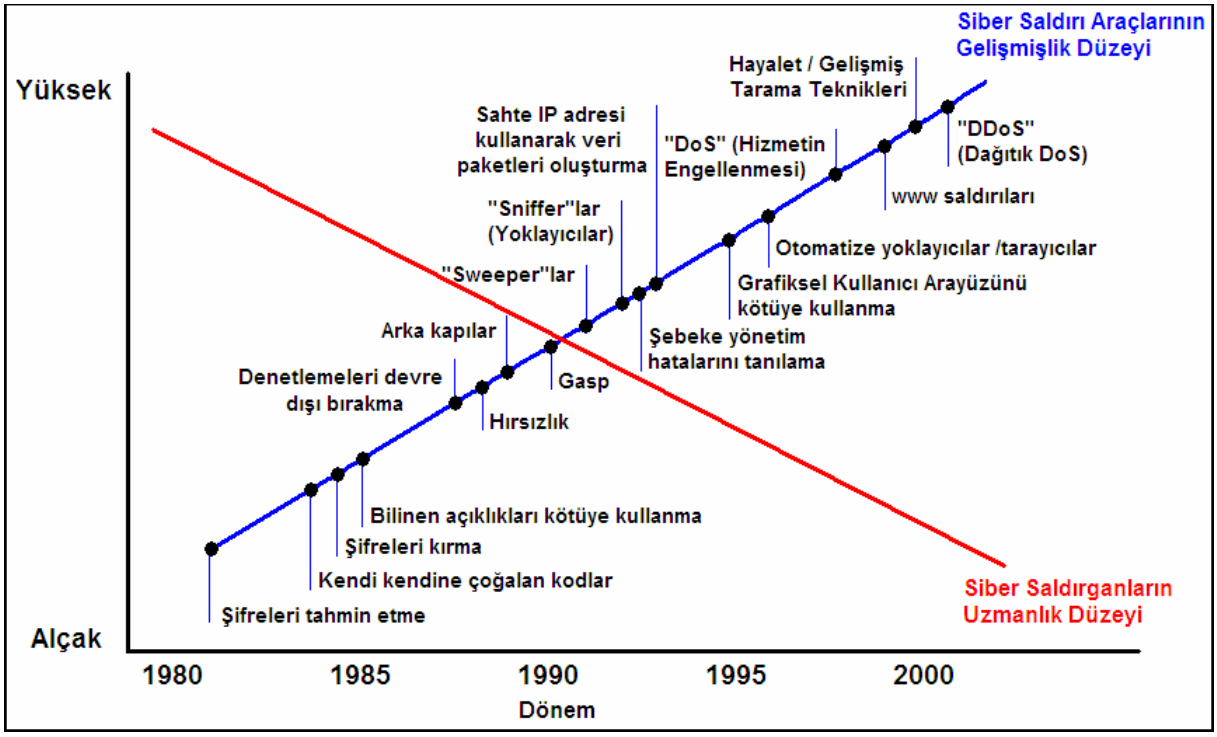
4.3.2.1. Mevcut durum

Geçmişte, BİT ile birbirine bağlanmamış olan şebekelerin güvenliğini sağlamak için, fiziksel güvenlik tedbirlerinin alınması yeterli olurken; günümüzde BİT' in gelişimi ile birbirine bağlanan şebekelerin sınırlarının belirsizleşmesi, taşınabilir cihazların kolaylıkla şebekelere dâhil olup ayrılabilmesi, farklı güvenlik seviyelerine sahip şebekelerin birbirlerine bağlanması ve şebekelerin çok çeşitli kullanıcı sınıfları tarafından kullanılması gibi hususlar siber güvenliğin sağlanmasını güçleştirmektedir. Siber saldırılar incelendiğinde, saldırı araçlarının kapsamı ve etkisi arttığı halde, siber

[37] y.a.g.e.

saldırganların bu saldırıları düzenlemek için ihtiyaç duydukları bilgi ve uzmanlık düzeyinin giderek azalmakta olduğu görülmektedir. (Şekil 4.2)

Şekil 4.2. Siber Saldırgan Bilgi Düzeyi – Siber Saldırı Gelişmişliği



Kaynak: Carnegie Mellon Üniversitesi, 2002

Dolayısıyla, siber saldırıların hazırlanması gün geçtikçe kolaylaşmakta ve sayıları artmaktadır. Ayrıca, saldırılar uygulama yazılımlarını olduğu kadar, aygıt yazımlarını da hedef alır duruma gelmiştir.

BİS'lerin güvenliğini sağlamak amacıyla pek çok değişik teknoloji kullanılmaktadır. Kurumsal sistemler genellikle güvenlik duvarları, dıştan içe saldırı tespit sistemleri ve erişim denetimi ile korunurken, içten dışa saldırı tespit sistemlerinin de kullanımı giderek yaygınlaşmaktadır. Şebekeler arasında taşınan verilerin bütünlüğünü ve gizliliğini sağlamak amacıyla da kimlik doğrulama ve trafik verilerinin şifrelenmesi tercih edilmektedir. Sunucu güvenliği için fiziksel ayrım, 24 saat izleme, konfigürasyon yönetimi gibi yöntemler ve anti-virüs yazılımlarına başvurulurken, istemci güvenliğinde kişisel güvenlik duvarları, anti-virüs ve anti-spyware araçları tercih edilmektedir. Siber güvenlik konusunda kayda değer başarılar elde edilmesine karşın, bu yöntemlerin etkinliği aşağıdaki gelişmeler karşısında yetersiz kalmaktadır:

- Birbirine bağlı, milyonlarca kullanıcı tarafından erişilebilen, üzerinde çok çeşitli işlemler yapılabilen şebekelerin giderek artması
- Mobil şebekelerin yaygınlaşması ve mobil cihazlarda taşınan kişisel bilgilerin artması
- Kullanılabilirlik ve güvenlik arasında bir denge kurulması gerekliliği
- Siber suçluların "sosyal mühendislik" gibi yöntemlerle birçok güvenlik stratejisini aşabilmeleri
- Yeni Nesil Şebekelerin (YNŞ) kullanımının yaygınlaşması
- Kurumsal şebekeler arasında veya farklı coğrafi alanlara yayılmış sistemlerin güvenlik seviyeleri arasında ciddi farklar bulunması [38].

4.3.2.2. Hedefler

Etkin siber güvenlik tedbirleri sadece saldırı tespit ve hasarları iyileştirme ile veya bunlara ilişkin yerel tedbirlerle sınırlı kalmamalı, farklı şebeke ve altyapı türleri, sunucular, istemciler, uygulamalar, hizmetler ve kullanıcılara hitap eden kapsamlı bir yaklaşım ile ele alınmalıdır. Siber güvenliğin nihai amacı, gelişmiş teknolojiler ve süreçler kullanarak, siber tehditlerin taşıdığı riskleri kabul edilebilir seviyelere çekmek ve güvenlik tedbirlerini mümkün olan en verimli ve en etkin hale getirmektir [39]. Siber güvenliğin teknik boyutunda gözlenen eksikliklerin azaltılması, teknik çözümlerin etkinliğinin sağlanabilmesi amacıyla yapılması gereken çalışmalar aşağıda belirtilmektedir.

1. Güvenliği kanıtlanmış standartların ve teknik çözümlerin kullanılması

Siber güvenlik kavramı her ülkede farklı yorumlansa da, uluslar arası standartlar ile ortak yaklaşımlar oluşturulmaya çalışılmaktadır. Bu standartların başında gelen ISO/IEC 27001 ve 27002 (Bilgi Güvenliği Yönetim Sistemleri) standartları siber tehdit ve saldırılara müdahale edebilen ve kendini yenileyen bir bilgi güvenliği sisteminde

[38] y.a.g.e.
[39] y.a.g.e.

yer alması gereken bileşenleri tanımlamakta, bilgi güvenliğinin bir süreç olarak ele alınmasını ve sürecin planlama, uygulama, kontrol etme ve önlem alma adımlarından oluşan bir döngü şeklinde çalıştırılmasını önermektedir.

Ayrıca, ISO/IEC 15408 (Ortak Kriterler - Bilgi Teknolojileri Güvenliği için Değerlendirme Kriterleri) standardında, işletim sistemleri, güvenlik duvarları, anti-virüs yazılımları gibi ürün grupları güvenlikle ilgili bir takım fonksiyonel ve kalite gereksinimlerine göre değerlendirilmektedir. Ortak Kriterler, herhangi bir ürünün tamamen güvenli olduğunu garanti etmese de, daha gelişmiş bir güvenlik seviyesine sahip olmasını sağlamaktadır.

2. Kurum ve kuruluşların bazı teknik ve işlevsel tedbirleri almalarının teşvik edilmesi

BİŞ'de güvenlik bileşenlerinin dışsallaştırılması, güvenlik fonksiyonlarının merkezileşmesi, birlikte çalışılabilirlik yeteneklerini arttıran açık standartların kullanımının yaygınlaşması, kişisel bilgisayarlar ve mobil cihazlarda saklanan kritik ve hassas bilgi miktarının artması gibi eğilimler göz önünde bulundurularak, teşvik edilmesi gereken tedbirler şunlardır [40]:

- Siber güvenlik olaylarının güvenilir şekilde raporlanması

- Gerçekçi ve uygulanabilir acil durum yönetimi planları hazırlanması

- Daha sağlam ve dinamik şifreler, çok parametreli kimlik doğrulama, denetim ve cihaz kimlik doğrulaması ile desteklenen kullanıcı kimlik doğrulaması uygulanması

- Tekrarlanan istemler gönderen blok cihazların tespiti ve bunlardan gelen istemlerin reddedilmesi

[40] y.a.g.e.

- Anti-virüs ve anti-spyware sistemlerinin düzenli olarak güncellenmesi, yetkisiz konfigürasyon değişikliklerine duyarlı donanım sistemlerinin kullanılması

- Güvenlik duvarı ve dıştan içe saldırı tespit sistemleri kullanılması, sistemlerin sürekli izlenmesi ve denetlenmesi, sistemlerin sadece belli güvenlik düzeyine sahip olan kısımlarının İnternete açılması

- Yeni teknolojilere ilişkin yeterli düzeyde kullanıcı eğitimi verilmesi

3. Farklı güvenlik seviyelerine sahip BİŞ arasındaki farkın kapatılması

Kamu ve özel sektör şebekelerinin ve sıklıkla etkileşimde bulunan diğer şebekelerin güvenlik seviyeleri arasındaki farkların mümkün olduğunca kapatılması ve tüm İnternet kullanıcılarına daha güvenli bir siber ortam sunulmasına yönelik çalışmalar yapılmalıdır.

4. Şebekelerde veya sistemlerde bulunan açıklıkların kamuoyuna açıklanması, incelenmesi ve iyileştirilmesi esnasında belli bir sorumluluk bilinci ve etik anlayışı içinde hareket edilmesi [41]

Her teknolojik çözümün güvenlik açıkları olduğu göz önünde bulundurulmalı, herhangi bir üründe tespit edilen bir güvenlik açığının, önce bu ürünün üreticisine bildirilmesi ve bu açığın kamuoyuna ifşa edilmeden önce düzeltilebilmesi için üreticiye bir fırsat tanınması sağlanarak, gereksiz kaos yaratılmaması ve son kullanıcıların üreticinin sunduğu bir takım eklentilerle bu açıktan asgari düzeyde etkilenmeleri sağlanmalıdır.

5. Güvenlik çözümleri üreticilerinin işbirliği içinde çalışması

[41] y.a.g.e.

Günümüzde siber saldırılar uygulama yazılımlarını olduğu kadar, aygıt yazımlarını da hedef alır hale gelmiştir. Dolayısıyla, çok katmanlı güvenlik sunan siber güvenlik çözümlerine ihtiyaç duyulmaktadır. Bu sebeple, farklı şebeke katmanlarına yönelik çözümler üreten üreticilerin işbirliği içinde çalışmaları teşvik edilmelidir.

4.3.3. Kurumsal yapılanmanın oluşturulması

4.3.3.1. Mevcut durum

Çeşitli ülkelerin siber güvenlik yapılanmaları incelendiğinde, siber güvenliği sağlamak amacıyla bazılarının yeni kurumlar oluşturduğu, bazılarının ise mevcut kurumların görev alanını genişlettiği, oluşturulan veya görev alanı genişletilen kurumların daimi komiteler, çalışma grupları, danışma kurulları, disiplinler arası merkezler gibi çok çeşitli yapılara sahip oldukları görülmektedir. Bazı ülkeler ulusal izleme, uyarı ve olaylara müdahale birimleri kurmuş ve siber saldırılara müdahale faaliyetlerini koordine etmek üzere gereken kurumsal yapıları oluşturmuş durumdadırlar.

Ayrıca, bazı uluslar arası kuruluşlar bünyesinde siber güvenliğin sağlanması ile ilgili merkezler oluşturulmuş durumdadır. Örneğin, ulusal emniyet teşkilatları arasında uluslar arası işbirliğini amaçlayan Interpol bünyesinde siber suçların soruşturulmasında gereken uluslar arası yazışmalarda yaşanabilecek gecikmelerin elektronik delillerin kaybına yol açmasını engellemek amacıyla ülkelerin doğrudan başvurabilecekleri I-24/7 sistemi oluşturulmuş ve Ulusal Merkezi Referans Noktaları belirlenmiştir. NATO da Estonya'daki siber saldırıların ardından 2008 yılında siber saldırılara karşı savunma konusunda bir araştırma merkezi kurarak, tüm üye ülkelerden bu merkez için birer Ulusal Temas Noktası bildirmelerini talep etmiştir. Avrupa Konseyi Siber Suç Sözleşmesine taraf olan ülkeler de kendi 7 gün 24 saat erişilebilir temas noktalarını oluşturmakla yükümlüdürler.

Avrupa Birliği'ne bağlı bölgesel bir kuruluş olan Avrupa Şebeke ve Bilgi Güvenliği Ajansı (ENISA)[42] da Avrupa Birliği kuruluşlarına ve üye ülkelere siber güvenlik konusunda tavsiyelerde bulunma, veri analizi yapma, farkındalığın arttırılmasını ve

[42] http://www.enisa.europa.eu/

işbirliğini destekleme gibi hizmetler sunan bir uzmanlık kuruluşudur. ENISA Yönetim Kurulunda yer alan ülke temsilcilerinin unvanları Tablo 4.1' de sunulmaktadır.

Tablo 4.1. ENISA Yönetim Kurulu Üyeleri

AB Üyesi Ülke Temsilcileri	
Almanya	İçişleri Bakanlığı BT Dairesi – Başkan Vekili
Belçika	Posta Hizmetleri ve Telekomünikasyon Kurumu – Kurul Üyesi
Bulgaristan	Bilgi Teknolojileri ve İletişim Kurumu – Başkan Vekili
Çek Cumhuriyeti	İçişleri Bakanlığı e-Devlet Projesi ve Hizmet Geliştirme Birimi – Başkan
Danimarka	Bilgi Teknolojileri ve Telekomünikasyon Kurumu – Daire Başkanı
Estonya	Mali İşler ve İletişim Bakanlığı – BT Danışmanı
Finlandiya	Ulaştırma ve İletişim Bakanlığı – Bakanlık Danışmanı
Fransa	Bilgi Sistemleri Güvenliği Başkanlığı – Direktör
Güney Kıbrıs	Elektronik Haberleşme ve Posta Hizmetleri Düzenleme Kurumu – Uzman
Hollanda	Mali İşler Bakanlığı Enerji ve Telekomünikasyon Genel Müdürlüğü –Politika Danışmanı
İngiltere	Bilgi Güvenliği Politikaları Ekibi – Başkan
İrlanda	İletişim Bakanlığı – Telekomünikasyon Danışmanı
İspanya	Telekomünikasyon ve Bilgi Toplumu Müsteşarlığı – Bilgi Toplumu Hizmetleri Müdür Vekili
İsveç	Enerji ve İletişim Bakanlığı – Daire Başkanı
İtalya	Ekonomik Kalkınma Bakanlığı – Genel Müdür
Latviya	Ulaştırma Bakanlığı İletişim Dairesi – Başkan
Litvanya	Ulaştırma ve İletişim Bakanlığı Müsteşarlığı
Lüksemburg	Maliye Bakanlığı
Malta	Altyapı, Ulaştırma ve İletişim Bakanlığı – Bilgi ve İletişim Teknolojileri Politikası Yöneticisi

Polonya	Araştırma ve Akademik Bilgisayar Ağı – Teknik Müdür
Portekiz	Ulusal Bilgisayar Bilimleri Enstitüsü – Yönetim Kurulu Başkanı
Romanya	İletişim ve Bilgi Teknolojileri Bakanlığı – Bilgi Teknolojileri Genel Müdürü
Slovakya	Maliye Bakanlığı Bilgi Toplumu Dairesi
Slovenya	ARNES CI-CERT – Başkan
Yunanistan	Bilgisayar Bilimleri Enstitüsü Araştırma ve Geliştirme Birimi – Direktör
Avrupa Ekonomik Alanı Ülke Temsilcileri (Gözlemciler)	
İzlanda	Posta ve Telekomünikasyon Kurumu – Hukuk Müşaviri
Lihtenştayn	İletişim Kurumu – Direktör
Norveç	Ulaştırma ve İletişim Bakanlığı Sivil Havacılık, Posta Hizmetleri ve Telekomünikasyon Genel Müdürlüğü – Genel Müdür Vekili

Kaynak: http://www.enisa.europa.eu/pages/03_02_view_all_representatives.htm#4

Ülkemizde, hâlihazırda siber güvenlik konusunda yasal olarak yetkilendirilmiş bir kurum veya kuruluş bulunmamaktadır. Bununla birlikte, 2006-2010 Bilgi Toplumu Stratejisi Eylem Planının 88. Maddesine binaen TÜBİTAK UEKAE tarafından TR-BOME[43] adlı bir ulusal Bilgisayar Olaylarına Müdahale Ekibi (BOME) oluşturulması çalışmaları yapılmaktadır. Ayrıca, TÜBİTAK ULAKBİM tarafından ulusal akademik ağ kapsamında Ulak-CSIRT[44] adıyla kurulmuş bir BOME de mevcuttur. Her iki BOME de ENISA tarafından akredite edilmiş durumdadır. ENISA tarafından akredite edilen veya akreditasyon süreci devam eden tüm BOME'lerin listesi EK-3'te sunulmaktadır.

4.3.3.2. Hedefler

Siber tehditlerle mücadele için etkin kurumsal yapılar oluşturmak ve konuyla ilgili mevcut ve yeni girişimler arasında koordinasyon sağlamayı amaçlayan birimleri tesis

[43] http://www.tr-cert.gov.tr
[44] http://csirt.ulakbim.gov.tr/

etmek son derece önemlidir. Bu bağlamda gerçekleştirilmesi gereken çalışmalar şunlardır:

1. Kamu - Özel Sektör - Üniversite - Sivil Toplum işbirliği modelinin oluşturulması

Tek başına kamunun veya özel sektörün çabalarının siber ortam güvenliğini sağlamakta yetersiz kalacağı aşikârdır. Dolayısıyla, kurumsal yapılanma oluştururken tüm paydaşları kapsayan bir işbirliği modeli benimsenmelidir.

Kamu sektörü; özel sektör ve vatandaşların çıkarları, yasal mevzuat, standartlar ve kamusal farkındalık gibi hususlarda bir denge unsurudur. Hukukun ve düzenin kendi yetki sınırları dahilinde korunmasından sorumludur ve BİT' in kullanımında güven ve güvenliğin tesis edilmesinde lider rolü üstlenerek, ulusal bilgi toplumuna dönüşümü desteklemelidir [45].

Özel sektör; siber saldırılarla mücadele konusunda edinmiş olduğu uzmanlık ve tecrübe ile teknik çözümler üzerine araştırma ve geliştirme yeteneği sayesinde siber güvenlik konusunda önemli bir rol oynamaktadır. Uygun maliyetli güvenlik teknolojilerinin geliştirilmesi, sistemlerde bulunan açıklıkların azaltılmasını amaçlayan tedbirlerin alınması hususlarında öncülük yapmalıdır [46].

Üniversiteler; siber güvenlik konusunda araştırmaları desteklemek, yeni fikirler ve teknolojilere dayalı çözümler geliştirmek, kamu - özel sektör - üniversite işbirliğine dayalı projelerde yer almak, konferanslara ev sahipliği yapmak ve son gelişmeler hakkında bilgi alışverişini sağlayan makaleler yayımlamak suretiyle siber güvenliğe katkıda bulunmalıdır [47].

Sivil Toplum Kuruluşları (STKlar); vatandaşların büyük bir güvenlik zincirinin parçaları olduklarının farkında olmalarına yardımcı olmalıdır. Kullanıcıların kendi güvenliklerini ve değerlerini korumak için siber ortamda doğru ve etik davranışlar sergilemeleri,

[45] ITU, 2008 (2), a.g.e.
[46] y.a.g.e.
[47] y.a.g.e.

güvenlik araçları kullanmaları, düzenli virüs güncellemeleri yapmaları ve güvenlik uyarılarını izlemeleri gibi sorumlulukları yerine getirmelerini teşvik etmelidir. Tüketicinin korunmasında ve siber güvenlik konusunda farkındalık oluşturulmasında sivil toplumun rolü yadsınamaz [48].

2. Ulusal Siber Güvenlik Otoritesi oluşturulması

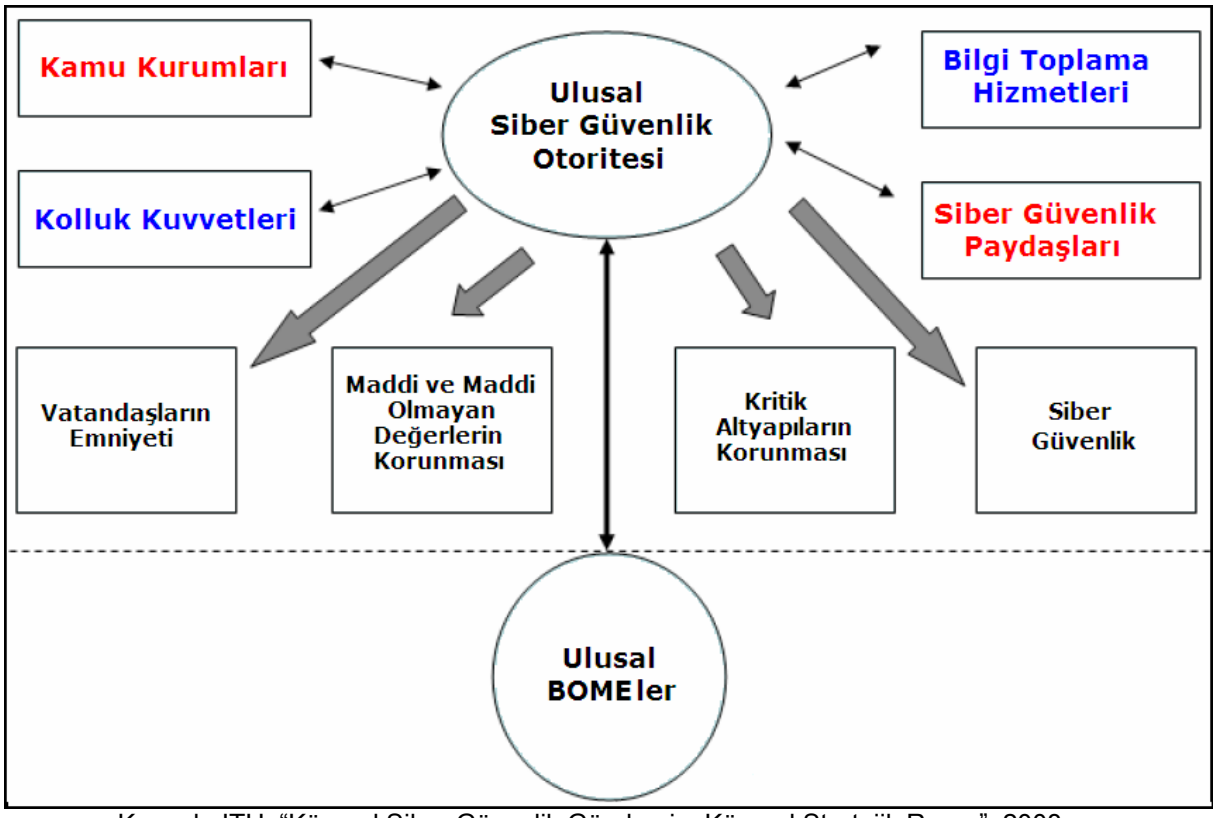
Siber güvenlikten sorumlu olmak üzere Ulusal Siber Güvenlik Otoritesi (USGO) kurulmalı veya mevcut kamu kurumları arasında bu görevi yerine getirebilmeye en yetkin kuruma bu görev verilmelidir. Ulusal Siber Güvenlik Otoritesi, ulusal siber güvenlik politikasının yönetiminin ve bölgesel ve uluslar arası işbirliğinin tek elden koordine edilmesini sağlamalıdır. Politika ve stratejinin belirlenmesini ve uygulanmasını birbirinden ayırabilmek için, Ulusal Siber Güvenlik Otoritesi müdahalelerden uzak, bağımsız bir konumda bulunmalıdır. USGO;

- Ulusal siber güvenlik politikasının tanımlanması,
- Ulusal siber güvenlik girişimleri için önceliklerin belirlenmesi,
- Siber güvenlik faaliyetlerinin ulusal seviyede koordine edilmesi,
- Siber güvenlik sorunlarını ele almak üzere paydaşların ve kamu-özel sektör ilişkilerinin belirlenmesi,
- Bölgesel ve uluslar arası taraf, kurum ve kuruluşlarla işbirliği yapılması,
- Kamuya ait BİS' in ve BİŞ' in izlenmesi ve risk değerlendirmesi yapılması,
- Siber güvenlik ile ilgili uluslar arası standartların uygulanması,
- Bilgi ve iletişim altyapılarının, hizmetlerinin veya işletmecilerinin sertifikasyonu,

[48] y.a.g.e.

- Sayısal kimlik sistemlerinin işletilmesi, geliştirilmesi ve yönetilmesi gibi hususlarda lider rolü üstlenmelidir [49]. (Şekil 4.3)

Şekil 4.3. Ulusal Siber Güvenlik Otoritesi



Kaynak: ITU, "Küresel Siber Güvenlik Gündemi – Küresel Stratejik Rapor", 2008

3. Ulusal BOME'lerin oluşturulması

BOME'ler, bilgisayar ve şebeke güvenliğini izleyen ve siber saldırı mağdurlarına olaylara müdahale hizmeti sunan teknik birimlerdir. BOMEler, açıklıklara ve tehditlere ilişkin uyarılar ve bilgisayar ve şebeke güvenliğini geliştirmeye yönelik bilgiler yayımlar; farkındalık oluşturma, güvenlik danışmanlığı gibi kalite hizmetleri ve teknolojiyi izleme, güvenlik araçları geliştirme gibi proaktif hizmetlerin yanı sıra, siber saldırılara karşı koyma ve bunların yol açtığı zararın azaltılması gibi reaktif hizmetler de sunarlar [50]. (Tablo 4.2)

[49] y.a.g.e.
[50] y.a.g.e.

Tablo 4.2. BOME'ler Tarafından Sunulan Hizmetler

Reaktif Hizmetler	Proaktif Hizmetler	Güvenlik Kalite Yönetimi Hizmetleri
– Uyarma – Saldırılara müdahale – Saldırı analizi – Açıklıklara müdahale – Açıklık analizi – Koordinasyon	– Bilgilendirme – Teknolojiyi izleme – Güvenlik denetimi ve değerlendirme – Güvenlik yönetimi – Güvenlik araçları geliştirme – Saldırı tespit hizmetleri	– Risk analizi – İş sürekliliği ve felaket kurtarma – Güvenlik danışmanlığı – Farkındalık oluşturma – Eğitim verme – Ürün değerlendirme veya belgelendirme

Kaynak: ITU, "Küresel Siber Güvenlik Gündemi – Küresel Stratejik Rapor", 2008

BOME'lerin görev ve sorumlulukları ülkeden ülkeye değişebilse de, tümünün ortak görevi en yeni tehditlere ilişkin güncel bilgiler sunmak ve ihtiyaç duyan paydaşlara siber saldırılarla mücadele konusunda teknik destek sağlamaktır.

BOME'ler;

- Yetki alanlarına giren bilgisayar güvenlik olaylarını engellemeye veya çözmeye çalışmalı,
- Tüm paydaşlar ile güvenilir ilişkiler kurarak saldırı ve açıklıkları izleme, tespit etme ve analiz etme aşamalarında onlarla birlikte etkin şekilde çalışmalı,
- Tüm paydaşları siber tehditler konusunda uyarmalı, siber saldırılara maruz kalan paydaşlara saldırı tespitinden çözümüne kadar gereken desteği sunmalı,

- Mevcut küresel veya bölgesel forumlara ve diğer girişimlere katılım sağlamalıdırlar[51].

Bu ekiplerin yaşaması muhtemel güçlükler tespit ve müdahale sistemlerinin ulusal çapta bilinirliğinin az olması veya kapasite olarak yetersiz olması dolayısıyla tespit aşamasından öteye gidememeleri olabilir. Bu güçlükleri aşmak için gereken tedbirler alınmalıdır [52]. BOMEler USGO ile ilişkili olmalı ve faaliyetleri USGO tarafından düzenlenmelidir.

4.3.4. Ulusal kapasitenin geliştirilmesi ve farkındalığın arttırılması

4.3.4.1. Mevcut durum

Siber güvenliğin sağlanması konusunda benimsenen genel yaklaşım gerek kamu sektöründe gerekse özel sektörde büyük ölçekli kurum ve kuruluşlarda risk yönetimi uygulamak ve mevcut riski azaltarak bu kurum ve kuruluşların BİT kaynaklarını korumak şeklindedir [53].

Ayrıca, siber güvenliğin öteden beri sadece teknik boyutta ele alınması ve teknik çözümler geliştirmeye öncelik verilmesi; yasal, idari, ekonomik ve sosyal boyutlarda siber güvenlik kapasitesinin geliştirilmesini engellemektedir.

Yasal boyutta; hem yasaların siber güvenliği bütünüyle ele alacak kadar kapsamlı olmadıkları, hem de kolluk kuvvetleri ve adli personelin siber güvenlik konusunda yeterli bilgi ve uzmanlık düzeyine sahip olmadıkları gözlenmektedir.

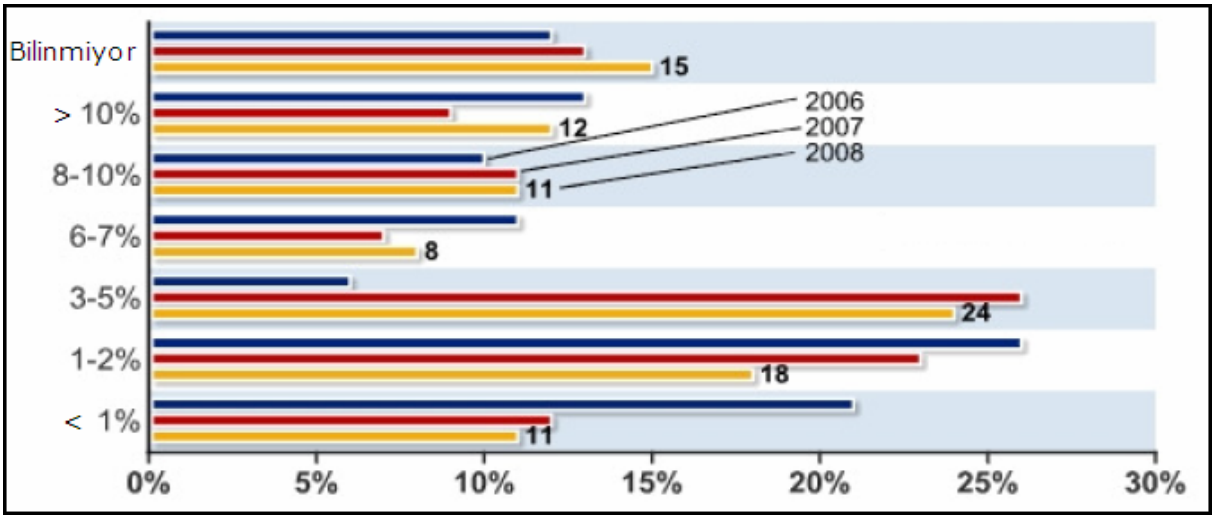
---

[51] y.a.g.e.
[52] y.a.g.e.
[53] y.a.g.e.

İdari boyutta; özellikle kamu yönetiminde yeterli bir siber güvenlik farkındalığı bulunmadığı ve siber güvenlik kapasitesinin gelişmemiş durumda olduğu değerlendirilmektedir.

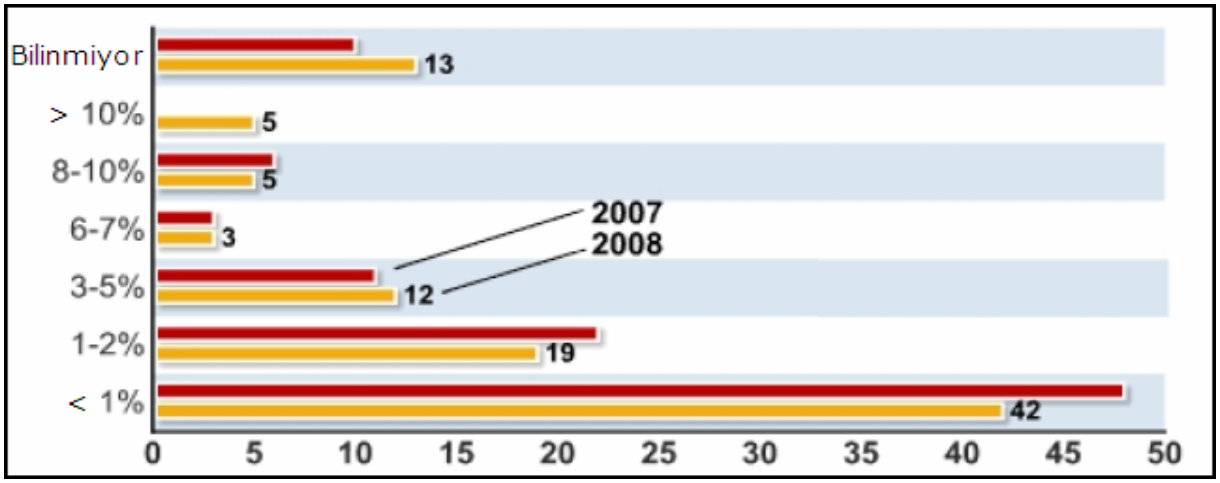
Ekonomik boyutta; siber güvenlik konusunda alınması gereken teknik tedbirlere ve farkındalık eğitimlerine yeterince kaynak ayrılmadığı görülmektedir. FBI tarafından yapılan CSI Bilişim Suçları ve Güvenlik Araştırmasının sonuçları Bilgi Teknolojileri (BT) bütçelerinin güvenliğe ayrılan kısmının ve güvenlik bütçelerinin farkındalık eğitimine ayrılan kısmının çok düşük düzeylerde olduğunu göstermektedir. (Şekil 4.4 ve Şekil 4.5)

Şekil 4.4. BT Bütçesinin Güvenliğe Ayrılan Kısmı



Kaynak: FBI, "CSI Bilişim Suçları ve Güvenlik Araştırması", 2008

Şekil 4.5. Güvenlik Bütçesinin Farkındalık Eğitimine Ayrılan Kısmı



Kaynak: FBI CSI Bilişim Suçları ve Güvenlik Araştırması 2008

Sosyal boyutta ise; İnternet kullanıcılarının çok farklı bilinç ve güvenlik farkındalığı düzeylerine sahip oldukları değerlendirilmektedir. Örneğin, kullanıcılar çoğu zaman siber tehditlere hedef olduklarının farkında bile olmadan güvenilir olmayan İnternet siteleri üzerinden kişisel bilgilerini paylaşabilmekte veya alışveriş yapabilmektedirler.

Kullanıcıların siber güvenlik farkındalığının yetersizliği, gerek itibar kaybı kaygısı, gerekse kolluk kuvvetleri ve yargının siber suçlar alanındaki uzmanlığından endişe duymaları dolayısıyla yaşadıkları siber güvenlik ihlallerini bildirmemeleri sebebiyle, sağlıklı siber saldırı istatistiklerine ulaşılamamasına neden olmaktadır. Oysaki gerek kolluk kuvvetleri ve adli merciler, gerekse USGO ve BOMEler kısıtlı kaynakları en acil ihtiyaçlara yönlendirmek amacıyla, siber saldırı istatistikleri ve siber saldırganların hareket tarzı gibi çeşitli bilgilerden yararlanmak durumundadırlar.

Ülkemizdeki durum incelendiğinde ise, ülkemizde İnternet kullanım oranlarının gelişmiş ülkelere göre oldukça düşük olduğu görülse de, yukarıda özetlenen genel sorunların ülkemiz için de geçerli olduğu gözlenmektedir. Dolayısıyla, ülkemizde de siber güvenlik konusunda ulusal kapasitenin geliştirilmesi ve farkındalığın arttırılmasına ihtiyaç duyulmaktadır.

4.3.4.2. Hedefler

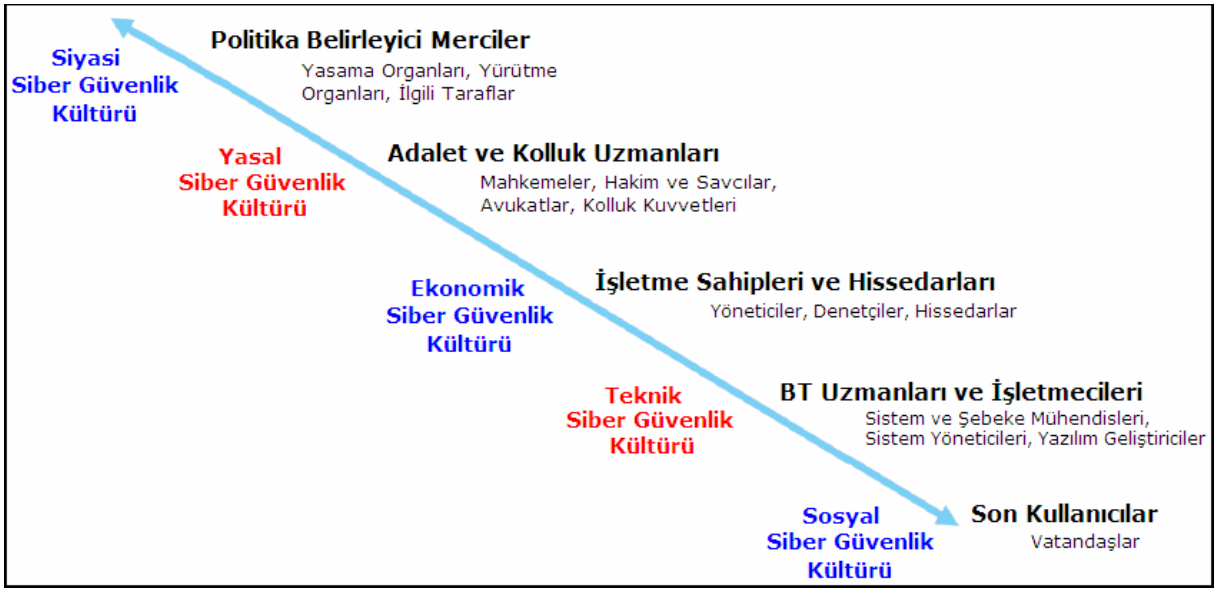
Siber güvenliği tesis etmek üzere kapasitenin geliştirilmesi ve farkındalığın arttırılması için yapılması gereken çalışmalar şunlardır:

1. Ulusal siber güvenlik kültürünün oluşturulması

Siber suçlarla mücadele edebilecek düzeyde siber güvenliğin sağlanması ancak İnternet kullanıcılarının bazı normlara gönüllü olarak uyduğu, siber güvenliği siyasi, yasal, ekonomik, teknik ve sosyal boyutları ile ele alan bir küresel siber güvenlik kültürünün oluşturulması ile mümkündür [54]. (Şekil 4.6)

[54] y.a.g.e.

Şekil 4.6. Siber Güvenlik Kültürü



Kaynak: ITU, "Küresel Siber Güvenlik Gündemi – Küresel Stratejik Rapor", 2008

Küresel siber güvenlik kültürünün oluşturulmasına dair yaklaşımlar ulusal düzeyde de benimsenerek ulusal siber güvenlik kültürü tesis edilmelidir. Bu hususta Birleşmiş Milletler Genel Kurulu'nun 57/239 sayılı Küresel Siber Güvenlik Kültürünün Oluşturulması üzerine kararından[55] ve OECD'nin Bilgi Sistemleri ve Şebekeleri için Güvenlik Kılavuzundan[56] yararlanılabilir.

2. Farkındalığın arttırılması

Farkındalığın arttırılması konusunda en önemli rol STKlara düşmekle birlikte, kamu kurum ve kuruluşlarının ve özel sektör kuruluşlarının da rolü yadsınamaz. Örneğin, Milli Eğitim Bakanlığı okul müfredatlarına siber ortamda güvenli davranışları öğreten dersler koyarak siber güvenlik farkındalığının oluşturulmasına katkıda bulunabilir. OECD tarafından yapılan bir çalışmada, ulusal düzeyde bir güvenlik kültürünün oluşturulmasına katkıda bulunan temel etkenlerin e-devlet uygulamalarının yaygınlaştırılması ve kritik bilgi altyapılarının korunması olduğu belirlenmiştir [57]. Özel sektör de çeşitli girişimlerde bulunabilir. Estonya'da finans ve elektronik haberleşme

[55] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[56] http://www.oecd.org/dataoecd/16/22/15582260.pdf

[57] ITU, 2008 (2), a.g.e.

sektörü işletmecileri 2009 itibarıyla en güvenli siber-ülke olma hedefiyle yola çıkarak bir farkındalık kampanyası başlatmışlar ve Açık Anahtar Altyapısı ve Sayısal Kimlik kullanılan bir takım projeler yürütmektedirler [58].

Farkındalığın arttırılmasına yönelik olarak yürütülmesi gereken çalışmalar şunlardır[59]:

- Güvenlik zincirinde en zayıf halkanın bireyler olduğu göz önüne alınarak, sadece büyük ölçekli kurum ve kuruluşların değil, bireylerin ve küçük ve orta ölçekli kuruluşların da güvenlik ihtiyaçlarının karşılanması
- BİS ve BİŞ kullanıcılarına yönelik siber güvenlik farkındalığı programları sunulması
- Özel şirketlerde güvenlik kültürü geliştirilmesinin teşvik edilmesi (Devlet tarafından İnternet üzerinden veya diğer yollarla bilgilendirme yapılması, şirketlere kendilerini değerlendirebilecekleri araçlar sunulması, güvenli sistemlerinin arttırılması amacıyla mali destek sağlanması veya vergi indiriminde bulunulması gibi)
- Sivil topluma yönelik destek programları sunulması (Ebeveynlere yönelik dersler, eğitimcilere yönelik destek malzemeleri, çocuklara yönelik gelişim kitapları veya oyunlar gibi)
- Kapsamlı bir ulusal farkındalık programının tesis edilmesi (Kamu personelinin eğitilmesi, yaygın kabul gören güvenlik sertifikasyonlarının alınması gibi)
- İnternet kullanıcılarının kişisel mahremiyet ve siber ortamdaki kimliğin sınırları hakkında eğitilmesi
- Siber saldırılarla ilgili daha sağlıklı istatistiklerin toplanabilmesi amacıyla İnternet kullanıcılarının siber tehditlere ilişkin farkındalığının arttırılması

[58] y.a.g.e.
[59] y.a.g.e.

Farkındalık kampanyaları, siber suçları ele alan güçlü yasalar ve gelişmiş teknik ve işlevsel tedbirler, suçlular tarafından algılanan riski ve siber suç işlemek için gereken çabayı arttırmak ve siber suçlardan elde edilen maddi menfaati azaltmak suretiyle caydırıcılık oluşturmaya, suçların daha etkin şekilde soruşturulmasına ve kovuşturulmasına yardımcı olurlar. Farkındalığın arttırılması aynı zamanda BİS' de bulunan açıklıkların ve siber saldırılara hedef olabilecek BİS oranının da azaltılmasına katkıda bulunur [60].

3. Ulusal kapasitenin geliştirilmesi

Siber güvenlik konusunda ulusal kapasitenin geliştirilmesi için alınması gereken tedbirler, BİS'e yönelik tehditleri etkin şekilde analiz etmeyi gerektiren proaktif faaliyetler, bunları tamamlayan teknik, idari ve yasal tedbirler ile etkin ulusal, bölgesel ve uluslar arası işbirliğidir. (Şekil 4.7)

Şekil 4.7. Kapasitenin Geliştirilmesi

Kaynak: ITU, "Küresel Siber Güvenlik Gündemi – Küresel Stratejik Rapor", 2008

[60] y.a.g.e.

Ulusal kapasitenin geliştirilmesi amacıyla yürütülmesi gereken çalışmalar şunlardır [61]:

- Kamudaki karar verici merciler, adli merciler, kolluk kuvvetleri ve özel sektörde yer alan BİT üreticilerinin ve hizmet sağlayıcılarının siber güvenlik konusunda eğitim, bilinç düzeyi, teknik ve idari yetkinliklerinin arttırılması

- Siber güvenlik konusunda bilim ve teknoloji, araştırma ve geliştirme programları ve projeleri geliştirilmesi

- BİT yazılımlarının ve donanımlarının güvenlik kapasitelerinin güçlendirilmesi

- Kritik bilgi ve altyapılar başta olmak üzere kamuya ait BİS için bir siber güvenlik planı (risk yönetimi, acil durum yönetimi, bilgi paylaşımı, kamu BİS kullanıcılarının eğitimi ile güvenlik eğitimi konusunda kamu, özel sektör ve sivil toplum arasında işbirliği hususlarında yol haritası) oluşturulması

- Siber güvenlik ile ilgili olaylara medyada yer verilmesinin sağlanması

- Siber güvenlik uzmanları arasında bilgi alışverişine imkan veren eğitim programları, çalıştaylar, konferanslar, toplantılar gibi etkinliklerin düzenlenmesi

- Siber güvenlik politikasını belirleyen merciler tarafından;

[61] y.a.g.e.

- Gerektiğinde kamu - özel sektör - üniversite - sivil toplum ortaklıkları oluşturulması,
- Farklı kanallardan siber ortamda güvenli davranışlara ilişkin mesajlar verilmesi,
- Ulusal düzeyde uygulanabilir ve uluslar arası mevzuatla uyumlu etkin bir yasal mevzuat oluşturulması,
- Gereken her türlü teknik ve işlevsel siber güvenlik tedbirinin alınması,
- Gereken kurumsal yapılanmanın sağlaması,
- Ulusal, bölgesel ve uluslar arası işbirliğinin desteklenmesi,
- Bilgi toplumunun tüm paydaşlarının eğitilmesi,
- BİT ve güvenlik araçları üreticilerine ürünlerini kapsamlı ve eğitimsiz kullanıcılar tarafından bile anlaşılır şekilde belgeleme yükümlülüğü getirilmesi.

4.3.5. Uluslararası işbirliğinin sağlanması

4.3.5.1. Mevcut durum

Siber ortamda koruma, gözetme ve yargılama yetkilerinin belirsizliği ile siber suçların pek çok ülke mevzuatında suç olarak tanımlanmamış oluşu nedeniyle siber saldırganların lehine oluşan güvenli sığınaklar, yurtdışından delil toplama esnasında yaşanan gecikmeler, yurtdışında bulunan suçluların iadesinde yaşanan güçlükler gibi sorunlar, ulusal siber güvenliğin sağlanması hususunda uluslar arası işbirliğinin olmazsa olmaz önemde olduğunu göstermektedir.

Ayrıca, siber alem olarak nitelenen İnternetin sınır tanımayan küresel yapısı ve meydana getirdiği küresel bağlantılılık, siber saldırganlara bulundukları ülke dışında bulunan herhangi bir BİS veya BİŞ üzerinden de suç işleyebilme imkanı sunmaktadır.

Siber suçlar, çoğunlukla büyük maddi menfaatler elde eden organize suç örgütleri tarafından işlenmekte olup, bu örgütlerin pek çok ülkeyle bağlantısı olabilmektedir. Zira İnternet başta olmak üzere BİŞ farklı ülkelerdeki ve kıtalardaki siber saldırganlara birbirleriyle iletişim kurma, bilgi paylaşma, propaganda yapma, yeni üyeler kazanma gibi fırsatlar sunmaktadır. Tüm bu güçlükler, siber suçlarla mücadele konusunda uluslararası işbirliğine duyulan ihtiyacı attırmaktadır.

Hâlihazırda, siber güvenlik konusunda yürütülen bölgesel ve uluslararası girişimlerin listesi EK-2'de sunulmaktadır.

4.3.5.2. Hedefler

BM bünyesinde ilk aşaması Aralık 2003'te İsviçre'de, ikinci aşaması ise Kasım 2005'te Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesinde (DBTZ) BİT' in kullanımında güven ve güvenliğin küresel bilgi toplumunun yapıtaşları arasında olduğu kabul edilmiştir. Siber güvenlik, bilgi güvenliği ve şebeke güvenliği konusunda yaşanan küresel çaptaki sorunlar ancak temel paydaşları kapsayan uluslar arası bir işbirliği stratejisi ve siber güvenlik kültürü ile ele alınabilir. Söz konusu strateji ve kültürün teşkil edilebilmesi amacıyla yürütülmesi gereken çalışmalar şunlardır:

1. Bölgesel işbirliğinin sağlanması

Hâlihazırda, Avrupa Birliği, Avrupa Konseyi, G8, APEC, OAS, ASEAN, Arap Birliği, Afrika Birliği gibi bölgesel kuruluşlar bünyesinde gerçekleştirilen çalışmalardan elde edilen en iyi uygulamalar analiz edilerek ülkemize uyarlanmalıdır. Ülkemiz bu bölgesel kuruluşlardan ilgili olanlarının çalışmalarına aktif olarak katılmalı, katılmadıklarını izleyerek işbirliği imkânlarını araştırmalıdır.

Bu bağlamda ülkemiz öncelikli ve ivedi olarak Avrupa Konseyi Siber Suç Sözleşmesine taraf olmalıdır.

2. Uluslararası işbirliğinin sağlanması

Pek çok ülkeyi aynı anda etkileyebilen siber suçlarla mücadele edebilmek için uluslararası diyalog ve işbirliğine duyulan ihtiyaç yadsınamaz durumdadır. Siber güvenlik konusunda ülkemizin uluslar arası girişimlerde proaktif rol alması, diğer ülkeler ile bilgi ve en iyi uygulama paylaşımında bulunması, araştırma ve eğitim faaliyetlerine katılması sağlanmalıdır.

DBTZ sonucunda tüm ülkelerin mutabakatıyla "BİT'in kullanımında güven ve güvenliği tesis etmek" konusunda ITU küresel koordinatör olarak belirlenmiştir. Bu itibarla ITU'nun siber güvenlik konusundaki tüm çalışmalarının izlenmesi, bu çalışmalara katılım ve katkı sağlanması gerekmektedir.

5 SONUÇ

Günümüzde ekonomik, sosyal, kültürel ve siyasi açıdan gücü temsil eden bilginin çok hızlı ve düşük maliyetle saklanabilmesini, işlenebilmesini ve dağıtılabilmesini sağlayan İnternet başta olmak üzere BİT hızla gelişmektedir. Söz konusu gelişim bir yandan hayatı kolaylaştıran yeni araçlar ve iş yapma süreçleri sunarken, diğer yandan hayatı zorlaştıran pek çok siber tehdidin oluşumuna da zemin hazırlamaktadır. Bu bağlamda, gerek siber ortamda hızla artan tehditlerle mücadeleyi, gerekse BİT'lere giderek artan derecede bağımlı hale gelen kritik altyapıların korunmasını amaçlayan siber güvenliğin sağlanması konusu tüm dünyanın gündemine girmiştir.

Bu gelişme doğrultusunda, BM, OECD, ITU, AB, AK gibi bölgesel ve uluslar arası kuruluşlar küresel siber güvenlik kültürünün oluşturulması ve siber güvenlik konusunda ortak bir anlayışın benimsenmesi amacıyla çeşitli girişimlerde bulunmakta; toplantılar, seminerler, konferanslar, çalıştaylar gibi etkinlikler düzenlemekte ve politika/strateji belgeleri ile kılavuzlar yayınlamaktadırlar. Bu kuruluşların çalışmalarından da yararlanarak pek çok gelişmiş ve gelişmekte olan ülke siber güvenliğin sağlanmasını ve kritik bilgi ve altyapıların korunmasını teminen önemli adımlar atmışlar; birçok ülke de bu konuda çalışmalarına devam etmektedirler.

Ülkemiz gelişmekte olan ülkelerin önde gelenlerinden olmasına rağmen ne yazık ki siber güvenlik konusunda iyi bir durumda değildir. Ülkemizin siber güvenlik konusunda yasal, teknik ve idari açılardan pek çok eksikliği bulunmaktadır. Ülkemizin siber tehditlerin ve saldırıların önemli kaynaklarından olması ve bunlardan gördüğü zararın sürekli artması da mevcut durumun olumsuzluğunu teyit etmektedir. Söz konusu eksikliklerin giderilebilmesini teminen, mevcut bölgesel ve uluslar arası kuruluşlar ile gelişmiş ülke uygulamalarından ve Başbakanlığın inisiyatifiyle hazırlanan Ulusal Sanal Ortam Güvenlik Politikası belgesinden yararlanmak suretiyle siber güvenlik konusunda atılacak ulusal adımlar belirlenmelidir. Bu bağlamda,

öncelikle ülkemizde siber güvenlik konusunda mevcut bulunan yasal boşluğun giderilmesini teminen kişisel verilerin korunması ve ulusal bilgi güvenliği konuları başta olmak üzere gerekli kanunlar süratle yasalaştırılmalıdır. Bu yasalarla USGO, görev ve sorumlulukları ile çalışma usul ve esasları belirlenmelidir. USGO, kişisel, kurumsal ve ulusal ölçekte siber güvenliğin sağlanması için gerekli düzenlemeler, standartlar, rehberler ve kılavuzları hazırlamalı veya hazırlanmasına öncülük etmelidir. Siber güvenliğin sağlanması noktasında farkındalığın oluşturulması büyük önem taşımaktadır. Bu itibarla, Ulusal Farkındalık Oluşturma kampanyası başlatılmalı ve her düzeydeki ilgili tüm paydaşlarla işbirliği ve dayanışma içinde eğitim programları, seminerler, konferanslar düzenlenmeli; medya imkanları kullanılarak tanıtıcı film ve reklamlar hazırlanmalıdır. Aynı şekilde ulusal kapasitenin geliştirilmesi ve ülkemizin ihtiyaç duyduğu bilgi ve uzmanlık ihtiyacının karşılanması için sürekli eğitim ve sertifika programları geliştirilmelidir. Yapılacak tüm çalışmalarda uluslar arası uyum ve koordinasyonun sağlanmasına özen gösterilmelidir.

EKLER

EK – 1

ÜLKE	YASAL DÜZENLEMELER
ABD	– The Privacy Act (1974) – Computer Security Act (1987) – The Digital Millennium Copyright Act (1998) – FISMA - Federal Information Security Management Act (2002) – Adam Walsh Child Protection and Security Act (2006) – Can-Spam (Controlling the Assault of Non-Solicited Pornography and Marketing) Act (2004) – US Code (Article 1030 → Illegal access, Article 2702 → Expedited preservation and partial disclosure)
Almanya	– German Data Protection Act – German Law regarding Information Society Services – Law No. 1786 (2007) – German Criminal Code (Article 202 → Illegal interception, Article 303 → Data interference, System interference, Article 223 → Computer related fraud)
Arjantin	– Personal Data Protection Act (2000) – Draft Law on Electronic Communication Services, Information Society and Electronic Commerce (Anti-Spam legislation) (2003)
Avrupa Konseyi	– Convention on Cybercrime (2001)
Avrupa Birliği	– Data Protection Act (1998) – Regulation of Investigatory Powers (2000) – E-Privacy Directive: Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002) – E-Commerce Directive: Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (2000) – Telecommunications Privacy Directive: Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (1998) – Distance Contracts Directive: Directive 97/7/EC on the Protection of Consumers in Respect of Distance Contracts (1997) – Data Protection Directive: Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on

	the Free Movement of Such Data (1995)
Avustralya	– The Privacy Act (1988) – Spam Act (2003)
Avusturya	– Telecommunications Act (2003) – Penal Code (Article 119 → Illegal interception, Article 126 → Data interference, System interference, Misuse of devices, Article 223 → Computer related forgery, Article 148 → Computer related fraud, Article 207 → Child pornography) – Federal Law on Copyright (Article 91 → Copyright infringement) – Criminal Procedure Code (Article 109, 134 → Expedited preservation of stored computer data, Article 109, 134 → Expedited preservation and partial disclosure, Article 109, 119-122 → Search and seizure of stored computer data, Article 134, 137 → Real time collection of data, Article 134, 137 → Interception of content data)
Bulgaristan	– Personal Data Protection Act – Penal Code (Article 172 → Copyright infringement) – Criminal Procedure Code (Article 125, 159, 162, 163 → Expedited preservation of stored computer data, Article 159, 160, 161 → Search and seizure of stored computer data, Article 172 → Interception of content data)
Çek Cumhuriyeti	– Act No. 480/2004 Coll., on Certain Information Society Services – Act No. 127/2005 Coll., on Electronic Communications
Ermenistan	– Law on Personal Data – Criminal Code (Article 158 → Copyright infringement)
Estonya	– Information Society Service Act – Personal Data Protection Act – Telecommunications Act – Criminal Code (Article 217 → Illegal access) – Criminal Procedure Code (Article 118 → Interception of content data)
Finlandiya	– Communications Market Act (2003) – The Act on the Protection of Privacy on Electronic Communications (2004)
Fransa	– Data Protection Act (1974, rev 2004) – Law No. 88-19 (1988) – “Computer fraud” – Law No. 1062 (2002) – “Continuity of security” – Law No. 204 (2004) – “Healthy adaptation of justice to the evolution of criminality”

	– Law No. 575 (2004) – "Confidence in the digital economy" → Spam – Penal Code (Article 226 → Data interception, Article 323 → System interference, Article 227 → Child pornography) – Code de Procedure Penale (Article 706, 100 → Interception of content data)
Güney Kıbrıs	– Electronic Communications and Postal Services Law (2004) – Processing of Personal Data (Protection of the Individual) Law (2001) – Law No. 22 (2004) (Article 5 → Illegal interception, Article 6 → Data interference, Article 7 → System interference, Article 9 → Computer related forgery, Article 10 → Computer related fraud, Article 12 → Child pornography, Article 12 → Copyright infringement)
Hırvatistan	– Law No. OG 105 (2004) (Article 223 → Illegal interception, Misuse of devices, Computer related forgery, Article 233 → Data interference, Article 230 → Copyright infringement)
Hollanda	– Dutch Telecommunications Act – Dutch Data Protection Act – Criminal Code (Article 138 → Illegal access, Article 350 → Data interference)
Hindistan	– Information Technology Act (2000)
Hong Kong	– Personal Data (Privacy) Ordinance
İngiltere	– Data Protection Act (1998) – Electronic Communications Act (2000)
İrlanda	– Data Protection Act, 1988 – Statutory Instrument, S.I. No. 535 of 2003, European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003
İspanya	– Spanish Data Protection Act (1992) – Organic law 15/1999 on personal data protection
İsveç	– Personal Data Act (1998)
İsviçre	– Data Protection Law
İtalya	– Personal Data Protection Code (196/2003) – DL 675/1996 on privacy protection states – DL 171/1998 on telecommunications privacy protection

	– DL 185/1999 on customer protection with respect to long-distance contracts
Japonya	– Law on Regulation of Transmission of Specified Electronic Mail (2002)
Kanada	– Privacy Act (1980-81-82-83) – Personal Information Protection and Electronic Documents Act – Anti-Spam Action Plan
Kore	– Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection (2001, rev 2002)
Litvanya	– Law on Electronic Communications – Law on Legal Protections of Personal Data – Criminal Code (Article 198 → Illegal access)
Malta	– Data Protection Act (2003)
Macaristan	– Act CVIII of 2001 on Electronic Commerce – Act C of 2003 on Electronic Communications – Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest
Malezya	– Electronic Transaction Act (1998) – Communications and Multimedia Act (1998)
Polonya	– Polish Law Concerning the Provision of Electronic Services (2003) – Personal Data Protection Act (1997) – Telecommunication Law (2004) – Act on providing services by electronic means (2002)
Portekiz	– Law No. 109 (1991) (Article 7 → Illegal access, Article 8 → Illegal interception, Article 4 → Computer related forgery) – Penal Code (Article 221 → Computer related fraud) – Penal Procedure Code (Article 190 → Interception of content data)

Romanya	– Law 365/2002 on the electronic commerce – Law No. 161 (2003) (Article 42 → Illegal access, Article 43 → Illegal interception, Article 44 → Data interference, Article 45 → System interference, Article 46 → Misuse of devices, Article 48 → Computer related forgery, Article 49 → Computer related fraud, Article 51 → Child pornography, Article 54 → Expedited preservation of stored computer data, Article 54 → Expedited preservation and partial disclosure, Article 54 → Real time collection of data, Article 57 → Interception of content data, Article 65 → Transborder access to stored computer data with consent)
Ukrayna	– Criminal Code (Article 176, 216 → Copyright infringement)
Şili	– Act on the Protection of Personal Data (1998)
Yeni Zelanda	– Privacy Act (1993)

ASEAN Ülkelerinde Siber Güvenlik Düzenlemeleri

	YASAL DÜZENLEMELER								
ÜLKE	Tüketicinin korunması	Kişisel mahremiyet	Siber suçlar	İstemdışı e-posta	İçerik düzenlemesi	Sayısal telif hakları	Alan Adları	Elektronik sözleşmeler	Uyuşmazlık Çözümü
Brunei	-	-	Yasa	-	Yasa	Yasa	Yasa	Yasa	-
Kamboçya	-	-	-	-	-	Yasa	Yasa	Taslak	-
Endonezya	Taslak	Taslak	Taslak	-	-	Yasa	Taslak	Taslak	-
Malezya	Yasa	Taslak	Yasa	Yasa	Yasa	Yasa	Yasa	Yasa	-
Mynmar	-	-	Yasa	-	Yasa	Plan	-	Yasa	-
Filipinler	Yasa	-	Yasa	Taslak	-	Yasa	-	Yasa	Yasa
Singapur	-	Yasa	Yasa	Yasa	Yasa	Yasa	-	Yasa	-
Tayland	-	Taslak	Yasa	Plan	-	Plan	-	Yasa	Plan
Vietnam	-	-	Yasa	-	-	-	Yasa	Yasa	-

Yukarıda listelenen düzenlemelere ek olarak, pek çok ülkenin Rekabet, Tüketicinin Korunması, Elektronik Haberleşme gibi kanunlarında siber güvenliğe ilişkin düzenlemeler bulunmaktadır.

Ek – 1'de yer alan bilgiler aşağıdaki kaynaklardan yararlanılarak derlenmiştir:

1. United Nations, "Information Economy Report 2007 -2008, Chapter 8 - Harmonizing cyber Legislation at the Regional Level: The Case of ASEAN", 2008

2. ITU, "ITU Survey on Anti-Spam Legislation Worldwide", WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005

3. Council of Europe Project on Cybercrime, "National Legislation Implementing the Convention on Cybercrime – Comparative analysis and good practices", 2008

4. ITU, "Global Cybersecurity Agenda High Level Experts Group Global Strategic Report", 2007

EK – 2

BÖLGESEL GİRİŞİMLER

Avrupa Konseyi Girişimleri:

- Avrupa Konseyi Siber Suç Sözleşmesi (2001): Siber suçlarla mücadele konusunda önemli bir aşamadır. Tunus'ta düzenlenen Dünya Bilgi Toplumu Zirvesi'nde bölgesel bir girişim olarak kabul edilmiştir. Temmuz 2004'te yürürlüğe konan sözleşmeyi Ocak 2008 itibarıyla 21 devlet onaylamış, 22 devlet de imzalamıştır. Bu sözleşmeyi onaylamakla, devletler, bu sözleşmede suç olarak tanımlanan davranışların, kendi ulusal mevzuatlarında da suç olarak tanımlanmasını sağlamayı ve bu suçların soruşturulması ve kovuşturulması için gereken tüm işlevsel araçları tesis etmeyi kabul ederler.

- 2005 yılında yürürlüğe giren "Bilgi Sistemlerine Yönelik Saldırılar Konusunda Avrupa Konseyi Çerçeve Kararı", Siber Suç Sözleşmesini tamamlayıcı nitelikte olup, bilgi sistemlerine ve verilere yasa dışı erişim konularında maddeler içermektedir.

- "Terörizmi Bastırma Sözleşmesi" (1977, Avrupa Konseyi)

- "Terörizmi Önleme Sözleşmesi" (2005, Avrupa Konseyi)

Avrupa Birliği Girişimleri:

- AB Komisyonu tarafından Mayıs 2007'de kimlik bilgileri hırsızlığına karşı "Siber suçlarla mücadele üzerine genel bir politikaya doğru" adıyla bir girişim başlatılmış, Kasım 2007'de toplanan bir AB uzmanlar toplantısında ise bu politika tasarısının uygulanması ile ilgili hususlar görüşülmüş ve şu tespitlerde bulunulmuştur:
  "Siber suçların Avrupa çapında giderek yaygınlaşması – Estonya'yı hedef alan büyük saldırılar, İspanya'da yaşanan kimlik bilgileri hırsızlığı, Avusturya, Almanya, İtalya ve İngiltere'de yaşanan yasadışı içeriğin yayılması ve İnternet yoluyla çocukların cinsel istismarı vakaları – birlikte hareket etmenin gerekliliğine dikkat

çekmektedir. 'Koala Operasyonu', 'Vico' adlı saldırganın yakalanması gibi başarılı operasyonlar da bölgesel ve uluslar arası işbirliğine dayanmaktadır."

G8 Girişimleri:

- G8 ülkeleri tarafından 1997'de kurulan "Yüksek-Teknoloji Suçları (Leon)" Grubu, 1997 yılında siber suçluların dünyanın hiçbir yerinde sığınabilecekleri "güvenli sığınaklar" bulamamalarını hedefleyen siber suçlarla mücadele için benimsedikleri 10 temel prensibi beyan etmişlerdir.

- 2004 yılında G8 ülkelerinin Adalet ve İçişleri Bakanlarının katılımıyla gerçekleşen toplantıda ise, Avrupa Konseyi Siber Suç Sözleşmesinde yer alan yasal standartlara uyum sağlamanın özendirilmesi amacıyla G8 üyeleri tarafından gereken adımların atılacağını belirtmişlerdir.

- 2006 yılında düzenlenen benzer G8 toplantılarında da şu hususlar üzerinde durulmuştur:
  - Terörizm ve siber suçlarla mücadele
  - Bilgi güvenliği ve şebeke güvenliği konuları
  - Etkin karşı tedbirler geliştirmenin gerekliliği
  - Siber suçlar konusunda uluslar arası tecrübe paylaşımı ve bütüncül yaklaşımlar benimsenmesi
  - Mevcut yasal mevzuatın ilgili kısımlarının karşılaştırmalı analizi
  - Uluslar arası yasal temellerin oluşturulması
  - Uluslar arası ortaklar ile işbirliği içinde çalışma

- 2007 yılında düzenlenen bir başka toplantıda ise her üye devletin kendi ulusal mevzuatında İnternetin terör amacıyla kullanımını suç olarak kabul etmesi kararlaştırılmıştır.

Asya Pasifik Ekonomik İşbirliği (APEC) Girişimleri:

- 2002 ve 2005 yılında düzenlenen çeşitli toplantılarda, APEC liderleri "siber güvenlik ve siber suçlar hakkında 55/63 (2000) sayılı Birleşmiş Milletler Genel Kurulu kararı ("Bilginin Suç Amaçlı Kötüye Kullanımı ile Mücadele") ve Avrupa Konseyi Siber Suç Sözleşmesi gibi mevcut uluslar arası yasal düzenlemelerle uyumlu kapsamlı bir dizi yasanın kabulünü" kararlaştırmışlardır.

- APEC bünyesinde siber güvenlik ve siber suçlar konularında çalışan Bilgi ve İletişim Çalışma Grubu (TEL WG), 2002 yılında liderler tarafından belirlenen bu hedeflerinin nasıl uygulanacağına dair tespitler içeren "APEC Siber Güvenlik Stratejisi"ni yayınlamış ve kapasite geliştirme ve yasal mevzuat taslakları oluşturma amacıyla konferanslar düzenlemiştir. Bunların başarısının ardından APEC üyesi devletlere kendi yasal düzenlemelerini yapma ve siber suçları araştırma birimlerini kurma konularında destek sağlanmıştır. Ayrıca, üye devletler için, Siber Suçlar ve hukuki yaptırımları uygulama konusunda Hakim ve Savcılara yönelik bir kapasite geliştirme projesi de planlanmaktadır. "APEC Siber Güvenlik Stratejisi"nin yasal düzenlemeler bölümünde Siber Suç Sözleşmesi ilk çok taraflı yasal belge olarak tanınmaktadır.-

- "APEC Siber Güvenlik Stratejisi"ni tamamlayıcı nitelikte olan ve TEL WG tarafından 2005 yılında yayınlanan "APEC Güvenli, Güvenilir ve Sürdürülebilir Çevrimiçi Ortamın Sağlanması Stratejisi" de çevrimiçi güvenliği sağlamak için APEC üyelerinin yakın işbirliği içinde bulunmasını teşvik etmektedir.

Amerikan Devletleri Topluluğu (OAS) Girişimleri:

- 2004, 2005 ve 2006 yıllarında düzenlenen toplantılarda üye devletlerin Avrupa Konseyi Siber Suç Sözleşmesi'nde yer alan prensiplerin kendileri için uygulanabilirliğini ve kabul edilebilirliğini değerlendirmeleri ve topluluk olarak da Avrupa Konseyi ile işbirliğinin geliştirilmesi kararlaştırılmıştır. Ayrıca, Birleşmiş Milletler, APEC, OECD, G8, Commonwealth, Interpol gibi uluslar arası kuruluşlarla

siber suçlar konusunda bilgi alışverişi yapmak üzere gereken mekanizmaların geliştirilmesine de önem verilmektedir.

İngiliz Milletler Topluluğu (Commonwealth) Girişimleri:

- Üye devletlerin ceza kanunlarını birbirine uyumlu hale getirmek amacıyla Siber Suç Sözleşmesine paralel "Bilgisayar ve Bilişim Suçları Yasası" adlı bir model yasa tasarlanmıştır. (2002)

Güney Doğu Devletleri Topluluğu (ASEAN) Girişimleri:

- 2006 yılında düzenlenen ASEAN Bölgesel Forumu (ARF) sonunda "siber saldırılar ve siber ortamın terörist amaçlı kötüye kullanımı ile mücadelenin, yasal ve diğer konularda hızlı ve iyi işleyen bir işbirliği ile mümkün olacağının bilincinde olarak, üye devletler bir an önce siber suçlar ve siber güvenlikle ilgili ulusal yasalarını çıkaracak ve bu yasaları ilgili uluslar arası tavsiyelerden veya rehberlerden yararlanarak kendi ulusal koşullarına uygun şekilde uygulayacaklardır" ifadesi vurgulanmıştır.

Arap Devletleri Topluluğu Girişimleri:

- Birleşik Arap Emirlikleri başta olmak üzere Pakistan ve Suudi Arabistan siber suçlar ile yasalarını yürürlüğe koymuşlardır. Gulf İşbirliği Konseyi ülkeleri (Bahreyn, Kuveyt, Katar, Umman, S. Arabistan ve BAE) de 2007 yılında siber suçlar üzerine bir anlaşma taslağı hazırlığında olduklarını açıklamışlardır.

Afrika Birliği Girişimleri:

- 2005 yılında Güney Afrika Gelişim Topluluğu (SADC) üyeleri Zambiya, Zimbabwe, Güney Afrika, Malawi ve Mozambik siber suç yasalarını uyumlu hale getirmek için çalışmalara başlamışlardır. Siber suç mevzuatının uyumlaştırılma süreci Doğu Afrika ülkelerinde (Tanzanya, Kenya, Uganda) daha yavaş ilerlemektedir.

Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Girişimleri:

- OECD 2002 yılında kritik bilgi altyapılarını koruma ile ilgili tavsiyeler içeren, ancak üye devletler için bağlayıcı nitelikte olmayan "Bilgi Sistemleri ve Ağlarının Güvenliği: Bir Güvenlik Kültürüne Doğru" adlı rehberi yayınlamıştır. Bilişim suçlarıyla mücadele üzerine bir rehber oluşturan ilk uluslar arası kuruluş olan OECD, siber suçlar ve siber güvenlik konularında pek çok forum ve çalıştay da düzenlemiştir. OECD siber suçlardan ziyade siber güvenlik üzerine odaklanmıştır ve güveni tesis etmek için küresel çapta koordine edilen bir politika oluşturma yaklaşımını benimsemektedir.

Şanghay İşbirliği Teşkilatı (SCO) Girişimleri:

- Çin, Rusya Federasyonu, Kazakistan, Kırgızistan, Tacikistan ve Özbekistan tarafından 2001 yılında kurulan SCO'nun yayınlamış olduğu Terörizm, Bölücülük ve Aşırılık Sözleşmesinde "Üye devletler, terörizm, bölücülük ve aşırılığın, amacı ne olursa olsun, hiçbir şekilde haklı sayılamayacağına ve bu suçları işleyenlerin yasalarla yargılanması gerektiğine inanmaktadırlar." ifadeleri yer almaktadır. SCO'nun 2007'de düzenlenen Konsey Toplantısında da üyeler "SCO ülkelerinin uluslar arası bilgi güvenliğini koruma eylem planı" imzalamışlardır.

ULUSLARARASI GİRİŞİMLER

Birleşmiş Milletler:

- Birleşmiş Milletler Ülkelerarası Organize Suçlarla Mücadele Sözleşmesi (2000) bu alandaki temel uluslar arası belge olup, ülkelerarası organize suçları önlemekte daha etkin bir işbirliğinin tesis edilmesini amaçlamaktadır.

- Birleşmiş Milletler' in çocukların cinsel istismarı (2007), mali sahtecilik ve kimlikle ilgili suçlar (2004, 2007), bilgi sistemlerinin suç amaçlı kullanımı (2000, 2001), uyuşturucu ticareti (2000, 2004, 2005) gibi suçlarla mücadele hususunda tavsiye kararları da mevcuttur.

- Birleşmiş Milletler Güvenlik Konseyinin 58/199 (2003) sayılı tavsiye kararında benimsenen prensiplere göre, ülkeler;
  - Siber tehditler, açıklıklar ve olaylar üzerine acil durum uyarı şebekeleri kurmalı,
  - Tüm paydaşların Kritik Bilgi Altyapılarının kapsamı ve kendilerinin bunlara ilişkin sorumluluğu hakkında farkındalığını arttırmalı,
  - Altyapılarını incelemek ve karşılıklı bağımlılıkları tespit etmek suretiyle bunların güvenliğini arttırmalı,
  - Paydaşlar arasında (kamu-özel sektör) bilgi paylaşımı amacıyla ortaklıklar kurulmasını teşvik etmeli,
  - Kriz iletişim şebekeleri kurmalı ve bunların acil durumlarda çalışabilir durumda olması için gereken testleri yapmalı,
  - Verilerin erişilebilirliğine ilişkin politikaların Kritik Bilgi Altyapılarının korunması ihtiyacını dikkate almasını sağlamalı,
  - Kritik Bilgi Altyapılarına yönelik saldırıların izini sürmeli ve mümkünse elde ettikleri bilgileri diğer ülkelerle de paylaşmalı,
  - Olaylara müdahale yeteneklerinin geliştirilmesi için gereken eğitim ve tatbikatları düzenlemeli, süreklilik ve beklenmedik durum planlarını test etmeli ve paydaşların da benzer faaliyetlerde bulunmalarını teşvik etmeli,
  - Siber suçlara ilişkin yeterli yasal düzenlemeler ile bunların soruşturma ve kovuşturmasında görev alacak eğitimli personele sahip olmalı ve gerekirse bu tür soruşturmaları diğer ülkelerle birlikte yürütmeli,
  - Kritik Bilgi Altyapılarının güvenliğini sağlamak için acil durum uyarı sistemleri oluşturma, tehditler, açıklıklar ve yaşanan olaylara ilişkin bilgi paylaşımında bulunma gibi amaçlarla oluşturulan uluslar arası işbirlikleri içinde yer almalı,
  - Ulusal ve uluslar arası araştırma ve geliştirme ile uluslar arası standartlara göre belgelendirilmiş olan güvenlik teknolojilerinin uygulanmasını teşvik etmelidirler.

ITU Girişimleri

- ITU tarafından düzenlenen ve ilk aşaması 2003'te Cenevre'de, ikinci aşaması ise 2005'te Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesi'nde birçok uluslararası kuruluş, şirket ve sivil toplum örgütü, geleceğin Bilgi Toplumu için ortak bir vizyon belirlemek amacıyla bir araya gelmiştir. Bu zirve sonunda ortaya çıkan 11 ana eylem maddesinden biri olan "Bilgi ve İletişim Teknolojilerinin Kullanımında Gizlilik ve Güvenliği Tesis Etmek" maddesini uygulamaya koyma sorumluluğu ITU' ya verilmiştir. Bunun üzerine ITU 17 Mayıs 2007 tarihinde küresel siber güvenliğin günden güne artan sorunlarına karşı uluslararası bir tepkinin nasıl koordine edilebileceğine dair saptamalar içeren "Küresel Siber Güvenlik Gündemi"ni yayınlamıştır. Bu dokümanda vurgulanan 7 ana hedef şunlardır:
    1. Küresel düzeyde uygulanabilir ve mevcut ulusal ve bölgesel mevzuatlara uyumlu bir siber suç mevzuatı geliştirilmesine,
    2. Siber suçlarla ilgili ulusal ve bölgesel kuruluşların ve politikaların oluşturulmasına,
    3. Küresel düzeyde kabul gören asgari güvenlik ölçütleri ve yazılım ve donanım sistemleri için akreditasyon planları oluşturulmasına,
    4. Mevcut ve yeni teşebbüsler arasında sınır ötesi koordinasyonu sağlamak amacıyla izleme, uyarma ve olaylara tepki için küresel bir çerçeve model kurulmasına,
    5. Evrensel bir sayısal kimlik sisteminin ve sayısal kimlik bilgilerinin tüm dünyada tanınmasını sağlayan kuruluşların oluşturulmasına,
    6. Sektörler arasında bilgi birikimi ve alışverişini sağlamak amacıyla kurumsal kapasitenin iyileştirilmesine,
    7. Tüm bu konularda uluslararası işbirliği, diyalog ve koordinasyonu tesis etmek üzere bir küresel çerçeve model kurulmasına yönelik stratejiler geliştirmektir.

EK – 3

ÜLKE	BİLGİSAYAR OLAYLARINA MÜDAHALE EKİPLERİ
Avusturya	ACOnet-CERT Kuruluş Tarihi: 2003 Statüsü: Akredite Üyeleri: ACOnet (Avusturya Akademik Bilgisayar Ağı) kullanıcıları http://cert.aco.net CERT.AT Kuruluş Tarihi: 2008 Statüsü: Akredite Üyeleri: Avusturya BT güvenliği ekipleri (Tıp alanından, Ticaret odalarından, İnternet Servis Sağlayıcılardan vs.) http://www.cert.at/
Belçika	BELNET CERT Kuruluş Tarihi: 2004 Statüsü: Akredite Üyeleri: BELNET kullanıcıları (Kamu kurumları, üniversiteler, liseler ve araştırma merkezleri) http://cert.belnet.be NCIRC CC Statüsü: Listede Üyeleri: NATO Bilgisayar Olaylarına Müdahale Kapasitesi – Koordinasyon Merkezi
Hırvatistan	CARNet CERT Kuruluş Tarihi: 1996 Statüsü: Akredite Üyeleri: ".hr" alanı içinde yer alan sistemlerin kullanıcıları http://www.cert.hr
Güney Kıbrıs	CYPRUS Statüsü: Listede Üyeleri: CYNET (Güney Kıbrıs Akademik ve Araştırma Ağı) kullanıcıları

Çek Cumhuriyeti	CESNET-CERTS Kuruluş Tarihi: 2004 Statüsü: Akredite Üyeleri: “cesnet.cz”, “cesnet2.cz”, “ces.net”, “ten.cz” ve “ipv6.cz” alanları içinde yer alan sistemlerin kullanıcıları http://www.cesnet.cz CSIRT.CZ Statüsü: Listede Üyeleri: Ulusal BOME http://www.csirt.cz/en/ CZNIC-CSIRT Statüsü: Listede Üyeleri: “.cz” üst düzey alanına yönelik BOME http://www.nic.cz/csirt/
Danimarka	CSIRT.DK Kuruluş Tarihi: 1999 Statüsü: Akredite Üyeleri: TDC’nin profesyonel kullanıcıları http://www.csirt.dk DK-CERT Kuruluş Tarihi: 1991 Statüsü: Akredite Üyeleri: UNI-C, Danimarka Araştırma ve Eğitim Ağları, Sektornet ve Forskningsnet http://www.cert.dk KMD IAC Kuruluş Tarihi: 1997 Statüsü: Akredite Üyeleri: KMD kullanıcıları ve Danimarka yerel yönetimleri
Estonya	CERT EE Kuruluş Tarihi: 2006 Statüsü: Akredite Üyeleri: Ulusal BOME http://www.cert.ee/

	SKY-CERT Kuruluş Tarihi: 2002 Statüsü: Listede Üyeleri: Skype üyeleri
Finlandiya	CERT-FI Kuruluş Tarihi: 2002 Statüsü: Akredite Üyeleri: Elektronik haberleşme şebekesi işletmecileri, servis sağlayıcıları ve kritik altyapı işletmecileri başta olmak üzere tüm kurum ve kuruluşlar http://www.cert.fi Ericsson PSIRT Statüsü: Akredite Üyeleri: Ericsson müşterileri ve ürün geliştirme birimleri Funet CERT Kuruluş Tarihi: 1995 Statüsü: Akredite Üyeleri: Funet tüketici dernekleri ve bu derneklerin ağları http://www.cert.funet.fi/english.html Nokia NIRT Kuruluş Tarihi: 1998 Statüsü: Akredite Üyeleri: “nokia.com” alanı içinde yer alan sistemlerin kullanıcıları
Fransa	Cert-IST Kuruluş Tarihi: 1999 Statüsü: Akredite Üyeleri: Sanayi, hizmet ve üçüncül sektör temsilcileri (ALCATEL, CNES, FRANCE TELECOM, SANOFI AVENTIS, TOTAL vs.) http://www.cert-ist.com/eng/ CERT-LEXSI Statüsü: Listede Üyeleri: CSI ve SERENIS aboneleri ve diğer özel şirketler http://www.lexsi.com/ CERTA Kuruluş Tarihi: 1999

	Statüsü: Akredite Üyeleri: Yerel yönetimler de dahil olmak üzere tüm kamu kurum ve kuruluşları http://www.certa.ssi.gouv.fr CERT-Renater Kuruluş Tarihi: 1993 Statüsü: Akredite Üyeleri: Eğitim Bakanlığı, Araştırma Bakanlığı, CNRS (Ulusal Bilimsel Araştırma Komitesi), CEA (Ulusal Nükleer Araştırma Enstitüsü), INRIA (Ulusal Bilgisayar Bilimleri Araştırmaları Enstitüsü), CNES (Fransa Uzay Ajansı), INRA ve CIRAD (Tarım Bilimleri Araştırma Enstitüleri) http://www.renater.fr/rubrique.php3?id_rubrique=19&lang=en
Yunanistan	AUTH-CERT Statüsü: Listede Üyeleri: Selanik Aristo Üniversitesi ağı kullanıcıları http://www.auth.gr FORTH CERT Statüsü: Listede Üyeleri: FORTH üyeleri, araştırma sektörü http://www.forth.gr/forthcert/ GRNET-CERT Kuruluş Tarihi: 2Q 2000 Statüsü: Akredite Üyeleri: Yunanistan Araştırma ve Teknoloji Ağı kullanıcıları http://cert.grnet.gr
Macaristan	CERT-Hungary Kuruluş Tarihi: 2004 Statüsü: Akredite Üyeleri: Kamu kurumları, belediyeler ve özel şirketler http://www.cert-hungary.hu/ HUN-CERT Statüsü: Listede Üyeleri: İnternet Servis Sağlayıcılar http://www.cert.hu/hun-cert/index.html

	NIIF-CSIRT Statüsü: Listede Üyeleri: NIIF/HUNGARNET (Üniversiteler, Yüksek öğretim kurumları, Orta öğretim kurumları, Akademik araştırma merkezleri vs.) kullanıcıları http://csirt.niif.hu
İrlanda	HEANET-CERT Statüsü: Listede Üyeleri: HEANET (İrlanda Eğitim ve Araştırma Ağı) kullanıcıları http://www.heanet.ie/services/services.php?serID=1&subID=6
İzlanda	RHnet CERT Statüsü: Listede Üyeleri: RHnet (İzlanda Üniversiteler Araştırma Ağı) kullanıcıları
İtalya	CERT-IT Kuruluş Tarihi: 1994 Statüsü: Listede Üyeleri: Tüm İnternet siteleri http://security.dsi.unimi.it CERT ENEL Üyeleri: ENEL S.P.A. üyeleri http://www.enel.it/attivita/servizi_diversificati/informatica/cert/ GARR-CERT Kuruluş Tarihi: 1999 Statüsü: Akredite Üyeleri: GARR (İtalya Akademik ve Araştırma Ağı) kullanıcıları http://www.cert.garr.it GOVCERT.IT Kuruluş Tarihi: 2004 Üyeleri: Merkezi yönetim kamu kurum ve kuruluşları ve CERT-AM (21)'i oluşturan 21 Bakanlık http://www.govcert.it/ CERT-Difesa Üyeleri: Savunma ağı http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/

	CERT-RAFVG Üyeleri: Yerel ajanslar http:/cert-rafvg.regione.fvg.it SICEI-CERT (formerly SOC-IDS-CEI) Üyeleri: Katolik Kilisesinin 80 piskoposluk bölgesi http://cert.chiesacattolica.it S2OC Üyeleri: Telecom Italia Grubu (30 şirket) http://www.tuconti.telecomitalia.it
Letonya	CERT NIC.LV Statüsü: Akredite Üyeleri: Letonya Üniversitesi Matematik ve Bilgisayar Bilimleri Enstitüsü ve ağa bağlı tüm kurum ve kuruluşlar http://cert.nic.lv/ DDIRV Statüsü: Listede Üyeleri: Kamu kurumları ve belediyeler http://www.ddirv.lv
Litvanya	LITNET CERT Kuruluş Tarihi: 1998 Statüsü: Akredite Üyeleri: LITNET (Üniversiteler, okullar, araştırma merkezleri vs.) kullanıcıları http://cert.litnet.lt CERT-LT Kuruluş Tarihi: 2006 Üyeleri: Ulusal BOME http://www.cert.lt/en/
Lüksemburg	CIRCL Statüsü: Listede Üyeleri: Merkezi ve yerel yönetimler http://www.circl.lu/

	CSRRT-LU Üyeleri: Ulusal BOME http://www.csrrt.org/wiki/index.php RESTENA-CSIRT Statüsü: Listede Üyeleri: RESTENA (Eğitim ve Araştırma Topluluğu) http://www.restena.lu/csirt/
Malta	mtCERT Kuruluş Tarihi: 2002 Statüsü: Akredite Üyeleri: Kamu kurum ve kuruluşları http://www.mtcert.gov.mt
Norveç	NorCERT Kuruluş Tarihi: 2004 Statüsü: Akredite Üyeleri: Kritik bilgi ve altyapı sahipleri http://www.cert.no/ UiO-CERT Kuruluş Tarihi: 2005 Statüsü: Akredite Üyeleri: Oslo Üniversitesi ve işbirliği yaptığı kurum ve kuruluşlar http://cert.uio.no UniNett CERT Kuruluş Tarihi: 1995 Statüsü: Akredite Üyeleri: Norveç Akademik Araştırma ve Eğitim Ağı kullanıcıları http://cert.uninett.no
Polonya	CERT GOV PL Kuruluş Tarihi: 2008 Üyeleri: Kamu kurum ve kuruluşları http://www.cert.gov.pl/ CERT POLSKA Kuruluş Tarihi: 1996 Statüsü: Akredite

	Üyeleri: ".pl" alanı içinde yer alan sistemlerin kullanıcıları http://www.cert.pl/english.html PIONIER-CERT Statüsü: Listede Üyeleri: PIONIER (Ulusal Bilimsel Optik Ağı) kullanıcıları http://cert.pionier.gov.pl/ TP CERT Statüsü: Listede Üyeleri: Tpnet kullanıcıları http://www.tp.pl/cert
Portekiz	CERT.PT Kuruluş Tarihi: 2002 Statüsü: Akredite Üyeleri: Portekiz Ulusal Araştırma ve Eğitim Ağı kullanıcıları http://www.cert.pt CSIRT.FEUP Kuruluş Tarihi: 2006 Statüsü: Akredite Üyeleri: Porto Üniversitesi Mühendislik Fakültesi ağı ve "fe.up.pt" alanı içinde yer alan sistemlerin kullanıcıları http://csirt.fe.up.pt CERT-IPN Kuruluş Tarihi: 2007 Statüsü: Listede Üyeleri: IPN (Pedro Nunes Enstitüsü) kullanıcıları http://www.cert.ipn.pt/
Romanya	RoCSIRT Statüsü: Listede Üyeleri: RoEduNet kullanıcıları http://www.csirt.ro/
Rusya	RU-CERT Kuruluş Tarihi: 1998 Statüsü: Akredite Üyeleri: RBNET kullanıcıları

	http://www.cert.ru WebPlus ISP Statüsü: Listede Üyeleri: ISP WebPlus kullanıcıları http://www.security.wplus.net
Slovenya	SI-CERT Kuruluş Tarihi: 1994 Statüsü: Akredite Üyeleri: ARNES ve ".si" alanı içinde yer alan sistemlerin kullanıcıları http://www.arnes.si/english/si-cert/
İspanya	CCN-CERT Kuruluş Tarihi: 2006 Statüsü: Akredite Üyeleri: Merkezi ve yerel yönetimler http://www.ccn-cert.cni.es CSIRT-CV Kuruluş Tarihi: 2007 Statüsü: Listede Üyeleri: " *.gva.es" alanı içinde yer alan sistemlerin kullanıcıları https://www.csirtcv.es/ e-LC CSIRT Kuruluş Tarihi: 2005 Üyeleri: La Caixa: e-lacaixa S.A. Yatırım Bankası ve müşterileri http://www.first.org/members/teams/e-lc_csirt/ esCERT-UPC Kuruluş Tarihi: 1994 Statüsü: Akredite Üyeleri: UPC (Barcelona Politeknik Üniversitesi) ve "*.upc.es" ve alanı içinde yer alan sistemlerin kullanıcıları http://escert.upc.es INTECO-CERT Kuruluş Tarihi: 2007 Statüsü: Akredite Üyeleri: Vatandaşlar ve Küçük ve Orta Ölçekli İşletmeler

	http://cert.inteco.es IRIS-CERT Kuruluş Tarihi: 1995 Statüsü: Akredite Üyeleri: RedIRIS kullanıcıları http://www.rediris.es/cert/index.en.html
İsveç	SITIC Kuruluş Tarihi: 2003 Statüsü: Akredite Üyeleri: Kamu kurum ve kuruluşları http://www.sitic.se SUNet CERT Kuruluş Tarihi: 2000 Statüsü: Akredite Üyeleri: SUNet (Üniversiteler, Yüksek öğretim ve araştırma kuruluşları) kullanıcıları http://www.cert.sunet.se TS-CERT Kuruluş Tarihi: 1997 Statüsü: Akredite Üyeleri: TeliaSonera'nın iç ve dış ağ kullanıcıları TS-CERT altında aşağıdaki alt-CERT ekipleri oluşturulmuştur: – SONERA-DATANET Sub-CERT SMO, Finlandiya – SONERA-MEDIANET Sub-CERT SMO, Finlandiya – SONERA-TRANSIT Sub-CERT TSF/Abuse – SONERA-FI Sub-CERT TSF/Abuse – SONERA-DIFFSERV Sub-CERT TSF/Abuse – TELIANET Sub-CERT Skanova/IRT, İsveç – TELIANET-SWEDEN Sub-CERT Skanova/Abuse, İsveç – TELIANET-DENMARK Sub-CERT DK, Danimarka – TELIANET-UK Sub-CERT Skanova/IRT, İsveç – TELIA-MULTINET Sub-CERT Skanova/IRT, İsveç – TELIA-TCN TS-CERT, İsveç – NETCOM-NORGE Sub-CERT Netcom , Norveç
İsviçre	CC-SEC Statüsü: Listede Üyeleri: Cablecom üyeleri

	http://www.first.org/about/organisation/teams/cc-sec/ CERN CERT Statüsü: Listede Üyeleri: CERN (Avrupa Nükleer Araştırma Topluluğu) üyeleri IP+ CERT Kuruluş Tarihi: 1995 Statüsü: Listede Üyeleri: Swisscom IP-Plus İnternet Hizmetleri müşterileri http://cert.ip-plus.net OS-CIRT Statüsü: Listede Üyeleri: Open Systems AG Güvenlik Hizmetleri müşterileri SWITCH-CERT Kuruluş Tarihi: 1995 Statüsü: Akredite Üyeleri: SWITCH ağı kullanıcıları http://www.switch.ch/cert
Türkiye	TR-CERT Statüsü: Akredite Üyeleri: Kamu kurum ve kuruluşları http://www.tr-cert.gov.tr Ulak-CSIRT Statüsü: Akredite Üyeleri: UlakNet (Ulusal Akademik Ağ) kullanıcıları http://csirt.ulakbim.gov.tr/eng/
İngiltere	BP DSAC Kuruluş Tarihi: 2004 Üyeleri: BP Pte Limited üyeleri http://www.first.org/members/teams/bp_dsac/ http://digitalsecurity.bp.com BTCERTCC Kuruluş Tarihi: 1999 Statüsü: Akredite

	Üyeleri: BT (British Telecommunication) müşterileri http://www.btcert.bt.com Cisco PSIRT Kuruluş Tarihi: 1995 Statüsü: Akredite Üyeleri: Cisco müşterileri CITIGROUP (UK) Statüsü: Listede Üyeleri: Citigroup üyeleri CSIRTUK Kuruluş Tarihi: 1992 Statüsü: Akredite Üyeleri: ".co.uk", ".org.uk" and ".com.uk" alanları içinde yer alan sistemlerin kullanıcıları http://www.cpni.gov.uk/ DAN-CERT Statüsü: Listede Üyeleri: GEANT (Avrupa Araştırma Ağı) üyeleri http://www.dante.net/sf/ DCSIRT Statüsü: Akredite Üyeleri: Diageo ve "diageo.com" alanı içinde yer alan sistemlerin kullanıcıları E-CERT Statüsü: Listede TI Listede since: 2002 Üyeleri: Energis Squared Limited üyeleri ve müşterileri EUCS-IRT Statüsü: Listede Üyeleri: Edinburgh Üniversitesi sistemlerinin kullanıcıları GovCertUK Kuruluş Tarihi: 2007 Üyeleri: Kamu kurum ve kuruluşları http://www.govcertuk.gov.uk/

	JANET-CSIRT Kuruluş Tarihi: 1993 Statüsü: Akredite Üyeleri: JANET (Yüksek öğretim ve araştırma kuruluşları) kullanıcıları http://www.ja.net/cert/ MLCIRT (UK) Statüsü: Listede Üyeleri: Merrill Lynch üyeleri MODCERT Statüsü: Listede Üyeleri: İngiltere Savunma Bakanlığı sistemlerinin kullanıcıları http://www.mod.uk/cert/ OxCERT Statüsü: Listede Üyeleri: Oxford Üniversitesi sistemlerinin kullanıcıları (“.ox.ac.uk”) Q-CIRT Statüsü: Listede Üyeleri: QinetiQ üyeleri http://www.qinetiq.com RBSG-ISIRT Statüsü: Akredite Üyeleri: İskoçya Royal Bank üyeleri http://www.rbs.co.uk RM CSIRT Kuruluş Tarihi: 2003 Üyeleri: Royal Mail Group üyeleri

GMK Bulvarı Yeşilırmak Sokak No:16 06570 Demirtepe / ANKARA
URL: http://www.btk.gov.tr