ULUSLARARASI KURULUŞLARIN SİBER GÜVENİLİK FAALİYETLERİ

Mustafa ÜNVER
Cafer CANBAY
Ayşe Gül MİRZAOĞLU

Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri

Mustafa ÜNVER
Cafer CANBAY
Ayşe Gül MİRZAOĞLU

ISBN: 978-605-62506-2-0

Kapak Tasarımı:
Evrim ÇETİNKAYA

1. Basım, Aralık 2011

Bilgi Teknolojileri ve İletişim Kurumu
Yeşilırmak Sokak No 16, 06430 Demirtepe/ANKARA
Tel: (312) 294 72 00
Faks: (312) 294 71 45
İnternet: http://www.btk.gov.tr

Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri

Mustafa ÜNVER

Cafer CANBAY

Ayşe Gül MİRZAOĞLU

İÇİNDEKİLER

İÇİNDEKİLER i
KISALTMALAR ii
1 GİRİŞ 1
2 BİRLEŞMİŞ MİLLETLER'İN ÇALIŞMALARI 1
2.1 BM GENEL KURULU KARARLARI 2
2.2 BM BİLGİ VE İLETİŞİM TEKNOLOJİLERİ GÖREV GÜCÜ 4
2.3 İNTERNET YÖNETİŞİM FORUMU 5
3 ULUSLARARASI TELEKOMÜNİKASYON BİRLİĞİ'NİN ÇALIŞMALARI 6
3.1 DÜNYA BİLGİ TOPLUMU ZİRVESİ SÜRECİ 6
3.2 WSIS SONRASI SÜREÇ 7
3.2.1 PP-06 Sonuç Raporunda Yayımlanan İlgili Kararlar 7
3.2.2 WTDC-06 Sonuç Raporunda Yayımlanan İlgili Kararlar 8
3.2.3 WTSA-08 Sonuç Raporunda Yayımlanan İlgili Kararlar 8
3.3 ITU BİRİMLERİNİN SİBER GÜVENLİK FAALİYETLERİ 9
3.3.1 ITU Genel Sekreterliğinin Faaliyetleri 9
3.3.2 ITU - Telekomünikasyon Geliştirme Sektörünün Faaliyetleri 12
3.3.3 ITU - Telekomünikasyon Standardizasyon Sektörünün Faaliyetleri 12
3.3.4 ITU - Radyokomünikasyon Sektörünün Faaliyetleri 13
4 EKONOMİK İŞBİRLİĞİ VE KALKINMA TEŞKİLATI'NIN ÇALIŞMALARI 14
4.1 OECD BÜNYESİNDEKİ İLGİLİ BİRİMLER 14
4.2 ICCP FAALİYETLERİ 15
4.3 ÖNEMLİ ETKİNLİKLER 18
4.4 "GÜVENLİK KÜLTÜRÜ" İNTERNET SİTESİ 19
5 AVRUPA BİRLİĞİ'NİN ÇALIŞMALARI 19
5.1 AB DÜZENLEMELERİ 19
5.2 AB PROJELERİ, PROGRAMLARI VE DİĞER FAALİYETLERİ 21
5.3 AVRUPA ŞEBEKE VE BİLGİ GÜVENLİĞİ AJANSI 22
6 AVRUPA KONSEYİ'NİN ÇALIŞMALARI 23
6.1 AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ 23
7 SONUÇ 25
EKLER 27
EK-1 27
EK-2 28

KISALTMALAR

AB	Avrupa Birliği
AET	Avrupa Ekonomik Topluluğu
AK	Avrupa Konseyi
APEC	Asia Pacific Economic Cooperation
	Asya Pasifik Ekonomik İşbirliği Teşkilatı
BM	Birleşmiş Milletler
BİŞ	Bilgi ve İletişim Şebekeleri
BİT	Bilgi ve İletişim Teknolojileri
BS	Bilgi Sistemleri
BŞ	Bilgi Şebekeleri
CERT	Computer Emergency Response Team
	Bilgisayar Olaylarına Müdahale Ekibi
ENISA	European Network and Information Security Agency
	Avrupa Şebeke ve Bilgi Güvenliği Ajansı
EPCIP	European Programme for Critical Infrastructure Protection
	Avrupa Kritik Altyapıların Korunması Programı
GCA	Global Cybersecurity Agenda
	Küresel Siber Güvenlik Gündemi
HLEG	High Level Experts Group
	Yüksek Seviyeli Uzmanlar Grubu
ICCP	Committee for Information, Computer and Communications Policy
	Bilgi, Bilgisayar ve İletişim Politikaları Komitesi

IGF	Internet Governance Forum
	İnternet Yönetişim Forumu
ITU	International Telecommunications Union Uluslararası Telekomünikasyon Birliği
ITU-D	ITU-Telekomünikasyon Geliştirme Sektörü
ITU-R	ITU-Radyokomünikasyon Sektörü
ITU-T	ITU-Telekomünikasyon Standardizasyon Sektörü
OECD	Organization for Economic Cooperation and Development
	Ekonomik İşbirliği ve Kalkınma Teşkilatı
STI	Directorate for Science, Technology and Industry
	Bilim, Teknoloji ve Sanayi Direktörlüğü
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi
WSIS	World Summit on the Information Society Dünya Bilgi Toplumu Zirvesi
WTSA	World Telecommunication Standardization Assembly
	Dünya Telekomünikasyon Standardizasyon Genel Kurulu
WTDC	World Telecommunication Development Conference
	Dünya Telekomünikasyon Kalkınma Konferansı
WPISP	Working Party on Information Security and Privacy
	Bilgi Güvenliği ve Gizlilik Çalışma Grubu

1 GİRİŞ

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 bilgi ve iletişim teknolojileri 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 bilgi ve iletişim teknolojilerine giderek artan derecede bağımlı hale gelen kritik altyapıların korunmasını amaçlayan siber güvenliğin sağlanması konusu tüm dünyanın gündemine girmiştir.

Günümüzde, pek çok bölgesel ve uluslararası kuruluş, siber güvenlik konusunda;

- Ülkeler arasında bilgi paylaşımı,
- Yasal ve teknik boyutta ulusal kapasitelerin geliştirilmesi,
- Farkındalığın arttırılması,
- Uluslararası işbirliğinin sağlanması

gibi hedefleri sağlamaya yönelik faaliyetler yürütmektedir.

Bu çalışmada, ülkemizin üyesi olduğu Birleşmiş Milletler ve bünyesinde yer alan Uluslararası Telekomünikasyon Birliği, Ekonomik İşbirliği ve Kalkınma Teşkilatı ve Avrupa Konseyi'nin yanı sıra, hâlihazırda tam üyelik müzakere sürecini sürdürdüğü Avrupa Birliği tarafından siber güvenlik konusunda yürütülmekte olan faaliyetler ele alınmaktadır.

2 BİRLEŞMİŞ MİLLETLER'İN ÇALIŞMALARI

İkinci Dünya Savaşı sonrasında bozulan uluslararası ilişkileri istikrara kavuşturmak ve barışı daha sağlam temeller üzerine oturtmak amacıyla, 1945 yılında kurulan Birleşmiş Milletler (BM), günümüzde, söz konusu faaliyetlerinin yanı sıra, çocuk gelişimi ve sağlığı, çevre koruma, insan hakları, yoksullukla mücadele ve ekonomik kalkınma, tarımsal kalkınma, eğitim, kadın hakları, doğal afet yardımı, atom enerjisinin barışçıl amaçlar için kullanılması,

iş ve işçi hakları gibi pek çok alanda çalışmalarını sürdürmektedir. BM, 1980'lerin sonundan beri siber güvenlik konusunda faaliyetler yürütmektedir. Söz konusu faaliyetler, BM Genel Kurulu tarafından alınan kararların yanı sıra, BM Bilgi ve İletişim Teknolojileri (BİT) Görev Gücü ve BİT ile ilgili çalışmalar yürütmekle sorumlu ana BM ajansı olan Uluslararası Telekomünikasyon Birliği (International Telecommunications Union - ITU) tarafından yapılan çalışmaları kapsamaktadır[1].

2.1 BM GENEL KURULU KARARLARI

BM Genel Kurulu tarafından çeşitli tarihlerde alınan siber güvenlik ile ilişkili kararlar şunlardır:

- "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanında Gelişmeler" başlıklı kararlar[2] BİT'in BM'nin hedef ve ilkelerine aykırı şekilde kullanımından doğan sorunları ele almaktadır.

- "Bilgi Teknolojilerinin Suç Amaçlı Kötüye Kullanımı ile Mücadele" başlıklı kararlar[3] Üye ülkelere bilgi teknolojilerinin suç amaçlı kullanımına karşı ulusal mevzuatlarında gereken tedbirleri almalarını ve suçluların yararlanabileceği güvenli sığınakları ortadan kaldırmalarını tavsiye etmektedir. Aynı zamanda, Avrupa Konseyi Siber Suç Sözleşmesine de atıfta bulunmakta ve söz konusu sözleşmeyi siber güvenlik konusunda uluslararası düzeyde önemli bir çalışma olarak kabul etmektedir.

- "Küresel Siber Güvenlik Kültürünün Oluşturulması" başlıklı karar[4] bilgi ve şebeke güvenliğinin geliştirilmesi için kültürel anlayışlarda değişikliğe gidilmesi gerektiğinden bahsetmekte, küresel siber güvenlik kültürünün oluşturulması için gereken temel unsurları;

[1] ITU tarafından yürütülen siber güvenlik faaliyetlerine 2. bölümde ele alınmaktadır.

[2] Aralık 1998 tarihli ve 53/70 sayılı, Aralık 1999 tarihli ve 54/49 sayılı, Kasım 2000 tarihli ve 55/28 sayılı, Kasım 2001 tarihli ve 56/19 sayılı, Kasım 2002 tarihli ve 57/53 sayılı, Kasım 2003 tarihli ve 58/32 sayılı, Aralık 2004 tarihli ve 59/61 sayılı, Ocak 2006 tarihli ve 60/45 sayılı, Aralık 2006 tarihli ve 61/54 sayılı, kararlardır,.

[3] Aralık 2000 tarihli ve 55/63 sayılı, Aralık 2001 tarihli ve 56/121 sayılı kararlardır.

[4] Aralık 2002 tarihli ve 57/239 sayılı karardır.
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

- Farkındalık,
- Sorumluluk,
- Güvenlik ihlallerine tepki verebilme,
- Etik,
- Demokrasi,
- Risk değerlendirme,
- Güvenlik tasarımı ve uygulaması,
- Güvenlik yönetimi ve
- Yeniden değerlendirme olarak ortaya koymaktadır.

Söz konusu ilkeler aynı zamanda OECD tarafından 25 Temmuz 2002 tarihinde kabul edilen "Bilgi Sistemleri ve Ağlarının Güvenliğine İlişkin OECD Rehber İlkeleri" [5] olup, tüm kurum ve kuruluşların küresel siber güvenliğin sağlanmasına yönelik çalışmalarında bu ilkelere yer vermesi gerektiği vurgulanmıştır.

- "Küresel Siber Güvenlik Kültürünün Oluşturulması ve Kritik Bilgi Altyapılarının Korunması" başlıklı karar[6] bilgi altyapıları ile küresel çaptaki diğer kritik altyapıların birbirine olan bağımlılığına ve bunlara yönelik, sayıları ve türleri giderek artan tehditlere dikkat çekmektedir. Söz konusu karar, kritik bilgi altyapılarının korunmasında izlenmesi gereken prensipleri aşağıdaki şekilde sıralamaktadır:

1. Siber tehditler, açıklıklar ve güvenlik ihlalleri ile ilgili acil durum uyarı şebekeleri kurulmalıdır.

2. Tüm paydaşların kritik bilgi altyapılarının kapsamı ve kendilerinin bunlara ilişkin sorumluluğu hakkında farkındalığı arttırılmalıdır.

3. Altyapıları incelemek ve bunlar arasındaki karşılıklı bağımlılıkları tespit etmek suretiyle bunların güvenliği arttırılmalıdır.

4. Paydaşlar arasında (kamu-özel sektör) bilgi paylaşımına imkân veren ortaklıklar kurulması teşvik edilmelidir.

[5] http://www.oecd.org/dataoecd/53/60/37019786.pdf

[6] Aralık 2003 tarihli ve 58/199 sayılı karardır.
(http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf)

5. Kriz iletişim şebekeleri kurulmalı ve bunların acil durumlarda çalışabilir durumda olması için gereken testler yapılmalıdır.

6. Verilerin erişilebilirliğine ilişkin politikaların kritik bilgi altyapılarının korunmasına duyulan ihtiyacı dikkate alması sağlanmalıdır.

7. Kritik bilgi altyapılarına yönelik saldırıların takibi kolaylaştırılmalı ve gerekli hallerde elde edilen bilgiler diğer ülkelerle de paylaşmalıdır.

8. Olaylara müdahale yeteneklerinin geliştirilmesi ve süreklilik ve beklenmedik durum planlarının test edilmesi için gereken eğitim ve tatbikatlar düzenlenmeli, paydaşların da benzer faaliyetlere katılımı teşvik edilmelidir.

9. Kritik bilgi altyapılarına yönelik saldırıların soruşturulabilmesi ve kovuşturulabilmesini, söz konusu işlemlerin gerekli hallerde diğer devletlerle işbirliği halinde yürütülebilmesini teminen gerekli yasal düzenlemeler yapılmalı ve ilgili personelin yeterli eğitim düzeyine sahip olması sağlanmalıdır.

10. Kritik bilgi altyapılarının güvenliğini sağlamak amacıyla, gerekli hallerde, acil durum uyarı sistemleri oluşturma, tehditlere, açıklıklara ve yaşanan olaylara ilişkin bilgi paylaşımında bulunma gibi uluslararası işbirlikleri içinde yer alınmalıdır.

11. Ulusal ve uluslararası araştırma ve geliştirme faaliyetleri ve uluslararası standartlara göre belgelendirilmiş olan güvenlik teknolojilerinin uygulanması teşvik edilmelidir.

Söz konusu ilkeler aynı zamanda G8 Ülkeleri Adalet ve İçişleri Bakanları tarafından 2003 yılında Paris'te kabul edilen "Kritik Bilgi Altyapılarının Korunmasına İlişkin" ilkelerdir.

2.2 BM BİLGİ VE İLETİŞİM TEKNOLOJİLERİ GÖREV GÜCÜ

BM BİT Görev Gücü, Kasım 2001'de BM Ekonomik ve Sosyal Konseyinin talebi üzerine kurulmuş, Milenyum Kalkınma Hedeflerine BİT'in kullanımı ile ulaşma konusunda küresel çapta destek olmayı hedefleyen bir birimdir. Görev Gücü, Eylül 2002'de "Bilgi Güvenliği – Siber Tehditlerin ve Siber Güvenliğin Keşfedilmemiş Bölgelerinde Hayatta Kalabilme Kılavuzu" (Information Security – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security) adlı bir kılavuz yayımlamıştır. Söz konusu kılavuz, bilgi

güvenliği sorununu ve önerilen çözümler, güvenlik olaylarına müdahale mekanizmalarını ve siber ortam güvenlik stratejilerini ele almaktadır. Kılavuz, aynı zamanda, siber ortamda güven ve güvenliğin sağlanabilmesine yönelik en iyi uygulamalardan ve standartlardan da bahsetmektedir.

2.3 İNTERNET YÖNETİŞİM FORUMU

Üçüncü bölümde ele alınan Dünya Bilgi Toplumu Zirvesi süreci sonunda katılımcılar arasında "İnternetin yönetişimi" konusunda mutabakat sağlanamaması üzerine, BM Genel Sekreterliğine, ilgili tüm paydaşların katılımıyla İnternet Yönetişim Forumu (Internet Governance Forum - IGF) [7] adıyla bir forum toplama sorumluluğu verilmiş ve bu forumda genel olarak;

- İnternetin istikrarı, güvenliği, gelişimi, sağlamlığı ve sürekliliğini sağlayacak İnternet yönetişimi ile ilgili politikaların tartışılması,
- İnternet ile ilgili hususların uluslararası kuruluşlara adreslenmesi,
- İlgili paydaşlar arasında işbirliği imkânlarının geliştirilmesi,
- İlgili tüm paydaşlar arasında bilgilerin ve en iyi uygulamaların paylaşılması,
- Gelişmekte olan ülkelerin kapasitelerinin geliştirilmesi (ekonomik, teknik vb.),
- Kritik İnternet altyapılarının iyileştirilmesi,
- Ortaya yeni çıkan sorunlarla ilgili bilgi ve tecrübe paylaşımında bulunulması

hedeflenmiştir.

Her yıl ayrı bir kıtada yapılması planlanan Forum, 2006 yılında Yunanistan'da, 2007 yılında Brezilya'da ve 2008 yılında Hindistan'da düzenlenmiştir. Forumun 2009 yılında Mısır'da, 2010 yılında da Litvanya'da düzenlenmesi planlanmıştır.

[7] http://www.intgovforum.org/

3 ULUSLARARASI TELEKOMÜNİKASYON BİRLİĞİ'NİN ÇALIŞMALARI

Uluslararası Telekomünikasyon Birliği (ITU), esas olarak BİT hakkında çalışmalar yürütmekte ve kamu ve özel sektör kuruluşlarına gelişmekte olan Bilgi ve İletişim Şebekeleri (BİŞ) ve hizmetleri alanında küresel çapta bir merkez sunmakta olan BM ajansıdır. ITU'nun başlıca görevleri;

- Radyo spektrumunun küresel çapta ortak kullanımını koordine etmek,
- Uydu yörüngelerinin tahsisinde uluslararası işbirliğini sağlamak,
- Gelişmekte olan dünyada elektronik haberleşme altyapısının da geliştirilmesini sağlamak,
- Farklı haberleşme sistemleri arasında sorunsuz bağlantılar kurulmasına imkân verecek, dünya çapında kabul gören standartlar oluşturmak ve
- Siber güvenliğin sağlanması gibi güncel konularda çalışmalar yapmaktır.

Merkezi İsviçre'nin Cenevre kentinde bulunan ITU'nun ülkemizin de aralarında bulunduğu 191 devlet bazında üyesi ve 700'den fazla sektör üyesi bulunmaktadır. ITU, özellikle aşağıda özetlenen Dünya Bilgi Toplumu Zirvesi süreciyle birlikte siber güvenlik konusunda etkin rol oynamaya başlamıştır.

3.1 DÜNYA BİLGİ TOPLUMU ZİRVESİ SÜRECİ

2001 yılında, ITU Konseyi, hükümetleri, uluslararası kurum ve kuruluşları, şirketleri ve sivil toplum örgütlerini, geleceğin bilgi toplumu için ortak bir vizyon belirlemek için bir araya getirmek amacıyla Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society - WSIS) adıyla uluslararası bir toplantı düzenlemeyi kararlaştırmıştır. Birleşmiş Milletler Genel Kurulunun 56/183 sayılı kararı ile de onaylanan söz konusu Zirvenin, ilk aşaması Aralık 2003'te Cenevre'de, ikinci aşaması Kasım 2005'te Tunus'ta yapılan konferanslar ile gerçekleştirilmiştir. İnternet eksenli konuların tartışıldığı bu iki konferans sonucunda Cenevre Deklarasyonu, Cenevre Eylem Planı, Tunus Taahhütleri ve Bilgi Toplumu İçin Tunus Gündemi başlıklı dört doküman üzerinde mutabakat sağlanmıştır.

WSIS İlkeler Bildirgesinde, bilgi ve şebeke güvenliği, kimlik doğrulama, tüketici haklarının ve kişisel mahremiyetin korunması gibi hususların bilgi toplumunun gelişiminde ve BİT kullanıcılarının bu teknolojilere duydukları güvenin arttırılmasında birer önkoşul oldukları ifade edilmektedir. Bildirgede, ayrıca, söz konusu önkoşulların yerine getirilebilmesi için, küresel bir siber güvenlik kültürünün, ilgili tüm taraflar ve uluslararası uzman kuruluşlar ile işbirliği içinde, etkin şekilde tanıtılması, geliştirilmesi ve benimsetilmesi gerektiği belirtilmektedir.

WSIS sonunda uluslararası toplumca benimsenen Cenevre Eylem Planında yapılacak çalışmalar 11 ana başlıkta toplanmış ve C5 numaralı **"Bilgi ve İletişim Teknolojilerinin Kullanımında Güven ve Güvenliğin Tesis Edilmesi"** başlığı altındaki eylem maddelerini uygulamaya koyma sorumluluğu ITU'ya verilmiştir. Söz konusu eylem planında yer alan diğer maddeler ve sorumlu kuruluşların listesi EK-1'de sunulmaktadır.

3.2 WSIS SONRASI SÜREÇ

WSIS sonuç dokümanlarında "**Bilgi ve İletişim Teknolojilerinin Kullanımında Güven ve Güvenliğin Tesis Edilmesi"** konusunda görevlendirilen ITU Zirve sonrasında düzenlediği konferanslarda siber güvenlik ile ilgili muhtelif çözüm kararlarını onaylamıştır.

3.2.1 PP-06 Sonuç Raporunda Yayımlanan İlgili Kararlar

Kasım 2006'da Antalya'da düzenlenen ITU Tam Yetkili Temsilciler Konferansı (Plenipotentiary Conference / PP-06) sonrasında yayımlanan sonuç raporunda yer alan 130 ve 149 sayılı kararlar [8] WSIS Eylem Planının C5 numaralı başlığı ile ilgilidir.

- 130 sayılı karar, BİT'in kullanımında güven ve güvenliğin tesis edilmesinde ITU'nun rolünün güçlendirilmesine,

- 149 sayılı karar ise, BİT'in kullanımında güven ve güvenliğin tesis edilmesi ile ilgili tanımlar ve terminoloji üzerinde çalışılmasına ilişkin yapılması gerekenleri ortaya koymaktadır.

[8] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf

3.2.2 WTDC-06 Sonuç Raporunda Yayımlanan İlgili Kararlar

Mart 2006'da Katar'ın Doha şehrinde düzenlenen 4. Dünya Telekomünikasyon Kalkınma Konferansı (World Telecommunication Development Conference/ WTDC-06) sonrasında yayımlanan sonuç raporunda yer alan 45 sayılı karar[9] WSIS Eylem Planının C5 numaralı başlığı ile ilgilidir.

Söz konusu karar, istem dışı elektronik haberleşme ile mücadele başta olmak üzere, siber güvenlik konusunda işbirliğinin geliştirilmesini, siber güvenlik konusunda fikir alışverişinde bulunmak üzere üye ülke temsilcilerinin ve sektör temsilcilerinin katılımıyla toplantılar düzenlenmesini ve bir mutabakat zaptı oluşturulmasını önermektedir.

3.2.3 WTSA-08 Sonuç Raporunda Yayımlanan İlgili Kararlar

Ekim 2008'de Güney Afrika'nın Johannesburg şehrinde düzenlenen Dünya Telekomünikasyon Standardizasyon Genel Kurulu (World Telecommunication Standardization Assembly / WTSA-08) sonrasında yayımlanan sonuç raporunda yer alan 50[10], 51[11] ve 52[12] sayılı kararlar WSIS Eylem Planının C5 numaralı başlığı ile ilgili olup, söz konusu kararlar Ekim 2004'te Brezilya'nın Florianópolis şehrinde düzenlenen WTSA-04 sonrasında yayımlanan aynı sayılı kararların devamı niteliğindedir.

- 50 sayılı karar, ITU-T'nin WSIS siber güvenlik faaliyetlerini ve ITU Genel Sekreterliğinin siber güvenliğe ilişkin olarak başlattığı girişimleri ilgili taraflarla işbirliği halinde sürdürmesini, siber tehditlere karşı savunmaya duyulan ihtiyaç hakkında genel farkındalık düzeyini arttırmasını,

- 51 sayılı karar, ITU-T'nin spam ile mücadeleye ilişkin uluslararası girişimler hakkında bir rapor hazırlamasını, üye ülkelerin ve sektör temsilcilerinin bu çalışmalara katkıda bulunmalarını ve üye ülkelerin ulusal mevzuatlarını spam ile mücadele için gerekli tedbirleri alacak şekilde iyileştirmelerini,

[9] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf
[10] http://www.itu.int/ITU-T/wtsa/resolutions04/Res50E.pdf
[11] http://www.itu.int/ITU-T/wtsa/resolutions04/Res51E.pdf
[12] http://www.itu.int/ITU-T/wtsa/resolutions04/Res52E.pdf

- 52 sayılı karar ise, ITU-T'nin spam ile mücadeleye ilişkin uluslararası girişimler hakkında bir rapor hazırlamasını ve geleceğe dair öneriler sunmasını, üye ülkelerin ve sektör temsilcilerinin bu çalışmalara katkıda bulunmalarını ve üye ülkelerin ulusal mevzuatlarını spam ile mücadele için gerekli tedbirleri alacak şekilde iyileştirmelerini talep etmektedir.

3.3 ITU BİRİMLERİNİN SİBER GÜVENLİK FAALİYETLERİ

3.3.1 ITU Genel Sekreterliğinin Faaliyetleri

3.3.1.1 Küresel Siber Güvenlik Gündemi

ITU Genel Sekreterliği, WSIS sonrasında ITU'ya verilen C5 numaralı başlık altındaki eylem maddelerini uygulamaya koyma sorumluluğuna binaen, 17 Mayıs 2007 tarihinde, bilgi toplumunda güven ve güvenliğin sağlanmasına yönelik uluslararası işbirliğinin nasıl sağlanabileceğine dair bir çerçeve model sunan "Küresel Siber Güvenlik Gündemi"ni [13] (Global Cybersecurity Agenda / GCA) yayımlamıştır.

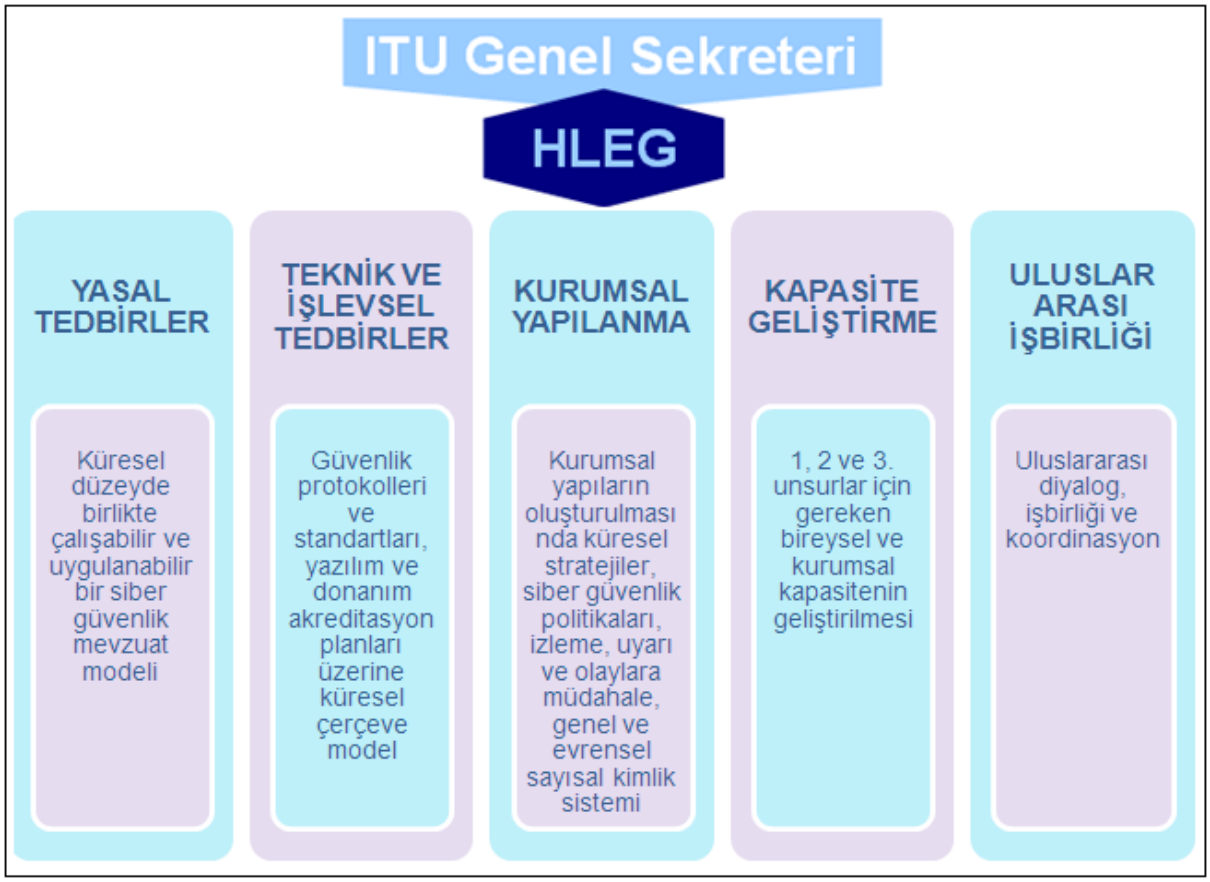
GCA'da vurgulanan 7 ana hedef:

1. Küresel düzeyde uygulanabilir ve mevcut ulusal ve bölgesel mevzuatlara uyumlu bir siber güvenlik mevzuatı geliştirilmesi,
2. Siber güvenlikle ilgili çalışan ulusal ve bölgesel kuruluşların kurulması ve politikaların oluşturulması,
3. Küresel düzeyde kabul gören asgari güvenlik ölçütlerinin ve yazılım ve donanım sistemleri için akreditasyon planlarının oluşturulması,
4. Mevcut ve yeni girişimler arasında uluslararası işbirliğini sağlamak amacıyla izleme, uyarı ve olaylara müdahale için küresel bir çerçeve model kurulması,
5. Evrensel bir sayısal kimlik sisteminin kurulması ve sayısal kimlik bilgilerinin tüm dünyada tanınmasını sağlayan bir yapılanmanın oluşturulması,
6. Sektörler arasında siber güvenlik konusunda gerçekleşen bilgi alışverişini sağlamak üzere kurumsal kapasitenin geliştirilmesi,
7. Tüm bu konularda uluslararası işbirliği, diyalog ve koordinasyonun tesis edilmesidir.

[13] http://www.itu.int/osg/csd/cybersecurity/gca/index.html

Tüm bu faaliyetlerin yürütülmesinde ITU Genel Sekreterliğine yardımcı olmak üzere; dünya çapında kamu kurum ve kuruluşlarında, özel sektörde, bölgesel veya uluslararası kuruluşlarda, araştırma merkezlerinde veya akademik kuruluşlarda görev yapan, siber güvenlik ile ilgili hususlarda yüksek düzeyde bilgili uzmanlardan oluşan bir "Yüksek Seviyeli Uzmanlar Grubu" (High Level Experts Group / HLEG) kurulmuştur. HLEG tarafından hazırlanan Küresel Stratejik Rapor (2008) siber güvenliğin beş ana unsurunu ayrıntılı şekilde açıklamaktadır. Küresel siber güvenliğin beş ana unsuru Şekil 1'de görüntülenmektedir.

Şekil 1. HLEG ve Küresel Siber Güvenliğin Ana Unsurları



3.3.1.2 Siber Güvenlik Kapısı

Siber Güvenlik Kapısı (Cybersecurity Gateway) [14], ITU Genel Sekreterliği tarafından koordine edilen ve kamu ve özel sektör kuruluşlarını, sivil toplum kuruluşlarını, akademik kuruluşları, uluslararası ve bölgesel kuruluşları bir araya getiren bir platformdur. Söz konusu platformda gerek ITU'nun siber güvenlik konusundaki faaliyetleri hakkında bilgiler, gerekse

[14] http://www.cybersecurity-gateway.org/

siber güvenliğin beş ana unsuru ile ilgili uluslararası, bölgesel ve ulusal çalışmalar ve yayınlar paylaşılmaktadır.

3.3.1.3 Siber Uzayda Çocukların Korunması Programı

Her yıl 17 Mayıs tarihinde kutlanan Dünya Telekomünikasyon ve Bilgi Toplumu Gününün 2009 yılı teması da "Siber Uzayda Çocukların Korunması" olmuştur. Bu çerçevede, Genel Sekreterlikçe Siber Uzayda Çocukların Korunması Programı geliştirilmiş olup, bu programın temel hedefleri;

- İnternet ortamında çocuklara yönelik riskleri ve açıklıkları belirlemek,
- Farklı kanalları kullanarak söz konusu risklerle ve açıklıklarla ilgili farkındalık yaratmak,
- Kamu ve özel sektör kuruluşlarının ve eğitimcilerin söz konusu riskleri ve açıklıkları asgari düzeye indirebilmelerine yardımcı olacak araçlar geliştirmek,
- Uluslararası stratejik ortaklıklar kurmak suretiyle bilgi ve tecrübe paylaşımında bulunmaktır.

3.3.1.4 IMPACT ile İşbirliği

ITU, küresel toplumun siber tehditlere ilişkin önleme, savunma ve karşı koyma kapasitesini geliştirmeyi hedefleyen uluslararası bir kamu-özel sektör girişimi olan Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (International Multilateral Partnership Against Cyber Threats /IMPACT) ile ortak çalışmalar yürütmektedir. Söz konusu çalışmalar,

- Siber tehditlerle ilgili küresel bilginin gerçek zamanlı olarak toplanmasına, analiz edilmesine ve dağıtılmasına,
- Küresel siber tehditlere karşı erken uyarı ve acil durum müdahale sistemi oluşturulmasına,
- Siber güvenliğin teknik, yasal ve politik yönleri ile ilgili kapasitenin geliştirilmesine

katkı sağlamaktadır.

IMPACT'in Malezya'nın Cyberjaya şehrinde bulunan merkezi, aynı zamanda GCA'nın fiziksel yerleşkesi konumundadır.

3.3.2 ITU - Telekomünikasyon Geliştirme Sektörünün Faaliyetleri

ITU-Telekomünikasyon Geliştirme Sektörü (ITU-D) bünyesinde, gelişmekte olan ülkelerde BİT-tabanlı şebekelerin, hizmetlerin ve uygulamaların kullanımlarını arttırmak ve bu ülkelerin siber güvenlik çalışmalarına ağırlık vermelerini sağlamak suretiyle sayısal uçurumu kapatabilmelerine yardımcı olmaya odaklı faaliyetler yürütmek üzere BİT Uygulamaları ve Siber Güvenlik Birimi kurulmuştur. Söz konusu birim, WTDC-06'da benimsenen Doha Eylem Planının 3 numaralı programını yürütmekle sorumlu olup, siber güvenliğin yaygınlaştırılması, e-stratejiler, BİT uygulamaları, İnternet ve IP şebekelerinin geliştirilmesi gibi konularda faaliyetlerini sürdürmektedir.

BİT Uygulamaları ve Siber Güvenlik Birimi tarafından;

- Gelişmekte olan Ülkeler için Siber Güvenlik Rehberi (2006, 2007)
- Gelişmekte olan Ülkeleri Destekleyici Siber Güvenlik Çalışma Programı 2007-2009
- Ulusal Siber Güvenlik/Kritik Bilgi ve Altyapıların Korunması Kendini Değerlendirme Kılavuzu (2008)
- Siber Suç Mevzuatı Hazırlama Rehberi (2009)
- Siber Suçları Anlamak: Gelişmekte Olan Ülkeler için Rehber (2009)

başlıklı dokümanlar hazırlanmış olup, bunlara Siber Güvenlik Kapısından erişilebilmektedir.

3.3.3 ITU - Telekomünikasyon Standardizasyon Sektörünün Faaliyetleri

ITU-Telekomünikasyon Standardizasyon Sektörü (ITU-T) bünyesinde, güvenlik ile ilgili faaliyetler yürüten çeşitli çalışma grupları (study groups / SG) bulunmaktadır. Söz konusu çalışma gruplarından;

- SG 17 elektronik haberleşme güvenliği ve siber güvenlikten sorumlu ana grup olup,
  - Güvenlik çalışmalarının koordinasyonu ve önceliklendirilmesi,
  - Güvenlik konusunda farkındalığın arttırılması,
  - Temel güvenlik tavsiye kararlarının geliştirilmesi,
- SG 2 kullanıcıların bakış açısından güvenlik ihtiyaçlarının tanımlanması,
- SG 4 şebeke yönetiminde güvenlik,
- SG 9 kablolu dağıtım sistemleri için güvenlik mekanizmaları oluşturulması,
- SG 13 yeni nesil şebekeler için güvenlik çerçeve modeli tanımlanması,

- SG 16 yeni nesil şebekelerde çoklu ortam uygulamalarının güvenliği

konularından sorumludur.

SG 17 tarafından hazırlanan siber güvenlik ile ilgili raporlardan bazıları şunlardır:

- Güvenlik Mimarisi - X.805: Uçtan uca haberleşme
- Güvenlik Yönetim Sistemi - X.1051: Risk değerlendirmesi, varlıkların belirlenmesi ve uygulama özellikleri
- Mobil Güvenlik - X.1121, X.1122: Mobil uçtan uca haberleşme
- Açık Anahtar ve Nitelikli Sertifika Modelleri - X.509
- Siber Güvenliğe Genel Bakış - X.1205
- Elektronik Haberleşme ve Bilgi Teknolojilerinde Güvenlik (2006)
- BİT Güvenlik Standartları Kılavuzu (2007)
- ITU-T Onaylı Güvenlik Tanımları (2009)

3.3.4 ITU - Radyokomünikasyon Sektörünün Faaliyetleri

ITU-Radyokomünikasyon Sektörü (ITU-R) bünyesinde siber güvenlik ile ilgili herhangi bir birim veya çalışma grubu bulunmamakla birlikte, sadece aşağıda listelenen tavsiye kararlarında elektronik haberleşme güvenliği ile ilgili hususlara yer verildiği görülmektedir:

- S.1250: Sabit uydu hizmetinde bulunan SDH ulaşım şebekelerini oluşturan sayısal uydu sistemleri için şebeke yönetim mimarisi
- S.1711: Uydu şebekelerinde iletim denetimi protokolünün performans iyileştirmeleri
- 1078: IMT-2000 için güvenlik prensipleri
- 1223: IMT-2000 için güvenlik mekanizmalarının değerlendirilmesi
- 1457: IMT-2000 güvenlik mekanizmaları
- M.1645: IMT-2000 ve arkasındaki sistemlerin gelişim modeli ve temel hedefleri
- M.2063: IMT-2000'de yazılım tanımlı telsizler, IMT-2000'in gelişimi ve IMT-2000'in arkasındaki sistemler

4 EKONOMİK İŞBİRLİĞİ VE KALKINMA TEŞKİLATI'NIN ÇALIŞMALARI

1960 yılında kurulan, tüm gelişmiş ülkeler ve ülkemiz dâhil 30 üyesi bulunan Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organization for Economic Cooperation and Development - OECD), ekonomiden çevreye, tarımdan teknolojiye kadar çok geniş bir alanda faaliyetler yürüten uluslararası bir kuruluştur. Siber güvenlik konusuna büyük önem veren OECD, bu konudaki çalışmalarını 1980'den bu yana sürdürmektedir.

4.1 OECD BÜNYESİNDEKİ İLGİLİ BİRİMLER

OECD bünyesinde siber güvenlik ile ilgili faaliyetleri yürüten ana birim, Bilim, Teknoloji ve Sanayi Direktörlüğüne (Directorate for Science, Technology and Industry - STI) bağlı olarak çalışan Bilgi, Bilgisayar ve İletişim Politikaları Komitesidir (Committee for Information, Computer and Communications Policy - ICCP)[15]. ICCP, temelde/esas itibariyle BİT'in sağladığı avantajlardan azami düzeyde yararlanmayı teminen politikalar geliştirmeyi hedeflemektedir. Bu amaçla, OECD üyeleri başta olmak üzere tüm ülkelere kapsamlı ve ileriye dönük politikalar geliştirme konusunda rehberlik etmek üzere, BİT'in gelişimini ve bunların sosyal ve ekonomik etkilerini analiz etmekte; ülkelerin, kamu ve özel sektör kuruluşlarının ve bireylerin siber güvenlik düzeyini geliştirmek amacıyla en iyi uygulama örnekleri, araştırma raporları, kılavuzlar, istatistikler vs. hazırlamakta ve yayımlamaktadır.

ICCP altında EK-2'de verilen değişik çalışma grupları yer almaktadır. Bu gruplardan biri olan Bilgi Güvenliği ve Gizlilik Çalışma Grubu (Working Party on Information Security and Privacy - WPISP) [16], İnternet ortamında güveni ve güvenliği arttırmak için yenilikçi politikalar oluşturmaya odaklanmıştır

Ayrıca, ICCP bünyesinde istem dışı e-posta ile mücadelede ulusal stratejilerin geliştirilmesini destekleyici faaliyetler yürütmesi amacıyla İstem Dışı E-posta ile Mücadele Görev Gücü (Anti Spam Task Force) adlı özel bir birim oluşturulmuştur.

[15] ICCP İnternet sayfası: www.oecd.org/sti/ict
[16] WPISP İnternet sayfası: www.oecd.org/sti/security-privacy

4.2 ICCP FAALİYETLERİ

ICCP'nin siber güvenlik konusunda yürüttüğü en önemli faaliyetlerden biri **Kişisel Verilerin Gizliliğinin Korunması ve Sınırlar Ötesi İletilmesine Dair Kılavuz**dur (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) [17]. Bu kılavuz ilk olarak 1980 yılında hazırlanmış, 2003 yılında da revize edilerek geliştirilmiştir. Kılavuz, küresel şebekelerde kişisel verilerin ve gizliliğin korunmasına yönelik temel prensipleri belirleyen uluslararası bir mutabakat metni niteliğindedir.

Bir başka önemli çalışma olan **Bilgi Sistemleri ve Şebekelerinin Güvenliğine Dair Kılavuz** (OECD Guidelines for the Security of Information Systems and Networks) [18] ise, siber terörizm, virüsler ve bilgisayar korsanlığı gibi iç ve dış tehditler ile mücadeleye ilişkin politika ve tedbir önerilerinde bulunarak bir küresel güvenlik kültürü oluşturmayı amaçlamaktadır. İlk sürümü 1992 yılında hazırlanan kılavuz, 1997 yılında revize edilmiş ve 11 Eylül saldırılarının ardından 2002 yılında tekrar gözden geçirilerek "Bilgi Sistemleri ve Şebekelerinin Güvenliğine Dair Kılavuz: Güvenlik Kültürüne Doğru" adıyla bugünkü halini almıştır. Söz konusu Kılavuz, OECD'nin siber güvenlik ve kritik bilgi ve altyapıların korunması konularında yaptığı en önemli çalışma olarak görülmektedir. Kılavuzun 2002 sürümü, BM Genel Kurulu tarafından alınan "Küresel Siber Güvenlik Kültürünün Oluşturulması" başlıklı kararı esas almaktadır.

Bilgi Sistemleri ve Şebekelerinin Güvenliğine Dair Kılavuz;

- Güvenlik kültürünün ilgili tüm paydaşlar ve kullanıcılar tarafından benimsenmesine duyulan ihtiyacı vurgulamakta,
- Devletleri, kamu ve özel sektör kuruluşlarını, sivil toplumu ve kullanıcıları siber güvenlik ile ilgili faaliyetlere aktif katılım sağlamaya çağırmakta,
- Bilgi güvenliğinin sürekli değişen yapısına, dolayısıyla dinamik risk analizine duyulan ihtiyaca dikkat çekmekte ve
- Siber güvenliğin insani boyutunu ele almaktadır.

[17] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

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

Kılavuzda bilgi güvenliğinin birbirini tamamlayan 9 prensibine yer verilmektedir:

1. Bilgi Sistemlerinin (BS) ve Bilgi Şebekelerinin (BŞ) güvenliğine duyulan ihtiyaca ve mevcut kapasiteye dair farkındalık
2. BS ve BŞ güvenliğinde sorumluluk ve hesap verebilirlik
3. Güvenlik ihlallerine zamanında ve işbirliği halinde tepki verebilme
4. Üçüncü tarafların haklarına saygılı davranma
5. BS ve BŞ güvenliğinde, demokratik toplum düzeninin açıklık, şeffaflık, kişisel mahremiyetin korunması, ifade özgürlüğü ve iletişimin gizliliği gibi temel değerlerine uyum sağlama
6. Mevcut ve olası tehditleri ve açıklıkları hesaba katarak, teknik, fiziksel ve insani faktörler gibi temel hususları kapsayacak boyutta risk değerlendirmesi yapma
7. Güvenliği BS ve BŞ'nin temel bir unsuru olarak görme ve tehditler ve açıklıklardan kaynaklanan zararı en aza indirmek için gereken çözümleri tasarlama ve hayata geçirme
8. Dinamik ve kapsamlı bir güvenlik yönetimi anlayışı benimseme
9. Sürekli olarak BS ve BŞ güvenliğini tüm boyutlarını gözden geçirme ve yeniden değerlendirme

Kılavuz, ayrıca, ülkelerin siber güvenliğin sağlanmasına ve kritik bilgi ve altyapıların korunmasına ilişkin ulusal politikalarını uygularken, aşağıdaki bileşenlere önem vermelerini tavsiye etmektedir:

- Ulusal strateji
- Yasal temeller
- Olaylara müdahale kapasitesi
- Kamu – özel sektör işbirliği
- Güvenlik kültürü
- Bilgi paylaşma mekanizmaları
- Risk yönetimi yaklaşımı

İstem Dışı E-posta ile Mücadele Görev Gücü, 2006 yılında İstem Dışı E-posta ile Mücadele Kılavuzunu (OECD Anti-Spam Toolkit) [19] ve İstem Dışı E-posta ile Mücadele Yasalarının

[19] http://www.oecd-antispam.org/article.php3?id_article=265

Uygulanmasında Uluslararası İşbirliğine Yönelik Tavsiye Kararını (OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam) [20] hazırlamış ve yayımlamıştır.

İstem Dışı E-posta ile Mücadele Kılavuzu, OECD üyeleri başta olmak üzere tüm ülkelere istem dışı e-posta ile mücadelelerinde kapsamlı bir politika yaklaşımı ve tutarlı bir çerçeve model sunmak amacıyla hazırlanmıştır. Kılavuz, birbiriyle ilişkili 8 ana unsura dikkat çekmektedir:

1. Düzenleyici yaklaşımlar
2. Yasaların uygulamaya konması ile ilgili hususlar
3. Özel sektör girişimleri
4. Teknik çözümler
5. Eğitim ve farkındalık
6. İstem dışı e-postaya karşı işbirliğine dayalı ortaklıklar
7. İstem dışı e-posta istatistikleri
8. Küresel işbirliği

İstem Dışı E-posta ile Mücadele Yasalarının Uygulanmasında Uluslararası İşbirliğine Yönelik Tavsiye Kararı ise, üye ülkelerin;

- Kendi ulusal çerçeve modellerini oluşturmak,
- İşbirliği yetkinliklerini ve süreçlerini geliştirmek ve
- İlgili özel sektör kuruluşları ile işbirliğinde bulunmak

suretiyle, istem dışı e-posta ile ilgili yasaların uygulanmasından sorumlu kuruluşları arasında daha yakın, hızlı ve etkin bir işbirliği kurmalarını tavsiye etmektedir.

[20] http://www.oecd-antispam.org/article.php3?id_article=237

4.3 ÖNEMLİ ETKİNLİKLER

OECD, 2002 yılında "Bilgi Sistemleri ve Şebekelerinin Güvenliğine Dair Kılavuz: Güvenlik Kültürüne Doğru" adlı kılavuzu yayımlamasından bu yana, ülkeleri güvenlik kültürünü hayata geçirme sürecinde desteklemek amacıyla pek çok çalışma yürütmektedir.

Söz konusu çalışmalardan biri 2003 yılının Ocak ayında APEC (Asia Pacific Economic Cooperation - Asya Pasifik Ekonomik İşbirliği Teşkilatı) ile birlikte düzenlenen "Sayısal Ekonomi için Politika Modelleri Küresel Forumu"dur (Global Forum on Policy Frameworks for the Digital Economy). Aynı yıl Ekim ayında OECD Bilgi Sistemleri ve Şebekelerinin Güvenliği Küresel Forumu (Global Forum on Information Systems and Network Security) adıyla bir başka etkinlik daha düzenlemiştir. Her iki Forum da;

- Gerek kişisel ve kurumsal bilgilerin, gerekse kritik altyapıların korunması için BS ve BŞ güvenliği hakkında var olan farkındalığı arttırmayı,
- BS güvenliğine yönelik politika modelleri üzerinde farkındalık ve mutabakat oluşturmayı,
- Teknik çözümlerin ve güvenlik standartlarının BS ve BŞ güvenliğinde kullanımını teşvik etmeyi,
- O tarihte yaklaşmakta olan Dünya Bilgi Toplumu Zirvesine girdi sağlamayı amaçlamıştır.

Ayrıca, 2005 yılının Eylül ayında Seul'de (Güney Kore) Bilgi Sistemleri ve Ağlarının Güvenliği konulu OECD-APEC Çalıştayı [21] düzenlenmiştir. Çalıştay kapsamında tartışılan başlıca konular; casus programlar ve bunlarla mücadele, küresel olaylara müdahalenin teşvik edilmesi, ortaya çıkan yeni güvenlik tehditleri ve bunların belirlenmesi için geliştirilen teknolojiler, araştırma ve geliştirme faaliyetlerinin önemi ve bilgi sistemleri ve ağlarının güvenliğinin ve yönetiminin sağlanması alanlarında politika yaklaşımlarının belirlenmesi ve bu konudaki yasal düzenlemelerin karşılaştırılmasıdır.

[21] http://www.oecd.org/document/25/0,3343,en_2649_34255_35481241_1_1_1_1,00.html

4.4 "GÜVENLİK KÜLTÜRÜ" İNTERNET SİTESİ

WPISP tarafından 2003 yılında kurulan "Güvenlik Kültürü"[22] adlı İnternet sitesi, tüm ülkelerin birbirleri ile güvenlik kültürünün tesisine ilişkin politikalarını ve en iyi uygulamalarını paylaşmalarına imkân sunan bir platform niteliğindedir. Söz konusu sitede OECD ve benzeri uluslararası kuruluşlar ile üye ülkelerin siber güvenlik ile ilgili çalışmaları yer almaktadır.

5 AVRUPA BİRLİĞİ'NİN ÇALIŞMALARI

İkinci Dünya Savaşı sonrasında Avrupa ülkeleri arasında oluşan ayrılığı gidermek ve ülkeler arasında kalıcı bir barışı sağlamak amacıyla ekonomik ve politik bir birlik oluşturmak hedefiyle Avrupa Ekonomik Topluluğu (AET) kurulmuştur. Kurulduğu günden bu yana çeşitli aşamalardan geçen AET, günümüzde Avrupa Birliği (AB) adıyla sadece ekonomik ve politik değil, sosyal ve kültürel alanlarda da faaliyetler yürüten ve 27 üyesi bulunan bölgesel bir kuruluş konumundadır. Hâlihazırda ülkemizin de AB'ye tam üyelik müzakere süreci devam etmektedir.

AB, siber güvenliği, bilgi toplumunun önemli bir bileşeni olarak ele almakta ve şebeke güvenliği, İnternet, elektronik ticaret, kişisel verilerin korunması, fikri haklar gibi konulara ilişkin araştırma, geliştirme ve düzenleme faaliyetleri yürütmektedir. AB, bir yandan BİT gelişimini destekleyici araştırma ve geliştirme projeleri yürüterek, bir yandan da AB vatandaşlarının söz konusu teknolojilerden mümkün olduğunca yararlanmalarını sağlamak amacıyla kişisel verilerin korunması ve şebeke güvenliği gibi hususlarda tavsiye kararları ve direktifler oluşturmak suretiyle bilgi toplumuna dönüşüme katkıda bulunmaktadır.

5.1 AB DÜZENLEMELERİ [23]

AB tarafından hazırlanan ve kısmen veya tamamen siber güvenliğin sağlanmasına yönelik hükümler içeren temel direktifler şunlardır:

- 1995/46/EC sayılı Kişisel Verilerin Korunması Direktifi

[22] http://www.oecd.org/sti/cultureofsecurity
[23] Düzenlemelere http://eur-lex.europa.eu/en/legis/latest/chap132060.htm adresinden erişilebilmektedir.

- 1999/93/EC sayılı Elektronik İmza Direktifi
- 2000/31/EC sayılı Elektronik Ticaret Direktifi
- 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Gizliliğin Korunması Direktifi
- 2006/24/EC sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına İlişkin Direktif

Direktiflerin yanı sıra, AB'nin siber güvenliğin sağlanması ile ilgili almış olduğu bazı tavsiye kararları da bulunmaktadır. Bunlar;

- Avrupa Birliği Konseyi ve üye ülke temsilcileri tarafından alınan 17 Şubat 1997 tarihli İnternet üzerindeki yasadışı içerik ile ilgili tavsiye kararı,

- Avrupa Komisyonu tarafından alınan 25 Ocak 1999 tarihli küresel şebekelerde yasadışı ve zararlı içerik ile mücadele etmek suretiyle İnternetin daha güvenli kullanımını sağlamaya yönelik bir kamusal eylem planı oluşturulmasına dair tavsiye kararı,

- Avrupa Birliği Konseyi tarafından alınan 18 Şubat 2003 tarihli şebeke ve bilgi güvenliği kültürüne ilişkin Avrupa Birliği yaklaşımı ile ilgili tavsiye kararı,

- Avrupa Birliği Konseyi tarafından alınan 24 Şubat 2005 tarihli bilgi sistemlerine yönelik saldırılara ilişkin çerçeve kararı, (Üye ülkeleri, bilgi sistemlerine ve bilgiye yetkisiz erişim ve müdahale fiillerini suç olarak düzenlemeye, söz konusu fiilleri etkin, makul ve caydırıcı şekilde cezalandırmaya ve işbirliğini güçlendirmek amacıyla 7 gün 24 saat ulaşılabilir temas noktaları oluşturmaya çağırmaktadır.)

- Avrupa Birliği Konseyi tarafından alınan 22 Mart 2007 tarihli Avrupa'da güvenli bir bilgi toplumu oluşturma stratejisine ilişkin tavsiye kararı,

- Avrupa Parlamentosu ve Konseyi tarafından alınan 16 Aralık 2008 tarihli İnterneti ve diğer iletişim teknolojilerini kullanan çocukları korumaya yönelik bir kamusal program oluşturulmasına dair tavsiye kararıdır.

5.2 AB PROJELERİ, PROGRAMLARI VE DİĞER FAALİYETLERİ

AB, siber güvenliğin sağlanması ve kritik bilgi ve altyapıların korunması için alınabilecek olası yasal, teknik ve idari tedbirleri belirlemek amacıyla;

- Bilgi Toplumu Teknolojileri ve Avrupa Güvenlik Araştırma Programı
- Kritik Bilgi Altyapıları Araştırma Koordinasyon Projesi
- Avrupa Kritik Altyapıların Korunması Programı (European Programme for Critical Infrastructure Protection - EPCIP)

gibi projeler ve programlar yürütmekte ve AB üyesi veya aday ülkelerin yürütmekte olduğu pek çok projeyi desteklemektedir.

EPCIP, Avrupa Komisyonu tarafından 17 Kasım 2005 tarihinde yayımlanan kritik altyapıların korunması ile ilgili "yeşil kitap"[24] ile başlatılan, AB üyesi ülkelerin kritik altyapıların korunmasına yönelik çalışmalarının ortak bir çerçeve etrafında koordine edilmesini ve etkin uyarı ve müdahale sistemlerinin oluşturulmasını amaçlayan bir programdır. Söz konusu raporda, EPCIP'in etkin ve tutarlı şekilde uygulanabilmesini teminen, üye ülkelerin tek bir denetleme organı oluşturmaları ve kendi ulusal kritik bilgi ve altyapılarının korunması programlarını EPCIP modeline dayandırmaları istenmektedir.

EPCIP'in temel ilkeleri yetki devri, bütünleyicilik, gizlilik, orantılılık ve paydaşlar arası işbirliği olarak belirlenmiştir. EPCIP'e göre Avrupa'daki;

- Enerji
- Nükleer ve kimyasal sanayi
- Bilgi ve iletişim teknolojileri
- Temel kamu hizmetleri
- Su
- Gıda
- Sağlık
- Finans
- Ulaşım

[24] Avrupa Toplulukları Komisyonu, Avrupa Kritik Altyapıların Korunması Programı Raporu, COM(2005) 576, Brüksel, 17.11.2005, http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf

- Uzay teknolojileri
- Araştırma tesisleri

sektörleri tarafından işletilen altyapılar kritik altyapılar olarak kabul edilmektedir.

Ayrıca, AB tarafından EPCIP dâhilinde oluşturulan Kritik Altyapı Uyarı Bilgi Ağı (Critical Infrastructure Warning Information Network) da siber tehditler, kritik altyapılarda bulunan açıklıklar, var olan risklere karşı alınabilecek tedbirler ve izlenebilecek stratejiler hakkında bilgi paylaşımına imkân veren bir platformdur.

Yine AB Komisyonu tarafından Mayıs 2007'de kimlik bilgileri hırsızlığına karşı "Siber Suçlarla Mücadele Üzerine Genel Bir Politikaya Doğru" adlı bir girişim başlatılmış, Kasım 2007'de yapılan bir AB uzmanlar toplantısında ise söz konusu 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 uluslararası işbirliğine dayanmaktadır."

5.3 AVRUPA ŞEBEKE VE BİLGİ GÜVENLİĞİ AJANSI

Avrupa Şebeke ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency - ENISA) [25], 2004/460/EC sayılı ve 10 Mart 2004 tarihli düzenleme ile AB bünyesinde kurulan bir uzmanlık kuruluşudur. ENISA'nın başlıca görevleri;

- AB'nin diğer kuruluşlarına, AB üyesi ülkelere ve iş dünyasına bilgi güvenliği konusunda tavsiyelerde bulunmak,
- Avrupa'daki güvenlik olayları ve artan riskler hakkında bilgi toplamak ve analiz yapmak,
- En iyi uygulamalar hakkında bilgi paylaşımına imkân sağlamak,

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

- AB'nin bilgi güvenliği tehditlerine ilişkin risk değerlendirme ve risk yönetimi kapasitesini geliştirmek,
- Bilgi güvenliği alanındaki paydaşlar arasında farkındalığı arttırmak ve işbirliğini geliştirmektir.

ENISA, ayrıca, AB üyesi veya adayı ülkelerde oluşturulan ulusal Bilgisayar Olaylarına Müdahale Ekiplerine (Computer Emergency Response Team - CERT) eğitim ve uzmanlık desteği de vermektedir. Ülkemizde 2006–2010 Bilgi Toplumu Stratejisi Eylem Planının 88. maddesine istinaden TÜBİTAK – UEKAE tarafından oluşturulan TR-BOME[26] ve ulusal akademik ağ kapsamında TÜBİTAK ULAKBİM tarafından kurulan Ulak-CSIRT [27] de ENISA tarafından akredite edilmiş durumdadır.

6 AVRUPA KONSEYİ'NİN ÇALIŞMALARI

Hâlihazırda ülkemizin de aralarında bulunduğu 47 üyesi bulunan Avrupa Konseyi (AK), 1949 yılından beri toplanan ve özellikle Avrupa'da istikrarın, ekonomik refahın ve sosyal bağlılığın korunması için gereken temel unsurlar olarak kabul ettiği insan hakları, demokrasi, eğitim ve kültür alanlarında Avrupa çapında anlaşmalar kabul eden bölgesel bir kuruluştur. Dolayısıyla, AK, siber güvenlik konusunu da söz konusu unsurlar bağlamında ele almakta ve bu yönde faaliyetler yürütmektedir.

6.1 AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

AK'nin siber güvenlik konusunda gerçekleştirmiş olduğu en önemli çalışma Avrupa Konseyi Siber Suç Sözleşmesidir (Council of Europe Convention on Cybercrime) [28]. 2001 yılının Kasım ayında Budapeşte'de imzaya açılan ve 2004 yılının Temmuz ayında yürürlüğe giren söz konusu Sözleşme, İnternet veya diğer bilgisayar şebekeleri yoluyla işlenen suçlarla mücadele konusunda uluslararası boyutta atılmış ilk ve en önemli adım olup, Dünya Bilgi Toplumu Zirvesi'nde de bölgesel bir girişim olarak kabul görmüştür.

[26] http://www.tr-cert.gov.tr
[27] http://csirt.ulakbim.gov.tr/
[28] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

AK Siber Suç Sözleşmesinin temel hedefi gereken yasal tedbirleri almak ve uluslararası işbirliğini teşvik etmek suretiyle toplumun siber suçlara karşı korunmasını amaçlayan ortak bir ceza politikası geliştirmektir. Bu sözleşmeye taraf olan ülkeler, sözleşmede suç olarak tanımlanan fiillerin, kendi ulusal mevzuatlarında da suç olarak tanımlanmasını sağlamayı ve bu suçların soruşturulması ve kovuşturulması için gereken tüm yasal tedbirleri almayı ve işlevsel araçları tesis etmeyi kabul etmektedirler.

AK Siber Suç Sözleşmesi, siber suçları;

1. Bilgisayar sistemlerinin ve bilginin gizlilik, bütünlük ve erişilebilirliğini hedef alan suçlar
2. Bilgisayarla ilgili suçlar
3. İçerikle ilgili suçlar
4. Telif ve benzeri hakların ihlali ile ilgili suçlar

olarak sınıflandırmaktadır.

Siber güvenlik ile doğrudan ilişkili olan suçlar ilk iki grupta yer almakta olup, bunlar;

- Bilgisayar sistemlerine ve bu sistemlerde saklanan verilere yetkisiz erişim ve müdahale,
- Bilgisayarların kötüye kullanımı,
- Bilgisayar yoluyla sahtecilik,
- Bilgisayar yoluyla dolandırıcılık

olarak sayılmaktadır.

Ayrıca, Avrupa Konseyi tarafından 28 Ocak 1981'de "Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme" (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) [29] kabul edilmiştir. Avrupa Konseyi üyesi olmayan ülkelerin de katılımına açık olan sözleşme, gerek kamu sektöründe, gerekse özel sektörde geçerli olmak üzere verilerin korunması alanında kabul edilmiş olan uluslararası hukukun ilk bağlayıcı sözleşmesidir. Sözleşmenin 4 üncü maddesinde, ülkelere, sözleşmeyi onaylamadan önce ulusal mevzuatlarında yapacakları yasal düzenlemeler ile, bu sözleşmede öngörülen temel ilkeleri yerine getirme yükümlülüğü getirilmektedir. Ülkemizde kişisel verilerin korunmasına dair yasal düzenleme mevcut olmadığından, sözleşme imzalanmış olmasına rağmen henüz onaylanmamıştır.

[29] http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm

Ülkemizin de siber güvenlik konusunda yasal kapasitesinin geliştirilmesini ve uluslararası işbirliğinin sağlanmasını teminen, öncelikli ve ivedi olarak Avrupa Konseyi Siber Suç Sözleşmesine taraf olması gerektiği değerlendirilmektedir.

7 SONUÇ

Günümüzde, toplumların bilgi toplumuna dönüşüm faaliyetleri ile bireylerin, kurumların ve ülkelerin İnternet başta olmak üzere BİT'e olan bağımlılığı giderek artmaktadır. Son derece bağımlı hale gelinen İnternetin sınır tanımayan küresel yapısı ve beraberinde getirdiği küresel bağlantılılık ise pek çok güvenlik açığı oluşturmakta ve siber tehditlere zemin hazırlamaktadır. Bu bağlamda, söz konusu siber tehditlerin bilgi toplumuna dönüşüm yolunda en önemli engel olduğu uluslararası kuruluşlarca da çok iyi anlaşılmıştır ve bu kuruluşlardan pek çoğu siber güvenliğin sağlanması konusunda ciddi faaliyetler yürütmeye ve organizasyonlar düzenlemeye başlamışlardır.

Ülkemizde ise her geçen gün gerek elektronik haberleşme altyapısının iyileştirilmesi, gerekse rekabetçi bir sektör yönünde ilerlemeler kat edilmesi; bu çerçevede de her geçen gün elektronik ortamı kullanan vatandaş sayısının artması ve bilgi toplumuna dönüşüm noktasında dünyada örnek olabilecek e-devlet projelerinin hayata geçirilmesi dolayısıyla siber güvenlik konusu ihmal edilemeyecek derecede önemli hale gelmiştir.

Bilgi Teknolojileri ve İletişim Kurumu (BTK), kurulduğu 2000 yılından bu yana elektronik haberleşme sektörüne yönelik pek çok düzenleyici faaliyetin yanı sıra, sektörün güvenliğine yönelik çalışmalar da yürütmektedir. Kasım 2006'da Antalya'da düzenlenen PP-06'da BTK ülkemiz adına "Sibergüvenlik ve Spam ile Mücadele'de İşbirliği'nin Gerçekleştirilmesi" konulu bir teklif sunmuştur. Söz konusu teklif "Bilgi ve Haberleşme Teknolojilerinin Kullanımında Güven ve Güvenliğin Tesisinde ITU'nun Rolünün Arttırılması" konulu ve 130 sayılı Çözüm Kararı ile birlikte Kurulmuş olan "Res130+TUR-2" alt çalışma grubunda görüşülmüş, söz konusu Çözüm Kararı içerisine eklenmiş ve PP-06 sonuç dokümanları arasında 130 sayılı Çözüm Kararı olarak yayınlanmıştır.

Ayrıca BTK 2006 yılından bu yana düzenlenen tüm IGF'lere katılım ve katkı sağlamakta, panellere iştirak etmekte ve sunumlar yapmaktadır. Hindistan'da yapılan üçüncü IGF'in "En İyi Uygulama" oturumlarından birinin ülkemize tahsis edilmesi sağlanmış ve bu oturumda BTK moderatörlüğünde, ilgili paydaşların katılımıyla Ülkemizdeki e-dönüşüm çalışmaları ve bu çalışmalarda sivil toplumun rolü, başarılı e-devlet projeleri ve mobil imza konularında sunumlar yapılmış, ilgili taraflarla bilgi ve tecrübe paylaşımında bulunulmuştur.

2009 yılında Mısırda yapılacak olan Forum içinde aktif katılım planlanmış ve

- 108 nolu "IPv6 Politikaları ve Geçiş"
- 194 nolu "İzleme, Uyarı ve Olay Yönetimi"
- 204 nolu "Ülke Kodu Üst Düzey Alan Adlarının Yönetimi"
- 245 nolu "İnternet Ortamında İfade Özgürlüğü ve Gizliliğin Dengelenmesi"

başlıklı çalıştaylarda BTK ve TÜBİTAK'tan temsilcilerin sunum yapmaları temin edilmiştir.

10 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile birlikte BTK siber güvenlik konusundaki faaliyetlerini yoğunlaştırmıştır.

Sonuç olarak, siber güvenlik konusunda uluslararası kuruluşlar nezdinde yürütülen faaliyetleri aktif olarak takip etmenin ülkemiz ve BTK açısından faydalı olacağı değerlendirilmektedir.

EKLER

EK-1

Ana Başlık	Sorumlu Kuruluş(lar)
C1. Kalkınma için BİT'in desteklenmesinde kamu idari otoritelerinin ve tüm tarafların rolü	ECOSOC/BM Bölgesel Komisyonları/ITU
C2. Bilgi ve iletişim altyapıları	ITU
C3. Bilgiye erişim	ITU/UNESCO
C4. Kapasitenin geliştirilmesi	UNDP/UNESCO/ITU/UNCTAD
C5. Bilgi ve İletişim Teknolojilerinin Kullanımında Güven ve Güvenliğin Tesis Edilmesi	ITU
C6. Çevrenin geliştirilmesi	ITU/UNDP/BM Bölgesel Komisyonları /UNCTAD
C7. BİT uygulamaları ▪ E-devlet ▪ E-iş ▪ E-öğrenme ▪ E-sağlık ▪ E-çalışma ▪ E-çevre ▪ E-tarım ▪ E-bilim	 ▪ UNDP/ITU ▪ WTO/UNCTAD/ITU/UPU ▪ UNESCO/ITU/UNIDO ▪ WHO/ITU ▪ ILO/ITU ▪ WHO/WMO/UNEP/BM-Habitat/ITU/ICAO ▪ FAO/ITU ▪ UNESCO/ITU/UNCTAD
C8. Kültürel çeşitlilik ve kimlik, dilsel çeşitlilik ve yerel içerik	UNESCO
C9. Medya	UNESCO
C10. Bilgi toplumunun etik boyutları	UNESCO/ECOSOC
C11. Uluslararası ve bölgesel işbirliği	BM Bölgesel Komisyonları/ UNDP/ITU/UNESCO/ECOSOC

EK-2

<table>
<tr><td colspan="2">OECD ICCP KOMİTESİ</td></tr>
<tr><td>• İletişim ve Altyapı Hizmetleri Politikaları Çalışma Grubu
(Genişbant, VoIP, yakınsama, mobil ve kablosuz hizmetler ...)</td><td rowspan="4">Ortak Çalışma Konuları:

İnternetin geleceği projesi, İstem dışı E-posta ile Mücadele Görev Gücü, Kötücül e-postalar, RFID ve algılayıcı ağları, İnternet Yönetişim Forumuna girdi sağlama</td></tr>
<tr><td>• Bilgi Ekonomisi Çalışma Grubu
(Uygulamalar, içerik, e-ticaret ve BİTin etkileri ...)</td></tr>
<tr><td>• Bilgi Güvenliği ve Gizlilik Çalışma Grubu
(İnternet ortamında güveni arttırmak için yenilikçi politikalar)</td></tr>
<tr><td>• Bilgi Toplumu Göstergeleri Çalışma Grubu
(Bilim, Teknoloji ve Endüstri Puan Tablosu, BİTin ekonomik kalkınmaya etkileri)</td></tr>
<tr><td colspan="2">OECD ICCP SEKRETERLİĞİ</td></tr>
</table>

ULUSLARARASI KURULUŞLARIN SİBER GÜVENİLİK FAALİYETLERİ

...
Günümüzde, toplumların bilgi toplumuna dönüşüm faaliyetleri ile bireylerin, kurumların ve ülkelerin internet basta olmak üzere BİT'e olan bağımlılığı giderek artmaktadır. Son derece bağımlı hale gelinen internetin sınır tanımayan küresel yapısı ve beraberinde getirdiği küresel bağlantılılık ise pek çok güvenlik açığı oluşturmakta ve siber tehditlere zemin hazırlamaktadır.

Bu bağlamda, söz konusu siber tehditlerin bilgi toplumuna dönüşüm yolunda en önemli engel olduğu uluslararası kuruluşlarca da çok iyi anlaşılmıştır ve bu kuruluşlardan pek çoğu siber güvenliğin sağlanması konusunda ciddi faaliyetler yürütmeye ve organizasyonlar düzenlemeye başlamışlardır.
...