SİBER GÜVENLİĞİN SAĞLANMASI, DÜNYA UYGULAMALARI

VE

ÜLKEMİZ İÇİN ÇÖZÜM ÖNERİLERİ

Meltem TURHAN

UZMANLIK TEZİ

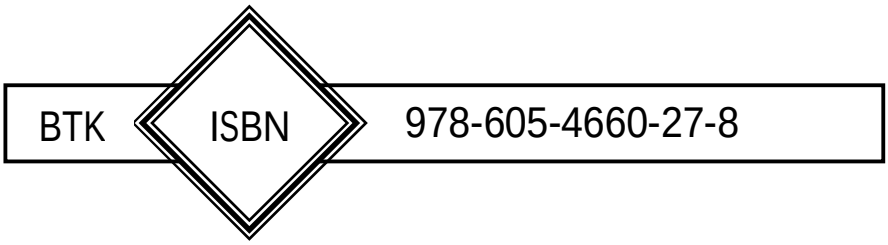
BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

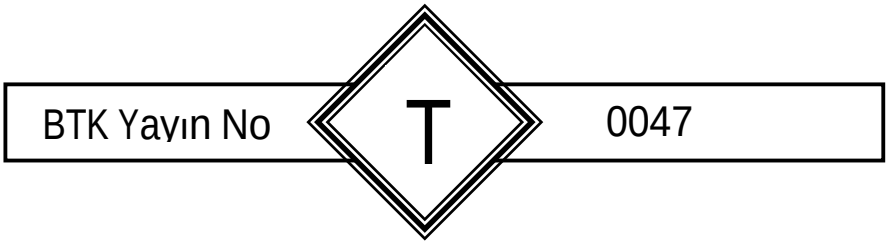
Ocak 2010

ANKARA

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





Meltem TURHAN tarafından hazırlanan SİBER GÜVENLİĞİN SAĞLANMASI, DÜNYA UYGULAMALARI VE ÜLKEMİZ İÇİN ÇÖZÜM ÖNERİLERİ adlı bu tezin Uzmanlık Tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Leyla KESER BERBER

Tez Yöneticisi

Bu çalışma, jürimiz tarafından Uzmanlık tezi olarak kabul edilmiştir.

Başkan : Dr. T. Ayhan BEYDOĞAN

Üye : Osman Nihat ŞEN

Üye : Mustafa AKAR

Üye : Mustafa ÜNVER

Üye : Cafer CANBAY

Üye : Yrd. Doç.Dr. Leyla KESER BERBER

Üye : Yrd. Doç. Dr. İsa DÖNER

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

İÇİNDEKİLER

ÖZET i

ABSTRACT ii

TEŞEKKÜR iii

ÇİZELGELERİN LİSTESİ iv

ŞEKİLLERİN LİSTESİ v

KISALTMALAR vi

1. GİRİŞ 1

2.SİBER GÜVENLİK VE SİBER GÜVENLİĞİN SAĞLANMASI 5

2.1. Siber Güvenlik 5

2.1.1 Siber güvenliğin hedefleri 5

2.1.1.1 Erişilebilirlik 6

2.1.1.2 Bütünlük 6

2.1.1.3 Gizlilik 6

2.2. Siber Güvenliğin Sağlanması 7

2.2.1 Kritik bilgi altyapısının korunması 7

2.2.1.1 Altyapı 8

2.2.1.2 Kritik altyapı 9

2.2.1.3 Kritik bilgi altyapısı 11

2.2.1.4. Kritik bilgi altyapısına yönelik son yıllarda yaşanan saldırılar 13

2.2.1.5 Kritik bilgi altyapısının korunmasında sorumluluklar 14

2.2.2 Kamu-özel sektör işbirliğinin sağlanması 15

2.2.3 Bilgisayar olaylarına müdahale ekipleri 16

2.2.3.1 BOME'ler tarafından sunulan hizmetler 18

2.2.3.2 Olaylara müdahale hizmeti 20

2.2.3.3 BOME Türleri 21

2.2.4 Siber güvenlik kültürünün oluşturulması 25

2.2.4.1 Farkındalığın oluşturulması 27
2.2.4.2. Kapasitenin geliştirilmesi 29
2.2.5 Uluslararası işbirliğinin sağlanması 30
2.2.6. Siber suçlarla mücadeleye ve siber güvenliğin sağlanmasına yönelik mevzuatın geliştirilmesi 31

3. SİBER GÜVENLİĞİ TEHDİT EDEN UNSURLAR 33

3.1. Siber Suçlar 33

3.2 Siber Suçların İşleniş Şekilleri 33
3.2.1 Oltalama (Phishing) 34
3.2.2 İstek dışı elektronik postalar 35
3.2.3 Kötücül yazılım 38
3.2.3.1 Truva atı 41
3.2.3.2 Arka kapılar 41
3.2.3.3 Solucanlar 42
3.2.3.4 Virüsler 43
3.2.3.5 Casus yazılımlar ve reklam destekli yazılımlar 44
3.2.4. BOTNET 44
3.2.5. Hizmetin engellenmesi saldırıları 45

3.3 Siber suçların sınıflandırılması 46
3.3.1 Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar 47
3.3.1.1. Yasa dışı erişim 47
3.3.1.2 Yasa dışı dinleme/izleme 48
3.3.1.3 Verilere müdahale 48
3.3.1.4 Sistemlere müdahale 49
3.3.1.5 Cihazların kötüye kullanımı 50
3.3.2 Bilgisayarlarla ilişkili suçlar 50
3.3.2.1 Bilgisayar yoluyla sahtekârlık 50
3.3.2.2 Bilgisayar yoluyla dolandırıcılık 51

4. ULUSLARARASI YAKLAŞIMLAR 52

4.1. Birleşmiş Milletler (BM) 52
4.1.1 BM Genel Kurulu Kararları 52

4.1.1.1 BM 4 Aralık 2000 tarihli ve 55/63 sayılı kararı 52
4.1.1.2 BM 19 Aralık 2001 tarihli ve 56/121 sayılı kararı 52
4.1.1.3 BM 20 Aralık 2002 tarihli ve 57/239 sayılı kararı 53
4.1.1.4 BM 23 Aralık 2003 tarihli ve 58/199 sayılı kararı 53
4.1.2 BM Bilgi ve İletişim Teknolojileri Görev Gücü 54
4.1.3 Dünya Bilgi Toplumu Zirvesi 54
4.1.3.1 Cenevre Zirvesi 55
4.1.3.2 Tunus Zirvesi 56
4.1.4 Uluslararası Telekomünikasyon Birliği 57
4.1.4.1 Küresel Siber Güvenlik Gündemi 57
4.1.4.2 Siber güvenlik kapısı 58
4.1.4.3 Gelişmekte olan ülkeler için siber güvenlik rehberi 58
4.1.4.4 Ulusal siber güvenlik / kritik bilgi altyapılarının korunması kendini değerlendirme kılavuzu 58

4.2 Avrupa Birliği (AB) 59
4.2.1 Avrupa Birliği tarafından kritik olarak kabul edilen sektörler 59
4.2.2. Avrupa Birliğinin siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması alanındaki çalışmaları ve politikaları 61
4.2.2.1 Yeşil Kitap 61
4.2.2.2 Kritik Altyapı Uyarı Bilgi Ağı 61
4.2.2.3 Avrupa Şebeke ve Bilgi Güvenliği Ajansı 62
4.2.3 AB'nin siber güvenliğin sağlanmasına ilişkin mevzuatı 63
4.2.3.1 1995 tarihli Verilerin Korunması Direktifi 63
4.2.3.2 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi 64
4.2.3.3 2006 tarihli Verilerin Saklanması Direktifi 65
4.2.3.4 24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı 66

4.3 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) 66
4.3.1 Bilgi sistemleri ve ağlarının güvenliğine ilişkin OECD rehber ilkeleri: güvenlik kültürüne doğru 67
4.3.2 Kritik bilgi altyapılarının korunmasına dair OECD tavsiye kararı 67
4.3.3 Spam görev gücü raporu 68
4.3.4 Spam karşıtı kanunların sınır ötesi uygulanmasına ilişkin OECD tavsiye kararları 69

4.3.5 Güvenlik kültürü İnternet sitesi 69
4.3.6 OECD forumları ve çalıştayları 70

4.4. Avrupa Konseyi 71
4.4.1 Avrupa Konseyi Siber Suçlar Sözleşmesi 71
4.4.1.1 Avrupa Konseyi Siber Suçlar Sözleşmesi'nin temel hükümleri 73
4.4.1.2 Sözleşmeye getirilen eleştiriler 74
4.4.2 Avrupa Konseyi Siber Suçlar Sözleşmesine Ek Protokol 75
4.4.3 Avrupa Konseyi Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme 76

4.5 G8 Grubu (G8) 77
4.5.1. Küresel Bilgi Toplumu Okinowa Şartı 78
4.5.2. Kritik bilgi altyapılarının korunması hakkında G8 ilkeleri 78
4.5.3 Yüksek teknoloji suçları alt grup faaliyetleri 80

5. ÜLKE YAKLAŞIMLARI 82

5.1 Avustralya 82
5.1.1 Avustralya'da kritik altyapının korunmasına yönelik çalışmalar 82
5.1.1.1 Avustralya'nın kritik altyapının korunması politikasında rehber ilkeler 83
5.1.1.2 Avustralya'nın kritik altyapının korunmasına yönelik terörle mücadele politikası 84
5.1.1.3 E-güvenlik ulusal gündemi 84
5.1.2 Avustralya'nın kamu-özel sektör işbirliğinin sağlanmasına yönelik çalışmaları 89
5.1.2.1 Kritik Altyapının Korunması Güvenli Bilgi Paylaşım Ağı 89
5.1.3 Avustralya'nın bilgisayar olaylarına müdahale faaliyetleri ve siber güvenlik kültürü oluşturulmasına yönelik çalışmaları 89
5.1.3.1 ISIDRAS 90
5.1.3.2 AusCERT 90
5.1.3.3 OnSecure 91
5.1.3.4 Stay Smart Online 91
5.1.3.5 Cybersmart 92
5.1.4 Avustralya'nın siber güvenliğin sağlanmasına yönelik mevzuatı 92
5.1.4.1 1988 tarihli Kişisel Gizlilik Kanunu 92
5.1.4.2 1999 tarihli Elektronik İşlemler Kanunu 93

5.1.4.3 2001 tarihli Siber Suçlar Kanunu 93
5.1.4.4 2003 tarihli Spam Kanunu 94

5.2. İngiltere 95
5.2.1 İngiltere'de kritik bilgi altyapının korunmasına yönelik çalışmalar 95
5.2.1.1 Ulusal Bilgi Güvencesi Stratejisi 95
5.2.1.2 Ulusal Altyapı Koruma Merkezi 96
5.2.1.3 Sivil Riskler Sekreterliği 97
5.2.2 İngiltere'nin kamu-özel sektör işbirliğinin sağlanmasına yönelik çalışmaları 98
5.2.3 İngiltere'nin bilgisayar olaylarına müdahale faaliyetleri ve siber güvenlik kültürü oluşturulmasına yönelik çalışmaları 99
5.2.3.1 CSIRTUK 99
5.2.3.2 GovCertUK 99
5.2.3.3 Savunma Bakanlığı Bilgisayar Acil Durum Müdahale Ekibi 100
5.2.3.4 GetSafeOnline 100
5.2.4. İngiltere'nin siber güvenliğin sağlanmasına yönelik mevzuatı 100
5.2.4.1 Bilgisayarların Kötüye Kullanılması Kanunu 100
5.2.4.2 1997 tarihli Telekomünikasyon (Sahtecilik) Kanunu 101
5.2.4.3 1998 tarihli Verilerin Korunması Kanunu 101

5.3 Amerika Birleşik Devletleri (ABD) 102
5.3.1 ABD'de kritik altyapının korunmasına yönelik çalışmalar 102
5.3.1.1 İç Güvenlik Bakanlığı 103
5.3.1.2 Siber güvenliğin sağlanmasına ilişkin ulusal stratejiler 103
5.3.2 ABD'nin kamu-özel sektör işbirliğinin sağlanmasına yönelik çalışmaları. 105
5.3.2.1 Bilgi Paylaşımı ve Analiz Merkezleri 105
5.3.2.2 InfraGard 106
5.3.2.3 Ulusal Siber Güvenlik İttifakı 106
5.3.2.4 Çapraz Sektör Siber Güvenlik Çalışma Grubu 107
5.3.2.5 Bilgi Altyapısının Korunması Kuruluşu 107
5.3.3 ABD'nin bilgisayar olaylarına müdahale faaliyetleri ve siber güvenlik kültürü oluşturulmasına yönelik çalışmaları 107
5.3.3.1 CERT Koordinasyon Merkezi 107
5.3.3.2 US-CERT 108
5.3.3.3 OnGuardOnline.gov 108
5.3.3.4 Staysafeonline.org 108

5.3.4. ABD'nin siber güvenliğin sağlanmasına yönelik mevzuatı 109
5.3.4.1 1986 tarihli Bilgisayar Dolandırıcılığı ve Bilgisayarların Kötüye Kullanılması Kanunu 109
5.3.4.2 1994 tarihli Bilgisayarların Kötüye Kullanılması Değişiklikler Kanunu 110
5.3.4.3 2002 tarihli İç Güvenlik Kanunu 110
5.3.4.4 1974 tarihli Kişisel Gizlilik Kanunu 110
5.3.4.5 2002 tarihli Federal Bilgi Güvenliği Yönetimi Kanunu 111
5.3.4.6 2004 tarihli Can-Spam Act 111

5.4 Kanada 112
5.4.1 Kanada'da kritik altyapının korunmasına yönelik çalışmalar 112
5.4.1.1 Kanada Kamu Güvenliği 113
5.4.1.2 Kritik Altyapı Ulusal Stratejisi ve Eylem Planı 113
5.4.2 Kanada'nın kamu-özel sektör işbirliği sağlanmasına yönelik çalışmaları .. 114
5.4.2.1 Kanada Siber Olaylara Müdahale Merkezi 114
5.4.2.2 Devlet Operasyon Merkezi 115
5.4.3 Kanada'nın siber güvenliğin sağlanmasına ilişkin mevzuatı 115
5.4.3.1 Kanada Ceza Kanununun ilgili hükümleri 115
5.4.3.2 Acil Durum Yönetimi Kanunu 115
5.4.3.3 Kişisel Gizlilik Kanunu 116
5.4.3.4 Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu 117

6. TÜRKİYE'DE SİBER GÜVENLİĞİN SAĞLANMASI 118

6.1. Siber güvenliğin sağlanmasına yönelik çalışmalar 118
6.1.1 "Bilgi Sistem ve Ağları İçin Güvenlik Kültürü" konulu genelge 118
6.1.2 DPT Bilgi Toplumu Stratejisi ve Bilgi Toplumu Stratejisi Eylem Planı 118
6.1.3 Ulusal Sanal Ortam Güvenlik Politikası 120
6.1.4. Ulusal Bilgi Güvenliği Teşkilat ve Görevleri Hakkında Kanun Tasarısı Taslağı 123

6.2 Ülkemizde BOME Faaliyetleri 123
6.2.1 Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi 124
6.2.1.1 BOME danışmanlığı 124
6.2.1.2 Olay müdahale koordinasyon hizmeti 124
6.1.2.3 Alarm ve uyarılar kapsamındaki faaliyetler 125

6.2.2 Ulak –CSIRT 125

6.3. Siber Güvenlik Kültürü Oluşturulmasına Yönelik Çalışmalar 126
6.3.1 BTK'nın faaliyetleri 126
6.3.1.1 Spam ile mücadele projesi 127
6.3.1.2 Farkındalık oluşturma çalışmaları 127
6.3.2 Güvenli Web 128
6.3.3 İnternetin bilinçli kullanımı ve internet güvenliği projesi 129
6.3.4 Ulusal Bilgi Güvenliği Kapısı 130
6.3.5 İnternet haftası etkinlikleri 130

6.4. Siber Suçlara ve Siber Güvenliğin Sağlanmasına İlişkin Mevzuatımız 130
6.4.1 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümleri 130
6.4.1.1 Bilişim sistemine girme suçu 131
6.4.1.2 Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları 131
6.4.1.3 Banka veya kredi kartlarının kötüye kullanılması suçları 132
6.4.1.4 Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (m. 142) 132
6.4.1.5 Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu ... 132
6.4.2 Elektronik Haberleşme Kanunu 133
6.4.3 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 133
6.4.4 Elektronik İmza Kanunu 134
6.4.5 Elektronik Haberleşme Güvenliği Yönetmeliği 134
6.4.6 Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı 135

7. SONUÇ VE ÖNERİLER 137

KAYNAKLAR 152

EK AVRUPA KONSEYİ ÜYESİ ÜLKELERDE SÖZLEŞMENİN İMZALANMASI, ONAYLANMASI VE YÜRÜRLÜĞE GİRİŞ TARİHİNE İLİŞKİN DURUM **167**

ÖZGEÇMİŞ 170

SİBER GÜVENLİĞİN SAĞLANMASI, DÜNYA UYGULAMALARI VE ÜLKEMİZ İÇİN ÇÖZÜM ÖNERİLERİ

(Bilişim Uzmanlık Tezi)

Meltem TURHAN

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

Ocak 2010

ÖZET

Bu çalışmada bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte önem kazanan siber güvenliğin sağlanması konusu ele alınmıştır. Siber güvenliğin sağlanmasının unsurlarından birisi olan kritik bilgi altyapılarının korunmasına ilişkin bilgiler verilmiş, siber güvenliğin sağlanmasında kamu-özel sektör işbirliğinin önemi, bilgisayar olaylarına müdahale ekiplerinin fonksiyonları, siber güvenlik kültürünün oluşturulmasının gerekliliği, uluslararası işbirliğinin ve yasal mevzuatın geliştirilmesinin önemi vurgulanmış, siber suçlar ve siber suçların işleniş şekilleri hakkında bilgi verilmiştir. Uluslararası kuruluşların çalışmaları ve farklı ülke örnekleri değerlendirilmiş, buna paralel olarak ülkemizde siber güvenliğin sağlanmasına yönelik çalışmalar ve düzenlemeler üzerinde durulmuştur. İncelemeler sonucunda, siber güvenliğin sağlanmasına yönelik stratejinin geliştirilmesi, kritik bilgi altyapısının korunmasına yönelik ulusal bir plan hazırlanması, sorumlu kurum ve kuruluşların tespit edilmesi, kamu-özel sektör işbirliğinin sağlanması gerektiği değerlendirilmiş ve ülkemiz için çözüm önerileri geliştirilmiştir.

Anahtar Kelimeler :Siber güvenlik, kritik bilgi altyapısı, bilgisayar olaylarına müdahale ekibi, siber güvenlik kültürü

Sayfa Adedi : 170

Tez Yöneticisi : Yrd. Doç.Dr. Leyla KESER BERBER

ENSURING CYBER SECURITY, GLOBAL EXPERIENCES AND SOLUTION PROPOSALS FOR OUR COUNTRY

(ICT Expertise Thesis)

Meltem TURHAN

INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY

January 2010

ABSTRACT

In this study the issue of ensuring cyber security which has gained importance along with the development of information and communication technologies is discussed. Information about the protection of critical information infrastructures which is one of the elements of ensuring cybersecurity is given, the importance of public-private sector cooperation, functions of computer emergency response teams, necessity of establishing the culture of cyber security and importance of building international cooperation and legislation is emphasized, cyber crimes and modus operandi of cyber crimes are explained. International organizations' studies and experiences of different countries are assessed and in parallel with these, studies and regulations on ensuring cyber security in Turkey are focused on. As a result of analysis, it is determined as necessary to develop strategies to ensure cyber security, to prepare a national plan for the protection of critical information infrastructure, to determine responsible institutions and organizations, to ensure public-private sector cooperation and then proposals of solutions for Turkey are developed.

Key words :Cyber security, critical information infrastructure, computer emergency response team, culture of cyber security

Page number :170

Advisor : Assistant Prof. Leyla Keser BERBER

TEŞEKKÜR

Çalışmam boyunca yönlendirici ve yol gösterici olan ve değerli görüş, öneri ve deneyimlerini benden esirgemeyen tez danışmanım Sn. Yrd. Doç.Dr. Leyla KESER BERBER'e, tez dönemimde göstermiş olduğu anlayıştan ve katkılarından ötürü Daire Başkanım Sn. Mustafa ÜNVER'e, tezin şekillenmesine yardımcı olan değerli görüş ve önerilerinden dolayı Cafer CANBAY'a, çalışmalarımın her aşamasındaki yardımlarından dolayı Mahire KAR'a, M.Salim KETEVANLIOĞLU'na, K.Sacid SARIKAYA'ya, ilgi ve desteğini her zaman hissettiren sevgili eşim Oğuz TURHAN'a, sevgisiyle hayatıma anlam katan biricik Oğluma ve hayatımın her döneminde yanımda olan Anneme, Babama ve Kardeşime sonsuz teşekkürü borç bilirim.

ÇİZELGELERİN LİSTESİ

		Sayfa
Çizelge 2.1	Ulusal Kritik Altyapı Tanımları	9
Çizelge 2.2	Ülkelere Göre Kritik Sektörler	10
Çizelge 2.3	Ülkeler Tarafından Kullanılan Kısaltmalar	17
Çizelge 2.4	BOME'ler Tarafından Sunulan Hizmetler	19

ŞEKİLLERİN LİSTESİ

		Sayfa
Şekil 2.1	Siber Güvenliğin Hedefleri	6
Şekil 2.2	Siber Güvenliğin Unsurları	7
Şekil 2.3	ENISA üyesi BOME'ler	23
Şekil 3.1	Örnek bir oltalama e-postası	35
Şekil 3.2	En Fazla Spam Yayan Ülkeler	37
Şekil 3.3	Yıllara Göre Spam Gönderilme Oranları	38
Şekil 3.4	Kötücül Yazılımların Artışı	39
Şekil 3.5	Kötücül Yazılım Türleri	40
Şekil 3.6	Kötücül Yazılım Barındıran Ülkeler	40
Şekil 7.1	Kritik Altyapının Korunması Kurulu	142

KISALTMALAR

Kısaltma	Açıklama
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ACMA	Australian Communications and Media Authority Avustralya Telekomünikasyon ve Medya Kurumu
AFP	The Australian Federal Police Avustralya Federal Polisi
AGD	Attorney-General's Department Avustralya Başsavcılık Makamı
AGIMO	Australian Government Information Management Office Avustralya Hükümeti Bilgi Yönetim Ofisi
AHTCC	Australian High Tech Crime Centre Avustralya Uluslararası Suçları Merkezi
APEC	Asia Pacific Economic Cooperation Asya Pasifik Ekonomik İşbirliği Teşkilatı
ASIO	Australian Security Intelligence Organisation Avustralya Güvenlik İstihbarat Teşkilatı
AusCERT	Australian Computer Emergency Response Team Avustralya Bilgisayar Acil Durum Müdahale Ekibi
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CCIRC	Canadian Cyber Incident Response Centre Kanada Siber Olaylara Müdahale Merkezi

CCS	Civil Contingencies Secretariat Sivil Riskler Sekreterliği
CERT/CC	CERT Coordination Centre CERT Koordinasyon Merkezi
CFAA	Computer Fraud and Abuse Act Bilgisayar Dolandırıcılığı ve Bilgisayarların Kötüye Kullanılması Kanunu
CIWIN	Critical Infrastructure Warning Information Network Kritik Altyapı Uyarı Bilgi Ağı
CMA	Computer Misuse Act Bilgisayarların Kötüye Kullanılması Kanunu
CPNI	Centre for the Protection of the National Infrastructure Ulusal Altyapı Koruma Merkezi
CS&C	Office for Cybersecurity and Communications Siber Güvenlik ve İletişim Dairesi
CSCSWG	The Cross Sector Cyber Security Working Group Çapraz Sektör Siber Güvenlik Çalışma Grubu
CSIA	Central Sponsor for Information Assurance Bilgi Güvencesi Merkezi Üstlenici Kurumu
CSIRTUK	Combined Security Incident Response Team Müşterek Güvenlik Olayları Müdahale Ekibi
CSTD	Commission on Science and Technology for Development BM Kalkınma için Bilim ve Teknoloji Komisyonu
DBCDE	Department of Broadband, Communications and the Digital Economy Genişband, İletişim ve Dijital Ekonomi Bakanlığı
DHS	Department of Homeland Security İç Güvenlik Bakanlığı
DoS	Denial of Service Hizmetin Engellenmesi
DPA	Data Protection Act Verilerin Korunması Kanunu

DSD	Defence Signals Directorate Savunma Sinyalleri Müdürlüğü
ECOSOC	UN Economic and Social Counsil BM Ekonomik ve Sosyal Konsey
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
ESNA	E-Security National Agenda E-Güvenlik Ulusal Gündemi
FICORA	Finnish Communications Regulatory Authority Finlandiya İletişim Düzenleyici Otoritesi
FIRST	Forum of Incident Reponse and Security Teams Olay Müdahale ve Güvenlik Ekipleri Forumu
FISMA	Federal Information Security Management Act Bilgi Güvenliği Yönetimi Kanunu
GCA	Global Cybersecurity Agenda Küresel Siber Güvenlik Gündemi
GOC	Government Operations Centre Devlet Operasyon Merkezi
HLEG	High Level Experts Group Üst Düzey Uzmanlar Grubu
I3P	Institute for Information Infrastructure Protection Bilgi Altyapısının Korunması Kuruluşu
IAAGs	Assurance Advisory Groups Altyapı Güvencesi Danışma Grubu
ICCP	Committee for Information, Computer and Communications Policy Bilgi, Bilgisayar ve Haberleşme Politikaları Komitesi
IGF	Internet Governance Forum İnternet Yönetişimi Forumu

ISACs	Information Sharing and Analysis Centers Bilgi Paylaşımı ve Analiz Merkezleri
ISIDRAS	Information Security Incident Detection Reporting and Analysis Scheme Bilgi Güvenliği Olay Tespit Raporlama ve Analiz Programı
ITU	International Telecommunication Union Uluslararası Telekomünikasyon Birliği
MEB	Milli Eğitim Bakanlığı
MODCERT	Ministry of Defence Computer Emergency Response Team Savunma Bakanlığı Bilgisayar Acil Durum Müdahale Ekibi
NATO	North Atlantic Treaty Organization Kuzey Atlantik İttifakı
NCC	National Coordinating Center Ulusal Koordinasyon Merkezi
NATO NCIRC	NATO Computer Incident Response Capability NATO Bilgisayar Olaylarına Müdahale Yeteneği
NCSA	National Cyber Security Alliance Ulusal Siber Güvenlik İttifakı
NCSD	The National Cyber Security Division Ulusal Siber Güvenlik Bölümü
NCTC	National Counter Terrorism Comittee Ulusal Terörle Mücadele Komitesi
NCTP	National Counter Terrorism Plan Terörle Mücadele Ulusal Planı
NIAS	National Information Assurance Strategy Ulusal Bilgi Güvencesi Stratejisi
NIPP	National Infrastructure Protection Plan Ulusal Altyapı Koruma Planı
NIST	National Institute of Standarts and Technology Ulusal Standartlar ve Teknoloji Kurumu

OECD	Organization for Economic Cooperation and Development Ekonomik İşbirliği ve Kalkınma Teşkilatı
OIP	Office of Infrastructure Protection Altyapının Korunması Dairesi
PIPEDA	Personal Information Protection and Electronic Documents Act Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu
SCID	Security and Critical Infrastructure Division Güvenlik ve Kritik Altyapı Bölümü
SSP	Sector-Specific Plans Sektöre Özgü Planlar
STK	Sivil Toplum Kuruluşu
TCK	Türk Ceza Kanunu
TISN	Trusted Information Sharing Network for Critical Infrastructure Protection Kritik Altyapının Korunması Güvenli Bilgi Paylaşım Ağı
TR-BOME	Türkiye Bilgisayar Olaylarına Müdahale Ekibi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi
ULAKNET	Ulusal Akademik Ağ
UNITAR	UN Istitute for Training and Research BM Eğitim ve Araştırma Enstitüsü
WARPs	Warning Advice and Reporting Points Uyarı, İhbar ve Raporlama Noktaları
WPISP	Working Party on Information Security and Privacy Bilgi Güvenliği ve Gizlilik Çalışma Grubu
WSIS	World Summit on the Information Society Dünya Bilgi Toplumu Zirvesi

1. GİRİŞ

Bilgi ve iletişim teknolojileri (BİT) her geçen gün hızlı bir şekilde gelişmekte ve tüm dünya çapında yayılmaktadır. Bu hızlı gelişim ve yayılım ile birlikte klasik düşünme, çalışma, eğlenme yöntemleri değişmeye ve yaşam yeni şekilleriyle elektronik ortama taşınmaya başlamıştır. Yazılı bilgilerin yerini elektronik ortamdaki bilgiler almaya başlamış, iş ve işlemler elektronik ortamda yapılır hale gelmiş ve bilginin üretilmesi, işlenmesi, depolanması, kullanılması ve dağıtılmasında yeni imkânlar ortaya çıkmıştır.

Bu gelişmeler emek, kaynak ve zaman tasarrufu ile mekâna bağlılıktan kurtulma başta olmak üzere pek çok faydalar sağlamaktadır. BİT bir yandan bireylerin yaşam kalitesini artırmak suretiyle gündelik hayatı kolaylaştırırken diğer yandan güvenlik açıkları ve zafiyetleriyle siber saldırganlar için vazgeçilmez bir araç haline gelmekte ve toplumu katlanmaya mecbur bıraktığı birçok zararlı eylem ve davranışı da beraberinde getirmektedir. Siber saldırganlar BİT'lerin kendilerine sunduğu araçları kullanarak bilişim sistemlerine saldırmakta, bu sistemlere zarar vermekte ve bu sistemlerde yer alan askeri, sağlık, finans, istihbarat dâhil pek çok önemli kişisel veya kurumsal bilgi üzerinde tasarruf sahibi olmaktadır.

İnternetin gelişmesi, siber suçlar işlemek ve ulusların kritik bilgi altyapılarına zarar vermek amacıyla güvenlik açıklarını fırsat bilen bireyler için yeni kapılar açmıştır. Spamler, kötücül yazılımlar, hizmetin engellenmesi saldırıları, oltacılık gibi tehditler sanal ortamın başlıca tehlikeleri haline gelmiştir. Nitekim İnterneti iletişim, bilgi edinme ve paylaşım gibi iyi amaçlarla kullanan kullanıcıların varlığına karşılık, intikam alma duygusu, güce sahip olma, macera gibi geleneksel olarak bireyleri suç işlemeye götüren nedenlerle hareket eden, sabotaj veya kaos yaratmak, dünyanın bilgi haritasına sahip olarak uluslararası arenada üstünlük sağlamak gibi amaçlarla sistemlerin açıklarını bularak bu sistemlere saldırılarda bulunan ve sistemlere izinsiz girerek çeşitli hasarlar yaratan bilgisayar korsanları ortaya çıkmıştır. BİT'den faydalanarak İnternette yer edinmek isteyen terör örgütlerinin faaliyetlerini bu ortama taşıması, hırsızlık ve dolandırıcılık gibi suçların bu ortamda işlenmeye

başlanması İnternetin kötü amaçla kullanılabileceğini açıkça gözler önüne sermektedir [1].

Siber saldırıların ve siber saldırganların sayısı gün geçtikçe artmaktadır. Bu saldırılar ve saldırganlardaki artış bireylerin, kurumların ve ülkenin güvenliği ile siber ortamın güvenilirliği açısından büyük sorunlara yol açmaktadır. Bu sorunların başında ulusların güvenliği için siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması gelmektedir. Enerji, ulaştırma, sağlık, su, bankacılık, gıda, kamu hizmetleri gibi kritik altyapı sektörleri bilgi ve iletişim sistemleri ve şebekelerine bağımlı hale geldiğinden, bu sistem ve şebekelerin güvenli ve güvenilir olmasının sağlanması ve siber saldırılara karşı korunması gerekmektedir.

Günümüzde İnternet kullanıcılarının birçoğunun siber ortamda güvenlik kaygıları nedeniyle bazı işlemleri yapmaktan kaçındığı görülmektedir. Nitekim yetersiz güvenlik önlemleri kişisel verilerin yok olmasına, kimlik hırsızlığı ve diğer dolandırıcılık olaylarına neden olmaktadır. Siber güvenliğin sağlanması kişisel verilerin ve mahremiyetin korunmasında, şebekelerin güvenliğinin ve güvenilirliğinin sağlanmasında ve siber suçlarla mücadelede önemli bir unsurdur. Bu nedenle de gelişmiş ve gelişmekte olan ülkeleri ilgilendiren küresel bir konu haline gelmiştir. Siber güvenliğin sağlanabilmesi için devletlerin ortaklaşa bir çaba göstermesi, uluslararası işbirliğini sağlamaları gerekmektedir. Nitekim sınırötesi işbirliğindeki eksiklik, ülke düzeyindeki önlemlerin etkinliğini azaltmaktadır. Üstelik bir ülkedeki kritik bilgi altyapısının korunmasındaki ve dayanıklılığındaki zafiyet diğer ülkelerdeki güvenlik açıklarını ve riskleri de artırmaktadır. Ulusal düzeyde siber güvenliğin sağlanmasında ise hükümetler, özel sektör kuruluşları, üniversiteler, sivil toplum kuruluşları (STK) ve bireyler de dâhil olmak üzere BİT kullanıcılarının bu sürece müdahil olmaları gerekmektedir.

Kritik bilgi altyapısının korunması, kamu-özel sektör işbirliğinin sağlanması, bilgisayar olaylarına müdahale ekiplerinin (BOME) kurulması, siber güvenlik kültürünün oluşturulması, uluslararası işbirliğinin sağlanması ve siber güvenliğin sağlanmasına yönelik yasal mevzuatın oluşturulması siber güvenliğin sağlanmasının

başlıca unsurlarıdır. Dolayısıyla siber güvenliğin sağlanmasında bu unsurlar birlikte ele alınmalı ve değerlendirilmelidir.

Bu çalışmanın amacı; siber güvenliğin sağlanması için yöntemlerin neler olabileceğini belirlemek, siber güvenliğin sağlanmasında kritik bilgi altyapısının korunmasının önemini vurgulamak, bu konuda sorumlulukların ve görevlerin belirlenmesi suretiyle öneriler geliştirmektir.

Giriş bölümünü takiben ikinci bölümde; siber güvenlik ve hedefleri açıklandıktan sonra siber güvenliğin sağlanmasının unsurları olan kritik bilgi altyapısının korunması, kamu-özel sektör işbirliğinin önemi, BOME'ler oluşturulması, siber güvenlik kültürünün oluşturulması, uluslararası işbirliği ve yasal mevzuatın geliştirilmesinin önemi üzerinde durulmuştur.

Üçüncü bölümde; siber suçlara ve siber suçların sınıflandırılmasına yer verilmiştir. Siber güvenliği tehdit eden spam, oltacılık, kötücül yazılımlar, botnet ve hizmetin engellenmesi saldırıları hakkında bilgi verilmiştir.

Dördüncü bölümde; siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması ile ilgili Birleşmiş Milletler (BM), Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Avrupa Birliği (AB), Avrupa Konseyi ve G8 gibi uluslararası ve uluslarüstü kuruluşların düzenlemeleri, çalışmaları, değerlendirmeleri ve önerileri incelenmiştir.

Beşinci bölümde; siber güvenliğin sağlanması ve kritik bilgi altyapısının korunmasına ilişkin yapıları ve politikaları itibariyle farklılıklar gösteren Amerika Birleşik Devletleri (ABD), Avustralya, İngiltere ve Kanada ülke örnekleri hakkında bilgi verilmiştir.

Altıncı bölümde; siber güvenliğin sağlanması hususunda ülkemizdeki mevcut durum ele alınmış ve değerlendirmelerde bulunulmuştur.

Yedinci bölümde; siber güvenliğin sağlanmasına ve kritik bilgi altyapısının korunmasına ilişkin değerlendirmeler yapılmış ve ülkemiz için çözüm önerileri geliştirilmiştir.

2.SİBER GÜVENLİK VE SİBER GÜVENLİĞİN SAĞLANMASI

Siber güvenlik, gelişmiş ve gelişmekte olan ülkeler tarafından en çok tartışılan ve önem verilen konulardan birisi haline gelmiştir.

2.1. Siber Güvenlik

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 [2].

2.1.1 Siber güvenliğin hedefleri

Siber güvenliğin hedefleri bilginin erişilebilirliğinin, gizliliğinin ve bütünlüğünün sağlanmasıdır [3].

Kaynak [4]

Şekil 2.1 Siber Güvenliğin Hedefleri

2.1.1.1 Erişilebilirlik

Erişilebilirlik; enerji kesintileri, doğal afetler, kazalar ya da saldırılar gibi olağanüstü durumlarda dahi verilerin erişilebilir olması ve hizmetlerin sunulmaya devam edilmesinin sağlanmasıdır. Bu durum özellikle haberleşme şebekelerindeki aksaklıkların hava taşımacılığı ya da güç kaynakları gibi diğer kritik altyapılar bakımından aksaklıklara yol açması durumunda hayati önemi haizdir [5].

2.1.1.2 Bütünlük

Bütünlük; gönderilen, alınan ya da saklanan verilerin eksiksiz ve değiştirilmemiş olmasının sağlanmasıdır. Bütünlük özellikle sözleşmelerin kurulması sırasında kimlik doğrulamasının sağlanması ya da verilerin doğruluğunun kritik öneme sahip olduğu sağlık verileri, sanayi tasarımları gibi alanlar için önemlidir [5].

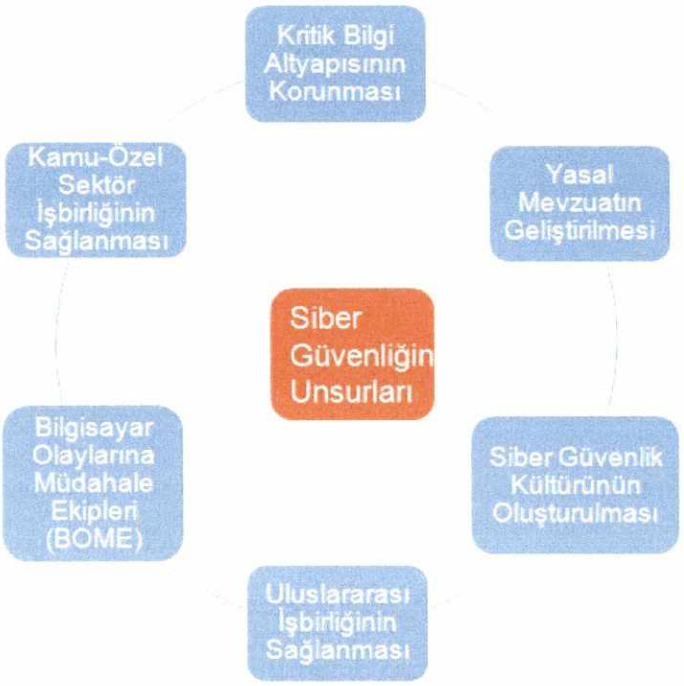
2.1.1.3 Gizlilik

Gizlilik; bilgi ve iletişim şebekeleri üzerinden yapılan haberleşmenin ya da bilgi ve iletişim sistemlerinde saklanan verilerin yetkisiz erişime karşı korunmasıdır. Özellikle kişisel verilerin iletilmesi ile haberleşmenin gizliliğinin sağlanması

alanlarında bilgilerin gizliliğine ihtiyaç duyulmaktadır [5].

2.2. Siber Güvenliğin Sağlanması

Siber güvenlik, gelişmiş ve gelişmekte olan ülkeleri ilgilendiren küresel bir sorun haline gelmiştir ve bilgi ve iletişim şebekelerinin güvenliğinin, güvenilirliğinin sağlanmasında ve siber suçlarla mücadelede önemli bir unsurdur.



Şekil 2.2 Siber Güvenliğin Unsurları

Siber güvenliğin sağlanmasında kritik bilgi altyapısının korunması, kamu-özel sektör işbirliğinin sağlanması, BOME'lerin kurulması, siber güvenlik kültürünün oluşturulması, uluslararası işbirliğinin sağlanması ve yasal mevzuatın geliştirilmesi bir bütün olarak ele alınmalıdır.

2.2.1 Kritik bilgi altyapısının korunması

BİT'in gelişmesiyle birlikte, ulusal güvenliğin ve gündelik yaşamın temelini

oluşturan fiziksel, ekonomik ve kurumsal altyapıların kritik bilgi altyapısına olan bağımlılığı artmaktadır. Bilgisayar sistemleri ile en karışık üretim süreçleri dahi kontrol edilebilmekte; elektrik, su ve doğalgaz sistemleri, barajlar ve hava trafik kontrol sistemleri bilgisayar sistemleri tarafından yönetilmektedir. Ayrıca küçük ve orta büyüklükte işletmeler BİT sayesinde verimliliklerini ve üretim kapasitelerini artırmakta, bu işletmelerin BİT'e olan bağımlılıkları da her geçen gün artmaktadır.

Kritik altyapıların birbirlerine bağımlılıkları göz önüne alındığında, bir hizmetteki aksamanın diğer temel hizmetlere ve sistemlere etkisi de büyük olmaktadır. Örneğin 2003'te yaşanan Kuzey Amerika elektrik kesintisi olayında sokak lambaları çalışamaz hale gelmiş, insanlar karanlıkta kalmış, karanlık nedeniyle suç oranlarında artışlar görülmüş, fabrikalar üretimlerini durdurmuş, bankacılık ve kamu hizmetleri kesintiye uğramış, benzin, su, doğalgaz dağıtımı yapılamamıştır. Burada da görülmüştür ki bir sektördeki kesinti diğer sektörleri ve halkın yaşam kalitesini önemli oranda etkilemektedir [6].

Kritik bilgi altyapısının korunmasının öneminin anlaşılabilmesini teminen, altyapı, kritik altyapı ve kritik bilgi altyapısı kavramlarının açıklanmasında fayda görülmektedir.

2.2.1.1 Altyapı

İngilizce "alt" anlamına gelen "infra" ve "yapı" anlamına gelen "structure" kelimelerinin birleştirilmesiyle oluşturulan altyapı kelimesi ilk defa ABD'de "Harabe İçinde Amerika" adlı kitabın yayımlanmasıyla öne çıkmıştır [7]. Söz konusu kitapta ülkenin altyapı krizi içerisinde olduğunun, bayındırlık hizmetlerinin kötü idare edildiğinin ve yıllardır yetersiz yatırımlar yapılmakta olduğunun ifade edilmesi suretiyle kamu politikası tartışmaları başlatılmıştır. Bunun üzerine altyapı kelimesinin tanımı yapılmaya ve kapsamı belirlenmeye çalışılmıştır [8].

Altyapı terimi genellikle bayındırlık tesisleri olarak algılanmakla birlikte, taşımacılığın kolaylaştırılması, içme suyu sağlanması ve toplumun kirli atıklarının

güvenli bir şekilde bertaraf edilmesi, gerekli durumlarda enerji sağlanması ve topluluklar arasında ve içinde bilginin aktarımı gibi birçok kullanım alanlarında, toplumsal talep ve fiziki dünya ile etkileşim halinde olan işletim süreçlerini, yönetim uygulamalarını ve kalkınma politikalarını da kapsamaktadır [7].

2.2.1.2 Kritik altyapı

Kritik altyapı, zarar görmesi veya tahrip olması durumunda kendisine bağlı sistemlerin veya yapıların da ciddi zarar görmesine, kesintiye uğramasına neden olan yapılardır [8]. Örneğin sel, deprem veya fırtına gibi olağanüstü bir durum bir şehirde ulaşımın aksamasına neden olurken; bir nehirdeki köprülerin yıkılması da insanların şehri tahliye etmesinin ve acil yardım hizmetlerinin aksaması sonucunu doğurmaktadır [7].

Ülkelerin kritik altyapıyı tanımlama şekilleri ve kapsamları benzerlik göstermektedir.

Çizelge 2.1 Ulusal Kritik Altyapı Tanımları

ABD	Kritik altyapı, fiziksel ya da sanal olsun, yetersizliği veya tahribatı halinde güvenlik, ulusal ekonomi güvenliği, ulusal kamu sağlığı veya güvenliği veya bunların hepsinin birden üzerinde zayıflatıcı etkiye yol açacak olan sistemler ve varlıklardır.
Almanya	Kritik altyapı, zarar görmesi ya da kaybı halinde önemli kesintilere yol açacak, kamu düzenini önemli ölçüde bozacak veya diğer önemli sonuçlara yol açacak olan toplum için hayati önemi haiz tesisler ya da kuruluşlardır.
Avustralya	Kritik altyapı, zarar görmesi, bozulması veya kullanılamaz hale gelmesi durumunda ulusun sosyal veya ekonomik refahı üzerinde önemli etkisi olabilecek veya ülkenin ulusal savunmasının ve ulusal güvenliğinin sağlanması üzerinde etkisi olabilecek fiziksel

	donanımlar, tedarik zincirleri, bilgi teknolojileri ve iletişim ağlarıdır.
Hollanda	Kritik altyapı, zarar görmesi ya da kaybı halinde önemli toplumsal kargaşaya yol açacak olan ürünler, hizmetler ya da süreçlerdir. Bu büyük oranda can kaybı ya da ciddi ekonomik zarar şeklinde olabilir.
İngiltere	Kritik altyapı, zarar görmesi ya da kaybı halinde hayat kaybına yol açabilecek, ulusal ekonomi üzerinde önemli etki doğuracak, toplumun önemli bir kısmını ve hükümetin işleyişini önemli ölçüde etkileyecek, İngiltere'nin ekonomik, politik ve sosyal yaşantısını etkileyen mal varlıkları, hizmetler ve sistemler bütünüdür.
Kanada	Kritik altyapı, halkın sağlığı, emniyeti, güvenliği, ekonomik refahı gibi değerlerinden, fiziksel ve bilgi teknolojileri olanaklarından, şebekelerden ve de hükümetin etkili işleyişinden oluşmaktadır.

Kaynak [9]

Kritik altyapı sektörleri de ülkeler arasında farklılık arz etmekte, bazı ülkeler kendi ihtiyaçları ve yapıları doğrultusunda farklı sektörleri kritik sektör olarak kabul edebilmektedirler.

Çizelge 2.2 Ülkelere Göre Kritik Sektörler

Sektörler	AB	ABD	Avustralya	Hollanda	İngiltere	Kanada
Enerji	x	x	x	x	x	x
BİT	x	x	x	x	x	x
Finans	x	x	x	x	x	x

Sağlık	x	x	x	x	x	x
Gıda	x	x	x	x	x	x
Su	x	x	x	x	x	x
Ulaşım	x	x	x	x	x	x
Güvenlik	x	Acil hizmetler	Acil hizmetler	x	Acil hizmetler	x
Devlet Yönetimi	x	x		x	x	x
Kimyasallar	x	x		x		x
Savunma sanayi		x	x	x		x
Diğer sektörler ya da faaliyetler	Uzay ve araştırma tesisleri	Barajlar, ulusal anıtlar ve ticari tesisler	Ulusal anıtlar ve meydanlar	Adalet/ Yargı		

Kaynak [9]

2.2.1.3 Kritik bilgi altyapısı

OECD tarafından kritik bilgi altyapısı "kesilmesi veya tahribatı halinde vatandaşların sağlığı, güvenliği, ekonomik refahı üzerinde veya hükümetin ve ekonominin işleyişi üzerinde etki doğuracak birbiriyle bağlantılı bilgi sistemleri ve ağları" olarak tanımlanmıştır [9].

Kritik bilgi altyapısı ülkelerin siber saldırılara karşı korunmasında, ulusal güvenlik açıklarının azaltılmasında ve oluşan hasarların ve kurtarma sürelerinin en aza indirilmesi gibi alanlarda hayati önemi haizdir [10].

Kritik bilgi altyapılarına saldırıların muhtemel sonuçları şu şekildedir [11]:

- Taşımacılığın, iletişimin, veri iletiminin, hava trafik kontrolünün engellenmesi, elektrik ve su kaynaklarının ve nükleer santrallerin zarar görmesi,
- Ticari şirketlerin iflası, uluslararası ticari işlemlerin başarısızlığı, piyasaların ve mali kurumların istikrarının bozulması, para ve kimlik hırsızlığı,
- Bireylerin mağduriyeti veya maddi kayıplar,
- Yetkisiz erişim ve/veya kişisel bilgilerin değiştirilmesi,
- Diğer ülkeleri/hükümetleri terör eylemlerinde bulunmakla suçlamak suretiyle uluslararası ilişkilerde gerginliğin tırmandırılması.

Kritik bilgi altyapısına saldırılarla, ordunun haberleşme sistemine girilip yanıltıcı bilgiler bırakılabilmesi, kentin bütün trafik ışıklarının söndürülebilmesi, telefon hatlarının felç edilebilmesi, elektrik ve doğal gaz hatlarının kapatılabilmesi, ulaşım ve su sistemlerinin, bankacılık ve finans sektörünün çökertilebilmesi, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasının engellenebilmesi, kamu kurumlarının sistemlerine girilip gizli bilgilerin elde edilebilmesi mümkün olmaktadır. Bütün bu durumlar değerlendirildiğinde tehlikenin boyutu gözler önüne serilmektedir [7].

Kritik bilgi altyapısına olan bağımlılığın bu kadar yoğun olması, kritik bilgi altyapısının sınır ötesi niteliği ve diğer altyapılarla örneğin enerji altyapılarıyla olan ilişkisi nedeniyle, saldırılara, arızalara karşı dayanıklılığının artırılması ve güvenlik açıklarının azaltılması gerekmektedir. Yetersiz güvenlik önlemleri kişisel bilgilerin yok olmasına, kimlik hırsızlığına veya diğer dolandırıcılık olaylarına yol açabilmektedir [11].

2.2.1.4. Kritik bilgi altyapısına yönelik son yıllarda yaşanan saldırılar

Son yıllarda ülkelerin kritik bilgi altyapılarına yönelik olarak önemli saldırılar gerçekleştirilmiştir. Bu saldırılardan bazılarına aşağıda yer verilmektedir:

- 26 Nisan 2007'de Estonya'nın, Nazi istilasından korunması amacıyla Rusya'nın verdiği mücadeleyi sembolize eden "Bronz Asker Heykeli"ni yerinden kaldırması sonucunda, Estonya'nın başkentinde ayaklanmalar ortaya çıkmış, iki gün sonra devletin İnternet sayfaları ele geçirilmiş, e-postalara saldırılar olmaya başlamıştır. Dördüncü günde ulusal bilgi sistemlerine, internet servis sağlayıcılarına, bankalara saldırılar olmuş ve bunun sonucunda Estonya'nın ulusal bilgi sistemleri büyük zarar görmüş ve ülkedeki İnternet sistemi çökme tehlikesiyle karşı karşıya kalmıştır [12].
- 2007 yılının Eylül ayının ilk haftasında Pentagon ve çeşitli Fransız, Alman ve İngiliz hükümeti bilgisayarları Çin kaynaklı bilgisayar korsanları tarafından saldırıya uğramıştır[13].
- Gürcistan, 2008 Güney Osetya Savaşı sırasında siber saldırılara maruz kalmış, siber saldırılar Rusya-Gürcistan savaşının bir parçası haline gelmiştir. Saldırılar sonucu Gürcistan'ın iletişim, İnternet, radyo ve TV'lerine erişim engellenmiştir [14].
- ABD, Çin ve Rus kaynaklı bilgisayarlar tarafından saldırıya uğramıştır. Bunlardan "Titan Rain" adı verilen saldırı, 2003 yılında Amerikan bilgisayar sistemlerine gerçekleştirilen planlı saldırılardır. Bu saldırılar sonucunda saldırganlar, NASA gibi önemli kuruluşların bilgisayar ağlarına girmeyi başarmışlardır [15]."Moonlight Maze" adı verilen saldırı ise, 1999 yılında Rusya kaynaklı bilgisayarlar tarafından yapılmıştır. Bu saldırı sonucunda bilgisayar korsanlarının denizcilikle ve füze yönlendirme sistemleri ile ilgili önemli bilgilere ulaştığı ifade edilmiştir [16].
- 2009 yılının Şubat ayında, Fransız Savunma Bakanlığı'nın İnternet ağına giren ve iki hafta boyunca bakanlığın ağlarında dolaşan bir virüs nedeniyle ülke savunmasına yönelik bazı güvenlik sistemleri kullanılamamış, virüs

dolayısıyla savaş uçakları kalkış yapamamıştır [17].

- Temmuz 2009'da Güney Kore siber saldırıya uğramıştır. Gürcistan, Avusturya, Almanya, Güney Kore ve ABD'de olduğu tespit edilen 5 farklı noktadan başlayan siber saldırılar sonucunda Güney Kore'nin Başkanlık Sarayı'na ait sistemler de dâhil olmak üzere pek çok İnternet hizmeti kullanılmaz hale gelmiştir. Günlerce süren saldırılarda hizmetin engellenmesi (DDoS) olarak adlandırılan saldırı tekniğinin kullanıldığı belirtilmiştir [18].
- Ocak 2010'da İnternet arama motoru Google'a "Gmail" e-posta hesaplarını ele geçirmeyi amaçlayan Çin kaynaklı olduğu iddia edilen bir siber saldırı düzenlenmiştir [19].

2.2.1.5 Kritik bilgi altyapısının korunmasında sorumluluklar

Kritik bilgi altyapısının korunması kollektif bir çaba gerektirmektedir ve bu doğrultuda kamu kurumlarına, özel sektöre, üniversitelere ve STK'lara önemli görevler düşmektedir. Bütün paydaşların tehlikelere, güvenlik açıklarına, çözüm önerilerine ve siber güvenliğin sağlanmasına yönelik başarılı işletim modellerinin geliştirilmesi hususlarında bilgi paylaşımı yoluna gitmeleri gerekmektedir [8].

Hükümetlerin kritik bilgi altyapısının korunmasına yönelik ulusal bir politika ve güvenlik stratejisi geliştirmesi gerekmektedir. Bu doğrultuda öncelikle kendi ülkeleri için kritik sayılan sektörleri belirlemeli, buna göre de sorumlu kurum ve kuruluşları oluşturmalıdır. Ayrıca kanunlar, yönetmelikler gibi düzenlemelerle, kamu kurum ve kuruluşlarına, özel sektöre bazı güvenlik önlemlerinin alınmasını, standartların kabul edilmesini zorunlu tutmalıdır [8].

Özel sektöre de bu konuda önemli görevler düşmektedir. Özel sektör, hükümet tarafından belirlenen düzenlemelere uymalı ve kamu ile işbirliği içerisinde hareket etmelidir. Ayrıca bilgi sistemlerinin saldırılara, kesintilere, hırsızlığa, sabotaja, yetkisiz kullanıma veya erişime karşı güvenliğini sağlamalıdır. Ticari işletmelerin bilgi altyapılarına bir saldırı; müşteri listelerinin kaybı, müşterilerine ait kişisel bilgilerin çalınması, yönetim stratejilerinin, fikri ve mülkiyet hakları gibi bilgilerin

ziyaı sonucunu da doğurabilir ki, bu durum kendi karlılıklarını da doğrudan etkilemektedir [8].

Üniversiteler kritik bilgi altyapısının korunması 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 katkıda bulunmalıdır [2].

STK'lar ise bireylerin büyük bir güvenlik zincirinin parçası olduklarının farkında olmalarına yardımcı olmalıdır. Kullanıcıların kendi güvenliklerini ve değerlerini korumak için siber ortamda doğru ve etik davranışlar sergilemeleri, güvenlik araçları kullanmaları, düzenli virüs güncellemeleri yapmaları ve güvenlik uyarılarını izlemeleri gibi sorumlulukları yerine getirmelerini teşvik etmelidir [2].

2.2.2 Kamu-özel sektör işbirliğinin sağlanması

Siber güvenliğin sağlanması kamu sektörü ve özel sektör arasında paylaşılması gereken bir sorumluluktur. Birçok ülkede kritik altyapılar özel sektör tarafından işletilmektedir ya da özel sektöre aittir. Kamu sektörü ise kritik altyapı sektörlerinin sahibi ya da işletmecisi konumunda olmamakla birlikte, ulusal güvenliğin, kamu düzeninin sağlanması, acil durumlara müdahale gibi fonksiyonlarının ve sorumluluklarının idamesi bakımından söz konusu altyapıların güvenliğine, güvenilirliğine ve erişebilirliğine bağımlıdır. Aynı durum özel sektör için de geçerlidir. Nitekim bir ticari işletme ne kadar büyük olursa olsun kendi başına diğer ülkelerin terör saldırılarından ya da ekonomik casusluk faaliyetlerinden korunması, siber saldırıları soruşturması ya da kovuşturması mümkün olmamaktadır [8].

Kamu sektörü siber güvenliğin sağlanmasında [20];

- Kritik bilgi altyapısının korunmasına yönelik düzenlemeler yapmakla ve politikalar geliştirmekle,
- Kritik bilgi altyapısına yönelik tehditler durumunda işletmecilere doğru, güncel ve gerekli bilgileri vermekle,
- Özel sektörü güvenlik konusunda yatırımlar yapmaya yönlendirmekle,
- Kritik bilgi altyapısının korunmasına yönelik araştırmalar için destek sağlamakla,
- Herhangi bir olay olması durumunda güncel bilgileri özel sektör ile paylaşmakla

yükümlüdür

Özel sektör ise [20];

- Güvenliğe ilişkin yazılım-donanım geliştirmekle,
- Güvenlikle ilgili olaylar konusundaki deneyim ve uzmanlığını kamu sektörüyle paylaşmakla,
- Bilgi ve iletişim şebekeleri, bilgi ve iletişim sistemleri ve diğer teknik hususlar konusunda sahip olduğu bilgiyi paylaşmakla,
- İhtiyaçlar doğrultusunda ürün, hizmet ve teknoloji sağlamak ve BİT'deki gelişmeleri takip etmekle

yükümlüdür

2.2.3 Bilgisayar olaylarına müdahale ekipleri (BOME)

BOME'ler, bir bilgisayar güvenlik olayı durumunda müdahale etmekle ve koordinasyon faaliyetlerinde bulunmakla görevlendirilmiş kuruluşlardır. BOME'ler hükümetler, özel sektör kuruluşları, üniversiteler veya kar amacı gütmeyen kuruluşlar için oluşturulabilir. BOME'lerin amacı, olaylar sonucu meydana gelebilecek hasarları kontrol etmek, müdahale ve tepki faaliyetleri için rehberlik hizmeti sağlamak ve gelecekte meydana gelebilecek olayları engellemektir [21].

1988'de "Morris" adlı solucanın İnternet sistemlerinin %10'unu işlemez hale getirmesi sonucu[1], bu tip büyük ölçekli olayların tekrar yaşanmasını engellemek amacıyla Carnegie Mellon Üniversitesi'nde CERT/CC (CERT Coordination Center) adı verilen ve koordinasyon görevi üstlenecek bir Bilgisayar Acil Durum Müdahale Ekibi oluşturulmuştur. CERT/CC, bilgisayar güvenlik olayları müdahale ekipleri türlerinin ilk organizasyonlarından biridir ve ilk oluşturulduğunda esas amacı güvenlik uzmanlarını bir araya getirmekti. İlerleyen zamanlarda benzer amaçlarla çeşitli ekipler kurulmuştur. Bu ekipler çoğunlukla ilgilendikleri ağın adıyla CERT kısaltmasını birleştiren isimler edinmişlerdir [21].

Zaman içerisinde CERT'lerin üstlendiği görevler değişmiş ve "Bilgisayar Acil Durum Müdahale Ekibi" anlamına gelen CERT terimi yeterli gelmemeye başlamış, bunun sonucunda 90'lı yılların sonunda "Bilgisayar Güvenlik Olayı Müdahale Ekibi" anlamına gelen CSIRT terimi kullanılmaya başlanmıştır. Günümüzde her iki terim de eş anlamlı olarak kullanılmaktadır [22].

Ayrıca çeşitli ülkeler tarafından kullanılan farklı kısaltmalar da bulunmaktadır:

Çizelge 2.3 Ülkeler Tarafından Kullanılan Kısaltmalar

CSIRT	Bilgisayar Güvenlik Olayı Müdahale Ekibi
CIRC	Bilgisayar Olayı Müdahale Gücü
CIRT	Bilgisayar Olayı Müdahale Ekibi
IRC	Olay Müdahale Merkezi
IRT	Olay Müdahale Ekibi
SERT	Güvenlik Acil Durum Müdahale Ekibi
SIRT	Güvenlik Olay Müdahale Ekibi

Kaynak [22]

[1] Morris solucanı bilinen ilk bilgisayar solucanıdır. Cornell Üniversitesinden Robert Tapan Morris tarafından üretilmiştir ve bu nedenle Morris adını almıştır. Robert Tapan Morris şu an MIT'de Doçent olarak görev yapmaktadır.

BOME'ler itfaiye ekiplerine benzetilmektedirler. Nasıl ki bir yangın olması ya da yangından şüphelenilmesi durumunda itfaiyenin aranabilecek bir acil numarası varsa, benzer şekilde BOME'nin de bilgisayar güvenliğiyle ilgili herhangi bir olaydan şüphelenilmesi durumunda iletişim kurulabilecek bir numarası ve e-posta adresi vardır. Her ne kadar BOME'ler itfaiye gibi kapıda belirmese de (bu hizmeti sağlayan BOME'ler de bulunmaktadır), iletişimlerini telefon ya da e-posta ile sağlarlar [21].

ITU'nun Ekim 2008 tarihli ve 58 sayılı Konsey Kararında üye ülkelere, hangi alanlarda BOME'lere ihtiyaçları olduğunu belirlemeleri, ulusal BOME'ler kurulması konusunda uluslararası destek almaları ve işbirliğine gitmeleri, ayrıca diğer ulusal BOME'lerle bilgi paylaşımı, kapasitenin geliştirilmesi gibi alanlarda birlikte çalışmaları tavsiye edilmektedir. Ayrıca ülkeler, ulusal BOME'lerin oluşturulmasını öncelik olarak kabul etmeye ve diğer üye ülkeler ve sektör üyeleriyle işbirliği yapmaya davet edilmektedir.

2.2.3.1 BOME'ler tarafından sunulan hizmetler

BOME'ler tarafından sunulabilecek birçok hizmet mevcuttur. BOME hizmetleri temel olarak üç kategoride gruplandırılabilir [21].

- Reaktif Hizmetler: Bu hizmetler bir virüsün, kötücül yazılımın yayılması, yazılımlara ait güvenlik açıkları ya da saldırıların tespit edilmesi gibi bir olay ya da talep olması durumunda başlatılır. Reaktif hizmetler BOME'nin temel faaliyet alanlarıdır.
- Proaktif Hizmetler: Bu hizmetler saldırıların ve olayların öngörülmesi suretiyle sistemlerin güvenliğinin sağlanması konusunda destek sağlamaktadır. Bu hizmetlerin yerine getirilmesi ve performansı gelecekteki olayların sayısını doğrudan azaltacaktır.
- Güvenlik Kalite Yönetimi Hizmetleri: Bu hizmetler olaylara müdahaleden bağımsız, mevcut ve iyi yönetilen hizmetleri ve bilgi teknolojileri, denetim ya

da eğitim gibi bölümlerin sorumluluğunda bulunan alanlardaki hizmetleri sunmaktadır. BOME'ler tarafından bu hizmetler desteklendiği takdirde kuruluşun genel güvenliği BOME'nin yardımları ile artırılmakta ve güvenlik açıkları, tehlikeler belirlenmektedir. Güvenlik kalite yönetimi hizmetleri genel olarak proaktif hizmetler olmakla birlikte, olayların sayısının azaltılmasına direkt olarak katkı sağlamaktadır.

Çizelge 2.4 BOME'ler Tarafından Sunulan Hizmetler

Reaktif Hizmetler	**Proaktif Hizmetler**	**Güvenlik Kalite Yönetimi Hizmetleri**
Uyarı ve İhtarlar	Duyurular	Risk analizi
Olaylara Müdahale	Teknolojiyi takip etme	İş sürekliliği ve felaket onarımı planlama
Olay analizi • Olaylara yerinde tepki verme • Olay tepki desteği • Olay tepki koordinasyonu	Güvenlik denetimi ve değerlendirme	Güvenlik danışmanlığı
Güvenlik açıklarına müdahale • Güvenlik açığı analizi • Güvenlik açığı tepkisi • Güvenlik açığı tepki koordinasyonu	Güvenlik altyapılarının, araçlarının ve uygulamalarının yapılandırılması ve bakımı	Farkındalık oluşturma
Saldırılara Müdahale • Saldırı analizi • Saldırı tepkisi • Saldırı tepki koordinasyonu	Güvenlik araçlarının geliştirilmesi	Eğitim faaliyetleri
	Saldırı Tespit hizmetleri	Ürün değerlendirme veya belgelendirme
	Güvenliğe ilişkin bilgilerin yayılması	

Kaynak [21].

BİT'in gelişmesiyle birlikte bu hizmetlerin sayısında ve niteliğinde artış ve değişim

olacağı muhakkaktır. Ayrıca her ne kadar ayrı ayrı belirtilse de, bazı hizmetler hem reaktif, hem de proaktif özellik göstermektedir. Bazı BOME'ler bu hizmetlerin tamamını sunarken, bazıları sadece birkaç tanesini sunmaktadır. Fakat BOME olarak faaliyet gösterebilmek için ekibin olaylara müdahale hizmetleri olan olay analizi, olaylara yerinde müdahale, olay müdahale desteği ya da olay müdahale koordinasyonu gibi hizmetlerin birini veya birkaçını yerine getirmesi zorunludur. Sunduğu hizmetler kadar, bu hizmetlerin sunulmasında gerekli nitelikli iş gücü, ekipman, altyapının sağlanması da çok önemlidir. Aksi takdirde BOME'ler başarılı olamayacak ve olaylar kendilerine raporlanmayacaktır [21].

2.2.3.2 Olaylara müdahale hizmeti

Olaylara müdahale hizmeti bir BOME'nin en öncelikli görevidir ve BOME tarafından sunulabilecek reaktif bir hizmettir. Olay raporlama, olay analizi ve olaylara müdahale olmak üzere 3 fonksiyona sahiptir [21]:

- Olay raporlama fonksiyonu yerel problemlerin raporlanmasında BOME'nin merkezi irtibat noktası olarak hizmet etmesini sağlamaktadır. Bu sayede bütün olaylar ve raporlar tek bir merkezde toplanmakta ve böylece bilgiler diğer kuruluşlarla da paylaşılmaktadır.

- Olay analizi kısmında, elde edilen bilgiler daha sonraları saldırı faaliyetlerinin öngörülmesini sağlamak amacıyla kullanılabilmekte ve önleyici tedbilerin alınmasını ve bu amaçla stratejiler geliştirilmesini kolaylaştırmaktadır. Bu olaylar analiz fonksiyonunun sadece bir kısmıdır. Olay analizin diğer kısmında ise olayın büyüklüğü, öncelik derecesi ve olayın tehlikesininin belirlenmesi bakımından raporlar derinlemesine incelenmektedir.

- Olay müdahale fonksiyonu çeşitli şekillerde olabilir. BOME tarafından sistem yöneticisine tavsiyelerde bulunulması ya da BOME tarafından resen olaylara müdahale edilmesi şeklinde gerçekleşebilir. Müdahale aynı zamanda bilgi

paylaşımı veya diğer BOME'ler ile somut örneklerin paylaşılması şeklinde de olabilir.

2.2.3.3 BOME Türleri

BOME'ler farklı büyüklükte ve niteliktedir ve hizmet ettikleri kitle de değişiklik göstermektedir. BOME'ler kuruluş amaçlarına göre çeşitli sınıflara ayrılabilirler [23]:

2.2.3.3.1 Ulusal BOME'ler

Ulusal BOME'ler, bir ülkede meydana gelebilecek güvenliğe ilişkin olaylara müdahale hizmeti sunmak amacıyla oluşturulurlar. JPCERT/CC (Japonya), SingCERT(Singapur),USCERT(ABD),AUSCERT(Avustralya),TR-BOME (Türkiye) Ulusal BOME'lere örnektir.

2.2.3.3.2 Kurum BOME'leri

Kurum BOME'leri, bir şirkette, kurumda veya üniversitede meydana gelen güvenlik olaylarına müdahale edilmesi ve olay sonrası elde edilen bilgilerin söz konusu kurumların güvenliğinin arttırılması amacıyla kullanılması için oluşturulur ve salt kurulduğu kurum için hizmet sunarlar. BOEING Firması tarafından kurulmuş BOEING CERT, Commerzbank tarafından kurulmuş olan Commerzbank CERT (ComCERT), Cisco tarafından kurulmuş olan Cisco Systems CSIRT, IBM tarafından kurulmuş olan IBM CERT, Oxford Üniversitesi tarafından kurulmuş olan OxCERT, Massachusetts Üniversitesi (MIT) tarafından kurulmuş olan MIT Network Security kurum BOME'lerine örnektir.

2.2.3.3.3 Uluslararası koordinasyon merkezleri

Diğer BOME'lerle koordinasyon içerisinde olmak suretiyle dünyada mevcut olan güncel güvenlik tehditleri ile ilgili bilgi sahibi olmak ve BOME'ler arasında güven ilişkisini sağlamak amacıyla kurulurlar. Uluslararası Koordinasyon Merkezleri,

koordinasyon faaliyetleri suretiyle çeşitli BOME'ler arasında olaylara müdahaleyi kolaylaştırmaktadırlar. Genel kabul görmüş Uluslararası Koordinasyon Merkezlerine aşağıda yer verilmiştir:

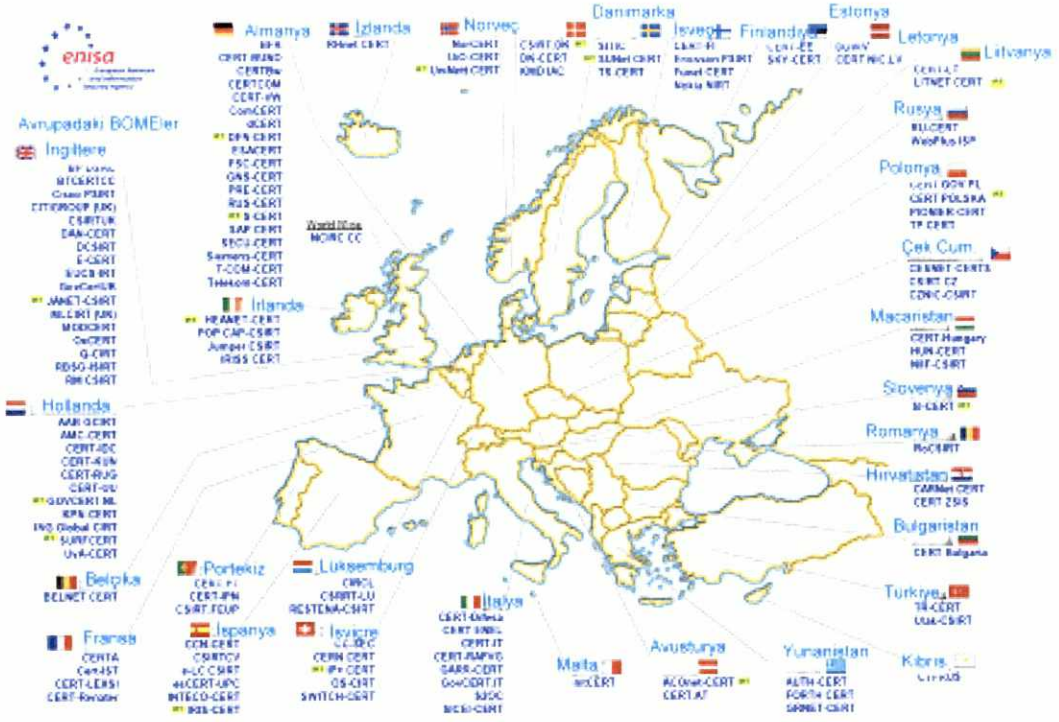
2.2.3.3.3.1 FIRST

Ekim 1989'da politik mesaj içeren ilk solucan olan "wank" solucanının tüm dünyayı etkilemesi üzerine, ekipler arası iletişim ve koordinasyon ihtiyacı duyulmuş ve bunun üzerine 1990 yılında FIRST oluşturulmuştur. FIRST, olaylara müdahalede en önemli ekiplerden birisidir ve bu alanda lider olarak kabul edilmektedir [24].

FIRST, dünyanın çeşitli bölgelerinden hükümet, özel sektör, üniversite olaylara müdahale ekiplerinin biraraya gelmesiyle oluşturulmuştur. Olayların önlenmesi, olaylara hızlı bir şekilde müdahale edilmesi gibi alanlarda üye olsun olmasın, ekipler arasında bilgi paylaşımının teşvik edilmesini amaçlamaktadır. Şu an dünyanın çeşitli bölgelerinden 200'den fazla üyesi bulunmaktadır [24].

2.2.3.3.3.2 ENISA

Şebeke ve bilgi güvenliğinin sağlanması amacıyla oluşturulmuş olan ENISA'nın görevlerinden birisi de Avrupa'daki BOME'ler arasında koordinasyonu ve işbirliğini sağlamaktır. Bu görev doğrultusunda ENISA tarafından BOME oluşturulmasına dair rehberler hazırlanmakta ve bu amaçla ülkelere yol gösterici faaliyetlerde bulunulmaktadır [25].



Kaynak [26]

Şekil 2.3 ENISA üyesi BOME'ler

ENISA tarafından Avrupa'daki BOME faaliyetleri hakkında bir envanter hazırlanmıştır. Envanter'de BOME'lerin listesi yayımlanmakta ve işbirliği, destek ve standardizasyon faaliyetleri hakkında bilgiler verilmektedir [27].

Ülkemizde kurulmuş olan TR-BOME ve ULAK-CSIRT de ENISA[2] üyesidir.

2.2.3.3.3.3 NATO NCIRC (Computer Incident Response Capability)

NATO tarafından oluşturulmuş olan NATO NCIRC, olağan BOME fonksiyonlarının

[2] TR-BOME ve ULAK-CSIRT hakkında açıklamalara Türkiye'deki durumun anlatıldığı altıncı bölümde yer verilmiştir.

yanı sıra, ülke deneyimlerinin paylaşılması ve işbirliğinin sağlanması amacıyla siber savunma tatbikatları düzenlemektedir. Ayrıca her 6 ayda bir NATO üyesi ülkelerinin temsilcilerinin katılımıyla çalıştaylar yapılmakta ve bu çalıştaylarda bilgi alışverişinde bulunulmakta, ülkeler tarafından deneyimler paylaşılmaktadır [28].

TR-BOME, NATO NCIRC ile 2007 tarihinde mutabakat zaptı imzalamıştır ve söz konusu çalıştaylara ve tatbikatlara ülkemizi temsilen katılım sağlamaktadır.

2.2.3.3.3.4 AP-CERT

Asya-Pasifik bölgesindeki 13 ülkenin BOME'lerinin birleşmesiyle oluşturulmuş bir BOME'dir. Asya-Pasifik bölgesinde bilgi güvenliğinin sağlanması amacıyla bölgesel ve uluslararası işbirliğinin sağlanması, güvenliğe ilişkin önlemler geliştirilmesi, bilgi paylaşımının sağlanması, ortak araştırmalar yürütülmesi, bölgedeki diğer BOME'lerin desteklenmesi gibi amaçlarla oluşturulmuştur [29].

2.2.3.3.3.5 TF-CSIRT (TERENA)

TF-CSIRT, BOME'ler arasında Avrupa düzeyinde işbirliğini sağlamayı hedefleyen bir görev gücüdür ve diğer bölgelerdeki benzer gruplar arasında bağlantı sağlamaktadır. TF-CSIRT, BOME'lerin deneyimlerini ve bilgilerini paylaşabileceği forumlar vasıtasıyla güvenilir bir ortam sağlamakta ve Avrupa ülkelerinde ve diğer komşu ülkelerde BOME hizmetleri sunmaktadır. TF-CSIRT, bilgisayar güvenlik olaylarına müdahalede ortak standartların ve süreçlerin kullanımını ve yeni ekiplerin kurulmasını teşvik etmekte ve mevcut ekiplerin üyelerine de en yeni olay müdahale teknikleri ve araçları konularında eğitimler vermektedir. TR-BOME, 2008 yılında TF-CSIRT'e üye olmuştur [30].

2.2.3.3.3.6 Avrupa hükümetleri BOME'leri (EGC Group)

Avrupa Hükümetleri BOME'leri, üyeleri olan kamu BOME'leri arasında olay müdahale konularında işbirliği sağlamak amacıyla oluşturulmuş, resmi olmayan bir

gruptur. Avrupa Hükümetleri BOME'leri üyeleri [31];

- Geniş ölçekli ya da bölgesel şebeke güvenlik olayları ile ilgili ortak önlemler geliştirmekle,
- Çeşitli güvenlik olayları, kötücül yazılımlar ve güvenlik açıkları ile ilgili bilgi paylaşımını kolaylaştırmakla,
- Avrupa ülkelerinde kamu BOME'lerinin oluşturulmasını teşvik etmekle,
- Diğer kuruluşlar ve organizasyonlarla ortak bir görüş oluşturmak amacıyla iletişim kurmakla

yükümlüdür.

Avrupa Hükümetleri BOME'leri üyeleri arasında Finlandiya (CERT-FI), Fransa (CERTA), Almanya (CERT-Bund), Macaristan (CERT-Hungary), İspanya (CCN-CERT), Hollanda (GOVCERT.NL), Norveç (NorCERT), İngiltere (CSIRTUK)-(GovCertUK), İsveç (SITIC), Norveç (NorCERT) yer almaktadır. TR-BOME tarafından da üyelik başvurusunda bulunulmuştur ve sürecin sonuçlanması beklenmektedir.

2.2.4 Siber güvenlik kültürünün oluşturulması

BİT'lerin kullanımının artışıyla birlikte siber güvenlik kültürünün oluşturulması da önem kazanmıştır. Siber güvenlik kültürünün oluşturulması işbirliğini gerektirmektedir ve bu doğrultuda sorumluluk hükümet, özel sektör, STK'lar, üniversiteler ve bireyler arasında paylaşılmalıdır. Nitekim BM'nin 20 Aralık 2002 tarihli ve 57/239 sayılı "Küresel Siber Güvenlik Kültürünün Oluşturulması" konulu kararında, siber güvenliğin sağlanmasında salt hükümet düzeyinde çalışmaların yeterli olmadığı, özel sektör kuruluşlarının, kamu kurumlarının ve bireylerin ortak çalışması gerektiği ve uluslararası işbirliğinin de önemli olduğu vurgulanmıştır. Ayrıca kararın ekinde OECD tarafından 25 Temmuz 2002 tarihinde kabul edilen

dokuz ilkeye yer verilmiş ve tüm kurum ve kuruluşların küresel siber güvenliğin sağlanmasına yönelik çalışmalarında bu ilkeleri dikkate almasının gerektiği vurgulanmıştır. OECD ilkeleri siber güvenlik kültürünün oluşturulması hususunda genel kabul görmüş, önemli ilkelerdir. Söz konusu ilkeler [32]:

1. Farkındalık: Bilgi sistemlerinin ve şebekelerin güvenliğinin gerekliliği ve güvenliğin artırılması için neler yapılabileceğine dair farkındalık
2. Sorumluluk: Bilgi sistemlerinin ve şebekelerin güvenliğine dair sorumluluk
3. Tepki: Güvenlikle ilgili olayları önlemek, ortaya çıkarmak ve bu olaylara tepki vermek için zamanında ve işbirliği içerisinde hareket etmek
4. Etik: Üçüncü tarafların yasal haklarına saygı göstermek
5. Demokrasi: Bilgi sistemlerinin ve şebekelerin güvenliği sağlanırken demokratik toplumun temel değerleri olan açıklık, şeffaflık, ifade özgürlüğü ve iletişimin gizliliği gibi değerlerle uyum içerisinde olmak
6. Risk Değerlendirmesi: Mevcut ve olası tehditleri ve açıklıkları hesaba katarak, teknik, fiziksel ve insani faktörler gibi temel hususları kapsayacak boyutta risk değerlendirmesi yapmak
7. Güvenlik modeli ve uygulanması: Güvenliği, bilgi sistemlerinin ve şebekelerin temel bir unsuru olarak ele almak ve tehditler ve açıklıklardan kaynaklanan zararları en aza indirmek için gerekli çözümleri tasarlamak, hayata geçirmek
8. Güvenlik yönetimi: Güvenlik yönetimi için geniş kapsamlı ve dinamik bir yaklaşım benimsemek
9. Yeniden değerlendirme: Bilgi sistemlerinin ve şebekelerin güvenliğinin denetimini yapmak ve güvenlik politikaları, uygulamaları, önlemleri ve süreçleri ile ilgili gerekli değişiklikleri ve düzeltmeleri yapmak

olarak belirtilmiştir.

BM'nin 23 Aralık 2003 tarihli ve 58/199 sayılı "Küresel Siber Güvenlik Kültürünün Oluşturulması ve Kritik Bilgi Altyapılarının Korunması" konulu kararıyla ise ülkeler,

siber güvenliğin sağlanmasında destek olmak için en iyi uygulama örneklerinin ve önlemlerin paylaşılması alanlarında ortak çalışmaya davet edilmektedir. Yine söz konusu kararda, sosyo-ekonomik gelişmede bilgi teknolojilerindeki gelişmenin ve ulusal ve uluslararası işbirliğinin önemi vurgulanmaktadır.

2005 yılında düzenlenen Bilgi Toplumu Tunus Zirvesinde ise İnternetin güvenliğinin, sürekliliğinin ve istikrarının öneminin, İnterneti ve diğer BİT ağlarını tehlikelerden ve güvenlik açıklardan korumanın önemli bir gereksinim olduğunun altı çizilmiştir. Ayrıca İnternetin güvenliği ile ilgili sorunların ortak bir anlayışla çözülmesinin gerekliliği ve güvenlik tehditleriyle ilgili ulusal ve uluslararası düzeyde mücadelede paydaşlar arasında en iyi uygulama örneklerinin paylaşılması, güvenlikle ilgili bilgilerin toplanması ve yayılması ve bu bilgilere erişimin kolaylaştırılması konularında alınacak önlemler vurgulanmıştır.

Ulusal düzeyde siber güvenlik kültürünün oluşturulmasında farkındalığın oluşturulması ve kapasitenin geliştirilmesi önemli role sahiptir [33].

2.2.4.1 Farkındalığın oluşturulması

Siber güvenlik kültürünün oluşturulmasının en önemli unsurlarından birisi, toplumda siber güvenliğe ilişkin farkındalığın oluşturulmasıdır. Günümüzde birçok bilgi sistemi güvenlik açığı kullanıcıların siber güvenlik konusunda farkındalığının oluşmamasından kaynaklanmaktadır. Bu güvenlik açıkları da kritik bilgi altyapısını siber saldırılara açık hale getirmekte ve siber güvenliği tehlikeye sokmaktadır [10].

Siber güvenliğin sağlanmasında ve güvenlik kültürünün oluşturulmasında en zayıf halka insandır. İnsan faktörü uygun ve yeterli seviyede güvenliğin sağlanmasında anahtar role sahiptir. Bu çerçevede, gündelik yaşantımızın birçok alanında hızla yaygınlaşmakta olan BİT ile ilgili olarak çocukların, öğrencilerin, ailelerin, yöneticilerin, kısacası toplumun her kesiminin bilinçlendirilmesi, BİT'in faydalarından istifade ederken hayatımızın birçok alanına girmesi muhtemel tehlikeler ile ilgili toplumda siber güvenlik şuuru ve farkındalık oluşturulması,

önlemlerin alınması gerekmektedir.

Kişisel bilgilerimizin saklandığı bilgisayarlarımızın güvenliğinin önemi anlaşılmalıdır. Son yıllarda popülaritesi artmış olan facebook, twitter gibi sosyal paylaşım siteleri vasıtasıyla kullanıcılar sahte sitelere yönlendirilerek, kullanıcıların oturum açma bilgileri (kullanıcı adı, şifre vs.) ele geçirilmekte ve bu bilgiler haksız maddi kazançlar uğruna kullanılmaktadır. Bu nedenle, eğitim faaliyetleri suretiyle bireylerin farkındalıklarının artırılması gerekmektedir.

Eğitim faaliyetleri çeşitli yöntemlerle gerçekleştirilebilmektedir. İnternet siteleri oluşturulması, seminerler düzenlenmesi, siber güvenliğe ilişkin kampanyalar düzenlenmesi, bilgisayar ve İnternet kullanıcılarının güvenlikle ilgili gelişmeler hakkında, spam, kötücül yazılım, kişisel verilerin korunması gibi konularda bilgilendirilmesi bu alanda düzenlenebilecek başlıca eğitim faaliyetleridir. Ayrıca gelişmiş ülkeler ve uluslararası kuruluşlar tarafından bilgi güvenliğinin teşvik edilmesi ve geniş kitlelere ulaşılabilmesi amacıyla özel günler ve etkinlikler düzenlenmektedir. Televizyon, radyo gibi kitle iletişim araçları da farkındalığın oluşturulmasında önemli göreve sahiptir. Nitekim eğitici, bilgilendirici programlar vasıtasıyla bireylerin farkındalıklarının artırılması gerekmektedir.

Etkili bir siber güvenliğe ilişkin farkındalığın geliştirilmesi planında kamu ve özel sektör paydaşları arasında işbirliğinin sağlanması hedeflenmelidir. Bunun için kamu sektörü, özel sektör ve üniversite temsilcileri arasında güvenilir ilişkiler oluşturulmalı ve STK'ların desteği de alınmak suretiyle işbirliği sağlanmalıdır. Hükümetler tarafından özel sektör ve STK'ların işbirliği ile bilinçlendirme ve eğitime yönelik çalışmaların yapılması, eğitim kampanyalarının düzenlenmesi en etkili yöntemlerdendir. Bu noktada da bireylere bilgisayarlarını ve İnterneti nasıl kullanmaları gerektiği, İnternet'ten gelen tehditler ve bunlardan korunma şekilleri ile hangi hataları yaptıklarında hangi saldırıyla karşı karşıya olabilecekleri öğretilmelidir.

2.2.4.2. Kapasitenin geliştirilmesi

Siber güvenlik kültürünün oluşturulmasında kapasitenin geliştirilmesi önemli bir unsurdur. Kapasitenin geliştirilmesi; uygun yasal çerçeve oluşturulması ve politika belirlenmesi, toplumların katılımı, insan kaynakları gelişimi ve yönetim sistemlerinin güçlendirilmesi de dahil olmak üzere kurumsal gelişmeler üzerine önemli katkılar sağlamaktadır. Kapasitenin geliştirilmesi insan kaynaklarının, organizasyonların, kurumsal ve yasal çerçevenin geliştirilmesini içerir [34].

Kapasitenin geliştirilmesi için [2];

- 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 bilgi ve iletişim sistemleri için bir siber güvenlik planı (risk yönetimi, acil durum yönetimi, bilgi paylaşımı, kamu bilgi ve iletişim sistemleri kullanıcılarının eğitimi ile güvenlik eğitimi konusunda kamu, özel sektör ve STK'lar arasında işbirliği hususlarında yol haritası) oluşturulması,
- Siber güvenlik uzmanları arasında bilgi alışverişine imkân veren eğitim programları, çalıştaylar, konferanslar, toplantılar gibi etkinliklerin düzenlenmesi

gerekmektedir.

2.2.5 Uluslararası işbirliğinin sağlanması

Günümüzde siber tehditler küresel bir hale gelmiştir. Zaman farkları ve coğrafi etkenler siber saldırganlar için artık engel teşkil etmemekte, ülkelerin dışarıdan gelen siber tehditlere karşı sınırlarını kapatması mümkün olmamaktadır [35].

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 bilgi ve iletişim şebekeleri farklı ülkelerdeki ve kıtalardaki siber saldırganlara birbirleriyle iletişim kurma, bilgi paylaşma, propaganda yapma, yeni üyeler kazanma gibi fırsatlar sunmaktadır. Siber saldırganlar herhangi bir ülkede bulunup bilgisayar veya şebekeleri kullanmak suretiyle izlerini bırakmaksızın başka bir ülkede suç işlemekte ve mevzuatlardaki boşluklar nedeniyle suçlara ve suçlulara ilişkin soruşturma ve yargılama güçleşmektedir [36].

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, siber güvenliğin sağlanması hususunda uluslararası işbirliğinin olmazsa olmaz önemde olduğunu göstermektedir [2].

Siber ortamda gerçekleştirilen hukuka aykırı bir eylemin kimin tarafından ve nerede yapıldığını ve sonuçlarının nerelerde etkili olduğunu saptamak amacıyla ilgili ülke makamlarının işbirliği yapmaları gerekmektedir. Bu suçların çoğunun uluslararası niteliğinin bulunması uluslararası alanda yapılacak çalışmaları zorunlu hale getirmektedir. Bu amaçla BM, AB, OECD, Avrupa Konseyi gibi kuruluşlar üye devletlerin girişimiyle işbirliğini arttırıcı çeşitli çalışmalar yapmaktadır. Bu konudaki en somut adım ise, Avrupa Konseyi Siber Suçlar Sözleşmesidir. Bu sözleşmenin usule ilişkin bölümlerinde siber suç işleyenlerin takibi ve yakalanması için

sözleşmeye taraf devletlere işbirliği açısından önemli ve etkili kurallar getirilmiştir. Bu suretle devletler siber suçlarla mücadelede uluslararası işbirliğini gerçekleştirmektedir [37].

2.2.6. Siber suçlarla mücadeleye ve siber güvenliğin sağlanmasına yönelik mevzuatın geliştirilmesi

BİT'deki gelişmelere paralel olarak siber suç türleri de her geçen gün artmakta, karmaşık bir hal almakta, bu suçların işlenmesinde yeni teknikler ve yöntemler kullanılmaktadır. Siber güvenliğin sağlanmasında siber suçların önlenmesi, kovuşturulması ve bu suçlarla mücadele edilmesi amacıyla yasal mevzuatın ve yargılama usullerinin oluşturulması hayati önemi haizdir. Yasalardaki yetersizlikler dolayısıyla bir ülkede suç olarak kabul edilen bir fiilin başka bir ülkede suç sayılmaması veya o ülkede söz konusu fiile ilişkin bir mevzuatın bulunmaması önemli sorunlara yol açmaktadır [2].Ülkelerin mevzuatının diğer ülkelerle işbirliğine cevaz verecek şekilde olması, mevcut ve gelecekte meydana gelebilecek sorunlarla mücadele için elverişli olması, BİT'deki gelişmelere uyumlu olması gerekmektedir [37].

Siber suçların önlenmesi, suç gerçekleştiğinde ise faillerin yakalanması açısından önemli bir zorluk, siber suçlarla mücadele için çalışan personelin nitelik açısından yetersizliğidir. Ülkeler kritik bilgi altyapılarına saldırı durumunda soruşturma ve kovuşturma yapabilecek ve bu kovuşturmaları diğer ülkelerle işbirliği içerisinde yürütebilecek mevzuata ve eğitimli personele sahip olmalıdır. Gelişmişlik düzeyleri ne olursa olsun siber suçları soruşturma kapasitesine sahip olmalı ve bu amaçla görevli birimler oluşturmalıdır. Ayrıca siber suçların delillendirilmesi ve adli bilişim konularında yasal düzenlemeler yapılmalı, nitelikli personel yetiştirilmelidir [37].

Siber suçlarda delil toplama konusu ve bu konuda eğitimli personel bulundurulması, delillerin saklanması bu suçların en önemli sorunlarından birisini oluşturmaktadır. Bu nedenle siber suçlarla ilgili delil elde etmek olarak adlandırılabilecek olan adli

bilişim (computer forensics) uzmanlık gerektiren, sıra dışı ve zor bir iş halini almıştır. Günümüzde kolluk ve mahkemelerin ayrılmaz bir parçası haline gelmiş olan adli bilişim, kavram olarak potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan bir uygulamayı ifade etmektedir [38].

Siber suçlarla mücadele edilebilmesi için kolluk kuvvetlerinin BİT konusunda bilgi ve becerilerinin artırılması gerekmektedir. Kolluk görevlilerinin el konulacak bilgisayar ve ekipmanlarına ve diğer araçlara nasıl el koymaları gerektiği, incelemenin nasıl yapılacağı, incelemenin yapılacağı yere nasıl götürüleceği, nerede ve nasıl muhafaza etmeleri gerektiğine ilişkin tavsiye kurallarını veya örnek uygulamaları bilmeleri ve uygulamaları, hukuka aykırı delil iddialarının önüne geçilebilmesi bakımından son derece önemlidir. Bu doğrultuda kolluk kuvvetlerinin görevli personelinin bilişim sistemleri konusunda ve bu alanda delil ve suçlu arama konularında iyi eğitilmeleri ve güncel teknolojik gelişmelerin yanısıra geliştirilen yazılımları da yakından takip etmeleri ve bu gelişmeler açısından da eğitilmeleri gerekmektedir [37].

Aynı şekilde, bu suçlarla mücadele edilebilmesi için suçların işleniş şekillerini bilen ve BİT'i kullanabilen hukukçulara ihtiyaç bulunmaktadır. Hâkimlerin ve savcıların bilgisayarlar, donanımlar, yazılımlar ve şebekeler konusunda bilgilerinin artırılması gerekmektedir [37].

3. SİBER GÜVENLİĞİ TEHDİT EDEN UNSURLAR

BİT'deki gelişmelere paralel olarak siber suçlar da önemli oranda artmış ve gün geçtikçe daha çok işlenir ve gündemi işgal eder hale gelmiştir.

3.1. Siber Suçlar

Siber suçlar; bilgisayarların ya da bilgi ve iletişim şebekelerinin suç işlenmesinde araç, amaç veya ortam olarak kullanıldığı suçlardır [39]. Siber güvenliğin sağlanabilmesinin en önemli unsurlarından birisi siber suçlar ile mücadele ve bu suçların önlenmesidir. Siber suçlarla mücadele BİT'lerin suç işlemek amacıyla veya kanuna aykırı amaçlarla kullanılmasının ve kritik altyapıların bütünlüğüne yönelik saldırıların önlenmesi alanlarında önem taşımaktadır [40].

3.2 Siber Suçların İşleniş Şekilleri

Siber suçları diğer suçlardan, yani geleneksel anlamdaki suçlardan ayıran en önemli özelliklerden birisi, bu suçların işleniş şekillerinin tespitinin zorluğudur. Söz konusu suçlar yepyeni ve çok farklı yollarla işlenebilmektedir. Nitekim İnternette virüsler, solucanlar, truva atları gibi binlerce kötücül yazılım yer almakta ve bunlara her geçen gün yenileri eklenmektedir. Özellikle sosyal amaçlı eğlence ve paylaşım siteleri siber tehditlerin ve kötücül yazılımların dağıtılması için araç olarak kullanılmaktadır.

Siber suçların önlenmesi ve bu suçlarla mücadele edilebilmesi bakımından siber tehditlerin tanımlanmasında ve tespit edilmesinde yarar görülmektedir. Bu tanımlama ve tespit işlemi sınırlayıcı değil, örnekleyicidir. Her yeni olay yeni bir işleniş şekli ortaya çıkarabildiğinden, aşağıda incelenecek olan teknikler sadece günümüze kadar görülmüş olan işleniş şekillerden en sık rastlanılanlardır.

3.2.1 Oltalama (Phishing)

Oltalama; İnternet kullanıcılarının kandırılması veya ikna edilmesi suretiyle kişisel bilgileri, kredi kartı bilgileri gibi önemli bilgilerinin ele geçirilmesini sağlayan İnternet dolandırıcılığı yöntemidir. İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğünün "f" harfinin yerine "ph" harflerinin konulmasıyla türetilen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuştur [1].

Oltalama yöntemi ile banka hesap numaraları, kredi kartı numaraları gibi kişisel bilgiler, banka gibi resmi bir kurumdan gerçekten gönderilen resmi bir mesaj gibi gözüken e-postalarla bireylerden elde edilmektedir. Sosyal mühendisliğin bir uygulama alanı olan bu tür sahte e-postaları alan bireyler, istenilen gizli bilgileri göndererek, bu bilgilerin kötü niyetli üçüncü şahısların eline geçmesine ve akabinde oluşabilecek zararlara maruz kalınmasına neden olmaktadırlar [41].

En sık görülen oltalama yöntemi, İnternet kullanıcısının müşterisi olduğu bankanın, e-posta veya bunun gibi bilgi girmeyi gerektiren bir kuruluşun İnternet sayfasının bir kopyasının yapılarak söz konusu kullanıcının hesap bilgilerinin çalınmasıdır. Sahtekârlığı gerçekleştirecek kişi/kişiler; bir banka, kart şirketi veya finansal işlemler gerçekleştiren bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir. Şekil 3.1.de de görüldüğü üzere e-postanın konusu müşterilerin bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacını içeren ifadelerden ve ilgili kurumların sayfalarının bire bir kopyası şeklinde görünen İnternet sayfalarına giden linklerden oluşmaktadır. Bazı İnternet kullanıcıları, tehlikenin farkında olmadan istenilen bilgileri doldurarak e-postalara cevap vermekte ve bunun sonucunda bu kişilerin kişisel bilgileri ve şifreleri siber saldırganlar tarafından ele geçirilmiş olmaktadır.

Kaynak [42]

Şekil 3.1. Örnek bir oltalama e-postası

Oltalama metodu dünyada gün geçtikçe yaygınlaşmakta olan bir metottur. Bunun nedeni ise bu metotla yüksek miktarlarda kolay ve haksız para kazanma ihtimalinin olmasıdır. ABD'de en fazla müşteriye sahip Lloyds, Citibank, PayPal ve Bank of America gibi bankaların en çok oltalama saldırısına uğrayan bankalar arasında yer aldığı bilinmektedir [43].

Oltalama saldırılarının hedefi ağırlıklı olarak finans sektörüdür. Ayrıca Facebook, Myspace, Twitter gibi sosyal paylaşım siteleri de oltalama saldırılarından önemli ölçüde etkilenmektedirler [44].

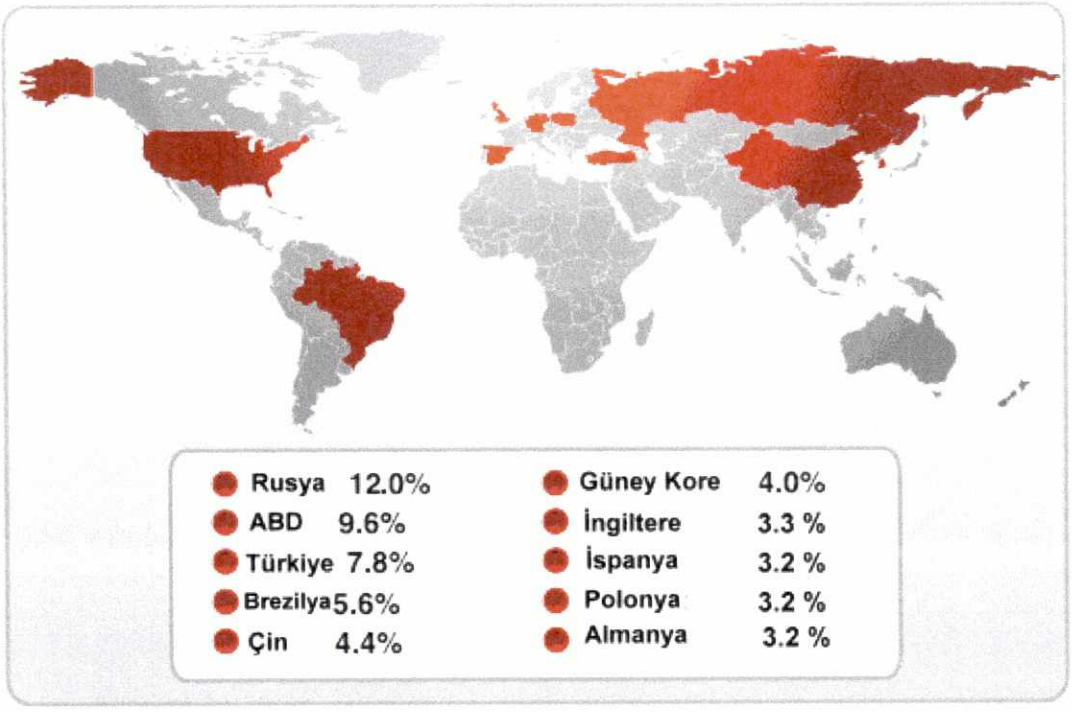
3.2.2 İstek dışı elektronik postalar (Spam)

Spam, Amerikan kökenli bir kelime olup, bir Amerikan firmasının baharatlı domuz eti ve jambon için kullandığı "Spiced Pork And Ham" kelimelerinin baş harflerinin alınması ile oluşturulmuştur [45]. Spam genellikle pazarlama, reklâm veya sosyal içerikli olarak büyük kitlelere ulaştırılmak istenen mesajların kullanıcının isteği dışında kendisine İnternet ya da cep telefonu gibi teknolojiler aracılığı ile yollanmasına dayanmaktadır [46].

Spam ilk başlarda sadece rahatsızlık verici bir durum olarak algılanırken, gün geçtikçe gerek bireyler, gerekse işletmeler için ciddi bir siber güvenlik problemi olarak görülmeye başlanmıştır. Spam bilgisayar yoluyla dolandırıcılık amacıyla araç olarak kullanılabileceği gibi, kötücül yazılım türlerinin yayılmasında ve bilgisayar kullanıcılarının oltalama vb. yollarla kendileri hakkında kötü sonuçlar doğurabilecek önemli bilgilerin verilmesinde de kullanılabilmektedir [47].

Sophos tarafından yapılan bir araştırmaya göre, günümüzde ticari e-posta'ların %97'si istek dışı elektronik postadır [48].Ayrıca söz konusu tehdit teknolojinin gelişmesiyle birlikte cep telefonları ve anlık mesajlaşma hizmetleri gibi teknolojilere de yayılmaktadır [47].

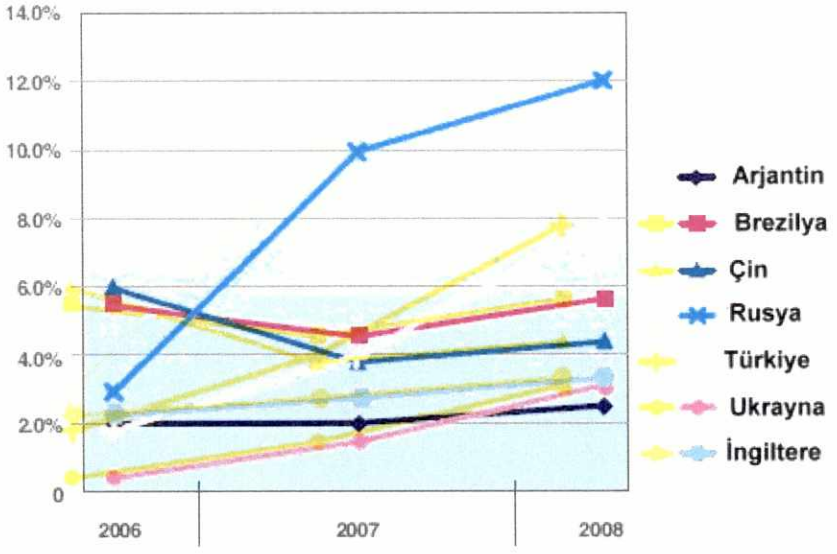
2008 yılının Kasım ayında gerek ABD'de, gerekse dünyada hayatın üzerine odaklandığı başkanlık seçimi yarışında bir spam dalgası başlatan kötü niyetli saldırganlar adres satırına yazdıkları "Obama başkanlığı reddedecek" mesajı ile kurbanlarını avlayıp; e-postanın zararlı eklentilerini kullanıcının bilgisayarına bulaştırmak suretiyle büyük miktarda zarara yol açmışlardır [49].



Kaynak [50]

Şekil 3.2 En Fazla Spam Yayan Ülkeler

IBM tarafından 2009'da yayımlanan İnternet Güvenlik Sistemleri X-Force Tehditler Raporuna göre, spam gönderilmesi konusunda Rusya 12.0% ile birinci, ABD 9.6% ile ikinci ve Türkiye ise 7.8% ile üçüncü sırada yer almaktadır [50].



Kaynak [50]

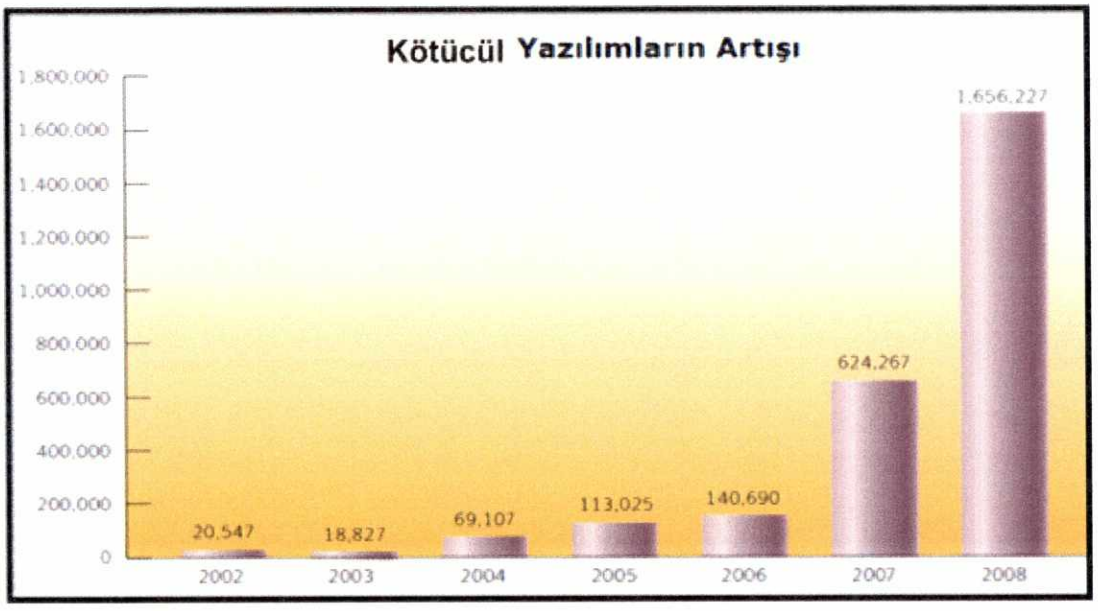
Şekil 3.3 Yıllara Göre Spam Gönderilme Oranları

IBM tarafından yayımlanan aynı rapora göre Türkiye'de spam gönderilme oranları 2006 yılında 2.0% iken, 2007 yılında 4.0% ve 2008 yılında 8.0% olmak üzere, 3 yılda yaklaşık 4 katına ulaşmıştır. Türkiye'de İnternet kullanım oranlarının artmasına rağmen siber güvenliğe ilişkin farkındalığın oluşmamış olmasının bu durumun en önemli nedenlerinden birisi olarak gösterilebileceği değerlendirilmektedir.

3.2.3 Kötücül yazılım (MALWARE)

Kötücül yazılım; sahibinin bilgisi dışında bilgisayarlara sızmak ya da zarar vermek amacıyla tasarlanmış yazılımların ortak adıdır ve bir bilişim sistemine söz konusu sisteme zarar vermek amacıyla veya kullanıcılarının amaçları dışında kullanılmak üzere yerleştirilir [51].

Her geçen gün artan ve çeşitlenen kötücül yazılımların 2002–2008 yılları arasındaki artışı Şekil 3.4'te gösterilmektedir.

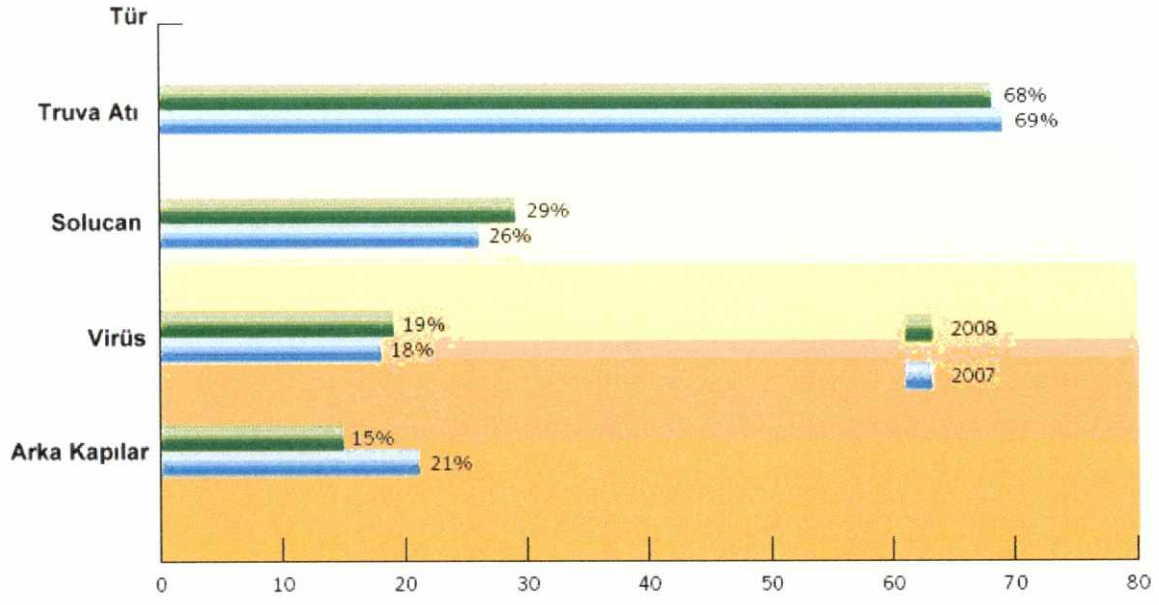


Kaynak [52]

Şekil 3.4 Kötücül Yazılımların Artışı

Geçtiğimiz yirmi yıl süresince dünya genelinde kötücül yazılım üretimi ve yayılması milyonlarca dolar değerinde gelir kaybına yol açmıştır. Nitekim ABD'nin kötücül yazılımlar nedeniyle 2007 yılında 67.2 milyon dolar değerinde zarara uğramış olduğu belirtilmiştir. Bu rakamların, kötücül yazılımların suç aracı olarak kullanılması ve bu faaliyetlerin önlenmesi için alınacak tedbirler de düşünüldüğünde, önemli oranda artacağı değerlendirilmektedir [51].

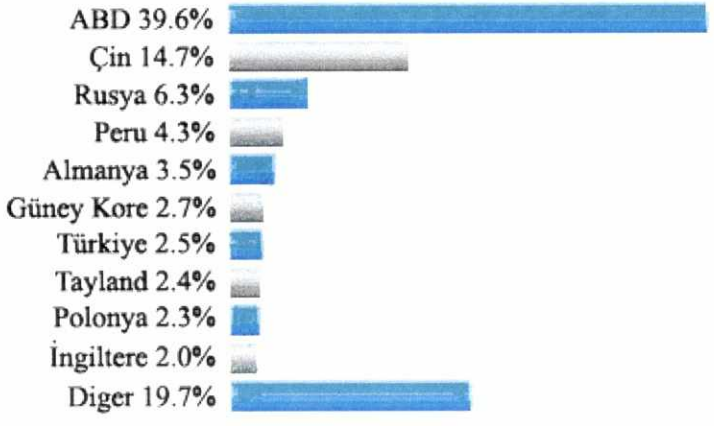
Kötücül yazılımın çeşitli türleri vardır. Son birkaç yıl öncesine kadar en sık görülen kötücül yazılım türleri virüsler ve solucanlar iken, 2009 yılında Symantec tarafından yayımlanan Küresel İnternet Güvenlik Tehdit Raporuna göre, 2008 yılında en sık görülen kötücül yazılım türleri truva atları, solucanlar, virüsler ve arka kapılar olmuştur [52].



Kaynak [52]

Şekil 3.5 Kötücül Yazılım Türleri

Ülkemiz en fazla kötücül yazılım barındıran ülkelerden olup, 2009 verilerine göre %2,5' lik bir pay ile dünya sıralamasında 7 nci sırada yer almaktadır.



Kaynak [48]

Şekil 3.6 Kötücül Yazılım Barındıran Ülkeler

3.2.3.1 Truva atı

Truva atı; yararlı gibi görünen fakat arkasında gizli bir kodun da yer alması nedeniyle bilişim güvenliğine zarar veren bir program olarak ifade edilir [51].Yunan mitolojisinde bir armağan gibi görünüp, aslında Truva kentini ele geçirme hedefi olan Yunanlı askerleri taşıyan tahta bir ata verilen isim olan truva atları diğer kötücül yazılımlar olan bilgisayar virüsleri ve bilgisayar solucanları gibi kendi başlarına işlem yapamazlar. Aynen Yunanlıların planlarının işleyebilmesi için atın Truvalılar tarafından içeri alınması gerektiği gibi Truva atlarının zararlılığı da kullanıcının hareketlerine bağlıdır. Truva atları kendilerini kopyalayıp dağıtsalar bile her kurbanın programı (Truvayı) çalıştırması gerekir [37].

Truva atları bilgisayarları uzaktan yönetmek için arka kapı açan programlardır. Lisanslı programların yasa dışı kopyalarının veya aktivasyon kodlarının dağıtıldığı "warez"[3] olarak adlandırılan siteleri veya bedava mp3, oyun veya yetişkin içerik dağıtan siteleri ziyaret eden kullanıcılar, farkında olmadan yukarıda belirtilen programları bilgisayarlarına indirirken, aynı zamanda kötü niyetli programları da indirmiş olurlar. Bilgisayara kurulan bu programlar arka plandan çalışarak, kullanıcının sistemine uzaktan erişim imkanı sağlar. Truva atlarıyla sisteme arka kapıdan (backdoor) ulaşan bilgisayar korsanları, bilgisayarın sistem yapılanmasını değiştirebilir, kullanıcının şifrelerine ve diğer kişisel bilgilerine ulaşma imkanına sahip olabilirler. Yani truva atı sisteme bulaştıktan sonra, sistemin açılmasıyla beraber kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren taraf olan bilgisayar korsanının isteklerini yerine getirir [53].

3.2.3.2 Arka kapılar (Backdoor)

Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o

---

[3] Warez, şifreli olarak kullanılan her türlü program veya verinin şifrelerinin kırılarak ücretsiz olarak dağıtıldığı sitelere verilen isimdir.

bilgisayara uzaktan erişmeyi sağlayan yöntemler arka kapı olarak adlandırılmaktadır. Bir sisteme sızmak için oldukça zahmetli bir çaba harcayan bilgisayar korsanları, daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklemek isterler. En sık karşılaşılan arka kapı yöntemi, hedef sistemde dinleme ajanı iliştirilmiş bir kapıyı (port) açık tutmaktır. Arka kapılar kimi zaman, sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına varan kötü niyetli kişiler, bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir. Arka kapılar çoğunlukla Truva atları ile karıştırılabilmektedirler. Her ikisi de hedef sisteme sızmaya yarayan kötü amaçlı yazılımlardan; truva atları faydalı bir program gibi gözükürken; arka kapılar sadece sisteme erişimi sağlayan gizli yapılardır [41].

3.2.3.3 Solucanlar (Worms)

Solucanlar; bilgisayar ağları arasında herhangi bir donanıma veya yazılıma zarar verme zorunluluğu olmadan dolaşan, kullanıcı müdahalesine gerek kalmadan kendi kendini aktif hale getirebilen ve bir kopyasını ağa bağlı olan diğer bilgisayarlara bulaştırabilen programlardır [7]. Solucanlar genellikle virüslerle karıştırılmaktadır ancak solucanlar, virüsler gibi sisteme zarar verme zorunluluğu olmaksızın da sistemin içinde hareket edebilmektedirler [51].

Solucanları yaymak için hedef sistemdeki korunmasızlıklardan faydalanmak veya sosyal mühendislik gibi yöntemler kullanılmaktadır. Solucanlar başka dosyaları değiştirmez fakat etkin bir şekilde bellekte durur ve kendilerini kopyalarlar. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında, diğer işlemekte olan görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir [41].

İlk bilinen solucan, 1988 yılında ortaya çıkan Morris solucanıdır ve dünya üzerinde yaklaşık altı bin bilgisayarı etkilemiştir. Daha sonra NIMDA, The Code Red, Mi2g gibi solucanlar dünya çapında milyarlarca dolar değerinde zarara yol açmışlardır [7].

TR-BOME tarafından Ocak 2009'da yapılan bir bildiride, son yılların en büyük saldırılarından biri olan ve tüm dünyada 15 milyon bilgisayara bulaştığı tahmin edilen "Conficker" isimli solucanın, zayıf şifrelere sahip kullanıcı hesaplarını, ağ üzerindeki paylaşımları ve solucanın bulaştığı bilgisayarlara takılan harici taşınabilir bellekleri kullanarak yayıldığı belirtilmiştir [54].

3.2.3.4 Virüsler (Viruses)

Virüsler; bilgisayar belleğine yerleşen, çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen programlardır [7].

Virüsler en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedirler. Organizmalardaki hücrelere bulaşan küçük parçacıklar olarak tanımlanan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirilerek yayılan ve kendi kendine çoğalan programlardır. Ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın, çoğu virüs programlarının, önemli dosyaları silmek veya konak (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Virüsler bir dosyanın açılması, bir e-postanın okunması veya virüs bulaşmış bir programın çalıştırılması gibi yöntemlerle yayılırlar [41].

Virüslerin yol açtığı zararlar küçük gibi gözükse de toplamda çok büyük zararlara yol açabilmektedirler. Nitekim 3 Mayıs 2000 günü tüm dünyada yayılan ve e-postaya ekli olarak gelen "I Love You" olarak bilinen bir virüs, çok kısa zamanda 55 milyon bilgisayara ulaşmış ve bunlardan 2.5-3 milyonuna bulaşarak 8.8 milyar dolar zarara sebebiyet vermiştir [55].

3.2.3.5 Casus yazılımlar (spyware) ve reklam destekli yazılımlar (adware)

Casus yazılımlar; kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılımlardır [51].

Casus yazılımlar virüs ve solucanlardan farklı olarak, sistemlere bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımların amacı, kurban olarak seçilen sistem üzerinde gizli kalarak istenen bilgileri toplamaktır. Bunun dışında şirketler, İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedirler. Kullanıcıların haberi olmadan sistemlere bulaşabilen casus yazılımlar, kişisel gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir [41].

Reklam destekli yazılımlar ise, yüklenildiği bilgisayara yüklenme işleminden sonra program kullanımdayken otomatik olarak çalışan, gösteren ve indirme yapan yazılımlardır. Amaçları, bilgisayar kullanıcılarına reklâmları göstermektir. Casus yazılımlar gibi, üzerinde bulundukları sistemdeki kişisel veya istatistiksel verileri sahibinin bilgisi ya da izni olmadan üçünü kişilere göndermek suretiyle kişisel verilerin elde edilmesi amacıyla kullanılmaktadırlar [56].

3.2.4. BOTNET

Botnet; robot kelimesinin ikinci hecesi ile network kelimesinin ilk hecesinin birleştirilmesinden oluşmuş bir kelimedir ve merkezi bir kontrol noktasına bağlanmış tehlikeli bilgisayar ya da diğer adıyla zombi[4] bilgisayar yığınını ifade etmektedir [51]. Botnet ile, virüs ya da diğer kötücül yazılımların bulaştırılması suretiyle birçok

---

[4] Zombi, sahibinin haberi olmadan kendisine kötücül bir yazılım bulaşmış olan, uzaktan erişen yetkisiz kullanıcılara kendisini kullanma ve kontrol etme yeteneği veren ve bunlardan dolayı tehlike arz eden bilgisayarlara verilen isimdir.

bilgisayar, sahiplerinin izni ve haberi olmaksızın uzaktan ve tek bir noktadan kötü amaçlar doğrultusunda yönetilmekte ve kontrol edilmektedir. Dolayısıyla aynı anda binlerce bilgisayar, bir ağ sistemi ile gizlice yönetilmiş olmaktadır. Bu ağ sistemini yönetmek için özel olarak tasarlanan kötü niyetli programlara ise "bot"[5] adı verilmektedir [57]. Bir Botnet sahibi saldırgan, ağındaki tüm bilgisayarları dünyanın herhangi bir yerinden kolay bir şekilde yönetebilmekte, botnet ağındaki masum kullanıcılar da saldırganların siber suçlarına haberleri bile olmadan büyük destek oluşturmaktadırlar.

Botnetlerin asıl hedefi ev kullanıcılarıdır ve dünya üzerindeki ev bilgisayarlarının %10 luk bir kısmının Botnet ağlarının bir parçası olduğu bilinmektedir. Nitekim arama motoru Google tarafından, 100 milyondan fazla bilgisayarın zombi ağlarında olduğu belirtilmiştir [58].

Birleşmiş Milletler (BM) 2008 yılının başında Botnet saldırısına uğramıştır. Resmi İnternet sitesini ele geçiren bilgisayar korsanları, kurumun sitesine "Hey İsrail ve ABD, çocukları ve diğer insanları öldürmeyin. Barış evrenseldir. Savaşa hayır" mesajını bırakmıştır [58].

3.2.5. Hizmetin engellenmesi saldırıları (DoS/DDoS)

Hizmetin engellenmesi saldırıları kurumların veya şirketlerin bilgi ve iletişim sistemlerini ve hizmetlerini devre dışı bırakmak için yapılan saldırılardır ve saldırıya uğrayan sistemlerin aşırı şekilde yüklenmesi ile oluşmaktadır. Bilgisayar korsanları bilgisayar kullanıcılarına bir program yüklemekte ve belirlenen günde bütün bilgisayarlar aynı anda, önceden belirlenmiş bir İnternet sitesine giriş talebi göndermeye başlamaktadır. Bu tür talep sayısı on binleri bulduğunda karşı tarafın

---

[5] Bot, ingilizce robot kelimesinin kısaltması olup çeşitli komutları çalıştırabilen otomatik bir yazılım programı olarak tanımlanmaktadır. Kullanıcıların müdahalesi olmadan bilgi sistemlerine sessizce yüklenen küçük programlardır.

sunucusu yanıt veremez duruma gelmekte; sonuçta İnternet sitesi çökmekte, işlem yapamaz hale gelmekte ve site sahipleri maddi zarara uğramaktadır [51].

14 Aralık 2007 tarihinde Kırgız Merkez Seçim Komisyonu İnternet sitesi seçim süresince saldırıya uğramış ve "Bu site Estonya Rüyası Örgütü tarafından saldırıya uğratılmıştır" mesajı bırakılmıştır. Seçim kampanyası süresince ve seçimden önce meydana gelen ayaklanmalarda Kırgız internet servis sağlayıcılarına hizmetin engellenmesi saldırıları düzenlenmiştir. Ağustos 2009'da ise dünyaca ünlü paylaşım sitesi Twitter hizmetin engellenmesi saldırıları nedeniyle erişime kapatılmıştır [59].

3.3 Siber suçların sınıflandırılması

Siber suçların genel kabul görmüş tek bir sınıflandırması bulunmamakta, uluslararası kuruluşlar tarafından farklı sınıflandırmalar yapılmaktadır. BM tarafından siber suçlar aşağıdaki şekilde sınıflandırılmıştır [60]:

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme
- Bilgisayar Sabotajı
- Bilgisayar Yoluyla Dolandırıcılık
- Bilgisayar Yoluyla Sahtecilik
- Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı
- Diğer Suçlar (Yasadışı-Pornografik Yayınlar, Hakaret – Sövme)

Tez kapsamında Avrupa Konseyi Siber Suçlar Sözleşmesinde yer alan sınıflandırma esas alınmıştır. Avrupa Konseyi Siber Suçlar Sözleşmesinde siber suçlar dört kategoriye ayrılmıştır:

1. Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar
2. Bilgisayarlarla ilişkili suçlar
3. İçerikle ilgili suçlar
4. Telif hakları ve bağlantılı hakların ihlali ile ilgili suçlar

3.3.1 Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar

Bu kategoride tanımlanan suç türleri ile bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması hedeflenmiştir.

3.3.1.1. Yasa dışı erişim

Yasa dışı erişim, bir bilgisayar sistemine yetkisiz olarak erişmek suretiyle bilgilerin güvenliğine yönelik tehditler ve saldırılar şeklindeki temel suçları kapsamaktadır. Bir bilgisayar sistemine kötücül yazılımlar yüklenmesi gibi yöntemlerle hukuka aykırı olarak erişmek suretiyle söz konusu sistemlere yetkisiz kişilerce ulaşılmasını ifade etmektedir [61].

Avrupa Konseyi Siber Suçlar Sözleşmesinin "Yasa dışı Erişim" kenar başlıklı 2 nci maddesinde tarafların, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacağı ifade edilmek suretiyle hukuka aykırı erişim suçu düzenlenmiştir [62].

3.3.1.2 Yasa dışı dinleme/izleme

Bir bilişim sisteminde bulunan verilerin iletimine hukuka aykırı olarak müdahale edilmesi yasa dışı dinleme/izleme suçu kapsamında değerlendirilmektedir. Bu suçla, Avrupa İnsan Hakları Sözleşmesinin 8 inci maddesinde de yer alan iletişimin gizliliği hakkının korunması hedeflenmiştir [63].

Verilerin iletimine müdahale; iletişimin içeriğinin dinlenmesi, denetlenmesi ya da izlenmesi ve verilerin içeriğinin bilgisayar sistemine erişim ve sistemin kullanımı yoluyla doğrudan ya da elektronik gizli dinleme cihazlarının yardımı ile dolaylı olarak elde edilmesi ile ilgilidir [63].

Avrupa Konseyi Siber Suçlar Sözleşmesinin 3 üncü maddesinde düzenlenen bu suçla, taraflardan her birinin, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar sistemi üzerinden veri iletimine kasıtlı olarak ve haksız surette dahil olması durumunda, kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacağı ifade edilmiştir [61].

3.3.1.3 Verilere müdahale

Verilere müdahale bilgisayar verilerinin ve programlarının kullanımına, bütünlüğüne ve işleyişine zarar verme şeklindeki eylemleri kapsamaktadır. Bir bilişim sistemine yetkisiz erişim sağlayanlar sadece eriştiği bilgileri incelemekle, kopyalamakla kalmamakta, bu bilgileri değiştirmekte, silmekte veya bu bilgileri kanun dışı kullanmak isteyenlere vermekte ise verilere müdahale suçunu işlemiş olmaktadırlar [64].

Bilgisayar verileri kurumlar, şirketler ve bireyler için hayati önemi haizdir. Verilere erişilememesi kurumlar, şirketler ve bireyler açısından önemli zararlara yol açabilmektedir. Siber saldırganlar tarafından verilerin bütünlüğü, söz konusu

verilerin silinmesi, değiştirilmesi, gizlenmesi ve/veya erişimlerinin sınırlandırılması suretiyle ihlal edilmektedir. Verilerin silinmesinin en bilinen örneklerinden birisi bilgisayar virüsleridir [40].

Avrupa Konseyi Siber Suçlar Sözleşmesinin 4 üncü maddesinde taraflardan her birinin, bilgisayar verilerinin tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin kasıtlı olarak yapıldıklarında kendi ulusal mevzuatları kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacağı ifade edilmiştir [62].

3.3.1.4 Sistemlere müdahale

Sistemlere müdahale, bilgisayar sabotajı olarak da nitelendirilmektedir ve bilgisayar sisteminin işleyişini engelleyecek her türlü müdahale suç kapsamında değerlendirilmektedir. Hedef alınan sisteme fiziksel zarar vermek ya da sistem başında bulunarak bilgisayardaki bilgileri silmek, yok etmek veya değiştirmek suretiyle zarar vermek, sistemlere müdahale suçu olarak nitelendirilebilir. Bilgisayar solucanları ve hizmetin engellenmesi (DoS/DDoS) saldırıları sistemlere müdahale suçuna örnek olarak verilebilir [40].

Sistemlere müdahale suçunda mala verilen zarardan ziyade, içindeki bilgilere verilen zarar önem arz etmektedir. Hukuka aykırı erişimin aktif sahası olarak da nitelendirilen suç kapsamında yalnız sisteme erişimle kalınmamakta, hukuka aykırı olarak erişilen bilişim sisteminin içerdiği bilgilerin silinmesi veya değiştirilmesi de söz konusu olmaktadır [1].

Avrupa Konseyi Siber Suçlar Sözleşmesinin 5 inci maddesinde taraflardan her birinin bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilini kasıtlı olarak yapmaları durumunda kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer

işlemleri yapacağı ifade edilmektedir [62].

3.3.1.5 Cihazların kötüye kullanımı

Cihazların kötüye kullanımı suçu yasa dışı erişim, yasa dışı dinleme/izleme, verilere müdahale ve sistemlere müdahale suçlarının işlenmesi için yapılan hazırlık hareketleri niteliğindeki fiilleri suç kapsamına almaktadır. Bu suçları işlemek için genellikle erişim araçlarının ya da başka araçların bulundurulması gerekmektedir. Ayrıca suçun kasıtlı olarak ve haksız biçimde işlenmiş olması gerekmektedir [1].

3.3.2 Bilgisayarlarla ilişkili suçlar

3.3.2.1 Bilgisayar yoluyla sahtekârlık

Bilgisayar yoluyla sahtekârlık suçu, hukuka aykırı bir şekilde menfaat temini veya başkasına zarar vermek kastıyla bilişim sistemlerindeki veri veya programların silinmesi, değiştirilmesi, bunlara müdahale edilmesi ve bu şekilde hukuken delil niteliğine sahip bir belge veya bilgi oluşturulmasıdır [61] Söz konusu suç, BİT'leri kullanmak suretiyle siber saldırganların kimliklerini gizleyebilmelerine imkân sağladığından, İnternetteki en popüler suç türlerinden birisidir. Elektronik belgelerin tahrifi, kendisine aitmiş gibi elektronik imzaların kullanılması, bankacılık alanında hesap sahiplerinin hesabının yapılan her işlem sonunda küsuratlarının ayrı bir hesaba otomatik olarak kesilmesi bu suça verilebilecek örneklerdir [40].

Avrupa Konseyi Siber Suçlar Sözleşmesinin 7 nci maddesinde tarafların, bilgisayar verilerine yeni veriler ilave etme, bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiillerinin, söz konusu verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasıtlı olarak ve haksız şekilde yapıldığında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacağı belirtilmiştir [62].

3.3.2.2 Bilgisayar yoluyla dolandırıcılık

Bilgisayar yoluyla dolandırıcılık suçunda bilgisayar bağlantısıyla yapılan her türlü dolandırıcılık fiili suç kapsamında yer almaktadır [65]. Bireyler, bilişim sistemlerinde yer alan programların veya verilerin değiştirilmesi, bu sistemlere sahte veya değiştirilmiş veriler girilmesi, mevcut verilerde oynamalar yapılması, hileli hareketlerle bilişim sistemlerinin işleyişinin değiştirilmesi suretiyle kendileri veya başkaları lehine hukuka aykırı yararlar sağlayabilmektedirler.

Siber suçların işleniş şekillerinden birisi olan oltalama (phishing) yöntemi, bilgisayar yoluyla dolandırıcılığın en sık görülen çeşitlerinden birisidir. Aynı şekilde, gerçek veya tüzel kişilere ait kişisel bilgilerin yetkisiz kişilerce dolandırıcılıkta veya diğer suçların işlenmesinde kullanılmak üzere ele geçirilmesi, iletilmesi, muhafaza edilmesi veya kullanılması olarak tanımlanabilecek olan kimlik hırsızlığı suçu da bilgisayar yoluyla dolandırıcılık suçuna örnek olarak verilebilir [66].

Avrupa Konseyi Siber Suçlar Sözleşmesinin 8 inci maddesinde kendisine veya üçüncü bir şahsa haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine yeni veriler ekleme, bilgisayar verilerini değiştirme, silme, erişilemez kılma veya kendisine veya üçüncü bir şahsa haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme fiillerinde bulunmak suretiyle bir başkasının mülkiyetinin ziyanına sebep olanların cezalandırılacağı hüküm altına alınmıştır [62].

Avrupa Konseyi Siber Suçlar Sözleşmesinin içerikle ilgili suçlar kategorisi kapsamında çocuk pornografisi ile ilgili suçlar yer almaktadır. Telif hakları ve bağlantılı hakların ihlali ile ilgili suçlar kapsamında ise İnternette en sık görülen suç çeşitlerinden birisi olan fikri mülkiyet haklarının, özellikle de telif haklarının ihlaline yönelik suçlar yer almaktadır.

4. ULUSLARARASI YAKLAŞIMLAR

Siber güvenlik ve kritik bilgi altyapısının korunması konusunda BM, AB, OECD, Avrupa Konseyi, G8 gibi kuruluşlar önemli çalışmalarda bulunmakta ve raporlar yayınlamak, çalıştaylar düzenlemek suretiyle çalışmalarını paylaşmaktadırlar.

4.1. Birleşmiş Milletler (BM)

1980'li yılların sonlarından itibaren kritik bilgi altyapılarının korunması ve siber güvenlikle ilgili konular BM ve kendi yapıları içinde tartışılmaya başlanmakla birlikte, bu konudaki resmi çabalar daha yakın tarihlerde görülmektedir.

4.1.1 BM Genel Kurulu Kararları

4.1.1.1 BM 4 Aralık 2000 tarihli ve 55/63 sayılı kararı

BM Genel Kurulunun 55 inci oturumunda alınan "Bilgi teknolojilerinin suç amaçlı kullanımı ile mücadele" konulu kararıyla, siber güvenliğin sağlanması amacıyla ülkelerin yasal mevzuatlarının siber suçlarla mücadele için elverişli olmasının sağlanması, araştırma ve soruşturmalarda işbirliğinin ve bilgi alışverişinin sağlanması ve bu amaçla eğitimli ve donanımlı personelin bulundurulması, hukuk sistemlerinin bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini koruması ve bilgisayar sistemlerinin yetkisiz erişime ve kötüye kullanmaya karşı korunması, hukuk sistemlerinin verilerin korunmasına cevaz vermesi, kamunun bu konuda farkındalığının geliştirilmesi, kişisel verilerin ve bireylerin mahremiyetinin sağlanmasının gerektiğine ilişkin karar alınmış ve üye ülkelerin bu konularda gerekli önlemleri almalarının sağlanması gerektiği ifade edilmiştir [67].

4.1.1.2 BM 19 Aralık 2001 tarihli ve 56/121 sayılı kararı

BM Genel Kurulunun 56 ncı oturumunda alınan "Bilgi teknolojilerinin suç amaçlı kullanımı ile mücadele" konulu kararıyla, ülkeler arasında ve kamu-özel sektör

arasında işbirliğinin önemine değinilmiştir. Kararda, Avrupa Konseyi Siber Suçlar Sözleşmesi ve G8 tarafından yapılan çalışmaların da uluslararası alanda önemli olduğu belirtilmiş ve BM'nin 55/63 sayılı kararı doğrultusunda belirtilen hedeflerin yerine getirilmesi amacıyla çalışmalara devam edilmesi kararı alınmıştır [68].

4.1.1.3 BM 20 Aralık 2002 tarihli ve 57/239 sayılı kararı

BM Genel Kurulunun 57 nci oturumunda alınan "Küresel siber güvenlik kültürünün oluşturulması" konulu kararıyla, siber güvenliğin sağlanması için sadece hükümet düzeyinde çalışmaların yeterli olmadığı, özel sektör kuruluşlarının, kamu kurumlarının ve bireylerin ortak çalışması gerektiği ve uluslararası işbirliğinin de önemli olduğu vurgulanmaktadır. Kararda ayrıca üye ülkeler, 10–12 Aralık 2003 tarihinde Cenevre'de ve 2005'de Tunus'ta düzenlenecek Dünya Bilgi Toplumu Zirvesine katılmaya ve bu amaçla hazırlık yapmaya davet edilmiştir. Kararın ekinde OECD tarafından 25 Temmuz 2002 tarihinde kabul edilen dokuz ilkeye yer verilmiş ve tüm kurum ve kuruluşların küresel siber güvenliğin sağlanmasına yönelik çalışmalarında bu ilkeleri göz önünde bulundurmasının gerektiği vurgulanmıştır [69].

4.1.1.4 BM 23 Aralık 2003 tarihli ve 58/199 sayılı kararı

BM Genel Kurulunun 58 inci oturumunda alınan "Küresel siber güvenlik kültürünün oluşturulması ve kritik bilgi altyapılarının korunması" konulu kararıyla, ülkelerin kritik altyapıları arasında artan bağımlılıklar ve bu altyapıları bekleyen çeşitli tehlikeler belirtilmektedir. Kararın ekinde G8 ülkeleri Adalet ve İçişleri Bakanları tarafından 2003 yılında Paris'te kabul edilen kritik bilgi altyapılarının korunmasına ilişkin 11 ilkeye yer verilmektedir. BM Genel Kurulu, üye ülkeleri ve uluslararası kuruluşları kritik bilgi altyapısının korunması konusunda bu ilkeleri esas almaya ve siber güvenliğin sağlanmasına destek sağlanması için en iyi uygulama örneklerinin ve önlemlerin paylaşılması alanlarında ortak çalışmaya davet etmektedir. Ayrıca kararda 2005 yılının Kasım ayında Tunus'ta düzenlenecek olan Dünya Bilgi Toplumu Zirvesi'nin ikinci aşamasına hazırlık çalışmalarında bu ilkelerin de göz önünde bulundurulması gerektiği ifade edilmektedir. Son olarak BM Genel Kurulu

tarafından, gelişmekte olan ve az gelişmiş ülkelerin de kritik bilgi altyapısının korunması çabalarına dâhil edilmesi ve bu suretle bilgi teknolojilerinin transferi ve kapasitenin geliştirilmesi çabalarının güçlendirilmesi gerektiği belirtilmektedir [70].

4.1.2 BM Bilgi ve İletişim Teknolojileri Görev Gücü (UN ICT Task Force)

Kasım 2001'de BM Ekonomik ve Sosyal Konsey'in (ECOSOC) talebi üzerine BM Bilgi ve İletişim Teknolojileri Görev Gücü kurulmuştur. Görev Gücü, BİT'in kullanılması suretiyle "Milenyum Kalkınma Hedeflerine" ulaşmak amacıyla dünya çapında destek vermek ve seferberlik başlatmakla görevlendirilmiştir. Nisan 2004'te BM Genel Merkezinde "Bilgi teknolojilerinde politika ve güvenlik" konulu bir seminer düzenlenmiştir. BM Görev Gücü ve BM Eğitim ve Araştırma Enstitüsü (UNITAR) tarafından ortaklaşa düzenlenen seminerde, politika bilinci ve bilgi teknolojilerinde eğitim konuları ele alınmıştır [71].

Ayrıca Eylül 2002'de Görev Gücü tarafından "Bilgi Güvensizliği – Siber Tehditlerden Korunma ve Siber Güvenlik Kılavuzu" adı verilen bir rehber yayımlanmıştır. Bu rehberde bilgi güvensizliği sorunu genel olarak ele alınmış ve güvenlikle ilgili olayların önlenmesi ve tepki oluşturulması amacıyla standartlar ve uygulama örnekleri de dahil olmak üzere çözüm önerileri sunulmuştur [10].

4.1.3 Dünya Bilgi Toplumu Zirvesi (WSIS)

Dünya Bilgi Toplumu Zirvesi (WSIS), BM ve Uluslararası Telekomünikasyon Birliği (ITU) tarafından iki aşamalı olarak düzenlenen bir Dünya Zirvesidir. "İki aşamalı, tek bir zirve" olarak anılan WSIS'ın temelleri, 1998 yılında ITU tarafından alınan 73 nolu karara dayanmaktadır. Bu kararla ITU, WSIS ile ilgili bir çalışma yapmak, çalışmaların sonucunu BM İdari Koordinasyon Komitesi'ne rapor etmek ve zirvenin düzenlenmesi için yapılabilecek çalışmaları tespit etmekle görevlendirilmiştir [72].

BM, Ocak 2002'de aldığı 56/183 nolu kararla Zirvenin birinci aşamasının 10–12

Aralık 2003 tarihlerinde Cenevre'de, ikinci aşamasının 16–18 Kasım 2005 tarihlerinde Tunus'ta yapılmasını karara bağlamıştır. Ayrıca bu kararla BM'nin tüm organlarının, uluslararası ve bölgesel kuruluşların, STK'ların ve özel sektörün zirveye aktif destek vermesi ve üst düzey katılımda bulunması için çağrıda bulunulmuştur

4.1.3.1 Cenevre Zirvesi

WSIS'in I. Aşaması 10 – 12 Aralık 2003 tarihleri arasında Cenevre'de yapılmıştır. I. Aşamada WSIS'in amacı "bilgi toplumu için ortak bir vizyon ve anlayışın geliştirilmesi; hükümetlerin, uluslararası kuruluşların, özel sektörün ve sivil toplumun uygulayacağı bir eylem planının ve ilkeler bildirgesinin kabul edilmesi ve herkes için bilgi toplumu hedefine ulaşmak üzere gerekli organizasyonların kurulması yönünde kesin adımların atılması" şeklinde ortaya konulmuştur. Zirvenin I. Aşamasında İlkeler Bildirgesi ve Eylem Planı kabul edilmiştir.

WSIS İlkeler Bildirgesinin ana hatları şu şekildedir [72]:

- Bilgi ve şebeke güvenliğini, kimlik denetimini, mahremiyeti ve tüketici haklarını da kapsayacak şekilde BİT'e duyulan güven artırılmalıdır.
- Kapasitenin geliştirilmesi amacıyla, toplumda farkındalığın artırılması yönünde çalışmalar yapılmalıdır.
- Taraflar arasındaki sayısal uçurumun uluslararası işbirliği suretiyle kapatılması amacıyla koşulsuz destek sağlanmalıdır.

Bu bildirgenin ve Zirvede oluşturulan ortak görüşlerin ışığında oluşturulan Eylem Planı hükümetlerin ve diğer kuruluşların işbirliği ile aşağıda yer alan eylemlerden oluşmaktadır [72]:

1. Kalkınma için BİT'in desteklenmesinde hükümetlerin ve tüm paydaşların rolü
2. Bilgi ve iletişim altyapısı: Bilgi toplumunun temeli

3. Bilgilere erişim
4. Kapasitenin geliştirilmesi
5. BİT kullanımında güvenin ve güvenliğin sağlanması
6. Uluslararası ve bölgesel işbirliği

4.1.3.2 Tunus Zirvesi

Zirvenin II. Aşaması 16–18 Kasım 2005 tarihlerinde Tunus'ta düzenlenmiştir. Zirvenin bu aşamasında "Tunus Taahhüdü" ve "Bilgi Toplumu için Tunus Gündemi" başlıklı iki doküman kabul edilmiştir. Tunus Taahhüdü ağırlıklı olarak politik taahhütleri içermektedir. Bilgi Toplumu için Tunus Gündemi'nde ise sayısal uçurumun azaltılması amacıyla kullanılacak finansal mekanizmalar, İnternet yönetişimi ile ilgili hususlar ile Cenevre ve Tunus kararlarının uygulanması ve takip edilmesi konuları ön plana çıkmaktadır.

Tunus Zirvesi'nde kabul edilen "Bilgi Toplumu için Tunus Gündemi" dokümanının Uygulama ve İzleme başlığı altında yer alan 105 nolu paragrafı; WSIS'in Cenevre ve Tunus'ta kabul edilen çıktılarının genel olarak izlenmesi görevinin BM Ekonomik ve Sosyal Konseyine (ECOSOC) verilmesini öngörmektedir. Bu karar uyarınca, Haziran 2006'da yapılan ECOSOC toplantısında 2006/46 sayılı nihai karar kabul edilmiştir. Bu kararla; BM Kalkınma için Bilim ve Teknoloji Komisyonu'nun (CSTD) WSIS uygulamalarının izlenmesinde odak noktası olarak görev yapacak ECOSOC'u etkin bir biçimde desteklemesi, özellikle Zirve çıktılarının uygulanmasındaki ilerlemelerin gözden geçirilmesi ve değerlendirilmesinde CSTD'nin görev alması sağlanmıştır [73].

Bilgi Toplumu için Tunus Gündemi'nde kişisel bilgilerin ve mahremiyetin korunmasında uluslararası işbirliğinin güçlendirilmesinin gerekliliği vurgulanmaktadır. İnternetin güvenliği ve sürekliliğinin önemi belirtilmekte, İnterneti ve diğer BİT şebekelerini tehlikelerden ve güvenlik açıklardan korumanın önemli bir gereksinim olduğunun altını çizilmektedir. Ayrıca İnternetin güvenliği ile ilgili sorunların ortak bir anlayışla çözülmesi gerekliliğinin ve güvenlik tehditleriyle

ilgili ulusal ve uluslararası düzeyde mücadelede paydaşlar arasında en iyi uygulama örneklerinin paylaşılması, güvenlikle ilgili bilgilerin toplanması ve yayılması ve bu bilgilere erişimin kolaylaştırılması konularında alınacak önlemler vurgulanmaktadır [74].

4.1.4 Uluslararası Telekomünikasyon Birliği (ITU)

WSIS Zirvesi ve 2006 ITU Tam Yetkili Temsilciler Konferansı sonrası ITU, BİT kullanımında güven ve güvenliğin sağlanmasını koordine etmekle görevlendirilmiştir. Nitekim 2005 yılı Tunus Zirvesinde ITU "BİT kullanımında güven ve güvenliğin sağlanması" konulu C5 numaralı Eylem Planının uygulanmasını sağlamakla görevlendirilmiştir [75].

ITU tarafından siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması ile ilgili birçok çalışma yapılmaktadır. Söz konusu çalışmalardan bazıları aşağıda yer almaktadır:

4.1.4.1 Küresel Siber Güvenlik Gündemi (GCA)

ITU 17 Mayıs 2007'de Küresel Siber Güvenlik Gündemini (GCA) yayımlamıştır. GCA'nın amacı, siber güvenlikle ilgili sorunların ele alınması ve koordine edilmesi ile bu sorunlarla ilgili olarak uluslararası tepki geliştirmek amacıyla bir çerçeve oluşturmaktır [76].

GCA, siber güvenlik alanında dünya çapında tanınmış hükümetlerden, özel sektör temsilcilerinden, uluslararası kuruluşlardan, araştırma kuruluşlarından ve akademisyenlerden oluşan 100'den fazla üst düzey uzmanlar grubunun (HLEG) tavsiyelerinden yararlanmak suretiyle oluşturulmuştur [77].

GCA 5 bölüme ayrılmıştır. Bu bölümler aşağıda yer almaktadır:

1. Yasal Önlemler

2. Teknik ve Usule İlişkin Önlemler
3. Organizasyon Yapısı
4. Kapasitenin Geliştirilmesi
5. Uluslararası işbirliği

4.1.4.2 Siber güvenlik kapısı

ITU tarafından siber güvenliğin sağlanmasına yönelik çözüm önerileri sunulması amacıyla "Siber güvenlik kapısı" adı altında bir İnternet sitesi oluşturulmuştur. Sitede STK'ların, özel sektörün, hükümetlerin, uluslararası kuruluşların çalışmaları hakkında bilgiler verilmekte, ayrıca yasal önlemler, teknik önlemler, kapasitenin geliştirilmesi, organizasyon yapıları ve uluslararası işbirliğinin sağlanmasına yönelik çözüm önerilerine ve ITU'nun çalışmalarına yer verilmektedir [78].

4.1.4.3 Gelişmekte olan ülkeler için siber güvenlik rehberi

2007'de yayımlanan Gelişmekte Olan Ülkeler İçin Siber Güvenlik Rehberinde, gelişmekte olan ülkelerde bilgi teknolojilerine ilişkin konuların daha iyi anlaşılmasının sağlanması ve gelişmiş ülkelerin sorunlarla mücadele amacıyla geliştirdikleri çözüm örneklerinin paylaşılması amaçlanmıştır. Bu çerçevede Rehberde siber güvenlik ve siber suçlara ilişkin bilgiler verilmekte, siber saldırıların türlerinden bahsedilmekte, siber güvenliğin sağlanmasına ilişkin teknik önlemlerin neler olabileceği belirtilmektedir.

4.1.4.4 Ulusal siber güvenlik / kritik bilgi altyapılarının korunması kendini değerlendirme kılavuzu

2008 yılında yayımlanmış olan ve GCA'nın bir parçası olan kılavuzda, ITU üyesi ülkelere siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması alanlarında mevcut politikalarını gözden geçirmeleri ve ulusal siber güvenlik politikası oluşturmalarının sağlanması amaçlanmaktadır [79].

ITU bu çalışmalarının yanı sıra, BOME'ler oluşturulması, ulusal siber suçlara ilişkin ülkelerin mevzuatlarının değerlendirilmesi, şebeke güvenliğinin sağlanması, kötücül yazılımların ve spam'ın önlenmesine ilişkin araştırmalar yapmaktadır. ITU yukarıda belirtilen amaçlar doğrultusunda birçok bölgesel forum ve çalıştay düzenlemektedir. Bunlardan bazıları, Ağustos 2007'de Vietnam'da, Ekim 2007'de Arjantin'de, Kasım 2007'de Cape Verde'de, Şubat 2008'de Katar'da, Haziran 2008'de Avustralya'da, Ağustos 2008'de Zambia'da, Ekim 2008'de Bulgaristan'da, 2009'da Tunus'ta düzenlenmiş olan çalıştaylardır.

4.2 Avrupa Birliği (AB)

Siber güvenliğin sağlanması konusunda AB uluslararası arenada önemli role sahiptir. AB tarafından siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması önemli konular olarak algılanmakta ve bu doğrultuda politikalar geliştirilmektedir.

4.2.1 Avrupa Birliği tarafından kritik olarak kabul edilen sektörler

Avrupa Komisyonu 10 Ekim 2001 tarihli ve 574/2001 sayılı bildirisinde siber saldırılara karşı güvenlik önlemlerinin güçlendirilmesi görevinin özel sektörle birlikte önemli oranda kamu kurumları ve devlete ait olduğunu ve bu nedenle kamu sektörünün üzerine de önemli görevler düşmekte olduğunu ifade etmiştir. AB Komisyonu, kritik altyapıların belirlenmesinde aşağıda yer alan 3 faktörün göz önüne alınması gerektiğini belirtmektedir [10]:

- Kapsam: Kritik bir altyapının kaybı coğrafi alanın büyüklüğü ile değerlendirilir.(Kaybı ya da erişilemezliği durumunda uluslararası, ulusal, yerel olarak etkilenilecek olan alan)
- Büyüklük: Kaybın ya da etkinin derecesi "hiç", "minimum", "orta" veya "büyük" olarak sınıflandırılabilir. Bir olayın büyüklüğünün değerlendirilmesinin kriterleri arasında; kamuya olan etkisi (etkilenen kişi sayısı, hayat kaybının olup olmaması, hastalıklara yol açıp açmadığı, ciddi yaralanmalar, tahliye gerektirip gerektirmemesi); ekonomik etkisi (gayri safi

milli hasılaya olan etkisi, ekonomik kaybın ve/veya ürün ve hizmetlerin bozulmasına yol açması); çevresel etkisi (kamu ve çevre üzerine etkisi); diğer kritik altyapı unsurlarıyla olan bağlılığı; politik etkisi (mücadelede hükümetlere olan güven üzerindeki etkisi) yer almaktadır.

- Zaman etkisi: Etkilendiği takdirde ne kadarlık bir süre zarfında kayıplara yol açacağı (örneğin, hemen, 24–48 saat içerisinde, bir hafta içerisinde)

20 Ekim 2004 tarihinde oluşturulan Terörle Mücadelede Kritik Altyapının Korunması Avrupa Toplulukları İletişim Komisyonu tarafından kritik altyapının tanımı yapılmış, kritik sektörler belirlenmiş ve potansiyel altyapıların belirlenmesi için kriterlerin neler olabileceği tartışılmıştır. Komisyonda, kritik altyapılar "zarar verilmesi ya da yok edilmesi durumunda vatandaşların sağlığı, güvenliği, huzuru ve ekonomik refahı üzerinde veya üye ülkelerin hükümetlerinin işleyişi üzerinde önemli etkilere yol açacak olan fiziksel ve bilgi teknolojileri ağları, hizmetleri, olanakları ve varlıkları" şeklinde tanımlanmıştır. Kritik altyapılar ekonominin birçok sektöründen temel devlet hizmetlerine kadar uzanan geniş bir alanı kapsamaktadır [80].

Avrupa Komisyonu tarafından Avrupa Kritik Altyapıların Korunması Programı (EPCIP) hakkında yayımlanmış olan Yeşil Kitapta kritik sektörler ve bunların ürün ve hizmetleri şu şekilde belirtmiştir [81]:

- Enerji: Petrol ve gaz üretimi, rafine edilmesi, arıtılması, depolanması, iletimi, elektrik üretim ve dağıtımı)
- BİT: Bilgi sistemleri ve şebekelerinin korunması; İnternet; sabit telekomünikasyon hizmetleri; mobil telekomünikasyon; uydu haberleşmesi; radyo ve televizyon yayınları; denizcilik ve radyokomünikasyon
- Su: İçme suyu tedariki, su kalitesinin ve miktarının denetimi
- Gıda: Gıda tedariki, gıda sağlığı ve güvenliğinin denetimi
- Sağlık: Sağlık hizmetleri; ilaçlar, serumlar, aşılar ve eczacılık, biyoloji laboratuarları
- Finans Sistemi: Ödeme Hizmetleri/ödeme yapıları; devlet mali yapılanması

- Kamu ve Hukuk Düzeni ve Güvenlik: Kamu ve hukuk düzeninin yönetimi, güvenlik ve emniyetin sağlanması, yargı kararlarının yerine getirilmesi
- Devlet Yönetimi: Silahlı kuvvetler, hükümet fonksiyonları ve yönetimi, acil yardım hizmetleri, posta ve kargo hizmetleri
- Taşımacılık: Karayolu taşımacılığı; demiryolu taşımacılığı; hava taşımacılığı, deniz taşımacılığı; okyanus ve deniz aşırı taşımacılık
- Kimyasal ve Nükleer Sanayi: Üretim ve depolama/ kimyasal ve nükleer maddelerin işlenmesi; tehlikeli maddelerle ilgili boru hatları (kimyasal maddeler)
- Uzay ve araştırma

4.2.2. Avrupa Birliğinin siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması alanındaki çalışmaları ve politikaları

4.2.2.1 Yeşil Kitap

24 Kasım 2005 tarihinde AB Komisyonu tarafından yayımlanmış olan Yeşil Kitapta AB tarafından kritik altyapıların korunması amacıyla alınması gereken önlemler, hazırlıklar ve sorumluluklar ana hatlarıyla belirlenmiş ve kritik altyapıların korunmasında işbirliğinin önemi vurgulanmıştır. Ayrıca Yeşil Kitapta, EPCIP'in amacı, AB kritik altyapılarının tanımları ve birbirlerine olan bağımlılıkları, ulusal kritik altyapılar, kritik altyapı sahiplerinin, işletmecilerinin ve kullanıcılarının rolü ile Kritik Altyapı Uyarı Bilgi Ağı (CIWIN) gibi konularda bilgi verilmektedir [81].

4.2.2.2 Kritik Altyapı Uyarı Bilgi Ağı (CIWIN)

AB Komisyonu tarafından ortak tehditler ve güvenlik açıkları konusunda AB içerisinde bilgi alışverişini kolaylaştırmak amacıyla Kritik Altyapı Uyarı Bilgi Ağı (CIWIN) oluşturulması kararlaştırılmıştır. AB CIWIN ile üye ülkelere, AB kurumlarına, kritik altyapı sahiplerine ve işletmecilerine ortak tehditler, güvenlik açıkları, alınması gereken tedbirler ve stratejiler konularında kritik altyapıların korunmasına destek vermek suretiyle riskin azaltılmasını ve yardımı amaçlamaktadır

[10].

4.2.2.3 Avrupa Şebeke ve Bilgi Güvenliği Ajansı (ENISA)

5 Haziran 2003 tarihinde ENISA'nın bir tüzel kişilik olarak kurulması kararının alınmasıyla birlikte AB, siber güvenliğin sağlanması konusunda Avrupa koordinasyonunu sağlamak için çabalarını artırmış ve bunun üzerine 14 Mart 2004 tarihinde ENISA kurulmuştur [82].

ENISA toplumda üst düzeyde şebeke ve bilgi güvenliğinin sağlanmasını amaçlamaktadır. Bu nedenle AB vatandaşlarının, tüketicilerin, şirketlerin ve kamu-özel sektör kuruluşlarının yararına şebeke ve bilgi güvenliğinin gelişmesine katkıda bulunmaktadır.

ENISA Avrupa Komisyonunun, üye ülkelerin ve iş dünyasının şebeke ve bilgi güvenliği gereksinimlerini karşılamakta ve hem üye ülkeler hem de AB Kurumları için şebeke ve bilgi güvenliği ile ilgili konularda uzmanlık merkezi hizmeti sunmaktadır. Ayrıca üye ülkelerde şebeke ve bilgi güvenliği alanında çalışan kurumların iletişim bilgilerinden oluşan bir kim kimdir rehberi hazırlamıştır [83].ENISA, Avrupa'daki BOME faaliyetleri hakkında bir envanter oluşturmuştur ve üç ayda bir bülten yayımlamaktadır [84].

ENISA'nın Sinerji Üzerine- Başarı Elde Etmek olarak adlandırılan 2009 yılı Çalışma Programı 2008'de yayımlanmıştır. Programda, ilgili paydaşlarla işbirliği suretiyle ajansın şebeke ve bilgi güvenliği alanında etkisinin artırılması amaçlanmakta ve en iyi uygulama örneklerinin paylaşılması, farkındalık yaratılması ve işbirliğinin sağlanması da dahil olmak üzere, ENISA'nın faaliyetleri hakkında genel bilgi verilmektedir [85].

Ayrıca üye ülkelerde örnek uygulamaların paylaşılması ve geliştirilmesi amacıyla çalıştaylar düzenlemekte, bireysel kullanıcılar gibi spesifik bazı gruplar için özel bilgi paketleri hazırlamakta, farkındalığın geliştirilmesi amacıyla çalışmalar

yapmaktadır.

4.2.3 AB'nin siber güvenliğin sağlanmasına ilişkin mevzuatı

4.2.3.1 1995 tarihli Verilerin Korunması Direktifi (95/46/AT)

1995 tarihli Verilerin Korunması Direktifi (95/46/AT) 24 Ekim 1995'de kabul edilmiştir [86].Mahremiyetin korunmasına kişisel verilerin işlenmesi bakımından bir sınırlama getirmekte olan Direktif, üye ülkelerin anayasaları tarafından hüküm altına alınmış olan bireylerin mahremiyetlerine ilişkin olarak herhangi bir özel hak vermemekte, bunun yerine veri işlemenin bireylerin mahremiyetlerini ihlal etmeyecek şekilde nasıl gerçekleştirileceği konusunda kurallar öngörmektedir [87].

Direktifle, kişisel verilerin işlenmesi sırasında kişi hak ve özgürlükleri ile mahremiyetin korunmasının sağlanması amaçlanmakta ve kişisel bilgilerin AB üyesi ülkelerin ulusal sınırları içerisinde güvenli ve serbest bir şekilde dolaşımını sağlamak üzere düzenleyici bir çerçeve oluşturulmaktadır. Direktifte yalnızca gerçek kişilere ilişkin düzenlemeler yer almakta, tüzel kişilere ilişkin düzenleme bulunmamaktadır. Fakat üye ülkeler bu konuda düzenleme yapma konusunda serbestiye sahiptir.

Direktifte kişisel veri, anonim veri, kişisel verilerin işlenmesi, veri koruma görevlisi gibi kavramlar tanımlanmıştır. Ayrıca verilerin kaliteli olması, kişisel verilerin hukuka uygun olarak işlenmesi, kişisel verilerin ancak ilgili kişinin açık rızası ile işlenebileceği, veri işlem sorumlusunun kişiye bilgi verme yükümlülüğü, ilgili kişinin bu bilgileri elde edebilme hakkı, kişinin haklı sebepler olması durumunda verilerin işlenmesine itiraz edebilme hakkı gibi ilkelere yer verilmiştir.

Direktif kapsamında kişisel verilerin üçüncü ülkelere transferi ancak bu ülkelerde uygun bir koruma düzeyinin bulunması halinde mümkündür. Direktifin 26 ncı maddesi uyarınca verilerin aktarılacağı üçüncü ülkede kişisel verilerin korunmasına ilişkin yeterli düzenleme ve koruma mevcut değilse, aktarma ancak;

- İlgilinin rızası,
- Veri aktarımının sözleşmeden kaynaklanan bir yükümlülüğün yerine getirilmesi için gerekli olması,
- Kamu yararının gerektirmesi,
- Mahkeme kararının yerine getirilmesi

gibi durumlardan birinin veya birkaçının gerçekleşmesi halinde mümkün olmaktadır.

25 inci madde uyarınca ise eğer veri transferi yapılacak ülke AB üyesi ülke değilse fakat Komisyon tarafından o ülkede verilerin korunmasına ilişkin yeterli koruma düzeyi olduğu kabul edilmişse, bu ülke AB üyesi ülkelerle eşit işlem görmektedir.

4.2.3.2 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi (2002/58/AT)

2002 tarihli direktif, 1995 tarihli Verilerin Korunması Direktifini elektronik haberleşme sektörü bakımından tamamlayıcı niteliktedir ve 1997 yılında kabul edilen Telekomünikasyon Hizmetlerinde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Direktifinin yerini almıştır [88].

1995 tarihli direktifte sadece gerçek kişilerin verileri korunmakta fakat üye ülkeler tüzel kişileri koruma kapsamına almak konusunda serbest bırakılmakta iken, 2002 tarihli direktifle tüzel kişilerin verileri de açıkça korunmaktadır.

Direktif elektronik verilerin toplanması ve saklanması; üye ülkelerde verilerin gizliliği, trafik verilerinin saklanmasının sınırlandırılması ve ulusal güvenlikle ilgili istisnaların belirlenmesi ile ilgili mevzuatın oluşturulması konularında üye ülkelere yükümlülük getirmektedir. Ayrıca direktifle, gerekli olmadığı durumlarda trafik verilerinin silinmesi ya da etkisiz hale getirilmesi gerekliliği belirtilmektedir. Fakat bununla birlikte üye ülkelere verilerin belirli süreler için saklanması hususunda kanunlar hazırlamasına izin verilmektedir. Bu kanunlar ulusal güvenliğin, kamu güvenliğinin sağlanması, suçların araştırılması, tespiti ve kovuşturulması ile

elektronik iletişim sistemlerinin yetkisiz kullanılmasının önlenmesi amaçlarıyla uygun ve orantılı olmalıdır [89].

Direktifle elektronik haberleşme alanında temel hak ve özgürlüklere saygı gösterilmesinin, özel yaşamın gizliliği ve verilerin korunmasının sağlanması amaçlanmış, yeni teknolojik gelişmeler karşısında kişisel verilerin korunmasına yönelik düzenlemeler getirilmiştir. Ayrıca bu direktifte yer almayan hususlarla ilgili olarak 1995 tarihli Verilerin Korunması Direktifinin esas alınması gerektiği ifade edilmiştir [89].

Direktifte spame ilişkin düzenlemeler de yer almakta, bireyin önceden rızası bulunmuyorsa spam gönderilmesi yasaklanmaktadır. Ancak spam mevcut müşteri ilişkileri kapsamında reklam, benzer ürünler ve hizmetler için yapılıyor ve bilgisi olan müşteriye reklamdan sonra artık kendi verilerinin reklam amacıyla kullanılmasını ücretsiz ve sorunsuz olarak reddetme seçeneği sunuluyorsa, bu durumda spam gönderilmesi serbest bırakılmaktadır. Ayrıca direktif ile doğrudan reklam amacıyla gönderilen e-postalarda reklam göndericisinin isminin saklanmaması ve geçerli bir adresin bulunmasına ilişkin hükümler de yer almaktadır.

4.2.3.3 2006 tarihli Verilerin Saklanması Direktifi (2006/24/AT)

Verilerin Saklanması Direktifi 15 Mart 2006'da kabul edilmiştir ve bu direktifle 2002/58/AT sayılı direktifte değişiklikler yapılmıştır [90].

Direktifin amacı, üye ülkelerin kendi yasal mevzuatlarında tanımlanmış olan telefon ve e-posta verilerinin, suçların soruşturulması, tespiti ve kovuşturulması amacıyla saklanması hususlarında üye ülkelerin yasal mevzuatlarının uyumunu sağlamaktadır. Direktif gerek tüzel kişilerin gerekse gerçek kişilerin abone veya kayıtlı kullanıcıyı tanımlamak için gerekli yer ve trafik verileri hakkında uygulanmaktadır. Elektronik haberleşmenin içeriği, elektronik haberleşme ağı kullanılarak elde edilen bilgiler de dâhil olmak üzere direktif kapsamında değildir. Üye devletler, internet servis sağlayıcıların iletişim bilgilerini iletişim tarihinden itibaren 6 aydan az 2 yıldan fazla

olmamak üzere saklamalarını sağlamakla yükümlüdür.

4.2.3.4 24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı

24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı (2005/222/JHA) ile etkili araçlar ve yöntemler geliştirmek suretiyle bilgi sistemlerine karşı saldırılarla ilgili ceza yargılamasını güçlendirmek amacıyla işbirliği hedeflenmektedir [91]. Çerçeve kararı kapsamında cezalandırılabilecek suçlar bilgi sistemlerine yetkisiz erişim ve sistemlerin engellenmesi (kasıtlı olarak bir bilgi sistemindeki verileri iletmek, silmek, bozmak, değiştirmek, ortadan kaldırmak veya etkisiz hale getirmek suretiyle bilgi sisteminin işleyişini engellemek veya kesintiye uğratmak) suçlarıdır. Üye ülkeler bu suçların orantılı, etkili ve caydırıcı olması bakımından kanunlarında para cezası hükümlerine yer vermekle yükümlüdür. Ayrıca, çerçeve kararının 11 inci maddesi kapsamında işbirliğinin geliştirilmesi için üye ülkeler 7 gün 24 saat çalışan operasyonel temas (irtibat) noktaları belirlemek zorundadır.

4.3 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)

OECD kritik bilgi altyapılarının, bilgi sistemlerinin ve şebekelerin güvenliği konularında uzun yıllardır yol gösterici çalışmalar yapmakta ve aynı zamanda siber suçlarla, özellikle kötücül yazılımlarla mücadelede önemli görevler üstlenmektedir. OECD bilgi güvenliğinin sağlanması, İnternet ekonomisi açısından bilgi güvenliğinin önemi konusunda toplumda farkındalığının artırılması ve toplum genelinde güvenlik kültürünün geliştirilmesinin sağlanması için hükümetlere ve özel sektöre hizmet etmesi amacıyla raporlar, istatistikler, bildiriler ve tavsiye kararları yayınlamaktadır.

Belirtilen amaçlar doğrultusunda OECD Bilgi Güvenliği ve Gizlilik Çalışma Grubu (WPISP) bu alanlarda güvenliğin sağlanması için küresel çaplı politika belirlenmesi yaklaşımını teşvik etmektedir [92].

İlave olarak Bilgi, Bilgisayar ve Haberleşme Politikaları Komitesi ise (ICCP) bilgi altyapıları ve bilgi toplumu konularında geniş bir politika çerçevesi belirlemek için çalışmaktadır [93].

4.3.1 Bilgi sistemleri ve ağlarının güvenliğine ilişkin OECD rehber ilkeleri: güvenlik kültürüne doğru

OECD ilkeleri ilk olarak 1992 yılında hazırlanmış, 1997 yılında tekrar gözden geçirilmiş, 2001 yılında ise ilkelere son şekli ICCP'nın talebi üzerine WPISP tarafından verilmiştir. 11 Eylül 2001 terör saldırıları OECD'nin siber güvenliğin sağlanması ve kritik bilgi altyapısının korunmasına dair çabaları için bir dönüm noktası olmuş, bu saldırılar üzerine ilkelerin yayımlanması hızlandırılmıştır. 25 Temmuz 2002 tarihinde OECD'nin 1037 nci oturumunda Bilgi Sistemleri ve Ağlarının Güvenliği OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru adlı 9 yeni ilke kabul edilmiştir [32]. Bağlayıcı nitelikte olmayan bu ilkeler, OECD üye ülkeleri ile bilgi teknolojileri sektörü ve STK temsilcilerinin fikir alışverişleri ve konsensusları sonucunda oluşturulmuştur. OECD, üyesi olmayan ülkeleri de kritik bilgi altyapısının korunması alanında benzer bir yaklaşımı benimsemeye davet etmektedir. Ayrıca özel sektör temsilcilerinden kendi alanlarında güvenliklerini artırmaları ve kullanıcıların bilgi ve güncellemeler konusunda bilgilendirilmesini sağlamaları, bireysel kullanıcıların da önlemler almaları ve sorumluluk bilinci içerisinde olmaları konusunda teşvik edilmeleri istenmektedir. OECD ilkeleri tamamlayıcı ilkelerdir ve bir bütün olarak ele alınmaları gerekmektedir.[6]

4.3.2 Kritik bilgi altyapılarının korunmasına dair OECD tavsiye kararı

17–18 Haziran 2008'de Seul'de OECD Konseyi tarafından Kritik Bilgi Altyapılarının Korunmasına Dair Tavsiye Kararı alınmıştır. Amacı kritik bilgi

---

[6] Söz konusu ilkelere 2 nci bölümde "Siber Güvenlik Kültürünün Oluşturulması" başlığı altında yer verilmiştir.

altyapısının korunması için uluslararası işbirliğinin geliştirilmesi olan bu kararda, kritik bilgi altyapılarının önemine değinilmiş, ülkelerin bilgi ve deneyimlerini paylaşmasının ve bu doğrultuda özelikle gelişmekte olan ülkelerle işbirliği içerisinde bulunulmasının önemine değinilmiş, ayrıca bu doğrultuda özel sektöre de önemli görevler düşmekte olduğu ifade edilmiştir. Ayrıca 17–18 Haziran 2008'de Seul'de kötücül yazılımlarla ilgili bir rapor yayımlanmıştır [94].

Tavsiye kararında, uluslararası işbirliğinin güçlendirilmesi ve İnternete küresel bir altyapı olarak önem verilmesinin gereği vurgulanmakta, ulusal kritik altyapıların güvenliğinin ve özel sektörle işbirliğinin önemine, bilginin paylaşılması konusunda gönüllülük ve yeterliliğe, hızlı teknolojik gelişmeler karşısında güçlü bir güvenlik kültürüne ve toplumsal değişime olan ihtiyaç belirtmektedir. Tavsiye kararında bu konularda ilerleme kaydedebilmek için üye ülkeler ortak bir yaklaşım benimsemeye davet edilmektedir.

4.3.3 Spam görev gücü raporu

OECD tarafından 19 Nisan 2006'da Spam Görev Gücü Raporu yayımlanmıştır. Raporda somut düzenleme önerileri, teknik çözümler ve özel sektör girişimleri konusunda bilgiler sunulmaktadır. Ayrıca spamle mücadelede uluslararası işbirliğinin önemine değinilmekte ve ülkelerin tek bir irtibat noktası belirlemeleri gerektiği ileri sürülmektedir. Bireylerin spam konusunda eğitilmelerinin önemli olduğu, bu amaçla hükümetlerin özel sektörle birlikte kampanyalar yürütmesi gerektiği belirtilmekte ve okullarda bu amaçla dersler ve eğitimler verilmesinin, farkındalığın artırılmasının önemine değinilmektedir [95].

Rapor, birbirleriyle bağlantılı olan aşağıdaki unsurlardan oluşmaktadır:

- Spame ilişkin düzenlemeler
- Uluslararası uygulamalarda işbirliği
- Özel sektör önderliğinde spam karşıtı çözümler
- Mevcut ve gelişmekte olan spam karşıtı teknolojiler

- Eğitim ve farkındalık
- Spam ile mücadelede işbirliği
- Spame ilişkin istatistikler
- Küresel işbirliği

4.3.4 Spam karşıtı kanunların sınır ötesi uygulanmasına ilişkin OECD tavsiye kararları

13 Nisan 2006 tarihinde Konseyin 1133 üncü oturumunda alınan kararlar doğrultusunda, üye ülkelerin spame ilişkin kanunları uygulamakla görevli olan kurumlarının kendi aralarında daha hızlı ve etkili işbirliğini sağlamaları amacıyla bir çerçeve oluşturmaları kararlaştırılmıştır [96].

Bu amaçla üye ülkeler;

1. Spame ilişkin kanunlar hazırlamalı ve bu kanunları uygulamakla görevli kurumları belirlemelidir. Ayrıca bu kurumlara spamle mücadele amacıyla gerekli yetki verilmelidir.
2. İşbirliğini geliştirmelidir.Ülkeler, yabancı ülkelerin kurumlarıyla işbirliği içerisinde çalışabilmek amacıyla elde edilen bilgileri paylaşmalı ve bu tavsiye kararları doğrultusunda irtibat noktası belirlemelidir.
3. İlgili özel sektör kuruluşlarıyla işbirliğini sağlamalıdır.

4.3.5 Güvenlik kültürü İnternet sitesi

Aralık 2003'te, küresel güvenlik kültürünü teşvik etmek amacıyla OECD tarafından Güvenlik Kültürü İnternet sitesi kurulmuştur. Sitede, üye ve üye olmayan ülke hükümetlerine OECD Güvenlik İlkelerinin uygulanması konusunda girişimlerde bulunmaları için bilgi alışverişi sağlanmaktadır. Ayrıca OECD çalışmaları, çalıştayları ve uluslararası işbirliğinin sağlanması hakkında bilgiler ve öneriler yer almaktadır [97].

4.3.6 OECD forumları ve çalıştayları

Siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması alanlarında OECD forumlar ve çalıştaylar düzenlemek suretiyle faaliyetlerde bulunmaktadır. Bunlardan birisi, Ocak 2003'te Honolulu'da düzenlenen "Sayısal Ekonomiye İlişkin Politika Modelleri" konulu OECD-Asya-Pasifik Ekonomik İşbirliği (APEC) küresel forumudur [98].

Bu Forum'da bilgi sistemleri ve şebekelerin güvenliğinin sağlanması ile OECD Güvenlik İlkelerinin uygulanmasının önemine değinilmiş ve Aralık 2003'te Cenevre'de düzenlenecek olan WSIS'e hazırlık çalışmalarının önemi üzerinde durulmuştur.

Ayrıca birçok APEC üye ülkesi, Honolulu'da OECD ile APEC arasında işbirliğinin geliştirilmesi amacıyla yapılan anlaşma gereğince 2003 yılında Oslo'da düzenlenecek olan "Bilgi Sistemleri ve Şebekelerinin Güvenliği" konulu OECD Küresel Forumuna davet edilmiştir. Oslo Forumu, siber güvenlik alanında ulusal ve uluslararası çabaların önemli bir diğer aşamasıdır. Oslo Forumunun önemli politika hedefleri arasında şu hususlar yer almaktadır [99]:

- Kritik bilgi altyapılarının korunması doğrultusunda, bilgi sistemlerinin ve şebekelerin güvenliğinin önemi hakkında bireysel kullanıcıların ve ticari işletmelerin farkındalıklarının artırılması,
- OECD Rehber İlkeleri hakkında bilincin artırılması,
- Kuruluşların bilgi sistemlerinin etkili bir şekilde korunmasını sağlayan güvenlik yapılarının geliştirilmesinin teşvik edilmesi,
- Bilgi teknolojileri altyapılarının korunmasında teknolojinin ve güvenlik standartlarının kullanımının teşvik edilmesi.

2005 yılının Eylül ayında Seul'de Bilgi Sistemleri ve Ağlarının Güvenliği konulu OECD-APEC Çalıştayı düzenlenmiştir [100]. Çalıştay kapsamında tartışılan başlıca konular; kötücül yazılımlar ve bunlarla mücadele, küresel olaylara etkili tepkinin

teşvik edilmesi, hükümetlerin ve BOME'lerin rolü, ortaya çıkan yeni güvenlik tehditleri ve bunların belirlenmesi için geliştirilen teknolojiler, araştırma ve geliştirme faaliyetlerinin önemi, bilgi sistemleri ve şebekelerinin güvenliğinin ve yönetiminin sağlanması alanlarında politika yaklaşımlarının belirlenmesi ile bu konudaki kanuni düzenlemelerin karşılaştırılmasıdır.

OECD Mart 2006'da Paris'te ABD Ulusal Bilim Kuruluşu ile birlikte "İnternetin Geleceği" konulu bir çalıştay düzenlemiştir. Bu çalıştayla, "İnternetin Geleceği" konulu projenin ICCP tarafından başlatıldığı belirtilmiştir [101]. Ayrıca 2007 yılında OECD, ABD Ulusal Bilim Kuruluşu ile birlikte "İnternetin Geleceğini Şekillendirmede Etkili Sosyal ve Ekonomik Faktörler" konulu ikinci bir çalıştay düzenlemiştir. Söz konusu çalıştayla, teknolojik ve politik bakış açılarıyla İnternetin geleceği ile ilgili stratejik yönetimlerin tartışılması amaçlanmıştır [102].

Son olarak 16-18 Haziran 2008 tarihleri arasında Seul'de, 30 OECD ülkesinden bakanlar, özel sektör temsilcileri, teknik uzmanlar, üniversiteler ve STK temsilcilerinin ve 15'den fazla OECD üyesi olmayan ülke temsilcisinin katıldığı bir toplantı yapılmıştır. Bu toplantının amacı, İnternet ekonomisinin geliştirilmesine yönelik uygun zemin sağlanması amacıyla İnternet ekonomisinin geleceğinin tartışılması ve politika ve uygulamalar konusunda küresel diyalog, işbirliği ve koordinasyonun sağlanmasıdır [103]. Kritik bilgi altyapısının korunması da dahil olmak üzere İnternet ve diğer bilgi sistemlerinin güvenliğinin sağlanması tartışılan konuların başında gelmiştir.

4.4. Avrupa Konseyi

4.4.1 Avrupa Konseyi Siber Suçlar Sözleşmesi

Avrupa Konseyi, ABD'nin de katkı ve görüşleriyle 19 Eylül 2001 tarihinde siber suçlar hakkında uluslararası bir sözleşme taslağı üzerinde anlaşmaya varmış ve taslak sözleşme metnine yönelik nihai kararı 8 Kasım 2001 tarihinde bakanlar düzeyinde yapılan toplantıda ele alarak, sözleşmeyi 23 Kasım 2001 tarihinde Macaristan'ın

Başkenti Budapeşte'de imzaya açmıştır.

Yürürlüğe girebilmesi için üçü Avrupa Konseyi üyesi olmak üzere beş ülkenin onaylaması gerekmekte olan sözleşme 1 Temmuz 2004'te yürürlüğe girmiştir. Sözleşme 48 maddeden oluşmakta olup, sözleşmeye uygun ulusal düzenlemelerin yapılması, uluslararası işbirliğinin geliştirilmesi ve bu sözleşmeyi imzalayan tüm taraf devletlerde benzer suç tipleri tespit edilerek uluslararası yeknesaklık sağlanması ve böylece toplumun siber suçlara karşı korunması için ortak bir ceza politikasının oluşturulması amaçlanmıştır [1].

Siber suçlarla ilgili ilk ve tek uluslararası sözleşme olan Avrupa Konseyi Siber Suçlar Sözleşmesi, uluslararası alanda siber suçlar konusunda devletler nezdinde en kapsamlı uzlaşmayı sağlamakta ve siber suçlarla mücadelede büyük bir önem taşımaktadır. Ayrıca bilgisayar teknolojisi ve ceza hukuku konusunda da ilk uluslararası belge olma niteliğini haizdir. Sözleşmede ele alınan konular telif hakları ihlalleri, bilgisayarlarla ilgili sahtecilik fiilleri, çocuk pornografisi, şebeke güvenliği ihlalleri, siber suçlarla mücadelede kullanılacak olan yetki ve prosedürlerden oluşmaktadır.

Sözleşmeyi bugüne kadar Avrupa Konseyi üyesi ülkelerden kırkiki (42) ülke imzalamış, bu ülkelerden yirmibeş (25) tanesi ise onaylayarak iç hukuku haline getirmiştir. Sözleşme, üye olmayan ülkelerden Kanada, Japonya, Güney Afrika ve ABD tarafından imzalanmış fakat bu ülkelerden sadece ABD tarafından onaylanarak 1 Ocak 2007 tarihinden itibaren yürürlüğe sokulmuştur. Türkiye ise Avrupa Konseyi Daimi üyeliğine rağmen sözleşmeyi hala imzalamamıştır [104]. Avrupa Konseyi Üyesi olan ülkelerin sözleşmeyi imzalama, onaylama durumlarına ve sözleşmenin yürürlüğe giriş tarihlerine ilişkin çizelge EK'te yer almaktadır.

4.4.1.1 Avrupa Konseyi Siber Suçlar Sözleşmesi'nin temel hükümleri

Sözleşmede yer alan fillerin ortak özelliği, hak sahibi olmadan ve kasıtlı olarak işlenmiş olmalarıdır. Söz konusu fiiller rıza, meşru müdafaa veya zaruret hali gibi durumlarda suç kapsamı dışında bırakılmaktadır. Örneğin Sözleşmenin 8 inci maddesinde düzenlenen bilgisayarla dolandırıcılık suçunda ekonomik kazanç elde etmeye yönelik bir amaç aranmaktadır. Bununla birlikte kamu düzenini sağlamak, ulusal güvenliği korumak veya suça konu filleri araştırmak ve soruşturmak amacıyla gerçekleştirilen eylemler suç kapsamı dışında kalmaktadır.

Sözleşme dört bölümden oluşmaktadır. Birinci bölümde terimler, ikinci bölümde ulusal düzeyde alınacak önlemler, üçüncü bölümde uluslararası işbirliği, dördüncü bölümde ise diğer hükümler başlıkları altında düzenlemeler yer almaktadır.

Sözleşmede bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik bilgisi tanımlarına yer verilmiş, tarafların söz konusu kavramları ülkelerindeki yasalarda tutarlı ve eşdeğer bir biçimde kullanmaları gerektiği fakat kelimesi kelimesine bu yasalara aktarmakla yükümlü olmadıkları ifade edilmiştir [1].

Sözleşmede ulusal düzeyde alınacak önlemler iki kısma ayrılarak düzenlenmiştir. Birinci kısım "maddi ceza hukuku", ikinci kısım ise "usul hukuku" başlığını taşımaktadır. Maddi ceza hukuku başlığı altında düzenlenen kısımda bilgisayar ya da bilgisayar ile ilgili suçlar alanında hem suç sayılacak eylemleri belirleyen hükümler, hem de bağlantılı diğer hükümler yer almaktadır. Bu düzenlemelerin amacı, bilgisayarla işlenen ya da bilgisayarla ilişkili suçlar için ortak bir minimum standart oluşturarak bu suçları önleyici veya tespit edici önlemlerin alınmasıdır [63].

Usul hukuku başlığı altında düzenlenen kısımda ise, maddi ceza hukuku başlığı altında düzenlenen kısımda tanımlanan suçların cezai soruşturması, bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlar ve cezai bir suça ilişkin olarak

elektronik ortamda delil toplanması amacıyla ulusal düzeyde alınacak usul tedbirleri açıklanmaktadır

Avrupa Konseyi Siber Suçlar Sözleşmesinin bir diğer özelliği de uluslararası işbirliğine ilişkin genel kurallar belirlemesidir. Sözleşmede ülkelerin işbirliğini geliştirmeleri ve bilgi alışverişini engelleyecek uygulamalardan kaçınmaları öngörülmektedir. Söz konusu işbirliği bilgisayar sistemleri ve veri ile ilişkili her türlü suçu kapsayacak şekilde sağlanmalıdır. Yardımlaşma, ilke olarak geniş olmalı ve yardımlaşmayı engelleyen unsurlar sınırlandırılmalıdır. İşbirliği yükümlülüğü hem bilgisayar sistemleri ve verileriyle bağlantılı suçlar hem de elektronik ortamda bir suçun delillerinin toplanması konularında geçerli olmalıdır [63].

Sözleşmenin 35 inci maddesi uyarınca taraflar günde 24 saat, haftada 7 gün ulaşılabilen bir irtibat noktası belirlemek zorundadır. Böylelikle soruşturmalarda ani yardım ihtiyacı olduğunda, bilgisayarlarla ilgili suçlara yönelik olarak hizmet verecek etkin bir ağ kurulmuş olacaktır.

4.4.1.2 Sözleşmeye getirilen eleştiriler

Uluslararası alanda siber suçlar konusunda devletler nezdinde en kapsamlı uzlaşmayı sağlayan sözleşme olan ve ayrıca bilgisayar teknolojisi ve ceza hukuku konusunda ilk uluslararası belge olma niteliğini haiz olan Avrupa Konseyi Siber Suçlar Sözleşmesi yaklaşık dört yıl süren uzun bir çalışmanın sonucu olarak ortaya çıkmış olmasına rağmen STK'lardan ve konuyla ilgili sektörlerden pek çok eleştiriye maruz kalmıştır. Sözleşmeye getirilen başlıca eleştirilere aşağıda yer verilmektedir:

- Sözleşmenin hazırlık aşamasında yeterli oranda STK'nın ve konuyla ilgili sektörlerin görüşlerinin alınmadığı ve şeffaflık ve açıklık ilkelerine yer verilmediği iddia edilmiştir. Nitekim Avrupa Konseyi'nin bu tarz belgeleri katılımcı bir süreç içerisinde, tarafların katkılarıyla oluşturma geleneği bulunmaktadır. Sözleşmenin son halini almasına kadar geçen sürede pek çok

sayıda taslak yayınlanmış, ilk taslak 2000 yılında yayınlandığında bu taslağa birçok eleştiri ve birçok katkı yapma isteği yöneltilmiştir. Fakat sözleşmenin son hali itibariyle bu eleştirilerden ve katkılardan pek etkilenmediği iddia edilmiştir.

- Sözleşmenin metninin açık olmadığı ve açıklayıcı metinde de söz konusu boşluğun giderilememiş olduğu belirtilmektedir.
- Sözleşmenin 1981 tarihli Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme ile uyumluluk göstermediği, kişisel verilerin korunması konusuna önem verilmediği belirtilmektedir.
- Sözleşmenin Avrupa İnsan Hakları Sözleşmesi ile uyum içerisinde olmadığı, temel kişilik haklarına saygı gösterilmediği iddia edilmektedir.
- Sözleşmede ön plana çıkan noktanın usule ilişkin hükümler olduğu ve siber suçların bir bölümünün dışında genel olarak siber suçlarla mücadelede kullanılan yetki ve prosedürlere yer verildiği belirtilmektedir [105].

4.4.2 Avrupa Konseyi Siber Suçlar Sözleşmesine Ek Protokol

1990 yılı sonrası Berlin Duvarının yıkılmasını takiben, örgütlü ırkçılık ve yabancı düşmanlığı eylemlerinin artması ve bu örgütlerin birbirleriyle bilişim sistemlerini ve İnterneti kullanarak haberleşmeleri üzerine, Avrupa Konseyi tarafından Siber Suçlar Sözleşmesine ek olarak "Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suçlar Sözleşmesine Ek Protokol" hazırlanarak 28 Ocak 2003 tarihinde imzaya açılmıştır. Bugüne kadar Protokol yirmi ülke tarafından imzalanmıştır. Bu Ek Protokol ile her türlü ırkçı ve yabancı düşmanlığı içeren verinin üretilmesi, bunların bilişim sistemleri aracılığıyla yayılması, bu tür düşüncelerin sanal ortamda propagandasının yapılması eylemleri suç olarak düzenlenmiştir [61].

4.4.3 Avrupa Konseyi Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme (108 nolu sözleşme)

Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde kabul edilmiştir [106]. 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. Üye ülkeler sözleşme hükümlerini doğrudan iç hukuka aktarmakla veya sözleşme hükümlerine uygun olarak kendi verilerin korunması kanunlarını çıkartmakla yükümlüdür. Ayrıca ülkelerin sözleşmede yer alan korumadan daha geniş bir koruma benimsemelerine de engel bulunmamaktadır.

Sözleşmeye göre kişisel veriler:

- Hukuka ve dürüstlük kurallarına uygun olarak elde edilmeli ve işlenmeli,
- Belirli ve meşru amaçlar için saklanmalı ve bu amaçlara uygun bir şekilde kullanılmalı,
- Saklandığı amaca uygun ve yeterli olmalı,
- Doğru olmalı ve gerekli olduğu hallerde güncel olarak saklanmalı,
- Verilerin saklanmasını gerektiren amaç bakımından gerekli olduğundan daha uzun süre saklanmamalıdır.

Ayrıca veri güvenliği açısından ise, saklanan kişisel verilerin kazalara, yetkisiz erişimlere, değiştirilmelere veya yaymalara karşı korunması için uygun güvenlik önlemlerinin alınması gerektiği ifade edilmiştir [87].

Avrupa Konseyi tarafından 2007 yılından itibaren sözleşmenin kabul edildiği 28 Ocak günü "verilerin korunması günü" olarak kutlanmaya başlanmıştır ve bu kapsamda çeşitli etkinlikler düzenlenmektedir.

Sözleşme 44 üye ülke tarafından imzalanmış ve bu ülkelerden sadece Türkiye, Rusya

ve Ukrayna tarafından onaylanarak iç hukukları haline getirilmemiştir [107]. Sözleşmenin 4 üncü maddesinde ülkelerin sözleşmeyi onaylamadan önce iç hukukta yapacağı yasal düzenlemeler ile bu sözleşmede öngörülen temel ilkeleri yerine getirme yükümlülüğü getirilmektedir. Ülkemizde henüz kişisel verilerin korunmasına dair yasal düzenleme mevcut olmadığından, sözleşme imzalanmış olmasına rağmen henüz onaylanmamıştır.

4.5 G8 Grubu (G8)

1995 yılından bu yana G8 siber güvenlik, bilgi toplumu ve kritik bilgi altyapısının korunması konularına her geçen gün daha fazla müdahil olmaktadır. 1995 yılında düzenlenen Halifax Zirvesinde organize suçlarla mücadele amacıyla mevcut uluslararası anlaşmaları ve mekanizmaları incelemek ve değerlendirmek üzere Üst Düzey Uzmanlar Grubu görevlendirilmiştir. Bu zirve sonrasında G8 Üst Düzey Uzmanlar Grubu tarafından kırk önemli tavsiye kararı alınmış ve bu kararlar 1996 yılında Lyon'daki G8 zirvesinde kabul edilmiştir. Lyon Grubu olarak bilinen G8 Üst Düzey Uzmanlar Grubu yüksek teknoloji suçlarının öneminin anlaşılmasını sağlayan ilk uluslararası forumdur.

15–17 Mayıs 2000 tarihleri arasında Fransa'nın başkenti Paris'te, G8 ülkeleri ve diğer ilgili tarafların hükümet yetkilileri ve özel sektör temsilcilerinin katıldığı "Kamu Kurumları ve Özel Sektör Temsilcileri Arasında Sanal Ortamda Güven ve Güvenilirliğin Sağlanmasına ilişkin Diyalog Geliştirilmesi" konulu konferans düzenlenmiştir [108]. Konferansın amacı, yüksek teknoloji suçları ve İnternetin suç işlemek amacıyla kullanılması ile ilgili ortak problemlerin tartışılması ve çözüm önerileri getirilmesidir. Söz konusu konferansla G8 üye ülkeleri, BİT'in hukuka aykırı ya da zarar verme amacıyla kullanılmasıyla mücadelede hükümet ve özel sektör arasında bir diyalog sağlanmasının gerekli olduğu konusunda ikna olmuş ve siber suçların açık ve şeffaf bir çerçevede ele alınması gerektiği hususunda anlaşmışlardır.

11 Eylül 2001 saldırılarından sonra Ekim 2001'de G8 Adalet ve İçişleri Bakanlıkları

temsilcilerinin katılımıyla Roma'da düzenlenen toplantıda, uluslararası terörle mücadele kararı alınmış ve uluslararası suçlarla mücadele eden Lyon Grubu ile uluslararası terörle mücadele eden Roma Grubu birleştirilmiştir. Lyon/Roma Grubu yılda 3 kez düzenli olarak toplantılar düzenlemektedir. Lyon/Roma Grubu, uluslararası terörle mücadele faaliyetlerini sürdürmekle birlikte, hukuk sistemlerinin geliştirilmesi ve İnternetin terör amaçlı kullanımının önüne geçilmesi gibi amaçlarla faaliyetler yürütmektedir [109].

4.5.1. Küresel Bilgi Toplumu Okinowa Şartı

Küresel Bilgi Toplumu Okinowa Şartı Temmuz 2000'de yayımlanmıştır [110]. Şartta, BİT'in toplumların sosyal ve ekonomik olarak ilerlemelerini sağlayan, 21. yüzyılı şekillendiren en etkili güçlerden biri olduğu ifade edilmiş, toplumun tüm kesimlerinin BİT kullanmasının sağlanmasının önemine değinilmiş ve bu hedefin sağlanmasında gerek kamuya, gerekse özel sektöre önemli görevler düştüğü belirtilmiştir. Şartta, küresel bilgi toplumunun oluşturulabilmesi için suç işlenme oranının minimum olduğu güvenli bir sanal ortamın şart olduğu ve bu amaçla uluslararası işbirliğinin önemi vurgulanmıştır. Ayrıca OECD İlkelerinde yer alan güvenlik önlemlerinin siber suçlarla mücadeledeki önemine değinmek suretiyle bilgi sistemlerinin güvenliği hususunda OECD İlkelerine atıfta bulunulmuştur. Lyon Grubu çerçevesinde G8 faaliyetlerinin hızlandırılacağı ve bu amaçla özel sektörle de işbirliği içerisinde olunacağı kararlaştırılmıştır. Sayısal uçurumun azaltılmasının öneminden bahsedilmiş ve bu amaçla eğitim faaliyetleri yürütülmesinin önemi vurgulanmıştır. Bununla birlikte gelişmekte olan ülkeler için de uluslararası işbirliğinin güçlendirilmesinin önemine değinilmiştir.

4.5.2. Kritik bilgi altyapılarının korunması hakkında G8 ilkeleri

G8 ülkesi üyelerden üst düzey uzmanlar ve bu alanda faaliyet gösteren işletmeciler, kritik bilgi altyapılarının korunması amacıyla ilk çok uluslu toplantıyı Mart 2003'de Paris'te düzenlemiştir. Bunun üzerine 5 Mayıs 2003 tarihinde G8 Adalet ve İçişleri Bakanları tarafından kritik bilgi altyapılarının korunması hakkında 11 ilke kabul

edilmiştir. Bu ilkelere aşağıda yer verilmiştir [111]:

1. Ülkelerin siber güvenlik açıkları, tehlikeler ve olaylar için acil durum uyarı ağlarını oluşturmaları gerekmektedir.
2. Ülkelerin kritik bilgi altyapılarının yapısı, kapsamı ve bunların korunmasında herkesin üzerine düşen görevler hakkında paydaşlarının farkındalıklarını artırmaları gerekmektedir.
3. Ülkeler kritik altyapılarının korunmasının sağlanması amacıyla altyapılarını incelemeli ve kritik altyapıları arasındaki bağlantıları belirlemelidir.
4. Ülkeler bilgi ve iletişim sistemlerine saldırıların ve zararın önlenmesi, soruşturulması amacıyla kritik bilgi altyapısının paylaşımı ve analizi suretiyle kamu veya özel sektör paydaşları arasındaki işbirliğini teşvik etmelidir.
5. Ülkeler kriz haberleşme ağları oluşturmalı ve acil durumlarda sağlam ve dayanıklı olabileceklerine dair bu ağları test etmelidir.
6. Ülkeler verilerin elde edilebilirliğine dair politikalarının kritik bilgi altyapısının korunması ihtiyacına cevap verebilecek durumda olmasını sağlamalıdır.
7. Ülkeler kritik bilgi altyapılarına olan saldırıların takibini kolaylaştırmalı ve gerektiği durumlarda bu bilgileri diğer ülkelerle de paylaşmalıdır.
8. Ülkeler kritik bilgi altyapılarına saldırı durumunda sürekliliğin sağlanması için eylem planlarını kontrol etmeli, müdahale yeteneklerini artırmak için eğitim faaliyetleri yürütmeli ve paydaşlarını da benzer faaliyetlerde bulunmaları için teşvik etmelidir.
9. Ülkeler kritik bilgi altyapılarına saldırı durumunda soruşturma ve kovuşturma yapabilecek ve bu kovuşturmaları diğer ülkelerle işbirliği halinde yürütebilecek, ana hatları Avrupa Konseyi Siber Suçlar Sözleşmesinde belirlenmiş usul ve esasla ilgili mevzuata ve eğitimli personele sahip olmalıdır.
10. Ülkeler kritik bilgi altyapılarının güvenliğinin sağlanması amacıyla uluslararası işbirliğine gitmeli, güvenlik açıkları, tehlikeler ve olaylar karşısında acil durum uyarı sistemlerinin geliştirilmesi ve iç hukukları

kapsamında soruşturmaları takip etmek suretiyle kritik bilgi altyapılarının güvenliğini sağlamalıdır.

11. Ülkeler ulusal ve uluslararası araştırma ve gelişmeleri takip etmeli ve uluslararası standartlara uygun güvenlik teknolojilerinin uygulanmasını teşvik etmelidir.

Belirtilen 11 ilke kritik bilgi altyapısının korunması konusunda ulusal bazda neler yapılması gerektiğine dair bir rehber niteliği taşımaktadır. Bu ilkelerin kabul edilmesiyle yeni bir "güvenlik kültürü" ortaya çıkmış ve G8 üye ülkelerine uluslararası işbirliğinin güçlendirilmesi, acil durum uyarı ağlarının geliştirilmesi, en iyi uygulama örneklerinin paylaşılması gibi yükümlülükler getirilmiştir.

Ayrıca "Küresel siber güvenlik kültürü oluşturulması ve kritik bilgi altyapısının korunması" konulu Ocak 2004 tarihli ve 58/199 sayılı BM Genel Kurulu Kararının ekinde bu 11 ilkeye yer verilmek suretiyle söz konusu ilkelerin önemi bir kez daha vurgulanmıştır [112].

4.5.3 Yüksek teknoloji suçları alt grup faaliyetleri

Lyon Grubunun alt gruplarından birisi olan Yüksek Teknoloji Suçları Alt Grubu, siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması ile ilgili konular üzerinde çalışmaktadır. Grubun amacı, G8 Ülkelerinin bağlı olduğu kritik altyapıların korunmasını sağlamak ve G8 Ülkeleri ile ortaklaşa iş yapan çok uluslu şirketlere uluslararası bilgi paylaşım mekanizması kurulması konusunda yol göstermektir [10].

2005 yılında G8 Başkanlığı döneminde İngiltere, kritik bilgi altyapısının korunmasında ana hedeflerinin uluslararası işbirliğinin geliştirilmesi olduğunu belirtmiştir. 15–17 Haziran 2005 tarihleri arasında Sheffield'da G8 Adalet ve İçişleri Bakanlarının katıldığı bir toplantı düzenlenmiştir. Bu toplantı sonrasında Adalet ve İçişleri Bakanları tarafından bir bildiri yayınlanmıştır. Bildiride şu kararlar yer almıştır [10] :

- Özel sektörle işbirliğinin sürdürülmesi ve güçlendirilmesi,
- Kurumların siber saldırılara ve olaylara anında müdahale edebilmelerinin sağlanması,
- G8 Ülkelerinin güvenlik açıklarının ve tehlikelerin ortaya çıkarılabilmesi amacıyla izleme ve uyarı birimleri kurmalarının sağlanması,
- İzleme ve uyarı birimleri ile kurumlar arasında iletişimin ve bilgilerin paylaşılmasının sağlanması ve geliştirilmesi,
- Ulusal ve uluslararası eğitim faaliyetlerinin yürütülmesinin sağlanması.

5. ÜLKE YAKLAŞIMLARI

Bu bölümde, siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması alanlarında başarılı olan Avustralya, İngiltere, ABD ve Kanada'nın uygulamalarına ve politikalarına yer verilmiştir.

5.1 Avustralya

5.1.1 Avustralya'da kritik altyapının korunmasına yönelik çalışmalar

Avustralya'da kritik altyapı "Zarar görmesi veya kullanılamaz hale gelmesi durumunda ulusun sosyal, ekonomik refahı veya ülkenin ulusal savunmasının ve ulusal güvenliğinin sağlanması üzerinde etkisi olabilecek fiziksel donanımlar, tedarik zincirleri, bilgi teknolojileri ve iletişim şebekeleri" şeklinde tanımlanmıştır [113].

Avustralya'da kritik altyapıların korunması programı Avustralya Başsavcılık Makamı (AGD) sorumluluğunda, Kritik Altyapının Korunması Güvenli Bilgi Paylaşım Ağı (TISN) tarafından yönetilmektedir. TISN tarafından Avustralya için kritik sayılabilecek dokuz sektör şu şekilde belirlenmiştir [114]:

- İletişim
- Enerji
- Bankacılık ve Finans
- Gıda Tedariki
- Acil Hizmetler
- Sağlık
- Kitlelerin Toplanma Alanları
- Ulaştırma
- Kamu Hizmetleri

5.1.1.1 Avustralya'nın kritik altyapının korunması politikasında rehber ilkeler

Avustralya'da birçok ülkede de olduğu gibi kritik altyapılar ticari işletmeler tarafından kurulmakta ve işletilmektedir. Kritik altyapıların korunması, altyapı sahipleri ve işletmecilerinin, düzenleyici kurumların, sanayi kuruluşlarının hükümet ve kamu ile her düzeyde işbirliğini ve aktif katılımını gerektirmektedir. Bu işbirliği ve koordinasyonun sağlanması için bütün katılımcıların kritik altyapıların korunmasına ilişkin genel ilkelere uyum sağlaması gerekmektedir. Her bir ilke diğeriyle bağlantılı olduğundan bu ilkelerin bir bütün olarak değerlendirilmesi gerekmektedir. Söz konusu ilkelere aşağıda yer verilmektedir [115]:

- Kritik altyapının korunması kamu sağlığı, kamu güvenliği ve güveninin sağlanmasına yönelik risklerin en aza indirgenmesi ile ülkenin rekabet edebilme gücünün sağlanmasında ve kamu hizmetlerinin devamlılığı açısından hayati önemi haizdir.
- Kritik altyapının korunmasının amacı, kritik altyapıların belirlenmesi suretiyle güvenlik açıklarının, tehlikelerin tespit edilmesi ve Avustralya'nın saldırılara karşı hazırlıklı olması ve korunmasının sağlanmasıdır.
- Altyapıların tümünün tamamen korunması söz konusu olamayacağından, risk yönetimi teknikleri geliştirilmeli, öncelikler belirlenmeli ve bu suretle iş devamlılığı sağlanmalıdır.
- Bilgi teknolojileri ve haberleşme şebekelerine yönelik risklerin yönetimi sorumluluğu öncelikli olarak altyapı sahipleri ve işletmecilerine aittir.
- Kritik altyapının korunmasında kamu kurumları ile altyapı sahipleri ve işletmecilerinin işbirliği içerisinde hareket etmesi gerekmektedir.
- Tehlikelere ve güvenlik açıklarına yönelik bilgi paylaşımının sağlanması amacıyla hükümet, kritik altyapı sahibi ve işletmecilerini riskleri daha iyi yönetebilmeleri konusunda destekleyecektir.

5.1.1.2 Avustralya'nın kritik altyapının korunmasına yönelik terörle mücadele politikası

Kritik altyapıların terör saldırılarına karşı korunmasından öncelikli olarak Ulusal Terörle Mücadele Komitesi (NCTC) sorumlu olmakla birlikte, özel sektör ile Avustralya federal, devlet ve bölge hükümetleri de bu sorumlulukları paylaşmaktadır. Bu amaçla Eylül 2005'te Terörle Mücadele Ulusal Planı yayımlanmıştır (NCTP). Planda sorumluluklar, yetkili kurum ve kuruluşlar ve terörü önlemek için gerekli mekanizmalar ana hatlarıyla belirlenmiş; bu planının gerek görüldükçe güncelleneceği, ayrıca en az üç yılda bir NCTC tarafından gözden geçirileceği ifade edilmiştir. NCTP'de kamu-özel sektör işbirliğinin önemi vurgulanmış ve terör faaliyetlerine karşı kritik altyapının korunmasına ilişkin önleyici tedbirlerin alınmasının önemi vurgulanmıştır. Ayrıca bu konuda kamunun güveninin sağlanmasının da önemli olduğu, bu amaçla halkın doğru ve güncel bir şekilde bilgilendirilmesinde medyanın da önemli bir göreve sahip olduğu belirtilmiştir [116].

5.1.1.3 E-güvenlik ulusal gündemi (ESNA)

2001 yılında BİT'deki gelişmelerin ışığı altında Avustralya hükümeti tarafından E-Güvenlik Ulusal Gündemi (ESNA) yayımlanmış, daha sonra ESNA yeniden gözden geçirilerek 2006 yılında yeni versiyonu yayımlanmıştır. ESNA'da, siber güvenliğin sağlanması amacıyla bütçede 73.6 milyon dolar ayrıldığı ifade edilmiştir [117].

ESNA'da, kritik altyapıların korunmasında ve siber güvenliğin sağlanmasında bireysel kullanıcıların, KOBİ'lerin ve hükümetin bir bütün olarak algılanması gerektiği ve aralarındaki işbirliğinin güçlendirilmesinin önemi vurgulanmış, bu amaçla E-Güvenlik Politikası ve Koordinasyon Komitesi oluşturulmuştur. Siber güvenliğin sağlanması ve kritik bilgi altyapısının korunmasını sağlamak amacıyla ESNA'da aşağıdaki kurumlar görevlendirilmiştir:

5.1.1.3.1 Savunma Sinyalleri Müdürlüğü (DSD)

DSD Avustralya'nın bilgi güvenliğinin, bilgi ve iletişim sistemlerinin ve resmi iletişiminin korunmasında önemli bir rol oynamaktadır. Bu görevini kriptografi, ağ güvenliği ve bilgi güvenliği konularında ilkeler ve politikalar geliştirerek uzman desteği sağlamak suretiyle yerine getirmektedir [118].

ESNA'da, kamu kurumlarının İnternet üzerinden sundukları hizmetlerin artmasıyla birlikte güvenlik tedbirlerinin alınmasının da zorunlu hale geldiği, bireylerin mahremiyetinin, kişisel verilerinin korunmasının, güvenliğinin sağlanmasının öncelikli konular arasında sayıldığından, DSD'nin kamu kurumlarına kendi bilgi ve iletişim şebekelerinin ve sistemlerinin güvenliğinin sağlanmasında sağlayacağı desteğin artırılması gerektiği ifade edilmektedir. DSD'nin özellikle kamu kurumlarının bilgi ve iletişim şebekelerinin güvenliğinin sağlanmasında, ulusal güvenliğin sağlanmasında ve gizli, özel bilgilerin korunmasında önemli görevleri olduğu belirtilmektedir.

5.1.1.3.2 Avustralya Hükümeti Bilgi Yönetim Ofisi (AGIMO)

Maliye ve İdari İşler Bakanlığı'nın bir bölümü olan AGIMO, BİT'in kamu yönetimi ve hizmetleri ile ilgili alanlarında stratejik tavsiye, faaliyet ve beyanlarda bulunmaktadır. Ayrıca hükümetin bilgi ve iletişim sistemlerine karşı bir saldırı olması durumunda kamu hizmetlerinin devamının sağlanabilmesi için yasal bir çerçeve oluşturmakla ve Avustralya'nın ulusal kritik bilgi altyapılarının korunmasının sağlanması ile yükümlü kılınmıştır.

AGIMO, diğer kamu kurumlarıyla işbirliği içerisinde Avustralya'yı BİT ile ilgili konularda uluslararası toplantılarda ve forumlarda temsil etmektedir. Ayrıca devlet ve bölge hükümetleri ile işbirliği suretiyle ".gov.au" alan adını yönetmektedir [119].

5.1.1.3.3 Başsavcılık Makamı (AGD)

AGD, Avustralya'nın hukuk ve adalet sisteminin geliştirilmesi ile ulusal güvenliğin sağlanmasına, acil durum yönetim sistemlerinin geliştirilmesine yönelik olarak hükümete uzman desteği sağlamakla görevlidir. AGD'nin amacı, adil ve güvenli bir toplum hedefine ulaşmaktır [120].

AGD bünyesinde terörle mücadele, ulusal güvenliğin sağlanması ve kritik altyapının korunması ile ilgili mevzuatın geliştirilmesi ve politikaların uygulanmasından sorumlu olan Güvenlik ve Kritik Altyapı Bölümü (SCID) bulunmaktadır. SCID, 1999 yılında hayata geçirilmiş olan "Ulusal bilgi altyapısının korunması projesi" ile bu konularda politika ve yasal düzenleme önerileri sağlamak amacıyla Avustralya hükümetinin kritik bilgi altyapısının korunması faaliyetlerini koordine etmektedir.

AGD GovCERT'in faaliyet alanlarını genişletmek suretiyle kritik altyapı sahiplerine, işletmecilerine ve kamu kurumlarına, bir saldırı olması durumunda alınması gereken önlemleri belirlemek ve bilgi paylaşımını sağlamakla görevlendirilmiştir.

5.1.1.3.4 Avustralya Federal Polisi (AFP)

2001 tarihli Siber Suçlar Kanunu'nun yürürlüğe girmesi, AFP'yi siber suç tehlikesine karşı devlet ve bölge polis güçlerini ulusal bir kurum bünyesinde birleştirmeye teşvik etmiş ve bu amaçla Avustralya Yüksek Teknoloji Suçları Merkezi (AHTCC) kurulmuştur. AHTCC kritik bilgi altyapısının korunması ile görevlidir ve bu görev kapsamında ulusal bilgi altyapısına karşı saldırıları da içeren yüksek teknoloji suçlarıyla mücadele amacıyla ulusal koordinasyon yaklaşımını benimsemektedir [121].

ESNA'da etkili ve güçlü bir kolluk kuvvetleri oluşturulmasının, hükümetin kritik bilgi altyapısının korunmasında ve güvenli bir sanal ortam oluşturulmasında önemli olduğu, bu amaçla AFP'nin gelişmiş soruşturma ve araştırma teknikleri vasıtasıyla suçları önleyebileceği veya suçluları tespit edebileceği ifade edilmiştir. Ayrıca Asya-

Pasifik Bölgesinde işbirliğini sağlamak suretiyle AFP'nin ülkenin güvenliğinin sağlanmasına önemli katkı sağlayacağı ifade edilmiştir.

5.1.1.3.5 Genişband İletişim ve Dijital Ekonomi Bakanlığı (DBCDE)

ESNA'da bireysel kullanıcıların ve KOBİ'lerin günlük hayatta BİT'i bankacılık, alışveriş gibi amaçlarla her geçen gün daha fazla kullandıkları fakat güvenlik konusunda yeterince bilgili olmadıkları, bu nedenle de bu konularda farkındalıklarının artırılması gerektiği ifade edilmiştir. DBCDE'nin bu amaçla eğitim faaliyetleri düzenlemesi, öğrencilerin ve velilerinin bu konuda bilgilendirilmelerinin sağlanması gerektiği belirtilmiştir. Ayrıca bilginin yayılması için en önemli projelerden birinin DBCDE tarafından idare edilen ve hükümetin web sitesi olan "staysmartonline" olduğu ifade edilmiştir [10].

5.1.1.3.6 Avustralya Telekomünikasyon ve Medya Kurumu (ACMA)

ESNA'da, bireysel kullanıcıların ve küçük işletmelerin spam gönderilmesi, hizmetin engellenmesi saldırıları düzenlenmesi ve kişisel ve mali bilgi hırsızlığı gibi suçların hedefinde olduğu ifade edilmiştir. Bu doğrultuda ACMA internet servis sağlayıcıları ile birlikte çalışmak suretiyle bireysel kullanıcıların ve KOBİ'lerin güvenliklerini sağlamakla yükümlü kılınmıştır. Ayrıca 2003 tarihli Spam Kanununun uygulanmasından ACMA sorumludur [122].

5.1.1.3.7 E- Güvenlik Politikası ve Koordinasyon Komitesi (ESPaC)

ESNA'da siber güvenliğe ilişkin farkındalığın artırılması, araştırma ve geliştirme faaliyetlerinin yürütülmesi ve siber güvenlikle ilgili kamu politikalarının koordine edilmesiyle görevlendirilmek üzere hükümet temsilcilerinden oluşan bir komitenin oluşturulacağı ifade edilmiş, bunun üzerine 2007 yılında ESPaC Komitesi oluşturulmuştur.

ESPaC Komitesi AGD tarafından yönetilmektedir ve

- ACMA
- AGIMO
- AFP
- ASIO
- DBCDE
- DSD
- Savunma Bakanlığı
- Başbakanlık ve Bakanlar Kurulu
- Ulusal Vergi Dairesi

temsilcilerinden oluşmaktadır.

Ayrıca gerek duyulduğunda, diğer kamu kurumu temsilcileri de gözlemci olarak komite toplantılarına davet edilmektedir. Bu grupların ESPaC Komitesi bünyesine katılması ile kritik altyapıların korunması alanında bireysel kullanıcılar, KOBİ'ler ve kamu kurumları arasında işbirliği ve koordinasyon sağlanmıştır [123].

ESNA kapsamında belirtilen kurumların yanı sıra, siber güvenliğin sağlanmasında Avustralya Güvenlik İstihbarat Teşkilatı (ASIO) da önemli görevler üstlenmektedir. ASIO, Avustralya'nın ulusal güvenlik servisidir ve görevleri 1979 tarihli Avustralya Güvenlik İstihbarat Örgütü Kanunu ile düzenlenmiştir. ASIO'nun esas görevi devletin ulusal güvenliğini tehdit edebilecek durumlara karşı önceden uyarıda bulunmak ve bilgi ve istihbarat toplamaktır. ASIO Kanununda güvenlik, "Avustralya'nın ve vatandaşlarının casusluk, sabotaj, toplumsal şiddetin teşvik edilmesi, Avustralya'nın savunma sistemi ve yabancı girişim eylemlerine karşı korunması" olarak tanımlanmaktadır [124].

5.1.2 Avustralya'nın kamu-özel sektör işbirliğinin sağlanmasına yönelik çalışmaları

5.1.2.1 Kritik Altyapının Korunması Güvenli Bilgi Paylaşım Ağı (TISN)

AGD tarafından yapılan bir açıklamada, salt hükümet tarafından düzenleme yapılması yolunun kritik altyapıların korunmasının en iyi şekli olmadığı belirtilmiştir. Kritik altyapı sahipleri ya da işletmeciler kritik altyapıların en iyi şekilde nasıl korunacağını, beklenmedik bir durum karşısında ne şekilde davranılacağını bilmekte olduğundan, kamu-özel sektör işbirliğinin sağlanmasının önemli bir unsur olduğu ifade edilmiştir [125]. Bunun üzerine 2002 yılında hükümet, kamu-özel sektör işbirliğinin teşvik edilmesi amacıyla TISN'ın kurulduğunu duyurmuştur [126].TISN, Avustralya'nın kritik altyapı sektörleri esas alınarak oluşturulmuştur.

TISN bünyesinde Altyapı Güvencesi Danışma Grubu (IAAGs) olarak adlandırılan her bir sektör grubuna o sektörden kritik altyapı temsilcisi başkanlık etmektedir [127]. Üyelik kritik altyapı sahipleri ve işletmecileri ile sınırlıdır. IAAGs'lara lojistik destek, o konularla ilgilenen hükümet temsilcileri tarafından (Örneğin, sağlık grubuna destek Sağlık Bakanlığı tarafından) sağlanmaktadır. Her bir sektör grubu TISN'da kendi başkanları tarafından temsil edilmekte ve sonuçlar başsavcıya raporlanmaktadır. Bu, kritik altyapı sahipleri ve işletmecilerinin Avustralya hükümetiyle üst düzeyde iletişim kurabilmelerinin yoludur.

5.1.3 Avustralya'nın bilgisayar olaylarına müdahale faaliyetleri ve siber güvenlik kültürü oluşturulmasına yönelik çalışmaları

Avustralya'da siber saldırılara karşı müdahale hizmeti sağlayan iki ana kuruluş vardır. Bunlar; Federal ve eyalet/bölge bilgi teknolojileri şebekeleri için destek sağlayan ve DSD tarafından yönetilen Bilgi Güvenliği Olay Tespit Raporlama ve Analiz Programı (ISIDRAS) ve kritik altyapı işletmecilerine benzer hizmetler sunan Avustralya Bilgisayar Acil Durum Müdahale Ekibidir (AusCERT). Ayrıca,

Avustralya Hükümeti tarafından siber güvenlik kültürünün oluşturulması amacıyla DSD denetiminde OnSecure adlı bir website uygulaması da başlatılmıştır [10].

5.1.3.1 ISIDRAS

ISIDRAS DSD tarafından yönetilmektedir ve amacı, hükümetin bilgi ve iletişim sistemlerinin güvenliğini etkileyen güvenlik olaylarına ilişkin bilgilerin elde edilmesidir. ISIDRAS, bilgi güvenliği olaylarının analizini yapmak ve Avustralya'nın kritik bilgi sistemlerine karşı tehlikeler ve güvenlik açıklarıyla ilgili bilgileri sağlamak suretiyle, bu sistemlerin en üst düzeyde nasıl korunabileceğine ilişkin bilgi sağlamaktadır. ISIDRAS olayları düzenli bir şekilde DSD'ye raporlamaktadır [10].

5.1.3.2 AusCERT

AusCERT, Avustralya ve Yeni Zelanda için oluşturulmuştur ve Asya/Pasifik bölgesinin önde gelen ulusal BOME'sidir. Queensland Üniversitesinde yer alan, kar amacı gütmeyen bağımsız bir kuruluş olan AusCERT'de üyelik hem bireylere hem de kurum ve kuruluşlara açıktır. AusCERT, ulusal bilgi altyapısını etkileyen bilgisayar acil durumlarıyla ilgili konularda Avustralya hükümetinin diğer ülkelerle irtibat noktasıdır. Yabancı ülkelerden bilgi almakta ve bu bilgileri Avustralya kritik bilgi altyapı sahipleri ve işletmecilerine aktarmaktadır. Fakat günlük bilgisayar olaylarına müdahale etmemektedir [128].

AusCERT, FIRST ve APCERT üyesidir ve bu sayede bölgesel ve küresel bilgisayar olaylarına ilişkin doğru, güncel bilgileri elde edebilmektedir. AusCERT üyelerine;

- Erken uyarı hizmetleri sağlamak,
- Günlük bülten yayımlamak ve bu bülteni üyelerine e-posta ile göndermek,
- Bilgisayar olaylarına müdahale hizmetleri sunmak,
- Tehlikeleri ve güvenlik açıklarını izlemek, değerlendirmek ve tavsiyelerde bulunmak,

- Eğitim amacıyla seminerler, konferanslar düzenlemek

gibi hizmetler sunmaktadır.

12 Mayıs 2009 tarihli bir haberde Avustralya hükümeti tarafından yeni bir ulusal CERT oluşturulacağı, bu yeni CERT'in AusCERT ile işbirliği içerisinde çalışacağı, fakat yeni kurulacak olan CERT'in AusCERT'den farklı olarak herkese açık olacağı ifade edilmiştir. Ayrıca siber güvenliğin sağlanması için AGD'ye 8.8 milyon dolar bütçe ayrıldığı da belirtilmiştir. Oluşturulması Temmuz 2010'u bulacağı söylenilen yeni CERT ile Avustralya İnternet kullanıcılarının siber tehditler, güvenlik açıkları ve kendi bilgilerinin güvenliğini nasıl sağlayabileceklerine ilişkin bilgileri elde edebilecekleri de ifade edilmiştir [129].

5.1.3.3 OnSecure

DSD ile AGIMO ortak girişimi olan İnternet sitesinin amacı kamu kurumlarına bilgi güvenliği ihlallerine ilişkin destek sağlamaktır. Kamu kurumları güvenlik ihlaliyle ilgili herhangi bir olayla karşılaştıkları takdirde, durumu OnSecure İnternet sitesinde yer alan Avustralya Bilgi Teknolojileri Güvenliği Olay Raporlama Formunu doldurmak suretiyle ihbar etmektedir. Bu raporlardan elde edilen bilgiler tehditlerin değerlendirilmesi ve güvenlik tavsiyeleri için esas oluşturmaktadır. DSD sorumluları tarafından tehdidin ciddi olduğuna karar verilirse, diğer kamu kurumları da durumdan haberdar edilmekte ve alınabilecek önlemler kendilerine belirtilmektedir. Ayrıca söz konusu sitede biri gizli, biri kamuya açık olmak üzere iki kısım vardır. Gizli olan kısım sadece kamu kurumlarının yetkili temsilcilerine açıkken, diğer kısımdan bilgi güvenliğine ilişkin bilgi edinmek isteyen herkes yararlanabilmektedir [130].

5.1.3.4 Stay Smart Online

DBCDE tarafından idare edilen ve diğer kamu kurumları tarafından da desteklenen İnternet sitesinde bireysel kullanıcılara ve küçük işletmecilere siber güvenlikle ilgili bilgiler verilmekte, e-ticaretin güvenilirliği, gençlerin ve ailelerin

bilinçlendirilmesine yönelik öneriler sunulmaktadır [131].

5.1.3.5 Cybersmart

ACMA tarafından oluşturulmuş olan ve Avustralya Hükümetinin siber güvenlik programı kapsamında yer alan İnternet sitesinde çocukların, gençlerin ve ailelerin bilinçlendirilmesine yönelik faaliyetler, kaynaklar ve tavsiyeler yer almakta, ayrıca okullar ve kütüphaneler için eğitim hizmetleri sunulmaktadır. Cybersmart ACMA aracılığı ile ihbar hattı vazifesi de görmekte, İnternet sitesi kapsamında çocuk pornografisi ve çocuk istismarı, şiddet, uyuşturucu kullanımına teşvik, teröre teşvik ve bahis gibi konularda ihbarlar kabul edilmektedir [132].

5.1.4 Avustralya'nın siber güvenliğin sağlanmasına yönelik mevzuatı

5.1.4.1 1988 tarihli Kişisel Gizlilik Kanunu

Kişisel Gizlilik Kanunu ile özel sektör kuruluşlarının kişisel verilerin işlenmesinde uyacakları kurallara ve kişisel bilgilerin korunmasına yönelik hükümlere yer verilmektedir. Kanunla bireylere bilgilerinin özel sektör kuruluşları tarafından bilinip bilinmediği, hangi bilgilere sahip oldukları, bilgilerin kimlere verildiği, hangi amaçlarla kullanıldığı ve bu bilgilerin doğru olup olmadığının takibine ilişkin haklar verilmekte ve düzenlemeler yer almaktadır. Özel sektör tarafından elde edilebilecek kişisel bilgiler; sağlık bilgilerine ilişkin kayıtlar da dahil olmak üzere işçi kayıtları, müşteri ve satıcıların listesi, müşterilerin mali bilgileri, müşteri şikayetleri gibi bilgilerdir [133].

Kanunda ayrıca Ulusal Gizlilik ilkelerine yer verilmiş ve bu ilkelere uyulmasının zorunlu olduğu ifade edilmiştir. Bu ilkeler; kişisel bilgilerin elde edilmesi, bu bilgilerin kullanılması ve yayılması, bilgilerin kaliteli olması, güvenliği, bilgilerin açıklığı ve erişilebilirliği, kişilerin kendilerine ilişkin bilgilere erişebilmeleri ve yanlışsa düzeltebilme hakkı, bireylerin tespiti amacıyla hükümet kayıtlarına ulaşılamaması, anonim kalabilme hakkı, kişisel bilgilerin Avustralya dışında başka

bir ülkeye aktarılmasına ilişkin kurallar ve hassas bilgilerin elde edilebilmesine ilişkin sınırlara dair kurallar ve hükümlerden oluşmaktadır.

5.1.4.2 1999 tarihli Elektronik İşlemler Kanunu

1999 tarihli Elektronik İşlemler Kanunu elektronik haberleşmenin kullanılması için yol gösterici ve esnek hükümlerden oluşan düzenleyici bir rejim öngörmektedir. Kanun bireylerle kamu kurumları arasındaki ilişkileri düzenlemekte, bireylerle özel sektör kuruluşları arasındaki ilişkileri kapsam dışında tutmaktadır. Bireylerin elektronik haberleşmeyi kullanmasını engelleyen mevcut yasal düzenlemeleri terk ederek, Avustralya'da elektronik ticareti kolaylaştırmaktadır. Kanunla, bireylerin kamu kurumlarıyla iletişim kurarken elektronik haberleşmeyi kullanmanın önü açılmaktadır [134].

5.1.4.3 2001 tarihli Siber Suçlar Kanunu

2001 tarihli Siber Suçlar Kanunu ile 1995 tarihli Ceza Kanunu değişikliğe uğramış, suçlar ve kovuşturma yetkileri Avrupa Konseyi Siber Suçlar Sözleşmesi ile tutarlı olacak şekilde düzenlenmiştir [135]. Kanunda:

- Zarara yol açmak amacıyla verilerin izin olmaksızın değiştirilmesi,
- Elektronik haberleşmenin yetkisiz olarak engellenmesi,
- Gizli bilgilere yetkisiz erişim veya bu verilerin değiştirilmesi,
- Saklanan verilerin bozulması,
- Suç işlemek amacıyla verilerin elde tutulması, üretilmesi veya tedarik edilmesi

gibi suçlara ilişkin düzenlemelere yer verilmiştir. Söz konusu hükümler, suçların tamamen veya kısmen Avustralya'da işlenmesi; sonucunun tamamen veya kısmen Avustralya'da gerçekleşmesi veya suçlunun Avustralya vatandaşı ya da şirketi olması durumunda uygulanabilmektedir.

5.1.4.4 2003 tarihli Spam Kanunu

Spam Kanunu spamin elektronik haberleşme ve ekonomi üzerindeki önemli etkileri nedeniyle 12 Aralık 2003'te onaylanmıştır [136].Kanunda spam, alıcının rızası olmaksızın e-posta, kısa mesaj servisi (SMS), multimedya mesaj servisi (MMS) veya anlık mesajlaşma yoluyla gönderilen ticari elektronik mesajlar olarak tanımlanmakta ve alıcının izni olmaksızın spam gönderilmesi yasaklanmaktadır. Ticari elektronik mesajlar toplu veya bireysel gönderilmiş olsun kanun kapsamında yer almaktadır.

Kanunla mesajın kimin tarafından gönderildiğinin ve gönderen kişinin geçerli bir adresinin bulunması zorunluluğu getirilmiş, ayrıca alıcıya söz konusu mesajı almak istemediği takdirde ücretsiz ve kolay bir şekilde reddetme imkânı sağlanması zorunlu kılınmış, elektronik adreslerin izinsiz toplanması, adres toplayan yazılımların kullanılması ya da izinsiz ele geçirilmiş adres listelerinin mesaj gönderiminde kullanılması yasaklanmıştır.

Spam Kanununun uygulanmasından ACMA sorumludur ve bu amaçla diğer kurum ve kuruluşlarla işbirliği içerisinde çalışmaktadır. ACMA spamle mücadele amacıyla eğitim faaliyetleri düzenlemekte, teknolojik çözümler getirmekte, diğer ülkelerle işbirliği faaliyetlerinde bulunmakta ve gelen ihbarları almaktadır. Ayrıca gelen ihbarları değerlendirmek üzere bir ihbar merkezi oluşturmuştur.

Avustralya'da mevcut spam mesajların %99 oranında ülke dışındaki kaynaklardan geldiği belirtilmiştir. Bu kapsamda Avustralya diğer ülkelerle işbirliği çalışmaları yapmaktadır. Söz konusu çalışmalara aşağıda yer verilmektedir [136]:

- Yeni Zelanda ile ikili mutabakat zaptı
- Tayvanla ikili mutabakat zaptı
- Seul-Melbourne çok taraflı mutabakat zaptı, Anti-spam Anlaşması
- Kore ile ikili mutabakat zaptı
- İngiltere ve ABD ile mutabakat zaptı

- Londra Eylem Planı
- Tayland müşterek beyanı

5.2. İngiltere

5.2.1 İngiltere'de kritik bilgi altyapının korunmasına yönelik çalışmalar

İngiltere'de kritik altyapı, "zarar görmesi ya da kullanılamaz hale gelmesi halinde hayat kaybına yol açabilecek, ulusal ekonomi üzerinde önemli etki doğuracak, toplumun önemli bir kısmını ve hükümetin işleyişini önemli ölçüde etkileyecek, İngiltere'nin ekonomik, politik ve sosyal yaşantısını etkileyen mal varlıkları, hizmetler ve sistemler bütünü" şeklinde tanımlanmıştır [137].

Aşağıda belirtilen on sektör İngiltere tarafından kritik sektör olarak kabul edilmektedir:

- Haberleşme
- Acil durum hizmetleri
- Enerji
- Finans
- Gıda
- Kamu hizmetleri
- Kamu güvenliği
- Sağlık
- Ulaştırma
- Su

5.2.1.1 Ulusal Bilgi Güvencesi Stratejisi (NIAS)

İngiltere, kritik bilgi altyapısını, bilgisayar ve haberleşme sistemlerini tehditlere ve saldırılara karşı korumak amacıyla NIAS'ı geliştirmiştir. NIAS, Bakanlar Kurulu

tarafından yönetilmektedir ve 2003 yılında Bakanlar Kurulu'nun bir birimi olan Bilgi Güvencesi Merkezi Üstlenici Kurumu (CSIA) tarafından yayımlanmıştır [138].

NIAS'ın amacı, bilgi ve iletişim sistemlerine bir saldırı olması durumunda bilgilerin korunacağına dair hükümete güvence sağlamaktır. NIAS'ta her geçen gün birbirine daha bağımlı hale gelen kritik bilgi altyapıları konusunda kamunun bilgi sistemlerinin gizliliğinin, erişilebilirliğinin ve bütünlüğünün sağlanması gerekliliğinin önemine değinilmiştir.

NIAS'ta bilgi güvencesi, "bilgi sistemlerinin mevcut bilgileri koruyacağına ve ihtiyaç duyulduğu takdirde yasal kullanıcılarının kontrolü altında olacağına ilişkin güven" olarak tanımlanmaktadır. CSIA, hükümete bilgi güvencesinin sağlanması konusunda yol göstermekte ve destek olmaktadır. CSIA'nın görevleri şunlardır [139]:

- Kamu hizmetlerinin sunulmasında BİT'in kullanılmasını sağlamak,
- Bilgi ve bilgi sistemlerinin korunması suretiyle İngiltere'nin ulusal güvenliğini güçlendirmek,
- Kamunun, özel sektörün ve bireylerin BİT'in olanaklarından faydalanmalarını sağlamak suretiyle İngiltere'nin ekonomik ve sosyal refahını sağlamak.

5.2.1.2 Ulusal Altyapı Koruma Merkezi (CPNI)

İngiltere'de kritik bilgi altyapısının korunması konusunda sorumluluk İçişleri Bakanlığına ait olmakla birlikte, uzman desteği sağlamak ve katkı sağlamakla görevli birçok kurum vardır. Bu katkı ve destekler 1 Şubat 2007'den bu yana, İngiltere'nin kritik bilgi altyapısını saldırılara karşı korumak için çalışmakta olan CPNI tarafından koordine edilmektedir [140].

İngiltere'de kritik bilgi altyapısının korunması politikası CPNI, Bilgi Güvencesi Merkezi Üstlenici Kurumu, İçişleri Bakanlığı, Devlet Haberleşme Genel Müdürlüğü,

Bakanlar Kurulu Güvenlik Politikaları Dairesi ve Sivil Riskler Sekreterliği gibi çeşitli kamu kurumları ve dairelerinden oluşan temsilcilerin katılımıyla geliştirilmiştir.

CPNI, kritik bilgi altyapısının sahibi olan ya da kritik bilgi altyapısını işleten ticari işletmelere ve kuruluşlara bilgi, personel ve fiziksel destekten oluşan güvenlik tavsiyelerinde bulunmaktadır. Ayrıca kritik altyapının terör saldırılarına ve diğer tehlikelere karşı korunması, güvenlik açıklarının azaltılması suretiyle güvenliğin sağlanması amacıyla kamu kurumlarıyla, üniversitelerle, özel sektörle ve istihbarat sağlayan kurumlarla işbirliği içerisinde hareket etmektedir.

CPNI güvenlik açıkları ve bazı tehlikelere ilişkin bilgileri Müşterek Güvenlik Olayları Müdahale Ekibi (CSIRTUK) ve GovCertUK vasıtasıyla kritik altyapı işletmecileri ve diğer kuruluşlarla paylaşmaktadır.

CPNI sorumluluklarını, kendi sektörlerine ilişkin güvenlik önlemlerini almakla yükümlü olan kamu kurumları vasıtasıyla paylaşmaktadır. Bu kurumlar aynı zamanda kendi sektörlerine ilişkin kritik altyapıların neler olduğunu CPNI ve sektör kuruluşlarıyla danışmak suretiyle belirlemekle yükümlüdür. CPNI polisle de işbirliği içerisindedir. Özellikle Terörle Mücadele Güvenlik Dairesi ve Terörle Mücadele Güvenlik Danışmanlarından oluşan uzman ekiplerle işbirliği içerisindedir.

5.2.1.3 Sivil Riskler Sekreterliği (CCS)

Bakanlar Kurulunun bir bölümü olan CCS, Temmuz 2001'de Başbakana güvenlik konusunda danışmanlık hizmeti sağlamak amacıyla kurulmuştur [141].CCS 'nin görevleri;

- Ulusal ve uluslararası kurum ve kuruluşlarla işbirliği suretiyle saldırılara karşı hazırlıklı olmak ve ülkenin dayanıklılığını sağlamak,
- Bir kriz durumunda kamu hizmetlerinin ve fonksiyonlarının devamlılığını sağlamak,

- Güvenliğe ilişkin politika geliştirilmesi hususunda Bakanlar Kuruluna tavsiyelerde bulunmak,
- Başbakana sunmak üzere raporlar hazırlamak

olarak belirtilmiştir.

5.2.2 İngiltere'nin kamu-özel sektör işbirliğinin sağlanmasına yönelik çalışmaları

İngiltere'de siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması konularında hükümet özel sektörle yakın işbirliği içerisindedir. Nitekim CPNI, özel sektör kuruluşlarıyla bilgi değişimi adı altında bilgilerini paylaşmakta ve bilgi paylaşımını aktif olarak desteklemektedir.

Ayrıca bilgilerin özel sektörle paylaşımı amacıyla CPNI bünyesinde faaliyet gösteren Uyarı, İhbar ve Raporlama Noktaları (WARPs) oluşturulmuştur. WARPs; güvenlik tehditleri, olayları ve çözümlerine ilişkin üyelerinin güncel bilgileri paylaşabileceği bir kamu hizmetidir ve kamu kurumlarına, yerel yönetimlere, ticari işletmelere, gönüllü kuruluşlara ve uluslararası kuruluşlara hizmet vermektedir [142].

Bunların yanı sıra, kamu-özel sektör bilgi paylaşımını sağlamaya yönelik olarak çalışan kurum/kuruluşlar bulunmaktadır. Bunlardan bazılarına aşağıda yer verilmektedir [10]:

- Bilgi Güvencesi Danışma Konseyi
- İngiliz Bilgisayar Topluluğu
- İnternet Güvenliği Forumu
- Ulusal Bilgi İşlem Merkezi
- İnternet İzleme Kurumu
- İngiltere Sanayi Konfederasyonu
- Bilgi Güvenliği Uzmanları Enstitüsü

- Avrupa Bilgi Toplumu Grubu
- Chatham Evi
- Kraliyet Birleşik Hizmetler Enstitüsü

5.2.3 İngiltere'nin bilgisayar olaylarına müdahale faaliyetleri ve siber güvenlik kültürü oluşturulmasına yönelik çalışmaları

5.2.3.1 CSIRTUK

CPNI, güvenliğe ilişkin tehditler karşısında ne şekilde tepki verileceğini ve bu durumların nasıl yönetileceğine ilişkin tavsiyelerde bulunmak amacıyla kritik altyapı sahipleri ve işletmecileri için CSIRTUK'u oluşturmuştur. Kritik altyapı sahipleri ve işletmecileri herhangi bir olayla karşılaşmaları durumunda CSIRTUK ile iletişim kurmakta, CSIRTUK tarafından elde edilen bilgiler gizlilik çerçevesinde ele alınmakta ve gerekirse kurumları veya şahısları belirtecek özel ayrıntılar gizlenmekte; böylece elde edilen bilgiler genel güvenlik tavsiyesine dönüştürülmektedir. Böylece tecrübeler diğerlerine yardım etmek üzere paylaşılmış olmaktadır. CSIRTUK güvenlik olaylarının raporlanmasında, tavsiye ve rehberlik hizmetlerinin sunulmasında merkez noktası olarak görev almaktadır [10].

5.2.3.2 GovCertUK

Bilgi Güvencesi Ulusal Teknik Kurumu tarafından 1 Şubat 2007'de oluşturulmuştur ve amacı bir saldırı olması durumunda ya da acil bir durum karşısında kamu kurumlarına teknik destek sağlamaktır [143].CSIRTUK hem kamu kurumlarına hem de özel sektöre danışmanlık hizmeti sunarken, GovCertUK sadece kamu kurumlarına hizmet etmek amacıyla oluşturulmuştur.

GovCertUK, kamu kurumlarının bilgi ve iletişim sistemlerine herhangi bir saldırı durumunda zararın en aza indirilmesi için çalışmakta, bu amaç doğrultusunda tehlikeler ve güvenlik açıkları konusunda kamu kurumlarını bilgilendirmekte ve herhangi bir bilgisayar olayı ile karşılaşılması durumunda derhal olaya müdahale

etmektedir.

5.2.3.3 Savunma Bakanlığı Bilgisayar Acil Durum Müdahale Ekibi (MODCERT)

İngiltere Savunma Bakanlığı Bilgisayar Acil Durum Müdahale Ekibi (MODCERT), Savunma Bakanlığı'nın bilgi güvenliğinin sağlanmasından sorumludur ve GovCertUK ve CSIRTUK ile işbirliği içerisinde faaliyet göstermektedir [10].

5.2.3.4 GetSafeOnline

GetSafeOnline, kamu-özel sektör işbirliği sonucu oluşturulmuş bir İnternet sitesidir. Bireylerin bilgisayar güvenliğini sağlamaları, kişisel bilgilerini korumaları ve bilgi teknolojileri alanlarında eğitilmelerinin sağlanması amaçlanmaktadır. GetSafeOnline, Ekim 2005'den bu yana erişime açıktır ve site içerisinde bireysel kullanıcıların ve küçük işletmecilerin bilgisayarlarını, cep telefonlarını ve diğer elektronik araçlarını siber saldırılara karşı nasıl koruyacaklarına ilişkin tavsiyeler yer almaktadır. Ücretsiz olan bu hizmetin amacı, kimlik hırsızlığı, virüsler ve spam gibi olaylara karşı kullanıcıları eğitmek ve kendilerini ve bilgisayarlarını sanal tehlikelerden korumalarını sağlamak suretiyle bu olayları en aza indirgemektir [144].

5.2.4. İngiltere'nin siber güvenliğin sağlanmasına yönelik mevzuatı

5.2.4.1 Bilgisayarların Kötüye Kullanılması Kanunu (CMA)

29 Temmuz 1990 tarihinde yürürlüğe giren CMA ile yetkisiz olarak bilgisayarlara erişilmesinin, bilgilerde değişiklik yapılmasının ya da benzeri müdahalelerde bulunulmasının önlenmesi amaçlanmıştır. CMA ile yetkisiz olarak bilişim cihazlarına, veri ve programlarına erişilmesi, başka bir suçun işlenmesini sağlamak veya kolaylaştırmak amacıyla yetkisiz olarak bilgisayarlara müdahale edilmesi ve yetkisiz olarak bir bilgisayardaki bilgilerin içeriğinde değişikliğe neden olunması konularında düzenlemeler ve yaptırımlar getirilmiştir [145].

5.2.4.2 1997 tarihli Telekomünikasyon (Sahtecilik) Kanunu

1997 tarihli Telekomünikasyon (Sahtecilik) Kanunu ile 1984 tarihli Telekomünikasyon Kanunu değişikliğe uğramıştır. Kanunun amacı, bir telekomünikasyon sistemi kullanılmak suretiyle sahtecilik yapılmasının önüne geçmektir. Kanunla bir kişinin, himayesi altında bulunan bir telekomünikasyon sistemini sahtecilik amacıyla kullanması, başkasının kullanımını sağlaması gibi durumlarda cezalandırılacağına ilişkin hükümler yer almaktadır [146].

5.2.4.3 1998 tarihli Verilerin Korunması Kanunu (DPA)

DPA bireylere ait bilgilerin elde edilmesi, paylaşılması veya kullanılması da dâhil olmak üzere kişisel bilgilerin işlenmesini düzenlemektedir. Söz konusu Kanun ile AB'nin 1995 tarihli verilerin korunması direktifine uyum sağlanması amaçlanmıştır. Kanun kapsamında bireylere, küçük bir ücret karşılığı bir kurum tarafından kendisi hakkında tutulan bilgileri görebilme, yanlış olan bilgilerin düzeltilmesini isteme, bilgilerin zarar verici veya kanuna aykırı amaçlarla kullanılmasını engelleme gibi haklar verilmektedir.

Kanunda kişisel verilerin korunmasına ilişkin ilkeler yer almaktadır. Bu ilkelere aşağıda yer verilmektedir [147]:

- Kişisel verilerin adil ve kanunlara uygun olarak işlenebilmesi,
- Kişisel verilerin sadece bir veya daha fazla kanuna uygun ve belirli amaçla elde edilebilmesi ve bu amaç veya amaçların dışında işlenememesi,
- Elde edilen kişisel verilerin işlenme amaçlarıyla yeterli, ilgili, orantılı olması, gereğinden fazla bilgi elde edilememesi,
- Kişisel verilerin doğru ve güncel olması,
- Kişisel verilerin işlenme amacına yetecek süre boyunca muhafaza edilmesi, gerek kalmadığında yok edilmesi,
- Kişisel verilerin yetkisiz veya kanuna aykırı amaçlarla işlenmesine ya da

verilerin yanlışlıkla yok edilmesi ya da tahrip edilmesine dair gerekli teknik veya kurumsal önlemlerin alınması,

- Kişisel verilerin transfer edileceği ülkede o verilerin işlenmesine uygun yeterli düzenleme olmadığı sürece, Avrupa Ekonomik Alanı dışında bir ülkeye ya da bölgeye transfer edilememesi.

5.3 Amerika Birleşik Devletleri (ABD)

5.3.1 ABD'de kritik altyapının korunmasına yönelik çalışmalar

ABD'de 2001 tarihli ABD Vatanseverlik Kanununda (USA Patriot Act) kritik altyapı "fiziksel ya da sanal olsun, yetersizlik veya tahribatı halinde güvenlik, ulusal ekonomi güvenliği, ulusal kamu sağlığı veya güvenliği ya da bunların hepsinin birden üzerinde zayıflatıcı etkiye yol açacak olan sistemler ve varlıklar" şeklinde tanımlanmıştır [148].

ABD'de aşağıda belirtilen 18 sektör kritik sektör olarak belirlenmiştir:

- Bilgi teknolojileri
- Telekomünikasyon
- Kimyasal maddeler
- Ticari olanaklar
- Barajlar
- Ticari nükleer reaktörler, maddeler ve atıklar
- Devlet imkanları
- Ulaşım sistemleri
- Acil hizmetler
- Postacılık ve taşıma hizmetleri
- Gıda ve tarım
- Kamu sağlığı ve sağlık hizmetleri
- İçme suyu ve atık su arıtma sistemleri

- Enerji
- Bankacılık ve finans
- Milli anıtlar ve simgeler
- Savunma sanayi
- Kritik Üretim

5.3.1.1 İç Güvenlik Bakanlığı (DHS)

11 Eylül 2001 saldırıları sonrasında ABD'de siber güvenliğin sağlanması ve kritik bilgi altyapılarının korunması alanlarında politika değişiklikleri olmuş ve Mart 2003'te bazı kurumların yetkileri devredilmek suretiyle DHS oluşturulmuştur [149].

Siber güvenliğin sağlanmasına yönelik olarak DHS bünyesinde Altyapının Korunması Dairesi (OIP) ve Siber Güvenlik ve İletişim Dairesi (CS&C) kurulmuştur. OIP, kritik altyapıların korunmasına ilişkin farklı sektörlerin çalışmalarını koordine etmek, kritik altyapı sektörlerinin güvenlik açıklarının değerlendirilmesine ilişkin çalışmaları desteklemek ve kritik altyapıların korunması için küresel bir güvenlik kültürü oluşturulmasını teşvik edici uluslararası programları ve ilişkileri oluşturmak ve sürdürmekle görevlidir. CS&C ise siber tehditlerin belirlenmesi, risk yönetimi ve farkındalık geliştirme konularında özel sektörle koordinasyonun sağlanması, acil durum haberleşmesinin sağlanması ve olaylara müdahale merkezlerinin oluşturulmasından sorumludur.

5.3.1.2 Siber güvenliğin sağlanmasına ilişkin ulusal stratejiler

5.3.1.2.1 İç güvenlik ulusal stratejisi

Temmuz 2002'de DHS tarafından ABD'nin siber terör saldırılarından korunması amacıyla İç Güvenlik Ulusal Stratejisi yayımlanmıştır. Stratejide altı kritik görev alanı belirlenmiş, bunlardan bir tanesi de kritik altyapıların ve ana varlıkların

korunması olarak ifade edilmiştir. Stratejinin amacı; terör saldırılarının önlenmesi, kritik altyapıların korunması, bilgisayar güvenlik olaylarına müdahale edilmesi ve siber saldırıların önlenmesi olarak ifade edilmiştir. Ekim 2007'de stratejinin güncellenmiş versiyonu yayımlanmıştır [150].

5.3.1.2.2 Sanal güvenlik ulusal stratejisi

Şubat 2003'te yayımlanan Sanal Güvenlik Ulusal Stratejisinde, sanal güvenliğin sağlanmasının devletin ve toplumun her kesiminden katılımın ve bu kesimler arasında koordinasyonun sağlanması gereken özel bir çaba gerektirdiği belirtilmektedir [151]. Stratejide sanal ortam, "birbirlerine bağlı olan bilgi ve teknolojileri şebekeleri altyapısı" olarak tanımlanmakta ve toplumun kontrol sistemi olarak gösterilmektedir.

Stratejinin amacı; ulusal kritik bilgi altyapısına yönelik siber saldırıların önlenmesi, siber saldırılara karşı ulusal güvenlik açıklarının azaltılması ve saldırılardan meydana gelecek hasarların ve kurtarma sürelerinin en aza indirilmesi olarak ifade edilmiştir. Ayrıca stratejide, kritik bilgi altyapısının sahibinin ve işletmecisinin çoğunlukla özel sektör olduğu, özel sektörün siber saldırılara karşı donanımlı olduğu ve bu nedenle kamu-özel sektör işbirliğinin geliştirilmesinin önemi vurgulanmıştır. İşbirliğinin ise farkındalık oluşturma çabaları, eğitim faaliyetleri gibi çeşitli şekillerde olması gerektiği ifade edilmiştir.

5.3.1.2.3 Kritik Altyapı ve Ana Varlıkların Fiziksel Korunmasına İlişkin Ulusal Strateji

Şubat 2003'te yayımlanan Kritik Altyapı ve Ana Varlıkların Fiziksel Korunmasına İlişkin Ulusal Stratejide ulusal kritik altyapıların, güvenlik açıklarının azaltılması suretiyle ülkenin terör faaliyetlerine karşı korunmasının sağlanması hedeflenmiştir [152].

Bir ülkenin kritik altyapılarına saldırıların sadece büyük çaplı can ve mal kayıplarıyla

sınırlı kalmadığı, aynı zamanda 11 Eylül 2001 saldırılarında da yaşandığı üzere ulusun prestijini, moralini ve güvenini de sarsmakta olduğu belirtilmiştir. Bu hedeflere ulaşılabilmesi için de federal, merkezi ve yerel yönetimlerin yanı sıra, özel sektör ve ilgili vatandaşların da eşgüdümlü olarak hareket etmesinin gerektiği, bu doğrultuda DHS'nin işbirliğinin sağlanmasını kolaylaştırıcı ve irtibat sağlayıcı rol üstlenmesinin önemi vurgulanmıştır.

5.3.1.2.4 Ulusal Altyapı Koruma Planı (NIPP) ve Sektöre Özgü Planlar (SSP)

2009 yılında DHS tarafından yayımlanmış olan NIPP, kritik altyapıların korunması amacıyla mevcut ve ileriye yönelik programlar ve faaliyetlere yönelik genel bir çerçeve sağlamaktadır. NIPP, terör tehlikesinin engellenmesi, güvenlik açıklarının azaltılması ve olası sonuçların hafifletilmesinden oluşan üç farklı koruma politikası ileri sürmektedir [153].

NIPP ile kritik bilgi altyapısının korunmasında kamu-özel sektör işbirliğinin sağlanması amacıyla her sektör, bilgi paylaşımı için politika koordinasyonu sağlamakla görevli bir konsey oluşturmakla ve Bilgi Paylaşımı ve Analiz Merkezleri (ISACs) gibi operasyonel kuruluşlar oluşturmakla yükümlü kılınmaktadır.

5.3.2 ABD'nin kamu-özel sektör işbirliğinin sağlanmasına yönelik çalışmaları

5.3.2.1 Bilgi Paylaşımı ve Analiz Merkezleri (ISACs)

ABD'de kritik altyapı sektörlerinin büyük çoğunluğu kendi ISACs'larını oluşturmuş durumdadır. Her bir ISACs, kurumsal ve iş süreçlerine karar veren bir yönetim kuruluna sahiptir ve özel sektör tarafından idare edilen üye kuruluşlardır. ISACs'ların görevi güvenlikle ilgili olaylara ve müdahalelere ilişkin bilgileri toplamak, analiz etmek, paylaşmak ve bu suretle özel sektör ile hükümet arasında bilgi alışverişini sağlamaktır. Kritik bilgi altyapısının korunması alanında en önemli ISACs'lardan bazıları şunlardır [154]:

- Bilgi Teknolojileri- ISACs: Faaliyetlerine Mart 2001'de başlamıştır. Üyeleri arasında Microsoft, Intel, Symantec, IBM, Oracle, Ebay, Hewlett Packard ve VeriSign da dahil olmak üzere dünyaca ünlü yirmi yazılım, donanım ve e-ticaret şirketi yer almaktadır [155].
- Telekomünikasyon Sektörü-ISACs: Ulusal Koordinasyon Merkezi (NCC) vasıtasıyla ISACs oluşturmuştur. NCC'ye üye olan her bir üye kendi ağını izlemekte ve analiz etmektedir. Olaylar NCC içerisinde tartışılmakta ve gerekli görülürse yetkili makamlara ihbar edilmektedir [156].
- Finansal hizmetler-ISACs: Ülkenin en büyük bankaları, menkul değer şirketleri, sigorta ve yatırım şirketleri Finansal Hizmetler-ISACs oluşturmak amacıyla bir araya gelmiştir. Amaçları kritik bilgi sistemlerini ve varlıklarını fiziksel ve siber güvenliğe ilişkin tehlikelerden korumak ve bu amaçla anlık bildirimlere ulaşmaktır [157].

5.3.2.2 InfraGard

Özel sektör ve FBI arasında bilgi alışverişini ve istihbaratı sağlamak üzere 1996 yılında oluşturulmuştur [158]. Amacı, üyeleri ile FBI arasında siber suçlarla mücadele, siber terörizmin önlenmesi gibi alanlarda iletişimi ve sürekli diyaloğu sağlamaktadır.

5.3.2.3 Ulusal Siber Güvenlik İttifakı (NCSA)

NCSA 2001 yılında oluşturulmuştur ve kamu-özel sektör işbirliğinin sağlanması suretiyle siber güvenliğe ilişkin farkındalığın artırılmasını hedeflemektedir. DHS ile Symantec, CISCO, Microsoft, McAfee gibi dünyaca ünlü şirketler NCSA üyesidir. NCSA bireysel kullanıcıları, küçük işletmecileri ve öğrencileri siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması konularında bilinçlendirmek amacıyla çeşitli etkinlikler düzenlemektedir. Bu amaçla "staysafeonline" isminde bir İnternet sitesi oluşturmuşlardır ve her yıl Ekim ayını "siber güvenlik farkındalık ayı" olarak kutlamaktadırlar [159].

5.3.2.4 Çapraz Sektör Siber Güvenlik Çalışma Grubu (CSCSWG)

CSCSWG, kritik altyapı sektörlerine yönelik risklerin belirlenmesi amacıyla özel sektör ve kamu temsilcilerini bir araya getirmek üzere oluşturulmuş bir gruptur. Özel sektör ve kamu temsilcileri eş başkanlığında yürütülmektedir. Siber güvenliğe ilişkin konularda sektörler arası koordinasyonun geliştirilmesine yönelik alternatiflerin belirlenmesi ve çeşitli grupların çalışmaları sonucu elde edilen bilgilerin paylaşılması ile görevlidir [10].

5.3.2.5 Bilgi Altyapısının Korunması Kuruluşu (I3P)

I3P, Dartmouth Koleji tarafından yönetilen ve akademik araştırma merkezleri, devlet laboratuarları ve kar amacı gütmeyen kuruluşlar da dâhil olmak üzere önde gelen ulusal siber güvenlik kuruluşlarından oluşan bir ortaklıktır. Eylül 2001'de kurulmuş olan I3P'nin esas görevi, ulusal siber güvenlik araştırma ve geliştirme programlarını koordine etmek ve üniversiteler, özel sektör ve kamu kurumları arasında köprü görevi görmektir [10].

5.3.3 ABD'nin bilgisayar olaylarına müdahale faaliyetleri ve siber güvenlik kültürü oluşturulmasına yönelik çalışmaları

5.3.3.1 CERT Koordinasyon Merkezi (CERT/CC)

1988 yılında "Morris" solucanının İnternet sistemlerinin %10'unu işlemez hale getirmesi sonucu, bu tip büyük ölçekli olayların tekrar yaşanmasını engellemek amacıyla Carnegie Mellon Üniversitesinde koordinasyon görevi üstlenecek bir BOME oluşturulmuştur [21]. CERT/CC, ilk bilgisayar güvenlik olayları müdahale ekibidir ve masraflarının bir kısmı hükümet tarafından karşılanmaktadır.

CERT/CC güvenliğe ilişkin olaylarda koordinasyon merkezi olarak görev almakta ve başka olayların oluşumunu engellemek için çalışmaktadır. CERT/CC uzmanları ilk olarak şebeke güvenlik açıklarını araştırıp değerlendirmek suretiyle risk

değerlendirmesi yapmakta, daha sonra düzenli güvenlik uyarıları ve sunumlarla bu bilgileri kamuyla paylaşmaktadır. Ayrıca CERT/CC üyeleri İnternet güvenliğinin geliştirilmesi ve şebeke devamlılığının sağlanabilmesi amacıyla çeşitli güvenlik gruplarına katılmaktadırlar.

5.3.3.2 US-CERT

15 Eylül 2003'de İç Güvenlik Bakanlığı tarafından US-CERT'in kurulduğu duyurulmuştur [160].US-CERT siber saldırıları önlemek, siber saldırıların etkilerini hafifletmek ve güvenlik açıklarını azaltmak amacıyla Ulusal Siber Güvenlik Bölümü (NCSD) ile birlikte çalışmaktadır ve DHS ile özel sektör arasında işbirliği sonucu oluşturulmuştur. US-CERT, NCSD ile birlikte bireysel kullanıcılara ve teknoloji uzmanlarına destek sağlamak amacıyla güvenli uyarı sistemi olan Ulusal Siber Uyarı Sistemini kurmuştur [161].Bu sistem ile virüs saldırıları veya diğer siber saldırılar oluşması durumunda bilgisayar kullanıcılarına e-posta gönderilmekte ve kendilerini saldırılardan koruyabilmeleri amacıyla ayrıntılı bilgiler verilmektedir.

5.3.3.3 OnGuardOnline.gov

OnGuardOnline.gov, bilgisayar kullanıcılarının İnternet dolandırıcılığı ve diğer tehlikelere karşı kişisel bilgilerinin ve İnternet ağlarının güvenliğini sağlamaları amacıyla özel sektörden ve hükümetten tavsiyelere yer vermektedir. Kapsamlı bir içeriğe sahip olan İnternet sitesinde makaleler, videolar ve siber güvenliğin sağlanmasına ilişkin önemli ipuçları yer almaktadır [162].

5.3.3.4 Staysafeonline.org

Staysafeonline.org, NCSA tarafından oluşturulmuştur ve amacı eğitim faaliyetleri düzenlemek suretiyle bireylerin, öğrencilerin ve küçük işletme sahiplerinin siber güvenliğin sağlanmasına ilişkin farkındalıklarının artırılması, kendilerini siber tehditlere karşı koruyabilmelerinin sağlanmasıdır [163].

5.3.4. ABD'nin siber güvenliğin sağlanmasına yönelik mevzuatı

5.3.4.1 1986 tarihli Bilgisayar Dolandırıcılığı ve Bilgisayarların Kötüye Kullanılması Kanunu (CFAA)

ABD'de devlet yönetiminde ve ticaret alanında bilgisayar kullanım oranlarının artmasıyla birlikte, 1980'li yılların başlarında bilgisayar suçlarına karşı yasal düzenlemeler yapma ihtiyacı ortaya çıkmıştır. CFAA yasama organları tarafından yıllardır yapılan araştırmalar ve tartışmalar sonucu hazırlanmıştır. Kanunla "Federal bilgisayarlara yetkisiz erişim" ve "bilgisayar şifrelerinin yetkisiz ele geçirilmesi" iki önemli suç olarak kabul edilmiştir. Bahse konu bilgisayarlar arasında devlet bilgisayarları, hastaneler, finans kuruluşları gibi kurumlara ait bilgisayarlar yer almaktadır. CFFA kapsamında suç sayılan fiillere aşağıda yer verilmiştir [1]:

- Kamu kurumlarına ait bilgisayarlara yetkisiz olarak erişmek suretiyle, bu kurumlar tarafından verilen hizmetleri aksatacak şekilde bilgileri değiştirmek, bozmak veya ifşa etmek,
- Herhangi bir bilgisayara dolandırıcılık veya hırsızlık yapmak gibi kanuna aykırı amaçlarla izinsiz ve yetkisiz olarak girmek,
- Kasten veya ihmal sonucu, korunan bir bilgisayara erişmek, bu bilgisayara veri veya program göndermek,
- Bilgisayar şifrelerini veya bilgisayarlara erişmekte kullanılabilecek herhangi bir bilgiyi dağıtmak, başkalarının kullanımına sunmak,
- Para veya para hükmünde olan herhangi bir değeri elde etmek maksadıyla bir bilgisayar veya bilgisayar sistemine zarar vermek yönünde tehditler savurmak.

Ayrıca, belirtilen fiillerden herhangi birinin suç olarak nitelendirilebilmesi için siber saldırganların bilgisayarlara yetkisiz veya mevcut yetkisini aşarak erişmiş olduğunun kanıtlanabilmesi gerekmektedir.

5.3.4.2 1994 tarihli Bilgisayarların Kötüye Kullanılması Değişiklikler Kanunu

1994 tarihli Bilgisayarların Kötüye Kullanılması Değişiklikler Kanunu ile virüsler ve diğer kötücül yazılımların da kanun kapsamına dâhil edilmesi suretiyle CFAA'nın kapsamı genişletilmiştir. Bu kanunla belirlenen şartlar daha sonra 26 Ekim 2001 tarihli ABD Vatanseverlik Anti Terör Kanunu ile teröre karşı düzenlemeler getirilmek suretiyle ağırlaştırılmıştır [164]. CFAA'nın ihlali durumunda FBI bünyesinde görev alan Ulusal Bilgisayar Suçları Ekibi tarafından soruşturma yapılmaktadır.

5.3.4.3 2002 tarihli İç Güvenlik Kanunu

Kritik bilgi altyapısının korunmasına ilişkin federal yasaların çoğunluğu siber tehlikelerin ortaya çıkışından önce düzenlenmiştir. Bu nedenle, mevcut yasal çerçeve kapsamında herhangi bir siber tehlike oluşması durumunda etkili ve zamanında bir tepki verilip verilemeyeceği merak edilmiştir. Bu kanun, İç Güvenlik Bakanlığının kurulması için düzenlenmiş olmakla birlikte, 2 nci kısmında bilgi analizi ve altyapının korunmasına ilişkin hükümler yer almaktadır [165]. Kanunla, çeşitli kurumların yetki ve görevlerinin İç Güvenlik Bakanlığına devredilmesinin yanı sıra, bilgi kategorileri de oluşturulmaktadır. Ayrıca Ülkenin korunabilmesi için istihbarat bilgilerine, altyapı güvenlik açıklarına ve diğer verilere Bakanlığa erişme yetkisi verilmektedir.

5.3.4.4 1974 tarihli Kişisel Gizlilik Kanunu

Kişisel Gizlilik Kanunu, kişisel bilgileri federal hükümetler tarafından tutulan bireyler hakkında uygulanmaktadır. Bu nedenle mahkemeler, kamu kurumları veya özel kurumlar tarafından tutulan bilgiler bu kanun kapsamında yer almamaktadır. Kişisel bilgilerin federal hükümetler tarafından elde edilmesi, kullanılması, işlenmesi ve yayılmasında uyulacak kurallara ilişkin düzenlemeler yer almaktadır. Kanunla federal hükümetler tarafından tutulan kişisel bilgilerin kişilerin yazılı izni olmaksızın dağıtılması veya yayılması yasaklanmaktadır. Kanunla ayrıca bireylere, söz konusu

kayıtlara ulaşabilmek ve yanlışlık olması durumunda bu kayıtları düzeltebilmek hakkı da tanınmaktadır [166].

5.3.4.5 2002 tarihli Federal Bilgi Güvenliği Yönetimi Kanunu (FISMA)

FISMA ile siber güvenliğin ülke ekonomisi için önemi vurgulanmış ve federal hükümetlerin bilgi güvenliğini sağlamaları amacıyla programlar oluşturmaları gerektiği hüküm altına alınmıştır. FISMA'da bilgi güvenliği, bilgilerin ve bilgi ve iletişim sistemlerinin bütünlüğünün, gizliliğinin ve erişilebilirliğinin sağlanması amacıyla yetkisiz erişimden, kullanımdan, engellenmeden ya da tahrip edilmeden korunması olarak tanımlanmıştır. FISMA kapsamında NIST (Ulusal Standartlar ve Teknoloji Kurumu) bilgi güvenliğine ilişkin standartlar, ilkeler ve metotlar geliştirmekle yükümlü kılınmıştır [167].

5.3.4.6 2004 tarihli Can-Spam Act

Can-Spam Act ile spame ilişkin düzenlemelere yer verilmiş ve spam "ticari bir ürün veya hizmetin reklâmı ya da promosyonu olan e-posta" şeklinde tanımlanmıştır. Kanuna göre, alıcının adresine gelen e-postanın ticari nitelikte bir içerik taşıdığının e-postanın konu kısmından açıkça anlaşılabilecek şekilde düzenlenmiş olması gerekmektedir. Ancak, önceden izin alınmış kişilere gönderilecek ticari e-postalar istisna bir durum olarak ele alınmış ve bu kapsamdaki e-postaların ticari nitelik taşıdığının belirtilmesi zorunlu kılınmamıştır.

Kanununun genelinde kapsam dışı (opt-out) yöntem benimsenmiştir. Buna göre, e-posta göndericileri alıcılarından izin almaksızın ticari e-posta gönderme hakkına sahiptir. Kanun kapsamında;

- E-posta göndericisinin mesaj içeriğinde kendisini tanımlayıcı bir bilgi bulundurması,
- Alıcının mesajı bir daha almak istememesi durumunda mesajın tekrar gönderilmemesine imkan tanıyan bir yöntemin alıcıya sunulması,

- Alıcının e-postayı gelecekte almayı reddetme hakkını kullanması durumunda göndericinin söz konusu talebi on iş günü içerisinde yerine getirmesi

zorunlu kılınmıştır.

Ayrıca;

- Göndericinin kendisini tanımlama konusunda aldatıcı ya da yanlış bilgiler vermesi,
- Gönderen e-posta adresinin sahte, geçersiz ya da yanlış bilgi içermesi,
- Reddedilen göndericinin başka bir gönderici aracılığıyla e-posta göndermeye devam etmesi,
- E-posta alıcısının adresinin başka göndericilerle paylaşılması ya da bu adreslerin satılması,
- E-posta adreslerinin izinsiz bir şekilde toplanması,
- İzin verilmemiş bir e-posta sistemini kullanmak suretiyle ticari amaçlı e-postalar gönderilmesi

yasaklanmıştır [168].

5.4 Kanada

5.4.1 Kanada'da kritik altyapının korunmasına yönelik çalışmalar

Kanada'da kritik altyapılar halkın sağlığı, emniyeti, güvenliği, ekonomik refahı gibi değerlerinden, fiziksel ve bilgi teknolojileri tesislerinden, şebekelerden ve hükümetin işleyişinden oluşmaktadır. Kanada hükümeti tarafından kritik altyapı sektörleri [169]:

- Enerji ve kamu hizmetleri
- Haberleşme ve bilgi teknolojileri
- Finans
- Sağlık hizmetleri
- Gıda

- Su
- Ulaştırma
- Güvenlik
- Yönetim
- Üretim

olarak belirtilmiştir

5.4.1.1 Kanada Kamu Güvenliği

Kanada Hükümeti tarafından, kritik altyapıların birbirlerine bağımlı hale gelmeye başlaması ve yeni tehlikelerin ortaya çıkması üzerine 2001 yılında kritik altyapıların ve kritik bilgi altyapılarının korunmasına yönelik politikalar uygulanmaya başlanmıştır. Kanada Kamu Güvenliği, Kamu Güvenliği Bakanına ulusal güvenlik, acil durum yönetimi, bilgi paylaşımı gibi konularda politika önerileri ve desteği sağlamaktadır. Ayrıca Kanada'nın kritik bilgi altyapılarına yönelik tehditler oluşması durumunda koordinasyonun sağlanmasından ve bilgi paylaşımından sorumludur. Herhangi bir ihbar alması durumunda Kanada Kamu Güvenliği bünyesinde yer alan Hükümet Operasyon Merkezi tehlikeyi değerlendirmekte ve bir bülten yayınlayarak kritik altyapı sahiplerini ve işletmecilerini durumdan haberdar etmekte, ayrıca Kanada'nın acil durum yönetim irtibat noktalarını da bilgilendirmektedir [170].

Kanada Kamu Güvenliği, kamu ve özel sektör kritik altyapı paydaşları arasında ulusal işbirliği geliştirilmesi amacıyla liderlik görevi üstlenmiş ve bu amaçla Kritik Altyapı Ulusal Stratejisi ve Eylem Planının geliştirilmesini sağlamıştır.

5.4.1.2 Kritik Altyapı Ulusal Stratejisi ve Eylem Planı

Kritik Altyapı Ulusal Stratejisi ve Eylem Planı ile kamu-özel sektör işbirliği modeli geliştirilmesi, bilgi paylaşımı çerçevesinin oluşturulması ve kritik altyapıların korunmasına yönelik ilkeler benimsenmiştir [171].

Planda hedeflenen amaçlara ulaşmak için kritik altyapı sahiplerinin;

- Riskleri ve tehlikeleri öngörebilmek amacıyla planlar ve programlar geliştirmeleri,
- Tehlike analizleri ve istihbarat bilgilerini içeren bilgi paylaşım ağlarına erişim sağlamaları,
- Daha etkin ve zamanında tepki ve kurtarmanın sağlanması amacıyla sektörler arası bağımlılıkları tanımlamalarının

gerektiği belirtilmektedir.

Planda hükümet özel sektörün risklere ve tehlikelere karşı zamanında ve doğru bilgiler sağlamasını ve mümkün olan en kısa zamanda risk yönetimi faaliyetleri ve acil durum yönetim planları hazırlamalarını sağlamakla yükümlü kılınmıştır. Hükümet her bir kritik sektör için sektör ağlarını oluşturacak ve böylece bilgi paylaşımı ve kritik altyapı öncelikleri belirlenmiş olacaktır. Ayrıca her bir sektör temsilcisinden oluşan Çapraz-Sektör Forumu oluşturulacaktır. Forumda çapraz-sektör bağımlılıkları belirlenecek ve Kamu Güvenliği Bakanlığına tavsiye ve önerilerde bulunulacaktır.

5.4.2 Kanada'nın kamu-özel sektör işbirliği sağlanmasına yönelik çalışmaları

Kanada'nın kritik altyapısının %80'i özel sektöre ait olduğundan veya özel sektör tarafından işletildiğinden dolayı siber güvenliğin sağlanmasında kamu-özel sektör işbirliğinin önemi büyüktür. Kanada hükümeti tarafından özel sektör kuruluşları ve kamu kurumları arasında bilgi paylaşımının artırılması için yoğun çaba harcanmaktadır [10].

5.4.2.1 Kanada Siber Olaylara Müdahale Merkezi (CCIRC)

CCIRC, siber güvenliğin sağlanması ve güvenliğe ilişkin olaylara müdahale alanlarında ulusal ve uluslararası konularda liderlik görevi üstlenmektedir. 7 gün 24 saat herhangi bir tehlike olup olmadığını izlemekte ve bir olay olması durumunda

müdahale etmektedir. Kritik altyapı sektörlerine olaylara müdahale, koordinasyon ve destek; izleme ve siber tehditleri analiz etme; bilgi teknolojileri alanlarında teknik danışmanlık sağlama ve farkındalığın artırılması ile ilgili eğitim faaliyetleri sunmaktadır [172].

5.4.2.2 Devlet Operasyon Merkezi (GOC)

GOC, Kanada Kamu Güvenliği bünyesinde yer almakta ve 7 gün 24 saat görev yapmaktadır [173]. Ulusal güvenliği ilgilendiren konularda Kanada Hükümeti adına stratejik düzeyde koordinasyonu sağlamakta ve kritik altyapılara ve güvenliğe yönelik tehlikelere ilişkin bilgi elde etmekte ve yayınlamaktadır.

GOC tarafından elde edilen bilgiler en hızlı şekilde değerlendirilmekte ve ilgili müdahale merkezlerine iletilmektedir. Bilgilerin iletilmesi, Kanada Kamu Güvenliği'nin diğer bakanlıklar, kamu kurumları ve özel sektörle arasındaki özel iletişim ağları vasıtasıyla yapılmaktadır.

5.4.3 Kanada'nın siber güvenliğin sağlanmasına ilişkin mevzuatı

5.4.3.1 Kanada Ceza Kanununun ilgili hükümleri

1892 tarihli Kanada Ceza Kanununun 342 nci maddesi uyarınca bireylerin hileyle ve yasal bir hakkı olmaksızın bilgisayar sistemini doğrudan ya da dolaylı yoldan ele geçirmesi, bilgisayar sisteminin işleyişini doğrudan veya dolaylı olarak engellemesi, bilgisayar sistemini doğrudan veya dolaylı olarak suç işlemek amacıyla kullanması, trafik verilerini kullanması veya suç işlemek amacıyla başka birine kullandırması durumunda cezalandıracağı hüküm altına alınmıştır [174].

5.4.3.2 Acil Durum Yönetimi Kanunu

Acil Durum Yönetimi Kanunu Ağustos 2007'de yürürlüğe girmiştir [175]. Kanunla, acil durumlar karşısında Kanada hükümetinin hazırlıklı olmasını sağlamak ve

olayların etkilerini en aza indirebilmek amaçlanmıştır. Ayrıca Kanunda acil durum yönetimi için özel sektör, kamu kurumları ve STK'lar tarafından müşterek çaba gösterilmesi gerektirdiği ifade edilmektedir.

Kanunda acil durum yönetiminde Bakana önemli görevler düşmekte olduğu ve bu görevler arasında, acil durumlarda müdahale faaliyetlerini koordine etmek, acil durum planları için standartlar oluşturmak, kamu kurumlarının acil durum planlarını izlemek, değerlendirmek ve test etmek, bilgi paylaşımı ve ortak standartlar geliştirmek amacıyla diğer kuruluşlarla işbirliğini geliştirmek olduğu belirtilmektedir.

5.4.3.3 Kişisel Gizlilik Kanunu

1 Temmuz 1983'de yürürlüğe girmiş olan Kanunda, hükümet tarafından kişisel bilgilerin ne şekilde kullanılacağı ve nasıl korunacağına ilişkin kurallar yer almaktadır [176].

Kanun kapsamında,

- Bir kamu kurumunun kişisel bilgileri bir program veya faaliyet için gerekli olmadığı sürece isteyemeyeceği ve istisnalar haricinde bu bilgileri elde etse bile kişiye hangi amaçla istenildiğini bildirmek zorunda olduğu,
- İsitisnalar haricinde, kişilerin rızası olmadıkça elde edilen bilgilerin sadece elde edilme amacına uygun şekilde ve yerlerde kullanılacağı ve başka kurum veya kuruluşlara verilemeyeceği,
- Bireylerin kamu kurumları tarafından kendileri hakkında tutulan bilgilere erişebileceğine ve şayet bilgiler yanlışsa düzeltilmesini isteyebileceğine

ilişkin hükümler yer almaktadır.

5.4.3.4 Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu (PIPEDA)

2000 yılında yürürlüğe giren PIPEDA ile özel sektör kuruluşlarının kişisel bilgileri ne şekillerde, hangi amaçlarla toplayabileceğine, hangi durumlarda 3. kişilere ifşa edebileceğine, ticari işlemlerde kullanabileceğine ve elektronik belgelerin kullanımının kolaylaştırılmasına ilişkin hükümler içermektedir. PIPEDA ile aynı zamanda bireylerin elektronik ticarete olan güvenlerinin artırılması ve AB'yi Kanada'nın kişisel bilgilerin korunmasına ilişkin yeterli derecede mevzuatının olduğuna dair ikna etmek amaçlanmıştır [177].

Kanunla kişisel bilgilerin korunmasına dair bazı önlemler alınmış ve kişilere bazı haklar tanınmıştır. Bunlar bireylerin [177];

- Bir şirket tarafından kişisel bilgilerinin hangi amaçlarla elde edildiği ve kullanıldığını bilme hakkı,
- Şirkette bilgileri toplamaya kimin yetkili olduğunu bilme hakkı,
- Kişisel verilerinin doğru, eksiksiz ve güncel olmasını isteyebilme hakkı,
- Kendi kişisel verilerine erişebilme hakkı ve yanlışlıklar varsa düzeltilmesini talep edebilme hakkı,
- Kişisel haklarına riayet edilmediği konusunda endişeleri varsa, yetkili makamlara şikâyet edebilme hakkı

gibi haklardır.

Ayrıca PIPEDA kapsamında şirketlere, kişisel bilgileri toplamadan önce bireylerin rızalarının alınması, bilgilerin hukuka ve ahlaka uygun amaçlarla elde edilmesi, amaca hizmet ettiği oranda ve ölçülülük ilkesi uyarınca toplanması ve toplanıldığı amaç dışında kullanılmaması, kişisel bilgilerin korunmasına ilişkin şeffaf ve anlaşılabilir politikaların geliştirilmesi ve bu amaçla yeterli güvenlik önlemlerinin alınmasının sağlanması gibi yükümlülükler getirilmiştir.

6. TÜRKİYE'DE SİBER GÜVENLİĞİN SAĞLANMASI

Türkiye'de siber güvenliğin sağlanmasına yönelik politikalar ve mevzuat çalışmaları 1990'lı yılların ikinci yarısından itibaren gündeme gelmeye başlamıştır.

6.1. Siber güvenliğin sağlanmasına yönelik çalışmalar

6.1.1 "Bilgi Sistem ve Ağları İçin Güvenlik Kültürü" konulu genelge

T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü tarafından yayımlanan 17 Şubat 2003 tarihli ve "Bilgi Sistem ve Ağları İçin Güvenlik Kültürü" konulu 2003/10 numaralı genelge ile, üyesi olduğumuz OECD tarafından hazırlanan "Bilgi Sistemleri ve Ağlarının Güvenliğine İlişkin OECD Rehber İlkeleri" ne yer verilmiş ve genelgenin ekinde bu ilkelerin türkçe çevirisine yer verilmek suretiyle öncelikle ve başta kamu kurum ve kuruluşları olmak üzere, bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda söz konusu ilkelerin göz önünde bulundurulması gerektiği belirtilmiştir [178].

6.1.2 DPT Bilgi Toplumu Stratejisi ve Bilgi Toplumu Stratejisi Eylem Planı

Ülkemizde siber güvenlik konusunda çalışmalar yapılması gerektiği 11/7/2006 tarihli ve 2006/38 sayılı Yüksek Planlama Kurulu Kararı ile ele alınmış ve bunun üzerine DPT Bilgi Toplumu Dairesi tarafından "Bilgi Toplumu Stratejisi" (2006–2010) ve "Bilgi Toplumu Stratejisi Eylem Planı" (2006–2010) yayımlanmıştır. Bilgi Toplumu Stratejisinde güvenlik, bilgi toplumuna dönüşüm sürecini etkileyen temel bir faktör olarak belirlenmiştir. Ayrıca bilgi toplumu uygulamalarında güvenliğin sağlanması kritik konulardan ve önceliklerden biri olarak ifade edilmiştir [179].

Bilgi Toplumu Stratejisi Eylem Planında ise İnternet güvenliği, bilgi güvenliği ve Ulusal Bilgi Sistemleri Güvenlik Programına yer verilmiş ve bu konularda düzenlemeler yapmak üzere sorumlu kurum ve kuruluşlar belirlenmiştir. Buna göre [180]:

- Bilgi Toplumu Stratejisi 10 numaralı Eylem Planında İnternet güvenliğine yer verilmiş ve "Bireylerin BİT kullanımına yönelik motivasyonlarının artırılması amacıyla İnternet ortamını güvenli hale getirecek yasal düzenlemelerin gerçekleştirileceği ve İnternet üzerinde çeşitli denetim ve yasakların düzenlenmesi, gereklilik ve ölçülülük kriterlerine bağlı kalınması şartıyla çocukların zihinsel ve bedensel sağlığının, kişilik haklarının, ailenin ve kamu düzeninin korunmasının sağlanacağı" ifade edilmiştir. Bu amaçları gerçekleştirmek üzere Adalet Bakanlığı sorumlu kuruluş olarak belirlenmiştir.

- Bilgi Toplumu Stratejisi 87 numaralı Eylem Planında bilgi güvenliği ile ilgili yasal düzenlemeler yapılması gerekliliğine yer verilmiş ve "Ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenleme yapılacağı ve uygulamaya konulacağı; Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Taslağının yasalaşacağı" ifade edilmiştir. Bu amaçları gerçekleştirmek üzere Adalet Bakanlığı sorumlu kuruluş olarak belirlenmiştir.

- Bilgi Toplumu Stratejisi 88 numaralı Eylem Planında Ulusal Bilgi Sistemleri Güvenlik Programına yer verilmiş, "Siber âlemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "Bilgisayar Olaylarına Acil Müdahale Merkezi" kurulacağı; kamu kurumları için gerekli minimum güvenlik seviyelerinin kurum ve yapılan işlem bazında tanımlanacağı, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyelerinin tespit edileceği ve eksikliklerin giderilmesi yönünde öneriler oluşturulacağı" ifade edilmiştir. Bu amaçları gerçekleştirmek üzere TÜBİTAK(UEKAE) sorumlu kuruluş olarak belirlenmiştir.

6.1.3 Ulusal Sanal Ortam Güvenlik Politikası

TÜBİTAK (UEKAE) koordinatörlüğünde 2008 yılı sonlarında, ülkemizi sanal ortamdaki saldırılara karşı hazır hale getirmek ve sanal ortamda yaşanacak sorunların ardından hızlı geri dönüşü sağlayacak sanal ortam güvenlik adımlarını belirlemek amacıyla "Ulusal Sanal Ortam Güvenlik Politikası" hazırlanmıştır [181]. Söz konusu politikayı hazırlayan kurum ve kuruluşlar aşağıda belirtilmiştir:

- Cumhurbaşkanlığı
- Başbakanlık
- Genelkurmay Başkanlığı
- Dışişleri Bakanlığı
- Adalet Bakanlığı
- Milli Savunma Bakanlığı
- Maliye Bakanlığı
- Ulaştırma Bakanlığı
- İçişleri Bakanlığı
- 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 (UEKAE)

Politika içerisindeki güvenlik adımları, tüm kurumsal ve kişisel bilgi sistemlerini ve bilgi sistemleri arasında iletişimi sağlayan sistemleri kapsamaktadır ve ulusal sanal ortamın ve bu ortamda işlenen bilginin gizlilik, bütünlük ve süreklilik kriterleri

çerçevesinde güvenliğini sağlamak hedeflenmektedir.

Politika kapsamında ülkemiz için bilgi ve iletişim sistemleri ile ilişkili risk unsurları şu şekilde belirtilmiştir [181]:

- Kamu kurumlarının ve özel kurumların birçoğunun sundukları hizmetleri İnternet üzerinden vermesi
- Kritik bilgi ve iletişim sistem altyapılarının birçoğunun İnternet'e bağlı olması
- Bilgi ve iletişim sistemlerinin sıklıkla güncellenmesi, bilgi ve iletişim sistemlerini kritik hizmetlerde kullanmak amacıyla hızla teknolojik projeler geliştirilmesi
- Kamu kurumlarının bilgi teknolojileri aracılığıyla verdiği hizmetlerin geniş halk kitlelerini etkilemesi
- Bilgi ve iletişim sistemleri güvenliği konusunun kurumların sadece bilgi işlem bölümlerinin sorumluluğunda görülmesi
- Kurumların üst yönetiminin yeterli düzeyde bilgiye sahip olmaması ve liderlik etmemesi
- Donanım ve yazılım olarak büyük oranda yurtdışına bağımlılık bulunması
- Kamu bilgi işlem birimleri çalışanlarının yeterli bilgi seviyesine sahip olmaması
- Kurumsal ve kişisel olarak yeterli bilinç seviyesinin yakalanamamış olması
- Özellikle kamu bilgi işlem birimleri yapılanmasının yetersiz olması
- Güvenliğin, bilgi ve iletişim sistemlerinin önemli bir unsuru olarak ele alınmaması.

Ulusal Sanal Ortam Güvenlik Politikasında siber güvenliğin sağlanması amacıyla aşağıda belirtilen çözüm önerileri kabul edilmiştir [181]:

1. Yasal Düzenlemeler: Bilgi ve iletişim sistemlerinin güvenliğinin sağlanması konusunda görev, yetki ve sorumluluklar ile organizasyon yapısını tanımlayan mevzuat altyapısı oluşturulacaktır.
2. Ülke Yeteneklerinin Geliştirilmesi: Kritik bilgi ve iletişim sistem altyapısına sahip kurumlar için personelin ve kurumun sahip olduğu teknik birikim, imkan ve kabiliyetler artırılacaktır.
3. Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu: Sanal ortamdaki tehditlerin hızlı tespiti, bilgi paylaşımı ve yaşanan olayların etkilerinin giderilmesi amacıyla Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu oluşturulacak ve ülkemiz kurum ve kuruluşlarının bilgisayar olaylarına müdahale yeteneği kazanması sağlanacaktır. Ülkeyi etkileyen sanal ortamdaki tehditlere karşı 7/24 müdahale esasında çalışacak "acil işlem merkezi" yapısı oluşturulacak ve diğer ülkeler ve uluslararası kuruluşlar için ulusal temas noktası olacaktır.
4. Bilgilendirme ve Bilinçlendirme Çalışmaları: Son kullanıcıların, sistem yöneticilerinin, teknoloji geliştiricilerinin, denetçilerin, orta ve yüksek seviyeli yöneticilerin bilgi ve iletişim sistemleri güvenliği bilincini artırmak amacıyla çalışmalar yapılacaktır
5. Ulusal Kritik Bilgi ve İletişim Sistem Altyapılarının Güvenliği: Ulusal kritik bilgi ve iletişim altyapıları tespit edilecek, bunların birbirleriyle ilişkileri, kritiklik seviyeleri ve sorumluları tespit edilecek ve bu altyapıların korunması sağlanacaktır.
6. Uluslararası Eşgüdüm: Diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapılacaktır.
7. Kurumsal Bilgi ve İletişim Sistemleri Güvenliği: Kurumlar, bilgi ve iletişim sistemleri güvenliği ile ilgili risk değerlendirmesi yapacak, standartlara uyum sağlayacaktır.
8. Ulusal Sanal Ortam Güvenlik Stratejisinin Hazırlanması: Bu hedeflerin gerçekleştirilmesi amacıyla Ulusal Sanal Ortam Güvenlik Stratejisi hazırlanacaktır.

6.1.4. Ulusal Bilgi Güvenliği Teşkilat ve Görevleri Hakkında Kanun Tasarısı Taslağı

Bilgi Toplumu Stratejisi 87 numaralı Eylem Planında bilgi güvenliği ile ilgili yasal düzenlemeler yapılması gerekliliğine yer verilmiş, "Ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenleme yapılacağı ve uygulamaya konulacağı" ifade edilmiş ve Adalet Bakanlığı sorumlu kurum olarak belirlenmiştir. Bu kapsamda ülkemizde Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, bu amaçla planların hazırlanması, ulusal güvenliği ilgilendiren bilgilerin korunması amacıyla "Ulusal Bilgi Güvenliği Teşkilat ve Görevleri Hakkında Kanun Tasarısı Taslağı" hazırlanmıştır [182].

6.2 Ülkemizde BOME Faaliyetleri

Bilgi Toplumu Stratejisi 88 numaralı Eylem Planında Ulusal Bilgi Sistemleri Güvenlik Programına yer verilmiş ve sanal ortamdaki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "Bilgisayar Olaylarına Acil Müdahale Merkezi (BOME)" kurulacağı, kamu kurumları için gerekli minimum güvenlik seviyelerinin kurum ve yapılan işlem bazında tanımlanacağı, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyelerinin tespit edileceği ve eksikliklerin giderilmesi yönünde öneriler oluşturulması gerektiği belirtilmiştir. Bu amaçları gerçekleştirmek üzere TÜBİTAK(UEKAE) sorumlu kuruluş olarak belirlenmiş, ayrıca ilgili kurum ve kuruluşlar olarak da üniversiteler ve kamu kuruluşları sıralanmıştır.

6.2.1 Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi (TR-BOME)

Ulusal Bilgi Sistemleri Güvenlik Programı çerçevesinde başta kamu kurum ve kuruluşları olmak üzere ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamak ve kamu bilgi sistemlerinin güvenliğinin sağlanması ile ilgili etkin önlemler alınmasına ön ayak olmak amacıyla Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) oluşturulmuş ve Dışişleri Bakanlığı'nın koordinasyonunda NATO'ya karşı bilgisayar güvenlik olayları ile ilgili ulusal temas noktası olarak TR-BOME belirlenmiştir. Ulusal bir BOME olan ve koordinasyon merkezi olarak görev yapan TR-BOME, BOME kurulum danışmanlığı, olay müdahale koordinasyonu ve alarm-uyarılar gibi hizmetler vermektedir [183].

6.2.1.1 BOME danışmanlığı

TR-BOME tarafından verilen danışmanlık hizmeti kapsamında, kurumların olay müdahale sorumluluğu bulunan çalışanlarının eğitilmesi, kurumda verilecek hizmetlerin belirlenmesi, bu hizmetlerin verilebilmesi için gerekli altyapının sağlanması ve olaylara müdahalede kullanılacak politika ve prosedürlerin belirlenmesi yer almaktadır. Ayrıca kurumlara, karşılaşacakları güvenlik olaylarına müdahale yeteneği kazandırmak amacıyla eğitimler verilmektedir.

6.2.1.2 Olay müdahale koordinasyon hizmeti

TR-BOME, İnternet sayfası üzerinden e-posta ve telefonla ihbar kabul etmekte, kendisine gelen ihbarları değerlendirip, gönüllülük esasıyla bu olayların çözümünü sağlamaya çalışmaktadır. Ülkemizde yaygın olarak kullanılan bilgi sistemi yazılım ve donanımlarında ortaya çıkan güvenlik açıklıkları takip edilip, özellikle yüksek, acil ve kritik önem derecesine sahip açıklıklara ve bu açıklıkların kapatılmasına ilişkin bilgi İnternet sayfasından yayınlanmaktadır. Ayrıca gerek e-posta listeleriyle

gerekse basın duyurusu hazırlanıp, ulusal basın aracılığıyla açıklıklardan vatandaşların haberdar edilmesi sağlanmaktadır.

TR-BOME, NATO bünyesinde siber savunmadan sorumlu olan NCIRC birimiyle 2007 yılında mutabakat zaptı imzalamıştır. Ayrıca 2008 yılında TF-CSIRT'e üye olmuş, EGC (European Government CERTs) için ise üyelik başvurusunda bulunmuş olup, sürecin sonuçlanmasını beklemektedir.

6.1.2.3 Alarm ve uyarılar kapsamındaki faaliyetler

Ulusal Bilgi Sistemleri Güvenlik Programı'nın en önemli unsurlarından birisi de Ulusal Bilgi Güvenliği Kapısı Projesidir. Ülkemizde bilgi güvenliği konusunda İnternet üzerinden bilgi paylaşımı sağlamayı amaçlayan İnternet sitesi "www.bilgiguvenligi.gov.tr" adresinden yayın yapmaktadır. Sitede, bilgi güvenliğiyle ilgili özel konularda okuyucu bilgilendirmeyi amaçlayan teknik yazılar, bilgi güvenliği ile ilgili kılavuzlar, ülkemizde yapılan etkinlik, toplantı, sempozyum vs. gibi organizasyonların duyuruları, önemli güvenlik açıklıklarıyla ilgili güvenlik bildirisi sayfası bulunmaktadır. Ayrıca ülkemizdeki bilgi sistemlerinde yaygın olarak kullanılan yazılım ve donanımlarda bulunan açıklıklar ve bu açıklıkların nasıl kapatılacağına ilişkin bilgiler söz konusu İnternet sayfasında yayınlanmaktadır [184].

TR-BOME tarafından virüs, solucan gibi kötücül yazılımların incelenmesi için laboratuar ortamında çalışmalar yapılmaktadır. Ayrıca kamu kurumlarına ait kritik bilgi sistemlerini hedef alan tehditleri tespit etmek amacıyla Ulusal Sanal Ortam Savunma Merkezi oluşturulmuştur. Bu sistem, birden fazla kamu kurumunu hedef alan koordineli saldırıları tespit edebileceği gibi bir kamu kurumunu hedef alan çok ciddi saldırıları da fark edebilecek yapıda oluşturulmuştur [185].

6.2.2 Ulak –CSIRT

Altyapısını Ocak 1997'de hizmete açmış olan Ulusal Akademik Ağ (UlakNet) üniversiteler ve araştırma kurumlarını birbirine bağlamaktadır ve TÜBİTAK'ın bir

enstitüsü olan ULAKBİM tarafından işletilen bu ağ üniversiteler ve birçok kamu kurum ve kuruluşuna hizmet sağlamaktadır.

Şubat 2006'da, ULAKNET bünyesinde bilgi güvenliği konusundaki bilincin artırılması, yaşanan bilgisayar güvenlik olayları sayısının azaltılması ve ağın kurulduğu tarihten beri sürdürülen çalışmaların daha koordineli bir hale getirilmesi için Ulak-CSIRT olarak adlandırılan UlakNet Bilgisayar Olaylarına Müdahale Birimi kurulmuş ve faaliyete başlamıştır [186].

2007 tarihinde The European CSIRT Directory'e akredite olan Ulak-CSIRT'in görev ve sorumlulukları şunlardır:

- Ağ genelinde bilgi güvenliği bilincini artırmak
- Akademik ağa yapılan bilgisayar güvenliğini tehdit edici saldırı sayısını azaltmak
- Güvenlik ihlali sorumlularını tespit etme aşamasının koordinasyonunu sağlamak
- Güncel açıklıklar ve çözümleri hakkında ağa bağlı uçların yöneticilerini bilgilendirmek
- Bağlı uç yöneticilerine bilgi güvenliği hakkında eğitim vermek
- Bilgi güvenliğini sağlamak için kullanılacak yöntemler hakkında Türkçe belgeleri sağlamak [187].

6.3. Siber Güvenlik Kültürü Oluşturulmasına Yönelik Çalışmalar

Genç nüfusa sahip bir ülke olarak ülkemizde İnternet ve bilgisayar kullanım oranları sürekli artmaktadır. Bu doğrultuda siber güvenliğin sağlanmasında siber güvenlik kültürünün oluşturulmasına yönelik çalışmaların büyük önemi bulunmaktadır.

6.3.1 BTK'nın faaliyetleri

BTK, gerek ITU nezdinde ülkemizi temsil eden kurum olması, gerekse 5809 sayılı

Elektronik Haberleşme Kanunu ile kendisine verilen bilgi, şebeke ve haberleşme güvenliği ile ilgili görevleri dolayısıyla düzenleme faaliyetlerinden farkındalık oluşturma etkinliklerine kadar siber güvenliğin sağlanması ile ilgili çalışmalar yapmaktadır.

6.3.1.1 Spam ile mücadele projesi

2009 yılı başında BTK koordinatörlüğünde TTNET, Çizgi Telekom, Doruknet ve Mynet'in işbirliğiyle "Spam ile Mücadele Pilot Projesi" uygulamaya geçirilmiştir. Pilot proje çıktılarının olumlu olması sonrasında diğer ilgili tarafların da katılım ve katkılarıyla Spam ile Mücadele Projesi 15-Haziran–19 Ekim 2009 tarihleri arasında tüm Türkiye'de 3 fazda uygulanmıştır. Proje sonucunda spam mesaj yayan IP sayısının %99 civarında düşüş gösterdiği ve TTNET'in yaydığı günlük spam mesaj sayısının 6,5 milyar düzeyinden 394 milyon düzeyine indiği görülmüştür.

6.3.1.2 Farkındalık oluşturma çalışmaları

BTK tarafından siber güvenliğe ilişkin farkındalık oluşturulması amacıyla birçok çalışma yapılmaktadır. Bu çalışmalara aşağıda yer verilmiştir:

6.3.1.2.1 Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler Raporu

BTK tarafından, siber güvenlik sorununun değişik boyutlarıyla anlaşılabilmesine, konu ile ilgili tarafların bilgilendirilmesine ve bilgi ve şebeke güvenliği konularında farkındalığın artırılmasına katkıda bulunmak amacıyla "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler" konulu rapor hazırlanmıştır. Rapor kapsamında siber tehditlere ve amaçlarının neler olduğuna, kritik bilgi altyapısının korunmasına ve siber güvenliğin sağlanmasına yönelik bilgiler verilmiş, ulusal siber güvenliğin sağlanması amacıyla neler yapılması gerektiği ve eksikliklerin neler olduğu belirtilmiştir [2].

6.3.1.2.2 Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri Raporu

BTK tarafından BM, ITU, OECD, Avrupa Konseyi ve AB tarafından siber güvenlik konusunda yürütülmekte olan faaliyetleri ele alan "Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri" konulu rapor hazırlanmıştır [188].

6.3.1.2.3 Botnet – Zombi Projesi

BTK tarafından 2010 yılı başında ilgili taraflarla işbirliği içerisinde zombi-botnetlerin tespit edilmesi ve temizlenmesine yönelik olarak Botnet – Zombi Projesi başlatılmıştır.

6.3.1.2.4 Bilgi Güvenliği ve Kriptoloji Konferansı

BTK, Bilgi Güvenliği Derneği, Gazi Üniversitesi ve Orta Doğu Teknik Üniversitesi işbirliği ile 2007 yılından itibaren her yıl Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı düzenlenmektedir. Konferansın temel hedeflerinden birisi, bilgi güvenliği ve kriptoloji kavramlarının toplumun bireyleri tarafından özümsenmesine yardımcı olmaktır. Konferans kapsamında her yıl farklı bir tema seçilmekte ve uluslararası katılım sağlanmaktadır[189]. Bilgi Güvenliği ve Kriptoloji Konferansı, ülkemiz adına kamu sektörü-üniversite-STK işbirliğinin sağlanması çalışmalarının en güzel örneklerindendir.

6.3.2 Güvenli Web

Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı tarafından, hızla yaygınlaşmakta olan İnternet dünyası ile ilgili olarak genelde toplumu, özelde ise çocukları, aileleri ve eğiticileri bilinçlendirmek, İnternetin en etkin ve faydalı kullanım metotları yanında, barındırdığı tehlikelere karşı toplumda bilişim şuurunu oluşturmak amacıyla "güvenliweb.org.tr" adı altında bir İnternet sitesi oluşturulmuştur.

Site kapsamında ülkemizde ve dünyada genel İnternet kullanım eğilimleri ve benzeri faydalı istatistikî bilgilendirmeler yapılmakta, özellikle İnternette içerik sunan özel veya tüzel kurum, kuruluş ve kişilerin daha etkin bir hizmet sunabilmeleri amacıyla referans alabilecekleri bilgiye ulaşmaları hedeflenmektedir. Ayrıca çocuklar, aileler, eğiticiler için çözüm önerileri sunulmakta ve siber güvenliğin sağlanması konusunda farkındalık oluşturulması hedeflenmektedir [190].

Bunun yanı sıra Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı tarafından intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama suçları ile 25/7/1951 tarihli ve 5816 sayılı "Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun" kapsamındaki suç düzenlemeleri çerçevesinde İnternetteki zararlı içerik hakkında ihbarların yapılabileceği "ihbarweb.org.tr" adresinden hizmet veren bir İnternet ihbar hattı oluşturulmuştur.

Ayrıca Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı tarafından Ulaştırma Bakanlığı ve MEB işbirliği ile "Güvenli İnternet Kullanımı İçin Tavsiyeler" adlı bir kitapçık yayınlanmıştır. Söz konusu kitapçıkta, öğrencileri ve velileri İnternette yer alan tehlikelerden korumaya yönelik ve bilgi teknolojilerinin doğru kullanılabilmesi amacıyla faydalı ve önemli bilgiler yer almaktadır [191].

6.3.3 İnternetin bilinçli kullanımı ve internet güvenliği projesi

MEB Eğitim Teknolojileri Genel Müdürlüğü tarafından yürütülen "İnternetin bilinçli kullanımı ve İnternet güvenliği projesi" kapsamında İnternet ihbar hattı oluşturulmuştur [192].İnternet ihbar hattı, İnternet ortamında yer alan zararlı içeriğin ihbar edilmesini sağlamak amacıyla oluşturulmuştur ve İnternette yer alan her türlü zararlı içeriğe ilişkin şikâyetin alınacağı, değerlendirileceği bir birim olarak faaliyetlerini sürdürmektedir.

İnternet ihbar hattı kapsamında cinsellik, şiddet, kumar, ideolojik propaganda, bomba yapımı gibi konularda zararlı içeriğe sahip İnternet sayfaları bir form doldurulmak suretiyle ihbar edilebilmektedir.

6.3.4 Ulusal Bilgi Güvenliği Kapısı

Ulusal Bilgi Güvenliği Kapısı, başta kamu kurumları olmak üzere tüm ülkenin bilgi güvenliği konusunda bilinçlenmesini sağlamak, bu konuda çalışan bireylerin bilgi seviyelerini arttırmak amacıyla kurulmuştur. Ulusal Bilgi Güvenliği Kapısının kurulması ve işletilmesi, Ulusal Bilgi Güvenliği Programının bir alt projesi olarak TÜBİTAK (UEKAE) tarafından gerçekleştirilmektedir. Ulusal Bilgi Güvenliği Kapısı kapsamında bilgi güvenliği ile ilgili güncel uyarılar, bilgilendirici rehberler ve teknik yazılar yayınlanmakta, bilgi güvenliği ile ilgilenen kamu kurumu çalışanlarının doğrudan bilgi alışverişi yapabilecekleri e-posta listeleri gibi interaktif ortamların sağlanması suretiyle güvenliğin sağlanmasına katkıda bulunulmaktadır [193]. Ayrıca TÜBİTAK (UEKAE) tarafından 2005 yılından bu yana "bilgi güvenliği günü" kapsamında çeşitli etkinlikler düzenlenmektedir.

6.3.5 İnternet haftası etkinlikleri

Bilişim sivil toplum kuruluşu platformu tarafından 1998 yılından bu yana her yıl nisan ayının ikinci ve üçüncü haftaları İnternet haftası olarak kutlanmakta ve bu kapsamda etkinlikler düzenlenmektedir [194]. İnternet Haftası etkinliği ile toplumda İnternet kültürünü yaymak, İnternet bilincini yaratmak, yeni projeler başlatmak, sorunları ve çözüm yollarını tartışmak amaçlanmaktadır. Söz konusu etkinliğe STK'lar büyük oranda destek vermektedir.

6.4. Siber Suçlara ve Siber Güvenliğin Sağlanmasına İlişkin Mevzuatımız

6.4.1 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümleri

5237 sayılı TCK'nın "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde siber

güvenliğin sağlanmasına yönelik hükümler yer almaktadır [195].

6.4.1.1 Bilişim sistemine girme suçu (m.243)

5237 sayılı TCK'nın "Bilişim sistemine girme" başlıklı 243 üncü maddesinde bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girilmesi ve orada kalmaya devam edilmesi suç olarak düzenlenmiştir. Bu madde ile Avrupa Konseyi Siber Suçlar Sözleşmesinin 2 nci maddesinde yer alan "hukuka aykırı erişim" düzenlemesiyle paralellik sağlanmaktadır. Söz konusu suçun meydana gelebilmesi için hukuka aykırı olarak bir bilişim sisteminin bir kısmına veya tamamına girilmiş olması yeterli kabul edilmemekte, aynı zamanda girme eyleminin belirli bir süre devam etmesi yani failin bir süre bilişim sisteminde kalması gerekmektedir [61].

Bilişim sistemine girme suçu ile bilgi ve iletişim sistemlerinin güvenliği korunmaktadır [37]. Ayrıca bilgi ve iletişim sistemlerinin kullanıcısı ve bu sistemlerden yararlanan bireyerin verilerinin gizliliğinin korunması, özel hayatlarının dokunulmazlığı gibi kişisel yararları da korunmaktadır [65].

6.4.1.2 Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları (m.244)

5237 sayılı TCK' nın 244 üncü maddesinin "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" kenar başlıklı 1 inci fıkrasında bir bilişim sisteminin işleyişini engelleyen veya bozan kişinin cezalandırılacağı, 2 nci fıkrasında ise bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin cezalandırılacağı belirtilmiştir. Bu suç ile Avrupa Konseyi Siber Suç Sözleşmesi'nin 4 üncü maddesinde öngörülen "verilere müdahale" ve 5 inci maddesinde öngörülen "sisteme müdahale" düzenlemeleri ile paralellik kurulmaya çalışılmıştır.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları ile bilişim sistemi ve/veya bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisi bulunan

kişilerin verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma gibi değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşmaları ve bunları kullanmaları amaçlanmaktadır [37].

6.4.1.3 Banka veya kredi kartlarının kötüye kullanılması suçları (m.245)

5237 sayılı TCK'nın 245 inci maddesi ile başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlaması durumunda cezalandırılacağı düzenlenmiştir.

245 inci maddenin gerekçesinde, maddenin banka ve kredi kartlarının haksız, hukuka aykırı olarak kullanılması üzerine bankaların ve kart sahiplerinin zarara sokulmasının ve bu yolla çıkar sağlanmasının önlenmesi ve faillerin cezalandırılması amacıyla söz konusu maddeye yer verildiği belirtilmiştir. Ayrıca bankaların hizmetleri aracılığıyla yürüyen ticari hayatın ve bankacılık sisteminin güvenilirliği de korunan hukuki yararlar arasında sayılmaktadır [196] .

6.4.1.4 Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (m. 142)

Hırsızlık suçunun nitelikli hallerini düzenleyen 5237 sayılı TCK'nın 142 nci maddesinin 2 nci fıkrasının (e) bendinde, hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde cezalandırılacağı düzenlenmiştir.

6.4.1.5 Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (m.158)

Dolandırıcılık suçunun nitelikli hallerini düzenleyen 5237 sayılı TCK'nın 158 inci maddesinin 1 inci fıkrasında dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde

cezalandırılacağı ifade edilmektedir.

6.4.2 Elektronik Haberleşme Kanunu

10 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun "İlkeler" kenar başlıklı 4 üncü maddesinin (l) bendinde, "İlgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi ilkesi" yer almaktadır [197].

Ayrıca Kanunun "İşletmecilerin hak ve yükümlülükleri" kenar başlıklı 12 nci maddesinde Kurumun işletmecilere, kişisel verilerin ve gizliliğin korunması, afet durumlarındaki haberleşmenin kesintisiz devam edebilmesi için gerekli tedbirlerin alınması, elektronik haberleşme şebekelerinin bütünlüğünün idame ettirilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması, hizmet kalitesi de dâhil olmak üzere standartlar ve spesifikasyonlara uyumluluk sağlanması gibi yükümlülükler getirebileceği düzenlenmiştir.

6.4.3 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

04 Mayıs 2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin usul ve esaslar düzenlenmiştir [198].

Kanun kapsamında İnternet ortamında yapılan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama, 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında

Kanunda yer alan ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlara yönelik yayınlara erişimin engellenmesi kararı verilebilmektedir.

6.4.4 Elektronik İmza Kanunu

23 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esaslar düzenlenmekte ve elektronik imzanın hukukî yapısı, elektronik sertifika hizmet sağlayıcılarının faaliyetleri ve elektronik imzanın kullanımına ilişkin hükümler yer almaktadır [199].

Kanun 5 inci maddesi ile güvenli elektronik imzanın elle atılan ıslak imza ile aynı hukukî sonucu doğuracağı fakat kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinin güvenli elektronik imza ile gerçekleştirilemeyeceği hüküm altına alınmıştır. Bu doğrultuda, örneğin tapu devrini sağlayan sözleşmeler, araç satışları, mal rejimi sözleşmeleri, vasiyet gibi sözleşmeler, evlenme gibi işlemler elektronik imza ile yapılamamaktadır [61].

Ayrıca Kanunun 16 ncı maddesinde imza oluşturma verisinin veya aracının ilgilinin rızası dışında elde edilmesi, verilmesi, kopyalanması, bu araçların yeniden oluşturulması, izinsiz elde edilen araçların kullanılması suretiyle izinsiz elektronik imza oluşturulması eylemleri, 17 nci maddesinde ise elektronik sertifikalarda sahtekârlık işlemleri suç olarak düzenlenmiştir.

6.4.5 Elektronik Haberleşme Güvenliği Yönetmeliği

BTK tarafından elektronik haberleşme güvenliğine ilişkin usul ve esasları belirlemek amacıyla düzenlenmiş olan Elektronik Haberleşme Güvenliği Yönetmeliği kapsamında işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden

ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesine veya azaltılmasına ilişkin olarak alacakları tedbirlere yer verilmektedir [200].

Yönetmeliğin 6 ncı maddesinde elektronik haberleşmeye ilişkin başlıca tehditler;

a) Yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi,
b) Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması,
c) Donanım-yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi,
ç) Deprem, sel, su baskını, yangın gibi doğal afetler ile grev ve lokavt hali,
d)Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,
e) Elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve/veya dinlenmesi,
f) Doğru olmayan bir bilgi üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafa gönderilmesi,
g) Elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez hale getirilmesi veya altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesi
olarak belirtilmiştir.

6.4.6 Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı

Adalet Bakanlığı tarafından 2009 yılı sonlarında elektronik ticarete ve bazı bilgi toplumu hizmetlerine ilişkin usul ve esasları düzenlemek amacıyla "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı" hazırlanmıştır [201]. Tasarı kapsamında ticarî elektronik iletilere[7] ilişkin düzenlemelere de yer verilmiş, ticarî

[7] Tasarı kapsamında spam (istenmeyen elektronik posta) kavramının karşılığı olarak "ticari elektronik ileti" ifadesi kullanılmıştır.

elektronik iletilerin alıcılara ancak önceden onayları alınmak kaydıyla gönderilebileceği belirtilmek suretiyle önceden izin alma şartı getiren "opt-in" yöntemi kabul edilmiştir. Ayrıca Tasarıda istisna olarak "Esnaf ve tacirlere önceden onay alınmaksızın ticarî elektronik iletiler gönderilebilir" hükmü ile alıcının ilk elektronik postadan sonra reddetme hakkı olarak tanımlanan "opt-out" yöntemi kullanılmıştır.

Belirtilen hükümlerin yanı sıra tasarıda;

- Ticarî elektronik iletinin içeriğinin alıcıdan alınan onaya uygun olması,
- İletide, göndericinin tanınmasını sağlayan bilgiler ile haberleşmenin türüne bağlı olarak telefon numarası, faks numarası, kısa mesaj numarası ve elektronik posta adresi gibi erişilebilir durumdaki iletişim bilgilerinin yer alması,
- İletide, haberleşmenin türüne bağlı olarak, iletinin konusu, amacı ve başkası adına yapılması hâlinde kimin adına yapıldığına ilişkin bilgilere de yer verilmesi,
- Alıcıların diledikleri zaman, hiçbir gerekçe belirtmeksizin ticarî elektronik iletileri almayı reddedebilme hakkı,
- Ret bildiriminin elektronik araçlarla kolay ve ücretsiz olarak iletilmesinin sağlanması ve gönderilen iletide buna ilişkin gerekli bilgilerin sunulması,
- Talebin ulaşmasını müteakip göndericinin, iki iş günü içinde alıcıya elektronik ileti göndermeyi durdurması

gibi hükümler yer almaktadır.

7. SONUÇ VE ÖNERİLER

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 tanımlanan 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 hedefleri, bilginin erişilebilirliğinin, bütünlüğünün ve gizliliğinin sağlanmasıdır.

Siber güvenliğin sağlanması ortaklaşa bir çaba ve sorumluluk gerektirmektedir. Bu doğrultuda kamu kurumlarına, özel sektöre, STK'lara, üniversitelere ve bireylere önemli görevler düşmektedir. Kritik bilgi altyapısının korunması, kamu-özel sektör işbirliğinin sağlanması, BOME'lerin oluşturulması, uluslararası işbirliğinin sağlanması, siber güvenlik kültürünün oluşturulması ve siber güvenliğin sağlanmasına yönelik yasal mevzuatın geliştirilmesi siber güvenliğin sağlanmasının başlıca unsurlarıdır. Siber güvenliğin sağlanmasında bu unsurların birlikte ele alınması ve değerlendirilmesi gerekmektedir.

Siber güvenliğin sağlanmasında siber suçlarla mücadele önemli bir rol oynamaktadır. Siber suçları diğer suçlardan, yani geleneksel anlamdaki suçlardan ayıran en önemli özelliklerden birisi bu suçların işleniş şekillerinin tespitinin zorluğudur. Söz konusu suçlar yepyeni ve çok farklı yollarla işlenebilmektedir. Oltalama, spam, kötücül yazılımlar ve botnet'ler siber suçların başlıca işleniş şekilleridir.

Siber güvenliğin sağlanması konusunda AB, BM, OECD, Avrupa Konseyi, G8 gibi uluslararası kuruluşlar önemli çalışmalar yapmaktadır. Aynı şekilde ABD, İngiltere, Kanada, Avustralya gibi gelişmiş ülkeler de siber güvenliğe yönelik tehlikelerin farkına varmış, kritik bilgi altyapılarının korunmasına yönelik önemli girişimlerde, düzenlemelerde bulunmuşlardır.

Tez çalışması kapsamında yapılan araştırmalar sonucu elde edilen sonuçlar doğrultusunda, Türkiye'de siber güvenliğin sağlanması konusunda yapılması gereken çalışmalara yönelik değerlendirme ve önerilere aşağıda yer verilmektedir:

7.1 Siber güvenliğin sağlanmasına yönelik değerlendirme ve öneriler

Ülkemizde hâlihazırda yürütülen çalışmalar olmakla birlikte henüz siber güvenliğin sağlanmasına yönelik bir politika ya da strateji mevcut değildir. Bu durumun, ülkemizin şimdiye kadar çok büyük oranda bir siber saldırıya maruz kalmamış olması, siber suçların en tehlikeli halleriyle tanışmamış, siber terörün korkutucu yüzüyle henüz karşılaşmamış olmasından kaynaklanmış olabileceği değerlendirilse de gelişmekte olan bir ülke olarak, siber güvenliğe ilişkin resmi bir politika oluşturulmasının, sorumlu kurum ve kuruluşların belirlenmesinin gerekli olduğu değerlendirilmektedir.

Önceki bölümlerde de ifade edildiği üzere, 2006–2010 Bilgi Toplumu Stratejisi Eylem Planında siber güvenliğin sağlanmasına ilişkin eylemlere yer verilmiştir. 2008 yılı sonlarında ise, TÜBİTAK (UEKAE) koordinatörlüğünde kamu kurumlarının da katılımıyla ülkemizi sanal ortamdaki saldırılara karşı hazır hale getirmek ve sanal ortamda yaşanacak sorunların ardından hızlı geri dönüşü sağlayacak sanal ortam güvenlik adımlarını belirlemek amacıyla "Ulusal Sanal Ortam Güvenlik Politikası" hazırlanmıştır. Ayrıca söz konusu politika kapsamında Ulusal Sanal Ortam Güvenlik Stratejisi hazırlanacağı belirtilmiştir.

Ulusal Sanal Ortam Güvenlik Stratejisinin hazırlanması ve politika belgesinde yer alan hususlar olumlu gelişmeler olarak değerlendirilmekle birlikte, bu konuda koordinasyonun TÜBİTAK (UEKAE) yerine, 3056 sayılı Başbakanlık Teşkilatı Hakkında Kanun hükümleri doğrultusunda T.C. Başbakanlık tarafından yürütülmesinin daha uygun olacağı değerlendirilmektedir.

Bu çerçevede siber güvenliğin sağlanmasına ilişkin yürütülecek çalışmalar ve hazırlanacak olan strateji kapsamında;

- BTK tarafından hazırlanmış olan "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler" konulu raporda yer alan ulusal siber güvenliğin sağlanmasına ilişkin öneriler de göz önüne alınmalı,
- Siber güvenliğin sağlanmasında kritik altyapıların ve kritik bilgi altyapısının korunmasının önemine yer verilmeli,
- Kamu-özel sektör işbirliğinin, bilgi paylaşımının ve BOME'ler oluşturulmasının önemi vurgulanmalı,
- Siber güvenlik kültürü oluşturulmasına ilişkin adımlara yer verilmeli,
- Uluslararası işbirliğinin sağlanmasının önemi vurgulanmalı ve bu doğrultuda çalışmalar yürütülmeli,
- Siber güvenliğe ilişkin yasal mevzuatımızın geliştirilmesine yönelik çalışmalarda bulunulmalıdır.

7.2. Kritik bilgi altyapısının korunmasına yönelik değerlendirme ve öneriler

"Kesilmesi veya tahribatı halinde vatandaşların sağlığı, güvenliği, ekonomik refahı üzerinde, hükümetin veya ekonominin işleyişi üzerinde etki doğuracak birbiriyle bağlantılı bilgi sistemleri ve ağları" olarak tanımlanmış olan kritik bilgi altyapısı, ülkelerin siber saldırılara karşı korunmasında, ulusal güvenlik açıklarının azaltılmasında ve oluşan hasarların ve kurtarma sürelerinin asgariye indirilmesi gibi alanlarda hayati önemi haizdir.

Yaşantımızın temelini oluşturan fiziksel, ekonomik, kurumsal altyapılarımız her geçen gün kritik bilgi altyapılarına bağımlı hale gelmektedir. Ülkemizde 18.000 kişinin yaşamını yitirdiği 17 Ağustos 1999 depremi sonrasında iletişim hatları devre dışı kalmış, telefon hatları çökmüş, bölgeyle saatlerce iletişim

kurulamamıştır. Yaşanmış olan bu ve buna benzer olaylara, meydana gelen can kayıplarına ve hasarlara rağmen, ülkemizde kamu güvenliğinin, düzeninin ve sağlığının korunabilmesi için hayati önemi haiz olan kritik altyapıların korunmasına ilişkin bir düzenleme, strateji bulunmamaktadır. Tez kapsamında kritik bilgi altyapısının korunmasına yönelik şu önerlerde bulunulmaktadır:

7.2.1. Kritik bilgi altyapısının korunmasına yönelik faaliyetlerinden sorumlu olacak bir Kurum tespit edilmelidir

Kritik bilgi altyapısının korunmasını teminen, öncelikle bu faaliyetlerden sorumlu olacak bir Kurumun tespit edilmesi gerekmektedir. Ülkemizde mevcut kurumların görev ve sorumlulukları değerlendirildiğinde, kritik bilgi altyapısının korunmasına yönelik faaliyetlerin Başbakanlık sorumluluğunda yürütülmesinin gerektiği değerlendirilmektedir.

Ülkemiz için kritik altyapıların neler olduğunun tespiti ve kritik sektörler arası iletişim sağlanması görevlerinin kamu kurumları, özel sektör temsilcileri ile işbirliği içerisinde Başbakanlık tarafından yürütülmesinin uygun olacağı değerlendirilmektedir.

7.2.2 Kritik bilgi altyapısının korunmasına yönelik ulusal bir plan hazırlanmalıdır

Başbakanlık tarafından ilgili kamu kurumları, özel sektör temsilcileri, STK'lar ve üniversitelerle işbirliği içerisinde "Ulusal Kritik Bilgi Altyapısının Korunması Planı" hazırlanmalıdır. Plan kapsamında aşağıda belirtilen hususlara yer verilmesi gerektiği değerlendirilmektedir:

- Kritik altyapılar ve kritik bilgi altyapıları tanımlanmalıdır.

İçerisinde bulunduğumuz bilgi çağında, kritik olsun-olmasın altyapılarımız bilgi

ve iletişim şebekelerine bağımlı hale gelmiştir ve bu da hangi sektör olursa olsun bilgi altyapısına bağımlı olduğumuzu göstermektedir. Bankacılık sektöründen ulaşım sektörüne, savunma sanayiinden enerji sektörüne bütün kritik sektörler bilgi altyapısını kullanmaktadır. Bu nedenle de görev ve sorumlulukların tespit edilebilmesi bakımından kritik altyapının ve kritik bilgi altyapısının ülkemiz açısından tanımının yapılması gerekmektedir.

Bu çerçevede, gelişmiş ülkelerin ve uluslararası kuruluşların tanımları da göz önüne alınarak, kritik altyapının "zarar görmesi veya kullanılamaz hale gelmesi durumunda ulusun sosyal, ekonomik refahı veya ülkenin ulusal savunmasının ve ulusal güvenliğinin sağlanması üzerinde etkisi olabilecek varlıklar, hizmetler ve sistemlerdir" şeklinde tanımlanabileceği değerlendirilmektedir.

Kritik bilgi altyapısının ise, OECD tarafından yapılan tanım da göz önüne alınarak, "Kesilmesi veya tahribatı halinde vatandaşların sağlığı, güvenliği, ekonomik refahı üzerinde, hükümetin veya ekonominin işleyişi üzerinde etki doğuracak birbiriyle bağlantılı bilgi sistemleri ve ağları" olarak tanımlanabileceği değerlendirilmektedir.

- Kritik altyapı sektörleri ve söz konusu sektörlerden sorumlu olacak Kurumlar belirlenmelidir

Kritik altyapı sektörlerinin belirlenmesi ve sorumlulukların sınırlarının tesbiti; siber güvenliğin sağlanmasında paylaşılması gereken sorumlulukların neler olduğunun belirlenmesi ile sektörler arası işbirliğinin sağlanması bakımından oldukça önemlidir. Bu bağlamda ülkemiz için kritik sektörlerin ve bu sektörlerden sorumlu olacak Kurumların şu şekilde belirlenebileceği değerlendirilmektedir:

1. Bilgi ve iletişim teknolojileri- BTK
1. Enerji- Enerji Piyasası Düzenleme Kurumu
2. Bankacılık ve Finans- Bankacılık Düzenleme ve Denetleme Kurumu

3. Savunma Sanayi- Mili Savunma Bakanlığı
4. Ulaştırma- T.C. Ulaştırma Bakanlığı
5. Acil durum hizmetleri- T.C. İçişleri Bakanlığı
6. Sağlık-T.C. Sağlık Bakanlığı
7. Su- Devlet Su İşleri Genel Müdürlüğü
8. Devlet yönetimi- T.C. Başbakanlık
9. Gıda-Tarım ve Köy İşleri Bakanlığı

- Kritik Altyapının Korunması Kurulu oluşturulmalıdır.

T.C. Başbakanlık koordinatörlüğünde yukarıda belirtilen kritik sektörlerin sorumlu kurumlarının temsilcilerinden oluşan Kritik Altyapının Korunması Kurulunun oluşturulması gerektiği değerlendirilmektedir. Kritik Altyapının Korunması Kurulu belirli aralıklarla toplanmak suretiyle sektörlerin güvenlik açıkları, alınması gereken önlemler ve bilgi paylaşımının sağlanmasına yönelik kararlar almalıdır.

Şekil 7.1 Kritik Altyapının Korunması Kurulu

- Kritik altyapı sektörleri arasında işbirliği, koordinasyon ve bilgi paylaşımı sağlanacak bir yapı belirlenmelidir.

Birçok ülkede olduğu gibi ülkemizde de kritik altyapıların büyük çoğunluğu özel sektör tarafından işletilmekte olduğundan, kritik altyapıların korunmasına yönelik olarak özel sektör ile bilgi paylaşımının, koordinasyonun sağlanmasının gerektiği değerlendirilmektedir. Bu çerçevede Ulusal Kritik Bilgi Altyapısının Korunması Planı kapsamında bilgi paylaşımını ve koordinasyonu sağlayacak bir yapı meydana getirilmelidir.

Söz konusu yapı içerisinde kritik altyapı sektörlerinden sorumlu Kurum koordinatörlüğünde o sektörde yer alan özel sektör kuruluşları ve STK'ların da içerisinde yer aldığı Kurullar oluşturulmalıdır. Kurullar tarafından kendi sektörlerinin güvenlik açıkları, alınması gereken önlemlere ilişkin raporlar hazırlanmalı ve bu raporlar Kritik Altyapının Korunması Kurulunda gündeme getirilmelidir. Örneğin bilgi ve iletişim teknolojileri sektöründen sorumlu olan BTK koordinatörlüğünde sektörde yer alan şirketlerin ve STK'ların temsilcilerinin de yer aldığı Bilgi ve İletişim Sektörü Kurulu oluşturulmalı ve söz konusu Kurul tarafından belirli aralıklarla toplanmak suretiyle sektöre ait güvenlik açıkları, alınması gereken önlemlere ilişkin raporlar hazırlamak gibi faaliyetlerde bulunulmalıdır.

- Sektörler arası bilgi paylaşımı sağlanmalıdır

Her sektörün kendi içerisinde bilgi paylaşımını sağlamasının yanı sıra, sektörler arası bilgi paylaşımının da sağlanması gerekmektedir. Bu bağlamda, sektörlerarası güvenli bilgi paylaşım ağları oluşturulmalıdır.

7.3 Kamu-özel Sektör İşbirliğinin Sağlanmasına Yönelik Değerlendirme ve Öneriler

Siber güvenliğin sağlanması kollektif çaba gerektirmektedir ve bu konuda kamu sektörünün ve özel sektörün işbirliği içerisinde hareket etmesi, bilgi paylaşımının sağlanması gerekmektedir. Elektronik haberleşme, enerji gibi birçok kritik sektörün özel sektör tarafından işletilmekte olduğu ülkemizde kamu-özel sektör işbirliği oldukça önemlidir. Bu nedenle sektörlerin birbirleriyle iletişim içerisinde olmaları, bilgi paylaşımı sağlamaları gerekmektedir.

Ülkemizde kamu-özel sektör işbirliğinin sağlanmasına yönelik bir çalışma, bilgi paylaşımı sağlanmasına yönelik bir zemin bulunmamaktadır. Yukarıda belirtilmiş olan yapı çerçevesinde bilgi paylaşımını sağlamaya yönelik çalışmalar yapılmasının gerektiği değerlendirilmektedir. Ayrıca kamu-özel sektör işbirliği ile konferanslar, paneller düzenlenmesi suretiyle bilgi paylaşımının sağlanması da önemlidir. Ülkemizde bu tarz etkinlikler yapılıyor olmakla birlikte, söz konusu etkinliklerin sayısının artırılması gerektiği değerlendirilmektedir.

7.4. BOME'lere yönelik değerlendirme ve öneriler

Bir bilgisayar güvenlik olayı durumunda müdahale etmek veya koordinasyon faaliyetlerinde bulunmakla görevlendirilmiş organizasyon kuruluşları olan BOME'ler; hükümetler, özel sektör kuruluşları, üniversiteler veya kar amacı gütmeyen kuruluşlar için oluşturulmakta ve olaylar sonucu meydana gelebilecek hasarları kontrol etmek, müdahale ve tepki faaliyetleri için rehberlik hizmeti sağlamak ve gelecekte meydana gelebilecek olayları engellemek amacıyla oluşturulmaktadırlar.

Ülkemizde Ulusal Bilgi Sistemleri Güvenlik Programı çerçevesinde başta kamu kurum ve kuruluşları olmak üzere ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamak ve kamu bilgi sistemlerinin güvenliğinin sağlanması ile ilgili etkin önlemler alınmasına ön ayak olmak amacıyla TÜBİTAK(UEKAE)

tarafından TR-BOME oluşturulmuştur. TR-BOME ulusal bir BOME'dir ve bu konuda ülkemizdeki siber güvenliğin sağlanması ile ilgili önemli bir açığı kapatmaktadır. Ayrıca ULAKNET bünyesinde bilgi güvenliği konusundaki bilincin artırılması, yaşanan bilgisayar güvenlik olayları sayısının azaltılması amacıyla Ulak-CSIRT kurulmuştur.

TR-BOME'nin ve Ulak-CSIRT'ın görev alanları incelendiğinde, her iki BOME'nin de kamu kurumlarına yönelik faaliyetlerde bulunduğu, özel sektörü ve bireysel kullanıcıları güvenlik açıkları konusunda bilgilendirmekten, güvenliklerini sağlamaktan uzak oldukları değerlendirilmektedir.

Bu kapsamda, ülkemizdeki mevcut İnternet kullanıcılarının, bireysel kullanıcıların siber tehditler, güvenlik açıkları ve kendi bilgilerinin güvenliğini nasıl sağlayabileceklerine ilişkin bilgileri elde edebilecekleri Ulusal bir BOME ihtiyacı bulunmaktadır. Bu çerçevede;

- T.C. Başbakanlık tarafından Ulusal bir BOME'nin oluşturulması ve özel sektörün de bilgi paylaşımı suretiyle söz konusu BOME'ye katkı sağlaması gerektiği değerlendirilmektedir. Belirtilen BOME kapsamında bireysel kullanıcıların ve KOBİ'lerin de güncel güvenlik açıkları konusunda bilgilendirilmesi, önlem almalarının sağlanmasının gerektiği değerlendirilmektedir.

- Özel sektör kuruluşlarının ve üniversitelerin de kendi bünyelerinde BOME'ler oluşturulması sağlanmalıdır. Bu çerçevede, BOME oluşturulması sürecinde ve sonrasında söz konusu kurumlara gerekli destek sağlanmalı ve ayrıca BOME'ler arasında işbirliği, bilgi paylaşımı sağlanmalıdır.

7.5 Uluslararası işbirliğine yönelik değerlendirme ve öneriler

Günümüzde siber tehlikeler ve saldırılar ulusal sınırları aşmış, uluslararası boyut kazanmıştır. Bu doğrultuda ülkemizde siber güvenliğin sağlanması için uluslararası işbirliğinin geliştirilmesinin gerektiği değerlendirilmektedir. Bu çerçevede;

- Siber güvenliğin sağlanması ile ilgili faaliyet gösteren BM, ITU, Avrupa Konseyi, AB, OECD, G8 gibi uluslararası kuruluşların çalışmaları takip edilmeli, uluslararası konferanslara, çalıştaylara katılım sağlanmalıdır.

- Dünyanın çeşitli bölgelerinden 200'den fazla hükümet, özel sektör, üniversite BOME'lerinin biraraya gelmesiyle oluşturulmuş olan ve olayların önlenmesi, olaylara hızlı bir şekilde müdahale edilmesi gibi alanlarda ekipler arasında bilgi paylaşımının teşvik edilmesini amaçlayan FIRST'e T.C. Başbakanlık tarafından oluşturulması önerilen BOME'nin ve mevcut BOME'lerin üye olmalarının sağlanması gerektiği değerlendirilmektedir.

- Siber suçların doğası gereği sadece ulusal kanunlarda yapılan düzenlemeler bu suçlarla mücadelede tek başına yeterli olmamaktadır. Siber suçlarla mücadele edebilmek için devletlerin ortak bir bilinçle hareket etmeleri gerekmektedir. Bu doğrultuda uluslararası alanda siber suçlar konusunda devletler nezdinde en kapsamlı uzlaşmayı sağlayan sözleşme olan ve ayrıca BİT ve ceza hukuku konularında ilk uluslararası belge olma niteliğini haiz olan Avrupa Konseyi Siber Suçlar Sözleşmesi imzalanıp onaylanmak suretiyle iç hukukumuz haline getirilmelidir. Nitekim Avrupa Konseyi Siber Suçlar Sözleşmesinin; siber suçlarla etkili biçimde mücadele edilmesi, siber suçların ulusal ve uluslararası düzeyde belirlenmesi, soruşturulması ve yargıya götürülmesinin kolaylaştırılması, uluslararası işbirliğinin sağlanması için gerekli düzenlemelerin

yapılmasını kolaylaştırması gibi nedenlerle siber suçlarla mücadelede fayda sağlayacağı değerlendirilmektedir.

- T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü tarafından 17 Şubat 2003 tarihli "Bilgi Sistem ve Ağları İçin Güvenlik Kültürü" konulu genelge ile bildirilmiş olan OECD'nin siber güvenlik kültürü ilkeleri ülkemizde halen uygulamaya geçirilmemiştir. Bu çerçevede, siber güvenlik stratejisi hazırlanırken söz konusu ilkelere de yer vermek suretiyle OECD'nin siber güvenlik kültürü ilkelerinin hayata geçirilmesi sağlanmış olmalıdır.

7.6 Siber güvenlik kültürü oluşturulmasına yönelik değerlendirme ve öneriler

Genç nüfusa sahip ve gelişmekte olan bir ülke olarak, ülkemizde siber güvenliğin sağlanabilmesinin en önemli unsurlarından birisi siber güvenlik kültürünün oluşturulmasının sağlanmasıdır. Bu bağlamda siber güvenlik kültürünün oluşturulması için aşağıda belirtilen hususlara yer verilmesinin gerektiği değerlendirilmektedir:

- Kamu-özel sektör işbirliği ile kampanyalar düzenlenmelidir

Ülkemizde bilişim STK'ları vasıtasıyla İnternet haftası etkinlikleri düzenlenmekle birlikte, bu konudaki çalışmaların kamunun da katılımının sağlanması suretiyle artırılması gerektiği değerlendirilmektedir. Bu çerçevede Ulaştırma Bakanlığı İnternet Kurulu ve Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı tarafından AB Komisyonu ile paralel olarak 23 Şubat 2010'da ilki düzenlenecek olan "Güvenli İnternet Günü" etkinliklerinin ilgili kamu kurumları, özel sektör, STK'lar ve üniversiteler işbirliği ile her yıl yapılması ve bu kapsamda konferanslar, paneller düzenlenmek suretiyle bireylerin siber güvenlik kültürünün oluşturulması sağlanmalıdır.

Ayrıca söz konusu etkinliklere medya desteğinin de alınmasının sağlanması suretiyle geniş kitlelere ulaştırılması sağlanmalıdır.

- Siber güvenlik kültürünün oluşturulmasında insan faktörü dikkate alınmalıdır.

Siber güvenliğin sağlanmasında ve güvenlik kültürünün oluşturulmasında en zayıf halka insandır. İnsan faktörü uygun ve yeterli seviyede güvenliğin sağlanmasında anahtar role sahiptir. Bu gerçekten hareketle, ülkemizde siber güvenliğin sağlanmasına yönelik çalışmalarda bireylere öncelik verilmeli ve bireylerin farkındalıklarının artırılması sağlanmalıdır. Bu konuda yapılacak araştırmalar desteklenmeli, BTK önderliğinde tezler yazılması, raporlar yayımlanması ve bu çalışmaların kamuoyu ile paylaşılması suretiyle geniş kitlelere ulaştırılması sağlanmalıdır.

- Çocuklara ve öğrencilere yönelik faaliyetler düzenlenmelidir

Günümüzde bilgisayar ve İnternet kullanım yaşı çocukluk yaşlarına kadar gerilemiştir ve ilköğretim öğrencileri dahi bilgisayar ve İnterneti etkin olarak kullanmaktadır. Öğrencilerin büyük bölümü okullarda BİT ile tanışmakta, İnternet ve oyun kültürü ile iç içe yaşamaktadırlar. Çocuklar ve öğrenciler İnterneti sosyal paylaşım sitelerinde vakit geçirmek, oyun oynamak amaçlı kullanmakta olduğundan, önlem alınmadığı takdirde kandırılması en kolay olan ve siber suçların işlenmesinde araç olarak kullanılabilecek olan hedef kitledir. Bu doğrultuda;

- Çocuklara kişisel bilgilerini İnternet ortamında tanımadıkları kimselerle paylaşmamaları, spamler, virüsler, solucanlar gibi siber tehditlere karşı bilinçli olmaları gibi temel güvenlik bilgileri öğretilmelidir. Bu amaçla konferanslar, paneller düzenlenmeli, eğitici televizyon, radyo programları hazırlanmalı, bilgisayar oyunları, videolar, kitaplar, broşürler gibi araçlarla çocukların farkındalıkları artırılmalıdır.

- Okullarda her yıl "bilgisayar ve İnternet güvenliği haftası" kutlanmalı ve bu hafta kapsamında öğrencilere İnternetten kaynaklanabilecek tehlikeler ve alınması gereken önlemlere ilişkin eğitici programlar sunulmalı, kişisel verilerini korumalarının önemi açıklanmalıdır. Bu suretle öğrencilerin farkındalıklarının artırılması sağlanmalıdır.

- Okulların ders müfredatına "bilgisayar ve internet güvenliği" dersi eklenmeli ve bu kapsamda öğrencilere güvenliklerini nasıl sağlayacaklarına ilişkin bilgiler verilmelidir. Ayrıca dersler kapsamında eğitici filmler, oyunlar ve videolar gibi yöntemlerle çocukların ve gençlerin farkındalıkları artırılmalıdır.

- Öğrencilerin ve çocukların güvenliklerini sağlamalarına yardımcı olacak eğitici bilgisayar oyunları hazırlanmalıdır.

- Bilinçlendirici İnternet siteleri oluşturulmalıdır.

Ülkemizde Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı ve MEB tarafından bilinçlendirici ve bilgilendirici İnternet siteleri oluşturulmuş olmakla birlikte, bu sitelerin sayısı artırılmalı ve kamu-özel sektör işbirliği ile bilgilendirici İnternet siteleri oluşturulmalıdır. Bu konuya özel sektörün, STK'ların ve üniversitelerin de müdahil olmaları ve içerik yönünden katkıda bulunmaları sağlanmalıdır.

- Medyanın desteği sağlanmalıdır

Siber güvenliğin sağlanmasına yönelik etkinliklere medya desteğinin de sağlanması suretiyle söz konusu etkinliklerin toplumun tüm kesimlerine ve bölgelerine ulaştırılmasının gerektiği değerlendirilmektedir. Bu şekilde toplumun tüm kesimlerinin siber güvenliğe ilişkin farkındalığının artırılması ve bilinçlendirilmesi sağlanmalıdır.

7.7. Ulusal siber güvenlik mevzuatının geliştirilmesine yönelik değerlendirme ve öneriler

Siber suçlar genellikle uluslararası boyutta işlenen olduğu için, suçlular hukuk sistemlerindeki boşluklardan yararlanarak tutuklanma ve/veya kovuşturmadan kaçabilmektedirler. Bu nedenle, siber suçlarla mücadele edebilmek için ülkelerin kendi hukuk sistemleri içerisinde ceza ve usul hukuklarında gerekli düzenlemeleri yaparak bu suçları işleyenleri cezasız bırakmamaları gerekmektedir. Bu çerçevede;

- Ülkemizde yıllardır gündemde olan, Adalet Bakanlığı tarafından hazırlanmış ve 22.4.2008 tarihi itibariyle Türkiye Büyük Millet Meclisine gönderilmiş olan Kişisel Verilerin Korunması Kanunu Tasarısının ve aynı şekilde yıllardır çalışmaları devam eden Ulusal Bilgi Güvenliği Kanunu Tasarısının bir an önce yasalaşmasının gerektiği değerlendirilmektedir.

- 5809 sayılı Elektronik Haberleşme Kanununun 6 ncı maddesinde düzenlenen BTK'nın görev ve yetkileri incelendiğinde söz konusu görev ve yetkilerin iletişim teknolojileri ve alt yapılarına yönelik olduğu, bilgi teknolojileri konusunda BTK'nın herhangi bir görev ve yetkisinin Kanunda tanımlı bulunmadığı değerlendirilmektedir. Bu doğrultuda 5809 sayılı Kanunun 6 ncı maddesine "Elektronik haberleşme şebekelerinin güvenliğinin sağlanmasına, kötücül yazılımlar ve tehditler marifetiyle elektronik haberleşme altyapısının kötüye kullanılmasının önlenmesine yönelik çalışmalar yapmak" şeklinde bir fıkra eklenmesinin uygun olacağı değerlendirilmektedir.

- Ülkemizin en fazla spam ve kötücül yazılım yayan ülkelerden birisi olduğu gerçeğinden hareketle, siber tehditlerle mücadele edebilmek

amacıyla söz konusu tehditleri düzenleyen ve müeyyideler getiren düzenlemelere yasal mevzuatta yer verilmesinin gerektiği değerlendirilmektedir.

- Ülkemizde siber suçların **soruşturulması ve yargılanması aşamasında** usul yönünden eksiklikler olduğu değerlendirilmektedir. Söz konusu eksikliklerin giderilmesi için adli bilişimle ilgili ayrıntılı hükümlerin hazırlanması ve yürürlüğe konulmasının gerektiği değerlendirilmektedir.

KAYNAKLAR

[1] Turhan, O., 2006, Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), Planlama Uzmanlığı Tezi, s.1,57,84,85,99,100,107,108, Ankara, Türkiye.

[2] BTK, Mayıs 2009, "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler" konulu Rapor, s. 3,42,48,49, Ankara, Türkiye.

[3] ITU, 2008, "ITU_T X.1205 Recommendation, Overview of Cybersecurity, Geneva, Switzerland.

[4] Bisson, J., Saint-Germain, R., The BS 7799 / ISO 17799 Standard For a Better Approach To Information Security.

[5] Commission of the European Communities, 2001, Network and Information Security: Proposal for a European Policy Approach, s.9, Brussels, Belgium.

[6] NewScientist, Carrington D.,Hecht J., 15 Ağustos 2003, http://www.newscientist.com/article/dn4062-worst-ever-power-cut-hits-north-america.html, 02.07.2009.

[7] Nıckolov, E., 7-8 Ekim 2008, Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure, Regional Cybersecurity Forum, Sofia, Bulgaria.

[8] Westby, J., 2004, International Guide To Cyber Security, s. 16,19,20,28, USA.

[9] OECD, Mayıs 2008, Protection of Critical Infrastructure' and The Role of Investment Policies Relating to National Security, s. 3,4,5.

[10] Wenger, A., Metzger, J., Dunn, M., International CIIP Handbook 2008/2009, s .33,36,41,54,59,430,431,453,467,470,489,493,512, Zurich, Switzerland.

[11] Nickolov, E.,2005, Criitical Information Infrastructure Protection: Analysis, Evaluation and Expectations, Information & Security An International Journal, Vol.17, 105-119, s.105,108.

[12] AfriNIC, http://meeting.afrinic.net/afrinic11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf,13.08.2009.

[13] The Washington Post, http://www.washingtonpost.com/wpdyn/content/article/2007/09/12/AR2007091200791.html, 02.04.2009.

[14] ComputerWeekly, Watts M., 13 Ağustos 2008, http://www.computerweekly.com/Articles/2008/08/13/231812/cyberattacksbecame- part-of-russia-georgia-war.htm, 02.04.2009.

[15] TIME, http://www.time.com/time/nation/article/0,8599,1098371,00.html 04.04.2009.

[16] PBS, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, 05.04.2009.

[17] "Fransız Ordusuna Sanal Saldırı", 10 Şubat 2009, http://www.timeturk.com/fransiz-ordusuna-sanal-saldiri–51458-haberi.html, 05.04.2009.

[18] Radikal, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalHaberDetay&ArticleID=944828&CategoryID=105 13 Temmuz 2009, 06.04.2009.

[19] BBC News, http://news.bbc.co.uk/2/hi/8455712.stm, 21.01.2010.

[20] ITU, Ocak 2008, Report on Best Practices For a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts,s. 19,20, Geneva, Switzerland.

[21] Handbook for Computer Security Incident Response Teams, April 2003, Carnegie Mellon Software Engineering Istitute, s.9,13,23,24,25,26.

[22] CERT/CC, http://www.cert.org/csirts/csirt_faq.html#1, 21.12.2009.

[23] CERT/CC, Creating and Managing Computer Security Incident Response Teams, s.14

[24] FIRST, http://www.first.org/, 02.05.2009.

[25] ENISA, 01 Mayıs 2009, Inventory of CERT activities in Europe.

[26] ENISA, Mayıs 2009, CERTs In Europe, Version 1.8.

[27] ENISA,http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe,10.05.2009.

[28] NATO, NCIRC, 15 Haziran 2004, 11th TF-CSIRT Meeting, Madrid, Spain.

[29] APCERT, http://www.apcert.org/, 15.05.2009.

[30] TERENA, http://www.terena.org/activities/tf-csirt/, 18.05.2009.

[31] EGC Group, http://www.egc-group.org/, 18.05.2009.

[32] OECD, 2002, OECD Guidelines For The Security of Information Systems and Networks: Towards a Culture of Security, http://www.oecd.org/dataoecd/16/22/15582260.pdf, 18.04.2009,19.05.2009.

[33] OECD, 16 Aralık 2005, The Promotion of a Culture of Security For Information Systems and Networks in OECD Countries,s.3.

[34] Schjolberg,S., Ghernaouti-Helie, S., 2009, A Global Protocol on Cybersecurity and Cybercrime,s.16.

[35] ITU, GCA A Framework for International Cooperation in Cybersecurity, s.5.

[36] ITU, 2008, Global Cybersecurity Agenda – Global Strategic Report, s.14, 15.

[37] Dülger, M.V.,2004, Bilişim Suçları, s. 70,212,231,322,323,327, Ankara,Türkiye.

[38] Berber, K,L., 2004,Adli Bilişim (Computer Forensics), s.39,Ankara,Türkiye.

[39] ITU-D, Ocak 2008, Draft Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, s. 27.

[40] ITU, Nisan 2009, Draft Understanding Cybercrime: A Guide for Developing Countries s.12,28,45.

[41] Sağıroğlu, Ş., Canbek, G., 2007, Kötücül ve Casus Yazılımlar:Kapsamlı Bir Araştırma, Gazi Üniv. Müh. Mim. Fak. Der. J. Fac. Eng. Arch. Gazi Univ. Cilt 22, No 1, 121-136,s.123,124,125,126,131.

[42] Akbank, http://www.akbank.com/duyurular-395.aspx#tbb, 08.12.2009.

[43] Computerworld, 19 Aralık 2008, Üsame İldar Özdemir, Phishing dolandırıcılarıtaktik değiştiriyor, http://www.computerworld.com.tr/phishing-dolandiricilari-taktik-degistiriyor-detay_2035.html, 18.12.2009.

[44] APWG, 2008,Phishing Activity Trends Report, http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf, 16.11.2009.

[45] Memiş, T., 18 Ağustos 2005, Hukuki Açıdan Kitlelere E-posta

Gönderilmesi, Saarbrücken Hukuki İnternet Projesi. www.jura.uni-sb.de/turkish/TMemis1.html, 18.12.2009.

[46] T.C. Ulaştırma Bakanlığı İnternet Üst Kurulu, 18 Ağustos 2005, İnternet Üst Kurulu SPAM Bildirgesi, Ankara, Türkiye.

[47] OECD, 19 Nisan 2006, Task Force On Spam, http://www.oecd.org/dataoecd/63/28/36494147.pdf,s. 6,17, 18.12.2009.

[48] Sophos, Temmuz 2009, Security Threat Report,s.4,9.

[49] Computerworld, 19 Ocak 2009, Üsame İldar Özdemir, Spamciler: "Obama başkanlığı reddedecek", http://www.computerworld.com.tr/spamciler-obama-baskanligi-reddedecek-detay_2268.html, 18.12.2009.

[50] IBM, Ocak 2009 X-Force 2008 Trend &Risk Report,s.50.

[51] OECD, 2009, Computer Viruses and Other Malicious Software, A Threat To the Internet Economy, s.21,69,227,229.

[52] Symantec, Nisan 2009, Global Internet Security Threat Report Trends for 2008,s.10,59.

[53] DEĞİRMENCİ, O.,2002 ,"Bilişim Suçları", Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, s.63,İstanbul,Türkiye.

[54] TÜBİTAK(UEKAE),http://www.tubitak.gov.tr/tubitak_content_files//basin/aciklama/01-29-uekae-virus.doc, 21.12.2009.

[55] Zetter, K., Aralık 2000, "Viruses, the Next Generation", PC Life,s.191-203.

[56] SpamLaws, http://www.spamlaws.com/what-is-adware.html, 21.12.2009.

[57] ITU, Ocak 2008, Botnet Mitigation Toolkit, s.5.

[58] Tüm Gazeteler, http://www.tumgazeteler.com/?a=4062763 , 16.11.2009.

[59] Cnetnews, http://news.cnet.com/8301-13577_3-10304633-36.html, 02.10.2009.

[60] BM, International Review of Criminal Policy – United Nations Manual on the Prevention and Control of the Computer- Related Crime, http://www.uncjin.org/Documents/irpc4344.pdf,s.13-16, 08.01.2010.

[61] Ergün, İ.,2008, Siber Suçların Cezalandırılması ve Türkiye'deki Durum s.29, 62,77,86,87,89,127, Ankara, Türkiye.

[62] Avrupa Konseyi, Convention on Cybercrime, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&

DF=&CL=ENG, 18.12.2009.

[63] Avrupa Konseyi, Convention on Cybercrime, Explanatory Report, http://conventions.coe.int/treaty/en/reports/html/185.htm, 18.12.2009.

[64] Yıldız, S., 2007, Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi,s.146, Ankara, Türkiye.

[65] Karagülmez, A., 2005, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,s.167,310, Ankara,Türkiye.

[66] OECD, Haziran 2008, OECD Policy Guidance on Online Identity Theft, s.2.

[67] UN, 22 Ocak 2001, Resolution adopted by the General Assembly, 55/63. Combating the Criminal Misuse of Information Technologies, http://www.itu.int/ITU D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, New York, USA,10.05.2009.

[68] UN, 23 Ocak 2002, Resolution adopted by the General Assembly, 56/121, Combating the Criminal Misuse of Information Technologies,http://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_resolution_56_121.pdf,10.05.2009.

[69] UN, 31 Ocak 2003, Resolution adopted by the General Assembly, 57/239. Creation of a Global Culture of Cybersecurity, http://www.oecd.org/dataoecd/53/60/37019786.pdf, New York, USA, 10.05.2009.

[70] UN, 30 Ocak 2004, Resolution adopted by the General Assembly, 58/199. Creation of a Global Culture of Cybersecurity and The Protection of CriticalInformationInfrastructureshttp://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, New York, USA,10.05.2009.

[71] UN ICT Task Force, http://www.unicttaskforce.org/, 06.06.2009.

[72] DPT, Ocak 2008, Dünya Bilgi Toplumu Zirvesi Nihai Dökümanları, Bilgi Toplumu Dairesi, Ankara, Türkiye.

[73] WSIS, 28 Temmuz 2006, Resolution 2006/46 Follow-up to the World Summit on the Information Society and review of the Commission on Science and TechnologyforDevelopmenthttp://www.un.org/docs/ecosoc/documents/2006/

resolutions/Resolution%202006-46.pdf, Geneva,Switzerland,18.05.2009.

[74] WSIS, 18 Kasım 2005, "Tunis Agenda for the Information Society", http://www.itu.int/wsis/docs2/tunis/off/6rev1.html,Geneva,Switzerland,19.05.2009.

[75] WSIS, 12 Aralık 2003, "Geneva Plan for Action". http://www.itu.int/wsis/docs/geneva/official/poa.html,19.05.2009.

[76] ITU, Overview of the GCA http://www.itu.int/osg/csd/cybersecurity/gca/overview/index.html, Geneva, Switzerland,22.05.2009.

[77] ITU, The High-Level Experts Group on Cybersecurity (HLEG), http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html, Geneva, Switzerland,22.05.2009.

[78] ITU, Cybersecurity Gateway, http://www.itu.int/cybersecurity/gateway/index.html, Geneva, Switzerland 23.05.2009.

[79] ITU, Nisan 2009, ITU National Cybersecurity/CIIP Self-Assessment Tool, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf, Geneva, Switzerland, 23.05.2009.

[80] Commission of the European Communities, 20 Ekim 2004,Critical Infrastructure Protection in the Fight against Terrorism, http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf, s.3,4,Brussels, Belgium,19.06.2009.

[81] Commission of the European Communities, 17 Kasım 2005, Green Paper On a European Programme For Critical Infrastructure Protection, http://eurlex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf , Brussels, Belgium, 19.06.2009.

[82] ENISA, About ENISA, http://www.enisa.europa.eu/about-enisa, Crete, Greece,25.06.2009.

[83] ENISA, Aralık 2006, Who is Who Directory on Network and Information Security, Version2.0, http://www.epractice.eu/files/media/media_944.pdf, Crete, Greece,25.06.2009.

[84] ENISA, ENISA Inventory of CERT Activities in Europe, Eylül 2007,

Version1.5,http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe, Crete, Greece,27.06.2009.

[85] ENISA, Work Programme 2009: "Build on Synergies – Achieve Impact." ,Crete, Greece,30.06.2009.

[86] EU, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf,05.07.2009.

[87] Berber, L.K., 2009, Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği,s.126, İstanbul, Türkiye,06.10.2009.

[88] EURLex,http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett,05.07.2009.

[89] EU Directive on Privacy Protection in the Electronic Communications Sector,October 2002, http://www.cdt.org/privacy/guide/protect/privacy-memo.pdf,14.06.2009.

[90] Official Journal of the European Union, 13 Nisan 2006, Directive 2006/24/EC of The European Parliament And of The Council, http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf, 13.07.2009.

[91] Official Journal of the European Union, 16 Mart 2005, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against informationsystems,http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF, 14.07.2009.

[92] OECD, What is the Working Party on Information Security and Privacy (WPISP),http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html,17.07.2009.

[93] OECD, Information, Computer and Communications Policy Committee (ICCP), http://www.oecd.org/dataoecd/18/39/37328586.pdf, 25.08.2009.

[94] OECD, 17-18 Haziran 2008, OECD Ministerial Meeting on the Future of the Internet Economy, OECD Recommendation of the Council on the Protection of Critical Information Infrastructures, http://www.oecd.org/dataoecd/1/13/40825404.pdf, Malicious Software (Malware): A Security Threat to the Internet

Economy,http://www.oecd.org/dataoecd/53/34/40724457.pdf, 18.07.2009.

[95] OECD, 19 Nisan 2006, Task Force on Spam, Report of the OECD Task Force on Spam: Antı-Spam Toolkit of Recommended Policies and Measures, http://www.oecd.org/dataoecd/63/28/36494147.pdf,19.07.2009.

[96] OECD, 13 Nisan 2006, OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam, http://www.oecd.org/document/27/0,3343,en_2649_22555297_37965659_1_1_1_1,00.htm,19.07.2009.

[97] OECD, Culture of Security, http://www.oecd.org/site/0,3407,en_21571361_36139259_1_1_1_1_1,00.html, 20.07.2009.

[98] OECD, 14-17 Ocak 2003, OECD-APEC Global Forum: Policy Frameworks for the Digital Economy, Honolulu, Hawaii, U.S., http://www.oecd.org/document/55/0,3343,en_2649_34223_2482679_1_1_1_1,00.html,22.07.2009.

[99] OECD, 13-14 Ekim 2003, OECD Global Forum on Information Systems and Network Security: Towards a Global Culture of Security,Hotel Bristol, Oslo, Norway, http://www.oecd.org/document/38/0,3343,en_2649_34487_16193702_1_1_1_1,00.html,23.07.2009.

[100]OECD, 5-6 Eylül 2005, OECD-APEC Workshop on Security of Information Systems and Networks, Seoul,http://www.oecd.org/document/25/0,3343,en_2649_34255_35481241_1_1_1_1,00.html,01.08.2009.

[101]OECD, 8 Mart 2006, OECD ICCP Workshop: "The Future of the Internet",Paris,http://www.oecd.org/document/5/0,2340,en_2649_34223_36169989_1_1_1_1,00.html,21.08.2009.

[102]OECD, 31 Ocak 2007, NSF/OECD Workshop "Social and Economic Factors Shaping the Future of the Internet, http://www.oecd.org/document/59/0,3343,en_2649_34223_37921851_1_1_1_1,00.html,20.08.2009.

[103]OECD,16-18 Haziran 2008, OECD Ministerial Meeting on the Future of

the Internet Economy, Seoul, Korea,http://www.biac.org/seoul_iccp_ministerial_2008.htm,15.08.2009.

[104]CouncilofEurope,http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 25.08.2009.

[105]Akdeniz Y., Mayıs 2008, An Advocacy Handbook for the Non Governmental Organisations,s.7-13.

[106]Council of Europe, 28.1.1981, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm,20.09.2009.

[107]Council of Europe, Status as of: 20/7/2009, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=20/07/2009&CL=ENG,20.07.2009.

[108]G8, Mayıs 15-17 2000, G8 Conference On Dialogue Between the Public Authorities and Private Sector On Security and Trust In Cyberspace Final Press Release, Paris, France http://www.g8.utoronto.ca/crime/paris2000.htm,22.09.2009.

[109]G8, Mayıs 11, 2004, Meeting of G8 Justice and Home Affairs Ministers, Washington,http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html,17.09.2009.

[110]G8, Temmuz 22, 2000, Okinawa Charter on Global Information Society, Okinawa,http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm,17.09.2009.

[111]G8, Mayıs 2003, G8 Principles for Protecting Critical Information Infrastructures(Adopted by the G8 Justice & Interior Ministers), http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf,17.09.2009.

[112]UN, General Assembly, 58/199. Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf,07.09.2009.

[113]Attorney-General's Department National Security Website,

http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection,29.09.2009.

[114]TISN, Infrastructure Assurance Advisory Groups, http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/About_the_TISNInfrastructure_Assurance_Advisory_Groups,30.09.2009.

[115]TISN, Welcome to the TISN website, http://www.tisn.gov.au/,30.09.2009.

[116]NCTC, 1 Ekim 2008, National Counter-Terrorism Plan, http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(3273BD3F76A7A5DEDAE36942A54D7D90)~National+CounterTerrorism+Plan++Alert+System+Changes+October+2008+PDF.PDF/$file/National+CounterTerrorism+Plan+-+Alert+System+Changes+October+2008+PDF.PDF,01.10.2009.

[117] TISN, Temmuz 2007, National Security Briefing Notes, E-Security National Agenda, http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf,01.10.2009.

[118]DSD, http://www.dsd.gov.au/,02.10.2009.

[119]AGIMO, http://www.finance.gov.au/agimo/index.html,02.10.2009.

[120]AGD,http://www.ag.gov.au/www/agd/agd.nsf/Page/About_the_Department,02.10.2009.

[121]AHTCC, http://www.ahtcc.gov.au/,03.10.2009.

[122]ACMA, How the ACMA is Fighting Spam, http://www.acma.gov.au/WEB/STANDARD/pc=PC_310308,03.10.2009.

[123]TISN, http://www.tisn.gov.au/,04.10.2009.

[124]ASIO, http://www.asio.gov.au/,05.10.2009.

[125]TISN,http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/About_Critical_InfrastructureFAQs,04.10.2009.

[126]DBCDE,http://www.dbcde.gov.au/policy_and_legislation/responsibilities_under_the_telecommunications_act/natural_disasters,04.10.2009.

[127]TISN, Infrastructure Assurance Advisory Groups Contacts, http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Home_InfrastructureAssuranceAdvisoryGroups(IAAGs)Contacts,05.10.2009.

[128]AusCERT, http://www.ag.gov.au/govcert,05.10.2009.

[129]AusCERT, 19 Mayıs 2009, Australian government announces new national

CERT arrangements for Australia on budget night, http://www.auscert.org.au/render.html?it=11012,04.10.2009.

[130]Onsecure, http://www.onsecure.gov.au/,10.10.2009.

[131]Staysmartonline, http://www.staysmartonline.gov.au/,10.10.2009.

[132] Cybersmart, http://www.cybersmart.gov.au/,10.10.2009.

[133] Avustralya, Privacy Act 1988, http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/F6CDB91759E0AF47CA2575F500041421/$file/Privacy1988_WD02HYP.doc, 12.10.2009.

[134]Avustralya, Electronic Transactions Act 1999, http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/F0E71528817DBCBDCA2573020000582B/$file/ElectronicTrans1999.doc, 12.10.2009.

[135]Avustralya, Cybercrime Act 2001, http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112.txt/cgibin/download.cgi/download/au/legis/cth/consol_act/ca2001112.rtf,12.10.2009.

[136]Avustralya, Spam Act 2003, http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366.txt/cgibin/download.cgi/download/au/legis/cth/consol_act/sa200366.rtf,09.10.2009.

[137]CPNI, http://www.cpni.gov.uk/,08.10.2009.

[138]CSIA,http://www.cabinetoffice.gov.uk/csia/national_ia_strategy.aspx,07.10.2009.

[139]A National Information AssuranceStrategy,2003,http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/nia_strategy.pdf,05.10.2009.

[140]CPNI, http://www.cpni.gov.uk/,05.10.2009.

[141]CCS,http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx, 06.10.2009.

[142]WARP, http://www.warp.gov.uk/,10.10.2009.

[143]GovCertUK, http://www.govcertuk.gov.uk/about_us.shtml,12.10.2009.

[144] Getsafeonline, http://www.getsafeonline.org/,13.10.2009.

[145]İngiltere, Computer Misuse Act

1990,http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm,14.10.2009.

[146]İngiltere, Telecommunications (Fraud) Act 1997,http://www.opsi.gov.uk/acts/acts1997/ukpga_19970004_en_1,14.10.2009.

[147] İngiltere, Data Protection Act 1998, http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980029_en_1,15.10.2009.

[148]USA Patriot Act, Title X, http://en.wikisource.org/wiki/USA_PATRIOT_Act/Title_X#Sec._1016._Critical_infrastructures_protection,18.10.2009.

[149]DHS, History: Who Became Part of the Department?, http://www.dhs.gov/xabout/history/editorial_0133.shtm,17.10.2009.

[150]National Strategy for Homeland Security, Ekim 2007,http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf,14.10.2009.

[151]The National Strategy to Secure Cyberspace, Şubat 2003, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf,14.10.2009.

[152]The National Strategy for Physical Protection of Critical Infrastructure and Key Assets, Şubat 2003, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf,16.10.2009.

[153]National Infrastructure Protection Plan, 2009, Partnering to enhance protection and resiliency, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf,18.10.2009.

[154]Isaccouncil.org,http://www.isaccouncil.org/,25.10.2009.

[155]IT-ISAC, https://www.it-isac.org/,25.10.2009.

[156]NCS, http://www.ncs.gov/ncc/,25.10.2009.

[157]Financial Services ISAC, http://www.fsisac.com/,25.10.2009.

[158] InfraGard, http://www.infragard.net/,26.10.2009.

[159] Staysafeonline,http://www.staysafeonline.info/ncsam,26.10.2009.

[160]US-CERT, http://www.us-cert.gov/,27.10.2009.

[161]US-CERT, National Cyber Alert System, http://www.us-

cert.gov/cas/alldocs.html,27.10.2009.

[162]Onguardonline, http://www.onguardonline.gov/,27.10.2009.

[163]Staysafeonline, http://www.staysafeonline.info/,27.10.2009.

[164]The USA Patriot Act, A Century Foundation Guide To The Issues, http://www.tcf.org/Publications/HomelandSecurity/USAPatAct.pdf,25.10.09.

[165]Homeland Security Act 2002, http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf,25.10,2009.

[166]ABD,The Privacy Act, 1974, http://www.usdoj.gov/opcl/privstat.htm, 26.10.2009.

[167]ABD,Federal Information Security Management Act 2002, http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act _of_2002,27.10.2009.

[168]Öztürk Ö., 2009, e-Postalarda Spam Sorunu ve Çözüm Önerileri, Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi, Ankara, Türkiye.

[169] Public Safety, http://www.publicsafety.gc.ca/prg/em/ci/about-eng.aspx,01.11.2009.

[170] Public Safety, http://www.publicsafety.gc.ca/index-eng.aspx,01.11.2009.

[171]Working Towards a National Strategy and Action Plan, Draft for Consultation, 2008,http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf,19.10.2009.

[172]CCIRC,http://www.publicsafety.gc.ca/prg/em/ccirc/indexeng.aspx,17.10.2009.

[173]GOC,http://www.publicsafety.gc.ca/prg/em/goc/index-eng.aspx,17.10.2009.

[174]Department of Justice, http://laws.justice.gc.ca/en/showdoc/cs/C46/boga:l_IXgb:s_335//en#anchorbo-ga:l_IX-gb:s_335,14.10.2009.

[175]Kanada, Emergency Management Act 2007, http://laws.justice.gc.ca/en/ShowTdm/cs/E-4.56/,28.10.2009.

[176]Kanada, Privacy Act, http://laws.justice.gc.ca/en/P-21/index.html,28.10.2009.

[177]Department of Justice, http://laws.justice.gc.ca/PDF/Statute/P/P-8.6.pdf,

13.01.2010.

[178]T.C. Başbakanlık, 17 Şubat 2003, Bilgi Sistem ve Ağları İçin Güvenlik Kültürü Konulu Genelge, http://www.oecd.org/dataoecd/37/34/36406374.pdf, 28.12.2009,02.11.2009.

[179]DPT, Temmuz 2006, Bilgi Toplumu Stratejisi, http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_BilgiToplumuStratejiBelgesi.pdf, 28.12.2009.

[180]DPT, Temmuz 2006, Bilgi Toplumu Stratejisi Eylem Planı, http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_EylemPlani.pdf,05.11.2009.

[181]TÜBİTAK (UEKAE), 5 Haziran 2009,Siber Savaş ve Sanal Ortam Güvenlik Politikası, Ünal Tatar.

[182]Adalet Bakanlığı, http://www.kgm.adalet.gov.tr/uck/uck.html, 30.12.2009

[183]TR-BOME,http://www.bilgiguvenligi.gov.tr/tr-bome hakkinda.html,28.12.2009.

[184] TÜBİTAK (UEKAE), 10.08.2009, Türkiye Bilgisayar Olayları Müdahale Ekibi Faaliyet Raporu 2007 – 2008 sürüm 1.00.

[185]TÜBİTAK(UEKAE), TR-BOME Faaliyet Raporu, 2007-2008.

[186]Soysal M., Karaarslan E., Eryol G., Yüce H., ULAK-CSIRT 1 Yaşında: Değerlendirmeler ve Yeni Hedefler.

[187]ULAK- CSIRT, http://csirt.ulakbim.gov.tr/,05.11.2009.

[188]BTK,Ekim 2009, http://www.btk.gov.tr/bt/sg/dokumanlar/uksgf.pdf,06.11.2009.

[189]ISC Turkey, http://www.iscturkey.org/, 08.01.2010.

[190]TİB, http://www.guvenliweb.org.tr/,11.11.2009.

[191]Güvenli İnternet Kullanımı İçin Tavsiyeler, http://www.guvenliweb.org.tr/files/file/e-kilavuz.swf, 17.11.2009.

[192]MEB, http://ihbarhatti.meb.gov.tr/,10.11.2009.

[193]Ulusal Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr/?Itemid=1,17.11.2009.

[194]Bilişim STK Platformu, http://internethaftasi.org.tr/hafta09/aktif_katilim_cagrisi.php, 17.11.2009.

[195] Türk Ceza Kanunu,26.09.2004,
http://www.tbmm.gov.tr/kanunlar/k5237.html, 17.11.2009.

[196]Adalet Bakanlığı, http://www.ceza-
bb.adalet.gov.tr/mevzuat/maddegerekce.doc, 18.11.2009.

[197]Elektronik Haberleşme Kanunu, 10 Kasım 2008,
http://www.tk.gov.tr/Duzenlemeler/Hukuki/Kanunlar/2008/elektronik_haberl
esme_kanunu.htm,18.11.2009.

[198]Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim
Başkanlığı,http://www.tib.gov.tr/node/76, 06.04.2010

[199]Elektronik İmza Kanunu, 23 Ocak 2004,
http://www.tk.gov.tr/eimza/eimza_yasasi.htm,11.11.2009.

[200]Elektronik Haberleşme Güvenliği Yönetmeliği, 20 Temmuz 2008,
http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/2008/elektronikhab
erlesmeguvenligi.pdf, 17.11.2009.

[201]Adalet Bakanlığı, http://www.kgm.adalet.gov.tr/gg/etic.pdf,11.01.2010.

EK AVRUPA KONSEYİ ÜYESİ ÜLKELERDE SÖZLEŞMENİN İMZALANMASI, ONAYLANMASI VE YÜRÜRLÜĞE GİRİŞ TARİHİNE İLİŞKİN DURUM

Ülkeler	**İmza Tarihi**	**Onay Tarihi**	**Yürürlüğe Giriş Tarihi**
Almanya	23/11/2001	09/03/2009	01/07/2009
Angola	-	-	-
Arnavutluk	23/11/2001	20/06/2002	01/07/2004
Avusturya	23/11/2001	-	-
Azerbaycan	30/06/2008	-	-
Belçika	23/11/2001		
Bosna-Hersek	09/02/2005	19/05/2006	01/09/2006
Bulgaristan	23/11/2001	07/04/2005	01/08/2005
Çek Cumhuriyeti	09/02/2005	-	-
Danimarka	22/04/2003	21/06/2005	01/10/2005
Ermenistan	23/11/2001	12/10/2006	01/02/2007
Eski Yugoslav Makedonya Cumhuriyeti	23/11/2001	15/09/2004	01/01/2005
Estonya	23/11/2001	12/05/2003	01/07/2004

Finlandiya	23/11/2001	24/05/2007	01/09/2007
Fransa	23/11/2001	10/01/2006	01/05/2006
Gürcistan	01/04/2008	-	-
Hırvatistan	23/11/2001	17/10/2002	01/07/2004
Hollanda	23/11/2001	16/11/2006	01/03/2007
İngiltere	23/11/2001	-	-
İrlanda	28/02/2002	-	-
İspanya	23/11/2001	-	-
İsveç	23/11/2001	-	-
İsviçre	23/11/2001	-	-
İtalya	23/11/2001	05/06/2008	01/10/2008
İzlanda	30/11/2001	29/01/2007	01/05/2007
Karadağ	07/04/2005	-	-
Kıbrıs	23/11/2001	19/01/2005	01/05/2005
Letonya	05/05/2004	14/02/2007	01/06/2007
Liechtenstein	17/11/2008	-	-
Litvanya	23/06/2003	18/03/2004	01/07/2004
Lüksemburg	28/01/2003	-	-
Macaristan	23/11/2001	04/12/2003	01/07/2004

Malta	17/01/2002	-	-
Moldavya	23/11/2001	12/05/2009	01/09/2009
Monako	-	-	-
Norveç	23/11/2001	30/06/2006	01/10/2006
Polonya	23/11/2001	-	-
Portekiz	23/11/2001	-	-
Romanya	23/11/2001	12/05/2004	01/09/2004
Rusya	-	-	-
San Marino	-	-	-
Sırbistan	07/04/2005	14/04/2009	01/08/2009
Slovakya	04/02/2005	08/01/2008	01/05/2008
Slovenya	24/07/2002	08/09/2004	01/01/2005
Türkiye	-	-	-
Ukrayna	23/11/2001	10/03/2006	01/07/2006
Yunanistan	23/11/2001	-	-

Kaynak [104]

ÖZGEÇMİŞ

MELTEM TURHAN

1978 yılında Samsun'da doğdu. 1995 yılında Samsun Anadolu Lisesi'nden mezun oldu. Aynı yıl Ankara Üniversitesi Hukuk Fakültesi bölümünü kazandı ve bu bölümden 2001 yılında mezun oldu. Aralık 2004-Şubat 2006 tarihleri arasında Türkiye İhracat ve Kredi Bankası A.Ş. (Türk Eximbank)'de uzman yardımcısı olarak çalıştı. 15 Şubat 2006 tarihinde Bilgi Teknolojileri ve İletişim Kurumunda uzman yardımcısı olarak görevine başladı. Bu süre zarfında, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı'nda siber suçlar ve alan adları ile ilgili alanlarda çalışmalarda bulunmuştur. Evli ve bir çocuk annesidir.