

T.C.
GENELKURMAY BAŐKANLIĐI
HARP AKADEMİLERİ KOMUTANLIĐI
STRATEJİK ARAŐTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĐÜ
YENİLEVENT/İSTANBUL

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŐMESİ
KAPSAMINDA TÜRKİYE’NİN GÜVENLİĐİ

ULUSLARARASI İLİŐKİLER
ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

Hazırlayan
Serdar HAVUZ

Tez Danıőmanı
Prof. Dr. Feridun YENİSEY

İSTANBUL - 2007

TEZ TANITIM FORMU

TEZİN TARİHİ : 07.06.2007

TEZİN TİPİ : Yüksek lisans tezi

TEZİN BAŞLIĞI : Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği

TEZİN YAPILDIĞI BİRİM: Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü

DAĞITIM LİSTESİ : Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü "Tez Hazırlama ve Değerlendirme Yönergesi"nde belirtilen yerlere

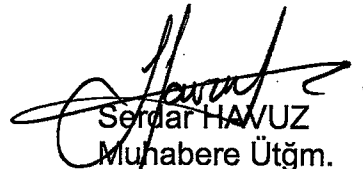
TEZİN ÖZETİ : Bu çalışmada; Avrupa Konseyi Siber Suçlar Sözleşmesi'nin, Türkiye'nin güvenliğine etkileri, Sözleşmenin siber suçlarla mücadeledeki etkinliği ulusal bilgi güvenliği kapsamında dikkate alınmak suretiyle incelenmiştir.

ANAHTAR KELİMELELER : Bilişim, Siber Suç, Siber Terör, Siber Suçlar Sözleşmesi, Ulusal Güvenlik, Bilgi Güvenliği.

SAYFA SAYISI: 239

GİZLİLİK DERECE: Tasnif Dışı

Bu tezin ihtiva ettiği hususlar şahsî görüşlerim olup; Türk Silâhlı Kuvvetlerinin resmî görüşünü yansıtmamaktadır.


Serdar HAVUZ
Muhabere Ütgm.
SAREN 2'nci Snf. Öğc.

**T.C.
GENELKURMAY BAŐKANLIĐI
HARP AKADEMİLERİ KOMUTANLIĐI
STRATEJİK ARAŐTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĐÜ
YENİLEVENT/İSTANBUL**

**AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŐMESİ
KAPSAMINDA TÜRKİYE’NİN GÜVENLİĐİ**

**ULUSLARARASI İLİŐKİLER ANA BİLİM DALI
YÜKSEK LİSANS TEZİ**

**Hazırlayan
Mu. Ütğm. Serdar HAVUZ**

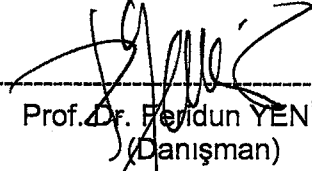
**Tez Danıőmanı
Prof. Dr. Feridun YENİSEY**

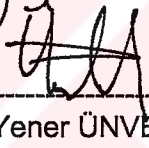
İSTANBUL - 2007

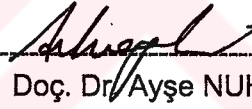
HARP AKADEMİLERİ KOMUTANLIĞI
STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Muhabere Ütğm. Serdar HAVUZ'un Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği konulu tez çalışması, jürimiz tarafından ULUSLARARASI İLİŞKİLER Ana Bilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan 
(E) Tugg. Atalay KOCATEPE

Üye 
Prof. Dr. Feridun YENİSEY
(Danışman)

Üye 
Doç. Dr. Yener ÜNVER

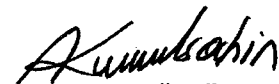
Üye 
Doç. Dr. Ayşe NUHOĞLU

Üye 
Doç. Dr. Mu. Bnb. Türker BAŞ

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

12/06/2007


Ahmet KÜÇÜKŞAHİN
Dr. P. Kur. Kd. Alb.
Str. Araş. Ens. Md.

TEŞEKKÜR

Tezimin planlama safhasından itibaren her aşamasında beni yönlendiren, konuya bilimsel bakış açısıyla farklı boyutlardan yaklaşmamı sağlayan, kendisinden aldığım dersler ve tez konusu haricinde de çok şey öğrendiğim, Prof. Dr. Feridun YENİSEY'e sonsuz teşekkürlerimi sunuyorum. Ayrıca yüksek lisans eğitimi almama imkân tanıyan Kara Kuvvetleri Komutanlığı'na; bugünlere gelmemizde emeği olan başta Enstitü Müdürümüz Dr. P. Kur. Kd. Alb. Ahmet KÜÇÜKŞAHİN'e ve tüm öğretim üyelerimize; tezin her safhasında yaptığı katkılardan dolayı Doç. Dr. Mu. Bnb. Türker BAŞ'a; ömür boyu sürmesini temenni ettiğim dostlukları için SAREN'de birlikte eğitim aldığım sınıf arkadaşlarıma ve tabii ki tez aşamasında bir yıl boyunca kendisine hemen hiç zaman ayıramadığım buna rağmen beni her zaman anlayışla karşılayan ve desteğini esirgemeyen sevgili eşime teşekkür etmeyi bir borç biliyorum.

Tez çalışmamdaki her türlü eksiklik ve yanlışlığın sorumluluğu bana aittir.

ÖZET

Bilişim ve iletişim teknolojisinde yaşanan devrim ve her ikisinin sonucu olan İnternet, siber uzay olarak adlandırılan yeni bir dünyanın kapılarını açmıştır. Siber uzay, insanlara büyük imkânlar ve kolaylıklar sunarken, yeni suç yöntemlerinin ve daha önce hiç karşılaşılmayan suç türlerinin ortaya çıkmasına da neden olmuştur. Siber uzayın sağladığı kolaylıklar sayesinde, suçlular gerçek kimliklerini gizleyerek, çok kısa sürede ve arkalarında neredeyse hiç iz bırakmadan suç işlemeyebilme kabiliyetine kavuşmuştur.

Bilgi toplumuna dönüşüm sürecinde, devletler de bilgi çağına ayak uydurmak zorunda kalarak, kurum ve hizmetlerini, vatandaşlarını ve etkileşimde olduğu özel sektör kuruluşları ile ilişkilerini siber uzaya taşımaktadır. Dolayısıyla, ulusal güvenliğe, siber uzaya taşınan ülkenin, siber uzaydaki güvenliği de eklenerek, ulusal bilgi ve bilişim sistemlerinin güvenliği, ulusal güvenliğin bir parametresi haline gelmektedir. Günümüzde giderek artan ekonomik suçlar, içerik suçları ve siber terör tehdidi göz önüne alındığında, siber suçların önlenmesi ve toplumun zararlı bilgidan korunması ulusal güvenlik açısından önem kazanmaktadır.

Ancak, İnternet teknolojisinden kaynaklanan teknik yetersizlikler, klasik ceza hukukunun suç tanımlarındaki eksiklikleri ve mevcut usul hukukunun soruşturma ve kovuşturmayaya yönelik yetersizlikleri, siber uzayda suçla mücadeleyi güçleştirmektedir. Buna bir de İnternet'in küresel yapısı nedeniyle, siber suçların sınır aşan niteliği ve uluslararası işbirliği ihtiyacı eklenince, mücadele daha da zorlaşmaktadır.

Avrupa Konseyi Siber Suçlar Sözleşmesi, ceza ve usul hukuku alanında getirdiği düzenlemeler ile siber suçlarla mücadelede etkin bir araç özelliği sergilemektedir. Sözleşme suçla mücadelede yaşanan yasal ve teknik güçlükleri en aza indirerek, kolluğun suçlular kadar hızlı tepki vermesi mümkün hale getirebilir. Sözleşmenin yargılama yetkisi, karşılıklı yardımlaşma ve suçluların iadesi gibi konulardaki hükümleri ise uluslararası işbirliği konusunda karşılaşılan güçlükleri büyük oranda ortadan kaldıracak niteliktedir. Ayrıca Sözleşme suçla mücadele ederken temel hak ve özgürlükler ile dengeyi de sağlamaktadır. Bununla birlikte, ISS'lere getirilen yükümlülüklerin yalnızca teknik imkânları ile sınırlandırılması, İnternet kafeler gibi İnternet'in toplu kullanıldığı mekânlara yönelik hükümlerin bulunmaması ve içerikle ilgili suçlar konusunda çekingen tavrı Sözleşmenin pratikte, teorideki kadar etkili olmayacağını ve zafiyetleri bulunduğunu göstermektedir.

Özellikle uluslararası işbirliği açısından hâlihazırda kendisinden beklenen faydayı göstermekten uzaktır.

Sözleşme'nin uluslararası işbirliği kapsamındaki maddeleri Türkiye için güvenlik açısından büyük bir önem taşımaktadır. Zira Türkiye'de "Devlet Sırrı Kanunu", "Kişisel Verilerin Korunması Hakkında Kanun" ve "Ulusal Bilgi Güvenliği Kanunu" gibi ulusal bilgi güvenliği konusunda büyük önem taşıyan hukuksal alt yapının henüz tesis edilmemiş olması, kimlerin, hangi bilgileri, hangi koşullar altında diğer ülke makamlarına verebileceği konusunda var olan belirsizlik nedeniyle, sınır ötesi erişime imkân sağlanmasının ve karşılıklı yardımlaşma gibi konular ulusal bilgi güvenliği açısından olumsuz sonuçlar doğurabilir. Buna ilaveten, Türkiye'nin henüz İnternet'in ulusal düzeyde denetimine yönelik yasal düzenlenmelerini tamamlamamış olması, uluslararası işbirliği çerçevesinde gelecek yardım taleplerine karşılık verilmesini güçleştirebilir.

Türkiye Sözleşmenin uluslararası işbirliği ve karşılıklı yardımlaşmada öncelik tanıdığı ve hazırlık sürecinde istifade edilen diğer Sözleşmelere zaten taraftır. Ayrıca Siber Suçlar Sözleşmesi ile karşılaştırıldığında, Türkiye'nin hâlihazırdaki hukuki mevzuatı büyük paralellik sergilemekte ve kısa sürede iç hukukta gerekli düzenlemeyi tamamlayabilecek durumdadır. Dolayısıyla öncelikle İnternet sükelerinin yükümlölüklerinin belirlenmesi, e-devlet sürecinde kurumlar arasındaki güvenlik standartlarını tesis edilmesi, kişisel verilerin korunması, devlet sırrı ve bilgi güvenliğine yönelik hâlihazırda taslak halde bulunan kanunları kabul edilmesi ve İnternet'in ulusal düzeyde denetimine yönelik düzenlenmelerin süratle gerçekleştirilmesi gerekmektedir. Bunlar tamamlandıktan sonra Sözleşmeye ve Ek Protokole zaman kaybedilmeden taraf olması uygun olacaktır.

ABSTRACT

The revolution in information technologies and its outcome Internet, opened the gates of a new world called cyberspace. While offering a great deal of easiness, and comfort, cyberspace has caused the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Using the opportunities provided by the cyberspace, cybercriminals took advantage of a complete anonymity, easiness of committing crime in a very short time and disappearing without almost any trace.

Following the information society revolution, states also has become obliged to adapt themselves to the information age and carried their institutions, services, citizens and related private sectors to the cyberspace. Therefore, security of the states in cyberspace has been added to national security, and securing the crucial national information systems has become a parameter of national security. Today, economic crimes, content crimes and cyber terrorism threat increases, and preventing cybercrimes and protecting society against harmful contents gains importance with respect to national security.

However, technical challenges of Internet technologies, absence of cybercrime definitions in existing criminal laws, and inappropriate investigative powers of existing procedural laws, make it hard for the law enforcement authorities to cope with cybercrimes. Given the cross-border nature of Internet, a concerted international effort is needed and it becomes harder to deal with cybercriminals.

The Council of Europe's Convention on Cybercrimes displays the feature of an efficient tool with regard to its regulations concerning substantial and procedural law issues. The Convention can minimize technical and legal difficulties and let the law enforcement authorities react as fast as cybercriminals. Articles of the Convention concerning jurisdiction, mutual assistance and extradition are able to eliminate the challenges to international cooperation. Moreover, while dealing with crime in cyberspace, the Convention balances between the needs of procedural powers and respects for human rights and fundamental freedoms. Nevertheless, limited ISP obligations depending on technical capabilities, absence of regulations concerning collective Internet usage such as Internet cafes, and hesitations at content related crimes weaken the effectiveness of the Convention in field, especially at international level.

With regard to Turkey's position, articles concerning international cooperation have a great importance. Since, Turkey has not adopted any detailed law concerning personal data protection, national information security or state secrets yet, and conditions and authorizations about information sharing with other states is not obviously stated in existing Turkish legislation, trans-border access and spontaneous information issues may be a threat to the national information security. Moreover, Turkey has not adopted a comprehensive domestic law governing Internet at national level, yet. Consequently, it may be difficult to respond to requests for mutual assistance.

Turkey has already signed and a party to the Council of Europe's conventions concerning mutual assistance and others mentioned in the Cybercrime Convention. Moreover, in comparison with the Cybercrime Convention, Turkey's existing legislation displays a parallelism, and Turkey is able to establish necessary regulations in domestic law in a very short time. Therefore, Turkey firstly should designate responsibilities of ISP's, information security standards among state institutions during e-government process, adopt draft laws about personal data protection, national information security and protecting state secrets, and take necessary steps to regulate Internet at domestic level immediately. Afterwards, Turkey should sign Convention and Additional Protocol as soon as possible.

İÇİNDEKİLER

	Sayfa
Özet	I
Abstract	III
İçindekiler	V
Şekiller Listesi	IX
Kısaltmalar Listesi	X
Ön Söz	XIII

BİRİNCİ BÖLÜM

GİRİŞ

1. ARAŞTIRMANIN PROBLEMİ	1
2. ARAŞTIRMANIN AMACI	9
3. ARAŞTIRMANIN ÖNEMİ	10
4. ARAŞTIRMANIN VARSAYIMLARI	11
5. ARAŞTIRMANIN KAPSAM VE SINIRLILIKLARI	12

İKİNCİ BÖLÜM

BİLİŞİM, SİBER SUÇ, SİBER TERÖR VE İLGİLİ KAVRAMLAR

1. BİLİŞİM KAVRAMI VE BİLİŞİM ALANININ TEMEL UNSURLARI	14
a. Bilişim Kavramı	14
b. İnternet'in Tanımı ve Tarihçesi	16
c. Siber Uzay Kavramı	20
2. SİBER SUÇ KAVRAMI	22
a. Siber Suç Kavramı	22
b. Siber Suç Olgusunun Tarihi Gelişimi	25
c. Siber Suçların İşlenme Yöntemleri	29
d. Siber Suçların Sınıflandırılması	37
3. SİBER TERÖR KAVRAMI	41
4. SİBER SUÇLARLA MÜCADELEDE KARŞILAŞILAN GÜÇLÜKLER ...	47
a. İnternet'in Çalışma Prensipleri	47
b. Teknik ve Yasal Güçlükler	49
c. Uluslararası İşbirliğindeki Güçlükler	53
d. Diğer Güçlükler	56

ÜÇÜNCÜ BÖLÜM

ULUSAL GÜVENLİK, BİLGİ GÜVENLİĞİ VE SİBER UZAYDA ULUSAL GÜVENLİĞE YÖNELİK TEHDİTLER

1.	GÜVENLİK KAVRAMI	58
	a. Ulusal Güvenlik Kavramı	60
	b. Genişletilmiş Güvenlik Anlayışı	62
2.	BİLİŞİM TEKNOLOJİLERİ VE ULUSAL BİLGİ GÜVENLİĞİ KAVRAMI	67
	a. Bilgi Güvenliği Kavramı	69
	b. Bilgi Güvenliğinin Bileşenleri	71
	c. Bilgi Güvenliğine Yönelik Tehditler	74
	d. Ulusal Bilgi Güvenliği Kavramı	76
	e. Kişisel Verilerin Güvenliği	77
	f. E-Devlet Dönüşüm Projesi ve Güvenlik	80
	(1) E-Devletin Tanımı	80
	(2) E-Devlet ve Bilgi Güvenliği Boyutu	81
3.	BİLGİ ÇAĞINDA İSTİHBARAT (SİBER İSTİHBARAT)	83
4.	SİBER TERÖR VE GÜVENLİK	87
5.	EKONOMİK BOYUT	96
6.	BİLGİ SAVAŞI (SİBER SAVAŞ)	102
7.	SOSYAL BOYUT	105
	a. İnternet'in birey ve aile üzerindeki etkisi	105
	b. Toplumsal etkisi	107
	(1) Pornografik içerik ve çocuk istismarı	108
	(2) İnternet ve Kumar Siteleri	109
	(3) Kin, nefret ve şiddetin desteklenmesi ve yayılması	112
8.	SİYASİ BOYUT	113
9.	HUKUKİ ANLAMDA ULUSAL GÜVENLİK VE TEMEL HAK VE ÖZGÜRLÜKLER	115
10.	SİBER SUÇLAR VE TÜRKİYE'DE ULUSAL BİLGİ GÜVENLİĞİ	130

DÖRDÜNCÜ BÖLÜM

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİNİN İNCELENMESİ VE İÇ HUKUKTA SİBER SUÇLAR

1.	AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ GENEL OLARAK	136
	a. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Hazırlanış Süreci.....	136

b. Sözleşme'nin Amaçları	138
c. Genel Hükümler ve Terimler	139
2. SÖZLEŞME KAPSAMINDA ULUSAL DÜZEYDE ALINACAK ÖNLEMLER	142
a. Maddi Ceza Hukuku	142
(1) Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar	142
(a) Madde 2-Yasadışı Erişim	142
(b) Madde 3-Yasadışı Araya Girme	145
(c) Madde 4-Verilere Müdahale	147
(d) Madde 5-Sistemlere Müdahale	149
(e) Madde 6-Cihazların Kötüye Kullanımı	150
(2) Bilgisayarlarla İlişkili Suçlar	152
(a) Madde 7-Bilgisayarla İlişkili Sahtecilik	152
(b) Madde 8-Bilgisayarla İlişkili Dolandırıcılık	153
(3) İçerikle İlgili Suçlar	156
(a) Madde 9-Çocuk Pornografisine İlişkin Suçlar	156
(b) Ek Protokol: Bilgisayar Sistemleri Aracılığıyla Irkçılık ve Yabancı Düşmanlığı	159
I. Irkçı ve Yabancı Düşmanlığı İçeren Malzemelerin Bilgisayar Sistemleri Aracılığıyla Yayılması	160
II. Irkçı ve Yabancı Düşmanlığı Motivasyonlu Tehdit	162
III. Irkçı ve Yabancı Düşmanlığı Motivasyonlu Aşağılama ...	162
IV. Soykırım ya da İnsanlığa Karşı Suçların İnkârı, Önemsizleştirilmesi, Onaylanması veya Haklı Görülmesi ...	162
(4) Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar	166
b. Usul Hukuku	168
(1) Genel Hükümler	168
(2) Madde 16- Depolanmış Bilgisayar Verilerinin Korunmasının Kolaylaştırılması	169
(3) Madde 17- Trafik Bilgilerinin Korunmasının ve Kısmen Açıklanmasının Kolaylaştırılması	172
(4) Madde 18- Üretim Talimatı	174
(5) Madde 19- Depolanmış Bilgisayar Verilerinin Aranması ve Bunlara El Konulması	176

(6) Madde 20-Trafik Bilgilerinin Gerçek Zamanlı Olarak	
Toplanması	181
(7) Madde 21-İçerikle İlgili Bilgilere Müdahale Edilmesi	184
(8) Madde 22-Yargı Yetkisi	190
3. ULUSLARARASI İŞBİRLİĞİ	193
a. Genel İlkeler	193
(1) Madde 24-İade	194
(2) Madde 25-Yardımlaşmaya İlişkin Genel İlkeler	197
(3) Madde 26-Anında İletilen Bilgiler	198
(4) Madde 27-Uluslararası Anlaşmaların Olmadığı Durumlarda	
Gelen Yardım Taleplerine İlişkin Usuller	199
(5) Madde 28-Kullanımda Gizlilik ve Sınırlama	202
b. Özel Hükümler	204
(1) Madde 29- Depolanmış Bilgisayar Verilerinin Korunmasının	
Kolaylaştırılması	204
(2) Madde 30-Korunan Trafik Bilgilerinin Açıklanması İşleminin	
Kolaylaştırılması	207
(3) Madde 31- Depolanmış Bilgisayar Verilerine Erişilmesine	
İlişkin Yardımlaşma	208
(4) Madde 32- Depolanmış Bilgisayar Verilerine İzinli Şekilde ya	
da Bu Verilerin Halka Açık Olduğu Durumlarda Sınır	
Ötesinden Erişim Sağlamak	208
(5) Madde 33-Trafik Bilgilerinin Gerçek Zamanlı Olarak	
Toplanması Konusunda Yardımlaşma	210
(6) Madde 34-İçerikle İlgili Verilere Müdahale Edilmesi Konusunda	
Yardımlaşma	211
(7) Madde 35-24/7 Ağı	211
BEŞİNCİ BÖLÜM	
SONUÇ VE DEĞERLENDİRME	
SONUÇ VE DEĞERLENDİRME	213
ALTINCI BÖLÜM	
KAYNAKÇA VE EKLER	
KAYNAKÇA	223

ŞEKİLLER

SAYFA

Şekil-1 : Uluslararası İlişkiler Boyutunda Güvenlik Yapılanması

66

Şekil-2 : Bilgi Güvenliği ve Karşı Tehdit Üçgeni

71



KISALTMALAR

AIHM	: Avrupa İnsan Hakları Mahkemesi
AIHS	: Avrupa İnsan Hakları Sözleşmesi
ARPA	: Advanced Research Projects Agency (İleri Düzey Araştırmalar Kurumu)
BBS	: Bulletin Board Service (Duyuru Tahtası Hizmeti)
CDPC	: European Committee on Crime Problems (Avrupa Suç Sorunları Komitesi)
CERN	: European Organization for Nuclear Research (Avrupa Nükleer Araştırma Örgütü)
CERT	: Computer Emergency Response Team (Bilgisayar Olayları Acil Müdahale Timi)
CIA	: Central Intelligence Agency (Merkezî Haber Alma Teşkilatı)
CMK	: Ceza Muhakemesi Kanunu
CSNET	: Computer Science Research Network (Bilgisayar Bilimi Araştırma Ağı)
DNS	: Domain Name Server (Alan Adı Sunucusu)
DoS	: Denial of Service (Hizmet İnkârı)
DDoS	: Distributed Denial of Service (Dağınık Hizmet İnkârı)
DTÖ	: Dünya Ticaret Örgütü
EMP	: Electromagnetic Pulse (Elektromanyetik Titreşim)
FBI	: Federal Bureau of Investigation (Federal Soruşturma Bürosu)
FSEK	: Fikir ve Sanat Eserleri Kanunu
FTP	: File Transfer Protokol (Dosya Transfer Protokolü)
HERF	: High Energy Radio Frequency (Yüksek Enerjili Radyofrekansı)
IANA	: Internet Assigned Numbers Authority (İnternet Tahsisli Sayılar Otoritesi)
IBM	: International Business Machines Corporation (Uluslararası İş Makinaları Şirketi)
IETF	: Internet Engineering Task Force (İnternet Mühendisliği Çalışma Gurubu)
IMP	: Interface Message Processor (Arayüz Mesaj İşlemcisi)

IP	: Internet Protocol (İnternet Protokolü)
ISOC	: Internet Society (İnternet Topluluğu)
İSS	: İnternet Servis Sağlayıcısı
MIT	: Massachusetts Institute of Tecnology (Massachusetts Teknoloji Enstitüsü)
MMS	: Multi Media Message (Çoklu Ortam Mesajı)
NASA	: National Aerospace Agency (Ulusal Uzay Ajansı)
NATO	: North Atlantic Treaty Organization (Kuzey Atlantik İttifakı Anlaşması)
NCP	: Network Control Protocol (Ağ Kontrol Protokolü)
NCSA	: National Center for Supercomputing Applications (Ulusal Süper Programlama Uygulama Merkezi)
NSA	: National Security Agency (Ulusal Güvenlik Teşkilatı)
NSF	: National Science Foundation (Ulusal Bilim Kurumu)
ODTÜ	: Orta Doğu Teknik Üniversitesi
PC	: Personal Computer (Kişisel Bilgisayar)
PC-CY	: Committee of Experts on Crime in Cyber-Space (Siber Uzay Suçları Uzmanları Komitesi)
PSVK	: Polis Vazife ve Selahiyet Kanunu
PTT	: Posta ve Telgraf Teşkilatı Genel Müdürlüğü
SCADA	: Supervisory Control and Data Acquisition (Veri Tabanlı Kontrol ve Gözetleme Sistemi)
SSCB	: Sovyet Sosyalist Cumhuriyetler Birliği
SRI	: Stanford Research Institute (Stanford Araştırma Enstitüsü)
STS	: Saldırı Tespit Sistemi
TCP	: Transmission Control Protocol (Transmisyon Kontrol Protokolü)
TCK	: Türk Ceza Kanunu
TEMPEST	: Transient Electromagnetic Pulse Standard (Elektromanyetik Salınım Standardı)
TRIPS	: Trade Related Aspects of Intellectual Property Rights (Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme)

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

UCLA : University of California at Los Angeles
(Los Angeles'ta Bulunan Kaliforniya Üniversitesi)

UCSB : University of California at Santa Barbara
(Santa Barbara'da Bulunan Kaliforniya Üniversitesi)

WIPO : World Intellectual Property Organization (Dünya Fikri Mülkiyet Teşkilatı)



ÖNSÖZ

Gün geçtikçe artan işlenme oranı ve büyüyen tehdit potansiyeli nedeniyle, siber suçlarla mücadele günümüzde hayati bir zorunluluk halini almaktadır. Bu zorunluluk, ülkeleri siber uzayın kendi yetkileri altındaki bölümünü kontrol etmeye; başka bir ifade ile İnternet'i kendi ülke sınırları içerisinde denetim altına almaya yöneltmektedir. Ancak, gerek İnternet'in ülke sınırlarından bağımsız olan doğası gereği, gerekse küreselleşme ile birlikte ülkeler arasında artan karşılıklı bağımlılık nedeniyle, siber suçlarla mücadelede uluslararası işbirliği ve karşılıklı yardımlaşma kaçınılmaz hale gelmektedir. Buna siber suçların ve özellikle siber terörün giderek artan biçimde ulusal güvenliği de tehdit eder hale gelmesi de eklenince ülkeler ve uluslararası örgütler işbirliği için yeni araçlar geliştirme ihtiyacı duymaktadır.

Siber suçlarla mücadelede uluslararası işbirliğine yönelik araçlardan birisi Avrupa Konseyi tarafından hazırlanan "Siber Suçlar Sözleşmesi"dir. Çalışmanın ana amacı, Avrupa Konseyi Siber Suçlar Sözleşmesini, TCK ve diğer ulusal mevzuat ile mukayeseli olarak inceleyerek, Türkiye'nin Sözleşme'ye mevcut hali ile taraf olması durumunda, siber suçlarla mücadelesini ne derecede kolaylaştıracağını ve üstleneceği yükümlülüklerin ulusal güvenlik üzerinde oluşturacağı olumlu ve olumsuz etkileri ortaya koymaktır.

Bu kapsamda, öncelikle siber suçlarla mücadelede karşılaşılan güçlükler ve değişik boyutları ile ulusal güvenliğe olan etkileri incelenerek, siber suçların ve siber uzayın kötü maksatlarla kullanımının günümüzde ulaştığı boyutu ile bir ulusal güvenlik problemi olarak görülebileceği ortaya konulmaya çalışılmıştır. Müteakiben Sözleşme maddeleri, ulusal mevzuat ile mukayeseli olarak incelenmek suretiyle, Sözleşmenin Türkiye'nin siber suçlarla mücadelede hâlihazırdaki zafiyetlerini gidermedeki etkinliğinin ve getirdiği yükümlülüklerin ulusal güvenlik açısından değerlendirildiğinde varsa olumsuz etkilerinin ortaya konulması amaçlanmıştır.

Çalışmada çok sayıda yerli ve yabancı kitap, makale, tez, düşünce kuruluşu yayınları ve incelemeden faydalanılmıştır. Son bölümünde ise ağırlıklı olarak Sözleşme maddelerinin nasıl yorumlanacağını belirleyen açıklayıcı rapordan istifade edilmiştir. Çalışmanın Sözleşmeye ulusal güvenlik bakış açısıyla yaklaşması bakımından getirdiği yenilikle, Sözleşmeye taraf olma konusunda ve ulusal mevzuatın düzenlenmesi konusunda karar alıcı konumundakiler ile konu ile ilgilenenlere faydalı olmasını umut ediyoruz.

BİRİNCİ BÖLÜM

GİRİŞ

1. ARAŞTIRMANIN PROBLEMİ

İnsanlık tarihine bakıldığında, teknolojik gelişmenin giderek artan bir ivme kazandığı ve özellikle 20. yüzyılda bilgisayar ve iletişim teknolojisinde yaşanan devrimin bunda önemli bir rol oynadığı söylenebilir. Bilgisayarın icadından günümüze kadar, insanoğlu kademeli olarak bilgisayar sistemlerine bağımlı hale gelmiştir. Bilgisayarlar başlangıçta büyük, hantal, kullanımı özel ihtisas gerektiren, sadece belli sektörlerle hitap eden, pahalı ve karmaşık makineler iken, gelişen teknoloji ile birlikte, bir yandan küçülmüş ve ucuzlamış, diğer yandan kullanım alanları artarak, herkesin elde edebileceği bir ihtiyaç haline gelmiştir. Bilgisayarlar yalnızca masaüstü ya da dizüstü bilgisayarlar olarak değil, karmaşık ve rutin birçok işi, insan kontrolü olmadan gerçekleştirebilen sibernetik sistemler aracılığıyla da insanoğlunu kendisine bağımlı hale getirmiştir. İnsanoğlu yarattığı bilgisayarlara görevlerinin bir kısmını devrederek, hayatı kolaylaştırma yoluna gitmiştir.

Gelişen teknoloji bir yandan insanlara yeni imkânlar ve kolaylıklar sunarken, kötü niyetli olan insanlara da yeni kapılar açmış ve suç işlemek için yeni fırsatlar yaratmıştır. Bir yandan bilinen suç türlerini işlemek için yeni yöntemler ortaya çıkarken, diğer yandan daha önce hiç karşılaşılmayan yeni suç türleri ve alanları oluşmuş, bilinen klasik suç türlerine yenileri eklenmiştir. Günümüzdeki anlamıyla siber suçların ortaya çıkışı, bilgisayarların ve bilgisayar ağlarının icadından çok daha öncesine, telefon altyapısının tesis edilmeye başlandığı yıllara rastlamakla birlikte, asıl artış ve gelişme İnternet döneminde olmuştur.

İletişim teknolojisinde kaydedilen gelişme ve özellikle İnternet sayesinde, bilgisayarlara olan talep ve İnternet kullanımındaki artış benzeri görülmemiş toplumsal değişimlere yol açmıştır. Kişisel bilgisayarları günlük hayatın vazgeçilmez bir parçası haline getiren asıl gelişme, şüphesiz İnternet olmuştur. İnternet, iyi ya da kötü tüm insanlara daha önce sahip olmadıkları bir özgürlüğün kapısını açmış, ülke sınırlarının, mesafelerin, mekânın ve zamanın kısıtlamalarından sıyrılmış, her türlü bilgiye erişilebilen yeni bir dünya yaratmıştır. Fiziksel olarak, kablolar, santraller, uydular, radyolinkler, bilgisayarlar, modemler, yönlendiriciler gibi teknik donanımdan, sanal olarak sohbet odaları, kütüphaneler, bankalar ve mağazalar gibi hizmetlerden oluşan bu dünya “siber uzay” olarak tanımlanmıştır.

Siber uzayın karanlık yüzünü oluşturan siber suçlarının gelişimi de bilişim teknolojisinin gelişimi ile paralel bir seyir izlemiştir. Siber suçlar bilişim sistemlerinin sağladığı yeni imkânlarla göre evrim geçirerek, ilave olan her yenilikle birlikte başka bir formda ortaya çıkmıştır. Başlangıçta basit bilgisayar ve ağ suçları olarak görülen siber suçlar, İnternet'in ortaya çıkışı ile birlikte yeni bir boyut kazanmıştır. Artık ağın ulaştığı her alanda suç işleme imkânı doğmuştur. Başlangıçta pek de kötü niyetli olmayan siber suçlulara çoğu kişi tarafından önem verilmemiş, hatta sempati ile karşılanmışlardır. Kullanıcı sayısının az olması ve henüz bilgisayarların günlük hayatın önemli bir bileşeni haline gelmemiş olması, bu suçları önemsiz kılmıştır.

İnternet bilişim suçlarının artışına hem bilgisayar kullanımında yarattığı artış, hem de siber uzaya taşınan hizmetlerde yarattığı çeşitlilik ile katkıda bulunmuştur. Sürekli artan İnternet kullanıcıları sayesinde gün geçtikçe büyüyen siber uzay ile gerçek dünya, her geçen gün biraz daha iç içe geçmiş ve gerçek dünyaya ait birçok kavramın önüne siber kelimesi eklenerek "siber uzay", "siber alışveriş", "siber aşk", "siber terörizm" gibi sanal kavramlar yaratılmıştır. Ancak, siber uzayın getirdiği sınırsız özgürlük ortamında yaratılan sanal kavramlar, zamanla gerçek dünyayı, kişileri ve ülkeleri etkileyecek sonuçlar doğurmaya başlamıştır. İnsanlık adeta iki ayrı dünyada yaşar hale gelmiştir. Bir tarafta ülke sınırlarının, ulusal egemenliklerin, mesafelerin, ahlaki ve toplumsal kuralların, hukuki düzenlemelerin, ölçülü özgürlüklerin ve hakların bulunduğu, herkesin belirli bir kimlikle tanımlandığı gerçek dünya, diğer tarafta ise hem fiziksel, hem de özgürlük anlamında sınırların, hukuksal düzenleme ve güvenlik tedbirinin bulunmadığı, kimliklerin gizlenebildiği siber uzay yer almıştır. Dolayısıyla, siber uzay suçlular için karşı konulamaz bir cazibe alanı haline gelmiştir. İnternet'in sağladığı sınırsız özgürlüğün farkına varan suçlular görünmeden, yakalanmadan ve hiçbir riske girmeden bu özgürlüğün keyfini çıkarmaya başlamıştır. İnternet yalnızca suçlular için yeni imkânlar sunmakla kalmamış, suç işlemeye eğilimli insanları da sağladığı kolaylık ve gizlilik sayesinde suça yöneltmiştir.

Başlangıçta kısıtlı işlevlere sahip olan, yalnızca üniversiteler ve bilimsel araştırma kuruluşları tarafından kullanılan İnternet üzerinden işlenen suçlar, bilgisayarlara yetkisiz erişim, verilere müdahale, kötü kodlar içeren yazılımlar yayma gibi nispeten basit suçlar olmuştur. Ancak İnternet'in ticari potansiyelinin fark edilmesi ve ekonomik hayatla bütünleşmesi üzerine bu suçlar yeni nitelikler kazanmıştır. Bilişim teknolojileri ve İnternet sayesinde insanlık sanayi toplumundan, bilginin üretiminin, iletiminin ve tüketiminin hızlandığı, insanların yaşamlarını

İlgilendiren çeşitli bilgilere kolayca erişebilmelerine ve dolayısıyla da kendilerini geliştirebilmelerine olanak sağlayan bilgi toplumuna evrilmeye başlamıştır. İnternet'in ekonomik ve ticari hayatın bir parçası haline gelmesi, küreselleşmenin etkisi ile birlikte bankacılık işlemlerinin, para transferlerinin, alım satımların, ticari işlemlerin İnternet aracılığıyla yapılmasına neden olmuştur. Bu işlemler, kişisel verilerin ve ticari değeri olan bilgilerin artan bir şekilde elektronik ortamda depolanmasını gerektirmiştir. Ticari sır içeren özel haberleşmeler İnternet üzerinden yapılmaya başlamıştır. Bilişim teknolojileri ve İnternet, bilginin elektronik olarak depolanması, işlenmesi ve süratle iletilmesi sağlanmış, elektronik ortamda yaratılan, aktarılan ve kullanılan bilginin miktarı da buna bağlı olarak artmıştır. Bilgi alınan, satılan, işlenen, depolanan bir değere dönüşmüştür. Ancak, geçmişte de değerli olan bilginin, elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması maruz kaldığı tehdidi artırmış ve bilgi güvenliği kavramına yeni bir boyut kazandırmıştır.

1990 yılından sonra ise mali kazanç sağlamaya yönelik, İnternet sayfası yönlendirme, kişisel verilerin, kredi kartı ya da banka hesap bilgilerinin çeşitli yollarla ele geçirilmesi suretiyle işlenen dolandırıcılık ve sahtekârlık suçları ortaya çıkmış ve giderek artış göstermiştir. Bu dönemde suç mağdurlarının daha çok bireyler olması ve hükümetlerin bilişim sistemlerine bağımlılığının günümüze kıyasla nispeten az olması, siber suçların ulusal güvenlik açısından önemli bir tehdit olarak algılanmamasına neden olmuştur. Bunun bir diğer nedeni de geleneksel güvenlik anlayışının, ulus devletin bağımsızlığının ve toprak bütünlüğünün korunmasını amaçlayan, askeri tehdit algılamasına dayanan yapısı olmuştur. Ancak, İnternet'in bugünkü şeklini aldığı dönem, aynı zamanda Soğuk Savaş'ın son erdiği ve güvenlik algılamalarının değiştiği dönem olmuştur. Soğuk Savaş sonrasında küreselleşmenin yarattığı dinamik ortam içinde ulusal güvenliğe yönelik tehditler farklılaşmış, terörizm, ayrılıkçı hareketler, etnik ve dinî çatışmalar, kitle imha silâhlarının yayılması, uluslararası organize suçlar ve siber terörizm gibi tehdit parametreleri ortaya çıkmış ve güvenlik algılamalarını değiştirmiştir.

Bilgi toplumuna dönüşüm sürecinde, devletin kaçınılmaz bir biçimde bilgi çağına ayak uydurmak zorunda kalması, kendi kurum ve hizmetleri ile birlikte vatandaşlarını ve etkileşim içerisinde bulunduğu özel sektör kuruluşlarını da siber uzaya taşımasına neden olmuştur. Diğer bir ifadeyle, devletin mevcut bilgi alt yapısı ve bilgi bankası güvenli olmayan İnternet ortamına taşınmıştır. Bir yandan devletin günlük hayatın devamı için bilgiye ve bilişim sistemlerine giderek artan bağımlılığı,

diğer taraftan bilginin ve bilişim sistemlerinin kötü niyetli saldırılara, terörist faaliyetlerine ve doğal afetlere karşı artan hassasiyeti, yeni bir tehdit algılamasının ve dolayısıyla yeni bir güvenlik ihtiyacının doğmasına neden olmuştur. Ulusal güvenliğe, siber uzaya taşınan ülkenin, siber uzaydaki güvenliği de eklenerek, ulusal bilgi ve bilişim sistemlerinin güvenliği, ulusal güvenliğin bir parametresi haline gelmiştir.

Devletlerin de siber uzayın bir aktörü haline gelmesi, siber suçların etki alanının genişlemesine ve yarattığı tehdit potansiyelinin artmasına neden olmaktadır. Bu durum, siber suçların daha ciddi bir şekilde ele alınmasını zorunlu hale getirmektedir. Siber suçlar karşısında, devletin güvenliğini tehlikeye sokabilecek her türlü bilginin ve bilişim sistemlerinin korunması, bilgi edinme hakkının kullanılmasına yönelik tehditlerin ortadan kaldırılması önem kazanmaktadır. Ulusal güvenliğin değişen tanımı kapsamında bilgi güvenliği bir ülkedeki her türlü bilginin (bilimsel, teknolojik, ekonomik, vs.) dış tehditlere karşı korunması olarak ifade edilmektedir. Günümüzde tehdidin kaynakları bireylerden, karmaşık ulusal organizasyonlara kadar geniş bir yelpazede ortaya çıkmakta, yetkisiz kullanıcılar, muhbirler, teröristler, uyuşturucu kaçakçıları ve toplumsal eylemciler gibi devlet dışı guruplar, dış istihbarat örgütleri ve yabancı ülke silahlı kuvvetleri ya da siyasi hasımlar olabilmektedir. Siber suçlar, devletler söz konusu olduğunda, siber istihbarat, ekonomik savaş ve siber savaş gibi daha ciddi boyutlarda ortaya çıkmaktadır.

Ülkelerin ekonomik refah ve istikrarının ulusal güvenliğin önemli bir bileşeni haline gelmesi ve küreselleşmenin getirdiği dünya genelinde rekabet edebilir olma ihtiyacı, devletlerin güvenliklerini tehlikeye sokabilecek bilgileri, sadece askerî bilgiler, savunma planları gibi gizli bilgilerle sınırlı olmaktan çıkararak, ekonomik ve ticari sırların da bu kategoriye dahil edilmesine neden olmaktadır. Ulusal bilgi güvenliğinden bahsedilirken, sadece devletin ulusal çıkarları doğrultusunda oluşturulan bilgiler değil; daha geniş anlamda özel sektörü ya da kişileri ilgilendiren her türlü ticari bilginin korunması da anlaşılmaktadır. Şirketlerin maliyetleri zaman zaman milyon dolarları bulan bilgileri, ihaleleri, gizli görüşmeleri, anlaşmaları, patenti alınmamış buluşları tehditle karşılaşmaktadır. Endüstri ve ekonomi casusluğu patenti alınmamış buluşların çalınması ya da uluslararası ihalelerin kaybedilmesi gibi ciddi sonuçlara varabilmektedir. İnternet'in ekonomik hayatın ayrılmaz bir parçası haline gelmesi, İnternet üzerinden yapılan mali işlemlerin ve elektronik ticaret hacminin artması, hem ülke bazında hem de küresel boyutta ekonomiyi siber

suçlar karşısında kırılgan bir hale getirmiştir. Bir yandan siber suçlar nedeniyle oluşan ekonomik kayıplar, diğer yandan bu suçların önlenmesi maksadıyla alınan güvenlik tedbirleri ülke ekonomilerine büyük maliyetler getirmektedir.

Siber suçların geçirdiği en uç evrim ise, 11 Eylül saldırıları sonrasında oluşan korku ve panik ortamıyla birlikte telaffuz edilmeye başlanan “siber terör” tehdididir. Teröristlerin kritik altyapı tesislerine yönelik olarak, bilgisayar sistemlerini kullanarak gerçekleştirebilecekleri saldırılar neticesinde, klasik bir terör eylemindekine benzer şekilde toplumda korku ve dehşet yaratabilecekleri öngörülmektedir. Siber teröristlerin bilişim sistemlerini kullanarak baraj kapaklarını açabilecekleri, hava trafik kontrol sistemlerini ele geçirerek, uçak kazalarına neden olabilecekleri ya da gıda fabrikalarının bilgisayar sistemlerini ele geçirerek, gıda karışım oranlarını değiştirebilecekleri ve böylece kitlesel ölümlere yol açabilecekleri iddia edilmektedir. Terör örgütlerince uygulandığında siber terör, devletler tarafından uygulandığında siber savaş kapsamında değerlendirilen, kritik altyapı tesislerine yönelik bu tarz saldırıların bir ulusun yeme, içme, hareket etme ya da yaşamasını engelleyebileceği öngörülmektedir. Bilişim sistemlerine bağımlılığı yüksek olan gelişmiş ülkeler, bugüne kadar resmi kayıtlara geçmiş tek bir siber terörizm örneği bulunmamasına rağmen, kritik altyapı tesislerinin siber terörden korunması için tedbir almaya başlamıştır.

Siber suçların bir diğer boyutu ise bilişim ve İnternet teknolojisi sayesinde düşünce ve fikirlerin dünya genelinde hızlı bir şekilde yayılması ile şekillenmiştir. Bilgi toplumunun özünde her türlü bilgiye serbestçe erişebilmesini ve haber alma özgürlüğünü ifade eden bilgi edinme hakkı bulunmaktadır. Ancak bilgi edinme hakkı, düşünce ve fikirlerin özgürce yayılması ile doğrudan ilişkilidir. Düşünce ve fikirlerin özgürce yayılmadığı yerde bilgi edinme hakkından söz etmek de mümkün değildir. İnternet sayesinde her türlü bilgiye kolayca erişilebilmesi, düşünce ve fikirlerin paylaşılması ve yayılması kolaylaşmıştır. Bununla birlikte her türlü fikrin özgürce yayılması her zaman olumlu sonuçlar doğurmamış, toplumun huzur ve refahının bozulması ihtimalini de beraberinde getirmiştir. Hakaret, aşağılama, ayrımcılık ve tehdit içeren fikirlerin İnternet sayesinde serbestçe yayılması, bu özgürlük içerisinde kabul edilmemektedir. Özellikle ulus devlet yapısını, devlet rejimini ve toplumsal barışı zedeleyen fikirlerin hiçbir kısıtlama olmadan yayılması, ülkeler için bir ulusal güvenlik problemi halini almaktadır. Bölücü ve yıkıcı unsurlar, aşırı uç gruplar İnternet’ten bir propaganda ve siyasi baskı aracı olarak istifade etmeye başlamıştır. Bu nedenle, ulusal güvenlik çerçevesinde bilgi edinme, düşünce ve fikirlerin

yayılması haklarının İnternet ortamında da ölçülü bir biçimde kısıtlaması ihtiyacı doğmuştur.

Buna ilave olarak İnternet ortamı, giderek artan oranda kötü maksatlarla kullanılmaya başlamıştır. Kumar siteleri, pornografik içerikli yayınlar ve özellikle çocuk pornografisi gibi toplumsal yapıyı ve genel ahlâkı olumsuz yönde etkileyebilecek zararlı, yanıltıcı ve suça yöneltici içerikten toplumun korunması ve İnternet üzerinde daha fazla denetim ihtiyacı ortaya çıkmıştır. Bu durum gerçek hayatta sahip olamadıkları sınırsız özgürlüğün tadını alan insanlarda, bu özgürlüğü kaybetme korkusu yaratmıştır. Ancak, zararlı içerik konusunda alınacak tedbirler devletin, toplumun ve bilginin niteliklerine göre değişiklik göstermekle birlikte, her türlü toplum için, bilgi bir toplumsal değer ve yerine göre bir toplumsal tehlike olabileceğinden, toplumun kısaca zararlı içerik olarak tanımlanabilecek olan bilgidan korunması, ulusal bilgi güvenliği politikası içerisinde büyük bir önem taşımaktadır.

Siber suçların bireyden ulusa kadar büyük bir tehdit halini aldığı ve artık ulusal güvenlikle ilgili önemli endişelere neden olduğu şüphe götürmeyecek bir gerçektir. Bununla birlikte asıl problem siber suçların yeni bir kavram olması ve mevcut hukuki kurallar ve toplumsal normların bu suçlar karşısında yetersiz kalmasından kaynaklanmaktadır. Sınırlarla bölünmüş yeryüzünde, sınır tanımayan bir olguyu kontrol etmek mevcut araçlarla neredeyse imkânsız gibi görünmektedir. Gün geçtikçe artan İnternet kullanımı ve siber uzaya taşınan hizmetlerin çeşitliliği neticesinde ortaya çıkan yeni suçlarla mücadelede, ceza hukukunun klasik düzenleme ve uygulamaları kimi zaman yetersiz kalmaktadır.

Türkiye’de bilişim suçlarının engellenmesi konusunda, 2005 yılında kabul edilen TCK ile önemli adımlar atılmıştır. Bu kapsamda siber suçların bir kısmı, bilişim alanında suçlar başlığı altında TCK’nın 243 ilâ 245. maddelerinde düzenlenmiştir. Ancak daha önce de belirtildiği gibi ulusal sınırlar içerisinde yapılan yasal düzenlemeler, siber suçlar söz konusu olduğunda yeterli olmamakta ve uluslararası işbirliği bu anlamda büyük önem taşımaktadır. Günümüzde siber suçlarla mücadelede en kapsamlı uluslararası sözleşme olarak değerlendirilen ve Türkiye’nin de üyesi olduğu Avrupa Konseyi tarafından hazırlanan, Siber Suçlar Sözleşmesi, Türkiye’nin önünde iyi bir alternatif olarak durmaktadır.

Bu çalışmada Avrupa Konseyi Siber Suçlar Sözleşmesinin kabulünün, Türkiye’nin güvenliğine olan etkileri ortaya konmaya çalışılmaktadır. Bu kapsamda cevap aranacak iki soru ortaya çıkmaktadır. Birincisi Sözleşmenin ulusal güvenlik

açısından bir tehdit olarak değerlendirilen siber suçlarla mücadelede etkili bir araç olup olmadığı, diğer bir ifade ile Türkiye'nin siber suçlarla mücadelede hâlihazırda var olan zafiyetlerini ne derecede giderebileceği sorusudur. İkincisi ise Sözleşmenin, özellikle uluslararası işbirliği hükümlerin çerçevesinde, kendisinin başlı başına ulusal güvenlik açısından bir tehdit teşkil edip etmediği sorusudur.

Sözleşmenin siber suçlarla mücadelede etkili bir araç olabilmesi için öncelikle hâlihazırda hukuksal çerçevede var olan çeşitli güçlükleri ortadan kaldırabilmesi gerekmektedir. Siber suçlarla mücadelede yaşanan problemlerin ilki "suçta ve cezada kanunilik ilkesi"nden kaynaklanmaktadır. Bu ilke gereği, hukuksal alanda suç olarak tanımlanmayan bir eylemin kovuşturulması ve kanunda yer almayan bir husustan dolayı bir kimsenin sorumlu tutulması mümkün değildir. Yasal zemin tam anlamıyla oluşturulmadığında, kanun uygulayıcılar zorlanmakta ve boşlukları yorum yaparak doldurmaya çalışmaktadırlar. Bu durum, yargılama sürecinin çıkmaza girmesine neden olabilmekte ve adalete olan güveni olumsuz etkileyebilmektedir. Dolayısıyla, öncelikle mevcut ceza kanunlarının siber suçları da kapsayacak şekilde düzenlenmesi veya siber suçlarda suçun maddi unsurunu oluşturan eylemin suç olarak tanımlandığı münferit kanunların düzenlenmesi gerekmektedir.

İkinci problem ise siber suçların doğası itibariyle klasik suçlardan büyük farklılıklar göstermesidir. Suçun gerçekleşme süresi, klasik suçların aksine saniyeler hatta saliselerle ölçülmektedir. İnternet ağı aynı anda birden çok suçun, birden çok kişiye karşı ve mağdurlarla temasa gerek kalmadan uzaktan işlenebilmesine imkân sağlamakta, çoğunlukla fail suç mahallinin yakınında bile bulunmamaktadır. Siber suçların elektronik ortamda işlenmesi nedeniyle, bu suçlara ait deliller varsa elektronik ortamda bulunmaktadır. Bu deliller maddi olmayan yapısı nedeniyle çok kolay değiştirilebilmekte, silinmekte ya da yok edilebilmektedir. Bu işlem yine tıpkı suçun işlenme şeklinde olduğu gibi uzaktan yapılmaktadır. Bunun bilincinde olan siber suçlular, suçu işledikten kısa süre sonra tüm delilleri yok ederek ya da gizleyerek arkalarında neredeyse hiçbir iz bırakmadan kaybolabilmektedirler.

Klasik usul hukukunun siber suçlarda, suçun ve suçlunun hızı yanında yavaş kalması veya koluğun gerekli ve yeterli yetki ile donatılmaması suçla mücadeleyi zorlaştırmaktadır. Klasik usul hukukunun arama ve el koyma yetkileri, gecikmesinde sakınca bulunan hâl kavramları, siber suçlar söz konusu olduğunda ağır ve hantal kalabilmektedir. Siber suçların aydınlatılmasında belirli bir suça istinaden, elektronik ortamda depolanan ve ileride delil olarak kullanılma olasılığı olan bilgilerin orijinal halinin hızlı bir şekilde korunmasına ihtiyaç duyulmaktadır. Benzer şekilde İnternet

servis sağlayıcılar (ISS) tarafından, kullanıcıların İnternet haberleşmesine ait trafik bilgilerinin belirli süreyle korunması, bunların gerektiğinde kısmen açıklanması veya haberleşmenin tespiti ve içeriğine müdahale edilmesi gibi yetkiler hayati önem taşımaktadır. Dolayısıyla, yalnızca eylemlerin suç haline getirilmesi suçla mücadele etmek için bir anlam ifade etmeyebilmektedir. Yeni gelişen bu suçların kovuşturulması için aynı zamanda, yeni usullerin geliştirilmesi gerekmektedir. Bir suçun nasıl kovuşturulacağı, kolluğun yetkilerinin neler olduğu ve bu yetkilerin nasıl uygulanacağını ortaya koyan yöntemlerin, yani usul hukukunun da bu yeni suç türüne uygun hale getirilmesi gerekmektedir.

Diğer bir problem ise siber suçluların, İnternet'in sağladığı özgürlükten sonuna kadar istifade etmesine karşın devletin, temel hak ve özgürlükleri de göz önüne alarak, güvenlik ve özgürlük arasında adil bir denge kurmak zorunda olmasından kaynaklanmaktadır. Devlet suçu önlemeye, suçla mücadele etmeye ve İnternet'in getirdiği özgürlük ortamına kısıtlama getirmeye çalışırken, hukuk devleti olarak kanunun ve kanunda öngörülen yetkilerin dışına çıkamamaktadır. Dolayısıyla, suçun kovuşturulmasına ilişkin usulün ve kanunu uygulayan kolluğun yetkilerinin açık ve net bir şekilde tanımlanması ve insan haklarına saygılı olunması gerekmektedir.

İnternetin küresel, merkezi olmayan ve sınır tanımayan doğası gereği siber suçların etki ve yetki bakımından ülke sınırlarını aşması da diğer bir problemi teşkil etmektedir. Siber suçların genellikle uluslararası bir nitelik sergilemesi, uluslararası işbirliği ve karşılıklı yardımlaşmayı zorunlu kılmaktadır. Siber uzayın, gerçek dünyanın fiziksel sınırlarından bağımsız bir şekilde, suçlulara dünyanın bir ucunda oturdukları yerden diğer ucunda suç işleme imkânı sunması ve siber suçluların kurbanlarını çoğunlukla başka ülkelerden seçmeleri, başta yargılama yetkisi olmak üzere birçok probleme neden olmaktadır. Birden çok ülkenin eşit yargılama yetkisi olduğu durumlarda, suçun işlendiği yerin kararlaştırılması (locus delicti) ve aynı fiilden ötürü bir kişinin yalnız bir kez yargılanması (ne bis idem) prensibinin uygulanmasında problemler ortaya çıkmaktadır.

Ulusal sınırlar içerisinde dahi yetersiz ve hantal kalan klasik usul hukuku düzenlemeleri, uluslararası işbirliği söz konusu olduğunda daha büyük bir sorun haline gelmektedir. Bu durum birden fazla ülkeyi ilgilendiren suçlarda suçun aydınlatılması için hayati önem taşıyan hızlı ve etkili bir koordinasyonu engellemektedir. Ayrıca, her ülkenin siber suçlara yönelik yasal düzenlemesinin bulunmaması, suç teşkil eden eylemlerin farklı olması, siber suçların izinin sürülmesi için gerekli olabilecek elektronik kayıtların tutulması veya trafik bilgilerinin

saklanması konusunda her ülkede zorlayıcı tedbir bulunmaması, siber suçlar konusunda yasal düzenleme bulunmayan ülkeleri suçlular için birer suç cenneti haline getirmektedir. Suça birden fazla ülkenin dahil olması durumunda, ülkelerden herhangi birinde eylemin suç olarak tanımlanmamış olması ya da elektronik kayıtların tutulmaması, soruşturma zincirinin kopmasına neden olabilmektedir. Suçlu tespit edilse dahi iadesi konusunda da sorunlar yaşanabilmektedir. Çifte suçluluk nedeniyle ülkeler kendi iç hukuklarında suç teşkil etmeyen eylemlerde, suçluları iade etmeyi reddedebilmekte ve bu durum işlenen suçların cezasız kalmasına neden olmaktadır. Bu sebeple, yargılama yetkisi, çifte suçluluk ve suçluların iadesi konusunda uzlaşmış kurallar ve esaslar üzerine inşa edilmiş uluslararası yardımlaşma ve işbirliği gerekmektedir.

Sözleşmenin, kendisinin başlı başına ulusal güvenlik açısından bir tehdit teşkil edip etmediği konusunda ise uluslararası işbirliği çerçevesinde, karşılıklı yardımlaşma amacıyla bilgi ve bilişim sistemlerinin diğer taraf ülkelerin doğrudan ya da dolaylı olarak erişimine açılması ya da yardımlaşma kapsamında talep edilen bilgilerin verilmesi gibi konuların ulusal bilgi güvenliği açısından bir tehdit oluşturup oluşturmadığı sorusu ön plana çıkmaktadır.

Uluslararası bir sözleşmeye taraf olmak devletler açısından maddi ve manevi çeşitli yükümlülüklerin de kabul edilmesi anlamına gelmektedir. Dolayısıyla bu yükümlülüklerin bir sözleşmeye taraf olmadan önce kapsamlı bir şekilde değerlendirilmesi gerekmektedir. Aksi takdirde, ayrıntılı olarak incelenmeden taraf olunan bir sözleşme devletleri uluslararası alanda zor durumda bırakarak çeşitli yaptırımlarla karşılaşmalarına yol açabilir. Bu nedenle, Sözleşmeye taraf olunmadan önce iç hukukta Sözleşmenin getireceği yükümlülüklerle uygun düzenlemelerin bulunması gerektiği değerlendirilmektedir. Siber suçlarla mücadelede süratli tepki verilmesinin gereği olarak görülen, resmi işlemler atlanarak gerçekleştirilen gayri resmi işbirliği ve yardımlaşma ihtiyacı, karşısında ihtiyaç duyulan yetki ve sorumlulukların iç hukukta düzenlenmesi büyük önem taşımaktadır.

2. ARAŞTIRMANIN AMACI

Çalışmanın ana amacı, Avrupa Konseyi Siber Suçlar Sözleşmesini, TCK ve diğer ulusal mevzuat ile mukayeseli olarak inceleyerek, Türkiye'nin Sözleşme'ye mevcut hali ile taraf olması durumunda, siber suçlarla mücadelesini ne derecede kolaylaştıracağını ve üstleneceği yükümlülüklerin ulusal güvenlik üzerinde oluşturacağı olumlu ve olumsuz etkileri ortaya koymaktır.

Bu kapsamda öncelikle siber suç ve siber terör kavramları, siber suç olgusunun gelişimi, bu suçların ortaya çıkmasında ve gelişiminde büyük bir rol oynayan İnternet'in tanımları ortaya konulmaya çalışılmıştır. Nispeten yeni sayılan bu suç türü ile mücadelede dünya genelinde karşılaşılan güçlükler hem teknik, hem de yasal boyutu ile incelenerek, siber suçların günümüz için yarattığı tehdidin genel olarak ortaya konulması amaçlanmıştır.

Müteakiben siber suçların, değişik boyutları ile ulusal güvenliğe olan etkileri incelenerek, siber suçların ve siber uzayın kötü maksatlarla kullanımının günümüzde ulaştığı boyutu ile gerçekten bir ulusal güvenlik problemi olarak görülebileceğinin ortaya konulması amaçlanmıştır. Bu kapsamda, özellikle ulusal bilgi güvenliğinin, değişen güvenlik algılamaları ile birlikte ulusal güvenliğin bir bileşeni haline geldiği, devletlerin kendilerini e-devlet uygulamaları ile siber uzaya taşımalarının ve bilişim sistemlerine bağımlı hale gelmelerinin ulusal bilgi güvenliğine ve bilişim sistemlerine yönelik siber suçları bir ulusal güvenlik meselesi haline getirdiği değerlendirilmiştir. Buna ilaveten, İnternet'in yalnızca teknolojik bir olgu olmadığından, sosyal ve siyasi boyutunun da bulunduğundan hareketle, gerek birey ve toplum üzerinde oluşturduğu olumsuz etki ve gerekse siyasi bir araç olarak kullanılma imkânı ile ulusal güvenliğe yönelik bir tehdit olduğu ortaya konulmaya çalışılmıştır.

Son olarak ise, Sözleşme maddeleri, TCK ve ilgili diğer ulusal mevzuat ile mukayeseli olarak incelenmek suretiyle, Sözleşmenin genel olarak siber suçlarla mücadeledeki etkinliğinin, Türkiye'nin bu konuda var olan zafiyetlerini gidermedeki yeterliliğinin ve Sözleşmenin getirdiği yükümlülüklerin güvenlik açısından değerlendirildiğinde varsa olumsuz etkilerinin ortaya konulması amaçlanmıştır. Dolayısıyla, çalışmada başlangıçtan itibaren siber suçların ulusal güvenliğe yönelik olarak oluşturduğu tehdidin boyutu, bu tehdit karşısında var olan hassasiyetler ve Türkiye'nin önünde bir alternatif olarak duran Siber Suçlar Sözleşmesi'nin, bu hassasiyetleri gidermek için gerekli ve yeterli bir araç olup olmadığının ortaya konulması amaçlanmıştır.

3. ARAŞTIRMANIN ÖNEMİ

Bilişim teknolojisinin paralelinde gelişen siber suçlar, günümüzde ulaştığı boyut ile artık yalnızca kişilerin, kurumların hatta devletlerin dahi tek başlarına mücadele edemeyeceği bir hal almıştır. Bilişim suçları ile ilgili literatürde mevcut çalışmalar çoğunlukla, hukuksal mevzuat açısından ya da teknik açıdan eğilmekte, güvenlik konusu ise çoğunlukla bilgisayar ve ağ güvenliği alanları ile sınırlı

tutulmaktadır. Bu çalışmanın, bilişim suçları ile mücadeleyi ulusal güvenlik perspektifi ile değerlendirmesi ve hukuksal bir inceleme yapması açısından, sınırlı sayıda çalışma bulunan bu alana önemli bir katkı sağlayacağı değerlendirilmektedir.

Bu çalışma ayrıca, İnternet'in ve siber suçların toplumsal etkilerini, sosyal ve siyasal boyutunu da ulusal güvenlik açısından ortaya koymak suretiyle, bu alanda yeni bir bakış açısı sunması bakımından önemli bir katkı olarak değerlendirilmektedir.

Siber suçlarla mücadelede karşılaşılan güçlüklerden birisinin, toplumda siber suçların önemi konusunda yeterli bilincin oluşmamasından kaynaklandığı çeşitli kaynaklarda belirtilmektedir. Bu çalışmanın, siber suçlara ve siber uzayın kötü amaçlarla kullanılması konusundaki faaliyetleri, güvenlik başlığı altında kapsamlı bir bakış açısıyla değerlendirmesi bakımından, bu konudaki bilincin oluşmasında ve artırılmasına fayda sağlayacağı değerlendirilmektedir.

Avrupa Birliği'ne tam üyelik süreci içerisindeki Türkiye'nin en kısa zamanda siber suçlarla ilgili ulusal mevzuatındaki düzenlemeyi tamamlaması gerekmektedir. Diğer tüm dünya ülkelerinde olduğu gibi Türkiye'de de siber suçlar gün geçtikçe artmaktadır. Bu nedenle, Türkiye'nin bu alanda yapılmış uluslararası çalışmaları bir an önce incelemesi, olumlu ve olumsuz yönlerini teşhis ederek, siber suçlarla etkin olarak mücadele edebilmek amacıyla, iştirak etmesi önem taşımaktadır. Bu çalışma, Türkiye'nin mevcut iç hukukunun, uluslararası işbirliği açısından en iyi alternatiflerden biri olarak görülen Avrupa Konseyi Siber Suçlar Sözleşmesi'nin uluslararası işbirliği ve karşılıklı yardımlaşmaya yönelik düzenlemeleri ile objektif bir bakışla mukayesesini sunması açısından; Sözleşmeye taraf olama ya da olmama konusunda karar alıcı konumundakiler için bir referans olabilir.

Türk Silahlı Kuvvetleri ve diğer kamu kurum ve kuruluşlarının ise kurumsal mücadele amacıyla, kendi talimname, yönetmelik ve talimatlarını hazırlamada istifade edebilecekleri bir kaynak olabileceği ve geniş bir bakış açısı sağlayabileceği değerlendirilmektedir.

4. ARAŞTIRMANIN VARSAYIMLARI

Siber suç kavramının tanımı ve sınıflandırılması üzerine fikir birliği bulunmamaktadır. Ancak, hangi eylemlerin bu suçlar kapsamında değerlendirileceği konusunda bir fikir birliği bulunduğu ifade edilebilir. Günümüzde bilgisayar suçu, bilişim suçu, İnternet suçu ve siber suç kavramları çoğunlukla birbirlerinin yerine

kullanılmakla birlikte; bu çalışmada siber suç kavramının, İnternet üzerinden işlenen bilgisayar suçlarını ifade ettiği varsayılmaktadır.

Siber suçlarla mücadele için teknik ve yasal tedbirlerin bir arada uygulanması gerekmektedir. Klasik suç türlerine göre oldukça yeni sayılabilecek olan siber suçlarla mücadelede mevcut ceza hukuku düzenlemeleri yetersiz kalmaktadır. Bu durum hukuki alanda suçla mücadeleyi mümkün kılacak düzenlemelerin yapılmasını, kolluğa suçla mücadele etmesine imkân verecek yetkilerin sağlanmasını ve İnternet servis sağlayıcıları başta olmak üzere, İnternet ile ilgili hizmet veren kuruluşların sorumluluklarının ayrıntılı olarak belirlenmesini gerektirmektedir.

Siber suçlar günümüzde ulaştığı boyutu değerlendirildiğinde, basit anlamda adi suçlar olarak ele alınmamalıdır. Siber suçların bilgi ve bilişim sistemlerini hedef alması, bilgi ve bilişim sistemlerinin güvenliğinin ulusal güvenlik tanımı içerisinde ifade bulan ekonomik, askeri, siyasi ve sosyal bileşenlerin tümüyle ilgili olması, bu suçların bir ulusal güvenlik tehdidi olarak görülmesini ve bu kapsamda değerlendirilmesi gerekli kılmaktadır.

Siber suçların asıl hayat alanı İnternet'tir. İnternet teknolojide yaşanan gelişmelerin hem bir sonucu hem de kaynağı olmuştur. Ancak, İnternet'in teknolojik olduğu kadar, sosyolojik bir olgu olduğu, toplumda sosyal ve siyasal etkiler yarattığı da gözden kaçırılmamalıdır. Bu nedenle güvenlik perspektifine siber uzayın sosyal ve siyasal yaşamdaki etkileri de dahil edilmelidir.

5. ARAŞTIRMANIN KAPSAM VE SINIRLILIKLARI

Çalışma, Avrupa Konseyi Siber Suçlar Sözleşmesini ve Türk Hukukunda bilişim alanında yapılan düzenlemeleri kapsamakta ve Sözleşme gereğince ulusal ve uluslararası düzeyde yapılması öngörülen maddi ve usul hukukuna yönelik düzenlemeler, Anayasa, TCK, CMK, PSVK ve bilişim alanındaki görev ve sorumlulukları düzenleyen yönetmelikler mukayese edilmektedir.

Güvenlik kapsamında ise güvenlik ve ulusal güvenlik kavramları ana hatları ile ortaya konulmaya çalışılmıştır. Ulusal güvenlik kavramı, bilgi ve bilişim sistemlerinin güvenliği temelinde ele alınmıştır. Ulusal güvenliğe yönelik tehditler de buna paralel olarak bilgi ve bilişim sistemlerine yönelik tehditlerin ulusal ölçekte tahlil edilmesi ile sınırlandırılmıştır.

Çalıřmada ağırlıklı olarak siber suçlarla mücadelenin hukuksal boyutu ele alınmıřtır. Siber suçlarla mücadele teknik ve hukuksal tedbirlerin bir arada uygulanması ile sağlanabilmektedir. Siber suçların oluřmadan önce engellenmesi ağıısından yazılım ve donanım ile ilgili alınması gereken teknik güvenlik tedbirleri büyük önem tařımaktadır. Bununla birlikte teknik tedbirlerin çok geniř bir konu olması ve ayrıntılı inceleme yapılmasının tezin konu ve kapsamı ile doğrudan ilgili bulunmaması nedeniyle, siber suçlarla ilgili teknik konulara yalnızca suçun oluřumunun, özelliklerinin ve bu suçlar karřısında mevcut hukuksal düzenlemelerin yetersiz kaldığının ortaya konması maksadıyla kısaca değinilmiřtir.



İKİNCİ BÖLÜM

BİLİŞİM, SİBER SUÇ, SİBER TERÖR VE İLGİLİ KAVRAMLAR

1. BİLİŞİM KAVRAMI VE BİLİŞİM ALANININ TEMEL UNSURLARI

a. Bilişim Kavramı

Bilişim sözcüğünün kökeni, Fransızcadan Türkçeye geçen "informatique" kelimesine dayanmaktadır. Türkçeye başlangıçta "enformasyon" olarak geçen kelimenin yerini daha sonra Türkçe bir kelime olan "bilişim" sözcüğü almıştır. Ancak, günümüzde her iki kelime de kullanılmaktadır.¹ Kavram olarak ise bilişimin kökenleri, 2. Dünya Savaşı sonrasında ortaya çıkan fikri ve teknolojik üç temel gelişmeye dayanmaktadır. Bu gelişmeler;

- Shannon-Weaver'in bilişim kuramı modeli,
- Norbert Wiener'in sibernetik kavramı ve
- Elektronik bilgisayarların tasarımı ve üretiminde yaşanan hızlı gelişmelerdir.

Bu gelişmeler pek çok disiplinin bir araya toplanabileceği, bağımsız bir inceleme alanı ve birleştirici bir kavram olan "bilişim" in ortaya çıkmasına neden olmuştur. İlk evrelerinde bilişim, temel olarak o dönemde henüz yeni olan bilgisayar teknolojisi yardımıyla bilginin saklanması, yeniden erişilmesi ve işlenmesi ile ilgili bir kavram olmuştur. Ancak, başlangıçta bilişim disiplininin bir parçası olan bilgisayar teknolojisi uygulamaları ve ardından bilişim disiplininin kuramsal boyutları, zamanla diğer birçok disiplinle iç içe geçmiş, hatta bu boyutlardan bazıları diğer disiplinler tarafından devralınmıştır. Bu durum bilişimin bağımsız bir disiplin olarak gelişmesini engellemiştir.²

Sözlük anlamı ile "insan bilgisinin, teknik, ekonomik ve sosyal alanlardaki iletişimin, otomatik makinelerde akılcı olarak işlenmesini konu alan bilim"³ olarak tanımlanan bilişim kavramının öğretilerinde de birçok tanımı yapılmıştır. Bu tanımlardan bazılarına göre bilişim;

¹ A. Caner Yenidünya, Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal, 2003, s.27.

² **Büyük Larousse Sözlük ve Ansiklopedi**, C.III, Gelişim Yayınları, 1986, s.229.

³ **AnaBritannica Genel Kültür Ansiklopedisi**, 15.bs., C.IV, Ana Yayıncılık, 2004, s.1645.

“ teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin, saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır.”⁴

“ bilgisayarın da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale getirilmesini konu alan akademik ve mesleki disipline verilen addır.”⁵

“ insanların teknik ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir.”⁶

Dolayısıyla öğretilen bilişim kavramını tanımlama ve bilişim süreci ile ilgili çok büyük görüş farklılığı olmadığı değerlendirilebilir. Tanımlarda da görüldüğü üzere bilişim kavramında ortak payda, bilgi ve bu bilginin otomatik olarak işlenmesidir. Bazı tanımlar, bilgiyi otomatik olarak işleyen aracın bilgisayar olduğunu doğrudan ifade ederek, bir anlamda bilgisayar kavramının da tanımını yapmıştır. Ayrıca bilgisayar kavramının kullanılması, bilişim tanımında bahsedilen bilginin elektronik hale getirilmiş, yani sayısal bilgi olması gerektiğini de dolaylı olarak ortaya koymaktadır.

Bilişim kavramını, yukarıda belirtilen değerlendirmeler ışığında “elektronik hale getirilmiş her türlü bilginin, özellikle bilgisayarlar aracılığıyla akılcı biçimde saklanması, işlenmesi ve iletilmesi yoluyla, bilginin kullanıma sunulması bilimi” olarak tanımlanır; “bu işlemlerin tamamını tek başına gerçekleştirme yeteneğine sahip olan araçları ya da bir araya getirildiklerinde bu yeteneği kazanan bileşenlerin oluşturduğu bütünü de bilişim sistemi” olarak adlandırmanın uygun olduğu ifade edilebilir. Günümüzde iletişim alt yapısı üzerine kurulu olan bilişim sistemlerinin oluşturduğu bilişim alanından bahsedildiğinde, akla çoğunlukla İnternet ve siber uzay kavramları gelmektedir.

⁴ Yenidünya, Değirmenci, a.y.

⁵ R. Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle**, İstanbul, Alfa, 1997, s.131.

⁶ M. Volkan Dülger, **Bilişim Suçları**, Ankara, Sekçin, 2004, s.47.

b. İnternet'in Tanımı ve Tarihçesi

İnternet insanoğlunun evinde ve işyerinde, günlük hayatının vazgeçilmez bir parçası olarak yerini almıştır. Çok eski sayılamayacak bu teknoloji ile insanlar yakın zamanda tanışmalarına rağmen, alışmaları ve kabullenmeleri çok zor olmamıştır. İnternet'i kısaca "karşılıklı olarak birbirlerine bağlanmış heterojen ağların oluşturduğu ağ"⁷ veya "ağların ağı"⁸ şeklinde tanımlamak mümkündür. İşlevsel olarak ise "insanların bilgiye erişmesine ve aktarmasına imkân sağlayan birbirine bağlı milyonlarca bilgisayarın oluşturduğu uluslararası ağ"⁹ olarak adlandırılmaktadır.

Günümüzde kullanılan küresel İnternet ağı, ARPANET isimli projenin devamı niteliğindedir. Sovyetler Birliği'nin 1957 yılında birer ay arayla, Sputnik I ve II uydularını yörüngeye yerleştirmesi, komünist yayılcılığı ve nükleer tehdidi esas alan dönemin güvenlik algılaması nedeniyle, ABD hükümetinde panik ve korku yaratır. Sputnik I'in fırlatılmasından bir yıldan kısa bir süre sonra NASA kurulur. Bunu 1958 yılında ABD'nin askeri teknoloji konusunda liderliğini koruması ve rakiplerinden gelecek benzer teknolojik sürprizlere hazırlıklı olması amacıyla, ARPA (Advanced Research Projects Agency)'nın kurulması takip eder.¹⁰ ARPA'nın başlangıçtaki amacı, bir Amerikan uydusu geliştirmektir. Ancak, hükümetin bir nükleer savaş olasılığında, haberleşmenin kesintisiz devamı için tedbir alınması gerektiğini düşünmesi üzerine, bilgisayar ve bilgisayar ağı teknolojisi üzerinde çalışmaya başlar.¹¹ Buna paralel olarak, farklı yerlerdeki bilgisayarlar arasında veri ve program alışverişine imkân sağlayan ağlar geliştirmeyi amaçlayan üniversite çalışmalarına da fon sağlar.¹²

İnternet'in fikri temelini ise Ağustos 1962'de, Massachusetts Institute of Technology (MIT) Üniversitesinden J.C.R. Licklider'in "Galaktik Ağ" kavramını ortaya koyduğu notlarında atıldığını ifade etmek mümkündür. Licklider, ortaya koyduğu bu kavramda, bugünkü İnternet'in temeli olarak görülen, isteyen herkesin program ve

⁷ Romualdo Pastor-Satorras, Alessandro Vespignani, **Evolution and Structure of The Internet: A Statistical Physics Approach**, Cambridge, Cambridge University Press, 2004, s.11.

⁸ Nobuyoshi Terashima, **Intelligent Communication Systems**, USA, Academic Press, 2002, s.20.

⁹ **Internet Explorer and Outlook Express 6.0**, Australia, Software Publications, 2002. s.1.

¹⁰ J.R. Okin, **The Internet Revolution: The not for Dummies Guide to the History, Technology, and Use of the Internet**, Maine, Ironbound Press, 2005, s.54-56.

¹¹ Debra L. Shinder, **Scene of the Cybercrime: Computer Forensics Handbook**, USA, Syngress Publication, 2002, s.59.

¹² Pastor-Satorras, Vespignani, a.g.e., s.2.

verilere çabucak ulaşabileceği, küresel olarak birbirine bağlanmış bir bilgisayarlar serisi kurgular. Licklider, 1962 Ekim ayında ARPA'nın bilgisayar araştırma bölümünün başına geçtikten sonra, ARPA'da çalıştığı dönemde halefi olan Ivan Sutherland, Bob Taylor ve MIT'de araştırmacı olan Lawrence G. Roberts'ı kurguladığı ağ kavramının önemi konusunda ikna eder.¹³

1965 yılında ise Lawrence G. Roberts, Thomas Merrill ile birlikte Massachusetts'teki TX-2 model bir bilgisayarı, Kaliforniya'daki Q-32 model bir bilgisayar ile çevirmeli bir telefon hattı üzerinden irtibatlandırarak, bilgisayarların birlikte çalışabileceğini ve uzaktaki bir bilgisayarla veri alışverişinde bulunabileceğini ispatlayan ilk geniş alan ağını yaratır.¹⁴

1966 yılında MIT araştırmacısı Roberts, ARPA'nın güneybatı Amerika'da bulunan dört büyük üniversiteyi birbirine irtibatlandırmayı amaçlayan "ARPANET" isimli projesinde çalışmaya başlar.¹⁵ ARPA, 1968 yılında BBN şirketinden Frank Heart'ın başkanlık ettiği bir gurupla bugünkü modern yönlendiricilerin (router) atası sayılacak IMP (Interface Message Processor) adlı bir cihazı geliştirmek üzere anlaşma yapar. Bu cihaz, veriyi küçük paketlere bölen, her pakete kaynak ve varış adresleri yerleştiren ve ağ içerisinde bu varış adresine gönderilmesini sağlayan paket anahtarlama adı verilen bir teknoloji kullanır.¹⁶ Bu gelişmeyle birlikte, Ekim 1969'da ARPANET kapsamında ilk mesaj, "University of California at Los Angeles (UCLA)"dan "Stanford Research Institute (SRI)"ye gönderilir ve ARPANET çerçevesinde 1969 yılında UCLA, SRI, "University of Utah" ve "University of California at Santa Barbara (UCSB)" olmak üzere dört merkez irtibatlandırılarak, bugünkü İnternet'in ilk adımı ortaya çıkar.¹⁷

1970-1971 periyodunda ARPANET 23 bağlantı noktasına ulaşır ve bilgisayarların birbirleriyle haberleşebilmeleri için Ağ Kontrol Protokolü (NCP-Network Control Protocol) ismi verilen bir protokol geliştirilir. Söz konusu protokol 1971-72 yıllarında uygulamaya geçirilir. Bilgisayarların kullanabileceği ortak güvenilir bir protokolün geliştirilmesini müteakip, araştırmacılar uygulamaya yönelik yazılım çalışmalarına başlar. 1972 yılında BBN şirketinden Ray Tomlison, basit e-

¹³ "A Brief History Of The Internet", Internet Society (ISOC) İnternet Sayfası, (Çevrimiçi), <http://www.isoc.org/internet/history/brief.shtml>, 12 Nisan 2007.

¹⁴ A.y.

¹⁵ Pastor-Satorras, Vespignani, a.g.e., s.4.

¹⁶ A.e., s.3.

¹⁷ A.e., s.4.

posta mesajlaşması için ilk yazılımı tasarlar.¹⁸ Ağ Çalışma Gurubu (The Network Working Group) ise aynı yıl Telnet protokolünü tamamlayarak, Dosya Transfer Protokolü (FTP) standardını geliştirir.¹⁹

1973 yılının Mart ayında ARPANET'in ilk uluslararası bağlantısı Londra University College ve NORSAR (Norveç) arasında gerçekleştirilir. Aynı yıl yeni bir protokol olan ve NCP'den daha fazla olanak sağlayan, İletişim Kontrol Protokolü (Transmission Control Protocol – TCP) geliştirilir. 1978 yılında TCP protokolü TCP/IP olmak üzere ayrılır. İnternet Protokolü (Internet Protocol – IP), sadece veri paketlerinin adresleme ve yönlendirme işlemini sağlarken, TCP paketlerin akışı ve kaybolan paketlerin tekrar istenmesi işlemini yürütmektedir. Bu protokollerin sağladığı genel maksatlı kullanım imkânı ve açık ağ mimarisi ARPANET'in hızla büyümesine imkân sağlar.²⁰

1979 yılında altı üniversitenin bir araya geldiği ve Bilgisayar Bilimi Araştırma Ağı (Computer Science Research Network – CSNET) adı altında bir ağ kurulması teklifinin ortaya atıldığı bir toplantı düzenlenir. Söz konusu teklif, Ulusal Bilim Kurumu (National Science Foundation – NSF) tarafından daha fazla üniversiteyi içerecek şekilde genişletilerek kabul edilir. Bu proje aynı zamanda NSF için de yeni bir devrin başlangıcı olur. Genişletilen teklif, ARPANET, TELENET ve sadece e-posta servisini içeren PostNet adı verilen üçlü bir yapıyı öngörmektedir. Bu üçlü yapı, geçiş kapıları sayesinde birbirine irtibatlanarak bir bütün oluşturmaktadır. NSF yönetim kurulu planı onaylayarak, beş yıl süre ile projeye toplam 5 milyon dolar fon ayırmaya karar verir. Böylece NSF, İnternet'in ilk destekleyicisi olur. 1983 yılı Ocak ayında ARPANET, Savunma Departmanı tarafından benimsenen TCP/IP protokolünü standart hale getirir. Aynı yıl Savunma Bakanlığı Haberleşme Ajansı ARPANET'i, gizlilik dereceli MILNET ve kamuya açık 45 kullanıcıli ARPANET olmak üzere iki bölüme ayırır.²¹

1986 yılında NSF artan kullanım oranı ve ticari önemin farkına vararak, IBM ve MCI tarafından desteklenen Merit Networks ile işbirliği anlaşması imzalar. Böylece ARPANET bilimsel araştırma kurumları dışında da kullanılmaya başlanarak, İnternet halini almaya başlar. 1988 yılında bant genişliği artırılan NSFNET'e, Kanada,

¹⁸ A.y.

¹⁹ "İnternet History", Computer History Museum İnternet Sayfası, (Çevrimiçi), http://www.computerhistory.org/exhibits/internet_history/index.shtml, 12 Nisan 2007.

²⁰ **From Gutenberg to the Internet: A Source Book on the History of Information Technology**, Ed. Jeremy M. Norman, California, Historyofscience.com, 2005, s. 6.

²¹ "İnternet History", a.y.

Danimarka, Finlandiya, Fransa, İrlanda, Norveç ve İsveç de bağlanır. 1990 yılında ARPANET resmi olarak kapatılır. Dört kullanıcı ile başlayan “ağ” yirmi yılda 300.000’in üzerinde kullanıcıya erişmiştir.²²

Ancak İnternet’in bugünkü anlamda kolay kullanımına yönelik ilk adım, grafik, ses ve görüntü erişimine imkân veren, kısaca “Web” olarak tanımlanan, “World Wide Web” kavramının ortaya çıkması ile atılır. Web, Avrupa Nükleer Araştırma Merkezi (European Organization for Nuclear Research – CERN)’ndeki Parçacık Fiziği Laboratuvarında çalışan İngiliz araştırmacı Tim Berners-Lee tarafından geliştirilen, “hypertext” diye adlandırılan bilgisayar yazılımına dayanmaktadır.²³ 1990 yılına gelindiğinde CERN, Avrupa’nın başta gelen İnternet sunucusu halini alır. 1990 yılı Ekim ayında Berners-Lee ve aynı kurumda araştırmacı olan Robert Cailliau’nun çalışmalarıyla Web konsepti, aynı yılın sonlarında ise Web sitesi tasarımı ve tanımlaması geliştirilir. 1991 yılı Aralık ayında projenin tamamlanmasını müteakip, CERN projeyi tüm dünyaya duyurur. 1992 yılı başlarında ilk basit İnternet tarama programını yine İnternet üzerinden temin edilebilecek şekilde kullanıma sunan CERN, “hypertext”i tüm dünyaya tanıtır. 1993 yılı Ocak ayında 50’den fazla bilgisayar sunucusu, CERN’in Web teknolojisini kullanmaya başlar. Web konsepti, Avrupa kökenli olmasına karşın web tarayıcı programları, Amerikan Ulusal Süper programlama Merkezi (National Center for Supercomputing Applications – NCSA) tarafından çok daha kullanışlı ve işlevsel hale getirilir.²⁴

Bugün kullanılanlara benzer ilk tarayıcı programı olan Mosaic, 1991 yılında NCSA tarafından kullanıma sunulur. Bundan üç yıl sonra Mosaic programının yaratıcıları, çok daha gelişmiş bir tarayıcı olan ve ses, yazı, görüntü alışıverişine imkân sağlayan Netscape Navigator programını kullanıma sunar. Bir sonraki yıl ise Microsoft kendi yazılımı olan ve hala en yoğun olarak kullanılan tarayıcı programı olan İnternet Explorer’ı geliştirerek kullanıma sunar.²⁵

Türkiye’nin İnternet’e bağlanması ise 1993 yılında gerçekleşir. İnternet’e bağlanmak için ilk girişim, ODTÜ-TÜBİTAK ortak organizasyonunun çalışmaları ile 1991 yılı Aralık ayında NSF ve CERN’e yapılan başvuru ile olur. Her iki kurum da talebi olumlu karşılar. Bununla birlikte kurum olarak TÜBİTAK ile gösterdiği benzerlik

²² A.y.

²³ **The U.S. History Highway: A Guide to Internet Resources**, Ed. Dennis A. Trinkle, Scott A. Merriman, New York, M. E. Sharpe Inc., 2002, s.6.

²⁴ Keith Kyker, **Wading the World Wide Web: Internet Activities for Beginners**, U.S.A., y.y., 1998, s.2-4.

²⁵ **The U.S. History Highway: A Guide to Internet Resources**, s.6.

NSF'nin tercih edilmesini sağlar. Temmuz 1992'de PTT'ye başvuru yapılarak, Eylül 1992'de ilk yönlendirici (router) kurulur ve 12 Nisan 1992 tarihinde Türkiye ilk kez İnternet'le tanışır. Daha sonra bu yapıya TR-NET adı verilir.²⁶ Günümüzde Türkiye'de İnternet hizmeti Türk Telekom Kurumu tarafından ve yine bu kurumdan işletmeci belgesi alan diğer İnternet Servis Sağlayıcılar (İSS) tarafından verilmektedir.

Hâlihazırda İnternet kullanıcılarının sayısı dünya nüfusunun %16,9'nu teşkil etmekte ve yaklaşık bir milyar yüz milyon insan İnternet'i kullanmaktadır. Türkiye'de ise İnternet'i kullananların sayısı 2006 yılı Eylül ayı itibariyle, toplam 16 milyon'a ulaşmıştır ki bu da ülke nüfusunun %21,1'ine karşılık gelmektedir.²⁷ Türkiye'de 2007 yılı itibariyle kablolu ve kablosuz İnternet servis sağlayıcılığı hizmeti veren 77 adet işletmeci bulunmaktadır.²⁸

Bugün için İnternetin teknik gelişimi, 1986 yılında oluşturulan ve protokol mühendisliği alanında İnternet'in geliştirilmesi amacıyla hizmet veren "İnternet Mühendisliği Çalışma Gurubu (Internet Engineering Task Force – IETF)", "İnternet Topluluğu (Internet Society – ISOC)" ve "İnternet Tahsisli Sayılar Otoritesi (Internet Assigned Numbers Authority – IANA)" tarafından koordineli bir şekilde yürütülmektedir. ISOC, İnternet'i geliştirmek ve resmi bir yapıya kavuşturmak amacıyla 1991 yılında kurulmuştur. Bununla birlikte, günümüzde ulusal, uluslararası ya da uluslarüstü boyutta İnternet üzerinde yasal otorite olarak görev yapan herhangi bir kural koyucu ya da düzenleyici kurum bulunmamaktadır.²⁹

c. Siber Uzay Kavramı

Siber uzay kavramı ilk olarak 1984 yılında "Neuromancer" adlı bilim kurgu romanında William Gibson tarafından kullanılmıştır.³⁰ Gibson siber uzayı aşağıdaki şekilde tanımlamıştır.³¹

²⁶ "ULAKBİM'in Tarihçesi", TUBİTAK ULAKBİM, (Çevrimiçi), <http://www.ulakbim.gov.tr/hakkinda/tarihce/>, 12 Nisan 2007.

²⁷ "Internet Usage In Europe", Internet World Stats, (Çevrimiçi), <http://www.internetworldstats.com/stats4.htm#europe>, 12 Nisan 2007

²⁸ Ayrıntılı Bilgi İçin Bkz.: Telekomünikasyon Kurumu İnternet Sayfası, (Çevrimiçi), <http://www.tk.gov.tr/doc/lisans/ISS.html>, 13 Nisan 2007.

²⁹ Işıklı Hasibe, "İnternet Alan İsimleri Sistemi – Markalar ve Alan İsimleri Arasındaki İlişki", DPT Yayınları, Ankara, 2001, s.8. akt: Tamer Soysal, "İnternet Servis Sağlayıcıların Hukuki Sorumlulukları", *Türkiye Barolar Birliği Dergisi*, Yıl.18, No. 61, Kasım-Aralık 2005, s.309.

³⁰ Jason Whittaker, *The Cyberspace Handbook*, Oxon, Routledge, 2004, s.4.

“Her milletten, milyonlarca meşru operatör (bilgisayar kullanıcısı), matematiksel kavramların öğretildiği çocuk tarafından, birlikte duyumsanan bir halüsinasyon... İnsani sistem içerisindeki her bir bilgisayardan alınan verinin grafiksel bir ifadesi. İnanılmaz bir karmaşıklık. Zihin boşluğunda sıralanan ışık çizgileri, demetleri ve verilerden oluşan takımyıldızları...”

Gibson, İnternet’in teknik anlamdaki kabullenilmiş yalın tanımından çok daha fazlasını ifade eden bir matris vizyonu ortaya koymuştur. O’na göre siber uzay, ağlar arasında iletilen verinin bilgisayarlar tarafından üretilen grafiksel gösterimi, çok karmaşık teknik bir konudur ve aynı zamanda psikoloji, epistemoloji, yargı ve sosyal sistemler tarafından şekillendirilmektedir.³²

“Siber uzay” kavramının, etimolojik açıdan ise siber ve uzay kelimelerinin bir araya gelmesinden oluşan bir isim tamlaması olduğu ifade edilebilir. Yalın olarak sözlüklerde yer almayan siber kelimesi, sibernetik kavramından türetilmiştir. Sibernetik, eski Yunancada “gemiyi yöneten pilot” kısaca “dümenci” anlamına gelen, “Kübernetes” sözcüğünden gelmektedir.³³ Türkçeye ise daha yatkın okunuş şekli ile Fransızcadan geçmiştir.³⁴

Sibernetik; “güdümbilimi, kübernitik”,³⁵ “teknolojik, biyolojik, sosyolojik ve ekonomik sistemlerde, kumanda uç iletişim süreçlerini incelemeye dayanan bir amaca doğru yönlendirilmiş etki bilimi”³⁶ ve daha genel olarak, “sistem davranışının ‘t’ anındaki gerçek değeri ile alması gereken değeri karşılaştıran bir gözleyici içeren sistemlerin modellerine ilişkin bir kuram”³⁷ şeklinde tanımlanmaktadır.

Daha basit olarak “otomatik kontrol sistemleri alanındaki çalışmalar”, “organizmalar, organik oluşumlar ve mekanik ya da elektronik sistemler içerisindeki haberleşmeyi inceleyen bilim” ve “teknoloji kullanımı ile biyolojik kontrol sistemlerinin taklit ya da kopya edilmesi”³⁸ anlamlarına gelmektedir. Buradan hareketle sibernetik sistemleri kısaca “algılayıcılarından aldığı bilgilerle geri besleme sağlayan ve kendi kendine işleyen otomatik sistemler” şeklinde tanımlamak mümkündür.

³¹ William Gibson, **Neuromancer**, London, 1984, s. 67, akt.: Charlie Gere, **Digital Culture**, London Reaktion Books, 2002, s.187.

³² Whittaker, a.y.

³³ Toygar Akman, **Sibernetik: Dünü, Bugünü, Yarını**, İstanbul, Kaknüs Yay., 2003, s.21.

³⁴ A.e., s.22.

³⁵ **Türkçe Sözlük**, 9.bs. Türk Dil Kurumu, Ankara, 1998, s.1978.

³⁶ **Büyük Larousse Sözlük ve Ansiklopedi**, C.XVII, Gelişim Yayınları, 1986, s.10470.

³⁷ **AnaBritannica Genel Kültür Ansiklopedisi**, 15.bs., C.XIX, Ana Yayıncılık, 2004, s.381.

³⁸ Microsoft Encarta 2006. Elektronik Sözlük.

Teknolojideki hızlı gelişmeyle birlikte sibernetik sistemler, bilgisayarlar ve bilgisayar kontrollü diğer cihazlar şeklinde insanoğlunun günlük hayatındaki yerlerini almıştır. Bilgisayar kullanımındaki artış benzeri görülmemiş toplumsal değişimlere yol açmış ve insan hayatını inanılmaz derecede kolaylaştırmıştır. İnternet'in yaygın olarak kullanılmaya başlanması ile coğrafi kısıtlamalar ortadan kalkmış, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan yeni bir dünya oluşmuştur. Bu dünya zamanla "siber uzay" olarak tanımlanmıştır.³⁹

Ancak çoğunlukla İnternet'i ifade etmek için kullanılan siber uzay günümüzde tek bir homojen uzaydan oluşmamaktadır. Çok sayıda, hızla genişleyen, her biri farklı bir sayısal etkileşim ve iletişim yöntemi sağlayan siber uzayların bir birleşimidir. Çeşitli alanlardaki teknolojilerin hızla birleşmesi melez uzayları ortaya çıkarmakta ise de; siber uzayı oluşturan uzaylar, İnternet teknolojisi içerisinde var olanlar, sanal gerçeklik içerisinde var olanlar ve telefon ya da faks gibi geleneksel iletişim sistemleri içerisinde var olanlar şeklinde sınıflandırılabilir.⁴⁰

Artık insanlar, cep telefonları ile konuştuklarında, dijital televizyonlarındaki kanalları değiştirdiklerinde ya da ATM cihazlarında bankacılık işlemlerini gerçekleştirdiklerinde siber uzaya girmektedirler. En geniş anlamıyla siber uzay bilişim ve iletişim ağlarının şekillendirdiği uzayı ifade etmektedir.⁴¹

2. SİBER SUÇ KAVRAMI

a. Siber Suç Kavramı

İnternetin insan hayatına kattığı olumlu değerlerin yanında, yeni suç türleri ve eski suç türlerinin bu yeni teknoloji aracılığıyla gerçekleştirilebilmesi gibi bir de karanlık yönü bulunmaktadır. Yaygın kullanılan ismi ile siber suçlar, diğer bir ifadeyle bilişim suçları ilk olarak bilgisayarın anavatanı olan Amerika Birleşik Devletleri'nde ortaya çıktığı için, bu yeni suç türünün isim babalığını yapmak görevi de Amerikalı hukukçulara düşmüştür.⁴² Bu amaçla "computer related crime (bilgisayarla ilgili suç)"⁴³, "computer assisted crime (bilgisayar yardımcı suç)" ya da "crimes against computer (bilgisayara karşı suçlar)"⁴⁴ terimleri kullanılmıştır. Nitekim günümüzde

³⁹ Rich Gibson, Schuyler Erle, **Google Maps Hacks**, U.S.A., O'Reilly Media Inc., 2006, s.97.

⁴⁰ Martin Dodge, Rob Kitchin, **Mapping Cyberspace**, London, Routledge, 2001, s.1

⁴¹ Whittaker, **a.g.e.**, s.5.

⁴² Dülger, **a.g.e.**, s.63.

⁴³ Yazıcıoğlu, **a.g.e.**, s.126.

⁴⁴ Yenidünya, Değirmenci, **a.g.e.**, s.30., Dülger, **a.g.e.**, s.63.

Amerikan öğretisinde bilişim alanındaki suçları tanımlamak için “computer crime (bilgisayar suçu)” terimi sıkça kullanılmaktadır.⁴⁵

Bilgisayar suçları, İnternet’in günlük hayata hızla girmesi ve siber uzayın bilgisayar suçları için yeni bir alan oluşturması ile birlikte “İnternet suçları” ya da “siber suçlar” şeklinde yeni bir tanım kazanmıştır. Günümüzde “bilgisayar suçu”, “bilişim suçu” ve “siber suç” kavramlarının birbirlerinin yerine kullanılması terim karmaşasını ortaya çıkarmaktadır.

Bilgisayar suçları tanımı konusunda yazar ve araştırmacılar değişik tarifler yapmaktadırlar; ancak konuya ilişkin tariflerde temelde üç görüşten hareket edilmektedir. Bu görüşlerden birincisi bilgisayar suçlarını “ekonomik suçlar” kategorisine koymaktadır. Diğer bir görüşe göre bilgisayar suçları “bilgisayar teknolojisini bilen ve bunu uygulayan kimselerin gerçekleştirdikleri istismar hareketleridir.” Üçüncü görüş ise bilgisayar suçlarını “bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış” olarak tanımlamaktadır.⁴⁶

Yukarıdaki görüşler içerisinde terimi en çok karşılayanın son görüş olduğu ifade edilebilir. Buna paralel olarak, bilgisayar suçlarını Yazıcıoğlu “ceza kuralları uyarınca, bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusu içeren fiiller”⁴⁷, Dülger ise “verilere karşı/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar” şeklinde tanımlamaktadır.⁴⁸

“Bilişim sistemi” ve “Bilgisayar sistemi” kavramları genelde birbirlerinin yerine kullanılmaktaysa da aslında aynı anlamda olmadığı değerlendirilmektedir. Bilişim kavramı bilgisayara oranla daha geniş bir kavramdır.⁴⁹ “Bilişim suçu” bilgisayarı da kapsayan ancak daha geniş bir alanda bilişim sistemlerine karşı veya bilişim sistemleri ile işlenen suçları ifade etmektedir.⁵⁰

⁴⁵ Yazıcıoğlu, **a.g.e.**, s.125., Dülger, **a.g.e.**, s.60, Yenidünya, Değirmenci, **a.y.**

⁴⁶ Yazıcıoğlu, **a.g.e.**, s.141.

⁴⁷ **A.e.**, s.142.

⁴⁸ Dülger, **a.g.e.**, s.67.

⁴⁹ Yazıcıoğlu, **a.g.e.**, s.130.

⁵⁰ Olgun Değirmenci, “Bilişim Suçları”, İstanbul, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2002, s.54.

Günümüzde bilgisayar dışında yazılımla çalışan, verileri depolayan, işleme tabi tutan ve ileten elektronik cihazlar oldukça çeşitlenmiş ve basit bilgisayar tanımından uzaklaşmıştır. Bugün cep telefonundan televizyona, çamaşır makinesinden mp3 çalara kadar birçok elektronik cihaz basit anlamda birer bilgisayar özelliği taşımakta, belli yazılımları kullanarak çalışmakta, programlanabilmekte ve veri depolayabilmektedir. Artık siber uzayın diğer bileşenleri de bilgisayarın özelliklerini kazanmaya başlamaktadır. Üçüncü nesil olarak tarif edilen cep telefonları bunun için iyi bir örnek teşkil etmektedir. Zira akıllı telefon olarak da adlandırılan bu mini bilgisayarlar, bilgisayar korsanlarının hedefi olmaktan kurtulamamaktadır. “Symbian OS” ya da “Windows Mobile” gibi işletim sistemlerine sahip bu cihazlar, kötü niyetli bilgisayar programlarından nasiplerini almaktadırlar. Çoğu zaman gönderilen bir Çoklu Ortam Mesajı (Multi Media Message – MMS) sayesinde bu cihazlara yetkisiz erişim sağlanabilmektedir.⁵¹ Buna rağmen pratikte, bilişim araçlarının en yaygın olanının bilgisayar olması, bilişim suçlarının çoğunluğunu bilgisayar suçlarının oluşturması ve “bilgisayar suçları” terimini kullanmanın bir alışkanlık haline gelmiş olması nedeniyle, genelde “bilişim alanındaki suçları” ifade etmek için de “bilgisayar suçları” terimi kullanılmaktadır.⁵²

Siber suç kavramını ise bilişim suçu ve bilgisayar suçu kavramlarının bir bileşimi olarak tanımlamak mümkündür. Siber uzay, bilişim sistemlerinin birbirlerine, kablolu, kablosuz, klasik yerel hatlar ya da uydu üzerinden bağlanması ile oluşan küresel bir ağı tanımlamaktadır. Bilişim sistemlerinin ve yine siber uzayın en önemli bileşeni bilgisayarlardır. Bu nedenle siber uzayda suçun aracı ve amacını çoğunlukla bilgisayarlar oluşturmakta⁵³ ve genel olarak işlenen her suç bilişim suçu olmakla birlikte özelde siber suç halini almaktadır. Ancak, bilişim suçları kavramı siber suç kavramına göre bir üst kavramdır ve siber suçları da içine almaktadır.⁵⁴ Zira bir bilişim sisteminin her zaman siber uzayın bir parçası olması gerekmektedir.

Dolayısıyla bir bilişim suçunun siber suç olarak tanımlanabilmesi için siber uzayda, siber uzayın bileşeni olan bilişim sistemleri ile yine bu bileşenlere karşı işlenmiş olması gerektiği ifade edilebilir. Siber suç kavramı genelde, siber uzay ya da diğer adıyla İnternet ortamında işlenen tüm suçları tanımlamak için

⁵¹ B. Emre Alkım, “Bilmediğiniz 10 Büyük Tehlike”, **CHIP Dergisi**, Ocak 2007, s.164.

⁵² Yazıcıoğlu, **a.g.e.**, s.131.

⁵³ Yenidünya ve Değirmenci, **a.g.e.**, s.33.

⁵⁴ **A.y.**

kullanılmaktadır. İnternete bağlantılı herhangi bir bilgisayar sisteminin ya da ağının diğer bilgisayar sistemleri ya da ağlarına karşı kötü maksatlı eylemler gerçekleştirmek amacıyla kullanılması, klasik suçların yeni teknolojiler kullanılarak işlenmesi ve İnternet'in ortaya çıkışıyla birlikte gelişen yeni suçlar da bu kapsamda değerlendirilmektedir.⁵⁵

Kısaca bir bilişim suçunun siber suç olarak kabul edilmesi için aşağıdaki özellikleri taşıması gerektiğini ifade edilebilir. Bunlar;

- Suç aracının bir bilişim sistemi olması,
- Suçun bir bilgisayarla/bilişim sistemine karşı işlenmiş olması,
- Suç aracı ya da amacı olan bilişim sisteminin siber uzayın bir bileşeni olmasıdır.

Burada dikkat edilmesi gereken husus her siber suçun mutlaka bilgisayar suçu olması gerekmediğidir. Zira siber uzayın en önemli bileşenleri bilgisayarlar olmasına karşın daha önce de değindiğimiz gibi başka birçok bilişim sistemi bulunmaktadır.

b. Siber Suç Olgusunun Tarihi Gelişimi

Siber suçlarının ortaya çıkışı ve gelişimi bilişim teknolojisinin gelişimi ile paralel bir seyir izlemiştir. Ancak sanılanın aksine günümüzdeki anlamıyla siber suçlarının ortaya çıkışı bilgisayarların ve bilgisayar ağlarının icadından çok daha öncesine, telefon altyapısının tesis edilmeye başlandığı 1800'lü yıllara rastlamaktadır. Günümüzde "sistemlere uzaktan erişerek zorla girme" anlamında kullanılan "hacking" bilgisayar ağları ile ortaya çıkmıştır. Bununla birlikte, bilgisayar ağlarının ve siber uzayın altyapısını oluşturan, bugünkü küresel telefon ağı 1800'lü yılların sonundan itibaren inşa edilmeye başlamış ve ilk bilgisayarın geliştirildiği 1940 yılına kadar 60 yıllık bir gelişim göstermiştir.⁵⁶

Dolayısıyla ilk "hacker"lar telefon sistemlerine girerek ücret ödmeden uluslararası görüşme yapan "phreaker"lardı. Bu kişilerin tekniği o dönemin tek telefon şirketi olan Bell Firmasının, frekansı 2600 Hz. olan uzak mesafe görüşme ton sinyalini taklit etmektir. Phreakerlar bu iş için "blue box" ya da "Mfer" adı verilen ve telefon sistemine Bell operatörleri gibi erişmelerini sağlayan çoklu frekans üreten

⁵⁵ Fausto Pocar, "New Challenges for International Rules Against Cyber-Crime", *European Journal on Criminal Policy & Research*, C.X, No.1, 2004, s.32.

⁵⁶ Shinder, a.g.e., s.52-53.

cihazlar kullanmaktaydı. Joe Engressia gibi bazı yetenekli phreakerlar ise bu sinyali, ısıklık olarak dahi üretebilmekteydi. En ünlü phreakerlardan birisi ise Captain Crunch markalı mısır gevreği kutularından çıkan oyuncak düdüğün, AT&T'nin uzak mesafe telefon servisine erişim sağlayan 2600 Hz. sinyali ürettiğini keşfeden ve bu nedenle "Captain Crunch" diye anılan John Draper'dı.⁵⁷

Ancak "phreaking" sadece uzak mesafe telefon görüşmelerinin yapılması amacıyla değil, aynı zamanda telefon üzerinden yönettikleri yasal olmayan faaliyetleri gizlemek için suçlular tarafından da kullanılmaktaydı. Bunun için aynı yerdeki iki telefon hattını birleştiren ve gerçek numaralarını gizleyerek uzak mesafe telefon görüşmesi yapılmasına imkân veren "Cheese box" adlı cihazdan istifade edilmekteydi.⁵⁸

Phreaking, 1983 yılında telefon hatlarının ses ve sinyal kanalları birbirinden ayrılacak şekilde geliştirilmesiyle son buldu. Phreaking zamanla demode olmaya başlarken, aynı dönemde kişisel bilgisayarların geniş kitlelere hitap edebilir hale gelmesi "hacker" dönemini açtı. Ancak, phreaking ruhu hackerları etkiledi ve eski phreakerlar yeni hackerlara dönüştü.⁵⁹

1970 yılında ilk kişisel bilgisayar Altair 8800 satışa sunuldu. Bunu daha sonra Commodore 64 takip etti. Ancak bu bilgisayarlar çalıştırıldığında kendiliğinden hiçbir işlem yapamıyordu. Kullanıcıların istedikleri işlemler için kendi programlarını yazmaları gerekiyordu. Bununla birlikte, bu ilk bilgisayarlar, kişilerin kendi bilgisayarlarına sahip olmaları ve program yazmayı öğrenmeleri açısından, hackerlığın da doğmasını sağladı. Özellikle popüler bir oyuncak olarak görülen Commodore 64, gençlerin programcılığın eğlencesine kapılmalarını ve son sürat hackerlığa başlamalarını sağladı. IBM'in ürettiği ve gerçek anlamda ilk kişisel bilgisayar olan PC(Personal Computer) insanlara daha fazla imkân sağlarken, hackerların önünü açan asıl gelişme ise bilgisayar ağları oldu. İlk ağlar günümüzdekilerden oldukça farklıydı. Bu ağlar ana gövde olarak da adlandırılan bir bilgisayar ve o bilgisayara bağlı terminallerden oluşmaktaydı. Terminaller ana bilgisayardaki programları çalıştırabilmekte ve dosyalara erişebilmekteydi. Ancak, kendi başlarına işlem yapma yetenekleri ve diğer terminallerle bağlantıları bulunmamaktaydı. Ana bilgisayara yapılan bir saldırı, sistemden kimsenin

⁵⁷ **Encyclopedia of New Media: An Essential Reference to Communication and Technology**, Ed. Steve Jones, U.S.A., Sage Publications, 2003, s.212.

⁵⁸ Shinder, a.g.e., s.54.

⁵⁹ **Encyclopedia of New Media**, a.y.

yararlanamaması anlamına geldiğinden, saldırganlar için de istenen bir durum değildi. Buna rağmen, hackerlara diğer kullanıcıların ana bilgisayardaki dosyalarına erişme imkânı vermesi açısından önemli bir aşamayı temsil etmekteydi.⁶⁰

1970'li yıllarda bilgisayarların birbirlerine irtibatlanmasına imkân sağlayan "ethernet" kartının geliştirilmesi ve kişisel bilgisayarların yaygınlaşması ile ana bilgisayara bağlı terminallerden oluşan ağ mimarisi ortadan kalkmaya başladı.⁶¹ Böylece tek bir ana bilgisayara bağlı ağ yapısından kaynaklanan dezavantajlar kaybolurken, diğer kullanıcıların bilgisayarlarına saldırmak da kolaylaştı.

Bu gelişmeyi PC'lerin birbirlerine yerel olarak irtibatlanması ile oluşturulan yerel ağlar ve daha sonra bir modem cihazı ve telefon hattı sayesinde kurulan uzak mesafeli ağlar izledi. Bu yeni imkân BBS (Bulletin Board Service)'lerin ortaya çıkmasına olanak sağladı. BBS'ler bir veya daha fazla modemle bağlandığı, kullanıcıların arama yaparak dosya indirmelerine veya mesaj göndererek toplu tartışma yapmalarına imkân sağlayan bilgisayarlardı. BBS'ler sayesinde ilk dönem hackerları birbirleri ile mesajlaşabilme, yeni yöntemleri, taktikleri ve kötü maksatlı yazılımları paylaşabilme imkânına kavuştu.⁶² "The Phoenix Fortress" ve "Plovernet" isimli BBS'ler bunlardan sadece ikisiydi. Yine aynı dönemde "The Hacker Quarterly" ve "Hacker'zine" gibi hackerlara yönelik süreli yayınlar da yöntemlerin hackerlar arasında paylaşılmasına ve pazarlanmasına imkân sunmaktaydı.⁶³ Bazı BBS'ler ise sadece pornografik görüntü ve hikâyeler konusunda hizmet vermekteydi.⁶⁴

1970'li ve 1980'li yılların en ünlü gurupları "414- Club", "Legion of Doom", "Chaos Computer Club" ve "Atlanta Three" gibi hacker gurupları oldu. Bu gurupların hepsi ya bedava telefon konuşması yapabilmek için telefon şirketlerini ya da kredi kartı ve kişisel hesap numaralarını çalabilmek için bilgisayar sistemlerini hedef almaktaydı.⁶⁵ Bu dönemde hacker faaliyetleri o kadar endişe verici bir hal aldı ki, FBI aktif bir şekilde takip ve tutuklamalara başladı. İlk tutuklanan hacker, 1981 yılında "Captain Zap" olarak bilinen Ian Murphy olurken, O'nu aynı yıl tutuklanan ünlü hacker Kevin Mitnick takip etti. Yine bu dönemde Avustralya, Almanya, Arjantin'den

⁶⁰ Shinder, a.g.e., s.55.

⁶¹ A.e., s.56.

⁶² A.y.

⁶³ Joseph M. Kizza, **Computer Network Security**, U.S.A., Springer Science+Business Media Inc., 2005, s.140.

⁶⁴ Shinder, a.y.

⁶⁵ Kizza, a.g.e., s.139.

rapor edilen saldırılarla birlikte hacker faaliyetleri ve kültürünün artık küresel bir hal aldığı ortaya çıkmaya başladı.⁶⁶

1983 yılı başında TCP/IP'nin standart hale gelmesi ile birlikte, küresel ağ gittikçe büyümeye başladı. ARPANET'in ilk günlerinde güvenlik askeri açıdan önemli bir konu idi ve bu durum ARPANET'in askeri ve sivil amaçlı olmak üzere ayrılması ile sağlanmaya çalışılmıştı. Bununla birlikte, 1988 yılında bir bilgisayar virüsü İnternet ortamına bırakıldığında, ABD'deki birçok bilgisayara bulaşarak İnternet'in büyük bir bölümünü işlemez hale getirdi. Bu olay İnternet kullanıcılarının, aralarında kötü niyetli olanların da bulunduğunu anlamalarını sağladı.⁶⁷ Robert Morris tarafından İnternet ortamına bırakılan söz konusu virüs, İnternet'e bağlı 6000 bilgisayarın çökmesine neden oldu.⁶⁸ Bu olay ABD hükümetinin, ulusal bilgisayar ağına karşı yapılan benzer ve ilgili saldırıları araştırmak üzere Bilgisayar Olayları Müdahale Timi (Computer Emergency Response Team – CERT)'ni kurması ile sonuçlandı.⁶⁹

1991 yılına gelindiğinde e-posta kullanıcıları İnternet haberleşmelerinin dinlenebileceğini fark etti ve bunun üzerine Philip Zimmermann geliştirdiği bir şifreleme programını kullanıma sundu. Ancak, bu program aynı zamanda suçlular tarafından haberleşmelerini polisten gizlemek üzere de kullanılmaya başladı.⁷⁰

Bilişim suçlarındaki asıl artış ve gelişme ise Web dönemi ile birlikte gerçekleşti. İnternet'e bağlı bilgisayar ve kullanıcı sayısı bu dönem de büyük artış gösterdi. Buna ilaveten, İnternet ortamına taşınan hizmetlerin artması, e-bankacılık ve e-ticaret'in gelişmesi, suç için yeni fırsatların, araç ve yöntemlerin ortaya çıkmasına neden oldu. 1994 yılında "First Virtual" adlı ilk sanal banka kuruldu.⁷¹ 1995 yılında Amerikalı ünlü hacker Kevin Mitnick FBI tarafından, ikinci kez tutuklandığında, binlerce kredi kartı numarasını çaldığı için bilgisayar dolandırıcılığı suçlamasıyla tutuklanan ilk kişi oldu.⁷² 1994 yılı Haziran ve Ekim ayları arasında Rus hacker Viladimir Levin tarafından yönlendirilen bir çete ise, Citibank'ın elektronik

⁶⁶ A.e. , s.140.

⁶⁷ Shinder, a.g.e., s.61.

⁶⁸ Mad Macz, **Internet Underground: The Way of the Hacker**, U.S.A., PageFree Publishing Inc., 2002, s.14.

⁶⁹ Kizza, a.y.

⁷⁰ Shinder, a.g.e., s.61.

⁷¹ Macz, a.g.e., s.17.

⁷² Kizza, a.g.e., s.141.

para transferi sistemine girerek, 10 milyon doların üzerindeki bir parayı Finlandiya, Rusya, Almanya, Hollanda, ABD ve İsrail'deki hesaplara transfer etti.⁷³

Web döneminde hackerlar İnternet sitelerine saldırarak bu siteleri çökertmeye ya da içeriklerini değiştirmeye başladı. Yine DoS saldırıları Web dönemi ile birlikte başladı. Virüs saldırıları ise bu dönemde yalnızca artmakla kalmayıp, çok daha tehlikeli bir hale geldi. 1998 yılında ortaya çıkan ve Çernobil virüsü olarak da bilinen CIH virüsü, 26 Nisan 1999 tarihinde etkin hale gelerek birçok kullanıcının verilerini kaybetmesine yol açtı. Bu virüsün yol açtığı mali kaybın ise toplamda yüz milyonlarca dolar olduğu tahmin edilmekteydi.⁷⁴ 2000 yılı ise "Mellisa", "Love Bug" ve "Killer Resume" gibi büyük mali kayıplara neden olan virüs saldırılarına sahne oldu.⁷⁵ Aynı yıl Yahoo, eBay, Amazon, CNN.com ve Buy.com gibi büyük İnternet sitelerine yapılan DoS saldırıları da İnternet kullanıcılarının erişimlerini saatlerce engelleyerek, ticari İnternet dünyasını felç etti.⁷⁶ İnternet'in yaygınlaşması ile birlikte özellikle mali çıkar amaçlı dolandırıcılık ve sahtekârlık suçları da artış gösterdi. Dolandırıcılık amaçlı sahte e-posta mesajları, banka ya da e-ticaret sitelerinin taklit edilerek kişisel bilgilerin, kredi kartı ve hesap bilgilerinin çalınması şeklindeki suçlar artış gösterdi.

Günümüzde bilişim suçları hala artan bir şekilde endişe konusu olmaya devam etmektedir. Birçok ülke bilişim suçlarını önlemek maksadıyla, teknik ve yasal tedbirler alırken, bu suçların küresel anlamda yayılması ve giderek artan bir şekilde maddi ve manevi zarara yol açması, hem ülkeleri hem de çeşitli uluslararası kuruluşları, uluslararası mücadele ve işbirliği konusunda çareler aramaya yöneltmektedir.

c. Siber Suçların İşlenme Yöntemleri

Bilişim suçlarının gelişiminin, bilişim teknolojisinin gelişimi, İnternet'in kullanım oranı ve artan hizmet çeşitliliği ile paralel olduğu daha önce belirtilmiştir. Teknolojinin sunduğu imkânlar geliştikçe, beraberinde suç işlemeye istekli kişiler de yeni fırsatlar elde etmiştir.

⁷³ Hedieh Nasheri, **Economic Espionage and Industrial Spying**, U.S.A., Cambridge University Press, 2005, s.39.

⁷⁴ David Salomon, **Foundations of Computer Security**, U.S.A., Springer-Verlag London Ltd., 2006, s.294.

⁷⁵ Kizza, a.y.

⁷⁶ Mark Manion, Abby Goodrum, "Terrorism or Civil Disobedience: Toward a Hactivist Ethic", **Internet Security: Hacking, Counterhacking & Society**, Ed. Kenneth Einar Himma, U.S.A., Jones and Barlett Publishers Inc., 2007, s.61.

Günümüzde bilişim suçlarının işlenme şekilleri çöpe dalma, gizlice dinleme, web sayfası yönlendirme ve kötü maksatlı yazılımlar gibi çok çeşitlilik göstermekte ve gelişen teknoloji ile bunlara yeni yöntemler eklenmekte veya var olanlar şekil değiştirebilmektedir. Bu nedenle yöntemlerin tamamını tanımlamak mümkün olmadığından ancak örnekleme yapılabilmektedir.⁷⁷

Çöpe Dalma (Scavenging)

Artık Toplama da denilen bu bilişim suçu, bir bilgisayar sisteminin çalışmasından geriye kalan veri ve bulguların toplanması suretiyle işlenmektedir. Yazıcıdan çıkan bir karbon kâğıdın veya bilgisayar çıktısının çevreden toplanması şeklinde olabileceği gibi bilgisayarda işlem görüp silinmiş, yok edilmeye çalışılmış verilerin elde edilmesi şeklinde de olabilmektedir.⁷⁸

Gizlice Dinleme (Eavesdropping)

Bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek veya bilişim sistemlerinin az da olsa yaydığı elektromanyetik dalgaların yakalanarak verilerin tekrar elde edilmesi tekniğidir. Gizlice dinleme tekniği özellikle bilgisayar ekranlarının yaydığı elektromanyetik dalgaların yakalanması ve tekrar ekran görüntüsüne dönüştürülmesi suretiyle işlenebileceği gibi, veri naklinde kullanılan iletişim hatlarına fiziksel olarak irtibat yapılması şeklinde de gerçekleştirilebilmektedir.⁷⁹

Veri Aldatmacası (Data Diddling)

Veri aldatmacası bu tür eylemler içerisinde hem basit ve güvenilir olması, hem de ortaya çıkarılması zor olduğu için en çok tercih edilen yöntemlerden birisidir. Veri aldatmacası verinin bilişim sistemlerine girilirken değiştirilmesi, diğer bir ifade ile yanlış veri girilmesi veya bazı verilerin kasten sistemde bırakılması şeklinde ifade edilebilir. Böylece, fail, bilgisayara girdiği veya bilgisayarda bıraktığı veriler ile mevcut veriler üzerinde istediği yönde değişiklik yapma veya cihazı istediği şekilde kullanma imkânına kavuşmaktadır.⁸⁰

Tarama (Scanning)

⁷⁷ Değirmenci, a.g.e., s.75.

⁷⁸ Kurt, a.g.e., s.62.

⁷⁹ Değirmenci, a.g.e., s.77.

⁸⁰ Yazıcıoğlu, a.g.e., s.152.

Biliőim sistemlerine, deęeri her seferinde deęiően verilerin hızlı bir őekilde girilmesi suretiyle, sistemin olumlu cevap verdięi durumların tespit edilmesine y6nelik bir tekniktir. Tarama, biliőim sistemlerinin telefon numaralarını veya İnternet'e baęlı sistemlerin IP numaralarını bulmaya y6nelik olabileceęi gibi numarası belli olan, fakat őifre ile korunmuő sistemler i6in bu őifreleri bulmaya y6nelik de olabilir.⁸¹

Süper Darbe (Super Zapping)

Süper darbe ismiyle bilinen programlar, bilgisayar sistemlerinin 6alıőırken oluőturduęu 6eőitli hatalar ya da programların kendiliklerinden oluőturdukları hatalar nedeniyle kilitlenmesi ve 6alıőamaz hale gelmesi durumunda yeniden eski haline getirilmesi amacıyla kullanılmaktadırlar. Bu programlar sistemin bu őekilde kilitlenmesi durumunda, büt6n g6venlik duvarlarını aőarak sistemin yeniden 6alıőmasını ve sorunların giderilmesini saęlarlar. Ancak yanlış ellere ge6tięinde 6ok tehlikeli bir su6 aracı da olabilmektedirler.⁸²

Salam Teknięi

Bu teknik genellikle bankacılık sektöründe yaygın olarak kullanılan bir y6ntemdir. 6ok fazla sayıdaki kaynaktan, 6ok az miktarda deęerin transfer edilmesi yoluyla ger6ekleőtirilir. Bu y6ntem i6in genellikle Truva atları kullanılır.⁸³ Bir6ok banka hesabındaki virg6lden sonraki son veya son iki rakamın baőka bir hesaba havale edilmesi suretiyle, hesap baőına fark edilmeyecek meblaęların, havale edilen hesapta b6y6k meblaęlara ulaőması őekilde kazan6 saęlanması ama6lanmaktadır.⁸⁴

Eőzamansız Saldırıları

6ok iőlevli program teknikleri, bilgisayarda 6alıőan bir6ok programın bilgisayar kaynaklarını 6eőitli usuller 6er6evesinde sırayla kullanmasına olanak saęlamaktadır. Sistem t6m programların isteklerine eő zamanlı olarak cevap veremedięinden, bazı istekleri kaynaklar uygun oluncaya kadar sıraya almakta ve bekletmektedir. Bu bekleme sırasında iyi programlama bilgisine sahip kiőiler verileri deęiőtirebilmektedir. 6rneęin yazıcıya g6nderilen bir 6ıktı isteęinin baőka bir iőlem nedeniyle beklemeye

⁸¹ Kurt, a.g.e., s.65.

⁸² Yazıcıoęlu, a.g.e., s.156.

⁸³ Deęirmenci, a.g.e., s.84.

⁸⁴ Yazıcıoęlu, a.g.e., s.155.

alınması durumunda, çıktısı alınacak veri üzerinde değişiklik yaparak çıktıyı değiştirmek mümkün olabilmektedir.⁸⁵

Sırtlama (Piggybacking)

Sırtlama fiziksel veya elektronik yollarla bilişim sistemlerine yetkisiz olarak girme tekniğidir. Fiziksel sırtlama olarak anılan teknikte, bilişim sistemlerinin girişi kontrol altına alınan alanlarına, girişe yetkili olan bir kimsenin giriş iznini kullanarak girmek ve mevcut verilere herhangi bir şekilde erişmek söz konusudur. Elektronik sırtlama ise, bilişim sistemine bağlı kullanıcılardan herhangi birinin kullandığı hattan, başka birinin yetkisiz olarak bağlanmasıdır.⁸⁶

Web Sayfası Yönlendirmesi

Web sayfası yönlendirme tekniğinde iki ayrı yöntem kullanılmaktadır. Bunlardan ilki DNS (Domain Name Server)'lere müdahale edilerek yapılan yönlendirmelerdir. İnternet sitelerine ait adresler aslında rakamlardan oluşmaktadır. Ancak kolaylık sağlaması bakımından rakam yerine kelimelerden oluşan adresler kullanılmakta ve kelimelerden oluşan adresler DNS'ler tarafından tekrar rakamsal adrese çevrilerek bağlantı sağlanmaktadır. Bu aşamada DNS'e müdahale edilerek, kullanıcının ulaşmayı istediği İnternet sayfasına benzer şekilde tasarlanan başka bir sayfaya yönlendirmesi ve kullanıcının şifre, banka hesap numarası veya kredi kartı numarası gibi özel bilgilerinin elde edilmesi amaçlanır. Diğer yöntem ise kullanıcılar tarafından bir adresin yazılması esnasında çoğunlukla yapılan yazım hatasını tahmin ederek, yanlış yazanların ulaşabilecekleri sahte bir İnternet sitesinin oluşturulmasıdır.⁸⁷

İstem Dışı Alınan Elektronik Postalar (Spam)

İstem dışı alınan elektronik postalar anlamına gelen "spam" genellikle bir ürünün reklâmı, pazarlanması veya sosyal içerikli bir mesajın büyük kitlelere ulaştırılması amacı ile kullanılmaktadır. Bu mesajlar veri tabanlarında kişilere ait elektronik posta adreslerini bulunduran kuruluşların bu adresleri büyük ücretler karşılığı satmaları sonucu ortaya çıkmıştır.⁸⁸

⁸⁵ Yazıcıoğlu, a.g.e., s.158.

⁸⁶ Değirmenci, a.g.e., s.101.

⁸⁷ A.e., s.99.

⁸⁸ A.e., s.96.

Spam zararsız gibi görölse ve diğér bilişim suçları kadar ciddi olmadığı düşünölse de aslında hem yerel hem de küresel anlamda büyük bir problemdir. Tüm dünya da iletilen e-postaların %59'u spamdır.⁸⁹ Türkiye'de ise spam oranı tüm e-posta trafiğinin %79'unu teşkil etmektedir.⁹⁰ Dolayısıyla Spam hem İnternet iletişimini gereksiz yere meşgul ederek bankacılık, ticaret ve resmi işlemler gibi önemli işlemleri yavaşlatmakta, hem e-postaların depolanması için kullanılan kişisel ve kurumsal alanları gereksiz yere işgal etmekte, hem de bunların okunması, silinmesi gibi işlemler zaman kaybına neden olmaktadır. Bazen e-posta sunucuları dahi çökebilmektedir.⁹¹ Spam'ın bir diğér zararı ise virüslerin yayılmasına imkân sağlayarak suç işlenmesi için fırsat yaratmasıdır.

Phishing

Phishing dolandırıcılık maksadıyla yapılan bir eylemdir. Genellikle mali kazanç sağlamak amacıyla, kişi, gurup ya da organizasyonların gizli bilgilerinin elde edilmeye çalışılmasıdır. Bu yöntemde kullanıcıların çeşitli şekillerde kandırılarak, kredi kartı numarası, İnternet bankacılığı bilgileri ve diğér hassas bilgilerini ifşa etmesinin sağlanması amaçlanmaktadır. Bu bilgiler daha sonra dolandırıcılık amacıyla kullanılmaktadır.⁹²

Bu maksatla genellikle sahte e-posta ve Web sayfaları kullanılmaktadır. Dolandırıcılar, tüketicilere tanınmış bir firmadan geliyormuş izlenimi verilmiş bilgi güncelleme talebi vb. içeren e-postalar göndermektedir. Bu e-postalarda genellikle cevap için e-postanın içindeki bağlantının takip edilerek gerekli siteye geçilebileceği belirtilmektedir. Ancak, verilen talimat uygulandığında gidilen site daha önce Web sayfası yönlendirmede anlatıldığı şekilde dolandırıcılar tarafından hazırlanmış ve gerçeğini taklit eden sahte bir Web sayfası olmaktadır.

Hizmet Reddi Saldırısı (Denial of Service Attack – DoS)

DoS saldırısının amacı, hedef alınan sunucu bilgisayarın imkânlarını aşacak miktarda hizmet talebinde bulunularak, sunucunun diğér bilgisayarların isteklerini reddetmesini sağlamaktır. DoS saldırılarının gelişmiş bir biçimi ise Dağıntık Hizmet Reddi Saldırısı (DDoS)'dır. Bu saldırı tarzı daha etkili ve zayıflatıcı bir tekniktir. Tek

⁸⁹ Symantec Internet Security Threat Report: Trends for July–December 06, C.XI, Mart 2007, s.8.

⁹⁰ Symantec EMEA Internet Security Threat Report: Trends for July–December 06, C.XI, Mart 2007, s.35.

⁹¹ Kurt, a.g.e., s.72.

⁹² Symantec Internet Security Threat Report:Trends for July–December 06, s.64.

bir saldırı bilgisayarı kullanılması yerine birden fazla noktadan birden fazla bilgisayarla gerçekleştirilir. Bunun için saldırgan önceden saldırıda kullanacağı bilgisayarlara, kontrollerini ele geçirmeyi sağlayacak küçük programlar yerleştirir. Bu bilgisayarlar çoğunlukla “zombi” olarak adlandırılırlar ve saldırgan tarafından kontrol edilerek topluca hedefe saldırımları sağlanır. Saldırı kaynağının dağınık olması, hedef tarafından tüm saldırı rotalarının kapatılmasını güçleştirmesi açısından, DoS’a göre daha etkili bir yöntem olmasını sağlamaktadır.⁹³

Kötü Maksatlı Yazılımlar

Bilişim suçlarının en yaygın işleme yöntemi hedef alınan sisteme kötü maksatlı yazılımların gizli bir şekilde yerleştirilmesidir. Yerleştirilen bu yazılımlar, tasarlanma amaçlarına ve saldırganın niyetine göre ileri saldırıların gerçekleştirilmesine imkân sağlayabileceği gibi, bu yazılımların bazıları bizzat saldırının kendisi de olabilmektedir. Kötü maksatlı yazılımların en önemlileri, virüsler, Truva atları, solucanlar, mantık bombaları, tavşanlar ve bukalemunlardır.

• Bilgisayar virüsleri

Bilgisayar virüsleri, “kendi kendini çoğaltma özelliğine sahip, kopyalarını başka bilgisayarlara bulaştırarak onları da enfekte edebilen programlardır.”⁹⁴ Virüsler kendilerini diğer çalıştırılabilir programlara ilişirirler. Bu nedenle virüsler kendi başlarına var olamazlar. Virüs eklenmiş bir program çalıştırıldığında virüs de çalışarak, işlevini yerine getirir. Bu işlev genellikle kendisini diğer programlara ve disklere bulaştırmaktır. Ancak virüslerin işlevleri içerdikleri kodlara ve yaratılma amaçlarına göre değişmektedir.⁹⁵

Genellikle virüsleri tahrip etmeye yönelik olanlar ve rahatsızlık verici olanlar olmak üzere ikiye ayırmak mümkündür. Birinciler, dosyaları kullanılmayacak hale getirerek bozar, bazıları tamamen siler ve bir kısmı ise tüm sistemi kullanılmayacak hale getirir. İkinci grupta ise ekranda çeşitli mesajların çıkmasına, bazı işlemlerin belli bir süre yapılamamasına veya programların geçici bir süreyle çalışmamasına neden olur. Virüsler yazılıma olduğu gibi donanıma da zarar verebilirler. Örneğin sabit diskin sürekli dönmesine yol açan bir virüs diskin aşırı ısınarak zarar görmesine

⁹³ Eric J. Sinrod, William P. Reilly, “Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws”, **Santa Clara Computer and High Technology Law Journal**, C.XVI, No.2, May 2000, s.12-16.

⁹⁴ Değirmenci, **a.g.e.**, s.88.

⁹⁵ Eric Maiwald, **Fundamentals of Network Security**, U.S.A., McGraw-Hill , 2004, s.67.

neden olabilir. Benzer şekilde merkezi işlemcinin gereksiz işlemlerle sürekli ve yoğun bir şekilde çalışmasına neden olan bir virüs, işlemcinin yeterince soğutulamamasına ve tahrip olmasına neden olabilir.⁹⁶

Virüsler genellikle diğer kötü amaçlı yazılımlarla karıştırılırlar. Ancak “virüsleri diğerlerinden ayıran en büyük özellikleri kendi kendilerine çoğalıp diğer programlara bulaşabilmeleridir.”⁹⁷ Bilgisayar virüslerinin pek çok çeşidi bulunmasına rağmen, genellikle yerleştikleri yere göre “boot virüsleri”, “dosya virüsleri” ve “makro/mail virüsleri” olmak üzere üçe guruba ayrılmaktadırlar.⁹⁸

• Truva Atı (Trojan Horse)

Truva atı yazılımı adını, Yunan Mitolojisinde bahsedilen, Troyalılar ile Akhalıların yaptığı savaşta Troyalılara masum bir hediye olarak sunulan, ancak içerisine Akhalı savaşçıların gizlendiği büyük tahta attan almaktadır.⁹⁹

Truva atı yazılımlarının çalışma mantığı da buna benzerdir. Truva atı yazılımları gizli işlevler taşıyan masum görünüşlü programlardır. Bu programlar bilgisayar yüklendikten sonra diğer programlar gibi çalışmaya başlar. Ancak, masum program içerisine gizlenmiş alt program, kullanıcının farkında olmadığı başka işlevler de gerçekleştirir. Truva atları genellikle orijinal kaynak kodları bir Truva atı yerleştirilerek değiştirilmiş popüler programlar şeklinde görülmektedir.¹⁰⁰ Truva atları kullanılarak hemen hemen bütün bilişim suçlarını işlemek mümkündür.¹⁰¹ Kısaca bir bilgisayara kullanıcısının haberi olmaksızın, çoğunlukla kötü amaçlar taşıyan bir programın yerleştirilme yoludur. Yerleştirilen bu programın işlevi ise başta bilgisayarın kontrolünün üçüncü bir kişinin eline geçmesini sağlamak olmak üzere tasarlayıcısının niyetine bağlı olarak çok çeşitli olabilir.

• Ağ Solucanları (Network Worms)

Ağ solucanları virüslere benzerler ancak en büyük farkları kendi kendilerine çoğalabilmeleri ve virüslerin aksine başka bir dosya ya da programa ihtiyaç

⁹⁶ Yazıcıoğlu, a.g.e., s.163.

⁹⁷ A.e., s.164.

⁹⁸ Değirmenci, a.g.e., s.90.

⁹⁹ Dülger, a.g.e., s.69.

¹⁰⁰ Sinrod, Reilly, a.g.e., s.43.

¹⁰¹ Berrin Akbulut, “Türk Ceza Hukunda Bilişim Suçları”, Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi, Konya, 1999, s.56., akt.: Dülger, a.g.e., s.70.

duymadan ağ üzerinde dolaşabilmeleridir.¹⁰² Ağ üzerinde bir bilişim sistemine gelen ağ solucanı, ya bir virüs gibi davranarak yazılıma zarar verir ya da sisteme bir Truva atı bırakır. Çoğu zaman yakalanmamak için kendilerinden kalan tüm izleri temizlerler.¹⁰³

• Mantık Bombaları

Mantık bombaları da aslında Truva atının bir türüdür. Truva atlarında olduğu gibi zararsız bir yazılım görünümü ile sisteme girer ve normal bir şekilde çalışarak herhangi bir zarar verici işlemde bulunmazlar. Ancak belirli bir zamanda, bir olayla veya kullanıcı tarafından gerçekleştirilen bir işlemle tetiklenirler. Bu tetiklenme bir tuşa basılması veya belli bir programın çalışması şeklinde olabileceği gibi ünlü bir şahsın doğum tarihi de olabilir.¹⁰⁴ Mantık bombalarının gerçekleştireceği işlem tamamen içerdiği kodlara bağlıdır. Bu yöntemi kullananların amacı hırsızlık, istihbarat, şantaj ya da sadece eğlence olabilir.¹⁰⁵

Mantık bombalarının bir türü de belli bir süre çalışmayı müteakip harekete geçer ve saatli bombaya benzemeleri nedeniyle “saatli bomba” olarak adlandırılırlar. Saatli bombalar, belli bir tarihin haftanın belli bir gününe rastlaması halinde veya günün belli bir saatinde harekete geçerler.¹⁰⁶

• Tavşanlar (Rabbits)

Bilgisayar virüsünün bir çeşidi olan tavşanlar girdikleri sistem içerisinde sürekli ve hızla çoğalan, yerleştiği bilişim sisteminin belleğini ve diskteki alanı koloni kurmak suretiyle dolduran, sisteme sürekli gereksiz komutlar göndermek suretiyle yavaşlatan ve en sonunda durma noktasına getiren yazılımlardır.¹⁰⁷ Tavşanları virüslerden ayıran en önemli özellikleri, başka dosyaların sonuna eklenmelerinin, faaliyete geçmek için dışarıdan müdahale edilmesinin gerekmemesi ve kendilerine yeter özellikte olmalarıdır.¹⁰⁸

• Bukalemun (Chameleon)

¹⁰² Sinrod, Reilly, a.g.e., s.42.

¹⁰³ Değirmenci, a.g.e., s.87.

¹⁰⁴ Bidgoli, a.g.e., s.373.

¹⁰⁵ Kurt., a.g.e., s.73.

¹⁰⁶ Değirmenci, a.g.e., s.102.

¹⁰⁷ Kurt, a.g.e., s.75.

¹⁰⁸ Değirmenci, a.g.e., s.103.

Bir Truva atı yazılımı olan bukalemun, normal bir programın tüm özelliklerini taklit edebilen ve bu sayede girdiği sistemdeki verileri, kullanıcı ad ve şifrelerini kopyalayıp gizli bir şekilde saklayabilen programlardır.¹⁰⁹

Bukalemun yazılımları özellikle çok kullanıcıli sistemlerde içine girdikleri bilişim sisteminde bulunan kullanıcı adlarını ve şifrelerini gizli bir dosyaya kaydettikten sonra kullanıcıya sistemin bakım için geçici bir süre kapatılacağı uyarısını verir. Daha sonra bukalemun programını kullanan şahıs sisteme girer ve kaydedilen gizli dosyadaki kullanıcı isimlerini ve şifreleri alır. Bundan sonra söz konusu çok kullanıcıli sisteme istediği gibi erişebilir.¹¹⁰

Hukuka Aykırı İçerik Sunulması

Bilişim suçlarının çok sık karşılaşılan bir başka şekli de hukuka aykırı içeriklerin bilişim sistemlerinde bulundurulması, diğer kullanıcıların erişimine sunulması veya gönderilmesidir. Bu içerikler ırkçı, ayrımcı, şiddeti teşvik eden içerikler, pornografik materyaller, terör örgütü propagandası veya suça teşvik edici içerikler olabilir. Bunun yanında yine hakaret, küçük düşürme, iftira, özel hayatın ihlali ve benzeri suçlar da işlenebilir.

Diğer Yöntemler

Çok rastlanan bir diğer yöntem ise “hackleme” olarak ifade edilen İnternet sitelerine saldırılarak, Web sayfalarının içeriğinin silinmesi, değiştirilmesi ya da başka bir adrese yönlendirilmesidir. Bu yöntemde genellikle hacklenen sayfaya siyasi, ideolojik mesajlar veya karalama içeren ifadeler bulunan içerikler yerleştirilir. Bahsedilen yöntemler en çok kullanılan yöntemlerdir. Bunun dışında daha pek çok yöntem bulunmaktadır. Bunlardan bazıları web sayfası hırsızlığı ve yerine geçme gibi nadir uygulanan yöntemlerdir.

d. Siber Suçların Sınıflandırılması

Bilişim suçlarının sınıflandırılması konusunda herhangi bir standart mevcut değildir. Bunun bir sebebi bilgisayar teknolojisinin akıl almaz bir hızla gelişmeye devam etmesi, dolayısıyla ortaya yeni suç türlerinin çıkmasıdır. Diğer bir nedeni ise bilişimle ilgili kavramların tanımlarında bulunan farklılıklardır. Suçların

¹⁰⁹ Kurt, a.g.e., s.75.

¹¹⁰ Emin D. Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yay., 1992, s. 51, akt.: Kurt, a.g.e., s.75.

sınıflandırılmasında kimi uzmanlar “bilgisayar suçları” kimileri ise “bilişim suçları” ana başlığını kullanmıştır. Ancak “bilişim suçları ile ilgili olarak uzmanlar tarafından yapılan tasniflerin birbirine çok yakın olduğu ve iç içe geçen fikirlerin bulunduğu değerlendirilmektedir.”¹¹¹

Mühlen, bilgisayar suçlarını, “bilgisayarlara yöneltilen veya bilgisayarların araç olarak kullanıldıkları her türlü suç eylemi” şeklinde iki başlık altında tasnif etmektedir.¹¹²

Sieber, bilgisayar suçlarını, bilgisayar verilerinin değiştirilmesi, veri casusluğu ve program korsanlığı, bu alanda yapılan sabotajlar ve sistemlere yetki dışı girilmesi şeklinde sıralamaktadır.¹¹³

Sarzana ise sınıflandırmasını, bilgisayar suçlarını üç alt kategoriye ayırarak yapmaktadır. Birinci kategoriye bilgisayar marifetiyle maddi yarar sağlamaya yönelik suçları, ikinci kategoriye bilgisayar sistemlerinin ve verilerin tahribine yönelik suçları, son kategoriye ise bilgisayar marifetiyle kişi ve toplumların fiziki varlıklarına yönelik filleri dahil etmektedir; Bu sınıflandırmaya göre;¹¹⁴

- Birinci kategorideki suçlar: bilgisayar veri ve program unsurlarına yönelik hırsızlıklar, hizmet hırsızlıkları, maddi menfaat elde etmeye yönelik hırsızlıklar, mali suçlar,
- İkinci kategorideki suçlar: endüstriyel sabotajlar, siyasi sabotajlar, Vandalizm,
- Üçüncü kategorideki suçlar ise: yok etme ve tahrip, katliamlar ve tehditlere ilişkin fillerdir.

Türkiye’de de hukukçular tarafından bilişim suçlarının sınıflandırılmasına yönelik çabalar bulunmaktadır. Aydın, bilişim suçu tanımlarını iki ayrı düzeyde incelemektedir. Bu açıdan Mühlen ile benzer şekilde “bilişim sistemlerine karşı işlenen suçlar” ve “bilişim sistemleri ile işlenen suçlar” ayırımını yapmaktadır. Ayrıca

¹¹¹ Yazıcıoğlu, a.g.e., s.143.

¹¹² Rainer A.H. Mühlen, **Computer-Kriminalität, Gefahren und Abwehrmaßnahmen, Neuwied/Berlin**, (Hermann Luchterhand Verlag), 1973, s.17., akt: Değirmenci, a.g.e., s.61.

¹¹³ Yazıcıoğlu, a.g.e., s.144.

¹¹⁴ Carlo Sarzana, *Profilo giuridico e criminologico delgi illeciti informatici*, Computer crime, virus, hackers, Buffetti, Roma, 1989, s.45., akt.: Yazıcıoğlu, a.g.e., s.145.

aşağıdaki eylemlerin de bilişim suçu kapsamında değerlendirilmesi gerektiğini ifade etmektedir;¹¹⁵

- İzinsiz olarak bilgisayarda bulunan kişisel dosyanın açılması,
- Bilgi hırsızlığına karşı koruma ile ilgili kanunların ihlal edilmesi,
- Kişisel bilgilerin verilmesi ve bilgi tecavüzü.

Önder, bilgisayarın araç olarak kullanıldığı suçları, bilgisayarın araç olarak kullanıldığı mala karşı suçlar, kişiye karşı suçlar ve topluma ait haklar üzerinde işlenmiş suçlar olmak üzere üç başlık altında toplamaktadır.¹¹⁶

İnanıcı da Aydın ile benzer şekilde ikili bir ayrıma gitmekte ve bilgisayar suçlarını bilişim suçları başlığı altında “bilişim sistemine karşı işlenen suçlar” ve “bilişim sistemi ile işlenen suçlar” olmak üzere sınıflandırmaktadır. Bu sınıflandırmaya göre;¹¹⁷

- Bilişim sistemine karşı işlenen suçlar: bilişim sisteminin kendisine karşı işlenen suçları, bilişim sistemindeki program ve verilere (bilgilere) karşı işlenen suçları ve bilgisayar kullanıcılarına karşı işlenen suçları,
- Bilişim sistemi ile işlenen suçlar: bilgisayarla işlenen ekonomik suçları, bilgisayarla işlenen sahtecilik suçlarını, bilgisayarla işlenen ahlaki suçları, bilgisayarla işlenen şahsi haklara tecavüz suçlarını içermektedir.

Ersoy ise benzer şekilde, bilişim sistemleri ile işlenen suçlar, bilişim sistemlerine karşı suçlar ve bilişim araçlarına karşı suçlar olmak üzere üç başlıklı bir sınıflandırma yapmaktadır.¹¹⁸

Bunlara ilaveten bilişim suçlarını “siber suç” başlığı altında suçun amacına, hedefine, işlenen suç tipine ve bilgisayarın suçta oynadığı role göre çoklu sınıflandırmaya tabi tutan yaklaşımlar da bulunmaktadır. Buna göre siber suçları;¹¹⁹

¹¹⁵ Emin D. Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yay., 1992, s.51, akt.: Değirmenci, **a.g.e.**, s.66.

¹¹⁶ Ayhan Önder, **Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar**, İstanbul, 1994, s.506. akt.: Değirmenci, **a.g.e.**, s.67.

¹¹⁷ Haluk İnanıcı, “Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü”, **İstanbul Barosu Dergisi**, C. 70, S. 7-8-9, 1996, s.514., akt.: Yazıcıoğlu, **a.g.e.**, s.147.

¹¹⁸ Yüksel Ersoy, “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”, **AÜSBFD**, C.49, S. 3-4, 1994, s.160., akt.: Yazıcıoğlu, **a.y.**

- Suçta bilgisayarın oynadığı role göre: bilgisayarın araç olarak kullanıldığı, bilgisayarın hedef olduğu ve bilgisayarın ikinci derecede kullanıldığı suçlar,
- Suçun hedefine göre: veri temelli (data-related) suçlar, ağ temelli (network-related) suçlar, erişim suçları, ilgili bilgisayar temelli suçlar, donanıma yönelik ve yazılıma yönelik suçlar,
- Suçun amacına göre: bilgisayar sistemlerine ve servislerine yetkisiz erişim, bilgisayar sabotajı, bilgisayar yoluyla dolandırıcılık, kanunla korunmuş bir yazılımın izinsiz kullanımı ve yasadışı yayınlar vb. şeklinde sınıflandırmak mümkündür.

Benzer bir sınıflandırmayı Kurt ise “bilişim suçları” ana başlığını kullanarak dört ayrı kategoride yapmıştır. Bu sınıflandırmaya göre bilişim suçları;¹²⁰

- Veri suçları: verilerin durdurulması, verilerin değiştirilmesi, verilerin çalınması,
- Ağ suçları: ağ engellemesi ve ağ sabotajı,
- Yetkisiz giriş suçları: bilişim sistemlerine izinsiz giriş, virüs yayılması,
- İlgili suçlar: bilgisayar yoluyla sahtecilik ve bilgisayarla bağlantılı dolandırıcılıklardan oluşmaktadır.

Çalışmanın inceleme konusu olan Avrupa Konseyi Siber Suçlar Sözleşmesi ise “siber suçlar” genel başlığını kullanmak suretiyle, dört ana kategori halinde sınıflandırma yapmayı uygun görmüştür. İleriki bölümlerde detaylı olarak incelenecek olması nedeniyle, kısaca bu dört kategorinin yukarıda yapılan sınıflandırma çalışmaları ile paralel olduğu değerlendirilmektedir. Siber Suçlar Sözleşmesine göre bu suçlar;¹²¹

- Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar,
- Bilgisayarlarla ilişkili suçlar,

¹¹⁹ Onur Şehitoğlu, “Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Mücadelenin Hukuksal ve Güvenlik Boyutu”, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2005, s.27-31.

¹²⁰ Kurt, a.g.e., s.77-84.

¹²¹ Avrupa Konseyi Siber Suçlar Sözleşmesi, “Convention on Cybercrime”, Council of Europe, (Çevrimiçi), <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, 10 Ekim 2006.

- İçerikle ilgili suçlar,
- Telif haklarının ve benzer hakların ihlaline ilişkin suçlardır.

Görüldüğü üzere bilişim suçlarının sınıflandırılması konusunda farklı yaklaşımlar bulunmaktadır. Bu yaklaşımları daha da artırmak mümkündür. Bazı sınıflandırma çabaları suçları, fiilin yöneltildiği hedefe, bazıları failin elde etmek istediği amaca, bazıları bilgisayarların suçta oynadığı role göre, diğerleri ise korunan kanuni hakkı gözetererek ele almıştır. Dolayısıyla bu sınıflandırmaların yalnızca farklı bakış açılarından kaynaklandığı değerlendirilebilir. Bilişim alanının sürekli teknolojik gelişmelerin yaşandığı dinamik bir alan olması, gelecekte yeni suç türlerinin ortaya çıkmasını mümkün kılmaktadır. Bu nedenle, yeni gelişebilecek suçlarla birlikte bu sınıflandırma çabalarına yenilerinin ekleneceği ifade edilebilir.

3. SİBER TERÖR KAVRAMI

Bilişim teknolojisinde yaşanan hızlı gelişmenin sonuçlarından birisi de özellikle 11 Eylül saldırıları sonrasında oluşan korku ve panik ortamıyla birlikte gündeme getirilen siber terör tehdididir. Kavram günümüzde dünya çapında medyanın, güvenlik çevrelerinin ve bilgi teknolojisi uzmanlarının ilgisini çekmektedir. Bazı gazeteciler, politikacılar ve uzmanlar siber teröristlerin bilgisayar altyapılarına müdahale ederek barajlardan trafik sistemlerine kadar birçok altyapıya zarar verebileceklerini ileri sürmektedirler. Bugüne kadar resmi kayıtlara geçmiş tek bir siber terörizm örneği bulunmamakla birlikte,¹²² siber terörizmin milyonların yaşamını engelleyebileceği ve küresel güvenliği tehdit edebileceği yönündeki felaket senaryoları oldukça popüler hale gelmiştir.

Teknolojiye bağımlı ülkelerin felaket senaryolarında, doğal afetlerden dahi ön sırada yer alan siber terörün tanımını yapmanın ve gerçekte ne derecede bir tehdit teşkil ettiğini belirlemenin, somut tedbirler alınması açısından da oldukça önemli olduğu değerlendirilmektedir.

“Siber terör” kavramı günümüzde çok sık kullanılıyor olmasına karşın, basit bilgisayar suçlarının “siber terör” adı altında tanımlanmasının doğruluğuna ilişkin yeterince kanıt ya da ispatlanmış olay bulunmamaktadır. Popüler kullanımına karşın, aynı şekilde hangi eylemlerin “siber terör” kavramı içerisinde değerlendirilebileceği üzerine de uzlaşma mevcut değildir. Kavram ilk olarak 1980’lerde Barry Collin

¹²² Atilla Sandıklı, Gökhan Yıvcı, TASAM Siber Terörizm Raporu, Stratejik Rapor, No:2, s.3.

- İçerikle ilgili suçlar,
- Telif haklarının ve benzer hakların ihlaline ilişkin suçlardır.

Görüldüğü üzere bilişim suçlarının sınıflandırılması konusunda farklı yaklaşımlar bulunmaktadır. Bu yaklaşımları daha da artırmak mümkündür. Bazı sınıflandırma çabaları suçları, fiilin yöneltildiği hedefe, bazıları failin elde etmek istediği amaca, bazıları bilgisayarların suçta oynadığı role göre, diğerleri ise korunan kanuni hakkı gözetererek ele almıştır. Dolayısıyla bu sınıflandırmaların yalnızca farklı bakış açılarından kaynaklandığı değerlendirilebilir. Bilişim alanının sürekli teknolojik gelişmelerin yaşandığı dinamik bir alan olması, gelecekte yeni suç türlerinin ortaya çıkmasını mümkün kılmaktadır. Bu nedenle, yeni gelişebilecek suçlarla birlikte bu sınıflandırma çabalarına yenilerinin ekleneceği ifade edilebilir.

3. SİBER TERÖR KAVRAMI

Bilişim teknolojisinde yaşanan hızlı gelişmenin sonuçlarından birisi de özellikle 11 Eylül saldırıları sonrasında oluşan korku ve panik ortamıyla birlikte gündeme getirilen siber terör tehdididir. Kavram günümüzde dünya çapında medyanın, güvenlik çevrelerinin ve bilgi teknolojisi uzmanlarının ilgisini çekmektedir. Bazı gazeteciler, politikacılar ve uzmanlar siber teröristlerin bilgisayar altyapılarına müdahale ederek barajlardan trafik sistemlerine kadar birçok altyapıya zarar verebileceklerini ileri sürmektedirler. Bugüne kadar resmi kayıtlara geçmiş tek bir siber terörizm örneği bulunmamakla birlikte,¹²² siber terörizmin milyonların yaşamını engelleyebileceği ve küresel güvenliği tehdit edebileceği yönündeki felaket senaryoları oldukça popüler hale gelmiştir.

Teknolojiye bağımlı ülkelerin felaket senaryolarında, doğal afetlerden dahi ön sırada yer alan siber terörün tanımını yapmanın ve gerçekte ne derecede bir tehdit teşkil ettiğini belirlemenin, somut tedbirler alınması açısından da oldukça önemli olduğu değerlendirilmektedir.

“Siber terör” kavramı günümüzde çok sık kullanılıyor olmasına karşın, basit bilgisayar suçlarının “siber terör” adı altında tanımlanmasının doğruluğuna ilişkin yeterince kanıt ya da ispatlanmış olay bulunmamaktadır. Popüler kullanımına karşın, aynı şekilde hangi eylemlerin “siber terör” kavramı içerisinde değerlendirilebileceği üzerine de uzlaşma mevcut değildir. Kavram ilk olarak 1980’lerde Barry Collin

¹²² Atilla Sandıklı, Gökhan Yıvcı, TASAM Siber Terörizm Raporu, Stratejik Rapor, No:2, s.3.

tarafından ortaya atılmış ve yakın geçmişte “kendinizi siber teröristlerden koruyun”, “siber terörizme karşı güvende olduğunuzdan emin olun” gibi ifadeler sıkça kullanılmıştır.¹²³

Siber terör kavramını anlamak ve bir tanımını ortaya koymak için öncelikle bileşenleri olduğu değerlendirilen siber suç ve terör kavramlarını incelemenin doğru bir yaklaşım olacağı değerlendirilmektedir. Siber suç kavramı daha önceki bölümlerde açıklanmaya çalışıldığından bu bölümde tekrar ele alınmamıştır. Ancak, siber suç kavramında karşılaşılan tanım birliği probleminin, terör kavramı için de geçerli olduğu ifade edilebilir. Bu nedenle, terörün tanımını yapmak için öncelikle daha önceden yapılmış tanımları incelemenin, ortak noktalarını bulmanın ve bu tanımlar üzerinden bir sonuca varmanın doğru olacağı değerlendirilmektedir.

Çeşitli kaynaklarda farklı ancak birbirine yakın tanımlara rastlamak mümkündür. ABD Savunma Departmanının tanımına göre terör;¹²⁴

“genelde siyasi, dini ya da ideolojik amaçlara ulaşmak maksadıyla; hükümetlere ya da toplumlara baskı yapmak ve zorlamak için kişilere ya da mala karşı belirli suç teşkil eden bir fiilin işlenmesi ya da böyle bir fiilin işleneceğine dair yapılan tehdittir.”

FBI tarafından teröre getirilen tanım da yukarıda ile benzeşmektedir. Buna göre terör;¹²⁵

“bir hükümet, sivil toplum ya da bunların herhangi bir kısmına siyasi ya da sosyal amaçlara ulaşmak maksadıyla; baskı yapmak ve zorlamak için kişi ya da mala karşı kanunsuz bir şekilde güç ve şiddet kullanımıdır.”

Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesinde, terörün tanımı yapılmamakla birlikte, taraf olan tüm ülkelerin diğer bazı Avrupa Konseyi Sözleşmelerindeki suikast, rehin alma, terörist bombalı saldırıları, terörün finansmanı ve uçak kaçırma gibi suçları ana terör suçları olarak kabul etmeleri ve bu suçlarla ilgili iade taleplerini yerine getirmeleri öngörülmektedir.¹²⁶

¹²³ Sarah Gordon, Richard Ford, “Cyber Terrorism?”, (Çevrimiçi), <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>, 12 Kasım 2006.

¹²⁴ Department of Defense Education Activity Internal Physical Security. Department of Defense. DoD EA Regulation 4700.2, (Çevrimiçi), http://www.dodea.edu/foia/iod/pdf/4700_2.pdf, 24 Aralık 2006.

¹²⁵ Code of Federal Regulations. 28 CFR. Section 0.85 on Judicial Administration, FBI, (Çevrimiçi), http://www.fbi.gov/publications/terror/terror2000_2001.htm, 24 Aralık 2006.

¹²⁶ Ayrıntılı Bilgi İçin Bkz.: Council of Europe Convention on the Prevention of Terrorism, Council of Europe, <http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm>.

Birleşmiş Milletler Genel Konseyi tarafından da teröre oldukça benzer bir tanımlama getirilmiştir. Konseyin ifadesi ile terör;¹²⁷

“toplumda bir terör ortamı yaratmak maksadıyla; bir insan gurubu ya da belli insanlar tarafından siyasi amaçlarla girşilen ya da niyet edilen ve haklı görölmesini sağlamak için politik, felsefi ideolojik, ırkçı, etnik, dini ya da diğer kavramlar kullanılabilen; ancak hiçbir şart altında haklı görölmemeycek suç teşkil eden davranışlardır.”

12 Nisan 1991 tarihli Terörle Mücadele Kanunu’nda ise terör aşağıdaki şekilde tanımlanmıştır;¹²⁸

“cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değıştirmek, devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girşilecek her türlü suç teşkil eden eylemler.”

Terörle ilgi tanımlar ve terör olayları incelendiğinde, farklılıklar olmasına rağmen ortak noktalarda birleştiğı görölmektedir. O halde ortak noktalara bakmak kavramın anlaşılmasını için yardımcı olabilir.

Tanımlarda;

- Siyasi, ideolojik, ırkçı, etnik veya dini bir amacı başarma niyeti taşıması,
- Her türlü yolla şiddet yaratmaya çalışılması,
- Korku ve dehşet oluşturarak düşman ya da düşman olarak görölenin bir şeye zorlanması ya da gözdağı verilmesi,
- Gerçek ve yakın bir bölme parçalama ya da ölüm tehdidi içermesi,¹²⁹

Eylemlerde ise,

¹²⁷ Susan Tiefenbrun, “A Semiotic Approach to a Legal Definition of Terrorism”, *ILSA Journal of International & Comparative Law*, C.IX, s.384,

¹²⁸ Terörle Mücadele Kanunu, 1991, Madde 1., Ayrıntılı Bilgi İçin Bkz.: <http://www.mevzuat.adalet.gov.tr>.

¹²⁹ Tiefenbrun, a.g.e., s.362.

- Masum sivillerin hedeflenmesi,
- Şiddet yaratma niyeti ya da eylemin sonuçlarını mantıksız bir şekilde göz ardı edilmesi,
- Saldırının psikolojik etki yaratması,
- Güven ya da inancın yok edilmesi,
- Uzun soluklu sonuçlar doğurması,
- Kurtulan şahıslarda terörün ölümcül olduğu fikri oluşturulması¹³⁰ ortak noktalardır.

Burada önem teşkil eden bir diğer nokta da incelenen terör tanımlarında genelde eylemin bir hükümet, bir topluma ya da toplumun bir kesimine yöneltilmesi ifadelerinin yer almasıdır. Ancak, hükümetlerin meşruluğunun herkes, hatta her ülke tarafından kabul edilmemesi, meşruluğun tartışılabilir bir konu olmasına neden olmaktadır. Dolayısıyla genel tanımlarda, hükümet ya da meşru yönetim gibi ifadelerin kavramı daha kapsayıcı hale getirmek yerine sınırlandırabileceği ve bazı eylemlerin terör tanımı dışında kalmasına neden olabileceği değerlendirilmektedir.

Yukarıdaki bilgiler ışığında bir suçun siber terör tanımına uyabilmesi için hem siber suç hem de terör tanımlamasındaki ortak noktaları taşıması gerektiği ifade edilebilir. Kısaca, işleniş biçimi açısından bir siber suç, amaç ve sonuçları bakımından ise terör suçu özelliği taşımalıdır. Siber terör kavramının da birçok tanımı bulunmaktadır.

FBI siber terörizmi aşağıdaki şekilde tanımlamaktadır;¹³¹

“etnik guruplar ya da gizli ajanlar tarafından yapılan önceden tasarlanmış, siyasi motivasyonlu, savaş dışı hedeflere karşı şiddetle sonuçlanan enformasyon, bilgisayar sistemleri, bilgisayar programları ve verilerine yöneltilen saldırılardır.”

Kavramın, “enformasyon teknolojisi ve vasıtalarının terörist guruplar ve ajanlar tarafından kullanılması”¹³² veya;¹³³

¹³⁰ Tiefenbrun, a.y.

¹³¹ U.S. Departman of Justice İnternet sayfası, (Çevrimiçi), <http://www.cybercrimes.net/Terrorism/ct.html>, 29 Aralık 2006.

“hayat kaybı ve ağır ekonomik zararı içeren ancak bununla sınırlı olmayan ciddi zarara sebep olmak amacıyla siyasi motivasyonlu olarak kullanılan bilgisayar korsanlığı teknikleri”

gibi daha dar kapsamlı ve yüzeysel olduğu değerlendirilen tanımları da mevcuttur. Siber terör amaç ve araç bakımından ise;¹³⁴

“korku yaratmak veya halkın temel kamu kurumlarına olan inancını sekteye uğratmak amacıyla bilgi veya hizmet akışında kitlesel bir yıkıma neden olmak için bilgisayar kodlarını ve ilgili aygıtları kullanmak”

şeklinde tanımlanmaktadır. Siber uzay teknolojileri ve güvenlik uzmanı olan Prof. Dorothy E. Denning’e göre ise siber terör;¹³⁵

“siber uzay ve terörizmin bileşimidir. Siber terör denince genellikle bilgisayarlara, ağlara ve buralarda saklanan bilgiye yöneltilen yasa dışı saldırı ve saldırı tehditlerinin siyasi ya da sosyal amaçlara ulaşmak için bir hükümet ya da çalışanlarına baskı yapmak ve gözdağı vermek maksadıyla yapılması anlaşılmaktadır. Daha da ötesi siber terörizm olarak tanımlanabilmesi için bir saldırının kişiler ya da mala karşı şiddetle sonuçlanması ya da en azından korku yaratacak kadar zarar verici olması gerekmektedir. Ölümle ya da yaralanma ile sonuçlanan saldırılar, patlamalar, uçak kazaları, su kirlenmeleri veya ciddi ekonomik kayıplar örnek olarak verilebilir. Kritik altyapı sistemlerine karşı yapılan saldırılar etkilerine bağlı olarak siber terörizm olarak adlandırılabilir. Önemsiz servisleri etkileyen saldırılar ve rahatsızlıklar siber terörizm olarak tanımlanamaz”

Buradan yola çıkarak bir suçun siber terör kapsamında değerlendirilebilmesi için,

- Siyasi, ideolojik, ırkçı, etnik veya dini bir amacı başarma niyeti taşıması,
- Bir yönetimi istenileni yapmaya zorlamayı veya gözdağı vermeyi amaçlaması,

¹³² Deborah H. Juhnke, “Cyber Terrorism or Cyber Crime”, s.1., (Çevrimiçi), <http://www.forensics.com/pdf/Cyber.pdf>, 29 Aralık 2006.

¹³³ Paul Larisa, “When Cyber Hacktivism Meets Cyberterrorism.”, Jan. 2001, (Çevrimiçi), <http://rr.sans.org/hackers/terrorism.php>, 11 Kasım 2006.

¹³⁴ Olivia Bosch, “Teknoloji ve Uluslararası Güvenlik Stratejileri”, Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, s.68.

¹³⁵ Dorothy E. Denning, “Cyberterrorism”, 23 Mayıs 2000, Georgetown University, (Çevrimiçi), <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>, 20 Ekim 2006.

TASNİF DIŞI

- Suç aracının bir bilgisayarla/bilişim sistemi olması,
- Suçun bir bilgisayarla/bilişim sistemine karşı işlenmiş olması,
- Suç aracı ya da amacı olan bir bilgisayarla/bilişim sisteminin siber uzayın bir bileşeni olması,
- Ciddi fiziki hasara yol açacak veya insan hayatını tehlikeye sokacak şekilde kritik altyapı sistemlerini hedef alması,
- Masum sivillerin hedeflenmesi, eylemin sonuçlarının mantıksız bir şekilde göz ardı edilmesi,
- Hedef toplum üzerinde korku ve dehşet yaratması,
- Suçun bir terör örgütü tarafından ya da terör örgütü adına işlenmiş olması gerektiği sonucuna ulaşılabilir.

Siber terör ile siber suç arasındaki farkı saldırganın temel motivasyon ve niyetinin oluşturduğu şeklinde görüşler de mevcuttur. Ancak, kamusal bir web sayfasına girerek bir terör örgütü propagandasını yerleştiren teröristin eylemini, sırf maksadı ya da terör örgütü üyesi olması nedeniyle siber terör olarak tanımlamanın uygun olmayacağı ifade edilebilir. Zira bu basit bir bilişim suçundan başka bir şey değildir. Çünkü etkisi bakımından bir terör eylemi ile benzeşmemektedir.

Bununla birlikte, terör örgütlerince yapılan yasadışı yayınları farklı değerlendirmek doğru olacaktır. İnternet aracılığıyla herhangi bir terör örgütünün propaganda yapması, adam devşirmeye yönelik faaliyetlerde bulunması, teröre mali destek sağlamak amacıyla yapılan sahtekârlık ve dolandırıcılık eylemleri ya da bomba yapımı, silahlı saldırı vb. terör suçu işlemeye yönelik eğitim amaçlı yayınların da siber terör kavramı içinde değerlendirilmesi yanlış olmayacaktır. Nitekim Türkiye de dahil 33 ülkenin imzaladığı ve Haziran 2007’de uygulamaya girecek olan Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesi’nde terörizm için adam devşirme ve terörizm amaçlı eğitim de terör suçu haline getirilmektedir.¹³⁶

Sonuç olarak siber terörün “siyasi, sosyal ve ideolojik hedeflerin elde edilmesi maksadıyla; bir terör örgütü tarafından gerçekleştirilen, toplumda dehşet ve korku yaratan, hedefi bilişim sistemleri tarafından kontrol edilen kritik altyapı sistemleri

¹³⁶ Ayrıntılı Bilgi İçin Bkz.: Council of Europe Convention on the Prevention of Terrorism, 6. ve 7. Maddeleri, (Çevrimiçi), <http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm>, 12 Şubat 2007.

veya bizzat kritik bilişim sistemleri, aracı ise yine bilişim sistemleri olan, etkisi bakımından klasik bir terör eylemine eşdeğer sonuçlar yaratan her türlü yasadışı saldırı ve saldırı tehdididir.” şeklinde tanımlanabileceği değerlendirilmektedir.

İnternetin teröristler tarafından iletişim amaçlı kullanımı, basit bilgisayar korsanlığı eylemleri, bilgisayarların elektronik parçalarının çeşitli el yapımı patlayıcıların ateşleyicisi olarak kullanılmaları ve klasik terör eylemlerini destekleyen bilgi toplama, planlamaya yardım ve bunun gibi faaliyetler ise siber terör kapsamında düşünülmemelidir.

4. SİBER SUÇLARLA MÜCADELEDE KARŞILAŞILAN GÜÇLÜKLER

İnternetin suçların soruşturulması ve kovuşturulması açısından ciddi güçlükler oluşturan iki temel karakteristiği bulunmaktadır. İlki yapısal açıdan İnternet’in ulusal sınırlardan bağımsız bir karakter göstermesi ve böylece küresel boyutta benzersiz bir bilgisayar sistemi oluşturmasıdır. Uluslararası hukukun geleneksel prensiplerine göre, ülkelerin sadece egemenlikleri altındaki bölgelerde yargılama yetkisine sahip oldukları kabul edilmektedir. Bu nedenle, küresel bir boyuta sahip olan siber suçlar ile ulusal sınırlarla bağlı usul hukuku uygulamaları arasında bir uyumsuzluk yaşanmaktadır.¹³⁷

Teknik açıdan ise sistemin işleyişi, iletilen bilginin geçici olmasını ve verilerin kısa sürede değişmesini gerektirmektedir. Veriler saniyeler içerisinde düzeltilebilir, taşınabilir veya değiştirilebilir. Buna rağmen kolluk kuvvetlerince usul hukukunun soruşturma ve kovuşturmaya yönelik tedbirlerini uygulamaya koymak hatırı sayılır bir zaman süreci gerektirmekte ve bu durum siber suçlarla mücadele de en önemli güçlüğü teşkil etmektedir.¹³⁸

a. İnternet’in Çalışma Prensibi

Siber suçlarla mücadelede karşılaşılan güçlüklerin anlaşılabilmesi için İnternet’in çalışma prensibinin çok kısa ortaya konulması faydalı olacaktır. İnternet’in tanımında da belirtildiği üzere İnternet, bilgisayarların çeşitli haberleşme sistemleri sayesinde birbirlerine bağlanması ile oluşan büyük bir ağıdır.

¹³⁷ Daniele Cangemi, “Procedural Law Provisions of The Council of Europe Convention on Cybercrime”, *International Review of Law Computers & Technology*, Vol. XVIII, No:2, July 2004, s.167.

¹³⁸ A.y.

b. Teknik ve Yasal Güçlükler

İnternet hizmeti, faturalandırma amacıyla etkili bir kayıt sistemine sahip telefon hizmetlerinin aksine, kullanıcı davranışlarını ya da kullanıcının yaptığı işlemleri kayıt ve takip etmek üzere tasarlanmamıştır. İnternet hizmetinin ücretlendirilmesinde bağlantı süresi ve kapasitesi ya da indirilen bilgi miktarı esas alınmaktadır. İnternet'in ilk kuruluş amacı üniversitelerde görevli araştırmacıların meslektaşlarıyla rahat bir şekilde bilgi alışverişi yapmalarını sağlamak olduğundan, önemli olan bilginin paylaşımı ve diğerlerinin istifadesine sunulmasıdır. Bu nedenle, başlangıçta güvenilir bir topluluk tarafından kullanıldığı değerlendirilen İnternet için teknik anlamda kapsamlı güvenlik tedbirleri alınmasına ihtiyaç görülmemiştir. Basit düzeyde parola kullanımı ile güvenlik sağlanacağı değerlendirilmiştir. Bu bakış açısı nedeniyle kötü niyetli kullanıcıları takip ve tespit etmeyi sağlayacak önlemler başlangıçta tasarlanmamış ve daha sonra da geliştirilmemiştir.¹⁴¹

Bir siber suçun failini tespit edebilmek için öncelikle suçlunun yerini bulmak yani saldırı kaynağının IP adresini tespit etmek gerekir. Bunun için izlenen yöntem hedeften geriye, saldırının kaynağına doğru yönlendiriciler arasındaki "hop"ları takip etmektir. Yönlendiriciler, İSS'ler tarafından kontrol edilir. Bu nedenle İSS'ler, çoğunlukla saldırganın izini sürmek için gerekli bilgiyi sağlayabilir. Bu metotla geriye doğru, mağdurun bilgisayarına saldırıda bulunan faille hizmet sağlayan son İSS belirlenerek, failin kimliği, telefon numarası, aradığı numaralar, cihaz türü, mobil kullanıcı ise saldırı esnasında bulunduğu konum elde edilebilir. Fail ve kullanılan cihaz belirlendikten sonra, ikinci adım saldırı aracı olarak kullanıldığı düşünülen bilgisayarın delil elde etmek amacıyla bir adli bilişim uzmanı tarafından incelenmesidir. Bu inceleme tespit edilen failin gerçek suçlu mu, yoksa bilgisayarının kontrolü habersiz bir şekilde ele geçirilerek başka biri tarafından suç aracı olarak kullanılan bir diğer mağdur mu olduğunun belirlenmesini sağlar. Bu inceleme için bilgisayarın içerisinde bulunan tüm verilerin birebir kopyasının alınması gerekir. Bu kopya "imaj" olarak adlandırılır ve daha önce silinmiş dosyalar ve dosya parçacıkları dahil bilgisayarın sabit diskini tam bir kopyası anlamına gelir. Bu sayede belli bir dosyanın ilk yaratıldığı andan itibaren silinmiş olanlarda dahil tüm versiyonlarını

¹⁴¹ Howard F. Lipson, **Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues**, Pittsburgh, Carnegie Mellon University, 2002, s.13.

yeniden yaratmak mümkün olur. Böylece fail saldırı izlerini yok etse dahi bunların büyük bölümü ortaya çıkarılarak, delil elde edilmiş olur.¹⁴²

Ancak bu süreçte, hem yasal hem de teknik güçlüklerle karşılaşılabilmekte ve bir anlamda failin tespit edilmesi de güçleşmektedir. Öncelikle, İSS'ler verilerin korunmasına yönelik kanunlar nedeniyle, ellerinde bulunan "log" bilgilerini gönüllü olarak açıklayamamaktadır. Bu bilgilerin elde edilebilmesi için yasaların buna imkân tanınması gerekir. Yasal olarak bu imkân var olsa dahi, bu bilgilerin açıklanması için ayrıca bir mahkeme kararı da gerekebilir. İlk İSS'den elde edilecek bilgiler, eğer iletişim sürecine başka İSS'ler dahil olmuşsa doğrudan faile değil, başka bir İSS'ye ulaşılmasını sağlamaktadır. Bu durumda yasal sürecin diğer İSS'ler için de tekrarlanması gerekir. Aynı şekilde saldırıda bulunduğu tespit edilen bilgisayarın incelenmesi, kopya alınması, dosya içeriklerine ulaşılabilmesi, şifre, parola ya da benzeri detayların elde edilebilmesi için de yasal düzenlemelerin bulunması gerekir. Klasik anlamda arama ve el koyma olarak değerlendirilebilen bu eylemlerin mahkeme kararına dayandırılmasına da ihtiyaç duyulabilmektedir.¹⁴³

Bunun yanında yasal mevzuat etkin ve hızlı bir reaksiyona imkân sağlasa dahi, İnternet'in tasarımı ve kaynaklanan açıklar da iz sürmeyi güçleştirebilmektedir. İnternet'in, güvenilir bir kullanıcı gurubuna hizmet edeceğinin düşünülmesi nedeniyle, IP paketleri içerisindeki bilgilerin orijinal halinin korunmasına yönelik hiç bir şifreleme önlemi alınmamıştır. Bu nedenle ileri seviyede bilgi sahibi bir kullanıcı, IP paketleri içerisindeki bilgileri isteği gibi değiştirebilir. Özellikle kaynak adresini değiştirerek çıkış noktasını gizleyebilir. Bunun için yapılması gereken, IP paketindeki kaynak adresine yanlış bir adres yerleştirmektir. Diğer bir yöntem ise saldırıda bulunmadan önce, Truva atı yerleştirme yöntemi ile bir grup bilgisayar ele geçirmektir. Ele geçirilen bu bilgisayarlar saldırı için atlama taşı olarak kullanılır. Böylece saldırı kaynağının ele geçirilen bilgisayarlar olarak görülmesi sağlanır.¹⁴⁴ Saldırganlar bunun dışında kendilerini gizlemek için kullanıcının IP adresini gizleyen ve genel olarak "anonimleştirici" adı verilen İnternet sitelerini de kullanabilmektedir. Bu siteler kullanıcı ile bağlanmak istediği İnternet siteleri arasında bir aracı olarak hizmet vermektedirler.¹⁴⁵

¹⁴² Anthony Riem, "To Catch a Cyber Thief: Tracing Internet Crime", *The In House Lawyer*, March 2007, s.44.

¹⁴³ A.y.

¹⁴⁴ Lipson, a.g.e., s.13.

¹⁴⁵ A.y.

Bunlara ilave olarak bir saldırganın IP adresi tespit edilse dahi, kendisinin tespit edilmesi her zaman mümkün olmamaktadır. İnternet'in hızla yayılması ve kullanıcı miktarının artması, kısıtlı olan IP adresleri nedeniyle İnternet'e bağlanan her bilgisayara ya da kullanıcıya sabit bir IP adresi verilmesini engellemektedir. Bu nedenle, Dinamik IP kullanımına geçme ihtiyacı duyulmuştur. Bu uygulamada kullanıcılara İnternet'e her bağlantılarında İSS'nin elindeki IP adresi gurubunda bulunan ve o an için kullanılmayan bir IP adresi atanmaktadır. Dinamik IP adresi kullanıcı İnternet'e bağlı kaldığı sürece sabit kalmakta, ancak bağlantısını kesip yeniden bağlandığında büyük bir olasılıkla yeni bir IP adresi atanmaktadır. Bu durumda bir saldırganın bulunabilmesi, tespit edilen IP adresini saldırının gerçekleştiği zaman dilimi içerisinde kimin kullandığının belirlenmesine bağlıdır. Bu da ancak İSS'nin söz konusu log kayıtlarını tutmasına bağlıdır.¹⁴⁶ İnternet trafiğindeki yoğunluk nedeniyle, İSS'ler hizmet verdikleri tüm kullanıcılara ait bağlantı bilgilerini depolama kapasitesine ya da bu kapasiteyi oluşturabilecek mali imkânlarla sahip değildir. Bu nedenle, en azından depolanan log bilgilerinin üzerlerine yenileri yazılmadan önce çok hızlı bir biçimde korunması, suçun takibi için hayati önem taşımaktadır.¹⁴⁷

Klasik yöntem olan IP adresi takibi ile suçlunun tespit edilmesi konusunda yaşanan bir diğer güçlük "öde ve git" adı verilen servis sağlayıcılar ve kablosuz iletişimin yaygınlaşmasından kaynaklanmaktadır. "Öde ve git" tarzı İnternet hizmeti, tıpkı kontrollü telefon kartları gibi önceden ödeme yapılarak belli bir İnternet erişim süresinin satın alındığı İnternet erişim kartlarıdır. Bu uygulamada geleneksel İnternet kullanım sözleşmelerine benzer bir sorumluluk veya uzun süreli bir sözleşme mevcut değildir. İSS hiçbir kimlik bilgisine ihtiyaç duymamakta ya da çok az bilgi talep etmektedir.¹⁴⁸ Buna rağmen bu durum saldırganın kesinlikle bulunamayacağı anlamına gelmemekte, sadece daha uzun bir yasal süreç gerektirebilmektedir. Örneğin saldırganın ödemeyi kredi kartı ile yapması durumunda, ödeme bilgileri sayesinde izi sürülebilmektedir.¹⁴⁹ Ancak, saldırganın ödemeyi peşin para ile veya çalıntı bir kredi kartı ile yapması durumunda, İnternet'e neredeyse tam bir gizlilik içerisinde erişmesi mümkün olabilmektedir.¹⁵⁰

¹⁴⁶ A.y.

¹⁴⁷ Riem, a.g.e., s.44.

¹⁴⁸ Lipson, a.g.e., s.13.

¹⁴⁹ Riem, a.g.e., s.44.

¹⁵⁰ Lipson, a.y.

Siber suçlarda suçun gerçekleşme süresi, klasik suçların aksine bilgisayarların işlem hızları ile yani milisaniye, mikro saniye ve nano saniye gibi değerler ile ölçülmektedir. Teknoloji aynı anda birden çok suçun, birden çok kişiye karşı ve mağdurlarla temasa gerek kalmadan işlenebilmesine imkân sağlamaktadır.¹⁵¹ Klasik yöntemde suçla mücadelede var olan tepkisel strateji siber suçlar söz konusu olduğunda yarar sağlamamaktadır. Çünkü tepki genellikle suç işlendikten ve izler soğuduktan oldukça sonra başlamaktadır. Siber suçlarda saldırganın nadiren suç mahallinde bulunması nedeniyle, klasik suçların aksine suç hazırlığı, icrası ve kaçış esnasında yakalanma olasılığı da ortadan kalkmaktadır.¹⁵² Böylece siber suçlular çok hızlı bir şekilde suçu işlemeyi müteakip, gerçek kimlik ve yer bilgilerini açığa vurmadan kaçabilmektedirler.¹⁵³

Siber suçların elektronik ortamda oluşması nedeniyle bu suçlara ait deliller varsa elektronik ortamda bulunmakta ve çok kolay yok edilebilmektedir.¹⁵⁴ Siber suçlular suçu gerçekleştirdikten sonra sıklıkla izlerini saklamak, kaybettirmek ya da izlerini sürenleri yanlış yönlendirmek için elektronik ortamdaki sistem kayıtlarını değiştirmekte veya yok etmektedirler. Bunun için çok gelişmiş program ve araçları da kullanmaktadırlar. Dolayısıyla bazen takip edilecek bir iz bulmak, doğru izi takip etmek veya var olan izleri takip ederek gerçek suçluya ulaşmak güçleşmekte¹⁵⁵ ve bu sayede siber suçlular klasik suçlulara nazaran mükemmel bir şekilde kendilerini gizleme olanağına sahip olabilmektedirler.¹⁵⁶

Çeşitli suç tipleri bu suçlarla ilgili uzman personeli gerektirmektedir. Örneğin narkotik, cinayet, kaçıcılık gibi suç alanları, bu alanlarda eğitim almış ve uzmanlaşmış kolluk personeli gerektirmektedir. Bu açıdan bakıldığında siber suçlar nispeten çok daha yeni bir alandır ve bu nedenle birçok ülke bu konuda yetişmiş yeterince personele sahip değildir.¹⁵⁷ Ayrıca, bu personelin eğitimi uzun süreli bir yatırım ve yüksek maliyet gerektirmekte, özel sektörde daha yüksek gelir imkânı nedeniyle yetişmiş personelin elde tutmasında güçlükler yaşanmaktadır. Bir diğer problemde sürekli gelişen teknoloji ve suç teknikleri karşısında personelin

¹⁵¹ Şehitoğlu, a.g.e., s.256.

¹⁵² Susan W. Brenner, "Distributed Security: A New Model of Law Enforcement", *Journal of Internet Law*, C. VIII, No.5, Nov 2004, s.10.

¹⁵³ Ajmal Edappagath, "Cyber-Laws and Enforcements to Optimize Benefits of ICT", *I-Ways*, C.XXVII, No. 3/4, 2004, s.171.

¹⁵⁴ Brenner, a.g.e., s.10.

¹⁵⁵ Lipson, a.g.e., s.18.

¹⁵⁶ Brenner, a.y.

¹⁵⁷ Edappagath, a.g.e., s.171.

bilgilerinin güncel tutulmasındaki zorluktur.¹⁵⁸ Dolayısıyla bu durum, kolluk güçlerinin siber suçlarla mücadelesini olumsuz yönde etkileyebilmektedir.

Siber suçlarla mücadele eden kolluk güçlerinin karşılaştığı bir diğer zorluk da kriptolardır. Kripto ticari açıdan hassas bilgi ve haberleşmelerin korunması gibi yasal amaçlarla kullanıldığında faydalı bir uygulamadır. Ancak, yüksek nitelikli kriptolama ürünlerinin artması ve kullanılması suçla mücadelede büyük bir engel teşkil etmektedir. Bu ürünler kolluk görevlilerinin yasal bir şekilde suçla ilgili haberleşmelere, dosyalara ve depolanmış verilere ulaşmalarını engellemektedir. Piyasadan temin edilebilen kriptolama ürünlerinin suçlular ve teröristlerce suçla ilgili haberleşme ve diğer bilgileri gizlemek için kullanılması ihtimali, kamu güvenliği ve ulusal güvenlik için ciddi bir tehdit oluşturmaktadır.¹⁵⁹

İnternet hizmetlerinde ve kullanımındaki artış, aktarılan bilgi hacmindeki yoğunluk suçların ve suçluların tespitinde yaşanan bir diğer güçlüktür. Örneğin çocuk pornografisi ile ilgili İnternet trafiği yoğunluğu, bu tarz siteleri ziyaret eden her bir kişiyi tespit etmeyi ve izlemeyi imkânsız hale getirmektedir. Birçok suçlu yakalanma şanslarının oldukça uzak olduğunun bilincindedir.¹⁶⁰

Tüm suçlarda olduğu gibi İnternet ortamında gerçekleştirilen suçlarda da, suçun oluşabilmesi için manevi unsurun bulunması, yani failin eylemi kasten veya taksirle işlenmiş olduğunun ispatlanması gerekmektedir. Ancak İnternet suçlarında kast ve taksirin, icrai veya ihmali bir hareket olarak algılanması problem yaratabildiğinden, suçun ispatlanmasında da zorluk yaşanmaktadır.¹⁶¹

c. Uluslararası İşbirliğindeki Güçlükler

Siber suçları klasik suçlardan ayıran en önemli özelliklerinden bir tanesi yargılama yetkisi sorunudur. Siber uzayın küresel yapısı suçlulara dünyanın bir

¹⁵⁸ "Effective measures to prevent and control computer-related crime Report of the Secretary-General", s.3., United Nations Economic And Social Council, 29 Ocak 2002, (Çevrimiçi), <http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf>, 9 Mart 2007,

¹⁵⁹ "Encryption: Impact on Law Enforcement", s.1., FBI, June 3, 1999, (Çevrimiçi), <http://sion.quickie.net/en60399.pdf>, 21 Mart 2007.

¹⁶⁰ Richard Wortley, Stephan Smallbone, "Child Pornography on the Internet", **Problem-Oriented Guides for Police Problem-Specific Guides Series Guide No. 41**, U.S. Department of Justice, 2006, s.27.

¹⁶¹ Feridun Yenisey, "Bilgisayar ve Bilgisayar Şebekelerinin Ortaya Çıkardığı Yeni Suç İşleme Yöntemleri". İçişleri Bakanlığı Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Sempozyumu, Bursa, 24 Mart 2001, s. 52., akt.: Şehitoğlu, a.g.e, s.262.

ucunda oturdukları yerden diğer ucunda suç işleme imkânı sunmaktadır.¹⁶² Yargılama yetkisi hususu ceza hukukunun en önemli meselelerinden birini oluşturmaktadır. Özellikle de suçun uluslararası alanda işlendiği, hiçbir bir ülkenin sınırları içerisinde olmadığı veya suçun faili ile mağdurunun farklı ülkelerde bulunmaları durumunda önem kazanmaktadır. Siber suçlar tek bir ülkenin yargı yetkilerini ilgilendirebileceği gibi genellikle birden fazla ülkeyi ilgilendirebilecek bir nitelik sergilemektedir.¹⁶³ Birden çok ülkenin eşit yargılama yetkisi olduğu durumlarda, suçun işlendiği yerin kararlaştırılması (locus delicti) ve aynı fiilden ötürü bir kişinin yalnız bir kez yargılanması (ne bis idem) prensibinin uygulanması problemleri ortaya çıkabilmektedir.¹⁶⁴

Hukuk kurallarının yer bakımından uygulanmasında normalde iki ilke mevcuttur. Bunlardan ilki her devletin sınırları dahilinde kendi hukuk kurallarını uygulamasını ve failin suçun işlendiği ülke mahkemelerinde yargılanmasını öngören kanunların mülkiliği (yerselliği) ilkesidir. Diğer ise devletin vatandaşlarını dünyanın her yerinde, bazı konularda dahi olsa koruyabilmesi için onları takip etmesi gerektiğini ve suçun işlendiği yerden bağımsız olarak vatandaşları üzerinde yargı yetkisi olduğunu öngören kanunların şahsiliği ilkesidir. Bu iki ilke tek başlarına uygulandığında devletin egemenlik haklarını kısıtlayabilmektedir.¹⁶⁵

Bunun yanında yargılama yetkisi ile ilgili çıkan uyuşmazlıklarda, bazı ülkelerde özellikle çocuk pornografisinde uygulandığı gibi evrensel yargılama yetkisi gibi diğer ilkeler de uygulanmaktadır.¹⁶⁶ Siber saldırıların izinin sürülmesi için gerekli olan kayıt tutma, iletişimi takip etme, karşılıklı yardımlaşma, bilgi paylaşımı ve yargılama yetkisi konusunda tüm ülkeleri kapsayan bir standart ya da anlaşma bulunmamaktadır. Buna ilaveten hangi fiillerin siber suç olarak değerlendirileceği, bu suçların nasıl cezalandırılacağı, idari sorumlulukların ne olması gerektiği konusunda da evrensel bir kabul bulunmamaktadır. Bu durum birden fazla ülkeyi ilgilendiren

¹⁶² Russell G. Smith, Peter Grabosky, Gregor Urbas, **Cyber Criminals on Trial**, Australia, Cambridge University Press, 2004, s.48.

¹⁶³ Hüseyin Çeken, "Council of Europe's Convention 2001 on Cybercrimes and Turkey", İstanbul, Marmara Üniversitesi Avrupa Topluluğu Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2003, s.104.

¹⁶⁴ Pocar, **a.g.e.**, s.36.

¹⁶⁵ **Temel Hukuk Bilgisi**, Ed. Yavuz Atar, Sami Karahan, Konya, Mimoza, 2006, s.61.

¹⁶⁶ Ulrich Sieber, "Legal Aspects of Computer-Related Crime in The Information Society-Comcrime Study", s.133., 1 Ocak 1998, (Çevrimiçi), <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc>, 10 Kasım 2006.

suçlarda suçun aydınlatılması için hayati önem taşıyan hızlı ve etkin bir koordinasyonu engelleyebilmektedir.¹⁶⁷

İkinci bir zorluk ise fiziksel arama ya da haberleşmenin dinlenmesi gibi yasal yetkilerin alınması için yasal süreci başlatacak ve kanunu harekete geçirecek yeterli delilin bir araya getirilmesinde yaşanmaktadır.¹⁶⁸ Siber suçlular, genellikle başka ülkelerdeki mağdurlara saldırmayı tercih etmektedir. Bu nedenle suç izlerini takip etmek için kolluk güçlerinin çeşitli ülkelerdeki diğer organizasyonlar ile elektronik ortamdaki suç delilleri yok olmadan, hızlı bir şekilde işbirliği sağlaması büyük önem taşımaktadır.¹⁶⁹ Yabancı bir ülkede bulunan delillerin elde edilmesi için normalde bu ülkedeki otoritelerden yardım talep edilmesini gerekir. Ancak, çeşitli nedenlerle yardım talep edilen ülke ya da ülkeler yardıma bulunmaya isteksiz olabilmekte ya da buna imkânları bulunmamaktadır. Özellikle de delillerden ziyade suçlunun kendisi başka bir ülkede ise bu zorluklar artabilmektedir.¹⁷⁰ Saldırganın kimliği ve yeri tespit edilse, deliller toplansa dahi saldırganı tutuklamak çok güç olabilmektedir. Suçluya ev sahipliği yapan ülke, soruşturma için işbirliğini ya da suçluyu iade etmeyi reddedebilmektedir.¹⁷¹ Mülkilik ilkesine dayanarak birçok ülke, kendi sınırları içerisinde bulunan çocuk pornografisi ya da bölücülük benzeri yasa dışı içerik sağlayan servis sunucuları konusunda ceza hukuku kurallarını uygulamamaktadır.¹⁷²

Uluslararası işbirliğinde ortaya çıkan diğer zorluk ise suçluların iadesi konusunda yaşanabilmektedir. Bir failin iade edilebilmesi için suça konu olan eylemin, belli bir ceza eşiğini geçen ağır bir suç olması ve “çifte suçluluk”¹⁷³ şartının sağlanması gerekmektedir. Çifte suçluluk, suçun maddi unsurun hem iade talep eden, hem de talep edilen ülke kanunlarında suç olarak tanımlanmış olması gerektiği anlamındadır.¹⁷⁴ Eğer talep edilen ülke kanunlarına göre eylem suç teşkil

¹⁶⁷ Lipson, **a.g.e.**, s.17.

¹⁶⁸ Smith v.d., **a.g.e.**, s.49.

¹⁶⁹ Edappagath, **a.g.e.**, s.171.

¹⁷⁰ Smith v.d., s.51.

¹⁷¹ Brenner, **a.g.e.**, s.10.

¹⁷² Sieber, **a.g.e.**, s.132.

¹⁷³ “Çifte suçluluk (eylemin talep eden ve talep edilen devlet kanunlarına göre suç olması) şartı” Suçluların iadesinin temel bir kuralı olan bu koşula göre, iadeye konu fiiller ilgili her iki devletin yasaları tarafından da suç sayılmalıdır. İade için talepten yazılı fiilin talep eden devlet ülkesinde cezalandırılabilir nitelik taşıması gerekir. Ayrıca fiilin kendisinden iade talebinde bulunulan devlet kanunlarına göre de suç teşkil etmesi gerekir. Bu ilkeye, “çifte suçluluk prensibi”, “aynı norm ilkesi” ya da “karşılıklı cezayı gerektirme kuralı” denmektedir. M. Zafer Erdoğan, “Hakimlerin Tarafsızlığı”, Adalet Dergisi, (Çevrimiçi), http://www.yayin.adalet.gov.tr/dergi/18_sayi.htm, 2 Haziran 2007.

¹⁷⁴ Smith v.d., **a.g.e.**, s.50.

etmiyorsa, çifte suçluluk sağlanamadığından iadesi mümkün olmamakta ve suçlu yargılanmaktan ve ceza almaktan kurtulabilmektedir.

d. Diğer Güçlükler

Siber suçlarla mücadele de karşılaşılan diğer güçlüklerden biri suçun boyutlarının tam olarak tespit edilememesidir. Siber suçlar bir anlamda buz dağına benzetilmektedir. Zira saldırıların büyük bölümü şirketlerin ve firmaların saldırıya uğradıklarını saklamak istemeleri nedeniyle gizli kalmaktadır. Maruz kalınan saldırıların rapor edilmemesinin en büyük sebebi ise firma hakkında kötü bir intiba oluşacağı endişesidir. Ayrıca rakip firmalar böyle bir bilgiyi kendi avantajlarına kullanabilmektedir. Firmaların maruz kalınan bir saldırının ortaya çıkması durumunda mali kayba uğrama, müşteri kaybetme ve marka imajlarının zedelenmesi konusunda duydukları endişe, bu suçların büyük bölümünün rapor edilmemesine neden olmaktadır. Siber suçların az rapor edilmesinin bir diğer nedeni de suç mağdurlarının suça maruz kaldıklarının farkında dahi olmamaları ya da maruz kaldıkları eylemin suç olduğunu bilmemeleridir. Diğer bir ifadeyle, siber suçlara yönelik toplumsal bilincin henüz yeterli olmamasıdır.¹⁷⁵

İnternet hizmetinin toplu olarak verildiği ortamlarda kullanıcıların takibi ile ilgili yaşanan sorunlar da suçla mücadelede karşılaşılan önemli bir güçlüğü teşkil etmektedir. Genellikle üniversiteler, kamu ve özel kurumlar ve şirketlerde sunulan toplu İnternet hizmetlerinde, kullanıcıların faaliyetleri takip edilememektedir. Ortak kullanılan bilgisayarlarda kimlerin, hangi zaman aralıklarında İnternet'i kullandığı kayıt altına alınmadığında, suçluların tespiti konusunda zorluklar yaşanmaktadır. Bu konuda en önemli sorun İnternet kafelerdir. Toplu İnternet hizmeti verilen mekânlarda genellikle bir yada birkaç İnternet hattı üzerinden hizmet verilir ve yine bir veya birkaç IP adresi bulunur. Dışarıdan bakıldığında tüm kullanıcılara ait IP adresleri değil, bu IP adresleri görünür. Ancak kullanıcılara içeride "hub" adı verilen cihazlar sayesinde farklı IP adresleri atanır. Eğer suçun işlendiği yer bir İnternet kafe veya toplu İnternet hizmeti sunulan bir mekân ise, suç işlediği belirlenen IP adresi sadece bu mekânın bulunmasını sağlar. Mekân bulunduktan sonra suçun işlendiği bilgisayar, ancak "log" kayıtları depolanmaktaysa ya da kullanıcı kimlikleri, zaman ve süreleri geleneksel yollarla kaydedilmekte ise bulunabilir. Belirsizlik ise bu noktadan sonra başlamaktadır. Zira suçun işlendiği anda bilgisayarı kullanan kişinin

¹⁷⁵ Charlie Fuller, "Law Enforcement and Security", **Cyber Crime**, 2003, s.77.

kaydı tutulmadıysa, işlenen bilişim suçunun failini bulmak neredeyse imkânsız hale gelmektedir.¹⁷⁶

Diğer bir güçlük ise İnternet kullanıcılarının bilgisayar güvenliği ve ağ yapısı konusundaki bilgi zafiyetleridir. İnternet'in ilk dönemlerinde ağa bağlı bilgisayar sayısının nispeten çok az olması, bu bilgisayarların ağ kurulumu ve işletilmesi konusunda oldukça bilgili, güvelik açısından ise en azından temel bilgiye sahip kişilerce yönetilmesine olanak sağlamıştır. Günümüzde ise İnternet'te bağlanan bilgisayar sayısının milyonları geçmesi, bu bilgisayarların çoğunun güvenlik konusunda hiç bilgisi olmayan ya da çok az bilgiye sahip kullanıcılar ve yöneticiler tarafından işletilmesi sonucunu doğurmuştur. Bu husus güvenlik bilincinde zafiyete ve tedbirsizliğe neden olarak, siber suçların işlenmesine olanak sağlayan birçok açığın ortaya çıkmasına yol açmaktadır.¹⁷⁷

¹⁷⁶ Cevat Özel, M. Gökhan Ahi, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", **Güncel Hukuk**, No. 6, Haziran 2004, s.22.

¹⁷⁷ Lipson, **a.g.e.**, s.16.

ÜÇÜNCÜ BÖLÜM

ULUSAL GÜVENLİK, BİLGİ GÜVENLİĞİ VE SİBER UZAYDA ULUSAL

GÜVENLİĞE YÖNELİK TEHDİTLER

1. GÜVENLİK KAVRAMI

Güvenlik kavramı, bireyden ulusa kadar tüm aktörler için önem taşıyan, her seviyede farklı anlam kazanan, ancak özünde her biri için hayati gereklilik ifade eden bir kavramdır. Bu nedenle güvenlik ihtiyacını, varlığı korumak ve sürdürmek amacı taşıyan her davranış biçiminin görmek mümkündür.¹⁷⁸

Güvenlik, Latince bir kelime olan “securitas” kökenli olup “garanti, güven, rahatlık ve huzur, temin etmek, garanti etmek, düzen, barış, eminlik” gibi eş anlamlara sahiptir.¹⁷⁹ Sözlük anlamı ile “toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet.”¹⁸⁰ veya “bedene zarar verebilecek tehlikeli durumları asgariye indirme ya da ortadan kaldırmaya yönelik etkinlikler” şeklinde tanımlanmaktadır.¹⁸¹ Güvenliğin teknik anlamda yapılan bir tanımı ise şöyledir;¹⁸²

“insanların, eşya ve maddelerin, araç ve bilgilerin tehlike ve tehditlerden uzak olma, güven, huzur ve sağlık içinde bulunmasını tehdit eden, zarara ve hasara veya faaliyet ve işlev ya da görevinden men etmeye veya kısıtlamaya baskı, cebir, şiddet, şantaj veya herhangi bir eylemle onu istenmeyen durumlara yönlendirmek için yapılan işleri durdurmaya, engellemeye, caydırmaya veya etkisini aza indirmeye yönelik plan, program ve prosedürlerle belirlenen etkinlikler sonucu arzulanan durumun oluşturulması.”

Buzan güvenliği başlangıçta “tehditten uzak olma arayışı” şeklinde tanımlarken, bu tanımını daha sonra “var olan tehditler karşısında hayatta kalmak” şeklinde geliştirmiştir.¹⁸³ Wolfers ise güvenliğe iki ayrı tanım getirmiştir. Wolfers subjektif açıdan güvenliği “kazanılmış değerlere yönelik tehdidin bulunmaması”, objektif anlamda ise “bu değerlere saldırılacağına dair korkunun bulunmaması”

¹⁷⁸ Beril Dedeoğlu, **Uluslararası Güvenlik ve Strateji**, İstanbul, Derin Yayınları, 2003, s.9.

¹⁷⁹ Mehmet Bal, **Modern Devlet ve Güvenlik**, İstanbul, IQ Kültür Sanat Yayınları, 2003, s.19.

¹⁸⁰ **Türkçe Sözlük**, s.915.

¹⁸¹ **AnaBritannica Genel Kültür Ansiklopedisi**, C.X, s.227.

¹⁸² Bal, a.g.e., s.18.

¹⁸³ Maria Stern, **Naming Security-Constructing Identity**, New York, Manchester University Press, 2006, s.17.

şeklinde tanımlamıştır. Ayrıca Wolfers güvenliğin, kişisel güvenlik ve siyasi güvenlik şeklinde devletten daha alt düzeyde tartışılabileceği gibi, bölgesel ve küresel güvenlik gibi devletten daha üst düzeyde de tartışılabileceğini belirtmiştir.¹⁸⁴

Güvenlik kavramı her varlık için farklı bir anlam taşıyan sübjektif bir kavram olduğundan genellikle bireysel güvenlik, toplumsal güvenlik, ulusal güvenlik, uluslararası güvenlik, askeri güvenlik, ekonomik güvenlik ve bilgi güvenliği gibi farklı kavramlarla ilişkilendirilerek kullanılmaktadır. Bunun neticesinde ilişkilendirildiği kavrama bağlı olarak farklı güvenlik tanımları ortaya çıkmaktadır.

Güvenlik tanımlarında kullanılan en önemli kavram tehdit ya da tehlike kavramıdır. Güvenliğin hangi boyutundan bahsedildiğinden bağımsız olarak salt güvenlik olgusundan bahsedebilmek için varlığın korunması ve sürdürülmesi açısından bir tehdidin bulunması gerekmektedir. Söz konusu tehdit içsel ya da dışsal olmak üzere bir veya daha fazla olabilir. Tehdidin gerçekten var olması yanında bu türden algılamalar veya tahminlerin bulunması durumu da yeterlidir.¹⁸⁵

Güvenliğin tanımını etkileyen unsur sadece tehdit algılaması, tehdidin varlığı ya da niteliği değildir. Kime göre, hangi değerler için, ne kadar, ne süre için ve hangi maliyetle sorularına verilecek cevaplara göre de güvenliğin tanımı değişebilmektedir.¹⁸⁶ Bireysel güvenlik tanımı ile ulusal güvenlik tanımı arasındaki fark güvenliğin “kime” göre ele alındığı ile ilgili iken, ekonomik güvenlik ve fiziksel güvenlik arasındaki fark güvenliğin “hangi değerlere” göre ele alındığı ile ilgilidir. Bu husus aynı zamanda tehdidin tanımını da içermektedir. Zira birey için ciddi bir güvenlik kaygısına yol açan tehdit, toplumsal açıdan ya da ulusal açıdan bir anlam taşımayabilir.

Uluslararası ilişkiler disiplininde güvenlik algılamaları ve arayışları aktörlerin amaçlarına, sistem içerisindeki ağırlıklarına ve rollerine göre değişiklik göstermektedir. Bu nedenle uluslararası ilişkilerde güvenlik kavramı birkaç düzlemde ifade bulunmaktadır. Bunlar;¹⁸⁷

- Uluslararası sistemin bütününe ya da bütününe yakınının güvenliği,

¹⁸⁴ David A. Baldwin, “Güvenlik Kavramı”, **Avrasya Dosyası**, Ankara, ASAM Yayınları, C.IX, No:2, Yaz 2003, s. 30.

¹⁸⁵ Dedeoğlu, a.g.e., s.10.

¹⁸⁶ Baldwin, a.g.e., s.16-19.

¹⁸⁷ Dedeoğlu, a.g.e., s.12.

- Coğrafi ya da işlevsel alt sistemlerin, bölgelerin güvenliği,
- Devletin güvenliği,
- Toplumun güvenliği, Toplumsal alt gurupların güvenliği,
- Bireylerin güvenliğidir.

Bu düzlemler değişen güvenlik anlayışı ile hiyerarşik bir yapıdan birbirleri ile doğrudan ilişkili ve etkileşim halinde olan yatay bir yapıya dönüşebilmektedir. Güvenlik kavramının günümüz için taşıdığı anlamı ve her seviyedeki aktörün güvenlik algılarının daha iyi anlaşılması için güvenlik kavramının özellikle 20. yüzyılda geçirdiği evrime değinmek fayda sağlayabilir.

a. Ulusal Güvenlik Kavramı

Güvenlik canlı ya da cansız her varlık için söz konusudur. Devletlerin varlıklarını sürdürebilmeleri, içinde bulundukları sistemde güvende olmaları ile ilişkilidir. Bu nedenle her devletin öncelikli ihtiyacı varlığını korumak ve sürdürmek olduğundan, hayati gereklilik olarak değerlendirilen güvenlik arayışının devletler için de geçerli olması doğaldır.¹⁸⁸ O halde devletlerin bireyler olarak görülebileceği uluslararası sistemde güvenlik, “uluslararası düzen içerisinde, devletlerin tehdit ya da tehdit algılamasının bulunmadığı bir ortamda varlıklarını sürdürebilmeleri durumu” şeklinde tanımlanabilir.

Uluslararası ilişkilerde güvenlik, uzun bir süre boyunca “devletin bütünlüğüne, bağımsızlığına ve temel değerlerine yönelik askerî bir tehdidin bulunmayışı”¹⁸⁹ olarak yorumlanmış ve uluslararası ilişkiler disiplini söz konusu olduğunda güvenliğin ilk akla gelen düzeyi ulusal güvenlik olmuştur. Güvenliğin varlığın sürdürülmesini amaçlayan tüm davranış şekillerinde görülebileceği gerçeğinden hareketle, ulusal güvenlikten bahsedebilmek için öncelikle ulus devletin varlığından söz etmek gerekmektedir. Bu nedenle, ulusal güvenlik kavramının ulus devletin ortaya çıkması ile birlikte anılmaya başladığı ve önem kazandığını ifade edilebilir. Ulusal güvenlik kavramının evrensel boyut kazanması 1. Dünya Savaşı ile başlamış, 2. Dünya Savaşı ve sonrasında yeni ulus devletlerin ortaya çıkması ile devam

¹⁸⁸ Anıl Çeçen, “Türkiye’nin Güvenliği”, **Uluslararası Çatışma Alanları ve Türkiye’nin Güvenliği**, Der.: Gamze G. Kona, İstanbul, IQKültür Sanat, 2005, s.107.

¹⁸⁹ J. H. Mathews; “Güvenliğin Yeniden Tanımlanması”, *Dışişleri*, 68, 2, 1989, s.162-177. akt: John Vogler, “Küreselleşmenin Çevresel Boyutları ve Güvenlik Stratejilerine Etkileri”, *Küreselleşme ve Uluslararası Güvenlik, Birinci Uluslararası Sempozyum Bildirileri* (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, s.49.

etmiştir. Bir ulus devletin varlığını koruması ve devam ettirmesi ile ilgili olan ulusal güvenlik kavramı bir devletin ve ulusun var oluşu ile eşdeğer bir anlam kazanmıştır.¹⁹⁰

Ulusal güvenlik kavramı ilk ortaya çıktığı dönemde bir savaş sırasında devletin varlığını korumasını sağlayacak askeri güç kapsamında, sadece askeri güvenlik ile açıklanmıştır. “Kopenhag Okulu” üyeleri (Buzan, Weaver, Wilde)¹⁹¹ için güvenlik, “referans objesinin” yaşamsal tehdit altında olduğunun ilan edildiği bir “konuşma” eylemidir. Yaygın görüşün güvenlik tartışmalarında referans nesnesi normalde devlettir ve tehditler genellikle “anarşik” uluslararası sistemin askerî eylemde bulunan diğer üyelerinden kaynaklanmaktadır.¹⁹² Bu algılama güvenliğin savaşa hazırlık anlamında doğrudan silahlı gücü etkileyecek faaliyetler şeklinde değerlendirilmesine neden olmuştur. Bu açıdan ulusal güvenlik kavramı, günümüzdeki anlamına göre dar bir çerçevede ele alınarak, silahlı kuvvetlerin sağladığı koruma ve caydırıcılığın artırılması üzerinde durulmuş¹⁹³ ve aşağıdaki şekilde tanımlanmıştır;¹⁹⁴

“Devletin bağımsızlığı ve ülke bütünlüğü ile millet egemenliğinin, milli veya milletlerarası alanda gerçek ve yakın bir tehlikeye düştüğü zamanlarda, Anayasanın gösterdiği yetkili organ veya organlar tarafından Devlet tüzel kişiliğinin korunması ve güvenlik altına alınması”

Ancak, bu tür tanımlar sadece bağımsızlık, ülke bütünlüğü ve egemenliği gibi eş değer kavramlar üzerinde durması nedeniyle kapsayıcı görülmemektedir. Uluslararası sistemin zamanla değişen yapısı, ortaya çıkan yeni aktörler ve tehdit algılamaları ulusal güvenlik kavramı algılamalarını da değiştirmiştir. Bu değişimle birlikte ulusal güvenlik kavramı, devletin siyasi, sosyal, dış politik, ekonomik ve askeri çıkarlarının korunması ve geliştirilmesi için stratejik seviyede yapılan çalışmalar bütünü olarak, güvenlik yapılanmasının en geniş güvenlik yaklaşımı halini almış¹⁹⁵ ve,¹⁹⁶

¹⁹⁰ **Milli Güvenlik Siyaseti ve Stratejisi**, İstanbul, Harp Akademileri Komutanlığı Yayınları, 1996, s.26.

¹⁹¹ Vogler, a.g.e., s.51.

¹⁹² A.y.

¹⁹³ **Milli Güvenlik Siyaseti ve Stratejisi**, s.26.

¹⁹⁴ Tayfun Akgüner, “1961 Anayasası’na göre Milli Güvenlik Kavramı ve Milli Güvenlik Kurulu”, **İÜSBF Yayınları**, 1983, s. 96. akt: Yusuf Şevki Hakyemez, “Demokratik Ülkelerde Milli Güvenlik Politikalarının Belirlenmesi ve Türkiye”, **AÜEHFD**, C.VII, No. 3-4, Aralık 2003, s.287.

¹⁹⁵ Kerem Alkin, Can Fuat Gürlelel, “Dünya Ekonomisine Yönelik Global Tehditler; Dünya da Güvenlik ve Tehdit Kavramının Evrimi ve Global Güvenlik İçinde Ulusal Güvenlik Perspektifi”, **İstanbul Ticaret Üniversitesi Dergisi**, Yıl 3, No.6, 2004, s.14.

“Devletin Anayasal düzeninin, milli varlığının ve bütünlüğünün milletlerarası alanda siyasi, kültürel ve ekonomik dahil bütün menfaatlerinin ve ahdi hukukunun her türlü dış ve iç tehditlere karşı korunması ve kollanması”

şeklinde daha geniş bir tanımlamaya gidilmiştir.

Görüldüğü üzere ulusal güvenlik devletin iç ve dış güvenliğini içine alan geniş bir kavrama dönüşerek, ulusal varlığın ve bütünlüğün korunmasının yanında bütün menfaatlerin kollanmasını da içerecek şekilde genişleme göstermiştir. Ulusal güvenlik algılamaları, analiz edildiği dönemdeki mevcut çıkarlar, tehdit algılamaları, ulusal güvenlik kültürü ve hatta ülkenin coğrafi konumu gibi faktörler çerçevesinden bir devletten diğerine farklılık göstermekle¹⁹⁷ birlikte, varlıklarını korumak ve devam ettirmek devletlerin hepsi için nihai amacı teşkil etmektedir.

Ulusal güvenlik kavramının günümüzde, ulusal menfaatlerin bir bütünü olarak ele alınması gereken bir kavram halini aldığı açıktır.¹⁹⁸ Küreselleşme ile birlikte küçülen, coğrafi mesafelerin ortadan kalktığı, yalnızca dış politika değil iç politika kararlarının dahi diğer ülkeleri ilgilendirebildiği günümüz dünyasında, ulusal güvenlik, birey olarak vatandaşların güvenliği, askeri güvenlik, ekonomik refah ve kalkınma gibi öğelerin oluşturduğu bir sinerji halini almıştır.¹⁹⁹

b. Genişletilmiş Güvenlik Anlayışı

Geleneksel güvenlik anlayışı ulus devlet kavramı ile ilişkilendirilmiş ve en önemli değer ya da öncelik devletin bağımsızlığının ve toprak bütünlüğünün korunarak bekasının sağlanması olarak görülmüş ve bu sayede ekonomik refahın da doğal olarak sağlanacağı değerlendirilmiştir.²⁰⁰ Uluslararası sistemde ise dengenin savaş ve askeri gücün kullanılması korkusu ile sağlanacağına inanılmıştır. Var olan bu savaş korkusunun devletlerin güvenliğini birey ve toplumların güvenliğinin önüne çıkarmış²⁰¹ ve güvenlik politikalarının askeri gücün kullanılması

¹⁹⁶ **Milli Güvenlik Siyaseti ve Stratejisi**, s.25.

¹⁹⁷ Hakan Uğurlu, “Küreselleşme ve Ulusal Güvenlik (1990 Sonrası)”, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2005, s.57.

¹⁹⁸ M. Ender Arkun, “Türkiye İçin Bir Enformasyon Politikasının Ana Öğeleri Neler Olmalı?”, **Bilgi Dünyası**, C.IV, No.2, 2003, s.184.

¹⁹⁹ Necdet Timur, “Ulusal Güvenlik”, **Uluslararası Çatışma Alanları ve Türkiye’nin Güvenliği**, Der.: Gamze G. Kona, İstanbul, IQKültür Sanat, 2005, s.560.

²⁰⁰ Gülgün Tuna, **Küresel Ekonomik ve Sosyal Tehditler, Yeni Güvenlik**, Ankara, Nobel, 2003, s.165.

²⁰¹ **Security and Development**, Ed. Robert Picciotto, Rachel Weaving, New York, Routledge, 2006, s.30.

üzerine şekillendirilmesine neden olmuştur. Kısaca geleneksel anlamda güvenlik askeri güç ve ulusal devlet merkezli olarak algılanmıştır.²⁰²

Dünya 20. yüzyılda ardı ardına iki büyük savaşa tanıklık etmiştir. 2. Dünya Savaşı'nın bitiminde yıllarca süren, büyük bir yıkıma, can ve mal kaybına yol açan savaşların kalıcı bir barışla ve genel bir silahsızlanma ile son bulacağı umudu doğmuştur. Ancak bu umut kısa zamanda sona ermiştir. Dünyanın iki kutuplu yeni düzeni, ABD ve SSCB etrafında oluşan Doğu ve Batı Blokları ve Üçüncü Dünyanın fazlasıyla silahlanmasına neden olmuştur. Doğu ve Batı arasındaki çekişmenin büyük bölümü teknolojinin gelişmesi ile birlikte nükleer, konvansiyonel ve ileri teknoloji olmak üzere her türden silahlanma yarışları biçiminde gelişmiştir.²⁰³

Soğuk Savaş boyunca süregelen askeri güç merkezli güvenlik anlayışı, doğal olarak bilim adamlarının güvenlik çalışmalarının çoğunlukla devletin askeri tarafıyla sınırlı kalmasına neden olmuştur. Bunun sonucunda askeri güçle ilgili olan konular birincil güvenlik meselesi olarak düşünülürken; diğer konular ikincil politika (low politics) kategorisine dahil edilmiştir.²⁰⁴

Silahlanma yarışı 1945'te ABD'yi müteakip 1949'da SSCB'nin de nükleer gücü elde etmesinden sonra nükleer kulvarda devam etmiştir. Sovyetler Birliği'nin 1957'de ilk uzay uydusu Sputnik'i fırlatması ile Sovyetlerin yarattığı tehlike Batı'da kaygı verici bir hale gelerek, yarışa bir de uzay boyutunu eklemiştir. Bu dönemde her iki tarafın savaş stratejisi, diğerinin saldırısına büyük çapta nükleer silah kullanımıyla karşılık vermek şeklinde belirlenmiştir. Bu nedenle, Soğuk Savaş süresince her iki süper güç, müttefiklerinin topraklarına ve kendi denizaltılarına nükleer silahlar yerleştirerek, nükleer ilk vuruş yeteneğini geliştirmeyi amaçlamıştır. 2. Dünya Savaşı sonrasının siyasi gelişmeleri insanlığa tehlikeli bir miras olarak nükleer ve konvansiyonel silahların yanı sıra kimyasal, biyolojik, genetik, lazer ve diğer gelişmiş teknoloji silahlarını bırakmıştır.²⁰⁵

Soğuk Savaş süresince güvenlik için bahis konusu tehdit, her iki taraf içinde belirgin bir şekilde var olmuştur. Ancak, Soğuk Savaş'ın bitimi ile birlikte ülkelerin tehdit algılamalarında ve uluslararası sistemin temel karakteristiklerinde hızlı ve derin değişimler gerçekleşmiştir. Bu değişimler, uluslararası politik yapıda farklı

²⁰² Helene Sjursen, "Security and Defence", s.1., (Çevrimiçi), http://www.arena.uio.no/publications/wp03_10.pdf, 24 Şubat 2007.

²⁰³ Tuna, a.g.e., s.165.

²⁰⁴ Baldwin, a.g.e., s. 11.

²⁰⁵ Tuna, a.g.e., s.165-180.

boyutlarda yeni güç dengelerinin ve yeni aktörlerin ortaya çıkması şeklinde gerçekleşmiştir. Değişikliğin en önemli boyutu güç dengeleri ve tehdit algılamasının değiştiği güvenlik konusunda yaşanmıştır. İki kutuplu yapılanmada geçerli olan askeri-ulus devlet merkezli güç algılamasına ilave olarak ekonomik ve teknolojik boyut ortaya çıkmıştır. Bunun sonucunda, ekonomik ve teknolojik güce sahip ülkeler yeni bir güç merkezi olarak ortaya çıkarken, ekonomi ve teknoloji kavramları güvenlik kavramı ile ilişkilendirmiştir.²⁰⁶

Geleneksel güvenlik anlayışında öne çıkan “kısa, askeri nitelikli ve doğrudan ulusun varlığına yönelik tehdit algılamasına”²⁰⁷ karşılık, son yıllarda uluslararası güvenlik algılamasında, güvenliğin askeri güçten farklı ya da ona ilave bir kavram olduğu anlayışı oluşmuştur. Güvenlik kavramının genişletilmesi gerektiği fikri üzerine inşa edilerek, “çok yönlü güvenlik”, “insan güvenliği”, “güveniksizleştirme”, “yumuşak güç” ve “yumuşak güvenlik” kavramları uluslararası güvenlik çalışmalarında dikkat çekmeye başlamıştır.²⁰⁸

Soğuk Savaş sonrası yaklaşımlar devletlere ilave olarak bireyler, sosyal guruplar, çok uluslu şirketler ve sivil toplum örgütleri gibi diğer aktörlerce karşılaşılan tehditleri ele alan bir çerçeve kazanmıştır. Yeniden yapılanan dünyada, uluslararası güvenlik ifadesinin geçerli bir etiket olmadığı tartışılmaya başlamıştır. Sadece devletler arasındaki yapıyı ifade eden uluslararası kavramının, dünya genelinde uluslar haricindeki birçok aktör tarafından karşılaşılan problemleri tanımlamak için yeterli olmadığı düşüncesiyle, “küresel güvenlik” ve “dünya güvenliği” terimleri alternatif olarak önerilmiştir.²⁰⁹

Soğuk Savaş sonrasında küreselleşmenin yarattığı dinamik ortam içinde ulusal güvenliğe yönelik tehditler farklılaşmış, terörizm, ayrılıkçı hareketler, etnik ve dinî çatışmalar, kitle imha silâhlarının yayılması, uluslararası organize suçlar ve siber terörizm gibi “asimetrik tehditler” yeni tehdit parametreleri olarak ortaya çıkmış ve güvenlik algılamalarını değiştirmiştir.²¹⁰

Buzan, Waever ve Wilde literatürde, güvenlikle ilgili iki görüşün var olduğunu

²⁰⁶ Uğurlu, a.g.e., s. 81.

²⁰⁷ Tuna, a.g.e., s. 181.

²⁰⁸ Sjursen, a.y.

²⁰⁹ Pınar Bilgin, “Individual and Societal Dimensions of Security”, *International Studies Review*, C.V, No.2, 2003, s.207.

²¹⁰ Reşat Turgut, “Küreselleşmenin Askerî Boyutları ve Güvenlik Stratejilerine Etkileri”, Küreselleşme ve Uluslararası Güvenlik, Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, s.42.

belirtmektedirler. Bu görüşler gelenekselcilerin askeri ve ulus merkezli eski görüşü ve genişleticilerin güvenliğin kavramsallaştırılmasında askeri güç ve ulusun önceliğini sorgulayan yeni görüştür.²¹¹ Genişletici görüşe paralel olarak Buzan ve diğerleri güvenlik çalışmalarında beş bölümlü bir yaklaşım önermişlerdir. Bu bölümler, askeri, ekonomik, siyasi, sosyal ve çevresel bölümdür.²¹² Her bölümle ilgili güvenliğin amacı farklıdır. Askeri ve politik bölümde var olan tehditler, genellikle ulus ya da bağımsızlık gibi ulusu teşkil eden prensipler kapsamında tanımlanırken, sosyal bölümde bahse konu amaç kültürün, dilin ya da dini ve ulusal kimliğin sürdürülebilirliğidir.²¹³

Wolfers²¹⁴, Buzan ve diğerleri güvenlik dinamiklerini yerelden, bölgesel ve küresele uzanan bir seviyede değerlendirirken,²¹⁵ benzer şekilde Dedeoğlu da her ne biçimdeki tehdide karşı olursa olsun her aktör için iç içe geçmiş üç halkalı bir güvenlik sistemi bulunduğunu belirterek, benzer bir tespitte bulunmuştur. Bun tespite göre;²¹⁶

“ En içteki halka (yerel), aktörün kendi iç güvenlik sistemidir. Bu sistem içten gelebilecek veya içte oluşabilecek tehditleri kapsamaktadır ve en sıkı halkadır. Bu halka doğrudan varlığa yönelecek birincil tehditleri kapsamaktadır. Bunlar var olan rejimin devamı, bağımsızlık, ülkenin bütünlüğü, sosyal ya da ekonomik sistemin devamının sağlanmasıdır.

İkinci halka (bölgesel), yakın çevre güvenlik halkasıdır. Bu halka ülke sınırlarına komşu ya da yakın olan devletlerden veya ülkenin ulusal çıkarları açısından ilgi alanındaki yakın çevreden müteşekkildir. Bu halka daha çok coğrafi bir yakınlık ifade ettiğindendir ki her devlet aynı biçimde davrandığında tehdidin de öncelikle bu halkadan gelmesi beklenmektedir.

Üçüncü ve en dıştaki halka (küresel) ise en gevşek halkadır. Daha çok yakın bölge dışında gelişen çatışmalar, savaşlar, küresel ekonomik krizler, doğal çevrenin kirlenmesi gibi konular bu halkaya dahil olmaktadır. Ancak ikinci halka ile üçüncü halka bazı konularda birbiri ile yer değiştirebilmektedir. Örneğin yağmur ormanlarının yok olması Kamerun için 2. halka olarak

²¹¹ Barry Buzan v.d., **Security: A New framework of Analysis**, London, Lynne Rienner, 1998, s.1.

²¹² A.e., s.vii.

²¹³ Ole Wæver v.d., **Identity, Migration and The New Security Agenda in Europe**, New York, St. Martin's Press, 1993, s.23.

²¹⁴ Baldwin, a.g.e., s.30.

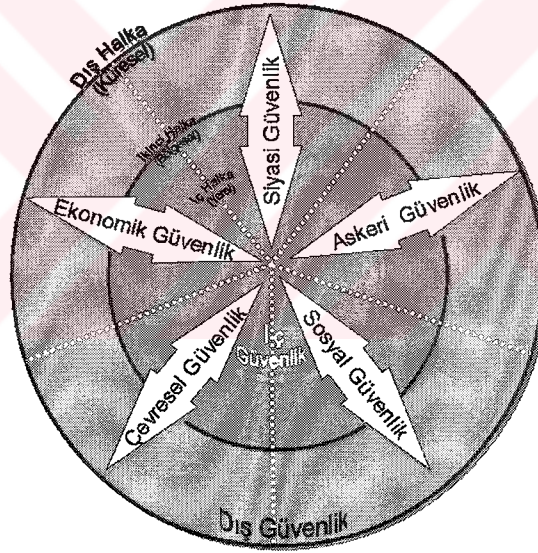
²¹⁵ Buzan v.d., a.g.e., s.1.

²¹⁶ Dedeoğlu, a.g.e., s.53.

değerlendirilebilirken, Türkiye için ancak 3. halkaya dahil olabilecektir.”

“Güvenlik artık çok daha geniş bir kavram olsa da halen çok büyük askeri unsurları ihtiva etmekte”²¹⁷ ve geleneksel güvenlik kavramları hala kabul görmektedir. Yeni zafiyetlerin ortaya çıkması nedeniyle, şu an bu güvenlik kavramları, küreselleşmenin devlet açısından yeni fark edilen etkileri tarafından sorgulanmaktadır.²¹⁸ Bu nedenle, değişen güvenlik anlayışı artık ulus devletin güvenliğinden bahsedilemeyeceği ya da askeri güce dayalı güvenlik yaklaşımının geçersiz olduğu şeklinde değil, güvenliğin tanımının genişletilmesi ve ilave faktörlerin güvenlik algılamalarına dahil edilmesi gerektiği şeklinde yorumlanmaktadır.

Kısaca yukarıdaki açıklamalar ışığında uluslararası ilişkiler açısından güvenliğin değişen tanımı çerçevesinde, aşağıdaki şekilde şematize etmenin mümkün olduğu değerlendirilmektedir.



Şekil-1: Uluslararası İlişkiler Boyutunda Güvenlik Yapılanması

Sonuçta uluslararası ilişkiler disiplini içerisinde ulusal güvenliğin yerel, bölgesel ve küresel seviyede olmak üzere, askeri, siyasi, ekonomik, sosyal ve çevresel bileşenlerin oluşturduğu kapsayıcı bir algılama ile bütün olarak en geniş güvenlik yaklaşımı ile değerlendirmek mümkündür. Dolayısıyla ulusal güvenliğin bu beş

²¹⁷ Chris Donnelly, “Küreselleşme Bağlamında NATO ve Avrupa Birliğinin Gelecekteki Roller”, Küreselleşme ve Uluslararası Güvenlik, Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, s.133.

²¹⁸ Vogler, a.g.e., s.55.

bileşeninden herhangi birine yönelik bir tehdit ister yerel, ister bölgesel, isterse küresel olsun ulusal güvenliğin konusunu teşkil etmektedir. Tez kapsamında Türkiye'nin güvenliği konusu ele alındığından ulusal güvenlik, genişletilen ulusal güvenlik tanımı çerçevesinde değerlendirilmektedir.

Küreselleşen dünya da bilgi ülkelerin sahip olduğu en önemli değerlerden biri olarak öne çıkmıştır. Bu önemli değerın bilişim sistemlerinin ve bilişim sürecinin devinimini sağlayan asıl unsur olması onu önemli kılarken, iletişim sistemleri üzerinden aktarılması da bilgi'nin güvenliğinin sağlanmasını gerektirmiş ve; "bilgi'nin artan önemi, bilgi güvenliğinin ülkelerin güvenliğinin sağlanması ile eşdeğer tutulmasına ve önem kazanmasına neden olmuştur."²¹⁹ Günümüz bilgi toplumunda, bilginin diğer güvenlik bileşenlerinin tamamı ile ilişkili olduğu ve her biri içerisinde ele alınması gereken ayrı bir boyut olarak ortaya çıktığı değerlendirilmektedir. Bu nedenle bilgiye yönelik tehditlerin, ulusal boyutta bir etki yaratabileceği ve bilgi güvenliğinin ulusal güvenliğin önemli bir bileşeni olduğu ifade edilebilir.

2. BİLİŞİM TEKNOLOJİLERİ VE ULUSAL BİLGİ GÜVENLİĞİ KAVRAMI

Bilginin kontrol edilmesi ve kullanılması artık insanoğlunun tüm faaliyetlerinde yer alan merkezi bir öneme ulaşmıştır. Bireyler, organizasyonlar ve ülkeler günden güne siber uzayda birbirleri ile daha fazla etkileşim içine girmektedirler. Bilişim teknolojilerinin küresel istikrar ve ulusal güvenlik üzerine etkileri henüz tam olarak bilinmemekle beraber, bilgi çağıının tehdit algılamalarında büyük bir değişikliğe yol açtığı kesindir.²²⁰ "Hükümetler, ekonomik ve askeri başta olmak üzere tümünden ulusal güvenlik gerekçesiyle bilgiye ulaşmanın ve saklamanın gerekliliğine uzun süredir inanmaktadırlar."²²¹

Bu durum ulusal güvenliğin yeniden değerlendirilerek, yeni tehditler karşısında yeni güvenlik uygulamalarının geliştirilmesini zorunlu kılmaktadır.²²² "Gerçek güvenlik anlayışının siyasi, ekonomik, ülke refahına yönelik çok yönlü risklerin

²¹⁹ "Çalışma Grubu 4, E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları", Çalışma / Belgeleme Grupları 2. Ara Değerlendirme Raporu, TBD Kamu-BİB Bilişim Platformu VIII (Antalya 25-28 Mayıs 2005), s.3.

²²⁰ Emily O. Goldman, "Introduction: Security in the Information Technology Age", **National Security in the Information Age**, Ed. Emily O. Goldman, London Portland, Frank Cass, 2004, s.1.

²²¹ Nedret Ersanel, **Siber İstihbarat**, Ankara, ASAM, 2001, s.2.

²²² Goldman, a.y.

başarılı bir şekilde yönetimini de içerdği"²²³ ve "ulusal güvenlik kavramının ulusal menfaatlerin bir bütün olarak korunması şeklinde ele alınması gerektiği"²²⁴ kabulleri göz önüne alındığında, bilişim teknolojileri ve bilgi güvenliğinin hem bireysel, hem de ulusal ölçekte büyük önem kazandığı ifade edilebilir.

1990'lardan önce bilgi güvenliği, bilginin çoğunlukla evrak ve doküman şeklinde olması nedeniyle fiziksel varlıkların korunması ile eşdeğer tutulmuştur. Ancak, bilginin bilgisayarlar ve bilişim sistemleri sayesinde hem elektronik ortamda saklanmaya, hem de bu yolla aktarılmaya başlanması, bu anlayışı büyük oranda değiştirmiştir. Herhangi bir tehdit karşısında bilgisayar sistemleri güvenli konuma getirilebilmekte veya İnternet bağlantısı kesilerek fiziksel olarak güvenlik altına alınabilmektedir. Bununla birlikte haftanın yedi günü 24 saat hizmet veren bir sistemin veri tabanları, diğer insanların özellikle de ticari olarak müşterilerin hizmetine açıkken, güvenliğin hizmetin devamı esnasında kesintisiz olarak sağlanması gerekmektedir. Bu nedenle bilginin korunması zorlaşmaktadır. "Bilgi ve bilişim alt yapısının korunması için, hem iş devamlılığı planlaması hem de güvenlik yönetimine yönelik bütünsel bir yaklaşım gerekmektedir."²²⁵

Ulusal bilginin güvenliği, bir zincirin halkalarını oluşturacak şekilde organize olmaktadır. Bu düzenleme, kişisel bilgisayarları koruyacak bir güvenlik sisteminden başlayarak, ağların ağı olarak bilinen İnternet ortamında kullanılan çok fonksiyonlu bilgi sistemlerinin korunmasına kadar geniş bir yelpazeye sahiptir.²²⁶ Aynı zamanda ulusal güvenlik politikaları, ulusal bilim ve teknoloji politikaları ile çok büyük paralellik sergilemektedir.²²⁷

Bilişim teknolojileri ve İnternet sayesinde bilginin elektronik olarak derlenmesi, iletilmesi ve kullanılması, elektronik ortamdaki bilgi miktarının da artmasına neden olmuştur. Bireyler, şirketler ve hükümetler, faaliyetlerini elektronik ortamda

²²³ Celeste A. Wallander, Helga Haftendorn, Robert O. Keohane, "Introduction", **Imperfect Unions: Security Institution over Time and Space**, Ed. Helga Haftendorn, Robert O. Keohane, Celeste A. Wallander, New York, Oxford University Press, 1999, s.2.

²²⁴ Arkun, a.g.e., s.184.

²²⁵ Bosch, a.g.e., s.74.

²²⁶ Mustafa Sağsan, "Bilgi Teknolojileri Güvenliği: Ulusal Bilginin Korunmasına Pragmatik Bir Yaklaşım ve Türkiye Perspektifi", **Stratejik Analiz**, C.II, No.22, Şubat 2002, s.75.

²²⁷ Y. Sharan, A. Hauptman, "The Israeli Science and Technology Foresight Study Towards the 21st Century", Report No. H/237, Tel-Aviv University, Samuel Neaman Institute Technion, Interdisciplinary Center for Technological Analysis & Forecasting (ICTAF) , Haifa March 2001., akt: Ersin Tulunay, Faruk Sarı, "Kamu Kurum ve Kuruluşları ile Özel Kurum ve Kuruluşların, Bilgi Teknolojisi Alanında Ulusal Güvenlik Politikası Doğrultusunda Yönlendirilmeleri" Konulu bildiri, s.1., (Çevrimiçi), <http://www.harpak.tsk.mil.tr/duyurular/SEMPOZYUM/09%20Prof%20Dr%20Ersin%20TULUNAY.DOC>, 07 Şubat 2007.

yürütmeye ve bilgilerini elektronik ortamda saklamaya başlamıştır. Bilgi alınan, satılan, işlenen, saklanan bir değere dönüşmüş, üretim sürecinde hem ham madde, hem ara ürün, hem de son ürün olarak yer almaya başlamıştır. Bir hırsız için çaldığı kimlik veya kredi kartı bilgileri banka kasasının anahtarına, telefon şirketleri için abonenin kullanım süresi bilgisi tahsil edilecek paraya ve bir öğretmenin öğrencisine aktardığı bilgi alacağı ücrete dönüşmektedir. Kısaca, bilginin kendisi değer ve zenginliğin temeli haline gelmiştir. Ancak, geçmişte de değerli olan bilginin, elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması nedeniyle maruz kaldığı tehdit artmış ve bilgi güvenliği kavramına yeni bir boyut kazandırmıştır. Günlük hayatın devamı için bilgiye ve bilişim sistemlerine giderek artan bağımlılık sonucunda, devlet yönetimi, ekonomik ve toplumsal hayatın ortak bileşeni haline gelen bilgi alt yapısının kötü niyetlere, terörist faaliyetlere, doğal afetlere vb. tehditlere karşı güvenliğinin sağlanması önem kazanmıştır.²²⁸

Dünyanın irili ufaklı pek çok devleti, bilişim politikaları geliştirme çabaları içindedir.²²⁹ Gelişmiş ülkeler kendi yapılarına uygun farklı önlemler almak mecburiyetinde kalmışlar ve ilgili teşkilatlarını kurmuşlardır.²³⁰ Bilgi güvenliği harcamaları bazı bütçelerde yerini almaya başlamıştır. Bu da bilgi güvenliğinin kurumsallaşmakta olduğunu göstermektedir.²³¹

a. Bilgi Güvenliği Kavramı

Bilgi güvenliğini kısaca aşağıdaki şekilde tanımlamak mümkündür;²³²

“bilginin ve verilerin, yetkisiz kullanımının, suiistimal edilmesinin, değiştirilmesinin ya da bunlarla ilgili kabiliyetlerin kullanımının engellenmesini önlemek için alınan tedbirler”

Buna ilaveten bilgi güvenliği “bilginin ve bilişim sistemlerin hassas taraflarının istismarının engellenmesi için alınan önleyici tedbirler”²³³ şeklinde de ifade edilebilir. Bilgi güvenliği daha önce de belirtildiği gibi yeni bir kavram değildir. Sadece

²²⁸ Kimberly Kiefer v.d., *Information Security: A Legal, Business, and Technical Hand Book*, U.S.A., American Bar Association, 2004, s.2-4.

²²⁹ Arkun, *a.g.e.*, s.177.

²³⁰ Olay Salcan, “Bilgi Güvenliği”, *Silahlı Kuvvetler Dergisi*, s.370, Ekim 2001, s. 59-60, akt: Zafer Metin, “Çağdaş Gelişme Eğilimleri Işığında Siber Suçlar ve Güvenlik Kuramı”, İstanbul, İstanbul Üniversitesi, Yayınlanmamış Yüksek Lisans Tezi, 2003, s.171.

²³¹ Bosch, *a.g.e.*, s.66.

²³² Eric Maiwald, *Fundamentals of Network Security*, U.S.A., McGraw-Hill , 2004, s.4.

²³³ *A.y.*

günümüzde yeni bir boyut kazanarak daha önemli bir hal almıştır.

“Bilgi güvenliği, bilginin kendisi kadar eskidir. İnsanlar ne zaman bilginin kaydedilmesi, depolanması veya aktarılması için yeni bir metot geliştirmişse, bunu kaçınılmaz bir şekilde kontrol altına alınmaları ve işlem yaptıkları bilginin korunmasına yönelik metotlar takip etmiştir. Örneğin Samuel Morse’un telgrafı bulması, aktarılan mesajların gizliliği konusunu gündeme getirmiş ve bir yıl sonra 1845 tarihinde mesajların gizliliğini sağlamak için bir kriptu kodu geliştirilmiştir.”²³⁴

Günümüzde tüm dünyada güvenlik sektörü uzmanları tarafından bilgi güvenliğinin ana unsurları olarak üç şarttan bahsedilmektedir. “Gizlilik, bütünlük ve kullanılabilirlik”²³⁵ olarak adlandırılan bu unsurlar, hem kullanıcıların bilgi sistemlerinden taleplerini, hem de iyi tasarlanmış bir bilişim sisteminin temelini ve amaçlarını oluşturmaktadır.²³⁶

- **Gizlilik (Confidentiality):** Önemli ve hassas bilgilerin, bilmesi gerekenler dışındakilere karşı güvende tutulmasıdır. Bu husus çoğu zaman “bilmesi gereken” prensibi olarak da adlandırılmaktadır. Gizlilik şartında, bilgiye yetkisiz erişimin ve bilginin kazara ifşa olmasının engellenmesi amaçlanmaktadır.²³⁷

- **Bütünlük (Integrity):** Bilginin kazara ya da kasıtlı olarak değiştirilmesinin engellenerek, güvenilirliğinin ve orijinalliğinin korunması ile ilgilidir. Bütünlük şartında bilginin yetkisiz kullanıcılar tarafından değiştirilmesinin yanı sıra, yetkili kullanıcılar tarafından da uygun olmayan değişikliklerin yapılmasının engellenmesi amaçlanmaktadır.²³⁸

- **Kullanılabilirlik (Availability):** Bilginin kendisinin ve depolandığı bilişim sistemlerinin, yetkili kullanıcılar için ihtiyaç duyulduğu her an erişilebilir olmasının sağlanmasıdır. Kullanılabilirlik daha çok kasıtlı ya da kazara oluşan servis reddi, doğal afetler ya da fiziksel saldırılar sonucu bilişim sistemlerinin zarar görmesi veya

²³⁴ Deborah Russell, G.T. Gangemi Sr., **Computer Security Basics**, U.S.A., O'Reilly&Associates Inc., 1992, s.24.

²³⁵ Michael G. Solomon, Mike Chapple, **Information Security Illuminated**, U.S.A., Jones and Barlett Publishers, 2005, s.2.

²³⁶ Jagdish Pathak, **Information Technology Auditing: An Evolving Agenda**, Berlin, Springer-Verlag, 2005, s.108.,

²³⁷ Mark S. Merkow, Jim Breithaupt, **Computer Security Assurance Using The Common Criteria**, Canada, Thomson Delmar Learning, 2005, s.9.

²³⁸ Merkow, Breithaupt, **a.g.e.**, s.10.

donanım arızaları ile ilgilidir.²³⁹

Bilgi güvenliği uzmanlarının güvenlik uygulamalarını gerçekleştirmek için oluşturdukları bu üçlü modele karşı, kötü niyetli kullanıcıların güvenlik hedeflerinin her birini çevreleyen kendilerine ait bir modelleri vardır. Bu modelleri hem tedbirleri hem de karşılık gelen tehditleri içerecek biçimde aşağıdaki şekilde bir arada göstermek mümkündür.²⁴⁰



Şekil-2: Bilgi Güvenliği ve Karşı Tehdit Üçgeni

Kaynak: Michael G. Solomon, Mike Chapple, **Information Security Illuminated**, U.S.A., Jones and Barlett Publishers, 2005, s.5.

b. Bilgi Güvenliğinin Bileşenleri

Bilgi güvenliğinin sağlanması çok yönlü bir güvenlik yaklaşımı ile birçok bileşenin aynı anda değerlendirilmesini gerektirmektedir. Bilginin gizliliğini, bütünlüğünü ve sürekli kullanılabilirliğini sağlamak, tek başına bir bilgisayarın güvenliğinden, tüm ağın güvenliğine ve hatta bilişim sistemlerinin fiziksel olarak bulunduğu ortamın güvenliğine kadar geniş bir bakış açısı gerektirmektedir. Bu bileşenler birbirinden bağımsız değildir.

Bilgisayar güvenliği çoğunlukla bilgi güvenliği olarak adlandırılmaktadır. Bunun nedeni, bilgisayar ve ilgili tüm çevre birimlerini, terminalleri, kabloları ve veri depolama ortamlarını kapsaması ve en önemlisi bilgisayar sistemleri içerisinde depolanan bilgiyi korumakla alakalı olmasıdır.²⁴¹ Ancak, günümüzde bilgisayar

²³⁹ A.y.

²⁴⁰ Solomon, Chapple, a.g.e., s.5.

²⁴¹ Russell, Gangemi, a.g.e., s.8.

kullanıp da İnternet bağlantısına sahip olmamak uzak bir ihtimal halini almıştır. Bu nedenle, artık tek başına bilgisayarın güvenliğinin sağlanması yeterli görülmemektedir. Bilgilerin aktarıldığı iletişim ortamı ve bilgisayar ağları da bilgi güvenliğinin bileşenleri haline gelmiştir.²⁴²

Bilgi güvenliğinin temel bileşenlerini tasnif etmeye yönelik yaklaşımlar bunları en az iki ana başlık altında ele almaktadır. Bu bileşenler “Bilgisayar Güvenliği” ve “İletişim (Haberleşme) Güvenliği” olarak adlandırılmaktadır. Bazı yaklaşımlar “İletişim Güvenliği”ni “Ağ Güvenliği”²⁴³ olarak ifade ederken, bu iki bileşene bir de “Fiziksel Güvenliği” ekleyenler mevcuttur. Ancak, genellikle “Bilgi Güvenliği”nin bilgisayar, iletişim ortamı ve fiziksel güvenlik olmak üzere üç ana bileşenden oluştuğunu kabul edilmektedir.²⁴⁴

Bilgisayar Güvenliği: Bilgisayar sistemi içerisinde depolanan bilginin güvenliği anlamına gelmektedir. Bilgisayar güvenliği, sistemde depolanan verilere kimlerin erişebileceği ile ilgili kontrol tedbirlerini, giriş parolalarını ve diğer fiziksel erişim kontrollerini içermektedir.²⁴⁵ Ayrıca, akıllı kartlar ve parmak izi, retina, el ve yüz geometrisi taraması veya ses tanıma gibi biyometrik sistemler de bilgisayar ve dolayısıyla veri güvenliği için kullanılan tekniklerdir.²⁴⁶ Diğer bir tedbir ise yazılımın ve donanımların amaçları dışında kullanılmaması ifade eden, yazılım ve donanım güvenliğidir.²⁴⁷

İletişim Ortamı (Haberleşme) Güvenliği: diğer adıyla ağ güvenliği, bilginin telefon, kablo, mikrodalga, uydu veya diğer yollarla aktarılması ile ilgili güvenlik tedbirlerini içermektedir. Bilgisayar sistemlerine ağ üzerinden erişim üzerine odaklanmaktadır.²⁴⁸ İletişim ortamı ve ağ güvenliği için alınabilecek birçok tedbir bulunmaktadır;

- Kriptolama, haberleşme güvenliğinin sağlanmasında temel mekanizmadır. Bu tedbir bilişim sistemleri arasında iletilen bilginin ele geçirilse dahi anlaşılmasını engelleyerek, korunmasını sağlamaktadır. Kriptolama aynı zamanda depolanan

²⁴² Solomon, Chapple, a.g.e., s.7.

²⁴³ Maiwald, a.g.e., s.10.

²⁴⁴ Russell, Gangemi Sr., a.g.e., s.17.

²⁴⁵ A.y.

²⁴⁶ Maiwald, a.g.e., s.13.

²⁴⁷ “Çalışma Grubu 4, E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları”, s.24.

²⁴⁸ Russell, Gangemi Sr., a.g.e., s.17.

bilgilerin korunması amacıyla da kullanılabilir. Ancak, kriptolama sistemleri kript anahtarına sahip olduğu sürece, bir kullanıcının yetkili ya da yetkisiz olmasını umursamamaktadır. Dolayısıyla kriptolama, kript anahtarlarının ve sistemin komple güvenliği alınmadığı sürece tek başına koruma sağlayamamaktadır.²⁴⁹

- Ağ güvenliği için en önemli tedbir güvenlik duvarlarıdır (Firewall). Güvenlik duvarları iç ağı dış saldırılardan korumak için kullanılmaktadır. İç ağdan dışarıya ve dış ağdan içeriye yapılan tüm iletişimi kontrol ederek kimin, nereye, ne zaman hangi servisi almak üzere bağlanabileceğini düzenler ve iç ağ ile dış ağ arasında bir sınır oluşturur. Bunlara ilaveten anti virüs yazılımları, ağa yapılan saldırıları haber veren saldırı tespit sistemleri (Intrusion Detection System), ağın açıklarını ve hassas taraflarını tespit eden zayıflık tarama yazılımları, iç ve dış ağda yapılan tüm iletişimlerini kaydeden "log"lama yazılımları ve yedekleme sistemleri de ağ güvenliği için alınan tedbirlerdir.²⁵⁰ Ayrıca ağ güvenliği için ağı oluşturan bileşenlerin birbiri ile uyumlu olması da gerekmektedir.

Fiziksel güvenlik: bilgi güvenliğinin anahtar kavramlarından bir tanesidir. Fiziksel güvenlik tedbirleri bilginin bulunduğu bina veya bölgeye girişin kontrolü, bilişim sistemlerinin bulunduğu oda ya da bina kapılarının kilitlemesi, giriş yetkilerinin ve anahtarların kimlerde bulunacağını belirlenmesi, bina içerisindeki haberleşme kabloları, bunların binaya giriş yerleri ve hat bağlantı kutularının emniyete alınması gibi fiziksel güvenlik tedbirlerini kapsamaktadır.²⁵¹

Bunlara ilaveten bilişim sistemlerini besleyen güç kaynaklarının sağlıklı işlemesi, jeneratörler ve kesintisiz güç kaynakları ile desteklenmesi, yangın ikaz ve söndürme sistemleri, bu sistemlerin sabotajlardan korunması, sistemlerin aşırı ısı, nem, gaz ve sıvılardan korunması, bakımları ve doğal afetlere karşı alınan tedbirleri de kapsamaktadır.²⁵²

Güvenlik bileşenleri çok çeşitli ve belirli başlıklar altında tasnif edilemeyecek şekilde birbirleriyle ilişkilidirler. Bazı konular birden fazla bileşenle ilgili olabilmektedir. Örneğin bir anti virüs yazılımı hem bilgisayar güvenliğinin, hem de ağ güvenliğinin konusudur. Bu nedenle belli bir kalıp içerisinde tasnif etmek mümkün

²⁴⁹ Maiwald, a.g.e., s.15.

²⁵⁰ A.e., s.12-15.

²⁵¹ A.e., s.207.

²⁵² Gerald Bowman, "Physical Security for Mission-Critical Facilities and Data Centers", **Information Security Management Handbook**, 5.bs., Ed. Harold F. Tipton, Micki Krause, Auerbach Publication, Vol. III, 2006, s.643.

gözükmemektedir. Yukarıda sıralananlar dışında kalan personel güvenliği, emisyon güvenliği ve doküman güvenliği gibi diğer güvenlik bileşenlerine de ayrıca değinmek gerekir.

Personel Güvenliği: bilişim sistemlerini yöneten, bakım yapan ve kullanan personelin güvenilir olmasını ve hangi çalışanların hangi bilgilere nüfuz edebileceğinin düzenlenmesini içermektedir. Çalışanlar kariyerlerinde yükseldikçe erişebilecekleri gizlilik dereceli bilginin seviyesi de değişecektir. Bu nedenle çeşitli seviyelere uygun kleransların düzenlenmesi gerekmektedir.²⁵³ Bilişim sistemlerinin güvenliği yalnızca sistemlerin güvenliği ile ilgili değildir. Bu sistemler sadece en zayıf halka kadar güvenlidir. Bu halkalardan bir tanesi de bilgisayarı kullanan insanlardır. Bir sisteme izinsiz girmenin en kolay yolu çoğunlukla içeriden birilerini, bir şekilde ele geçirmektir.²⁵⁴

Emisyon Güvenliği (TEMPEST) ise, bilişim sistemleri ve bileşenlerinden yayılan ve uygun filtreleme işlemlerinden geçirildiğinde bilginin tekrar elde edilmesine olanak veren kaçak elektromanyetik ışınlamaların, teknik tedbirler kullanılarak engellenmesini ifade etmektedir.

c. Bilgi Güvenliğine Yönelik Tehditler

Bilişim sistemlerine yönelik tehditler bilgi sızdırmak isteyen çalışanlardan, kendini ispatlamak ya da tatmin etmek isteyen bilgisayar korsanlarına ve terör örgütlerine kadar geniş bir aralık içerisindedir. Ancak, bu tehditler yalnızca kötü niyetli olanlarla sınırlı değildir. Doğal afetler ve kazara oluşan zararlar da bilişim sistemleri açısından büyük tehdit oluşturabilmektedir.²⁵⁵

Bilgi güvenliğinin tesis edilmesinde göz önüne alınması gereken en önemli husus var olan tehdit türlerinin tespit edilmesidir. Tehdit türlerini genel olarak üç ana başlıkta toplamak mümkündür. İlki, sisteme yetkisiz giriş, gizlice dinleme, hırsızlık, casusluk ve elektromanyetik dinlemeden oluşan kasıtlı eylemlerdir. İkincisi sel, yangın, elektrik kesintisi ve depremlerin toplamı olan doğal afetlerdir. Üçüncüsü ise malzeme ve sistemlerin kötü ve yanlış kullanımı ile kullanıcı ve işletici hatalarının

²⁵³ Metin, a.g.e., s.170.

²⁵⁴ Butler W. Lampson, "Computer Security in the Real World", s.1., (Çevrimiçi), <http://www.acsac.org/invited-essay/essays/2000-lampson.pdf>, 28 Aralık 2006.

²⁵⁵ Kiefer, v.d., a.g.e., s.11-13.

meydana getirdiği kaza sonucu oluşabilecek tehditlerdir.²⁵⁶

Tehdidin kaynakları ise bireylerden, karmaşık ulusal organizasyonlara kadar geniş bir yelpazede ortaya çıkmakta, yetkisiz kullanıcılar, muhbirler, teröristler, uyuşturucu kaçakçıları ve toplumsal eylemciler gibi devlet dışı guruplar, dış istihbarat örgütleri ve yabancı ülke silahlı kuvvetleri ya da siyasi hasımlar olabilmektedir.²⁵⁷ Bunları aşağıdaki şekilde özetlemek mümkündür;²⁵⁸

- Bilgisayar korsanları tarafından, özellikle kendilerini ispatlamak ve kendi camialarında saygınlık kazanmak amacıyla gerçekleştirilen eylemler,
- Organize suç örgütlerince gerçekleştirilen, ekonomik casusluk, hırsızlık ve sabotaj türü eylemler,
- İç saldırılar; eski ya da mevcut çalışanlar tarafından mali kazanç ya da öç almak amacıyla gerçekleştirilen eylemler,
- Devlet destekli olarak gerçekleştirilen ekonomik, siyasi ya da askeri amaçlar için hassas veya değerli bilgilerin elde edilmesini amaçlayan casusluk eylemleri,
- Endüstri casusluğu; rakipleri karşısında avantaj sağlamak isteyen organizasyonların hassas veya değerli bilgileri elde etmeye yönelik eylemleri,
- Terörizm ve bilgi savaşları; terör örgütleri ya da devletler tarafından siyasi, ideolojik, ekonomik ve askeri amaçları gerçekleştirmek için yapılan saldırılar,
- Kötü amaçlı yazılımlar; bilişim sistemlerine saldırarak, bilginin değişmesine ya da silinmesine yol açan eylemler,
- Sosyal mühendislik, bir organizasyonla ilgili bilgi elde etmek, şifre ya da PIN kodlarını ele geçirmek veya bilişim sistemleri ve tesislere girmek maksadıyla sosyal yeteneklerin kullanıldığı eylemler,
- Fiziksel güvenlik ihlali; ticari sır elde etmek, keşif yapmak veya daha sonraki saldırılar için hazırlık yapmak niyetiyle, organizasyonların kâğıt ya da diğer

²⁵⁶ Salcan, "Bilgi Güvenliği", s.56., akt.: Metin, a.g.e., s.165.

²⁵⁷ Metin, a.y.

²⁵⁸ Kiefer v.d., a.g.e. s.11-13.

türlü kayıtlarından bilgi edinmek için tesislere girilerek, çöplerinin, geri dönüşüm kutularının, kâğıt kıyma birimlerinin veya diğer atıkların araştırılması eylemleridir.

d. Ulusal Bilgi Güvenliği Kavramı

Bilginin değerli olduğu ve çeşitli tehditlere maruz kaldığı, bu nedenle de güvenliğinin sağlanması gerektiği açıkça görülmektedir. Ancak, önemli hususlardan biri de hangi bilginin kritik ve korunmaya değer olduğunun ortaya konulmasıdır. Her bilginin değerli olduğu düşünülse de tüm bilgilerin kritik olduğundan bahsedilemez. Bir takım bilgilerin değerli oldukları halde, paylaşılması ya da ifşa olması sorun yaratmazken; bazı bilgilerin güvenliğinin sağlanması ve sadece erişim yetkisi olanlarca ulaşılması önem teşkil etmektedir. Bu tür kritik bilgilerin başında ulusal güvenlikle ilgili bilgiler gelmektedir. Ulusal bilgi güvenliği;²⁵⁹

“ulusal güvenliği ilgilendiren, yetkisiz ellere geçtiği takdirde devletin güvenliğini tehlikeye sokabilecek veya devlet aleyhine kullanılabilecek her türlü bilgiyi, üretim, kullanım, işleme, saklanma, nakledilme ve imha sırasında yetkisiz kişilerin erişimine ve olası her türlü fiziksel ve elektronik müdahaleye karşı korumaya; bilgiye erişim ve kullanıma ait usulleri açık şekilde belirlemeye ve bilgiyi gerektiğinde hazır bulundurmaya yönelik tedbirler” olarak tanımlanmaktadır.

Tanımdan da anlaşılacağı üzere ulusal bilgi güvenliği devletin güvenliğini tehlikeye sokabilecek her türlü bilginin tehditlerden korunması, bilgi edinme hakkına yönelik usullerin belirlenmesi ve bilgiye erişimin yani bilişim sistemlerinin güvence altına alınmasını içermektedir. Ulusal bilgi güvenliği bir ülkedeki her türlü bilginin (bilimsel, teknolojik, ekonomik, vs.) dış tehditlere karşı korunmasını da hedef almaktadır. Devletin güvenliğini tehlikeye sokabilecek bilgiler devletin gizli askerî bilgileri, savunma planlarını veya ulusal menfaatlerine yönelik gizli bilgileri içerebileceği gibi ekonomik ya da ticari sırlar da devlet aleyhine kullanılabilecek bilgilerdir. Ulusal bilgi güvenliğinden bahsedilirken, sadece devletin ulusal çıkarları doğrultusunda oluşturulan bilgiler değil; daha geniş anlamda özel sektörü ilgilendiren bilgilerin korunması da anlaşılmalıdır. Zira özel sektöre karşı gelebilecek iç ve dış tehditlerden devlet de etkilenecek zor durumda kalabilmektedir.²⁶⁰

Özel sektörü ilgilendiren en önemli tehditler endüstri ve ekonomi casuslukları

²⁵⁹ “Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı”, Türkiye Bilişim Derneği, 01 Mart 2007, (Çevrimiçi), http://www.tbd.org.tr/genel/bizden_detay.php?kod=245&tipi=5&sube=, 05 Mart 2007.

²⁶⁰ Sağsan, “Bilgi Teknolojileri Güvenliği...”, s.74.

şeklinde gerçekleşmektedir. Şirketlerin maliyetleri zaman zaman milyon dolarları bulan bilgileri, ihaleleri, gizli görüşmeleri, anlaşmaları, patenti alınmamış buluşları tehditle karşılaşmaktadır.²⁶¹ Endüstri ve ekonomi casusluğu patenti alınmamış buluşların çalınması ya da uluslararası ihalelerin kaybedilmesi gibi ciddi sonuçlara varabilmektedir.

Ulusal bilgi güvenliğinin diğer bir ilgi alanı ise, sermaye ve mala dayalı üretimin, hammadde ve işgücünün önemini yitirerek yerini bilgi ve hizmet sektörüne bırakması ile ortaya çıkan, ticari ya da ekonomik anlamı olan bilgidir.²⁶² Geçmişte zenginliğin kaynağı olarak kabul edilen “para ve emek, benzeri maddi sermayeye duyulan ihtiyaç yerini bilgi, patent, telif hakkı gibi bilgi varlıklarına duyulan ihtiyaca bırakmıştır.”²⁶³ Parasal değer taşıyan düşünce ve sanat eserlerinin korunması, karşılıksız olarak kullanıma sunulmasının ve çoğaltılmasının engellenmesi, devletleri teknik ve yasal önlemler almaya yönelmektedir.²⁶⁴ İnternet başta olmak üzere enformasyon kanallarına serbestçe aktarılmakta olan birçok bilginin, ticari ve ekonomik değeri olan bilgileri veya bu bilgilere ulaşmaya olanak sağlayıcı ipuçlarını içermesi, kişi ya da şirketlerin ekonomik kayıplarla karşılaşmasına da neden olabilmektedir.²⁶⁵

Dolayısıyla ulusal bilgi güvenliğini yalnızca “devlet sırrı” kavramı ile değil, devlet güvenliğini ve milli menfaatleri tehlikeye düşürebilecek ekonomik ve ticari tüm bilgileri, kişiselden devlet kademesine kadar özel sektörü de dahil ederek belirlemek ve buna uygun bir ulusal bilgi güvenliği politikası oluşturmak önem kazanmaktadır.

e. Kişisel Verilerin Güvenliği

Kişisel veri genel anlamıyla, veri sahibinin tanımlanmasında ve teyit edilmesinde kullanılan her türlü bilgidir. Bilgisayar sistemleri ve İnternet sayesinde artık kişilere ait çok daha fazla bilgi alanı kayıt edilebilmekte, çeşitli amaçlarla işlenebilmekte ve paylaşılabilmektedir. Artık alışveriş yaparken ya da bir bankacılık işlemini gerçekleştirirken fiziksel para, basılı kimlik veya banka cüzdanı kullanımı ile yüz yüze yapılan iletişim yerini, önceden bilgi bankalarında depolanan kredi kartı

²⁶¹ Ersanel, a.g.e., s.90.

²⁶² Ebru Güzelcik, **Küreselleşme ve İşletmelerde Değişen Kurum İmajı**, Sistem Yayıncılık, Yayın No:222, İstanbul , 1999, s.64. akt: D. Arzu Akolaş, “Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları”, s.36., (Çevrimiçi), http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler%5CD.Arzu%20AKOLA%C5%9E%5C29-43+.pdf, 10 Şubat 2007.

²⁶³ A.y.

²⁶⁴ Arkun, a.g.e., s.180.

²⁶⁵ A.e., s.189.

bilgileri, kimlik bilgileri vb. elektronik ortamdaki kişisel verilerin teyit edilmesi yöntemine bırakmaktadır. Bu yöntem çeşitli vesilelerle kişisel bilgilerin toplanmasını, işlenmesini ve paylaşılmasını gerekli kılmaktadır. Kişiler artık sadece fiziksel görünümü ile yaşadığı kısıtlı çevrede değil, çok daha geniş bir çerçevede tanımlanabilmektedir. Bu durum bir başkasının verilerini kullanarak, o kişi adına devlet kurumlarında, bankalarda veya e-ticaret sitelerinde işlem yapmayı da mümkün kılmaktadır. Dolayısıyla, çeşitli vesilelerle toplanan kişisel verilerin kimler tarafından, ne amaçla toplanabileceğinin, nasıl depolanacağı ve korunacağı belirlenmesi büyük önem taşımaktadır.²⁶⁶

Kişisel verilere yönelik tehditler iki ana başlık altında tasnif edilebilir. İlki kişisel bilgilerin ele geçirilerek elektronik ortamda yapılan bankacılık, e-ticaret v.b. alanlarda başkasının adına sahte işlemler gerçekleştirilmesidir. İkincisi ise, bu yasal olmayan işlemlerin yanı sıra, kişilere ait özel bilgilerin kişilerin izni olmadan aleyhlerine olacak şekilde çeşitli ortamlarda açığa vurulmasıdır.

Kişisel verilerin yetkisiz kişilerce ele geçirilmesi, en basit anlamda kişilerin rahatsız edilmelerine yol açabilecek sonuçlar doğurabilir. Bunun yanında, kredi kartlarının kullanılmasına, banka hesaplarından para çalınmasına, dolandırılmalarına, belli bir ücret karşılığında kullandıkları hizmetlerden başkalarının haksız bir şekilde istifade etmesi gibi mali kayıplara da neden olabilir. Daha da önemlisi işlemedikleri suçlarla itham edilmelerine dahi yol açabilir. Çünkü siber uzayda kişisel veriler kullanılarak gerçekleştirilen eylemler, fiziksel dünya da bizzat kişi tarafından gerçekleştirilen eylemler gibi sonuç doğurmaktadır. Kişisel verinin bir diğer boyutunu da sadece kişinin kendisinin bildiği ve diğer insanların öğrenmesini istemediği özel hayatı ile ilgili bilgiler, kayıtlar, resim, yazı, görüntü gibi nesneler veya elektronik kayıtlar oluşturmaktadır. Bu bilgiler kimlik bilgilerinin dışında kalan kişisel bilgilerdir. Örneğin kişinin dini inancı ya da alkol bağımlısı olması, geçmişte işlediği bir suç dolayısıyla sabıkasının bulunması özel kişisel bilgileridir. Bu tip bilgilerin açığa vurulması çeşitli mahsurlara neden olabilir.²⁶⁷ Örneğin kişinin iş başvuruları alkolik olması ya da dini inancı sebebi ile kabul edilmeyebilir ya da şantaja maruz kalabilir.

²⁶⁶ Ceylin Beyli, "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler", s.3., (Çevrimiçi), http://www.bilisimsurasi.org.tr/hukuk/docs/tbs_kisisel_veri_ceylin_beyli_gorus1.pdf, 30 Mart 2007.

²⁶⁷ Eren Ersoy, "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", s.2., Akademik Bilişim 2006 + BilgiTek IV (Pamukkale Üniversitesi, Denizli, 9-11 Şubat 2006), (Çevrimiçi), <http://ab.org.tr/ab06/bildiri/6.doc>, 04 Nisan 2007.

Genellikle İnternet sitelerinin kişinin tercihlerine özel içerik hazırlaması gibi iyi niyetle kullanılan “cookiler”,²⁶⁸ özellikle hukuka ve ahlaka aykırı yayın yapılan İnternet siteleri tarafından bireylerin bilgisayarlarındaki bilgilerin ele geçirilerek kişilere karşı şantaj ve baskı amaçlı olarak kullanılması gibi kötü amaçlar için de kullanılabilir. ²⁶⁹

Bunun yanında kişisel veriler aracılığıyla bireylerin güvenliğini tehdit eden bir başka eylem de, verilerin merkezi bir sistem dahilinde izlenmesi yoluyla, kişiler hakkında çeşitli öngörülerde bulunmak amacını taşıyan veri madenciliğidir (data mining). Veri madenciliği kısaca aşağıdaki şekilde tanımlanmaktadır;²⁷⁰

“İstatistiksel analiz tekniklerinin yapay zekâ algoritmaları ile bir arada kullanılması suretiyle, veri içerisindeki gizli bilgilerin açığa çıkarılması ve verinin karar destek tabanlı bilgiye dönüştürülmesi süreci”

Veri madenciliği sisteminde, kişilerin İnternette gerçekleştirdiği işlemlerden elde edilen tüm verilerin çeşitli program ve algoritmalarla analiz edilmesi suretiyle, kişi hakkındaki davranış eğilimleri tespit edilerek, geleceğe yönelik muhtemel eylemleri tahmin edilmeye çalışılır. İş dünyasında özellikle finans ve yatırım sektörlerinde risk analizi ve uzun vadeli izdüşümü yapmak amacıyla kullanılan veri madenciliği sisteminin, kişilerin izni dışında kullanılması, kişisel verilerin korunması ve mahremiyet haklarına açıkça aykırılık teşkil etmektedir.²⁷¹ Zira “bazı sigorta şirketlerinin müşteri bilgilerinden yola çıkarak kanser gibi pahalı hastalıklar için risk oluşturan müşterilerini sigorta dışına çıkarmaya çalışmaları”²⁷² buna bir örnektir.

Kişisel verilerin ele geçirilmesinin ulusal boyutta yaratacağı tehdit daha çok veri madenciliği kapsamında öne çıkmaktadır. Ülkelerin ulusal bilgi alt yapıları finans, sağlık, gıda, tarım, tekstil vb. tüm alanlarda kamusal ve özel sektörde işbirliğini ve verimliliği artıracak şekilde birbiri ile bütünleşmektedir. Dolayısıyla vatandaşın kimlik, yerleşim, sağlık kayıtları, tüketim bilgileri ulusal bilgi sistemi

²⁶⁸ Cookiler (cookies), İnternet sitelerini ziyaret eden kullanıcıların sahip oldukları tarayıcıların (browser) sağladıkları imkân ile kullanıcının hard diskine yerleşen ve kullanıcı her internete bağlandığında hangi İnternet sitelerini dolaştığını kayıt altına alan ve bu bilgileri kendisini kullanıcının hard diskine yerleştiren İnternet sitesine ileten iletişim verisidir.

²⁶⁹ Yasin Beceni, “Siber Uzayda Mahremiyet”, Mart 2004, s.13., Türkiye 2. Bilişim Şurası, (Çevrimiçi), http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf, 08 Kasım 2006.

²⁷⁰ “SPSS Veri Madenciliği Çözümleri”, s.2., SPSS İnternet sayfası, (Çevrimiçi), <http://www.spss.com.tr/Web%20link/6-Veri%20Madenciligi.pdf>, 04 Nisan 2007.

²⁷¹ Beceni, a.g.e., s.14.

²⁷² Faruk Kahraman, “CRM (Customer Relationship Management)”, s.1., (Çevrimiçi), <http://tech-strategy.org/Manuel/CRM-Nedir-Ne-Degildir.pdf>, 04 Nisan 2007.

içerisinde depolanmaktadır. Bu sayede veri madenciliği kullanılarak çeşitli alanlarda ülke genelinde profil çıkarılması ve böylece;

- Ülkelerin etnik, dini haritalarının çıkarılması ve bölgesel olarak farklı psikolojik savaş tekniklerinin kullanılması,
- Farklı meslek gruplarının eğilimlerinin ve hassas taraflarının belirlenerek bunların kazanılması veya yozlaştırılmaya çalışılması,
- Ekonomik eğilimlerin tespit edilerek borsa manipülasyonlarının yapılması,
- Sağlık kayıtları ile gen haritaları çıkarılarak özel silah geliştirilmesi veya dışa bağımlı olunan bir gıda, ilaç ya da tüketim malzemesinin tedarikinin sınırlandırılması mümkün olabilir.

f. E-Devlet Dönüşüm Projesi ve Güvenlik

(1) E-Devletin Tanımı

Bilgi güvenliğinin ulusal güvenliğin önemli bir bileşeni haline gelmesinde, hâlihazırda dünyanın birçok devletinin bilgi toplumuna dönüşme çalışmaları kapsamında yürüttükleri, e-devlet uygulaması ile birlikte ortaya çıkan kaygılar büyük paya sahiptir. E-devlet kavramı, toplumun her alanında bilginin üretiminin, iletiminin ve tüketiminin hızlandığı, insanların yaşamlarını ilgilendiren çeşitli bilgilere kolayca erişebilmelerine ve dolayısıyla da kendilerini geliştirebilmelerine olanak tanıyan bilgi toplumunun²⁷³ ortaya çıkardığı bir gereklilik ve kolaylığın devlet yönetimi boyutunda oluşturduğu değişimi tanımlamaktadır. E-devlet projesi;²⁷⁴

“Modern çağın sunduğu bütün teknolojik, elektronik ve telekomünikasyon imkânları kullanılarak; devletin vermesi gereken kamu hizmetlerini daha hızlı ve verimli bir şekilde sunması ve vatandaşın devlete karşı yükümlülüklerini, daha kolay ve hızlı bir şekilde yerine getirmesi projesidir.”

İnternet sayesinde bankaya gitmeden e-şubeden işlemleri yapan, evinden çıkmadan mağazaları dolaşan ve siparişlerini evinden teslim alan, uçak ya da sinema biletini İnternet'ten satın alan vatandaş, zamanla bu kolaylığı ve konforu

²⁷³ (Faruk) Kocacık, “Bilgi Toplumu ve Türkiye”, **Sosyal Bilimler Dergisi**, Cilt: 27, No: 1, Sivas: Cumhuriyet Üniversitesi Yayını, s.3., akt.: Fulya Akyıldız, “Bilgi Toplumu Yönetim Anlayışı'nın Gerçekleşebilmesi İçin Zorunlu Bir Hak: Bilgi Edinme Hakkı”, s.446., 3. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi (Osman Gazi Üni. İktisadi ve İdari Bilimler Fakültesi, Eskişehir, 25-26 Kasım 2004), (Çevrimiçi), <http://iibf.ogu.edu.tr/kongre/bildiriler/11-01.pdf>, 20 Mart 2007.

²⁷⁴ Hakan Yıldırım, v.d., “**Her Şeyi e-leştirdik**”, 2.bs., Ankara, Macar Yayıncılık, 2003, s.103.

devlete karşı yükümlülüklerini yerine getirirken de aramaya başlamıştır. Bu değişim aynı zamanda müşterileriyle İnternet aracılığıyla iletişime geçen ve iletişim teknolojilerini kullanan organizasyonların verimliliğini de artırmıştır. Dolayısıyla, devlet de bilgi çağına ayak uydurmanın gerekliliğine inanmış ve değişim sürecine dahil olmuş ya da başka bir ifadeyle buna mecbur kalmıştır. Devlet, e-devlet kavramı içerisinde kendini şöyle tanımlamaktadır;²⁷⁵

“Yönetiminde bilişim teknolojilerinin stratejik kullanımı sayesinde, bilgi toplumunun ihtiyaçlarına cevap verebilecek, vatandaşı ve kurumları (özel ve/veya kamu) ile elektronik ortamda iletişimde bulunarak verimliliği, şeffaflığı ve kalkınmayı sağlayacak bir yeniden yapılanma modelidir.”

E-devlet modelinin vatandaşlarına ve vatandaşları ile olan ilişkilerine bakış açısı da klasik devlet modeline nispeten daha farklıdır. E- devlet teknik anlamda,²⁷⁶

“yurttaşların ‘müşteri’ kamu yönetimi faaliyetlerinde ‘hizmet’ olarak görüldüğü ‘kalite/fiyat performansı’ ölçütlerinin uyguladığı, en az maliyet ve emekle en kaliteli hizmetin üretilmesini hedefleyen verimlilik yönetim sistemidir.”

Türkiye’nin e-devlet uygulamalarına geçişi, nispeten yakın bir tarih olan 2000 yılına denk gelmektedir. Bu değişim 2002 yılına gelindiğinde bazı devlet kurumlarının sadece bilgilendirme ve basit bazı e-hizmetleri vermeye başlamaları ile hız kazanmıştır.²⁷⁷ Türkiye ulusal bilgi altyapısının oluşturulması ve e-devlete dönüşüm kapsamında birçok girişimde bulunmuş, bunlardan bir kısmı başarı ile tamamlanmış ve bir kısmı da halen devam etmektedir.

(2) E-Devlet ve Bilgi Güvenliği Boyutu

E-devlet uygulamaları ile birlikte devlet kendi kurum ve hizmetleri ile birlikte vatandaşlarını ve etkileşim içerisinde bulunduğu özel sektör kuruluşlarını da siber

²⁷⁵ T.C. Ulaştırma Bakanlığı Haberleşme Genel Müdürlüğü İnternet Sayfası, (Çevrimiçi), <http://www.ubak.gov.tr/tr/hgm/mevcut.htm>, 10 Ocak 2007.

²⁷⁶ Özgür Uçkan, **E-Demokrasi ve Türkiye, Kamu Yönetiminin Yeniden Yapılanması İçin Strateji ve Politikalar-I**, Literatür Yayıncılık, İstanbul, 2003, s.44-47, akt.: Ahmet Nohutçu, Demokaan Demirel, “E-Devlet:Genel Bir Çerçeve ve Teorik Bir Yaklaşım”, s.2., Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, (Çevrimiçi), http://www.nvi.gov.tr/attached/NVI/makale/e-devlet-genel_cerceve.pdf, 04 Nisan 2007.

²⁷⁷ R. Erdem ERKUL, “Dünyada Kamu Yönetimindeki Dönüşüm Ve Türkiye’de Kamu Yönetimi Öğretimine Yansımaları”, s.6., II. Kamu Yönetimi Forumu (Beytepe, Ankara, 7- 8 Ekim 2004), (Çevrimiçi), <http://www.digitaldevlet.net/edevlet.pdf>, 22 Aralık 2006.

uzaya taşımıştır. Bu nedenle ulusal güvenliğin tanımı da değişerek, bu tanıma “siber yurt’un siber uzaydaki güvenliği” açılımı eklenmiştir.²⁷⁸

E-devlet sürecinin getireceği faydaların, insanlara sağladığı kolaylıklar göz önüne alındığında inkâr edilemeyeceği bir gerçektir. Ancak, e-devlet uygulamaları sağladığı kolaylıklar yanında, ulusal bilgi güvenliği ile ilgili zafiyeti artıracak bir nitelik de taşımaktadır. Bunun sebebi, devletin tüm kurumları ve bu kurumların birlikte iş yürütmek zorunda olduğu kuruluşlarla ve vatandaşlarla arasında bir bilgi altyapısı oluşturması gerekliliğidir. Diğer bir ifadeyle devletin mevcut bilgi alt yapısı ve bilgi bankasını güvenli olmayan İnternet ortamına taşımasıdır. Bu durum, kullanıcılar, hizmet sunucular ve altyapı işletmecileri gibi ilgili tüm tarafların, birlikte çalışmalarına imkân verebilecek, kullanıcıların erişim yetkilerinin tanımlandığı, güvenli ve güvenilir bir teknik altyapının tesis edilmesini de gerekli kılmaktadır.²⁷⁹

İnternet aracılığıyla sunulan bilgi hizmetlerinin gizlilik ve güvenliği ile ilgili iki husus söz konusudur. İlki, yönetim birimlerinin vatandaşlara ve kurumlara hizmet sunarken kullandıkları elektronik bilgi havuzlarında depolanan kişisel verilerin, güvenlik zaafı nedeniyle art niyetli insanlar tarafından ele geçirilmesinin engellenmesidir. İkincisi ise İnternet’e bağlanan kamusal bilişim sistemlerinde depolanan kritik bilgilerin, ulusal güvenliği tehlikeye düşürecek şekilde elde edilmesinin önlenmesidir. Bu nedenle, e-devlet hizmetleri esnasında kamusal bilgilerin ve kişisel verilerin güvenli bir ortamda saklanması için gerekli olabilecek teknik ve yasal tedbirlerin alınması büyük önem taşımaktadır.²⁸⁰

E-devlet uygulamaları ile ulusal bilgi güvenliği açısından öne çıkan bir diğer konu ise hükümetlerin kullandıkları yazılım ve donanımların dışarıdan temin edilmiş olmalarıdır. Yabancılar tarafından üretilen ve işleyişi hakkında tam bilgi sahibi olunmayan yazılım ve donanımların, hassas bilgilerin depolanması ve işlenmesinde kullanılması ulusal bilgi güvenliği açısından büyük bir risk oluşturmaktadır. Bu yazılım ve donanımların istenen işlemler dışında, istenmeyen ve ulusal bilgi güvenliğini tehdit eden gizli işlemleri gerçekleştirme ihtimali de bulunmaktadır.²⁸¹ Dış kaynaklı yazılımlar İnternet üzerinden, gizli bir şekilde bilgi aktarabilmektedir. Almanya, Hindistan ve Çin gibi ulusal kimliğe önem veren ülkeler, özellikle devlet

²⁷⁸ “Çalışma Grubu, 4 E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları”, s.7.

²⁷⁹ “E-Dönüşüm Türkiye Projesi 2003-2004 KDEP Uygulama Sonuçları ve 2005 Eylem Planı”, s.14., Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi, Eylül 2005, (Çevrimiçi), http://www.bilgitoplumu.gov.tr/yayin/KDEPUygulamaSonuclari_2005EylemPlanı.pdf, 04 Nisan 2007.

²⁸⁰ Nohutçu, Demirel, a.g.e., s.13.

²⁸¹ Bosch, a.g.e., s.75.

kurumlarında kullanılmak üzere kendi yazılımlarını geliştirmişlerdir. Günümüzde hemen her türlü teknolojik, ticari, resmi ve askeri kurumun İnternet'i ya da kendi bilgisayar ağlarını kullanıyor olmaları, bilgi ve sistemlerin güvenliğine yönelik ihtiyacı doğurmaktadır.²⁸² Birçok ülke kendi yazılımlarını kullanmak suretiyle bu sorunu çözmeye çalışsa da yazılım geliştiren personelin güvenilirliği de riskin başka bir boyutunu oluşturmaktadır.²⁸³

3. BİLGİ ÇAĞINDA İSTİHBARAT (SİBER İSTİHBARAT)

İstihbarat kavramı bugün çok önemli bir evrim geçirmiş ve “elektronik İstihbarat”, “siber casusluk” ya da “teknolojik istihbarat” olarak tanımlanmaya başlamıştır.²⁸⁴ Bunun en önemli nedeni “milyonlarca insanın bilişim sistemleri ile bilgiye daha kolay erişmesi ve birçok kişi ve kurumun da bu sistemleri istihbarat için kullanıyor olmasıdır.”²⁸⁵ Bilgi çağıyla birlikte geleneksel istihbarat giderek yerini spesifik istihbarata bırakmıştır. Artık istihbarat ile ilgili açık kaynaklardan yapılan bilgi toplama, derleme ve üretme faaliyeti, İnternet sayesinde hem personel hem de lojistik açıdan daha ucuz hale gelmiş, dolayısıyla bilginin maliyeti düşmüştür.²⁸⁶

Kaynaklardaki artışın diğer etkisi ise istihbarat örgütlerinin inanılmaz miktardaki istihbarat bilgilerini depolamak, işlemek ve değerlendirmek zorunda kalmaları olmuştur. Büyük miktarda bilginin depolanması ve değerlendirilmesi ise ancak bilgisayar sistemleri ile mümkün olmaktadır²⁸⁷ ve böylece bilgisayarlar haber toplama ve değerlendirme işleminin vazgeçilmez bir parçası haline gelmektedir. İnternet ağı, bilgisayarlarla elektronik istihbarat üretiminin ortaya çıkmasında en ciddi rolü oynamıştır. Bu bilgi toplama işlemi, klasik televizyon, radyo veya gazete haberlerinin takip edilmesi suretiyle gerçekleştirilen haber toplama faaliyetine yeni bir boyut katmış ve İnternette yapılan “sanal sörf” dahi istihbarat faaliyetinin konusu haline gelmiştir.²⁸⁸

Bilgi çağının getirileri yalnızca açık kaynakların artması ve bilgiye ulaşma maliyetinin azalması olmamıştır. Bazı uzmanlar İnternet'e bağlı bilgisayarlara

²⁸² Tulunay, Sarı, a.g.e., s.4.

²⁸³ Bosch, a.y.

²⁸⁴ Ersanel, a.g.e., s.IX.

²⁸⁵ A.e., s.1.

²⁸⁶ Mustafa Sağsan, “Akıllı Toplum Olma Yolunda Ulusal Bilgi Stratejisi ve Bilgi Ortaklığı”, **Stratejik Analiz**, C.II, No.18, Ekim 2001, s.92.

²⁸⁷ Ersanel, a.g.e., s.10.

²⁸⁸ A.e., s.21-22.

duyulan yüksek bağımlılığın yarattığı casusluk imkânlarının, ulusal güvenlik açısından siber saldırılara nazaran daha büyük bir tehlike yarattığı görüşündedirler. İstihbarat servisleri, İnternette yalnızca açık haber toplama kaynaklarından yararlanmak için değil; aynı zamanda ağa bağlı bilgisayar sistemlerine gizlice girerek, aleni olmayan bilgileri toplamak için de faydalanmaktadır.²⁸⁹

Profesyonel ve örtülü ağ üzerinden yapılan istihbarat çalışmalarının hedefi ve metodu farklıdır. Artık hükümetler, resmi ya da özel kurumlar, bankalar, şirketler İnternet'i yoğun bir şekilde haberleşme ve hizmet için kullanmaktadırlar. İç işlemlerini kendi iç ağlarında, kendilerine has yazılımlarla gerçekleştirmekte ve tüm çalışmalarını, hizmetlerini, bilgilerini ve sırlarını bu iç ağ ile birbirlerine ulaştırmaktadırlar. Beraber iş yaptıkları veya bir şekilde iletişim halinde olmaları gereken dışarıdaki kuruluşlara bilgi göndermeleri veya almaları gerektiğinde ise İnternet'e açılan güvenli olduğuna inandıkları kapıları kullanmaktadırlar. Ancak, genel kabule göre bir kapı varsa, her iki tarafa da açılıyor demektir. Bu güvenli kapıları açmak için hazırlanan çok özel yazılım ve donanımların varlığı bir gerçektir ve istihbarat servisleri de bu yazılımları kullanmaktadır.²⁹⁰

Bunun ötesinde daha kolay ve zahmetsiz bir yöntem olarak, istihbarat servisleri bilgisayar korsanlarını kendi casusları ve haber toplama elemanları gibi kullanabilmektedirler. Bunun için çoğu zaman maddi menfaat, bazen de bilgisayar korsanları ile kurulan dostluklar yeterli olmaktadır. Nitekim 1986 ile 1989 yılları arasında Doğu Almanya'daki bilgisayar korsanları ABD, Batı Avrupa ve Japonya'daki birçok askeri, bilimsel ve endüstriyel kurumun bilgisayarlara girerek, parola, yazılım ve diğer bilgileri çalmış ve Sovyet gizli servisine satmıştır.²⁹¹

Siber istihbaratla ilgili genel kaygılardan biri de uzmanların sistem zayıflıklarından daha kolay ve akla yatkın olarak değerlendirdikleri bir yöntem olan, bilgisayar yazılımlarına dışarıdan hiçbir şekilde tespit edilemeyen gizli giriş şifrelerinin yerleştirilmesidir.²⁹² Bu konuda en büyük sansasyonu, bilgisayar donanım ve yazılım teknolojisinin lideri olan Microsoft firmasının geliştirdiği ve dünyanın her yerinde resmi ve özel kuruluşlar ile bireylerin çoğunluğunun bilgisayar sistemlerinde

²⁸⁹ James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", **Center for Strategic & International Studies**, s.9., December 2002, (Çevrimiçi), http://www.csis.org/media/csis/pubs/021101_risks_of_cyberterror.pdf, 23 Kasım 2006.

²⁹⁰ Ersanel, a.g.e., s.23.

²⁹¹ Anthony H. Cordesman, Justin G. Cordesman, **Cyber-Threats, Information Welfare, and Critical Infrastructure Protection: Defending the U.S. Homeland**, Connecticut, Praeger, 2001, s.18.

²⁹² Egmannt R. Koch, Jochen Sperber, **Bilgi Mafyası**, (Çev. Kaan Ökten), İstanbul, Sarmal Yay., 1996, s.23., akt.: Metin, a.g.e., s.162.

kullandıkları, Windows işletim sistemi ile ilgili ortaya atılan iddialar yaratmıştır. Kanadalı bir araştırmacı olan Endrew Fernandez, Windows programı içerisinde “NSA”²⁹³ harfleri ile kodlanmış bir şifre keşfetmiştir. Bunun üzerine ABD gizli servisi ajanlarının Washington’un dünyadaki haberleşmeyi izlemesini sağlayacak yazılım programları geliştirmek için Microsoft ile birlikte çalıştıkları iddia edilmiştir. Bu iddiaya göre, bugün kullanılan bilgisayarların yüzde 90’ında bulunan Microsoft yazılımlarına gizli kodlar yerleştirilerek, Windows uygulaması çalışan bilgisayarlar tarafından yapılan tüm işlemlerin, ABD istihbaratının eline geçmesi sağlanmıştır. Bu gelişmeler üzerine Rusya ve Almanya Microsoft programlarının resmi kurumlar tarafından kullanılmaması hususunda ciddi tedbirler almıştır.²⁹⁴

Siber istihbaratın bir diğer aracı da İnternette sürekli istifade eden hemen herkesin kullandığı elektronik posta (e-posta) servisidir. E-posta güvenliğini zora sokan birçok neden bulunmaktadır. Bu yolla dolaşan ve bulaşan virüsler, spam ve spammerlar (istenmeyen postalar) ve snifferlar (e-postaları 3. şahıslara gönderen ya da bildiren yazılımlar) bunlardan bazılarıdır. İstihbaratçıları ilgilendiren ise sonuncudur. Birçok kurum ve firma, e-posta güvenliğini yetkisiz kullanıcıların müdahalesini engelleyen, “fire-wall” adı verilen koruma tedbirleri ile sağlamaktadır. Ancak, iyi bir koruma sağlayan “fire-wall” sistemi e-postaların içeriğini kontrol etmediğinden, e-postalar sayesinde sisteme snifferları yerleştirmek mümkün olabilmektedir. Bu sayede gönderen ya da alanın haberi olmadan mesajın bir kopyası istihbaratçıları tarafından ele geçirilebilmektedir.²⁹⁵

Oldukça yeni ve son derece gelişmiş olan siber istihbarat yöntemlerinden bir diğeri de “Elektromanyetik Dinlemedir”. Bilgisayarın klavyesinden, ekranından, modem kablосundan ve diğer birçok bileşeninden yayılan elektromanyetik dalgalar, klavyede basılan tuşlar, ekrandaki görüntü ve modemle bilgisayar arasında geçen bilgileri de taşırlar. Yeterli donanıma sahip herhangi biri bu elektromanyetik dalgaları bir veya iki kilometreye varabilen bir mesafeden kaydedebilir ve ekrandaki görüntüyü, klavyede basılan tuşları veya modemden geçen bilgileri elektromanyetik ışınımı işleyerek tekrar oluşturabilir.²⁹⁶

Elektromanyetik dinlemenin yapılabilirliği ABD’de 1950’li yıllardan beri

²⁹³ Amerikan Ulusal Güvenlik Ajansı, National Security Agency (NSA).

²⁹⁴ Ersanel, a.g.e., s.25-28.

²⁹⁵ A.e., s.29-30.

²⁹⁶ “Elektromanyetik Dinleme ve Güvenlik (EDG)”, Olympos Security, 12 Mayıs 2001, (Çevrimiçi), http://www.olympus.org/article/articleview/278/1/10/elektromanyetik_dinleme_ve_guvenlik_edg, 15 Nisan 2007.

bilinmektedir. Bu konuda yapılan araştırmalar sonucu, devlet ve askeri kuruluşları elektromanyetik casusluktan korunması için TEMPEST²⁹⁷ adı verilen, elektronik aygıtların elektromanyetik ışıyım düzeylerinin azami sınırlarını ve zırlama metotlarını belirleyen bir standart çıkartılmıştır.²⁹⁸

İstihbarat teşkilatlarının bir diğer örtülü bilgi toplama aracı da bilgisayar yazılımlarıdır. Bu amaçla kullanılan yazılımların en önemlisi ve en çok sansasyon yaratanı ise PROMIS isimli programdır. 1980 yılında küçük bir Washington firması olan Inslaw Inc. tarafından, Adalet Bakanlığı savcılarını için geliştirilen program, üreticisinin dahi haberi olmadan hükümet tarafından çalınarak, birçok ülke istihbarat servisine satılmıştır.²⁹⁹ 1990 yılında CIA tarafından kullanıldığının açıklanması üzerine Kanada, İtalya, Hollanda ve İsrail gizli servislerinin de programı kullandıkları ortaya çıkmıştır. Bu program, birey bazında bilgi toplayabilmektedir. Telefon şirketi, elektrik şirketi, bankalar veya benzeri bir sistemden herhangi birine bu programa sahip bir bilgisayar ile sızılması yeterlidir. Program bir evde su tüketiminin artması veya telefon görüşmelerinin çoğalması durumunda, burada yaşayanların arttığı gibi mantıklı sonuçlar üreterek kullanıcıyı uyaramaktadır.³⁰⁰

Ancak PROMIS programının en büyük özelliği bu değildir. PROMIS'in üzerinde çok konuşulan bir program olmasının asıl sebebi, çalındıktan sonra Amerikan gizli servisi tarafından bir "arka kapı" yerleştirilerek diğer ülkelere satılmış olmasıdır. Bu arka kapı sayesinde program, satıldığı ülkelerin gizli servislerine, banka ve finans kuruluşlarına ait bilgileri, İsrail ve ABD gizli servisine göndermektedir.³⁰¹ Programın ABD tarafından Türkiye'de dahil³⁰² 40'tan fazla ülkeye satıldığı iddia edilmektedir.³⁰³

Günümüzde siber istihbaratın çok gelişmiş donanıma sahip istihbarat

²⁹⁷ TEMPEST kelimesi 'Transient ElectroMagnetic Pulse Standard' (Elektromanyetik Salınım Standardı) kelimelerinin kısaltılması ile oluşturulmuştur. Elektromanyetik güvenlik TEMPEST güvenliği olarak da bilinmektedir. Haberleşme sistemlerinden, bilgi işlem donanımından, kriptoloji cihazlarından salınan elektromanyetik dalgalardan yetkisiz kişilerin bilgi çıkarmalarını engelleyici güvenlik önlemlerinin tümüdür. Elektromanyetik güvenlik TEMPEST güvenliği olarak da bilinmektedir.

²⁹⁸ "Elektromanyetik Dinleme ve Güvenlik (EDG)", a.y.

²⁹⁹ Jerry Seper, "Software Likely in Hands of Terrorist (Promis/Inslaw)", **Washington Times**, June 14, 2001, (Çevrimiçi), <http://www.freerepublic.com/forum/a3b28933d7f22.htm>, 12 Mart 2007.

³⁰⁰ Ersanel, a.g.e, s.34-35.

³⁰¹ David Dastych, "Another Watergate? Promisgate: World's Longest Spy Scandal Still Glossed Over", **Canada Free Press**, January 31, 2006, (Çevrimiçi), <http://www.canadafreepress.com/2006/dastych013106.htm>, 12 Mart 2007.

³⁰² Ersanel, a.g.e., s.36.

³⁰³ Dastych, a.y.,

bilgisayarları, araştırma, bulma, yeni istihbarat edinme işlemlerini gerçekleştiren akıllı yazılımlar ve İnternet ağı üzerinden yürütüldüğü, istihbarat servislerinin siber uzayı örtülü bilgi toplama amaçlarını gerçekleştirmek için kullandıkları bilinmektedir.³⁰⁴ Dolayısıyla siber uzaya taşınan istihbarat faaliyetleri, ulusal bilgi güvenliğine yönelik en büyük tehditlerden birini oluşturmaktadır.

4. SİBER TERÖR VE GÜVENLİK

Günümüzde “siber terör” kavramının varlığı uzmanlar tarafından kabul edilmekte ise de, kavramın tanımı ve ulusal güvenlik açısından oluşturduğu tehdit derecesi konusunda farklı görüşler bulunmaktadır. Siber suçların kişilere, şirketlere, kurumlara ve hatta devletlere karşı işlenmesi mümkündür. Ancak, bir ülkenin kritik altyapı tesislerine yönelik toplumda büyük çaplı panik ve korku yaratabilecek siber terör saldırılarının gerçekleştirilebileceği konusunda, bazı uzmanlar riskin fazla abartıldığına inanmaktadır.

Bununla birlikte karşıt görüşlü birçok uzman, teknolojiadaki gelişmelerle birlikte siber terör tehdidinin de her geçen gün arttığına inanmaktadır. Farklı bakış açılarını destekleyen olgular incelendiğinde, her iki görüşünde doğruluk payının bulunduğu, ancak birçoğunun yalnızca birer öngörü ve tahmin niteliği taşıdığı dikkati çekmektedir. Bugüne kadar teröristler ya da terör örgütlerince kritik altyapı tesislerine karşı gerçekleştirilen ve siber terör kapsamında değerlendirilebilecek koordineli bir saldırı kaydedilmemiştir.³⁰⁵

Ancak, İnternet’in giderek artan bir şekilde teröristler ve diğer suç örgütleri tarafından kullanıldığı bir gerçektir. Genellikle kişisel amaçlarla motive olan ve bilgisayar korsanı olarak adlandırılan saldırganlar, sıklıkla gerek bireysel bilgisayarlar ve bilgisayar ağlarına ve gerekse kurumsal bilgisayar ağlarına karşı fiziksel tahrip içermeyen, ancak iş gücü ve zaman kaybına dolayısıyla da ekonomik zarara neden olan saldırılar düzenlemektedirler.³⁰⁶

³⁰⁴ Cordesman, G. Cordesman, **a.g.e.**, s.16.

³⁰⁵ John Rollins, Clay Wilson, “Terrorist Capabilities For Cyberattack: Overview and Policy Issue”, s.7., **CRS Report for Congress**, October 20, 2005, (Çevrimiçi), <http://www.usembassy.it/pdf/other/RL33123.pdf>, 27 Kasım 2006.

Ed Gabrys, “The International Dimensions of Cyber-Crime, Part 1.” **Information Systems Security**, September-October 2002, C.XI, No.4, s.26.,

James A. Lewis, “Cyber Terror: Missing in Action”, **Knowledge, Technology & Policy**, C.XVI, No.2, Summer 2003, s.34.

³⁰⁶ Osman AYTAÇ, “Siber Terör”, Terör Okulu Eğitim Programı Bildirisi, (Bahçeşehir Üniversitesi, İstanbul, 09 Aralık 2006).

Uzmanların bir kısmı siber terörün gerçek bir tehdit olduğundan hareketle, geniş çaplı bir siber saldırının etkilerinin önceden kestirilemeyeceğini ve terör olarak tanımlanacak derecede büyük bir ekonomik hasara, korkuya ve sivil kayıplara neden olabileceğini, teknolojideki gelişmelerle birlikte bu tehdidin her geçen gün arttığını ifade etmektedirler.³⁰⁷

Siber terör tehdidinin varlığını savunanlar, mevcut terörizm tanımlarından yola çıkarak, potansiyel siber terör eylemleri konusunda çeşitli senaryolar üretmektedirler. Buna göre bir siber terörist;³⁰⁸

- Gıda fabrikalarının üretim sürecini yöneten bilgisayar sistemlerini ele geçirerek, besin bileşenlerinin oranlarını değiştirip bütün bir ulusun sağlığını tehdit edebilir,
- Bankaları, uluslararası finans sistemlerini ve borsa işlemlerini çökerterek, vatandaşların ekonomik sisteme olan güvenlerinin kaybolmasına neden olabilir,
- Gelecek nesil hava trafiği kontrol sistemlerine saldırarak, yolcu uçaklarının çarpışmalarına ya da düşmelerine neden olabilir. Bu durum aynı zamanda demiryolları için de geçerli olabilir,
- İlaç üreten bir şirketin bilgisayarlarını ele geçirerek, ilaç bileşenlerini değiştirmek suretiyle tahmin edilemeyecek sayıdaki insanın hayatını yitirmesine sebebiyet verebilir,
- Bir şehrin trafik ışıklarını ya da metro trenlerine yön veren sinyalizasyon sistemine müdahale ederek kitlesel ölümlere yol açabilir,
- Bunlara ilaveten siber teröristler, elektrik ve gaz nakil hatları, petrol boru hatları, barajlar vb. kritik birçok tesise karşı yıkıcı ve ölümcül saldırılar gerçekleştirebilir. Sonuçta, siber teröristlerin bir ulusun yeme, içme, hareket etme ya da yaşamasını engelleyebileceği açıktır. Bu durum siber terör tehdidinin abartılı olmadığını düşünenler için bilim kurgu değildir ve bu senaryolar bugün gerçekleşebilecek niteliktedir.

³⁰⁷ Rollins, Wilson, **a.g.e.**, s.3.

³⁰⁸ Barry C. Collin, "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", 11th Annual International Symposium on Criminal Justice Issues, (Çevrimiçi), <http://afgen.com/terrorism1.html>, 07 Şubat 2007.

Siber terör tehdidinin gerçek potansiyelini anlayabilmek için iki unsur göz önüne alınmalıdır. Birincisi, bu tarz saldırıları gerçekleştirebilecek kabiliyet ve motivasyona sahip kişilerin var olup olmadığı, ikincisi ise şiddet ve ciddi hasara yol açacak derecede hassas hedefler bulunup bulunmadığıdır.³⁰⁹

İlk soruya verilecek cevap olumludur. Terör örgütlerinin bir gün bilgisayarları silah olarak kullanmak amacıyla, bilgisayar teknolojileri konusunda bilgi sahibi gençleri üye yapma konusunda her geçen gün daha fazla çalıştıklarına inanılmaktadır.³¹⁰ Buna ilaveten, yeni bilgisayar yetenekleri geliştirdikleri ya da kendilerine yüksek seviyede bilgisayar yeteneğine eriştirecek siber suçlularla ittifaklar kurabilecekleri birçok uzman tarafından belirtilmektedir. Tarihsel olarak bakıldığında teröristler bilgisayar başında günde yirmi saat civarında çalışan insanlar değildir. Ancak, bilgisayar korsanlarının çeşitli nedenlerle teröriste dönüşmesi ihtimali her zaman vardır.³¹¹

Bazı bilgisayar korsanı grupları uluslarüstü ya da dini veya diğer sosyo-politik ideolojilere dayalı siyasi çıkarlar için küresel olarak dağılmış olabilirler. Diğer bir kısmı ise, itibar veya kazanç sağlama arzusu ile motive olabilir ya da organize suç örgütleri ile bağlantı kurabilir. Bu durumda bilgisayar kabiliyetlerini siyasi motivasyonu önemsemeden bir ulus devlet ya da terörist guruba para karşılığı satmaya niyetlenebilir. Hindistan ayrılıkçı örgütü Harkat-ül Ansar'ın bilgisayar korsanlarından 1998 sonlarında askeri yazılım tedarik etmeye çalışması³¹² buna bir örnektir.

İnternet ve bilgisayar güvenliği yetersizlikleri konusunda devam eden kanı, teröristlerin muhtemel ağ saldırılarına ya da ülkelerin kritik altyapı tesislerine karşı siber saldırılara teşebbüs konusundaki ilgilerini artırabilir. FBI, teröristlerin büyük çaplı geleneksel saldırılarını siber saldırılarla destekleyeceklerini ya da bu amaçla bilgisayar korsanlarını kiralayabileceklerini öngörmektedir.³¹³ Mart 2000'de Japon başkent polisinin 150 polis aracını takip edebilmesi için temin edilen yazılım sisteminin, 1995 yılında Tokyo metrosunda zehirli gaz saldırısı ile 12 kişinin ölümüne 6000'den fazla kişinin ise yaralanmasına neden olan, Aum Shinryko isimli

³⁰⁹ Denning, a.y.

³¹⁰ Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", **CRS Report for Congress**, s.1., 17 Ekim 2003, (Çevrimiçi), <http://www.fas.org/irp/crs/RL32114.pdf>, 27 Kasım 2006.

³¹¹ Collin, a.y.

³¹² Wilson, a.g.e., s.14.

³¹³ Rollins, Wilson, a.g.e., s.1.

tarikat tarafından geliştirildiği tespit edilmiştir. Tespitin yapıldığı sırada tarikatın 115 polis aracına ait izleme bilgilerini elinde bulundurduğu belirlenmiştir. Tarikat aynı zamanda diğer firmaların taşeronu olarak da çalışmıştır.³¹⁴ Bunun da ötesinde, en az seksen adet Japon firmasına ve on kadar hükümet birimine yazılım sistemi tasarlamıştır. Grup başka yazılım firmalarının kritik kademelerinde örgütlenerek izlerini gizleyebilmiş ve bu yöntemle birçok özel ya da resmi birim için “Truva atları” hazırlayabilmiştir.³¹⁵

Siber terör tehdidini savunanlara göre ikinci sorunun cevabı da olumludur. Kritik altyapı sistemleri oldukça karmaşıktır ve bu karmaşıklık mutlaka terörist eylemlerin faydalanabileceği bir açık barındırmaktadır.³¹⁶ Bilgisayarlarla kontrol edilen sistemlerdeki birçok zayıflığın giderilebilir olmasına karşın, tümüyle ortadan kaldırılması mümkün değildir. Daha önce de belirtildiği gibi teknolojinin kendisi iyi bir güvenlik sağlasa dahi, sıklıkla tasarlanış ya da kullanılış şekli saldırılara karşı açıklar barındırmaktadır. Buna ilaveten, daima tek başlarına ya da teröristlerle birlikte hareket eden ve erişim yetkilerini kötü amaçlarla kullanabilecek iç saldırganların bulunma olasılığı da vardır. Rus doğal gazını tekelinde bulunduran Gazprom şirketi, içeriden bir çalışanla işbirliği yapan iki bilgisayar korsanı tarafından saldırıya uğramış, saldırganlar boru hatlarındaki gaz akışını kontrol eden ana kumanda merkezinin kontrolünü ele geçirmek için bir Truva atı kullandıklarını ifade etmişlerdir. Ancak, söz konusu iddia Gasprom yetkilileri tarafından inkâr edilmiştir.³¹⁷

Günümüzde birçok özel firmada ve kritik altyapı tesisinde, faaliyetlerin otomatik olarak gözlenmesine, üretim, uyarılma ve bir takım kontrol işlemlerinin algılayıcılardan alınan geri besleme ile gerçekleştirilmesine imkân veren, kısaca SCADA (Supervisory Control And Data Acquisition) olarak adlandırılan sistemler kullanılmaktadır. Bazı uzmanlar bu sistemlerin siber saldırılara hassas olduğu ve teröristler için çekici hedefler teşkil edebileceklerini belirtmektedirler. Son yıllarda, yeni altyapı kurmanın maliyeti ve zaman alması nedeniyle, endüstriyel kontrol sistemleri artan oranda piyasadan temin edilen yazılımlar ve İnternet üzerinden tesis edilen bağlantılarla çalıştırılmaktadır. Dolayısıyla bu durum söz konusu sistemlerin saldırılara karşı hassasiyeti artırmaktadır.³¹⁸

³¹⁴ Denning, a.y.

³¹⁵ Sandıklı, Yıvciger, a.g.e., s.10.

³¹⁶ Sandıklı, Yıvciger, a.g.e., s.14.

³¹⁷ Denning, a.y.

³¹⁸ Wilson, a.g.e., s.8.

Avustralya'da Nisan 2002'de meydana gelen bir olay SCADA istismarı ile ilgili iyi bir örnektir. Söz konusu olayda bir bilgisayar korsanı, İnternet bağlantısını kullanarak baraj kapaklarını açmış ve milyonlarca metre küp suyun akışını sağlamıştır. Polis tarafından yakalandığında, şahsın daha önceden barajlar için yazılım üreten bir şirkette çalıştığı tespit edilmiştir. Bu olay, terörist gruplar tarafından istismara meyilli çalışanların kendi saflarına katılmalarının mümkün olabileceğini göstermiştir.³¹⁹

Siber terör tehdidi konusunda karşıt ve iyimser görüşe sahip uzmanlar ise geniş çaplı bir siber saldırının bir bomba ya da diğer kimyasal biyolojik radyolojik veya nükleer patlayıcılar gibi terör etkisi yaratmayacağını, sadece basit bir rahatsızlık üretebileceğini düşündükleri için "siber terör" teriminin uygun olmadığını ve siber terör konusundaki risklerin fazla abartıldığını değerlendirmektedirler.³²⁰

Karşıt görüşlü uzmanlar, siber terör tehdidi ile ilgili literatürün en büyük hatasının, bilgisayar ağlarının hassasiyeti ile kritik altyapı tesislerinin hassasiyetinin eşit olarak kabul edilmesi ve bu hassasiyetlerin ulusal güvenliği önemli bir risk altında bıraktığı sonucuna varılması olduğunu ifade etmektedirler. Onlara göre bilgisayar teknolojisinin nispeten yeni olması ve her alanda hızla yaygınlaşması göz önüne alındığında bu kabul şaşırtıcı değildir. Ancak, bilgisayar ağları ve kritik alt yapı sistemlerine daha yakından bakıldığında, bu kabulün yanlış olduğunun ortaya çıktığını düşünmektedirler.³²¹

Kritik alt yapı sistemlerinin hassas olduğu konusundaki görüşe karşılık, ne kadar hassas olsa da bir saldırının yaratacağı zararın bahsedildiği kadar büyük olmayacağı görüşündedirler. Kritik altyapı sistemleri sağlam ve esnek olduğundan siber terör teorisyenlerinin sözünü ettikleri saldırılar sonrasında hızla eski haline geri dönebilecektir. Onlara göre, siber terör senaryosu içerisindeki ekonomik işlemler, güç kesintileri, hava trafiği karmaşaları, ulusal güvenliği hiçbir zaman etkilemeyen alışlagelmiş olaylardır. Bugüne kadar doğal afetlerden ya da diğer sistem arızalarından kaynaklanan sorunların hiçbir zaman ulusal güvenliği tehdit edecek boyuta ulaşmamış olması, kritik altyapı tesislerinin muhtemel bir siber terör olayından sonra da hızla toparlanacağını kanıttır.³²²

³¹⁹ Sandıklı, Yivoiger, a.g.e., s.14.

³²⁰ Wilson, a.g.e., s.1.

³²¹ James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", s.1.

³²² Rollins, Wilson, a.g.e., s.7.

Kritik alt yapı sistemleri oldukça karmaşıktır. Ancak, bu karmaşıklık tehdidi savunuların iddialarının aksine saldırıları güçleştirmektedir.³²³ Bahsedilen SCADA sistemlerini firmaların teknik donanımlı çalışanları dışında kullanabilecek insan sayısı çok azdır.³²⁴ Birbirlerine bağlı sistemlerin her birinde farklı teknolojilerin kullanılması, her bir sistemin detaylarının anlaşılması ve buna uygun saldırı tekniğinin uygulanmasını gerektirmektedir. Siber teröristlerin ulusal güvenlik açısından kayda değer bir tehlike yaratmaları için çok sayıda hedefe, eşzamanlı ve uzun süreli, hatta klasik terör saldırıları ile koordineli saldırılar düzenlemeleri gerekmektedir. Ancak, sürekli ve çok yönlü saldırı yapmak bilgisayar korsanları, teröristler ya da ülkeler için yakalanma riskini artıracığından makul bir seçenek değildir.³²⁵ Buna ilaveten kritik alt yapı tesislerinde çalışanlar doğal afetlere ve sistem arızalarına karşı deneyimli olduğu için, insan eliyle verilen bir zararı onarmakta da çok zorlanmayacaktır.³²⁶

Bu tarz saldırıları gerçekleştirebilecek kabiliyet ve motivasyona sahip kişilerin var olup olmadığına gelince birçok bilgisayar korsanı bilgisayar sistemlerine saldırarak bilgi, yetenek ve araçlara sahip olmalarına rağmen genel olarak şiddet ve ciddi ekonomik ya da sosyal zarar yaratma motivasyonundan yoksundur. Çünkü yaratacakları şiddet ve zarar kendilerini de etkileyecektir. Bunun aksine şiddet yaratmaya motive olmuş teröristler de siber uzayda bu derecede bir şiddet yaratma kapasitesinden ve yine motivasyonundan yoksundur.³²⁷

Diğer bir husus da terörün amacı ile ilgilidir. Teröristler siyasi bir ideoloji ortaya koymak amacıyla psikolojik etki ve fiziksel zarar yaratmaya çalışırlar. Terörizmin siyasi hedefleri gerçekleştirmek maksadıyla şiddet yaratmayı amaçlamasından dolayı, karşıt görüşlülere göre bu etkiyi yaratmayan siber saldırılar, amaca yönelik olmayacaktır. Patlayıcılar ve ateşli silahlar sürekli bir korku etkisi yaratmakta iken, kurbanların farkında bile olmayacakları, alışlagelmiş ve doğal sebeplere bağlanabilen siber saldırılar, bu açıdan yetersiz kalacak ve bir silah olarak tercih edilmeyecektir.³²⁸

³²³ Bosch, a.g.e., s.68.

³²⁴ Sandıklı, Yivciger, a.g.e., s.14.

³²⁵ Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", s.3.

³²⁶ Sandıklı, Yivciger, a.g.e., s.14.

³²⁷ Denning, a.y.

³²⁸ Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", s.8.

Bazı uzmanlar ise konuya daha da iyimser bakarak “saldırı” terimi yerine tarafsız bir kavram olarak değerlendirdikleri “kaza” terimini kullanmaktadır. Bunlara göre bilgisayar kazalarının en az yarısı sistem tasarımlarında yapılan hatalar, yazılımların virüs bulaşmasını kolaylaştıran algoritma hataları, bilgi güvenliği politikalarının teknik ve idari olarak yanlış uygulanması ve kullanıcıların eğitim eksikliği gibi hassasiyetler sonucunda meydana gelen kasıtsız olaylardır. Kazaların geri kalan yarısı ise öncelikle, genellikle kızgın çalışanların oluşturduğu, çoğunluğu kurum içinden çalışanların kötü, suç teşkil eden siyâsi niyetlerinden kaynaklanmaktadır. Kötü eylemin ufak bir bölümü, teröristlerden ziyade bilgisayar korsanları tarafından meydan okuyarak itibar kazanmak veya maddi menfaat sağlamak amacıyla gerçekleştirilmektedir.³²⁹

Siber terör tehdidi ister abartılı, ister gerçekçi bir değerlendirme olsun, geçmişte yaşanan bazı olaylar siber saldırıların ölümcül sonuçlara doğurabileceğini göstermiştir. 1998 yılında meydana gelen bir olayda, on iki yaşında bir erkek çocuğu Arizona’daki iki kasabayı sel altında bırakabilecek ve en az bir milyon insanın hayatını tehlikeye sokabilecek büyüklükteki Roosevelt barajının kontrol merkezine erişmeyi başarmıştır.³³⁰ Benzer şekilde 1994 yılında bir İngiliz bilgisayar korsanı, Liverpool hastanesi bilgisayar sistemine girerek, hastaların ilaç reçetelerindeki karışım oranlarında değişiklik yapmıştır. Reçetesinde zehirlenmeye sebep olacak dozda karışım bulunan dokuz yaşındaki bir hasta, hemşirenin reçeteleri yeniden kontrol etmeye karar vermesi neticesinde şans eseri kurtulmuştur. Silahla yaralanan bir hasta ise onun kadar şanslı olamamıştır. Söz konusu hasta, bilgisayar sistemine giren saldırganın değiştirdiği reçete gereği verilen yüksek dozda penisilinden dolayı hayatını kaybetmiştir.³³¹

Başka bir olayda ise Massachusetts’te bir genç, yerel bir telefon santralinin kontrolünü ele geçirmiş ve yerel telefon şebekesini servis dışı bırakmıştır. Ancak, bu santralin aynı zamanda yakında bulunan bir havaalanının pist ışıklarını kontrol etmesi, havaalanını da kullanılamaz hale getirmiştir. Şans eseri küçük bir havaalanı olması bir faciayı önlemiştir.³³²

³²⁹ Bosch, a.g.e., s.67.

³³⁰ Rohas Nagpal, “Cyber Terrorism in the Context of Globalization”, **II World Congress on Informatics and Law (Spain) Tebliği**, s.3., September 2002, (Çevrimiçi), <http://www.ieid.org/congreso/ponencias/Nagpal,%20Rohas.pdf>, 29 Aralık 2006.

³³¹ A.y.

³³² “Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport.”, U.S. Department of Justice, Press Release. Mar. 18, 1998, p.1., akt: Gabrys, a.g.e., s.25.

Buna rağmen bu örneklerin siber terör riskini doğruladığını değerlendirmek aceleci bir yaklaşım olacaktır. Zira “siber terörizm” ve “bilgisayar korsanlığı” arasındaki farkın anlaşılması son derece önemlidir. Kişisel ya da kurumsal bilgisayar sistemlerine zarar veren, kayıtlı bilgileri yok eden korsan saldırıları, siber terörizmde olduğu gibi politik maksatlarla motive olmamaktadır. Protesto amacı taşımazlar, öldürmek ya da yaralamak gibi amaçları yoktur. Bununla birlikte daha önce de belirttiğimiz gibi bilgisayar korsanlığı siber terörizmin tehlike potansiyeli hakkında ipucu vermekte ve teröristlerin de bilgisayar korsanlarının kullandığı metotlara benzer metotlar kullanarak büyük hasara yol açabileceklerini göstermektedir.³³³

Günümüzde İnternet ve terörizm arasındaki kesin olarak bilinen yegâne bağlantı, terör örgütlerinin İnternet’i sıklıkla haberleşme, fon sağlama, psikolojik savaş, propaganda, terör elemanlarının hareketliliğinin sağlanması, bilgi paylaşımı, planlama, koordinasyon ve gelecekteki hedefler için istihbarat sağlamak amacıyla kullanmalarıdır.³³⁴ Terör saldırıları için İnternet’in ya da bilgisayarların kullanımına ilişkin kesin bir delil bulunmamakla birlikte; kötü maksatlı saldırı programları hâlihazırda İnternet’ten temin edilebilmekte ve İnternet’e bağlı korumasız bilgisayarları tespit etme ve saldırma imkânı vermektedir. Hatta korunan bilgisayarları dahi rahatsız edebilmektedir.³³⁵

Teröristlerin 11 Eylül saldırılarının planlanması amacıyla İnternet’i kullandıkları konusunda güçlü kanıtlar bulunmaktadır.³³⁶ 11 Eylül saldırılarının lideri Muhammed Atta’nın uçak bileti rezervasyonunu İnternet üzerinden yaptığı bilinmektedir. Dünya Ticaret Merkezine yapılan saldırıların planlayıcısı Halit Şeyh Muhammed’in, uçakları kaçıran teröristlerden en az ikisi ile haberleşmek için İnternet’i ve bir sohbet programını kullandığı rapor edilmiştir. El Kaide’nin de aralarında bulunduğu uluslararası terör örgütlerinin aynı zamanda optik-elektronik (askeri gece görüş cihazları vb.) cihazlar, özel haberleşme donanımı ve benzeri teknolojiye sahip ilerlemelerden faydalandıkları bilinmektedir.³³⁷ Afganistan’da ele geçirilen bilgisayarlarda bulunan kayıtlardan El Kaide terör örgütünün hedefler hakkında bilgi toplamak ve şifreli mesajları iletmek üzere İnternet’i kullandıkları rapor edilmiştir. 16 Eylül 2002’de yayınlanan bir raporda yine El Kaide’nin Amerika’daki hücrelerinin

³³³ Sandıklı, Yiciger, a.g.e., s.7.

³³⁴ Charlie Fuller, “The Community of Cyberspace”, **Cyber Crime**, 2003, s.18.

³³⁵ Wilson, a.g.e., s.1.

³³⁶ Timothy L. Thomas, “Al Qaeda and The Internet: The Danger of Cyberplanning”, s. 112, 2003, (Çevrimiçi), <http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf>, 27 Kasım 2006.

³³⁷ Wilson, a.g.e., s.12.

kendi arasında ve denizaşırı hücrelerle haberleşme için İnternet tabanlı telefon sistemini kullandıkları belirtilmiştir. Bu olaylar İnternet'in teröristlerce planlama ve haberleşme aracı olarak kullanıldığını göstermektedir. Günümüz koşullarında siber uzayın planlama amaçlı kullanımı, teröristler açısından üzerinde çok konuşulan ve korkulan siber terör saldırılarına nazaran daha fazla önem arz etmektedir.³³⁸

Siber terörizm hâlihazırda yakın bir tehdit olarak görünmemekle birlikte, bu durum her an değişebilir. Bir terörist için siber terör eylemi klasik eyleme nazaran birçok avantaj sağlamaktadır. Bunlardan birisi de büyük bir medya ilgisidir. Gazetecilerin, habercilerin ve toplumun herhangi bir siber terör saldırısı karşısında neredeyse büyülenmişe dönmesi muhtemeldir. Aslında siber terörizm hükümetler ve medya tarafından gösterilen muazzam ilgi nedeniyle çok çekici hale gelebilir.³³⁹ Terör örgütlerince kullanılacak yeni taktikler bir kez medya da büyük yankı uyandırdığında, diğer gurupları da benzer taktikler kullanmak yönünde motive edebilir.³⁴⁰

Nükleer silahlar, hassas askeri sistemler ve dünyanın önde gelen ulusal teşkilatlarının bilgisayar sistemleri oldukça iyi korunmaktadır. Kritik tesislere herkese açık ağlardan hangi dereceye kadar erişilebileceği ve kritik işlemler sırasında insanların kontrol sürecindeki etkisi ve bu süreçlere dahil olma seviyeleri, bu sistemlerdeki süreçlerin sürekli gözlendiği düşünüldüğünde, endüstrileşmiş büyük ülkelerdeki altyapı tesislerinin siber saldırılara karşı dayanıklı ve esnek olduğu ortaya çıkmaktadır.³⁴¹ Bu sistemlere dışarıdan erişmek çok zordur. Bununla birlikte özel sektördeki sistemler daha az güvenli ve muhtemel tehlikelere karşı daha hassastır. Siber terörizm potansiyelinin abartıldığı düşünülebilir. Ancak böyle bir tehdidi inkâr etmek ya da görmezlikten gelmek yanlıştır. Terörle mücadelede elde edilen başarı teröristleri siber terörizm gibi olağandışı yöntemlere yöneltebilir.³⁴²

Terör uzmanlarının ifadesine göre; kaçırılan uçaklar, bomba yüklü kamyonlar ve biyolojik silahlar en azından şimdilik siber terörizme kıyasla daha fazla tehlikelidir. Ancak, 11 Eylül nasıl bütün dünyaya büyük bir sürpriz yaşatmışsa, gelecekte de siber saldırılar bütün dünyaya aynı şekilde büyük bir sürpriz yaşatabilir. Siber

³³⁸ Thomas, a.g.e., s.112.

³³⁹ Denning, a.y.

³⁴⁰ Wilson, a.g.e., s.12.

³⁴¹ Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", s.10.

³⁴² A.e., s.1.

terörizm kavramı yanlış kullanılıyor veya abartılıyor olabilir ancak bu inkâr edilmesi anlamına gelmemelidir.

Sonuç olarak; gelecek nesil teröristler bugünkülerden farklı olarak sayısal bir dünya içerisinde doğacak ve siber saldırı araçlarını daha kolay kullanacak şekilde yetişeceklerdir. Sahip olacakları siber yeteneklere ve bilgisayar bilgisine bağlı olarak, siber terör eylemlerinde daha büyük bir potansiyel görebileceklerdir. Mevcut siber terör tehdidi karşısında fazla endişeye gerek yok gibi gözükmektedir. Bununla birlikte, teknolojik gelişmelerin son yıllarda özellikle bilişim sektöründe müthiş bir atak yaptığı dikkate alınmalıdır. Günümüzde artık bilgi üretimi, bilgi depolanması ve yayını ile ilgili gelişmeler baş döndürücü bir hız almıştır. 1760 yılına kadar üretilen bilgi, 1760–1950 yılları arasında ikiye katlanmış ve her 2–3 yılda bir ikiye katlanmaktadır.³⁴³ Kimi kaynaklara göre ise, 1980’li yıllardan sonra bilginin ikiye katlanma süresi bir yılın da altına inmiştir.³⁴⁴ Bu hızlı gelişim ile gerçek dünya ve siber uzay her geçen gün yeni geliştirilen teknolojiler ve donanımlar sayesinde birbiri ile iç içe geçtikçe, siber terör daha çekici ve etkili bir hal alabilecek ve gelecekte sistemler yeterince güvenli hale getirilmediğinde, sanal dünya da gerçek zararlar yaratmak bugün bir İnternet sitesini çökertmekten daha kolay hale gelebilecektir.³⁴⁵

Bu nedenle, ulusal bilgi altyapısı oluşturulurken geleceğe yönelik bir vizyon içerisinde, hem teknik güvenlik tedbirlerinin tesisinde hem de yasal düzenlemelerde siber terör gerçeğinin şimdiden göz önünde bulundurulmasının büyük önem taşıdığı değerlendirilmektedir.

5. EKONOMİK BOYUT

Ekonomik güvenlik; “bir ülkenin, ekonomik çıkarlarını korumak maksadıyla, bu çıkarları önleyen veya tehdit eden olayları, gelişmeleri veya eylemleri durdurması”³⁴⁶ şeklinde tanımlanmaktadır. Ekonomik güvenlik çok boyutlu bir kavramdır ve ekonomi ile güvenlik arasında çok yönlü bir ilişki vardır. Ekonomi bir güvenlik tehdidi, güvenlik politikalarının bir amacı veya güvenliğin sağlanmasında bir araç

³⁴³ Mahmut Kiper, “Teknoloji Transfer Mekanizmaları ve Bu Kapsamda Üniversite Sanayi İşbirliği”, **TMMOB 50. Yıl Yayınları....Teknoloji**, Ed. Mahmut Kiper, Ankara, Kozan Ofset, 2004, s.64.

³⁴⁴ İsmail Hakkı Yücel, “Bilim-Teknoloji Politikaları ve 21 Yüzyılın Toplumu”, s.12., 1997, (Çevrimiçi), <http://ekutup.dpt.gov.tr/bilim/yuceli/biltek.html>, 07 Ocak 2007.

³⁴⁵ Denning, a.y.

³⁴⁶ Charles Wolf Jr., “The Economic Dimension of National Security”, RAND, National Defence Research Division, 1994, s.xii, akt: Hasan Köni, “Ekonomik Güvenlik ve Uluslararası İlişkiler ve Türkiye”, **Uluslararası Çatışma Alanları ve Türkiye’nin Güvenliği**, Ed: Gamze Güngörmüş Kona, İstanbul, IQ Kültür Sanat Yayıncılık, 2005, s.393.

olabilmektedir.³⁴⁷ Küreselleşme sürecinde ekonomik güç, yeni güç dengelerinin belirleyici bir unsuru olarak ön plana çıkmış³⁴⁸ ve yeni tehdit ve risklerin ortaya çıktığı günümüzde, güç mücadeleleri askeri zeminden daha çok ekonomik zemine kaymıştır.³⁴⁹ Bu nedenle küreselleşmenin şu anki lokomotifi olan bilişim teknolojileri ve bunun başlıca aracı ve simgesi olan İnternet'in güvenliği, ekonomik anlamda önem kazanmıştır.³⁵⁰

Bilişim sistemlerinin modern ekonomide çok önemli bir yeri olduğu ve bilgi dolaşımı gerçekleşmediğinde ekonominin tüm sektörlerinin de zafiyete uğrayacağı açıktır. Bilgisayar sistemleri ve ağ bağlantısı bulunmadığı zaman finans, bankacılık, toptan ve perakende satış, taşımacılık, üretimin büyük bir kısmı ve hizmet sektörü yavaşlayacak, hatta emeklemeye başlayacaktır. Hayati öneme sahip kamusal hizmetler, sağlık sektörü ve neticede ulusal güvenlik de eşit derecede etkilenecektir.³⁵¹

Siber saldırıların ekonomik kayıplara neden olduğu bilinmektedir. Ancak, saldırıların ekonomik maliyetini ölçmek için standart bir metot bulunmaması ve şirketlerin mali kaygılarla bu tarz saldırıları kamuoyundan gizlemek istemeleri, saldırıların kesin sayısının bilinmesine ve zararın gerçek maliyetinin hesaplanmasına engel olmaktadır.³⁵²

Bireylere yönelik saldırılar genellikle kişisel çapta mali kayıplara yol açtıkları için ulusal bir tehdit olarak görülmemektedir. Çoğunlukla kimlik ve banka hesap bilgilerinin veya kredi kartı bilgilerinin çalınması, sahte yatırım teklifleri ve ürünlerin teslim edilmediği siparişler şeklinde işlenen dolandırıcılık suçları ile karşılaşılmalıdır. Ancak, bireylere karşı işlenen bu suçların artması ve ciddi boyutlara ulaşması durumunda daha büyük ekonomik kayıplara neden olması da muhtemeldir. Avrupa genelinde 2001 yılında yapılan araştırma ekonomik suçların önemini gözler önüne sermiştir. Söz konusu araştırmaya göre 1999 ve 2000

³⁴⁷ Helen E. S. Nesadurai, "Introduction: Economic Security, Globalization and Governance", **The Pacific Review**, C.XVII, No.4, 2004, s.459.

³⁴⁸ Turgut, **a.g.e.**, s.42.

³⁴⁹ **A.e.**, s.44.

³⁵⁰ Dr. Andrew Mango, "Küreselleşme Bağlamında Medya Bilgi Harekatı ve Uluslararası Güvenlik", Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, s.114.

³⁵¹ Brian Cashell v.d., "The Economic Impact of Cyber-Attacks", s.1., **CRS Report for Congress**, April 1, 2004, (Çevrimiçi), http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf, 09 Mart 2007.

³⁵² **A.e.**, s.14.

yıllarında Avrupa genelindeki büyük şirketlerin %42,5'inin dolandırıcılığa maruz kaldığı tespit edilmiştir. Bunun sonucunda ortalama 6,7 milyon Euro ekonomik zarar meydana gelmiştir.³⁵³

Siber saldırılar konusunda ekonomik boyutun ilk akla gelen bileşeni siber saldırıların önlenmesi amacıyla, kişisel, resmi ya da özel kuruluşlar ve hükümetler tarafından alınan güvenlik tedbirleri için yapılan güvenlik harcamalarıdır. İnternetin giderek artan bir şekilde birey, hükümet, iş, finans, bankacılık ve ticaret hayatının vazgeçilmez bir parçası haline gelmesi ve buna bağlı olarak artan tehditler, ciddi ve yüksek maliyetli tedbirlerin alınmasını gerektirmektedir. Örneğin 1999 yılından 2000 yılına geçişte yaşanan ve dünya çapında büyük endişe yaratan 2000 yılı sendromu (Y2K) nedeniyle,³⁵⁴ hükümet kayıtları, bankacılık, sağlık ve birçok önemli sektördeki yazılım ve donanımların yedeklenmesi ve yenilenmesi amacıyla, yarısı ABD'de olmak üzere yaklaşık 200 milyar dolar harcanmıştır.³⁵⁵

Ekonomik boyutun diğer bir bileşeni ise saldırı sonrasında ortaya çıkan ekonomik maliyettir. Bu maliyetin hesaplanması ilkinde göre biraz daha karışık ve çok yönlüdür. Zira, birçok bileşenin göz önüne alınmasını gerektirmektedir. Saldırı sonrasında oluşan maliyet doğrudan ve dolaylı maliyet olmak üzere iki bölüme ayrılmaktadır.³⁵⁶ Doğrudan maliyet, saldırı sonrasında bilgisayar sistemlerinin ve verilerinin tekrar saldırı öncesi hale getirilmesi ve hizmet kesintisinden dolayı meydana gelen gelir kaybını içermektedir. Bir saldırı sonrasında sistemin yeniden eski haline getirilmesi uzman teknisyenlerin çalışması gibi ilave işgücü ve malzeme gerektireceğinden bir maliyet oluşturmaktadır. Saldırıdan sistemin fiziksel zarar görmesi, sistemin değiştirilmesini ya da zarar gören yazılımların yenilenmesini gerektirebilmektedir. Bunlar en kolay ölçülebilecek maliyetlerdir.³⁵⁷ Siber saldırılar, saldırı için gereken mali kaynak ile karşılaştırılamayacak derecede büyük ekonomik maliyetler yaratma riskini taşımaktadır. Filipinlerde bilgisayar eğitimi alan bir öğrencinin, basit bir bilgisayar ile yarattığı ve 2000 yılı Mayıs ayında İnternet'e

³⁵³ "Economic Crime Survey 2001: European Report", s.1., (Çevrimiçi), http://www.pwc.com/gx/eng/cfr/gecs/pwc_2001_europe_crimesurvey.pdf, 26 Mart 2007.

³⁵⁴ Cashell v.d., a.g.e., s.40.

³⁵⁵ "Y2K bug", **Britannica Concise Encyclopedia**, (Çevrimiçi), <http://concise.britannica.com/ebc/article-9383056/Y2K-bug>, 27 Mart 2007.

³⁵⁶ Cashell, v.d., a.g.e., s.15.

³⁵⁷ Michael Erbschloe, **Implementing Homeland Security for Enterprise IT**, Burlington, MA: Digital Press, 2004, s.125.

bulaştırdığı “The Love Bug” virüsünün,³⁵⁸ dünya genelindeki bilgisayar kullanıcılarına maliyeti tahminen 3 ila 15 milyar dolar arasında gerçekleşmiştir. Bu olay siber saldırıların küresel ekonomi için büyük bir tehdit olabileceğinin de göstergesi olmuştur.³⁵⁹

Diğer bir doğrudan maliyet ise saldırı sonucunda meydana gelen hizmet kesintisidir. Hizmet kesintisi, gelir kaybı ve çalışanların verimliliğinin kaybolması ile sonuçlanmaktadır. Kaybedilen gelir saldırı öncesi dönemle kıyaslanmak suretiyle bu maliyet kolayca bulunabilir. Ancak, önceden ödeme yapılan çalışanların kaybolan verimliliklerinin hesaplanması daha zor bir konudur. Kaybedilen gelir saldırı öncesi duruma tekrar dönülünceye kadar olan süresiyle sınırlıdır, daha sonra telafi edilebileceği için geçicidir. Ancak, müşterilerin hizmet kesintisi esnasında yapacakları rakip firma tercihleri değişmediği takdirde, bu sonuç kalıcı olmaktadır.³⁶⁰

Dolaylı maliyet ise bir saldırının gerçek hedefi dışında diğer bireyler ve kurumlar için oluşturacağı ekonomik zararı içermektedir. Bir şirketin bilgisayar sistemlerine yapılacak saldırı, bu şirketin tedarik zincirinin alt ve üst kademesinde bulunan diğer şirketleri de etkileyebilecektir. Bir İnternet servis sağlayıcı veya bir e-ticaret firması saldırı nedeniyle hizmet veremeyecek hale geldiğinde, müşteriler de bundan zarar görecektir. İlk bakışta bu durum saldırıya uğrayan şirket için zararın maliyetine etki etmiyor gibi görünse de aslında önemli etkiler yaratabilmektedir.³⁶¹

Günümüzde ekonomik kayıplara neden olan bir diğer husus da mali değeri olan ticari bilgiye yöneltilen yasadışı eylemlerdir. Elektronik ortamda bulunan fikir ve sanat eserlerine yönelik telif haklarının ihlal edilmesi, hem bu eserlerin sahipleri hem de bu eserlerin ticareti üzerinden vergi yoluyla kazanç sağlayan ülke ekonomisi açısından ekonomik bir kayıp oluşturmaktadır. Sayısal teknoloji ve İnternet yazılı eserler ile müzik ve film gibi çoklu ortam eserlerinin mükemmel bir şekilde çoğaltılmasına ve kolayca dağıtılmasına imkân vermektedir. Bu kolaylık eserlerin kişisel kullanım veya daha ucuz fiyatlara satılması için çalınmasını çekici hale

³⁵⁸ “Philippine Officials Charge Alleged 'Love Bug' Virus Creator”, CNN, June 29, 2000, (Çevrimiçi), <http://archives.cnn.com/2000/TECH/computing/06/29/philippines.lovebug.02/index.html>, 14 Mart 2007.

³⁵⁹ Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats”, s.9.

³⁶⁰ Cashell v.d., a.y.

³⁶¹ A.e., s.16.

getirmektedir.³⁶² Bu durum kayıt altına alınamayan ve haksız kazanç sağlanan kontrolsüz bir pazarın da ortaya çıkmasına neden olmaktadır.

Siber saldırıların toplumda yaratacağı olumsuz psikolojik etki ise bir diğer unsurdur. Ulusal güvenliğe etki edecek gizli bilgilerin çalınmasının ya da büyük bir şehrin elektriğinin kesilmesinin ulusal güvenlik, kamu güvenliği ve ekonomi için bir İnternet sitesine yapılan saldırıdan daha önemli sonuçlar doğuracağı açıktır. Ancak, en önemsiz kategoride değerlendirilebilecek suçlar dahi insanların İnternet üzerinden alış verişe duydukları güvenin yıkılması, gizliliğin veya telif haklarının ihlali gibi çok büyük sonuçlara neden olabilmektedir. Bir e-ticaret sitesinin kapanmasına neden olacak bir saldırı, İnternet'e dayalı ticaret sektörü üzerinde felaket etkisi yaratabilir. ³⁶³ Dünya da toplam e-ticaret hacminin, 2006 yılında 13 trilyon dolara ulaştığı,³⁶⁴ Türkiye'de ise 2005 yılı tahmini e-ticaret hacminin 6 milyar dolardan fazla³⁶⁵ olduğu göz önüne alındığında, e-ticaretin aksamasına neden olacak bir saldırının, ülke genelinde yaratacağı ekonomik kaybın da büyük olacağı açıktır. Benzer şekilde milyonlarca kredi kartı numarasının çalınması ile sonuçlanacak bir yasadışı erişimin, ülke genelinde kredi kartı ya da İnternet bankacılığı kullanımını önemli ölçüde etkileyerek, bankacılık ve finans sektöründe mali kayıplara neden olabilmesi ve tüketicilerin e-ticarete olan isteklerini azaltabilmesi mümkündür.³⁶⁶

Bunun yanında saldırıya uğrayan şirketlerin veya sektörlerin imajlarının zedelenmesi de yüksek sayıda müşteri kaybına yol açabilmektedir.³⁶⁷ Çok uluslu ya da dünya çapında pazara sahip bir şirketin ününün zedelenmesi, hem bu şirketin merkezi konumundaki ulusal ekonomiye hem de bağlantılı ülke ekonomilerine zarar verebilir. Örneğin 1994 yılında Rus bilgisayar korsanları tarafından Citibank'ın bilgisayar sistemlerine girilerek 10 milyon dolar çalmaları, bankanın en çok kazanç sağladığı yirmi müşterisini rakip bankalara kaptırmasına neden olmuştur.³⁶⁸

³⁶² Peter Grabosky, "Cyber Crime and Information Warfare", s.4., (Çevrimiçi), <http://www.aic.gov.au/conferences/transnational/grabosky.pdf>, 08 Kasım 2006.

³⁶³ Erbschloe, a.g.e., s.110.

³⁶⁴ "E-Ticaret", Bursa Ekonomi Bursa Sanayi ve Ticaret Odası Aylık Yayın Organı, Eylül 2006, <http://www.bursaekonomi.com.tr/default.asp?page=newsopen.asp&opennews=470&qmshow=223>, 11 Nisan 2007.

³⁶⁵ "ABD ve Avrupa, Aldı Başını Gidiyor", Bilişim Dünyası, Haziran 2006, (Çevrimiçi), <http://www.bilisimdunyasi.net.tr/yazi.asp?sayi=4&yazi=355>, 11 Nisan 2007.

³⁶⁶ Erbschloe, a.y.

³⁶⁷ Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", s.9.

³⁶⁸ Nasheri, a.g.e., s.52.

Güvenlik açıkları nedeniyle saldırıya uğrayan firmalar sadece saldırının etkisi ile değil; müşterilerin tepkileri nedeniyle de kayba uğrayabilmektedirler. 1996 ile 2002 yılları arasında meydana gelen 22 siber saldırının ekonomik etkisinin incelendiği bir araştırmada, saldırıya uğrayan firmaların hisse senetlerinin saldırıyı takip eden günde %2,7 oranında düştüğü, saldırıdan üç gün sonra ise bu düşüşün %4,5 seviyesine ulaştığı görülmüştür. Yine aynı araştırmada özellikle kredi kartı bilgilerinin çalınması olmak üzere, mali bilgileri tehlikeye düşüren saldırıların, hisse senedi değerlerinin ilk gün ortalama %9,3 oranında, üçüncü gün ise ortalama %15 oranında düşmesine neden olduğu görülmüştür.³⁶⁹ 2000 yılı ile 2006 yılı Mart ayı arasında müşterilere ait kişisel bilgilerin çalınması veya çalışanlarca satılması gibi toplam 79 olayın incelendiği başka bir araştırma ise güvenlik ihlalleri konusundaki olumsuz haberlerin firmaları, mali açıdan önemli oranda ve olumsuz bir şekilde etkilediğini ortaya koymuştur.³⁷⁰ Bu tespitlere paralel olarak, ülke genelinde meydana gelecek bir tepkinin, borsanın tamamını bir anda etkileyerek ülke ekonomisine büyük zarar vermesi de mümkün olabilir.

Siber saldırıların ekonomi üzerindeki psikolojik etkisi sadece bireysel boyutta değil; daha geniş bir çerçevede de yankı bulabilmektedir. Yatırımın maliyetli ve uzun soluklu bir faaliyet olması, hem yatırım yapılacak iş sektörünün hem de coğrafi bölgenin istikrarlı olmasını gerektirmektedir. Güvenlik, doğrudan yabancı yatırım için belirleyici bir etken olmaktadır. Örneğin Polonya'nın NATO'ya katılmasının üzerinden bir yıl geçtikten sonra doğrudan yabancı yatırım miktarı iki katına çıkmıştır.³⁷¹ Bu nedenle, fiziksel ortamın güvenliği ile paralel şekilde özellikle çok uluslu şirketler için faaliyetlerinin büyük bir çoğunluğunu yürüttükleri siber uzayın güvenliği de önem kazanmaktadır.

Bilgi çağı şirketlerin küresel boyutta rekabet etmelerini, hassas bilgileri rakiplerinden, kötü niyetli kişilerden, müşterilerinden ve yabancı hükümetlerden korurken, şubeleri ve birlikte çalıştıkları diğer şirketlerle güvenli şekilde paylaşımlarını gerektirmektedir. Bir ülkenin ekonomik istikrarı, ulusal güvenliğinin büyük bir bölümünü teşkil etmektedir. Ekonomik istikrar ise ülkenin dünya pazarında etkin bir şekilde rekabet edebilmesine bağlıdır.³⁷² Küreselleşme, artan rekabet ve

³⁶⁹ Ashish Garg, Jeffrey Curtis, and Hilary Halper, "Quantifying the Financial Impact of IT Security Breaches", *Information Management & Computer Security*, C.XI, No.2., pp.74-83. akt: Cashell, v.d., a.g.e., s.5.

³⁷⁰ Alessandro Acquisti, Allan Friedman, Rahul Telang, "Is There a Cost to Privacy Breaches? An Event Study", s.18, (Çevrimiçi), <http://weis2006.econinfosec.org/docs/40.pdf>, 25 Mart 2007.

³⁷¹ Donnelley, a.g.e., s.141.

³⁷² Nasheri, a.g.e., s.1.

fikri ürünlerin giderek önem kazanması, gerek yabancı istihbarat servisleri gerekse çalışanlar tarafından şirketlere ait gizli bilgilerin çalınmasını çekici hale getirmektedir. Az gelişmiş ve ekonomisi zayıf ülkelerin, teknoloji casusluğu ve endüstriyel casusluk gibi yöntemlerle daha çabuk ve masrafsız modernleşmeye çalışmaları da tehdidin başka bir boyutu olarak ortaya çıkmaktadır.³⁷³ Ulusal ekonomilere yönelik diğer bir tehdit ise siber istihbarat yöntemleri ve İnternet sayesinde fiyat tekliflerinin, kontratların ya da fiyat listelerinin gizlice ele geçirilmesi ve uluslararası pazarda rekabet avantajının elde edilmesi suretiyle oluşmaktadır.³⁷⁴

Siber saldırıların ulusal ekonomi açısından yaratacağı tehditlerin en önemlisi ve en etkilisi ise şüphesiz doğrudan haberleşme, finans, bankacılık sektörleri ve enerji sistemleri gibi kritik alt yapı tesislerine yönelik olarak terörist örgütler tarafından gerçekleştirilebilecek siber terör eylemleri ve düşman bir ülkenin ekonomik alt yapıya yönelteceği yıkıcı nitelikteki siber saldırılardır. Bu saldırılar birey ya da şirketlere yönelik saldırıların ulusal ekonomi üzerindeki dolaylı etkisinden çok daha ciddi bir şekilde, doğrudan ulusal ekonominin çökertilesi ile sonuçlanabilecektir. Ancak, küreselleşme ile birlikte artan ülkeler arası ekonomik bağımlılık ve çok uluslu şirketlerin genel çıkarları göz önüne alındığında, bir ulus devletin diğerinin ekonomik alt yapısını çökertmeye yönelik siber saldırı düzenlemesi, kendisi için de göze alınması zor bir risk olarak değerlendirilmektedir. Örneğin Çin askeri yayınlarının bazılarında, siber saldırıların Amerikan finans sektörünü işlemez hale getirebileceği konusunda yapılan spekülasyonlar, Çin'in de aynı finans sektörüne bağımlı olması ve bu saldırılardan belki de daha fazla etkilenebilmesi nedeniyle gerçekçi görünmemektedir. Ancak, bu tarz senaryolar ve siber saldırılar küresel pazar ekonomisine karşı olan devlet dışı aktörler açısından kullanılabilecek potansiyel araçlardır.³⁷⁵

6. BİLGİ SAVAŞI (SİBER SAVAŞ)

Bilgi toplumuna geçişin yarattığı değişikliklerin etkilerinden biri de konvansiyonel savaş anlayışı üzerine olmuştur. Askeri sistemlerin ve orduların teknolojiye ve bilişim sistemlerine olan bağımlılığı oldukça artmıştır. Günümüzde uçak, gemi füze sistemleri gibi birçok silah sistemi, hedef tespit ve ikaz sistemleri, komuta kontrol ve

³⁷³ A.e., s.52.

³⁷⁴ Udo Helmbrecht, "Economic Dimension in Cyber Security", s.2, (Çevrimiçi), http://www.bsi.bund.de/bsi/reden/2006_08_18_Erice.pdf, 26 Mart 2007.

³⁷⁵ Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", s.8.

haberleşme sistemleri bilgisayarlara ve yazılımlara bağımlı olarak çalışmaktadır.³⁷⁶ Buna ilaveten ordu birimleri arasında her türlü bilgi alışverişi, intranet adı verilen ve İnternet'ten bağımsız bilgisayar ağları sayesinde yapılmaktadır. Bu durum, askeri sistemleri ve ülke savunmalarını siber saldırılara karşı hassas hale getirmektedir.

Siber savaş kavramı giderek artan bir şekilde ülkelerin ilgisini çekmekte ve bu yeni savaş türü çeşitli ülkelerin doktrinlerinde yerini almaktadır. Siber savaş ya da bilgi savaşı kavramını kısaca aşağıdaki şekilde tanımlamak mümkündür;³⁷⁷

“Politik ve askeri hedefleri desteklemek için barış, kriz ve savaş dönemlerinde hasımın sahip olduğu bilgi altyapısı, sistem ve süreçlerinin işlevselliğini engellemek, imha etmek, bozmak ve kendi çıkarlarımız için kullanmak amacıyla yapılan hareketlerle; düşmanın bu faaliyetimize karşı önlem almasını engelleyecek ve benzeri harekâtına karşı koyacak tedbirler ve süreçlerin tamamıdır.”

ABD, İngiltere, Fransa, Almanya, Rusya Federasyonu ve Çin siber savaş konusunu ciddi şekilde ele almakta ve bu konuda araştırma ve geliştirme faaliyetlerinde bulunmaktadır.³⁷⁸

Siber savaş tanımından da anlaşılacağı üzere yalnızca askeri hedeflerin, silah ve sistemlerinin ya da komuta kontrol sistemlerinin değil, bir ülkenin ekonomisi dahil bilgi alt yapısının top yekûn hedef alınmasını veya bu alt yapının korunmasını da kapsamaktadır. Bundan dolayı siber savaşın hedeflerini askeri hedefler ve diğer hedefler olmak üzere ikiye ayırmak mümkündür. Ancak, hedefler farklı olsa da amaç bilgi sistemlerinin çökertilmesidir. Geleceğin bilgi savaşlarında kullanılacak saldırı teknikleri daha önce belirtilen siber saldırı teknik ve metotlarının yanı sıra, nano makineler, elektronik karıştırma uygulamaları, HERF (Yüksek enerji radyo frekans bombası) ve EMP (Elektromanyetik titreşim) bombaları gibi yeni teknoloji olanaklarının kullanılmasını da içermektedir.³⁷⁹

Günümüzde bütün ülkeleri tehdit edebilecek siber savaşla ilgili olası

³⁷⁶ Lionel D. Alford, “Cyberwarfare: Protecting Military Systems” **Acquisition Review Quarterly**, Spring 2000, s.100-120.

³⁷⁷ “Çalışma Grubu 4, E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları”, s.5.

³⁷⁸ Steven A. Hildreth, “Cyberwarfare”, s.2, **CRS Report for Congress**, June 19, 2001, (Çevrimiçi), <http://www.fas.org/irp/crs/RL30735.pdf>, 07 Kasım 2006.

³⁷⁹ **Yeni Dünya Stratejileri ve Kilit Ülke Türkiye**, Ed. Ali Kulebi, Ankara, TUSAM MET-VAK Yay., t.y., s.211.

senaryolar genelde iki başlık altında toplanmaktadır. Bunlar;³⁸⁰

- Askeri ve sivil kurumların sistemlerine şimdilik uykuda bulunan virüslerin, dışarıdan temin edilen yazılım ve donanımlara istenildiği zaman uzaktan ya da belli durumların gerçekleşmesi halinde kendiliğinden aktif hale geçecek kötü amaçlı kodların ya da arka kapıların yerleştirilmiş olması,
- Komşu ve potansiyel düşman ülke bilgisayar korsanlarının savaş ve gerginlik durumunda karşı ülke bilişim sistemlerine, kritik askeri ve sivil altyapı tesislerine siber saldırılar düzenlemesi, ülke orduları içerisinde oluşturulan özel birimlerin karşı ülke silah, komuta kontrol, haberleşme, istihbarat sistemlerine, askeri ve sivil bilişim sistemlerine siber saldırılar düzenlemeleri,

Siber savaşın bilinen ilk örneği ise 27 Nisan 2007 tarihinde Estonya'nın başkenti Tallinn'de bulunan ve 2. Dünya Savaşı'nda Alman ordusuna karşı savaşırken ölen Sovyet askerlerini sembolize eden meçhul asker heykelinin sökülmesi sonrasında yaşanmıştır. Avrupa'nın e-devlet uygulaması konusunda öncü ülkelerinden olan Estonya'nın birçok önemli kuruluşunun bilgisayarları aniden felç olmuştur. Devlet başkanlığı ve parlamentosu, bütün bakanlıklar, siyasi partiler, 6 büyük haberleşme kuruluşunun 3'ü, en büyük iki banka ve 2 büyük iletişim kuruluşundaki bilgisayarlar siber saldırılar sonucu çalışamaz duruma gelmiştir. Saldırıların dünyanın her yerinden kaynaklanmasına rağmen, erken aşamalarda bazı saldırganların internet adreslerinin belirlendiğini ve bunların çoğunun Rus kamu kuruluşları olduğunu tespit edilmiştir. 13 gün süren saldırılar, AB ve NATO'da büyük bir endişe ile karşılanmıştır.³⁸¹

Siber savaş bir anlamda daha önceki bölümlerde bilgisayar korsanları, organize suç örgütleri, terör örgütleri ve istihbarat teşkilatları tarafından kullanıldığı belirtilen saldırı araçlarının ve tekniklerinin, bir ülke tarafından veya inisiyatifinde diğer bir ülkeye karşı savaş ve barış zamanında kasıtlı olarak kullanılması anlamına gelmektedir. Kısaca siber savaş, siber saldırı ve siber terör taktik ve araçlarının ulusal bir hedefi gerçekleştirmek ya da süregelen bir savaş desteklemek amacıyla, bir ülke tarafından askeri ve sivil her türlü bilişim sistem ve altyapısına karşı kullanılması ve buna karşı alınan tedbirler şeklinde tanımlamak mümkündür.

³⁸⁰ A.y.

³⁸¹ "İlk Siber Savaş", Milliyet, 18 Mayıs 2007, s.22.

7. SOSYAL BOYUT

Buraya kadar ulusal bilgi güvenliği, kritik bilgilere yetkisiz erişimin engellenmesi ve kritik bilgi ve bilişim sistemlerinin korunmasını içeren “bilginin ve bilişim sistemlerinin korunması boyutu” ile ele alındı. Ulusal bilgi güvenliğinin diğer bir boyutu da haber alma özgürlüğü kapsamında toplumun her türlü bilgiye serbestçe erişebilmesini ve bilginin toplumun geniş kesimlerine yayılmasını sağlamaya yönelik tedbirleri içeren “bilgi edinme hakkı”nın korunması ve buna paralel olarak toplumun zararlı, yanıltıcı ve suça yöneltici bilgiden, yani “zararlı içerikten” korunmasıdır.

Zararlı içerik konusunda alınacak tedbirler devletin, toplumun ve bilginin niteliklerine göre değişiklik göstermekle birlikte her türlü toplum için, bilgi bir toplumsal değer ve yerine göre bir toplumsal tehlike olabileceğinden, toplumun kısaca zararlı içerik olarak tanımlanabilecek olan bilgiden korunması ulusal bilgi güvenliği politikası içerisinde büyük yer teşkil etmektedir.³⁸² Bunun nedeni, İnternet ortamının giderek daha fazla kötü kullanıma alet edilmesi ve gün geçtikçe daha fazla denetime ihtiyaç duyulmasıdır.³⁸³

a. İnternet’in Birey ve Aile Üzerindeki Etkisi

İnternetin bireyler üzerine olan etkileri ve sosyal boyutu tartışmalı bir konu olarak görülmektedir. Konu üzerine çalışma yapan araştırmacıların bir kısmı İnternet’in arkadaşlar, aile bireyleri ve uzak akrabalar ile ilave haberleşme imkânları sunmak suretiyle sosyal ilişkileri geliştirdiğini savunurken, diğerleri İnternet kullanımının, diğer sosyal aktiviteler ve yüz yüze iletişim için ayrılan zamanın yerini aldığı, bu nedenle olumsuz bir etki yarattığı görüşündedirler.³⁸⁴ İnternet’in toplumsal alanda ortaya çıkan olumsuz etkilerini vurgulayan görüşler, bunu desteklemek için birey, aile ve topluma getireceği yıkıcı etkileri dayanak almaktadırlar.³⁸⁵

İnternet’in bireyler üzerine olan etkilerinden bahsedildiğinde çoğunlukla olumsuz bir yaklaşım sergilenmektedir. İnternet’in toplumdan kopuk, izole olmuş bireyler yarattığı ve gerçek dünya ile olan etkileşimlerini kısıtladığından

³⁸² Arkun, a.g.e., s.177.

³⁸³ A.e., s.180.

³⁸⁴ Norman H. Nie, D. Sunshine Hillygus, Lutz Erbring, “Internet Use, Interpersonal Relations, and Sociability”, *The Internet in Everyday Life*, Ed. Barry Wellman, Caroline Haythornthwaite, Blackwell Publishers Ltd., 2002, s.216.

³⁸⁵ Cemal Yalçın, “Sosyolojik Bir Bakış Açısıyla İnternet”, *C.Ü. Sosyal Bilimler Dergisi*, C.XXVII, No.1, Mayıs 2003, s.79.

bahsedilmektedir. Bazı insanların İnternet'te uzun zaman geçirdikleri gerçekten doğru bir tespittir.³⁸⁶ Bilgisayarları başında uzun süreler geçirip sohbet eden, program, müzik, film indiren insanlar, siber uzayda harcadıkları zamanı fiziki çevresindeki insanlara ayıracakları zamandan kısmaktadırlar. Böylece çocukları, eşleri, ebeveynleri veya arkadaşları gibi sosyal hayatlarının büyük bir bölümünü teşkil eden insanlara daha az zaman ayırmakta ve izole bir hayat sürdürmektedirler.³⁸⁷ İnternet kullanımının kişinin kendisine ve ailesine ayırdığı zamanın azalmasına neden olduğu, özellikle de yemek yapma, çocuk bakımı ve alışveriş gibi temel ev işlerine ayrılan zamanı önemli ölçüde azalttığı bilinmektedir.³⁸⁸

İnternet'in toplumsal yapının çekirdeği sayılan aile üzerine en olumsuz etkisi ise aile bağlarının zayıflaması şeklinde ortaya çıkabilmektedir. İnternet başında fazla zaman harcayan ebeveynler hem birbirlerine hem de çocuklarına fazla zaman ayırmamaktadırlar.³⁸⁹ Bu durum eşler arasında var olanlar problemlerin çözümsüz kalmasına veya artmasına, çocukların ise ilgisizlik nedeniyle kötü alışkanlıklar veya suça yönelmelerine neden olabilmektedir.

İnternet'in birey, aile ya da toplum üzerine olan etkileri konusunda tam aksi görüşü destekleyecek bulguların elde edildiği araştırmalar ise İnternet'in günlük rutin hayatın bir parçası haline geldikçe, insanların haberleşme şekillerini değiştirdiği ve sosyal yaşamlarını genişlettiğini ortaya çıkarmıştır. İnsanlar fiziksel olarak dağınık bulundukları bir ağ ile sosyalleşme, bilgiyi arama bulma ve yardım alma imkânına kavuşmuştur. Buna ilaveten, insanlar İnternet sayesinde sadece sosyalleşmemiş; aynı zamanda bilgi, tavsiye ve karar verme sürecinde işbirliği yapabilir hale gelmiştir.³⁹⁰ Kısaca, İnternet'in insanların sosyal hayatında ve toplumsal yapıda gerçekleştirdiği değişimin iyi ya da kötü olduğuna dair kesin bir karara varmak doğru olmadığı gibi mümkün de görünmemektedir. Ailesine ayıracağı zamanın bir kısmını İnternet'te bilimsel ya da akademik çalışmalarına ayırarak değerlendiren bir insanın bu eylemini olumsuzluk olarak değerlendirmek mümkün olmayacaktır. Ancak, İnternet'in olumsuz etkileri bulunmaktadır ve bunu savunanlar sadece İnternet karşıtları değildir. İnternet'i toplumsal açıdan olumlu bir gelişme olarak görenler de

³⁸⁶ Yalçın, a.g.e., s.85.

³⁸⁷ A.y.

³⁸⁸ John P. Robinson v.d., "The Internet and Other Uses of Time", **The Internet in Everyday Life**, Ed. Barry Wellman, Caroline Haythornthwaite, Blackwell Publishers Ltd., 2002, s.253.

³⁸⁹ Yalçın, a.g.e., s.86.

³⁹⁰ Jeffrey Boase, v.d., "The Strength of Internet Ties", **PEW Internet & American Life Project**, Washington, 2006, s.42.

bu olumsuz etkilerin varlığını kabul etmekte ve düzeltilmesi gerektiği görüşünü paylaşmaktadırlar.³⁹¹

İnternet sayesinde insanlar gerçek dünya da maddi, ahlaki veya coğrafi nedenlerle gidemeyecekleri yerlere gidebilmekte ya da giremedikleri mekânlara kolayca girebilmektedir. Hayatında hiç kumarhane görmemiş bir insanın evinin rahat ortamında başında oturduğu bilgisayar masası, bir anda rulet masasına dönüşebilmekte ya da bir bayanın striptiz gösterisine sahne olabilmektedir. Üstelik bunu başka hiç kimse bilmeden ve ahlâki kaygılardan uzak bir şekilde yine gerçek dünyaya göre çok daha düşük maliyetle gerçekleştirebilmektedir. Sanal kumarhaneler, pornografik içerikli siteler ya da cinsel mesajlaşmaların yapıldığı sohbet odalarında dolaşmak, bir evin diğer odalarına girmekten daha kolay bir hal almaktadır. Bu kolaylık, İnternet'in sağladığı anonimlik ile birleşince, insanların eskiden imkânları olmadığı için yapamadıkları eylemleri gerçekleştirmelerine, hatta suç işlemelerine dahi neden olabilmektedir.

İnternetin yarattığı bir diğer değişim ise suç kavramında ya da suçlu psikolojisinde yarattığı değişimdir. Gerçek dünya da suçlu, suç mahallinde olduğundan mağdura verdiği zarara veya acıya bizzat şahit olmaktadır. Bu durum, suç işlemeye meyilli dahi olsa insanların suçu işlemekten önce bir vicdan muhasebesi yapmalarına ve suç işlemekten vazgeçmelerine neden olabilmektedir. Ayrıca, eylemin gerçekleştirileceği esnada ortaya çıkan heyecan ve korku da cesaretin kırılmasına ve eylemden vazgeçilmesine sebep olabilmektedir. Siber uzayda ise durum oldukça farklıdır. Mağdur ve fail ayrı yerlerde olduğundan bu etki gerçekleşmemektedir. Klasik bir suçtaki patlayan tabanca sesi, kapıda duran banka güvenlik görevlisi, yaklaşan polis sireni veya mağdurun yalvaran bakışları olmadığından, suç işlemek ve zarar vermek çok daha kolay bir hal alabilmektedir.³⁹²

b. Toplumsal Etkisi

İnternet'in toplum hayatında sosyal açıdan birçok değişikliğe neden olduğu artık şüphe götürmeyecek bir gerçektir. İnternetin bireyin kendi iç dünyasından başlamak üzere, aile, iş ve sosyal hayatından yarattığı değişiklikler, toplumsal ilişkiler üzerine de yansımıştır. Bu nedenle İnterneti sadece teknolojik bir gelişme olarak tanımlamak yeterli olmamakta, toplumsal hayatta yarattığı değişiklikler sosyolojik bir değerlendirmeyi de gerekli kılmaktadır. İnternetin sosyal hayatta

³⁹¹ Yalçın, a.g.e., s.79.

³⁹² A.e., s.83.

yarattığı değişimin olumlu ve olumsuz yanları bakış açısına göre değişmektedir. İnternetin sosyal açıdan getirdiği değişikliklerden en önemlisi ve bu çalışma ile ilgili boyutu, serbestçe dolaşan bilgi ve düşüncelerin zararlı ve suça yönettici olanlarından toplumun korunması ihtiyacıdır.

Geçmişte bilgi yetersizliğinden bahsedilirken, artık tasnif edilmemiş ve doğruluğu bilinmeyen aşırı bilgi kirliliğinden şikâyet edilmektedir. Günümüz dünyasında terör örgütlerinin dahi İnternet siteleri bulunmaktadır. Bu bilgi yığını içerisinde her türlü bilgi kolayca temin edilebilmektedir. Ancak, iletişim araçlarının çok sayıda ve küresel boyutta mevcut olduğu ortamda pek de popüler olmayan sansür uygulamasına gidilmesi güçtür ve İnternet'e sansür uygulanması neredeyse imkânsızdır. Demokratik ülkelerde medyanın güvenliğe olan zararlı etkilerini en aza indirmek için askeri ve sivil bürokratlar ve medya arasındaki uygulanan işbirliği ise İnternet açısından mümkün görülmemektedir.³⁹³

İnternetin toplumsal açıdan günümüzde yarattığı en büyük tehditler, pornografinin özellikle de çocukları tehdit edecek şekilde yaygınlaşmasına, toplumsal düzeni tehdit eden kin, nefret ve şiddetin teşvik edilmesine ve toplumsal bir tehlike olan kumarın yayılmasına olanak sağlamasıdır. Bunun dışında hırsızlık, dolandırıcılık, kimlik ve kredi bilgilerinin çalınması şeklinde işlenen adı suçların varlığı da tehdit olarak görülebilir. Bu tür suçlar şahsa ve mala karşı işlenen suçlar olduğundan, münferit olarak ele alındığında ulusal açıdan bir güvenlik kaygısı olarak görülmeyecektir. Ancak, ülkelerin sürdürülebilir kalkınması, toplumda huzur ve güvenliğin sağlanmasını gerekli kılmakta,³⁹⁴ bu nedenle toplum ve bireyi doğrudan etkileyen şahsa ve mala karşı suçların toplumda güvenlik endişesi oluşturmayacak düzeye çekilmesi zorunluluğu doğmaktadır.³⁹⁵ Ulusal güvenliğin iç ve dış güvenliği kapsadığı fikrinden hareketle, siber uzayda işlenen bu tür suçların artmasının da toplumsal huzuru ve otoriteye olan güveni sarsması nedeniyle ulusal güvenliğe genel bir tehdit olarak değerlendirilmesi mümkün görülebilir.

(1) Pornografik İçerik ve Çocuk İstismarı

Pornografinin çocuklar üzerinde iki etkisi bulunmaktadır. Bunlardan ilki nispeten daha az zararlı olan çocukların pornografik malzemelere erişiminin yarattığı

³⁹³ Mango, a.g.e., s.116.

³⁹⁴ Ali Yılmaz, Semra Günayergün, "Türkiye'de Şehir Asayiş Suçları: Dağılışı ve Başlıca Özellikleri", s.1., (Çevrimiçi), <http://yayim.meb.gov.tr/dergiler/170/170/ali%20yilmaz.pdf>, 28 Mart 2007.

³⁹⁵ A.e., s.10.

olumsuzluklardır. İkinci ve asıl tehlikeyi yaratan ise çocukların pornografik malzemelerin üretiminde kullanılmasıdır.

İnternet sayesinde çocuk istismarcıları ve pedofiller³⁹⁶ birbirini kolayca bulabilmekte, ev yapımı pornografik malzemeler geniş kitlelere hatta dünyanın bir ucundan diğer ucuna çabucak yayılabilmektedir.³⁹⁷ İnternet sohbet odaları sayesinde çocuk istismarcıları, çocuklarla doğrudan temas kurabilmektedir. İnternetin çocuk pornografisi üzerinde tetikleyici bir etkisi bulunmaktadır. Bu etki, İnternet'in çocuk pornografisi içeren yüksek kalitede resim, ses ve görüntü içeren materyalin daha ucuza dağıtımını ve teminini kolaylaştırması,³⁹⁸ bu kolaylığın çocuk pornografisi içeren malzeme için talebi artırması, talebin gayet kârlı bir pazar oluşturması ve bu pazarın malzeme üretimi için daha fazla çocuğun cinsel istismarına yol açması şeklinde ifade edilebilir.

Ayrıca, çocuk pornografisinin yaygın hale gelmesi hem çocuklarda bunun "olağan" ve normal bir şey olduğu duygusunun yerleşmesine yol açarak ruh sağlıklarını kalıcı bir biçimde bozmakta, hem de pedofillerin hızlı bir şekilde çoğalmasına neden olmaktadır.³⁹⁹ Bu durum çocukların İnternet üzerinden pornografik malzemelere erişimlerinin engellenmesini ve çocuk pornografisinin üretim, dağıtım, temin ve bulundurulması ile mücadele edilmesini toplumsal açıdan bir gereklilik haline getirmektedir.

(2) İnternet ve Kumar Siteleri

İnternet'te toplumu tehdit eden bir başka uygulama da kumar ve bahis oyunlarının oynanmasına imkân sağlayan İnternet siteleri ve İnternet'in bu amaçla kullanımıdır. İnternet üzerinden kumar tipik olarak İnternet'e bağlı bir bilgisayarın bir spor müsabakası veya oyunun ya da rasgele sonuçlar üreten bir bilgisayar yazılımının sonuçlarına bahis yatırmak amacıyla kullanılması ya da İnternet'e bağlı diğer oyuncularla gerçek zamanlı olarak kart ve gazino tipi oyunların oynanması şeklinde gerçekleşmektedir. Bunun yanında, para transferi İnternet üzerinden gerçekleştirilmese dahi İnternet'e bağlı bir bilgisayar kullanımı ile insanların bir spor

³⁹⁶ "Pedofil" kelimesi "Pedofili ile ilgili veya çocuklarla cinsel temastan hoşlanan kişi" anlamındadır. Pedofili ise "cinsel heyecana yönelik fantazilerde veya etkinliklerde özellikle veya sadece ergen olmayan çocukların tercih edilmesiyle tanımlanan bir cinsel sapma" olarak tanımlanmaktadır. Bkz.: <http://www.termbank.net/psychology/5575.html>.

³⁹⁷ Fûsun Sokullu-Akıncı, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", *İÜHFİM*, C.LIX, No.1-2, 2001, s.37.

³⁹⁸ Wortley, Smallbone, a.g.e., s.8.

³⁹⁹ Sokullu-Akıncı, a.y.

müşabakası ya da benzeri bir olaylar için bahse girmeleri ve kumar oynamaları da mümkün olabilmektedir.⁴⁰⁰

İnternet'in kumar ve bahis amacıyla kullanılması ülkeler için yeni bir durum teşkil etmiş ve bazı ülkeler buna yönelik yasal düzenlemelerini yapmıştır. Bu kapsamda, ABD 2006 yılında İnternet üzerinden kumar oynatılmasını yasaklayan yasayı (Unlawful Internet Gambling Enforcement Act 2006)⁴⁰¹ kabul etmiştir. Bu kanun ayrıca bankacılık sektöründeki kuruluşların sistemleri aracılığıyla kumarla ilişkili para transferlerini tespit etmelerini ve engellemelerini de öngörmektedir. İngiltere ise İnternet'te kumar oynatılmasını belirli lisans şartlarına bağlamak suretiyle kanunla düzenlemiş (Gambling Act 2005)⁴⁰² ve kontrol altına almıştır.

Türkiye'de İnternet üzerinden kumar ve bahis oyunlarına yönelik olarak hazırlanan bir raporda İnternet üzerinden kumar ve bahis oynayanların sayısının 1,5 milyonu bulunduğu belirtilmektedir. Milli Piyango İdaresi'ne göre Türkiye'de İnternet üzerinden kumar oynanan gazinoların yıllık cirosu 1 milyar doları, İngilizlerin Türkiye'de yaptığı bir araştırmaya göre ise bu rakam 5 milyar doları bulmaktadır. Üstelik bu paradan vergi de ödenmemekte ve havale, kredi kartı gibi yollarla ciddi miktardaki paralar yurtdışına transfer edilmektedir. Bu durum Türkiye'deki kumar pazarının ulaştığı boyutu gözler önüne sermektedir.⁴⁰³

Türkiye'de kumar oynanması için yer ve imkân sağlanması TCK 228. maddesi⁴⁰⁴ ile yasaklanmıştır. Kumarın yasaklanmasının gerekçesi ise “kumarın sosyal bakımdan ortaya koyduğu büyük tehlike ve doğurması olası facialar göz önüne alınması” şeklinde ifade edilmiştir.⁴⁰⁵ Bir diğer önemli husus da yine madde gerekçesinde yer alan “söz konusu suçun oluşabilmesi için, aleniyet şartı aranmamıştır.” ifadesi ile gizlice kumar oynanması ve oynatılmasının da cezai suç olarak düzenlenmiş olmasıdır.

⁴⁰⁰ Howard J. Shaffer, “Internet Gambling & Addiction”, s.5, January 16, 2004, (Çevrimiçi), <http://www.divisiononaddictions.org/html/publications/shafferinternetgambling.pdf>, 29 Mart 2007.

⁴⁰¹ Ayrıntılı Bilgi İçin Bkz.: Unlawful Internet Gambling Enforcement Act in October 2006, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr412p1.109.pdf.

⁴⁰² Ayrıntılı Bilgi İçin Bkz.: Gambling Act 2005, <http://www.opsi.gov.uk/acts/acts2005/20050019.htm>.

⁴⁰³ “ATO İnternet Kumarhaneleri Raporu”, ATO , (Çevrimiçi), <http://www.atonet.org.tr/turkce/bulten/bulten.php3?sira=281>, 29 Mart 2007.

⁴⁰⁴ TCK madde 228 “ (1) Kumar oynanması için yer ve imkân sağlayan kişi, bir yıla kadar hapis ve adli para cezası ile cezalandırılır.”

⁴⁰⁵ “Türk Ceza Kanunu Madde Gerekçeleri”, s.258., Adalet Bakanlığı, (Çevrimiçi), <http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc>, 10 Aralık 2006.

Ülkemizde kumar oynatılması toplumsal çıkar göz önüne alınarak yasaklanmış olduğundan, yurt içi ve yurt dışından İnternet üzerinden yayın yapan kumar sitelerine erişimin engellenmesi de büyük önem taşımaktadır. Bu kapsamda, 4 Mayıs 2007 tarihinde kabul edilen ve 23 Mayıs 2007 tarihinde Resmi Gazetede yayınlanarak yürürlüğe giren 5651 sayılı Kanun'un 8. maddesinde, İnternet ortamında yapılan ve içeriği TCK'nın 228. maddesinde belirtilen kumar oynanması için yer ve imkân sağlanması suçunu oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak, erişimin engellenmesine karar verilebilmektedir.⁴⁰⁶ Suç teşkil eden yayının yurt dışından yapılması durumunda erişimin engellenmesi kararı Telekomünikasyon İletişim Başkanlığı tarafından verilirken, yurt içi yayınlar için hâkim, mahkeme veya Cumhuriyet savcısı karar verebilmektedir. Bu durumda verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilmektedir. Ayrıca, Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulması da düzenlenmiştir. Bu nedenle, TCK'nın 228. maddesinde suçun İnternet ortamında gerçekleşmesi durumu ayrıca belirtilmemiş olsa da kumar oynanmasını sağlayacak bir İnternet hizmetinin Türkiye sınırları dahilindeki bir hizmet sağlayıcı veya içerik sağlayıcı tarafından verilmesi, maddede geçen "imkân sağlama" eylemini oluşturmakta ve suç teşkil etmektedir.

⁴⁰⁶ 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Madde 8: (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

- 1) İntihara yönlendirme (madde 84),
 - 2) Çocukların cinsel istismarı (madde 103, birinci fıkra),
 - 3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
 - 4) Sağlık için tehlikeli madde temini (madde 194),
 - 5) Müstehcenlik (madde 226),
 - 6) Fuhuş (madde 227),
 - 7) Kumar oynanması için yer ve imkân sağlama (madde 228),
- suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir." Ayrıntılı Bilgi İçin Bkz.: <http://mevzuat.basbakanlik.gov.tr/mevzuat/metinx.asp?mevzuatkod=1.5.5651>.

(3) Kin, Nefret ve Şiddetin Desteklenmesi ve Yayılması

İnternetin yarattığı bir diğer tehdit ise toplumsal düzen ve barışı bozmaya yönelik eylemler için kullanılabilmesidir. Gelişen haberleşme alt yapısı, küreselleşme ve özellikle İnternet sayesinde hem ülke sınırları içerisinde hem de dünya genelinde farklı ırk, din ve etnik guruplar birbirlerine daha yaklaşmış ve yakın bir etkileşim içerisine girmiştir. Benzer şekilde dünyanın farklı yerlerinde aynı ya da benzer görüşlere sahip insanlar ve gurupların bir araya gelerek düşünce ve fikirlerini paylaşması ve birlikte hareket edebilmeleri mümkün olmuştur. Bu etkileşim ırk, din, etnik köken, cinsiyet vb. özelliklere dayalı ayrımcılığa yeni bir imkân sağlamıştır.

Fiziksel olarak temas sağlayamayan aşırı uçlar hedef olarak seçtikleri kişi ve guruplarla siber uzayda temas kurabilme imkânına kavuşmuştur. İnternet bu amaçla hazırlanan elektronik ortamdaki yazılı, görsel ve işitsel malzemelerin paylaşılmasına, aşırı görüşlü kişi ve gurupların siber uzayda bir araya gelmelerine imkân sağlamış ve yeni bir tehlike yaratmıştır. İnternet sayfaların aracılığıyla kin ve nefret içeren makale ve yazılara ulaşılabilmekte veya elektronik ortamdaki birçok malzeme bu sayfalardan temin edilebilmektedir. E-postalar aracılığıyla kişi ya da guruplara can ve mal varlıklarına yönelik tehdit içeren mesajlar gönderilebilmektedir. Haber gurupları, panoları veya forum sayfaları aracılığıyla bu tür düşünce ve fikirlerin yayılması, yeni üyelerin kazanılması mümkün olmaktadır.⁴⁰⁷ Hatta İnternet üzerinden ırkçı ayrımcılık içeren bilgisayar oyunları dahi temin edilebilmektedir. Bunlar doğrudan İnternet üzerinde erişilebilir olmamakla birlikte, İnternet aracılığıyla temin edilebilmesi açısından önemlidir. Bu oyunların büyük çoğunluğu Yahudi düşmanlığı içerse de, Türk düşmanlığı veya göçmen düşmanlığı içeren oyunlarda bulunmaktadır.⁴⁰⁸

İnternet günümüzde;

- Kişi ya da topluluklara karşı ırk, etnik köken, din, renk ve cinsiyet ayrımcılığına yönelik olarak toplumda kin, nefret ve şiddet duygularının yayılması, teşvik ve tahrik edilmesi,
- Kişi ve topluluklara karşı hakaret, aşağılama ve tehdit eylemleri,
- Yabancı ve göçmen düşmanlığı,

⁴⁰⁷ Michael Whine, "The Far Right on the Internet", **The Governance of Cyberspace**, Ed. Brian D. Loader, New York, Routledge, 1997, s.213-219.

⁴⁰⁸ A.e., s.219.

- Suçu ve suçluyu övme, insanlığa karşı işlenen suçların ve genel kabul görmüş soykırımların inkârı amacıyla kullanılabilir. ⁴⁰⁹

8. SİYASİ BOYUT

Bilişim teknolojileri ve İnternet vatandaşlar ile hükümet arasında iki yönlü bir iletişim kanalı yaratmıştır. Hükümetler sadece vatandaşlara değil yerel yönetimlere erişmek için de yeni bir imkânı kavuşmuştur. Vatandaşların ülke yönetimine daha fazla etkide bulunmaları sayesinde temsili demokrasiden katılımcı demokrasiye bir geçiş yaşanmaktadır. ⁴¹⁰ Katılımcı demokrasi, vatandaşların ülke yönetimi ve diğer siyasi konularla ilgili karar alma sürecine gözlemci olması, katkıda bulunması ve bazen de müdahale etmesini gerektirmekte, ⁴¹¹ İnternetin getirdiği olanaklar, devleti tüm aktivitelerinde şeffaf, katılımcı ve hesap verebilir olmaya zorlamaktadır. ⁴¹² E-devlet sayesinde vatandaş, hükümetin tüm icraatlarından haberdar olmakta, temsilcilerine görüşlerini, önerilerini, dilek ve şikâyetlerini bildirebilmekte, bilgi talep edebilmekte, sonuçta yönetim sürecine dahil olmakta ve e-devletin nihai hedefi e-demokrasi olarak ortaya çıkmaktadır. ⁴¹³

Bilgi kaynaklarının çokluğu ve bunlara ulaşım imkânı sağlayan bilişim sistemlerinin çeşitliliği, toplum üzerinde devletin denetimini de imkânsızlaştırmaktadır. Kişiler İnternet sayesinde daha fazla özgürlüğe sahip olmakta ve kimlikler ön plana çıkmaktadır. Yine başta İnternet ve diğer iletişim vasıtaları sayesinde, hem benzer kimliklerle hem de ötekilerle etkileşim artmaktadır. Bu nedenle toplumlar üzerinde homojenleştirici etki sağlayan totaliter rejimleri uygulamak zorlaşmaktadır. İnsanların hem kendi toplumlarında hem de diğer

⁴⁰⁹ Ayrıntılı Bilgi İçin Bkz.: Siber Suçlar Sözleşmesi'ne Ek Protokol, "Additional Protocol to the Convention on Cybercrime, Concerning The Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems ETS No.: 189", <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.

⁴¹⁰ Ali Şahin, Handan Temizel, Metehan Temizel, "Türkiye'de Demokrasiden E-Demokrasiye Geçiş Süreci ve Karşılaşılan Sorunlar", s.255, 3. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi (Osman Gazi Üni. İktisadi ve İdari Bilimler Fakültesi, Eskişehir, 25-26 Kasım 2004), (Çevrimiçi), <http://iibf.ogu.edu.tr/kongre/bildiriler/06-02.pdf>, 24 Mart 2007.

⁴¹¹ A.y.

⁴¹² A.e., s.256.

⁴¹³ Özgür Uçkan, "E-Devlet, E-Demokrasi ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü", **Stradigma**, (Çevrimiçi), http://www.stradigma.com/turkce/haziran2003/print_09.html, 30 Mart 2007.

toplumlarda yaşananları izleyebildiği bir dünya da, herkesin diğerlerini takip edebildiği ve denetlendiği şeffaf bir düzen oluşmaktadır.⁴¹⁴

İnternet'in siyasete etkisi sadece doğrudan e-devlet uygulamaları sayesinde değil; İnternet üzerinden başlayan ve toplumsal harekete dönüşen olaylar sayesinde dolaylı yollarla da gerçekleşmektedir. Hızlandırılmış çoğulculuk etkisi ile "İnternet'te yapılan her türlü aktivite anında bir eylem olarak görülebilmekte ve etkileri hemen hissedilebilmektedir."⁴¹⁵ Bu sayede "İnternet'te örgütlenen protestolar çok kısa sürelerde eylemcilere ulaşmakta ve İnternet siyasi örgütlenmelerde büyük bir önem ve yer teşkil etmektedir."⁴¹⁶

İnternet ortamında bir araya gelen bu topluluklar, hak ve özgürlükler, yolsuzluklar ve hizmetler gibi birçok konuda ses getirecek aktivitelerde bulunabilmekte ve bu aktiviteler sivil toplum kuruluşlarının ortaya çıkması ile sonuçlanabilmektedir. İnternetin kontrol edilemeyen ve merkezi olmayan yapısı sayesinde sivil toplum örgütlenmeleri etki ve faaliyetlerini ulusal ve uluslararası ölçeklere genişletme imkânına kavuşmaktadır.⁴¹⁷ Böylece vatandaşlar, İnternet yoluyla sadece bilgiye ulaşmakla kalmayıp, tepkilerini veya desteklerini toplumsal bir harekete de dönüştürebilmekte, neticede ülke yönetimine ve siyasete etki edebilmektedir.⁴¹⁸

İnternet'in siyaset üzerine olan etkisi, demokrasinin gereği farklı düşünce ve fikirlerin iyi niyetli ve yapıcı şekilde dile getirilmesi şeklinde olumlu olarak algılanabilir. Ancak, İnternet yıkıcı, bölücü ve ulus devletlerin çözülmesini neden olabilecek mikro milliyetçi düşüncelerin yayılmasına da imkân sağlamakta ve bazen hükümetlere karşı siyasi bir baskı aracı olarak kullanılabilir. Bu haliyle İnternet'in siyasi yapı üzerindeki değiştirici etkisi, ulusal bir tehdit niteliği sergileyebilmektedir. Eskiden zihin içerisinde bir dinamik olan düşünce süreci, İnternet altyapısı sayesinde zihni sınırları daha kolay aşmaya ve pasif bir eylemden aktif bir eyleme daha kolay dönüşmeye başlamıştır. İyi ya da kötü tüm düşünceler artık daha kolay yayılmakta, paylaşılmakta ve eyleme dönüşebilmektedir. Bu

⁴¹⁴ İhsan D. Dağı, "İnternet Türkiye'de ve Dünyada Demokrasiye Neler Kattı?", s.2., (Çevrimiçi), <http://www.policy.hu/dagi/leftmenu/files/edevlet.pdf>, 24 Mart 2007.

⁴¹⁵ Bruce Bimber, "İnternet ve Siyasi Dönüşüm: Hızlandırılmış Çoğulculuk", *Cogito*, Sayı:30, ss: 168-169. akt.: Yalçın, a.g.e., s.83.

⁴¹⁶ Sagi Leizerov, "Privacy Advocacy Groups Versus Intel: A Case Study of How Social Movements Are Tactically Using the Internet to Fight Corporations" *Social Science Computer Review*, C. 18 No. 4, s.466., akt.: Yalçın, a.y.

⁴¹⁷ Uçkan, a.y.

⁴¹⁸ Dağı, a.y.

düşüncelerin zararlı olanları ise İnternet üzerinden ülke rejimlerini ve ulus devlet yapılarını tehdit edebilmektedir. Bu nedenle, İnternet'in sağladığı daha önce hayal bile edilemeyen özgürlüğün, devletlerce tehdit edildiğini düşünenler, İnternet'in getirdiği özgürlüğün bir noktadan sonra devlet tarafından, kendi varlığına bir tehdit olarak algılandığını görememektedir.

İnternet aşırı uç grup ve organizasyonlar tarafından fikir ve görüşlerin yayınlandığı bir forum olarak kullanılabilmekte ve hatta toplumun kasıtlı olarak yanlış bilgilendirilmesi amacıyla da yararlanılmaktadır. Bunun ötesinde, İnternet basılı olarak yayınlanması yasak olan mesaj ve fikirlerin yayınlanmasına da imkân tanımaktadır. İnternet yasadışı grup ve organizasyonlar arasında hem elektronik hem de lojistik bir bağ sağlamaktadır. Coğrafi olarak birbirinden ayrı ve az sayıda üyesi olan gruplar, tek bir grup haline gelebilmektedir. Bu durum sadece bilgi ve kaynakların paylaşılmasına değil; amaçlarının ve topluluğun daha büyükmüş gibi hissedilmesine yol açmaktadır. Böylece tek bir birey dahi büyük bir grupmuş gibi algılanabilmektedir. Hatta bu gruplar kendilerini daha önemli göstererek, daha fazla destek sağlayabilmek için İnternet sayfalarında bulunan ziyaretçi sayacılarını dahi yükseltmektedirler.⁴¹⁹

Dolayısıyla, İnternet bir yandan vatandaşlar tarafından siyasi sürece katılım için faydalı bir araç olarak kullanılırken; diğer yandan kötü niyetlerle hükümetlere karşı siyasi bir baskı aracı olarak da kullanılabilir.

9. HUKUKİ ANLAMDA ULUSAL GÜVENLİK VE TEMEL HAK VE ÖZGÜRLÜKLER

Bilişim sistemlerinde yaşanan devrim ve bilgi çağının getirdiği enformasyon zenginliği doğrultusunda siyasal sistemde ve devlet yönetiminde gerçekleşen değişim daha önce de belirtildiği gibi kamu yönetimlerini, sahip oldukları bilgileri bireylerle paylaşmaya yöneltmiş ve vatandaşların devlet yönetimine aktif olarak katılmalarını sağlamıştır. Bu durum katılımcı demokrasinin şartı olan “düşünce ve ifade özgürlüğü” ve bunun bir gereği olan “bilgi edinme hakkı”na daha fazla önem verilmesine neden olmuştur. Bununla birlikte bu hakların devletin güvenliğini ve bütünlüğünü koruyacak şekilde sınırlandırılması, doğası gereği diğer kitle iletişim araçları gibi sınırlandırılmayan İnternet açısından yeni bir gereklilik olarak ortaya çıkmıştır.

⁴¹⁹ Phyllis B. Gerstenfeld, Diana R. Grant, Chau-Pu Chiang, “Hate Online: A Content Analysis of Extremist Internet Sites”, **Analyses of Social Issues and Public Policy**, C.III, No.1, 2003, s.40.

En üst norm olan Türkiye Cumhuriyeti Anayasası, bir taraftan Türkiye Cumhuriyeti devletinin temel niteliklerini belirlerken, diğer taraftan vatandaşların temel hak ve özgürlükleri ile devlete karşı olan yükümlülüklerini düzenlemiştir. Ancak, Anayasa bireylere sağlanan ve yine Anayasa kapsamında koruma altına alınan temel hak ve özgürlüklerin belirli durumlarda sınırlandırılmasına da imkân tanımıştır. Kişi hak ve özgürlüklerinin sınırı ve yine güvence altına alındığı, Anayasa'nın 14. maddesinde aşağıdaki şekilde belirtilmiştir;

“Anayasada yer alan hak ve hürriyetlerden hiçbirisi, devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmayı ve insan haklarına dayanan demokratik ve laik Cumhuriyeti ortadan kaldırmayı amaçlayan faaliyetler biçiminde kullanılamaz.

Anayasa'nın hükümlerinden hiçbirisi, Devlete veya kişilere, Anayasayla tanınan temel hak ve hürriyetlerin yok edilmesini veya Anayasada belirtilenden daha geniş şekilde sınırlandırılmasını amaçlayan bir faaliyette bulunmayı mümkün kılacak şekilde yorumlanamaz.”

Anayasa'nın ikinci kısım, ikinci bölümünde “kişinin hakları ve ödevleri” başlığı altında düzenlenen hakların bir kısmına⁴²⁰ “milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden bir veya bir kaçını nedeniyle” sınırlama getirilebileceği açıkça düzenlenmiştir. Buna ilaveten 28. maddede belirtilen basın özgürlüğüne, süreli ve süresiz yayınlara devletin iç ve dış güvenliği, ülkesi ve milleti ile bölünmez bütünlüğünü, suç işlemeye ya da ayaklanmaya veya isyana teşvik veya devlete ait gizli bilgilerin korunması kapsamında sınırlama getirildiği görülmektedir.

Yine Anayasa'nın 13. Maddesinde temel hak ve hürriyetlerin ancak Anayasa'da belirtilen sebeplerle ve kanunla sınırlandırabileceği belirtilmiştir. Bu hükümle bağlantılı olarak TCK, CMK ve diğer çeşitli kanunlarla bu sınırlamalar düzenlenmiştir. Bu kapsamda TCK'nın 215. ve 216. maddelerinde düzenlenen “suçu ve suçluyu övme” ve “halkı kin ve düşmanlığa tahrik ve aşağılama” suçları, düşüncüyü açıklama ve yayma hürriyetine getirilen sınırlamalara bir örnek teşkil

⁴²⁰ Bu bölümde düzenlenen ve “milli güvenlik” kapsamında sınırlama getirilen haklar “ Madde-20: Özel Hayatın Gizliliği, Madde-21: Konut Dokunulmazlığı, Madde-22: Haberleşme Hürriyeti, Madde-26: Düşüncüyü Açıklama ve Yayma Hürriyeti, Madde-33: Dernek kurma hürriyeti, Madde-34: Toplantı ve Gösteri Yürüyüşü Düzenleme Hakkı'dır.

ederken, 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu⁴²¹ ile getirilen düzenleme ile toplantı ve gösteri yürüyüşü düzenleme hakkının sınırları çizilmiştir.

Benzer biçimde CMK'nın 182. maddesi⁴²² ile bilgi edinme özgürlüğünün kısıtlandığı ifade edilebilir. Anayasal bir hak olan dernek kurma hakkına ise 5253 sayılı Dernekler Kanunu ile çeşitli sınırlamalar getirilmiştir.⁴²³ Anayasa'da düzenlenen hak ve özgürlüklerin "milli güvenlik" gerekçesiyle sınırlanabileceği açık olmakla birlikte; "milli güvenlik" kavramının nasıl yorumlanacağı ve ne anlama geldiği ne Anayasa'da, ne de bu kanunlarda tanımlanmamıştır. Bu nedenle hukuksal anlamda "milli güvenlik" kavramının neyi ifade ettiğinin ortaya konulması bu sınırlamanın kesin çizgisinin belirlenmesini de sağlayacaktır. Milli güvenlik kavramı 2945 sayılı Milli Güvenlik Kurulu ve Milli Güvenlik Genel Sekreterliği Kanunu'nda aşağıdaki şekilde tanımlanmaktadır;

"Devletin anayasal düzeninin, milli varlığının, bütünlüğünün, milletlerarası alanda siyasi, sosyal, kültürel ve ekonomik dahil bütün menfaatlerinin ve ahdi hukukunun her türlü dış ve iç tehditlere karşı korunması ve kollanmasını ifade etmektedir."

Ancak, bu ifade o kadar geniş çizilmiştir ki içine girmeyecek siyasal, sosyal, kültürel, ekonomik husus bulunmamaktadır. Bu şekilde her konunun milli güvenlikle doğrudan veya dolaylı olarak ilgisi kurulabilmektedir.⁴²⁴ Dolayısıyla, İnternet alanında milli güvenlik kavramının daha belirgin bir çerçeve ile tespit edilmesi faydalı olacaktır. İnternet'in doğası gereği temel hak ve özgürlüklerden "düşünceyi açıklama ve yayma hürriyeti", "bilgi edinme hakkı" ve "özel hayatın gizliliği" haklarının ön plana çıktığı ve daha çok bu hakların milli güvenlik karşısında dengelenmesinin önem kazandığı açıktır. Anayasa'nın 90/5. maddesine göre usulüne uygun olarak

⁴²¹ Toplantı ve Gösteri Yürüyüşleri Kanunu Madde 17 "(Değişik: 4748 - 26.3.2002 / m.6 b) Bölge valisi, vali veya kaymakam, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlığın ve genel ahlakın veya başkalarının hak ve özgürlüklerinin korunması amacıyla belirli bir toplantıyı (Değişik ibare: 4963 - 30.7.2003 /m.20) "bir ayı aşmamak üzere erteleyebilir veya suç işleneceğine dair açık ve yakın tehlike mevcut olması halinde yasaklayabilir." ifadesi ile sınırlandırılmıştır.

⁴²² CMK Madde 182 "Genel ahlakın veya kamu güvenliğinin kesin olarak gerekli kıldığı hallerde, duruşmanın bir kısmının veya tamamının kapalı yapılmasına mahkemece karar verilebilir"

⁴²³ Dernekler Kanunu Madde 30 "Dernekler; a) Tüzüklerinde gösterilen amaç ve bu amacı gerçekleştirmek üzere sürdüreceği belirtilen çalışma konuları dışında faaliyette bulunamazlar.

b) Anayasa ve kanunlarla açıkça yasaklanan amaçları veya konusu suç teşkil eden fiilleri gerçekleştirmek amacıyla kurulamaz.

c) Askerliğe, millî savunma ve genel kolluk hizmetlerine hazırlayıcı öğretim ve eğitim faaliyetlerinde bulunamaz, bu amaçları gerçekleştirmek üzere kamp veya eğitim yerleri açamazlar. Üyeleri için özel kıyafet veya üniforma kullanamazlar."

⁴²⁴ Bülent Tanör, *Türkiye'de Demokrasi Standartlarının Yükseltilmesi*, İstanbul, 1999, Lebib Yalkın Yayınları, s.105-106. akt.: Metin, a.g.e., s.157.

yürürlüğe konan uluslararası anlaşmalar kanun hükmündedir ve bunlar hakkında Anayasa'ya aykırılık iddiasında bulunulamaz. Anayasa'nın 90. maddesine eklenen yeni hükme göre temel hak ve özgürlüklere ilişkin uluslararası anlaşma hükümlerinin aynı konuda kanunlarla farklı hükümler içermesi halinde anlaşma hükümleri geçerli olmaktadır.⁴²⁵ Buradan temel hak ve özgürlükleri düzenleyen uluslararası anlaşmaların hem Anayasaya aykırılık davası açılmayacağı, hem de kanunlardan üstün olduğu, dolayısıyla hukukumuz açısından en üst normu oluşturduğu sonucu çıkmaktadır. Avrupa Konseyi Siber Suçlar Sözleşmesinin giriş bölümünde, Sözleşme kapsamında suç olarak değerlendirilen eylemlere yönelik ceza sorumluluklarının düzenlenmesinde;

"Her bir bireyin herhangi bir müdahale olmaksızın düşünme, düşündüklerini ifade etme, her türlü bilgiyi ve düşünceyi sınırsız şekilde aramak, almak ve iletme hakkını ve özel hayata saygıya ilişkin hakları teyit eden 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Sözleşmesinin (AİHS) gereklerine uyulacağı ve yasaların yürürlüğe sokulması hususu ile temel insan haklarına saygı konusunda sağlıklı bir denge belirlenmesine ihtiyaç duyulduğu"

ifade edilmiş ve temel hak ve özgürlüklerin birinci derecede göz önünde bulundurulacağı vurgulanmıştır.⁴²⁶ Bunun sonucunda, İnternet alanında temel hak ve özgürlüklere getirilen sınırlamaların AİHS'de öngörülen sınırlamalarla paralel olması gözetilecektir.⁴²⁷ Dolayısıyla İnternet ortamında, "milli güvenlik" ve "temel hak ve özgürlükler" dengesini Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Avrupa İnsan Hakları Mahkemesi (AİHM) kararları kapsamında değerlendirmek uygun olacaktır.

AİHS'nin sağladığı temel hak ve özgürlüklerden, 8. maddede yer alan özel hayatın ve aile hayatının korunması, 10. maddesinde yer alan ifade özgürlüğü ve 11. maddede yer alan dernek kurma ve toplantı özgürlüğünün "milli güvenlik" gerekçesi ile sınırlanabileceği açıkça belirtilmiştir. AİHS'nin bu hükümleri Anayasa'nın ilgili maddeleri ile de örtüşmektedir.

Genel kabul gören bir düşünceye göre ifade özgürlüğü demokrasinin olmazsa olmaz şartıdır ve bu özgürlük sözlü ve yazılı anlatım, kişisel görünüm ve görüntü tercihi ile ifade bulabileceği gibi dernek kurmak, örgütlenmek, toplantı ve gösteri

⁴²⁵ Temel Hukuk Bilgisi, s.36.

⁴²⁶ Ali Karagülmez, **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, Ankara, Seçkin, 2005, s. 304, Kayıhan İçel, "Avrupa Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İÜHFM**, C.LIX, No.1-2, 2001, s.7.,

⁴²⁷ İçel, a.y.

yürüyüşü yapmak şeklinde de ortaya konulabilir.⁴²⁸ Düşüncenin açıklanabilmesi için öncelikle bir düşüncenin oluşması ve bunun için de bilgi edinme hakkının kullanılabilmesi gerekmektedir.⁴²⁹ Düşünce ve ifade özgürlüğünün diğer haklarla olan bu yakın ilgisi ve doktrinde bu hürriyetin diğer bütün kişi hak ve hürriyetlerinin “kökü, tohumu, çekirdeği”⁴³⁰ olarak görülmesi nedeniyle, bu hürriyete konulacak bir sınırlama, diğer birçok hürriyetin de sınırlanması anlamına gelmektedir.⁴³¹ Bu nedenle ağırlıklı olarak AİHS’nin 10. maddesinde yer alan ifade hürriyetinin ulusal güvenlik karşısındaki konumunun değerlendirilmesi diğer hak ve özgürlüklerin durumuna da ışık tutacaktır. AİHS’nin 10/2. maddesinde ifade hürriyetinin sınırları şu şekilde çizilmiştir;

“demokratik bir toplumda, zorunlu tedbirler niteliğinde olarak, ulusal güvenliğin, toprak bütünlüğünün veya kamu emniyetinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması veya yargı gücünün otorite ve tarafsızlığının sağlanması için yasayla öngörülen bazı biçim koşullarına, sınırlamalara ve yaptırımlara bağlanabilir.”

Vereniging Weekblad Bluf! davasında⁴³² AİHM, “ulusal güvenlik” ile ifade özgürlüğü arasındaki çatışmayı incelemiştir. Dava, Amsterdam’da bulunan bir derneğin sol görüşlü okuyucuya hitap eden Bluf! adlı haftalık dergisi tarafından, Hollanda’ya karşı açılmıştır. Olay 1987 yılında Hollanda iç istihbarat servisinin 1981 tarihli gizli bir raporunun Bluf!’un eline geçmesi ile başlamıştır. Raporda Hollanda gizli servisinin o dönemde ilgilendiği bazı konular hakkında bilgiler bulunmaktadır.

Derginin editörünün, söz konusu raporu derginin bir sayısıyla birlikte verileceğini duyurması ile aynı gün, Hollanda gizli servisinin başkanı bir mektupla savcılığa suç duyurusunda bulunmuştur. Rapordaki bilgilerin, tek tek ele alındığında devlet sırrı özelliği taşıyamalarına karşın, güvenlik servisinin değişik ilgi alanlarında sahip olduğu bilgiler, faaliyetler ve operasyon yöntemleri hakkında genel bir tablo elde etmeyi mümkün hale getirdiğini belirtmiştir. Bunun üzerine derginin ilgili sayısına, ilave de dahil olmak üzere, hakim kararı ile el konulmuştur. Ancak, aynı

⁴²⁸ M. Erdoğan, “Demokratik Toplumda İfade Özgürlüğü: Özgürlükçü Bir Perspektif, *Liberal Düşünce (Dergisi)*, Yıl:6, Sayı:24, Güz 2001, s.8., akt.: Burhan Kuzu, “Düşünceleri Açıklama Özgürlüğü Alanında Geldiğimiz Nokta”, *İÜHFİM*, C.LIX, No.1-2, 2001, s.247.

⁴²⁹ İ. Ö. Kabaoğlu, *Özgürlükler Hukuku, İnsan Haklarının Hukusal Yapısı Üzerine Bir Deneme*, İstanbul, 1994, s. 190. akt.: Kuzu, a.g.e., s.251.

⁴³⁰ R. Sarıca, “Hürriyetler Adına Hürriyetlere Karşı”, *Cumhuriyet*, 15.3.1967, akt.: Kuzu, a.g.e., s.252.

⁴³¹ Kuzu, a.y.

⁴³² Vereniging Weekblad Bluf!, Hollanda’ya karşı, Başvuru no: 44/1993/439/518, 09 Ocak 1995.

günün gecesinde Bluf!'un çalışanları sayıyı gizlice yeniden basmış ve 2500 dolayında nüshayı ertesi gün Amsterdam sokaklarında satmıştır.

Sorgu hâkimi Bluf! çalışanları hakkındaki soruşturmayı herhangi bir suçlama getirmeksizin kapatmıştır. Bu arada, dernek el konulmuş nüshaların iadesini talep etmiş, ancak başvuru reddedilmiştir. Savcının talebi üzerine, Hollanda mahkemeleri Bluf!'un ilgili sayısının bütün nüshalarının dolaşımdan çekilmesine karar vermiştir. Kararın gerekçesi “ulusal güvenliğin” korunması ve ceza kanununun ulusal güvenlikle ilgili belgelerin yasa dışı olarak elde bulundurulması ve yayınlanmasını yasaklayan ilgili maddelerine dayandırılmıştır.

Bunun üzerine Dernek Hollanda otoritelerinin AİHS'nin 10. Maddesi'nden doğan hakkı ihlâl etmiş olduklarını ileri sürerek AİHM'e başvurmuştur. Hükümet savunmasında, davacının ifade özgürlüğüne yapılan müdahalenin “ulusal güvenliği” koruma ihtiyacı zemininde meşru olduğunu öne sürmüştür.

Mahkeme sonuç olarak müdahalenin Hollanda kanunları ile öngörüldüğüne ve kanunda belirtilen ulusal güvenliğin korunması amacının varlığına karar vermiştir. Ancak müdahalenin “ulusal güvenliği” korumak için “demokratik bir toplumda gerekli” olmadığına ve 10. Madde'nin ihlaline karar vermiş ve bu kararını aşağıdaki gerekçelere dayandırmıştır;

Söz konusu belge altı yıl öncesine aittir ve güvenlik servisinin başkanı, 1987 yılına gelindiğinde ayrı ayrı ele alındığında artık birer devlet sırrı olmadığını beyan etmiştir. Raporun üzerinde düşük bir gizlilik derecesi olan “gizlidir” ifadesi yer almaktadır. Dolayısıyla rapordaki bilgilerin, derginin dağıtımını engellemeyi haklı gösterecek kadar hassas olup olmadığı tartışmalıdır.

Derginin ilgili sayısına el konulmasından sonra, yayıncılar 2500 adet nüshayı basarak, çok kalabalık olan Amsterdam sokaklarında satmışlardır. Dolayısıyla, söz konusu bilgiler derginin toplatılmasına karar verildiğinde zaten geniş bir kitleye ifşa edilmiş bulunmaktadır. AİHM, daha önceki bazı kararlarında belirli bilgilerin zaten açıklanmış ya da gizli olmaktan çıkmış olduğu görüldüğünde, bu bilgilerin açıklanmasını engellemenin gereksiz olduğuna hükmetmiştir. Söz konusu bilgilere çok sayıda insan ulaşmış ve başkalarına da aktarmış olması, medyanın yorumlar yapması, bu bilgilerin devlet sırrı olarak muhafazasını haklı göstermemektedir. dolayısıyla derginin ilgili sayısının toplatılması, izlenmekte olan “meşru amaca” ulaşma bakımından zorunlu görünmemektedir.

Benzer bir karar da The Observer ve The Guardian davasıdır.⁴³³ Bu iki gazete, emekli bir İngiliz istihbarat görevlisi olan Peter Wright'ın yazmış olduğu, ancak henüz basılmamış olan "Spycatcher" isimli kitabının el yazmalarından bir bölümünü 1986 yılında yayınlamak istemiştir. Peter Wright'ın kitabı, istihbarat servislerinin ve görevlilerinin yürüttüğü, kanunsuz olduğu iddia edilen bir takım faaliyetleri anlatmaktadır. Başsavcı mahkemelerden gazetelerin kitaptan bölümler yayınlamasını engelleyecek sürekli bir tedbir kararı çıkarmasını talep etmiştir. Mahkemeler sürekli tedbir kararının görüşülmesi süresince, yayını engellemek üzere geçici bir tedbir kararı çıkartmıştır. Ancak, Temmuz 1987'de kitap Amerika Birleşik Devletleri'nde basılmış ve Britanya'da da erişilir olmuştur. Buna rağmen gazetelere karşı verilmiş olan geçici tedbir kararları Ekim 1988'e kadar yürürlükte kalmıştır.

The Observer ve The Guardian gazeteleri geçici tedbir kararları aleyhinde AİHM'e başvurmuştur. Hükümet savunmasında geçici tedbir kararlarının alındığı dönemde, Peter Wright'ın ulaşmış olduğu bilgilerin devlet sırrı niteliği taşıdığını öne sürmüş ve söz konusu bilgilerin o dönemde yayınlanması halinde, Britanya istihbarat servisi, görevlileri ve üçüncü tarafların, görevlilerin kimliğinin ortaya çıkmasıyla büyük bir zarar görecekları, müttefik ülkelerle, kuruluşlarla ve kişilerle ilişkilerin de zarar göreceği ve neticede istihbarat servisine güvenlerini yitireceklerini belirtmiştir. Ayrıca Hükümet, Britanya istihbarat servisinin diğer eski ya da halen çalışmakta olan görevlilerinin de aynı yola sapabileceğini ileri sürmüştür. Kitabın yayınlanış tarihinden sonraki dönem açısından, Hükümet savunmasını müttefik ülkeleri Britanya istihbarat servisinin elindeki bilgileri sağlam biçimde muhafaza edeceğine inandırma gerekliliğine dayandırmıştır. Hükümet bu inancı sağlamanın yolunun, gizli bilgiyi açıklamaya yeltenen çalışanların yasal yoldan engellenebileceğinin açıkça gösterilmesi olduğunu belirtmiştir.

Mahkeme sonuç olarak müdahalenin kanunla öngörüldüğüne ve kanunda belirtilen ulusal güvenliğin korunması amacının varlığına karar vermiştir. Ancak, Mahkeme müdahalenin ulusal güvenliğini korumak için demokratik bir toplumda gerekli olup olmadığı konusunda davayı, kitap ABD'de basılmadan önceki dönem ve sonrası olmak üzere ele almıştır. Buna göre, Mahkeme Temmuz 1986 ile Temmuz 1987 dönemdeki geçici tedbirin demokratik bir toplumda gerekli olduğuna karar verirken; kitabın basılması ve İngiltere'de de ulaşılabilir olmasından sonra devam eden tedbirin, demokratik bir toplumda gerekli olmadığına ve 10. maddenin ihlaline karar vermiştir.

⁴³³ The Observer ve The Guardian, Birleşik Krallığa Karşı, Başvuru no.: 13585/88, 26 Kasım 1991.

Bu kararlar AİHM ifade özgürlüğü ve milli güvenlik dengesine yaklaşımı açısından iki önemli noktayı ortaya koymaktadır. Birinci ilke, ulusal güvenlik konusundaki bilgilerin, bir kez kamu alanına çıktıktan sonra yasaklanamayacağı, yayının toplatılamayacağı ve bilginin yayılmasına aracı olanların cezalandırılmayacağıdır. İkincisi ise, devletler tarafından ulusal güvenlik alanında her tür bilginin kayıtsız koşulsuz gizli olarak nitelenemeyeceği ve bu tür bilgiye ulaşma olanağına önceden bir sınırlama getirilemeyeceğidir. Bilginin gizlilik statüsü zaman açısından sınırlı olmalı ve statüsü periyodik olarak incelenmelidir. Ulusal güvenliğe ilişkin bilgilere gizlilik statüsünün verilmesinde ya da gizliliğin sona erdirilmesinde bilgi edinme hakkı da göz önüne alınmalıdır. Dolayısıyla, ulusal güvenlik alanında her tür bilginin yayılmasını mutlak ve koşulsuz tarzda yasaklayan, istihbarat servislerinin faaliyetleri üzerinde kamu denetimini ortadan kaldıran türden mevzuat, “demokratik bir toplumda gerekli” olmadığı için, 10. Madde’nin ihlali anlamına gelmektedir.⁴³⁴

AİHM’in ulusal güvenliğe yaklaşımını ortaya koyan bir diğer ilke Johannesburg İlkeleri arasında, 12. ilkede bulunmaktadır. Bu ilkede devletin ulusal güvenliğe ilişkin her türlü bilgiye ulaşmayı kategorik olarak reddedemeyeceği, gizlenmesi gereken bilgi kategorilerinin yasalarla tanımlanması ve dar tutulması gerektiği yönündedir.⁴³⁵ Buna ilaveten 15. ilkede, açıklanan bilginin meşru bir ulusal güvenlik çıkarına fiilen zarar vermemesi, zarar verecek nitelik taşınamamasının muhtemel olması veya bilginin öğrenilmesi ile zarara nispeten daha fazla kamu yararı doğması durumunda, ulusal güvenlik gerekçesi ile bir şahsa ceza verilemeyeceği öngörülmektedir.⁴³⁶

Bir diğer örnek dava da Sürek ve Özdemir davasıdır.⁴³⁷ Bu davada haftalık bir yayın olan “Haberde Yorumda Gerçek” adlı bültenin sahibi ve editörü olan davacılar bölücü propaganda yapma suçundan 6 ay hapis ve para cezasına çarptırılmıştır. Ayrıca bültenin basılmış sayıları da toplatılmıştır. Davacılar, bültende PKK’nın üst düzey bir sorumlusu ile yapılmış iki röportajı yayınlamıştır. Röportajda söz konusu şahıs, Türk otoritelerinin ülkenin güney doğusunda izlediği ve ona göre Kürtleri kendi bölgelerinden sürmeyi ve direnişlerini kırmayı amaçlayan politikalarını kınayan yorumlar yapmış ve yine kendisine göre Kürt halkı adına sürdürülen savaşla ilgili

⁴³⁴ Monica Macovei, “İfade Özgürlüğü AİHS’nin 10. Maddesi’nin Uygulanmasına İlişkin Kılavuz”, *İnsan Hakları El Kitapları*, No. 2, s.34., (Çevrimiçi), <http://www.inhak-bb.adalet.gov.tr/aihs/madde10.htm>, 29 Ocak 2006.

⁴³⁵ Macovei, a.y.

⁴³⁶ Macovei, a.g.e., s.35.

⁴³⁷ Sürek ve Özdemir, Türkiye’ye Karşı, Başvuru no.: 23927/94 ve 24277/94, 08 Temmuz 1999.

“bizim tarafta tek bir insan kalana kadar devam edecek” ifadesini içeren bir beyanda bulunmuştur. Davacılar, ayrıca, dört örgüt tarafından yapılmış bir ortak açıklamayı da yayınlamıştır. Bu örgütler de, aynen PKK gibi, Türk yasalarına göre yasadışı örgütlerdir. Ortak açıklamada, Kürt halkının kendi kaderini tayin etme hakkının tanınması ve Türk ordusunun sözde Kürdistan’dan çekilmesini savunulmuştur.

Bültenin terörist bir örgüte ait açıklama içermesi ve bölücü propaganda yapması nedeniyle savcı tarafından suç duyurusunda bulunulmuştur. Davacılar, İstanbul Devlet Güvenlik Mahkemesi tarafından, PKK lideri ile yapılan görüşme ve dört terörist örgüt tarafından yapılan açıklamayı yayınlamak suretiyle, devletin ülkesi ve milletiyle bölünmez bütünlüğüne karşı propaganda yapmakla suçlanarak, 1991 tarihli Terörle Mücadele Kanunu’nun 6. ve 8. maddeleri gereği cezalandırılmıştır.

Davacılar, olayı AİHM’e götürmüştür. AİHM kararında, hükümet söz konusu olduğunda, mazur görülebilecek eleştiri sınırlarının bir vatandaş, hatta bir politikacı için olduğundan çok daha geniş olduğu ve görüşmelerin yasaklanmış bir örgütün önde gelen bir üyesi ile yapılmış olmasının, devlet politikasına yönelik sert eleştiriler içermesinin ve Türkiye’nin güney doğusundaki durum ve çatışmaların sorumluluğu konularında tek yanlı bir görüşü aktarmasının tek başına davacıların ifade özgürlüğüne bir müdahaleyi haklı kılmayacağını belirtmiştir. AİHM’e göre, görüşmeler, hem Türkiye’nin güney doğusunda resmi politikaya muhalefetin ardındaki motivasyonu temsil eden insanların psikolojisinin, hem de çatışmanın ne gibi sonuçlar doğurabileceğinin anlaşılmasını sağlamak açısından, kamuya haber niteliğindedir. Mahkeme ayrıca, ulusal otoritelerin kendileri açısından ne kadar kabul edilemez olursa olsun, kamunun Türkiye’nin güney doğusundaki durum hakkında değişik bir bakış açısı konusunda bilgilenme hakkı ile ilgili olarak yeterince titizlik göstermediğine hükmetmiştir. Bu davada görevli yargıçlardan G. Bonello kararı destekleyici görüşünde demokratik bir toplumda hükümetlerin şiddeti destekleyen düşünceleri cezalandırmalarının, ancak yapılan kışkırtma ve tahrikin “açık ve yakın” bir tehlike oluşturması durumunda haklı görülebileceğini belirtmiştir.

Buna karşılık, Sürek (3) davasında,⁴³⁸ farklı bir yaklaşım sergilenmiştir. Yine aynı bültende yayınlanan bir haberde “Bugün bizim savaşımız, Türkiye Cumhuriyeti güçlerine karşı bir iç savaştır. Biz topyekûn bir bağımsızlık mücadelesi başlatmak istiyoruz.” ifadesi kullanılmıştır. Davacı İstanbul Devlet Güvenlik Mahkemesi

⁴³⁸ Sürek, Türkiye’ye Karşı, Başvuru no.:24735/94, 08 Temmuz 1999.

tarafından 1991 tarihli Terörle Mücadele Kanunu'nun 8. maddesi gereği devletin bölünmezliği aleyhine propaganda yapmak suçundan cezalandırılmıştır.

AlHM'de görülen davada, ifade hürriyetine müdahale bulunulduğu, ancak bunun kanunla öngörüldüğü ve demokratik bir toplumda gerekli olduğuna karar verilmiştir. Mahkeme, Türkiye'nin güney doğusundaki güvenlik hassasiyeti ve otoritelerin şiddeti körükleyecek faaliyetlere karşı tetikte olmaları ihtiyacı göz önüne alındığında, davacıya karşı alınan tedbirin ulusal güvenliğin, toprak bütünlüğünün veya kamu emniyetinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi amacını taşıdığına açık olduğunu değerlendirmiştir.

Söz konusu yazının içeriğinde bulunan ifadeler incelendiğinde okuyucular tarafından, yazarın Türkiye Cumhuriyetine karşı silahlı bir mücadeleyi cesaretlendirdiği hatta bir iç savaşa çağrıda bulunduğu şeklinde algılanabileceği ve bu nedenle şiddeti ve bölücülüğü destekler mahiyette olduğu değerlendirilmiştir. Yayın aracını sahibi olarak davacının, basım ve yayımla ilgili sorumluluğu üzerine aldığından hareketle ulusal güvenlik ve kamu güvenliğinin korunması ihtiyacı ile cezalandırılmasının toplumsal bir ihtiyaç baskısı gereği ve orantılı olduğuna, dolayısıyla 10. maddenin ihlalinin söz edilemeyeceğine karar verilmiştir.

Benzer bir davada ise Mehdi Zana⁴³⁹ Diyarbakır'ın eski Belediye Başkanı'dır. 1987 yılı Ağustos ayında Diyarbakır Askeri Cezaevinde hapis yataken, gazetecilerin kendisi ile yaptığı röportajda "PKK'nın ulusal kurtuluş hareketini destekliyorum. Katliamlardan yana değiliz, yanlış şeyler her yerde olur. Kadın ve çocukları yanlışlıkla öldürüyorlar." ifadesini kullanmıştır. Bu konuşmanın gazetede yayınlanması sonrasında Diyarbakır Devlet Güvenlik Mahkemesi, "kanunun cürüm saydığı bir fiili övdüğü" ve "kamu güvenliğini tehlikeye soktuğu" gerekçesiyle Zana'nın 12 ay ağır hapis cezasına çarptırılmasına karar vermiştir.

AlHM'e taşınan davada, AlHM kısaca röportajın, söz konusu dönemde aşırı bir gerilimin bulunduğu Türkiye'nin güneydoğusunda, PKK'nın sivillere yönelik olarak sürdürdüğü kanlı saldırılar ile aynı döneme rastlaması ve Türkiye'nin güneydoğusundaki en önemli kenti Diyarbakır'ın eski belediye başkanının, büyük günlük gazetelerden birinde yayınlanan röportajında kullandığı "ulusal kurtuluş hareketi" ifadesiyle PKK'ya destek vererek, o bölgede zaten var olan patlamaya hazır durumu daha da kötüleştireceğini değerlendirmiştir. Mahkeme, davacıya verilen cezanın toplumsal bir ihtiyaç baskısına makul bir yanıt olarak görülebileceğini

⁴³⁹ Zana, Türkiye'ye Karşı, Başvuru no.:69/1996/688/880, 25 Kasım 1997.

ve ulusal makamlarca gösterilen gerekçelerin uygun ve yeterli olduğunu kabul ederek, 8'e karşı 12 oy çoğunluğu ile 10.maddenin ihlalinin söz konusu olmadığına karar vermiştir.

İncelenen son iki davanın farkı ifade edilen düşüncelerin şiddete yöneltme kabiliyetinde ve bu şiddetin ortaya çıkması olasılığında yatmaktadır. Her ikisinde de açık ve yakın bir tehlikenin var olduğuna kanaat edilmiştir. Ayrıca Mahkeme, Zana davasında kişinin demokratik toplumda üstlendiği ödev ve sorumluluklar gereği, açıklama özgürlüğünün sınırlarının daralıp genişlediğine vurgu yaparak, kişinin bu özgürlüğü kullanırken taşıdığı sıfatın kendisine yüklediği görev ve sorumlulukları göz önünde tutmak zorunda olduğunu da ortaya koymuştur.

AlHM, AlHS'nin 8. ve 11. maddelerine "milli güvenlik" nedeniyle getirilecek sınırlamalar konusunda da 10. madde ile aynı sistemi izlediği görülmektedir. Ulusal güvenliği korumak amacıyla 8. maddede belirtilen hakların sınırlandırılmasına ilişkin Leander-İsveç⁴⁴⁰ davasında Mahkeme, bir bireyin 8. maddedeki haklarını korumak için gerekli usul önlemlerinin özelliklerini detaylı bir biçimde ele almıştır. Bu örnekte, davacının kadrolu olarak istihdam edilmesi önlenmiş ve otoritelerin görüşüne göre kendisini güvenlik açısından riskli kılan bazı gizli bilgiler nedeniyle, geçici istihdamı da sona erdirilmiştir. Davacı hem bu bilgilerin kaydedilmesi, hem de kullanılmasının yanı sıra, kendisine bu iddiaları çürütme fırsatı verilmemesinin, 8. Madde 1. fıkrada teminat altına alınan özel hayatına saygı gösterilmesi hakkını ihlal ettiği konusunda şikâyetle bulunmuştur. Mahkeme, dava sonunda personel kontrol sisteminin davacının özel hayatına müdahale olduğunu kabul etmekle beraber; davacının haklarının istismarına karşı mevcut önlemleri göz önünde bulundurarak, bu sistemin demokratik bir toplumda gerekli olduğunu da belirtmiştir.

Mahkeme, ulusal güvenliği korumak amacıyla, Devletlerin yetkililere kamunun ulaşmadığı kayıtlarda bilgi toplama ve kaydetme yetkisini veren kanunlara ihtiyaç duyduğunu kabul etmiştir. Ayrıca, ulusal güvenlik açısından önemli olan görevlere alınacak adayların değerlendirilmesinde bu bilgilerin kullanılmasının da kabul edilebilir bir uygulama olduğunu belirtmiştir. Söz konusu istisnai şartları ve özel görevleri tanımlamak, Devletin sorumluluğundadır. Ancak, Mahkeme bu tür davalarda, yetkinin istismarına karşı yeterli ve etkin teminatların olduğu konusunda tatmin olması gerektiğini de belirtmiştir. "Ulusal güvenliği korumak için oluşturulan bir gizli gözetim sistemi, demokrasiyi korumak adına demokrasiye zarar

⁴⁴⁰ Leander,İsveç'e karşı, 26 Mart 1987 tarihli karar.

verebileceği, hatta demokrasiyi yok edebileceği” riski göz önünde bulundurularak, teminatların gerekli olduğunu belirtmiştir.

Klass ve diğerleri Almanya davasında, davacılar 13 Ağustos 1968 tarihli “Mektup Posta ve Telekomünikasyon Gizliliğinin Sınırlandırılması Hakkındaki Kanun”un tanıdığı mektup ve posta açma ve inceleme, telgraf mesajlarını okuma, telefon konuşmalarını dinleme ve kaydetme yetkilerinin, kişinin haberleşmeye hürriyeti hakkını ihlal ettiğini ileri sürmüşlerdir. Bu davada, davacılar mağdur olmasalar da yasanın herkese uygulanabileceğinden hareketle mağdur olarak kabul edilerek, 8. maddeye uygunluğu denetlenmiştir. Mahkeme dava sonucunda devletin ulusal güvenlik amacıyla, suçu ve düzensizliği önlemek için demokratik bir toplumda gerekli olan bu yasayla müdahalesinin haklı olduğuna karar vermiştir. Mahkeme bu kararında özellikle davalı devlette, müdahaleyi düzenleyen kanunların devlet yetkililerince suiistimaline karşın yeterli ve etkili güvence sistemi kurulup kurulmadığını da incelemiştir.⁴⁴¹

Mahkeme; ayrıca, AİHS’nin “Başlangıç” bölümüne atıf yaparak, “Temel özgürlükler, bir yandan etkin bir siyasal demokrasi, diğer yandan etkin bir anlayış ve sözleşmecî devletin dayandığı insan haklarının yerine getirilmesi ile korunabilir.” saptamasını yapmıştır. Bu saptama 8. madde kapsamında birinci fıkrada garanti edilen hakkın, birey tarafından kullanılması ile 2. fıkraya göre, demokratik bir toplumun korunması için gizli izlemeye olan ihtiyaç arasında denge yaratılması gerektiği anlamına gelmektedir. Mahkeme söz konusu davada bu dengenin korunduğuna kanaat etmiştir.⁴⁴²

AİHM’e “ulusal güvenlik” kapsamında götürülen ve 11. maddede tanınan hak ile ilgili davalar, siyasi partiler hakkında alınan kapatma kararları ile ilgilidir. AİHM, siyasi partilerin sağlıklı bir demokratik sistem için taşıdığı önem nedeniyle, sınırlamaların siyasi partiler söz konusu olduğunda mümkün olduğunca dar yorumlanması gerektiğini ve sadece tatmin edici sebepler söz konusu olduğunda partilerin dernekleşme özgürlüklerinin kısıtlanmasının haklı karşılanabileceğini belirtmektedir. İtalya’ya karşı yapılan bir başvuruda, ulusal güvenlik ve başkalarının

⁴⁴¹ Mine Kaya, “Avrupa İnsan Hakları Sözleşmesinde Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı”, s.17, (Çevrimiçi), <http://www.inhak-bb.adalet.gov.tr/aihs/madde8.htm>, 29 Ocak 2006.

⁴⁴² Erkan Demirtaş, “İnsan Hakları Avrupa Sözleşmesinin 8. Maddesi ve İlgili Yargı Kararları”, s.15, Ocak 2004, (Çevrimiçi), <http://www.inhak-bb.adalet.gov.tr/aihs/madde8.htm>, 29 Ocak 2006.

hak ve özgürlüklerinin korunması gerekçesiyle faşist bir siyasi partinin yasaklanmasının meşru olduğuna karar vermiştir.⁴⁴³

Refah Partisi davasında,⁴⁴⁴ AİHM siyasal partilerin, Sözleşme'nin ve özellikle 11. maddenin sağladığı korumadan yararlanmak suretiyle, devletin yasal yapılanmasını ya da anayasal kuruluşların değiştirilmesini amaçlayan çalışmalar yürütebileceğini, ancak bunu yaparken, kullanılan yöntemler ve alternatif olarak önerilen değişikliğin, tümüyle yasal ve demokratik ilkelerle bağdaşır durumda olması gerektiğini belirtmiştir. Mahkeme, Refah partisi yetkililerinin laiklik ilkesine farklı bir içerik getirdikleri bahanesiyle dini inanç ayırımına dayalı çok hukuklu bir sistem kurmak, Sözleşme'nin benimsediği değerden tamamen farklı özelliklere sahip İslami yapıyı (şeriat) kurmak amacıyla oldukları ve iktidara gelmek, özellikle de iktidarda kalmak için kuvvete başvurma yönündeki davranışları konusunda bir kuşkunun doğmasına neden oldukları kanaatine varmış ve Sözleşme'nin sağladığı korumadan yararlanma hakkına sahip olmadıklarını belirtmiştir. Mahkeme'nin vardığı kanaata göre, ilgili devlet Avrupa Sözleşmesi normlarıyla çelişen bir siyasi parti projesini, ülkenin demokratik rejimini ve iç barışını tehlikeye atma riski taşıyan somut eylemlerle yaşama geçirilmesinden önce engelleme hakkında sahiptir.

AİHM, HEP kararında ise HEP tarafından savunulan self determinasyon ve ana dilde konuşma ve yayın haklarının tanınması gibi prensiplerin bu haliyle demokrasinin temel ilkelerine aykırı olmadığını kabul ederek, bu prensiplerin siyasi bir parti tarafından sadece savunulmasının terörist eylemlere destek olarak değerlendirilemeyeceği ve böyle değerlendirildiği takdirde bu sorunların demokratik bir tartışma çerçevesinde ele alma imkânının azalacağını belirtmiştir. Mahkeme kapatma kararında HEP' in siyasi projeleri aracılığıyla Türkiye'deki demokratik rejime zarar vermeyi amaçladığının yeterli şekilde kanıtlanmadığını değerlendirmiştir. HEP yöneticilerinin güvenlik güçlerinin terörizme karşı mücadelelerinde kimi davranışları hakkındaki sert ve muhalif eleştirilerinin, tek başına HEP'in şiddet eylemleri işleyen silahlı gruplarla bir tutmak için delil oluşturmadığını belirterek ve Hükûmete karşı kabul edilebilir eleştirilerin sınırlarının herhangi bir bireye göre daha geniş olduğunu hatırlatmıştır. Parti Başkanı ve Milletvekillerinin güvenlik güçlerinin eylemleri konusundaki eleştirilerinin seçmenlerin kaygılarını dile getirmekten farklı bir amaç taşımadığını belirtmiş ve partinin ülkedeki

⁴⁴³ Mustafa Duran, "AİHS 11. Madde Demek Kurma ve Toplantı Özgürlüğü", s.5, (Çevrimiçi), <http://www.inhak-bb.adalet.gov.tr/aihs/madde11.htm>, 29 Ocak 2006.

⁴⁴⁴ Refah Partisi ve Diğerleri, Türkiye'ye Karşı, Başvuru no.: 41340/98, 41342/98, 41343/98 ve 41344/98, 13 Şubat 2003.

demokratik rejime zarar verecek nitelikte siyasi bir projesinin bulunmaması, siyasi amaçlarla güce başvurulmasını haklı göstermemesi veya bu yönde çağrısının olmamasına rağmen kapatılmasının makul şekilde zorunlu bir sosyal ihtiyaca cevap vermediği ve 11. maddenin ihlal edildiği sonucuna varmıştır.⁴⁴⁵

Sonuç olarak AİHM'in, AİHS'nin 8,10 ve 11. maddelerinde öngörülen hakların milli güvenlik ve diğer hallerde kısıtlanması konusunda değerlendirme yaparken, sırasıyla üç hususu göz önüne aldığı görülmektedir. Öncelikle bir ülkenin yetkili organları, ancak o ülkenin yasalarındaki düzenlemeleri temel alarak bu hürriyetlere müdahale etmelidir. Yani müdahalenin ilgili ülkede yasal dayanağı bulunmalı, keyfiyetten kaynaklanmamalıdır.

İkinci husus müdahalenin ilgili maddelerde belirtilen amaçlara yönelik olması gerekliliğidir. AİHS söz konusu haklara hangi amaçlarla müdahale edilebileceğini sıralamıştır. Dolayısıyla, müdahalenin sadece bu amaçlardan bir veya birkaçına yönelik olması gerekmektedir. Bu amaçlar sınırlı sayıda olduklarından taraf devletlerin bunlara yenilerini ekleme veya bu amaçları genişletme yetkisi yoktur.

Son husus ise karar verilmesi en zor olan müdahalenin demokratik bir toplumda gerekli olması şartının tespitidir. Bu şart aynı zamanda orantılılık ilkesini de içermektedir.

"Mahkemeye göre düşünceyi açıklama özgürlüğü yalnızca tasdik eden, zararsız olduğu kabul edilen ya da ilgilenmeye değmez düşünce ve fikirler için değil, hoşla gitmeyen, rahatsız edici ve taraflı olanlar için de geçerlidir. Bunlar, demokratik bir toplumun olmazsa olmaz unsurları içerisinde yer alan çoğulculuk, hoşgörü ve açık fikirliğin gerekleridir."⁴⁴⁶

"Mahkeme, demokratik toplumda gereklilik koşulunun irdelerken de zorlayıcı toplumsal ihtiyaç kavramını kullanmaktadır. Bu ihtiyacı kanıtlayan uygun, inandırıcı ve yeterli gerekçe, tedbirin ölçülülüğü, bireysel yararın toplumsal yararlarla karşılaştırılması ve tercih ölçütlerinin dava konusu somut olaya uygulayarak karara varmaktadır."⁴⁴⁷

⁴⁴⁵ Duran, a.g.e., s.6-7.

⁴⁴⁶ Zana Türkiye'ye Karşı, Başvuru no: 18954/91, 25 Kasım 1997, Lingens Avusturya'ya Karşı, Başvuru no:9815/82, 08 Temmuz 1986.

⁴⁴⁷ Barthold/Almanya-1985, Young, James ve Webster/İngiltere-1981.

Orantılılık ilkesinde ise aynı amacı elde etmek için daha az sınırlayıcı başka bir yöntemin olmaması veya uygulanan yönteminin müdahale amacını elde etmeye imkân vermesi değerlendirilmektedir.

Diğer önemli bir husus ise Mahkemenin 8, 10 ve 11. maddelerde sağlanan özgürlüklerin kısıtlanması ile ilgili davalarda “açık ve mevcut tehlike” ölçütüne benzer bir yaklaşım kullanmasıdır.⁴⁴⁸ Bu konuda literatürde de ifade özgürlüğünün sınırının belirlenmesinde “açık ve mevcut tehlike” kriterinin kullanılması görüşü yaygındır. Bu kriter, Amerikan Yüksek Mahkemesi tarafından 20. yüzyılın ilk yarısında geliştirilen bir doktrindir. Doktrine göre kelimeleri açık ve mevcut bir tehlike yaratan ifadelerin, ifade özgürlüğü kapsamında korunmaları mümkün değildir. Başka bir anlatımla, eğer bir ifadenin açıklanması durumunda bireyler veya toplum için açık ve mevcut bir tehlike oluşuyorsa, bu açıklamanın sınırlanması mümkündür. Tehlikenin “açık” olması, şüpheyi meydan vermeyecek biçimde ortada olması, “mevcut” olması ise, kullanılan kelimelerin zarar yaratma ihtimalinin kesine yakın olması anlamına gelmektedir. Dolayısıyla, sırf bir tehlike ihtimali içermesi, kendiliğinden o ifadeyi korumasız bırakma nedeni olamaz, tehlikenin meydana gelmesinin de kesine yakın olması gerekir.⁴⁴⁹ Açık ve mevcut tehlike kavramına getirilen açıklamaların en çok bilineni, Yargıç Holmes’un kalabalık bir tiyatrodan yalan yere “yangın” diye bağırarak kişinin eyleminin bu korumadan faydalanamayacağına dair açıklamasıdır.⁴⁵⁰ Zira kalabalıkta oluşacak bir panik tehlikesi açık ve kesin görülmektedir.

Kısaca AİHM ve Avrupa’nın yaklaşımında “milli güvenlik” kapsamında dahi olsa, söz konusu özgürlüklerin kısıtlanması doğrudan şiddeti teşvik etmesi veya tehlikeyi doğurması ihtimalinin var olması durumunda haklı görülmektedir. Terör örgütünü ve eylemlerini destekleyen, kin ve nefreti arttırmaya yönelik beyanlar dışında, demokratik bir toplumda düzeni sorgulayan, şiddet içermeyen direniş çağrıları yapan, terör örgütü söylemiyle özdeşleşmeyen sosyolojik beyanlar içeren açıklamalara sınırlama getirilmesi uygun görülmemektedir. Bu durumda henüz İnternet konusunda Türkiye ile ilgili içtihat oluşturacak kararlar bulunmamasına rağmen; İnternet alanında ulusal güvenlik ile temel hak ve özgürlükler dengesi açısından aynı yaklaşımın korunacağı değerlendirilebilir.

⁴⁴⁸ Kuzu, a.g.e., s.320.,

⁴⁴⁹ İnsan Hakları, Ankara, Matus Basımevi, 2006, s.67.

⁴⁵⁰ Lee C. Bollinger, Geoffrey R. Stone, “Dialogue”, **Eternally Vigilant: Free Speech in the Modern Era**, Ed. Lee C. Bollinger, Geoffrey R. Stone, The University of Chicago Press, 2002, s.2.

10. SİBER SUÇLAR VE TÜRKİYE'DE ULUSAL BİLGİ GÜVENLİĞİ

Günümüzde bilgisayar sistemleri ve İnternet teknolojisi sayesinde ortaya çıkan yeni suç yöntemleri ve yeni suçlar için farklı isimler kullanılsa da, suçların amaç ve araçları çeşitlilik gösterse de, hedef her zaman bilgi ve bilişim sistemleri olmaktadır. Bilişim suçlarının toplumdaki oranı artık göz ardı edilemeyecek boyutlara ulaşmış ve bireyden devlete bilişim sistemlerine artan bağımlılık, bilgi güvenliğini ön plana çıkarmıştır. Ulusal bilgi güvenliği kapsamında Türkiye'nin hâlihazırdaki durumunu, teknolojik ve hukuksal alanda olmak üzere iki başlık altında ortaya koymak mümkündür.

Ulusal bilgi altyapısının oluşturulması konusunda ciddi çalışmalarda bulunan ve "e-devlet kapısı" ile küresel ağa açılan Türkiye'nin bilgi güvenliği konusunda teknik anlamda çeşitli yetersizlikleri bulunmaktadır. E-dönüşüm eylem planı kapsamında, TÜBİTAK tarafından örneklem olarak alınan kamu kurumlarının bilgi sistem güvenliklerinin analiz edildiği raporda;⁴⁵¹

- Her kamu kurumun farklı güvenlik seviyesinde olduğu ve bir standart bulunmadığı,
- Mükerrer ve yetersiz çalışmalar yaptığı,
- Yetkinliği şüpheli danışman firmaların yönlendirmelerine maruz kaldığı,
- Kurumların genelinde saldırı tespit sistemi (STS) bulunmadığı veya bu sistemler tarafından tutulan kayıtların incelenmediği tespit edilmiştir.

Kısaca kamu kurumlarının yetersizlikleri düzenlenen saldırılara karşı koyulmasını, STS'nin bulunmaması veya kayıtlarının incelenmemesi ise kurumlara karşı yapılan saldırılar arasında ilişki kurularak, genel değerlendirme yapılmasını engellemektedir. Bu durum, küçük ölçekli saldırılar biçiminde gizlenerek, farklı dönemlerde ve çeşitli kurumlara yapılan büyük çaplı eylemlerin tespit edilememesine neden olmaktadır.

Türkiye'nin bilgi güvenliği konusundaki bir diğer zafiyeti ise milli olmayan yazılımların hâlihazırda kişisel ve kamusal bilgisayarlarda kullanılıyor olmasıdır. Bu yazılımlar daha önce bahsedildiği gibi tasarım amaçları dışında ve istenilmeyen

⁴⁵¹ Mert Üneri, "e-Dönüşüm Türkiye Bilgi Güvenliği Projeleri", s.7., (Çevrimiçi), http://www.bilgilotplumu.gov.tr/duyuru/icraKurulu/20070123_IK_XX_UEKAE_BILGIGUVENLIGI.pdf, 04 Nisan 2007.

zamanlarda kötü sonuçlar doğuracak şekilde kodlanabilmekte ya da kullanıldıkları sistemlere uzaktan gizlice erişilmesine imkân verecek kodlar içerebilmektedir. Bu durum ulusal bilgi alt yapısı için büyük bir tehdit teşkil etmektedir.⁴⁵² Aynı durum bilişim sistemlerinde kullanılan donanım için de geçerlidir. Türkiye savunma sistem gereksinimlerinin yaklaşık %80'ini yurt dışından karşılamaktadır.⁴⁵³ Ayrıca “müttefik bile olsalar, cihazların temin edildiği ülkeler de üçüncü ülkelere temin yoluna gidebilmektedir.”⁴⁵⁴ Dolayısıyla, “Türkiye’de araştırma ve geliştirme yatırımlarının yetersizliği, teknolojiye dışa bağımlılık ve hazır sistemleri tercih etme eğilimi”⁴⁵⁵ bilişim, savunma ve silah sistemlerine yönelik ciddi bir tehdit oluşturmaktadır.

Dışa bağlı yazılım ve donanım konusunda hassas olan Türkiye’nin durumunu değerlendirmede, yenilikler ve ileri teknoloji kullanımında her zaman öncü konumda bulunan TSK’nın güvenlik önlemleri örnek olarak gösterilebilir. TSK bünyesinde kullanılan yazılımların güvelliğinin sağlanması ve olası bir casus sistemin yerleştirilmesinin engellemesi maksadıyla üniversitelerden ve ihtisas kurumlarından alınan destek çalışmaları, TSK’nın bilgi işlem uzmanları denetiminde gerçekleştirilmektedir. TSK kendi yazılım ihtiyaçlarını karşılamak için uzman personelini kendi bünyesinde eğitmekte veya üniversitelerde eğitim almalarını sağlamaktadır. Bu nedenle büyük bir güvenlik endişesi taşımamaktadır. Ancak, teknik altyapı güvenliği, donanım özelliklerinden başlayarak değerlendirilmesi gereken bir konudur. Son kullanıcı için tasarlanan ve ara yüz adı verilen yazılımlardan daha çok, kullanılan işletim sistemi ve bu sistemin üzerinde çalıştığı donanım daha büyük riskler içermektedir. Türkiye’de de TSK dahil kullanılan işletim sistemi dışarıdan temin edilmekte ve açık kaynak kodları bilinmemektedir. Benzer şekilde donanım parçalarının tamamına yakını dışarıdan temin edilmektedir.⁴⁵⁶

Teknoloji ihtiyacını çoğunlukla gelişmiş endüstrilerden karşılayan Türkiye’nin bilgisayar sistemlerine ve ağlarına bağımlılığı her geçen gün artmaktadır. Bugüne kadar özel olarak Türkiye’deki bilgisayar sistemlerine zarar vermiş saldırılar görülmemekle birlikte, dünya çapına yayılan virüs saldırılarından Türkiye de etkilenmiştir. Büyük bir firmanın 2007 yılında yayınladığı İnternet güvenliği tehdit raporunda Türkiye, en fazla saldırıya uğrayan ülkeler arasında 17. sırada

⁴⁵² “Çalışma Grubu 4, E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları”, s.7.

⁴⁵³ A.y.

⁴⁵⁴ Yeni Dünya Stratejileri ve Kilit Ülke Türkiye, s. 211.

⁴⁵⁵ “Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi”, s. 52, TUBİTAK, Kasım 2004, (Çevrimiçi), http://vizyon2023.tubitak.gov.tr/Strateji_Belgesi-V211.pdf, 04 Nisan 2007.

⁴⁵⁶ Sandıklı, Yıvcier, a.g.e., s.10.

gösterilmektedir. Orta Doğu ve Afrika bölgesinde ise ilk sırada yer almaktadır.⁴⁵⁷ Özellikle siber terörizm potansiyeli gelecekte çok daha endişe verici boyutlara ulaşabilir.⁴⁵⁸ İç ve dış terörist unsurların hedefleri arasında yer alan Türkiye'nin resmi ve özel kuruluşlarının teknolojik altyapıları daha güvenli hale getirilmezse, siber terörizm tehdidinin artması muhtemeldir.⁴⁵⁹

Hukuksal alandaki düzenlemeler açısından değerlendirildiğinde ise Türkiye'nin hala önemli eksikliklerin bulunduğu değerlendirilmektedir. İnternet üzerinden yapılan bilgi transferleri, alım satımlar, para transferleri, fikir ve irade beyanlarının hukuksal sonuçlar doğurmasının sağlanması önemlidir. Özellikle e-dönüşüm süreci ile birlikte devlet kurumlarının kendi aralarında, özel sektörle ve vatandaşlarla gerçekleştirdiği işlemlerde kullanıcı doğrulaması yapabilme, inkâr edilemezlik, mesaj bütünlüğünün garanti edebilmesi ve verilerin korunması gibi temel gereksinimler ön plana çıkmaktadır. Bu işlemlere hukuki sonuç yaratacak yetkinliğin kazandırılması ise ancak uygun kanunların çıkarılması ile mümkün olmaktadır.

Bu kapsamda, “Elektronik İmza Kanunu” 23 Temmuz 2004 tarihinde, “Bilgi Edinme Hakkı Kanunu” ise 24 Nisan 2004 tarihinde yürürlüğe girmiştir. Bilgi Edinme Hakkı Kanununun uygulanmasına ilişkin esas ve usulleri belirleyen yönetmelik 27 Nisan 2004 tarihinde yayımlanmıştır. İlgili mevzuat hükümleri doğrultusunda Bilgi Edinme Değerlendirme Kurulu oluşturulmuştur. Elektronik İmza Kanununda öngörülen ikincil mevzuatla ilgili çalışmalar da tamamlanarak ilgili Yönetmelik ve Tebliğ, 6 Ocak 2005 tarihli Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Elektronik ortamdaki sözleşmelerin tanınması için çalışma yapılması ile ilgili düzenleme “Elektronik İmza Kanunu” içerisinde değerlendirilmiş ve ilgili kanunun 5. maddesinde “güvenli elektronik imza, elle atılan imza ile aynı ispat gücüne sahiptir” hükmü getirilmiştir. Ayrıca Kanunun 22 ve 23. maddeleri ile Borçlar Kanunu ve Hukuk Usulü Muhakemeleri Kanununun sözleşmelerin geçerliliği ile ilgili maddelerine eklemeler yapılarak, “elektronik imza ile oluşturulan elektronik verilerin senet hükmünde” olduğu da düzenlenmiştir.⁴⁶⁰

Elektronik ortamda bulunan fikri hakların korunması için tedbir alınması kapsamında ise 5101 sayılı kanun ile düzenlemelere gidilerek, bu alanda mevzuatta

⁴⁵⁷ “Türkiye İnternet’te Saldırı Şampiyonu”, BTDünyası İnternet sayfası, 22 Mart 2007, (Çevrimiçi), http://www.btdunyasi.net/index.php?module=news&news_id=3556&cat_id=1, 09 Nisan 2007.

⁴⁵⁸ Sandıklı, Yivcier, a.g.e., s.3.

⁴⁵⁹ A.e., s.2.

⁴⁶⁰ “E-Dönüşüm Türkiye Projesi 2003-2004 KDEP Uygulama Sonuçları ve 2005 Eylem Planı”, s.16.

yer alan eksikler giderilmiştir. Diğer taraftan, 5194 sayılı Kanunla da; fikri haklar konusunda yargının işleyişine ve bu alanda uygulanacak yaptırımlara ilişkin yeni düzenlemeler getirilmiştir.⁴⁶¹

Ancak, Avrupa Konseyinin Siber Suçlar Sözleşmesi ve yabancı ülke mevzuatlarından yararlanılarak, giderek yaygınlaşan İnternet kullanımı sonucu ortaya çıkan suçların cezalandırılabilmesi ve TCK'da bu konuda mevcut boşluğun doldurulmasını amaçlayan, "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı", 4 Mayıs 2007 tarihinde "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" adı altında kabul edilerek yürürlüğe girmiştir. Türkiye'de hizmet veren İSS'lerin, yer ve içerik sağlayıcıların görev, yetki ve sorumlulukları ile ilgili düzenlemelerin bir kısmı "Elektronik İmza Kanununda" düzenlenmiş ve eylem bu kısım itibarıyla tamamlanmıştır. Ancak yürürlüğe giren kanunun, tasarıdan oldukça eksik ve uzak olması nedeniyle yetersiz olduğu değerlendirilmektedir. Zira sadece İnternet sùjelerinin yükümlölüklerini ve TCK'nın bazı maddelerinde tanımlanan suçları teşkil eden yayınlara erişimin engellenmesini düzenlemekte ve cezaî sorumluluktan çok idarî yaptırımlar getirmektedir.

Buna ilaveten ulusal bilgi güvenliği politikası kapsamında büyük önem taşıyan "devlet sırrı" niteliğindeki bilgiler ve kişisel verilerin korunması için gerekli yasal düzenlemeler hala tamamlanamamıştır. Bu kapsamda,⁴⁶²

Devlet sırlarının ve niteliği itibarıyla gizli kalması gereken bilgi ve belgelerin tanımının yapılması, mahiyetinin belirlenmesi, hangi makam ve kurullarca oluşturulacağı ve korunacağı, bu bilgi ve belgelerin yargı organlarına hangi hâllerde gönderileceği ve yükümlölüklere ilişkin esas ve usulleri düzenleyen, "Devlet Sırrı Kanunu Tasarısı" 24 Kasım 2005 tarihinde,

Kişisel nitelikteki verilerin tanımının yapılması, esas ve unsurlarının belirlenmesi ve korunması amacıyla idarî bir yapının oluşturulması ile bireylerin şahsiyet haklarının himayesine ilişkin düzenlemeleri içeren, "Kişisel Verilerin Korunması Hakkında Kanun" tasarısı 09 Kasım 2005 tarihinde, Başbakanlığa gönderilmiştir. Söz konusu tasarıların halen görüşölerek, kabul edilmesi ve yürürlüğe girmesi beklenmektedir.

⁴⁶¹ A.e., s.17.

⁴⁶² Ayrıntılı Bilgi için Bkz.: Adalet Bakanlığı İnternet Sayfası, "Başbakanlıkta Bulunan Kanun Tasarıları", (Çevrimiçi), <http://www.kgm.adalet.gov.tr/basbakanliktabulunanlar.htm>.

Ulusal bilgi güvenliğinin sağlanması için gerekli görülen düzenlemeleri içeren, ulusal güvenliği ilgilendiren bilgilerin korunması, Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, ölçüt ve standartlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi, kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve görevlerine ilişkin esas ve usulleri düzenleyen, “Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı” ise taslak halinde kalmıştır.

Siber suçlarla mücadele kapsamında ülkemiz açısından büyük önem taşıyan bir diğer husus da toplu İnternet kullanımının kontrol altına alınmasıdır. Özellikle artan İnternet kafe sayısı ve bu mekânlarda suç işlemenin kolaylığı göz önüne alındığında, toplu İnternet hizmeti verilen mekânların işletmecilerinin veya yöneticilerinin suçun önlenmesi ve İnternet kullanımının kayıt altına alınmasına yönelik yükümlülüklerinin belirlenmesi suçla mücadele açısından zorunludur. Ülkemizde toplu kullanım sağlayıcıların yükümlülükleri 5651 sayılı Kanun’un 7. maddesinde düzenlenmektedir.⁴⁶³ Ancak, hâlihazırda İnternet kullanımının kayıt altına alınması konusunda bir yükümlülük bulunmamakta ve diğer yükümlülüklerin yerine getirilmemesi halinde ise cezaî yaptırım yerine idarî para cezası öngörülmektedir.

Türkiye’nin zararlı içerikle ilgili problemleri ise yıkıcı ve bölücü terör örgütlerinin ve yandaşlarının propagandalarını yapan İnternet sitelerinin, özellikle çocuk pornografisi olmak üzere pornografik içerikli sitelerin ve kumar sitelerinin yayınlarının engellenmesidir. Türkiye aleyhine faaliyet gösteren terör örgütleri, İnternet’in sağladığı olanaklardan öncelikle propaganda ve eğitim amaçlı olarak yararlanmaktadırlar. Bölücü örgütler, özellikle PKK klasik terör eylemlerini yapamaz hale geldikten sonra “siyasallaşma” sürecine girmiştir. Bu süreçte istifade ettikleri en önemli araç ise sayıları binleri geçen ve hâlihazırda yüzlercesi aktif olan İnternet siteleridir. Genelde “com”, “org” veya “net” uzantılı olan bu siteler ABD, Almanya,

⁴⁶³ 5651 Sayılı Kanun Madde 7 “(1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.

(2) Ticarî amaçla olup olmadığına bakılmaksızın bütün toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlüdür.

(3) Birinci fıkrada belirtilen yükümlülüğe aykırı hareket eden kişiye mahallî mülkî amir tarafından üçbin Yeni Türk Lirasından onbeşbin Yeni Türk Lirasına kadar idarî para cezası verilir.”

TASNİF DIŐI

Hollanda ve diğ er Batı Avrupa  lkeleri  zerinden faaliyet g stermektedirler.⁴⁶⁴ Dolayısıyla, bu sitelerle sadece uluslararası iŐbirliđi  er evesinde m cadele edilebilmekte, ancak h lihazırda uluslararası iŐbirliđi  abalarından olumlu sonu  almak kolay olmamaktadır. Nitekim, Almanya, Bel ika ve Hollanda'ya  lkelerinde T rkiye aleyhine faaliyet g steren zararlı sitelerin kapatılması i in DıŐıŐleri Bakanlıđı aracılıđıyla yapılan taleplerin hi birine olumlu yanıt alınamamıŐtır.⁴⁶⁵



⁴⁶⁴ B nyamin Atıcı,  etin G m Ő, "Sanal Ortamda Ger ek Tehditler: Siber Ter r", **Polis Dergisi**, Yıl 9, No.37, Ekim-Kasım-Aralık 2003, s.61.

⁴⁶⁵ Mehmet  zcan, "Siber Ter rizm ve Ulusal G venliđe Tehdit Boyutu", **Turkish Weekly**, ( evrimi i), <http://www.turkishweekly.net/turkce/makale.php?id=87>, 01 Temmuz 2006.

DÖRDÜNCÜ BÖLÜM

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİNİN İNCELENMESİ VE İÇ HUKUKTA SİBER SUÇLAR

1. AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ GENEL OLARAK

a. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Hazırlanış Süreci

Bilgisayar suçları üzerine Avrupa'da atılan ilk adım, Avrupa Konseyi'nin 1976 yılında Strasbourg'da düzenlediği Ekonomik Suçların Kriminolojik Yönü konulu konferans olmuştur.⁴⁶⁶ Avrupa Konseyi 1985 yılında bilgisayarlarla ilişkili suçların hukuksal yönünü tartışmak üzere konu ile ilgili uzmanların bir araya geldiği bir toplantı düzenlemiştir. Bu toplantıda uluslararası yasaların getirdiği sorumluluklar çerçevesinde, ulusal yasalarda yapılması öngörülen düzenlemelerin ana hatlarını içeren 1989 tarihli Öneri (Recommendation (89) 9) kabul edilmiştir. Söz konusu Öneri, bilgisayar sahteciliği, bilgisayar dolandırıcılığı, bilgisayar verilerine ya da programlarına zarar verilmesi, bilgisayar sabotajı, yetkisiz erişim, müdahale ve bilgisayar programlarının yetkisiz olarak çoğaltılması eylemlerini içermiştir.⁴⁶⁷

Konsey 11 Eylül 1995 tarihinde, bilişim teknolojileri ile ilgili suçlarda arama ve el koyma, teknik gözetim, soruşturma makamları ile işbirliği mecburiyeti, elektronik delil, kripto kullanımı, inceleme, eğitim ve uluslararası işbirliği ile ilgili usul hukuku konularını ele alan bir Öneriyi (Recommendation (95) 13) daha kabul etmiştir.⁴⁶⁸

Müteakiben Avrupa Suç Sorunları Komitesi (CDPC), Kasım 1996 yılında siber suçlarla mücadele etmek üzere, uzmanlardan oluşan bir komite kurma kararı almıştır. CDPC bu kararını, R (89) 9 sayılı tavsiyeye ek raporda, R (95) 13 sayılı tavsiyede ve Profesör H.W.K. Kaspersen'in kendi isteği ile hazırladığı raporda ulaşılan, tavsiye kararından daha çok maddi ceza hukuku, usul hukuku ve uluslararası ceza hukuku usullerine dayanan, Sözleşme gibi yükümlülük getiren bir hukuki araca başvurulması gerektiği sonucuna dayandırmıştır.

⁴⁶⁶ 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, page 225-229., akt: Stein Schjolberg, "Computer-Related Offences", A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime (15-17 September 2004, Council of Europe, Strasbourg, France), s.1, (Çevrimiçi), <http://www.cybercrimelaw.net/documents/Strasbourg.pdf>, 09 Mart 2007.

⁴⁶⁷ A.e., s.3.

⁴⁶⁸ Stein Schjolberg, Amanda M. Hubbard, "Harmonizing National Legal Approaches on Cybercrime", ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 28 June – 1 July 2005), ITU, 2005, s.9.

TASNİF DIŞI

Yeni komitenin görevleri bilgisayar suçlarına ilişkin R (89) 9 sayılı ve bilişim teknolojisiyle ilgili ceza usulleri hukuku sorunlarına ilişkin R (95) 13 sayılı Tavsiyeleri göz önünde bulundurarak;

- Özellikle İnternet gibi telekomünikasyon ağlarının kullanımı yoluyla işlenen siber suçları,
- Uluslararası işbirliği ve siber uzay aktörlerinin sorumlulukları konusunda gerekli olabilecek ceza hukuku konularını,
- Teknoloji ortamında geleneksel usul hukuku önlemlerinin uygulanabilirliğini,
- Bilişim suçlarının ortaya çıkardığı yargı yetkisi sorunun çözülmesini,
- Siber suçların soruşturulması esnasında uluslararası işbirliği meselelerini incelemek olarak belirlenmiştir.⁴⁶⁹

Avrupa Konseyi Bakanlar Kurulu, 4 Şubat 1997 yılında aldığı kararla, Siber Uzay Suçları Uzmanları Komitesi (PC-CY) adı verilen yeni bir komite oluşturmuştur. Aynı yıl Nisan ayında siber suçlara ilişkin uluslararası bir sözleşme taslağı üzerinde çalışmalarına başlayan Komite, başlangıçta 31 Aralık 1999 tarihi olarak belirlenen bitirme tarihinde çalışmayı tamamlayamadığı için görev tanımı 31 Aralık 2000'e uzatılmıştır. Avrupa Adalet Bakanları ve Avrupa Birliğine üye ülkeler de PC-CY'nin çalışmalarını desteklemiştir.⁴⁷⁰

PC-CY Komitesi, Nisan 1997 ile Aralık 2000 tarihleri arasında 10 genel kurul toplantısı ve açık uçlu Taslak Grubuyla da 15 toplantı yapmıştır. Komite görev süresinin bitiminin ardından, CDPC'nin himayesinde, Parlamenterler Meclisinin görüşü ışığında, Açıklayıcı Rapor taslağını son haline getirmek ve Sözleşme taslağını gözden geçirmek üzere üç toplantı daha yapmıştır. Bakanlar Kurulu, Meclisten, Nisan 2001'deki genel kurul toplantısının ikinci bölümünde kabul ettiği Sözleşme taslağı üzerine görüş bildirmesini talep etmiştir.⁴⁷¹

Taslağın hazırlanması esnasında Parlamenterler Meclisinde, Siber Suçlar Sözleşmesi taslağına ırkçı ve yabancı düşmanlığını teşvik eden İnternet siteleri ile

⁴⁶⁹ Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Rapor, "Explanatory Report", (Çevrimiçi), <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>, 10 Ekim 2006, paragraf 11.

⁴⁷⁰ Açıklayıcı Rapor, paragraf 12.

⁴⁷¹ Açıklayıcı Rapor, paragraf 13.

ilgili maddelerin dahil edilip edilmemesi konusu da gündeme gelmiş ve müzakere edilmiştir. Meclisin 24 Nisan 2001 tarihinde yapılan toplantısında bazı üyeler ırkçı siteler konusunda gerekli olabilecek maddelerin de Sözleşme taslağına dahil edilmesini önermişlerdir. Bu konuda Avrupa'nın geçmişte ırkçı kin ve nefret nedeniyle karşılaştığı olaylar örnek verilerek destek aranmıştır. Ancak, Sözleşmenin bir an önce yürürlüğe girebilmesi ve dünya genelinde daha fazla devletin katılımının sağlanabilmesi hususları göz önüne alınarak, Mecliste yapılan oylama sonucunda bu konuda ayrı bir protokol hazırlanmasına karar verilmiştir.⁴⁷²

Gözden geçirilmiş ve son haline getirilmiş Sözleşme taslağı ve Açıklayıcı Raporu Haziran 2001'deki genel kurulda onaylanmak üzere CDPC'ye ve ardından Sözleşme taslağının metni kabul edilmek ve imzaya açılmak üzere Bakanlar Kuruluna sunulmuştur.⁴⁷³

Sözleşme metni Bakan Vekilleri komitesi tarafından 19 Eylül 2001 tarihinde onaylanmıştır. 8 Kasım 2001 tarihinde toplanan Dışişleri Bakanları tarafından resmen kabul edilen Sözleşme, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılmıştır.⁴⁷⁴ Avrupa Konseyi Siber Suçlar Sözleşmesi hâlihazırda 46 Avrupa Konseyi üyesi ülkenin 38'i ve Konsey üyesi olmayan ancak hazırlık aşamasında katkıda bulunan Kanada, Japonya, Montenegro, Güney Afrika ve ABD olmak üzere toplam 43 ülke tarafından imzalanarak, 1 Temmuz 2004 tarihinde yürürlüğe girmiştir.⁴⁷⁵ Türkiye Avrupa Konseyi üyesi olarak hazırlık çalışmalarına katıldığı⁴⁷⁶ Sözleşmeyi henüz imzalamamıştır.

b. Sözleşme'nin Amaçları

Sözleşme⁴⁷⁷ İnternet ve diğer bilgisayar ağları üzerinden işlenen suçlara ilişkin ilk uluslararası anlaşma olarak değerlendirilmektedir.⁴⁷⁸ Sözleşmenin taraf ülkelere,

⁴⁷² Niraj Nathwani, "Atlantic Divide on Fight Against Racist Websites", (Çevrimiçi), http://eumc.europa.eu/eumc/index.php?fuseaction=content.dsp_cat_content&catid=3e3e6e32a2316&contentid=3e3e8aedf03d5, 20 Şubat 2007.

⁴⁷³ Açıklayıcı Rapor, paragraf 15.

⁴⁷⁴ Niraj Nathwani, a.y.

⁴⁷⁵ Sözleşmeyi imzalayan ülkeler ve tarihler için Bkz.: "http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=3/15/2007&CL=ENG".

⁴⁷⁶ Çeken, a.g.e., s. 128,

"Main Lines of the Convention", Council of Europe, (Çevrimiçi), http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/e_lignesconv.asp, 10 Ocak 2007.

⁴⁷⁷ Avrupa Konseyi Siber Suçlar Sözleşmesi'nden bu bölümden itibaren yalnızca "Sözleşme" olarak bahsedilecektir.

⁴⁷⁸ Cangemi, a.g.e, s.165.

bilgisayarlarla ilgili tüm suçlarla mücadele etmek için gerekli maddi ceza hukuku ve usul hukukunun temel çatısını sağladığı ve uluslararası kovuşturmalarını birbirleriyle süratli bir biçimde koordine etmelerine imkân vereceği belirtilmektedir.⁴⁷⁹

Sözleşme temelde üç ana amacı gerçekleştirmeyi hedeflemektedir. Bunlar;

- Siber suçlarla ilgili ulusal düzeydeki yasal düzenlemeler ve bağlantılı hükümlerin uyumlu hale getirilmesi,
- Siber suçların ve ilaveten bilgisayar yardımıyla işlenen diğer suçlar ve elektronik delil içeren klasik suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku yetkilerini sağlamak,
- Uluslararası işbirliği alanında hızlı ve etkin bir rejim oluşturmaktır.⁴⁸⁰

Usul hukuku açısından bakıldığında çoğu ülkede henüz siber uzayda uygulanabilecek spesifik usul hukuku kuralları bulunmamaktadır. Kısaca gerçek dünya için geçerli olan geleneksel soruşturma yöntemlerinin siber dünya için büyük oranda uygulanamaz olduğu ortaya çıkmaktadır. Sözleşmenin usul hukuku bölümü bilgisayar ağlarını kapsayan yeni soruşturma yöntemlerini belirleyerek bu yetersizliği gidermeyi amaçlamaktadır.⁴⁸¹

c. Genel Hükümler ve Terimler

Sözleşme'ye genel olarak bakıldığında, ilk dikkati çeken nokta Sözleşme'nin adında geçen "siber suçlar" ifadesine karşılık, "siber suç" kavramının bir tanımının yapılmadığıdır. İlk bakışta bu yaklaşımı Sözleşme'nin bir eksiği gibi değerlendirmek mümkündür. Ancak, Sözleşme'yi hazırlayanlar daha önceki bölümlerde de ifade edildiği gibi üzerinde anlaşılmış tek bir tanımlı bulunmayan "siber suç" kavramını açıklamaya çalışmaktansa, bu kapsamda değerlendirilebilecek temel suçları belirlemeyi ve bunları tek tek sıralamayı uygun görmüştür. Bu sayede hem siber suç kavramı ile ilgili taraf ülkelerde ortaya çıkacak yorum farklarını ortadan kaldırmayı, hem de Sözleşme'ye mümkün olan en çok katılımı sağlamayı amaçladıkları değerlendirilmektedir.

⁴⁷⁹ Pocar, a.g.e., s.30.

⁴⁸⁰ Açıklayıcı Rapor, paragraf 16.

⁴⁸¹ Cangemi, a.g.e., s.166.

Söz konusu yaklaşımın diğer bir faydası da her geçen gün gelişen teknoloji ile birlikte yeni suçların ortaya çıkması durumunda, ortaya çıkan suçun bir madde olarak kolayca eklenmesini ve taraf ülkelerin kendi ulusal mevzuatlarında bu kapsamda değerlendirdikleri diğer suçları da dahil etmelerine imkân tanınmasıdır.⁴⁸²

Sözleşmenin Ulusal Düzeyde Alınacak Önlemler bölümünde madde 2 ile 11 arasında belirtilen suçlar dört ana başlık altında toplanmıştır. Bunlar;

Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar,

Bilgisayarlarla ilişkili suçlar (Computer Related Crimes),

İçerikle ilişkili suçlar (Illegal Contents),

Telif haklarının ve benzer hakların ihlaline ilişkin suçlardır.

Dolayısıyla daha öncede belirtildiği üzere Sözleşme suçları ayırmasına rağmen siber suçun genel bir tanımını ve çerçevesini koymaktan ziyade suçları sıralamış ve genel olarak tüm bu suçları siber suçlar olarak tarif etmiştir. Buna ilaveten, Sözleşme metninde kullanılan terimlerin anlamları Sözleşmenin ilk maddesinde tanımlar başlığı altında ifade edilmiştir. Birinci maddeye göre,⁴⁸³

- "Bilgisayar sistemi" terimi, bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı,

- "Bilgisayar verisi" terimi ise, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsepti ifade etmektedir.

- "Hizmet sağlayıcı" terimi;

- hizmetlerinden faydalanan kullanıcılara bir bilgisayar aracılığıyla iletişim kurma imkânı sağlayan her türlü kamu ve özel sektör tüzel kişisi, ve

- söz konusu iletişim hizmeti veya bu hizmetin kullanıcıları adına bilgisayar verilerini işleyen veya saklayan diğer her türlü kişi ve kuruluşu ifade etmektedir.

⁴⁸² Açıklayıcı rapor, paragraf 40.

⁴⁸³ Siber Suçlar Sözleşmesi Madde 1.

TASNİF DIŞI

• “Trafik bilgileri” terimi ise bir bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, söz konusu iletişim zincirinin bir halkası konumunda bulunan bir bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını, süresini veya bu iletişimde kullanılan hizmetin tipini gösteren herhangi bir bilgisayar verisini ifade etmektedir.

Ülkemizde TCK’da “siber suç” kavramı yerine daha önce de belirtildiği gibi daha geniş bir kavram olan “bilişim alanında suçlar” ifadesi kullanılmıştır. TCK bilişim alanındaki suçları dört başlık altında toplamıştır. Bunlar;

- Bilişim sistemine girme,
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme,
- Banka veya kredi kartlarının kötüye kullanılması,
- Tüzel kişiler hakkında güvenlik tedbirler uygulanmasıdır.

Buna ilave olarak TCK’da bilişim suçları sadece bu bölümde düzenlenmemiştir. TCK’da bilişim sistemleri aracılığıyla işlenen klasik suçlar bilişim alanında suçlar bölümüne dahil edilmekten ziyade, bilişim sistemlerinin ortaya çıkışı ve varlığı ile hayat bulan ve bilişim sistemleri ve verilere yönelik yeni suçlar bu bölümde düzenlenmiştir. Bununla beraber hırsızlık, dolandırıcılık gibi klasik suçların bilişim sistemleri aracılığıyla işlenmesi nitelikli hırsızlık ve nitelikli dolandırıcılık şeklinde ayrıca tanımlanmıştır. Bu nedenle, aslında TCK’da bilişim sistemlerine karşı veya bilişim sistemleri aracılığı ile işlenen suçlar ve bilişim sistemleri yardımıyla işlenen klasik suçlar birbirinden ayrı ele alınmıştır. TCK’nın diğer bölümlerinde ve yürürlükte olan diğer kanunlarda düzenlenen bilişim suçları da mevcuttur. Bunlar ise;

- Özel hayata ve özel hayatın gizli alanına karşı suçlar bölümünde düzenlenen suç tipleri,
- Bilişim sistemleri aracılığıyla işlenebilecek diğer suç tipleri,
- Fikir ve Sanat Eserleri Kanunu’nda düzenlenen bilişim suçları,
- Elektronik İmza Kanunu’nda düzenlenen bilişim suçlarıdır.

Ayrıca, daha önceki bölümlerde belirtildiği gibi 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” ile de İnternet sùjelerinin yükümlölükleri düzenlenmiştir.

2. SÖZLEŞME KAPSAMINDA ULUSAL DÜZEYDE ALINACAK ÖNLEMLER

Sözleşmede, ulusal düzeydeki yasal düzenlemelerin uyumlu hale getirilmesi ve siber suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku yetkilerinin sağlanması amacıyla yapılacak düzenlemeler, ulusal düzeyde alınacak önlemler başlığı altında iki bölümde düzenlenmiştir. Maddi ceza hukuku bölümünde Sözleşme kapsamında tarafların ulusal mevzuatlarına suç olarak düzenleyecekleri fiillerin maddi unsurları sıralanmıştır. Usul hukuku bölümünde ise bu suçların soruşturulması ve kovuşturulması için gereken yetkiler tanımlanmıştır.

a. Maddi Ceza Hukuku

(1) Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar

(a) Madde 2-Yasadışı Erişim

Sözleşmenin bu maddesinde, taraf ölkelerin kendi iç hukuklarında bir bilgisayar sistemine veya bu sistemin bir parçasına kasıtlı olarak ve haksız bir biçimde girilmesini suç haline getirmeleri öngörölmüştür. Taraf ölkelerin söz konusu suçu, bilgisayar verilerinin elde edilmesi veya sahtekârlığa yönelik başka bir amaçla, güvenlik önlemlerinin ihlal edilmesi şeklinde veya başka bir bilgisayar sistemine bağılı bir bilgisayar sistemini esas alarak tanımlayabilecekleri belirtilmiştir.⁴⁸⁴

Yetkisiz erişim fiili, yasal kullanıcıların sistemi veya verileri kullanmalarını engelleyebileceği gibi verilerin bozulmasına, değişmesine ya da sistemde bulunan özel bilgilere erişilmesine de sebep olabilir. Bu nedenle, suçun daha erken bir safhada iken engellemek veya suç işleme ihtimalini tamamen ortadan kaldırmak açısından, bir bilgisayar sistemine veya içerdiği verilere yönelecek tehlikenin ilk aşamasını oluşturan yasadışı erişimin suç olarak düzenlenmesi, sistemlere ve verilere ilave bir koruma sağlayabilecek niteliktedir.⁴⁸⁵

⁴⁸⁴ Siber Suçlar Sözleşmesi Madde 2.

⁴⁸⁵ Açıklayıcı rapor, paragraf 44.

Maddede bahsedilen "erişim" fiili bir bilgisayar sisteminin tamamına veya bir kısmına (donanım, bileşenler, saklanan verilere, dizinlere ve trafik ya da içerik bilgilerini ihtiva eden dosyalara) girilmesini ifade etmektedir. Bir dosyanın başka bir bilgisayar sistemine gönderilmesi ya da e-posta göndermek erişim kapsamında değerlendirilmemektedir. Erişim fiili iletişim yönteminden (uzaktan, kablosuz ya da yakından) bağımsız olarak, İnternet gibi açık veya intranet olarak tanımlanan kapalı kullanıcı guruplu özel bir ağdaki diğer bir bilgisayara girmek anlamındadır.⁴⁸⁶

Suçun oluşması için eylemin haksız bir şekilde gerçekleştirilmesi gerekmektedir. Hak sahibinin rızası varsa veya sistemin geliştirilmesi, eksik ve zayıf yönlerinin bulunarak giderilmesi amaçlanıyorsa suç oluşmamaktadır. Sözleşmeye göre taraflar, yalnızca erişim fiilini suç olarak tanımlayabilecekleri gibi suçun oluşması için sistemdeki verilerin elde edilmesini veya sahtekârlık amacıyla güvenlik önlemlerinin ihlal edilmesi niyetinin bulunmasını da şart koşabilmektedir. Ayrıca, suç yalnızca ağ üzerinden erişim ile değil; bir bilgisayarın başına bizzat oturulup izinsiz çalıştırılması suretiyle de gerçekleşebilmektedir.⁴⁸⁷

TCK'nın "Bilişim Sistemine Girme" başlıklı 243. maddesi Sözleşme'nin 2. maddesini karşılar niteliktedir.⁴⁸⁸ Maddenin ilk fıkrasında bilişim sistemine ya da bir parçasına yasa dışı olarak girme ve orada kalmaya devam etme fiili suç olarak tanımlanmıştır. 243. maddede de Sözleşmenin 2. maddesi ile paralel bir şekilde, suçun ilk aşamasının engellenmesi amaçlanmaktadır. "Maddede tanımlanan suç bir tehlike suçudur".⁴⁸⁹ Bu nedenle zararın ortaya çıkması hususu suçun oluşması için şart koşulmamakta ve zarar verme olasılığının oluşturduğu tehlike yeterli görülmektedir. Sözleşmeyle paralel bir şekilde "bilişim sisteminin ve içindeki verilerin zarar görme ve özel verilerin gizliliğinin ihlal edilme ihtimali cezalandırılmaktadır."⁴⁹⁰

Bilişim sistemine girme fiilinin işlenme yöntemi ile ilgili bir kısıtlama getirilmediği gibi sistemin ağa bağlı olması ya da bağımsız bir sistem olması veya fiilin taşıdığı amaç konusunda da herhangi bir bağlayıcılık bulunmamaktadır.⁴⁹¹ Sözleşme'ye paralel bir biçimde herhangi bir bilişim sistemi ya da bir parçasına yine herhangi bir şekilde girilmesi suçun oluşması için yeterli görülmektedir. Ancak,

⁴⁸⁶ Açıklayıcı rapor, paragraf 46.

⁴⁸⁷ Açıklayıcı Rapor, paragraf 47-50.

⁴⁸⁸ Kurt, **a.g.e.**, s. 147., Öngören, **a.g.e.**, s. 46.

⁴⁸⁹ Öngören, **a.g.e.**, s.46, Kurt, **a.g.e.**, s.152., Dülger, **a.g.e.**, s.218

⁴⁹⁰ Kurt, **a.g.e.**, s.153.

⁴⁹¹ Dülger, **a.g.e.**, s.218, Kurt, **a.g.e.**, s.151.

suçun seçimlik hareketli olup olmadığı konusunda farklı iki görüş bulunmaktadır. Birinci görüş, suçu seçimlik hareketli bir suç olarak görüp bilişim sistemine girilmesi veya sistemde kalmaya devam edilmesi eylemlerinden birisinin yapılmasıyla suçun gerçekleşeceğini belirtirken;⁴⁹² ikinci görüş, suçun maddi unsurunu bilişim sistemine girmek ve orada kalmaya devam etmek şeklinde kabul etmekte ve sadece bilişim sistemine girmenin suç teşkil etmeyeceğini, ancak teşebbüs sayılacağını savunmaktadır.⁴⁹³

Suçun oluşması için ayrıca failin verileri ele geçirmesi ya da sistemde bulunan bilgileri öğrenmesi şartının gerekmediği değerlendirilmektedir.⁴⁹⁴ Burada daha öncede belirtildiği gibi “açık ve mevcut” bir tehlike öngörülmektedir. Bu suçun daha sonra işlenecek suçlar için ilk adımı teşkil edebileceğini değerlendiren kanun koyucu, bu ilk aşamayı da suç olarak tanımlamayı uygun görmüştür. Gerçekten de kötü niyetli bir kullanıcı bilişim sistemine yetkisiz erişim sağlamış, ancak işe yarar bir şey bulamayarak sistemden geri çıkmış olabilir. Bu eylem hırsızlık amacıyla bir mülke girilmesi, ancak çalınacak bir mal bulunamayarak çıkılmasına benzetilebilir. Bu durumda zarar oluşmayacaktır, ancak ortada yasa dışı bir fiilin var olduğu da açıktır.

Diğer bir husus ise iç hukukta da suçun oluşumu için Sözleşme ile paralel bir şekilde kasıt unsurunun aranmasıdır. Failin eyleminin suç olduğunu bilip bilmemesi önemli değildir. Ancak, suçun oluşabilmesi için fail bilerek ve isteyerek bilişim sistemine girmeli ve orada kalmaya devam etmelidir.⁴⁹⁵ Bu nedenle söz konusu suçun taksirle işlenmesi mümkün değildir. İstemedi ya da yanlışlıkla bir bilişim sistemine girilmesi durumunda suç oluşmayacaktır. Yetkisiz erişim, bir bilgisayar sistemi ya da ağına sahibi ya da sorumlusunun izni olmadan gerçekleştirilen her türlü erişim olduğundan sadece ağ yoluyla değil aynı zamanda bir bilgisayar sisteminin açma düğmesinin izinsiz açılmasıyla da yetkisiz erişim gerçekleşmiş olacaktır.⁴⁹⁶ Bu nedenle, kanunda yöntemi ile ilgili bir kısıtlama getirilmediği için bilişim sistemine girme fiili, İnternet gibi bir bilgisayar ağı üzerinden başka bir bilişim

⁴⁹² Dülger, a.g.e., s.217.

⁴⁹³ Öngören, a.g.e., s.46., Kurt, a.y.

⁴⁹⁴ Kurt, a.g.e., s.151, Dülger, a.g.e., s.218.

⁴⁹⁵ Kurt, a.g.e., s.159, Dülger, a.g.e., s.221, Öngören, a.g.e., s.47.

⁴⁹⁶ Rohas Nagpal. “Tools and Techniques of Cyber Crime”, 2004, (Çevrimiçi), http://www.asianlaws.org/cyberlaw/library/cc/cc_tt.htm, 10 Aralık 2006.

sistemi vasıtasıyla uzaktan gerçekleştirilebileceği gibi bizzat sistemin fiziksel olarak başına oturularak açılması ve erişilmesi şeklinde de gerçekleştirilebilmektedir.⁴⁹⁷

Sözleşme bilgisayar korsanlarının yasadışı eylemlerini yetkisiz erişim adı altında tanımlayarak, bu eylemleri suç haline getirmektedir.⁴⁹⁸ Bilgisayar korsanları suçun ilk aşamasında çeşitli programlar kullanarak ağı taramakta, açık bir kapı barındıran bilgisayarları tespit etmekte ve daha sonra erişilen bilgisayarın barındırdığı fırsatlar dahilinde suça yönelik eyleme geçmektedirler.⁴⁹⁹ Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik tüm suçların ilk aşaması, bilgisayara yetkisiz erişimdir. Bu nedenle yetkisiz erişimin engellenmesi tüm suçların engellenmesinde kilit rol oynamaktadır. Ayrıca, bilgisayar suçlarının mutlaka ağ üzerinden işlenmesi gerekmemektedir. Fiziki güvenliğı alınmayan bir bilgisayarın başına oturup, açma düğmesinden açarak içindeki bilgileri silmek, verileri çalmak, değiştirmek, kopyalamak şeklinde suç işlemek mümkündür. Maddenin bu ihtimali de içermesinin, bilgi güvenliğinin fiziksel güvenlik bileşenini de kapsaması açısından yerinde olduğu değerlendirilmektedir. Yasadışı erişim fiili, TCK'da da, Sözleşme ile aynı şekilde ele alınmış ve suç haline getirilmiştir. Dolayısıyla, yasadışı erişim suçu bakımından TCK'nın Sözleşme ile uyumlu olduğu görülmektedir.

(b) Madde 3-Yasadışı Araya Girme

Sözleşme, tarafların kasıtlı ve haksız bir şekilde teknik araçlarla, kamuya açık olmayan bir verinin bir bilgisayar sisteminden diğerine veya bilgisayar sisteminin kendi içerisinde aktarımı esnasında araya girilmesini, iç hukuklarında suç olarak tanımlamalarını öngörmektedir. Bilgisayar siteminden yayılan elektromanyetik ışınının ele geçirilmesi de araya girme fiilini oluşturmaktadır. Taraflara söz konusu fiilin sahtekârlık amacıyla yapılması ya da başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilmeleri serbestliğı de tanınmaktadır.⁵⁰⁰

İlk bakışta araya girme suçunun Sözleşmenin ikinci maddesindeki yasadışı erişim suçu ile örtüştüğü düşünülebilir. Ancak, ikisi arasında korunan haklar bakımından fark bulunmaktadır. Yasadışı erişimde korunmak istenen bilişim sisteminin kendisi ve güvenliğıdır. Hak sahiplerinin sistemi etkin kullanım hakkının

⁴⁹⁷ Dülger, **a.g.e.**, s.217, Kurt, **a.g.e.**, s.156.

⁴⁹⁸ Çeken, **a.g.e.**, s.44.

⁴⁹⁹ "Hacking Techniques", High Tech Crime Brief, Australian Institute of Criminology, 2005, s.2.

⁵⁰⁰ Siber Suçlar Sözleşmesi Madde 3.

güvence altına alınması amaçlanmaktadır. Araya girme suçunda ise amaç bilişim sisteminden ziyade veri haberleşmesinin mahremiyetinin korunmasıdır.

Sözleşmenin bu maddesi AİHS'nin 8. maddesinde belirtilen kişilerin özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi ilkesinin telefon, faks, e-posta veya dosya iletimi şeklindeki bütün elektronik veri transferi biçimlerine uygulanmasıdır. Kişiler arasındaki sözlü telefon görüşmelerinin geleneksel yöntemlerle dinlenmesi ve kaydedilmesi ile gerçekleştirilen, iletişimin gizliliğinin ihlalini eylemini temsil etmektedir.⁵⁰¹

Madde metninde bulunan “teknik araçlar yoluyla araya girme” ifadesi, iletişimin içeriğinin bilgisayar sistemlerine erişim yoluyla doğrudan ya da elektronik dinleme cihazları yardımıyla dolaylı olarak elde edilmesi anlamındadır. İletim hatlarına yerleştirilen dinleme cihazlarının yanında, kablosuz iletişimi elde etmek için kullanılan cihazlar ya da yazılım, şifre ve kodların kullanımı da teknik cihazlar kapsamına girmektedir.⁵⁰²

Madde metninde belirtilen “kamuya açık olmayan iletişim” ifadesi ile iletilen verilerin niteliği değil, iletişimin niteliği tanımlanmaktadır. İletilen veriler kişisel olmayan, gizlilik taşımayan ve herkesin ulaşabileceği veriler dahi olsa, iletişimin tarafları bunları gizlice iletmeyi isteyebilmektedir. Dolayısıyla önemli olan iletişimin niteliğidir.⁵⁰³

Sözleşme kapsamında bilgisayar verilerinin iletimi, işlemciden ekrana ya da yazıcıya tek bir bilgisayar sisteminin içerisinde gerçekleşebileceği gibi, aynı kişiye ait iki bilgisayar sistemi arasında, birbiriyle iletişim halindeki iki bilgisayar sistemi arasında ya da örneğin klavyeden veri girişi şeklinde bir kişi ve bir bilgisayar sistemi arasında gerçekleşebilmektedir.⁵⁰⁴ Sözleşme bilgisayar sistemlerinden yayılan elektromanyetik dalgaları, birinci maddede belirtilen veri tanımı kapsamında değerlendirmemesine rağmen, verilerin bu dalgaların işlenmesi suretiyle yeniden oluşturulabilmesi nedeniyle, elektromanyetik dalgaların ele geçirilmesini bu madde kapsamında suç olarak tanımlamaktadır.⁵⁰⁵

⁵⁰¹ Açıklayıcı Rapor, paragraf 51.

⁵⁰² Açıklayıcı Rapor, paragraf 53.

⁵⁰³ Sokullu-Akıncı, a.g.e., s.17.

⁵⁰⁴ A.y.

⁵⁰⁵ Açıklayıcı Rapor, paragraf 57.

Cezai yükümlülüğün oluşabilmesi için araya girme eyleminin “kasıtlı olarak” ve “haksız biçimde” gerçekleştirilmesi gerekmektedir. Özellikle ulusal güvenlik ya da soruşturma mercilerinin suçları araştırma çalışmaları çerçevesinde yasal yetkiyle gerçekleştirilmesi durumunda eylem suç teşkil etmemektedir.⁵⁰⁶

Sözleşme bu madde ile daha önceki bölümde, bilgi güvenliğinin temel bileşenlerinden birisi olarak bahsedilen “İletişim Güvenliği”nin sağlanmasını amaçlamaktadır. İletişim güvenliğinin, iletişim mahremiyetinin korunması yanında, siber suçlarla mücadele açısından büyük önemi bulunmaktadır. Suç olarak tanımlanan bu fiil, kişisel bilgilerin, kredi kartı ya da banka hesap bilgilerinin veya sisteme yasadışı erişim olanağı sağlayan parola ve şifrelerin elde edilmesine yol açmaktadır. Bu suretle, özellikle dolandırıcılık ve sahtekârlık olmak üzere diğer siber suç türleri ve klasik suç türlerinin (şantaj, dolandırıcılık, sahtekârlık gibi) işlenmesine imkân sağlamaktadır. Sözleşmenin bu açıdan, siber suçlarla mücadeleye önemli bir katkı sağlayacağı ifade edilebilir. Ayrıca, elektromanyetik dinlemenin de suç haline getirilmesinin, Sözleşmenin etkinliğini artırdığı değerlendirilmektedir.

TCK’da ise bilişim alanında suçlar bölümünde yasadışı araya girme suçunu karşılayan ayrı bir bilişim suçu düzenlenmemiştir. Ancak, TCK’da şekli düzenleme korunan hak esasına göre olduğundan, Dokuzuncu Bölümde özel hayata ve hayatın gizli alanına karşı suçlar başlığı altında benzer düzenleme olduğu değerlendirilebilir.

TCK’nın 132. maddesindeki “Haberleşmenin Gizliliğinin İhlali”, 133. maddesindeki “Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması” ve 134. maddesindeki “Özel Hayatın Gizliliğinin İhlali” suçlarına yönelik düzenlemenin, İnternet ortamı ve diğer bilişim sistemleri de dahil olmak üzere her türlü yöntemle araya girmeyi suç haline getirdiği,⁵⁰⁷ dolayısıyla Sözleşmeyle uyumlu olduğu değerlendirilmektedir. Ancak, elektromanyetik dinleme fiili Sözleşmedeki kapsamıyla Türk hukukunda suç olarak açıkça düzenlenmemiştir. TCK’nın 133. maddesinde “kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen” ifadesi bulunmakla beraber, bu ifade ile kastedilen fiilin, Sözleşmede belirtilen elektromanyetik dinleme suçunun maddi unsurunu karşılamaktan oldukça uzak olduğu değerlendirilmektedir.

(c) Madde 4-Verilere Müdahale

⁵⁰⁶ Açıklayıcı Rapor, paragraf 55.

⁵⁰⁷ Öngören, a.g.e., s.58.

Verilere müdahale maddesinde Sözleşme, ilk fıkrada tarafların kendi iç hukuklarında bilgisayar verilerinin tahrip edilmesi, silinmesi, bozulması, değiştirilmesi ya da gizlenmesi fiillerini kasıtlı ve haksız bir şekilde gerçekleştirildiğinde suç olarak tanımlayacak yasal düzenlemeleri yapmalarını öngörmektedir. İkinci fıkrada ise taraflara söz konusu fiillerin suç sayılması için ciddi zarar oluşması şartını saklı tutma hakkı verilmektedir.⁵⁰⁸

Bu maddenin amacı, bilgisayar verilerinin ve programlarının da gerçek nesnelere benzer şekilde kasıtlı zarar verme eylemine karşı korunmasıdır. Korunan hukuki hak ise depolanan bilgisayar verilerinin ya da bilgisayar programlarının bütünlüğü, doğru çalışması veya amacına uygun kullanılabilmesidir.⁵⁰⁹

Açıklayıcı rapora göre birinci fıkrada belirtilen tahrip etme ve bozma fiilleri örtüşen fiillerdir ve içerik verilerinin ya da programların, olumsuz anlamda değiştirilmesine özgü eylemlerdir. Silme eylemi ise gerçek bir nesnenin yok edilmesi ile aynı anlamdadır. Kelime orijinal metinde “deletion” olarak kullanılmıştır ki bu da bilgisayar terminolojisinde ve programlama dilinde silmek anlamındaki “delete” komutuna karşılık gelmektedir. Sil komutu ile aslında veri değil; sadece veriyi içeren dosyanın diskteki adres bilgisi silinmektedir. Bu nedenle, eylemin gerçek bir nesneyi yok etmekle eşdeğer olduğu özellikle belirtilmektedir. Verinin gizlenmesi ise verinin depolandığı bilgisayar ya da veri taşıyıcıya erişimi engelleyen ya da imkânsız kılan her türlü eylemdir. Değiştirme terimi ise var olan verinin farklı hale getirilmesidir.⁵¹⁰

TCK’nın “Sistemi engelleme, bozma, verileri yok etme veya değiştirme” başlıklı 244. maddesinin 2. fıkrasının, Sözleşmenin 4. maddesine ile paralel olduğu değerlendirilmektedir.⁵¹¹ TCK’nın 244/2. maddesinde⁵¹² bir bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması veya sisteme

⁵⁰⁸ Siber Suçlar Sözleşmesi Madde 4.

⁵⁰⁹ Açıklayıcı Rapor, paragraf 60.

⁵¹⁰ Açıklayıcı Rapor, paragraf 61.

⁵¹¹ Yılmaz Yazıcıoğlu, “Bilişim Suçları”, **Bilişim Teknolojisi Hukuku Gündemi 2004-2005**, İstanbul, Bilgi Üniversitesi, 2006, s.73., Kurt, a.g.e., s.160., Dülger, a.g.e., s.230.

⁵¹² TCK Madde 244 “...(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

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

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

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

veri yerleştirilmesi ve var olan verilerin başka bir yere gönderilmesi filleri suç olarak tanımlanmıştır. Burada amaçlanan, Sözleşmeyle aynı kapsamda bilgisayar verileri ve programlarının da gerçek nesnelere benzer şekilde kasıtlı zarar verme eylemine karşı korunmasıdır. Suç teşkil edecek eylemlerin tamamının kapsanması amaçlanmıştır. Bu nedenle en alt düzeyde bulunan erişilmez kılma eyleminden, yok etmeye kadar, aradaki tüm eylemler maddeye dahil edilmiştir.⁵¹³

(d) Madde 5-Sistemlere Müdahale

Sözleşme, tarafların kendi iç hukuklarında bir bilgisayar sisteminin işleyişini, bilgisayar verileri yerleştirmek, göndermek, verilere zarar vermek, silmek, bozmak, değiştirmek ya da gizlenmek yoluyla ciddi olarak engellemek fiilini kasıtlı ve haksız bir şekilde işlendiğinde, suç olarak tanımlayacak yasal düzenlemeleri yapmalarını öngörmektedir.⁵¹⁴

Sözleşmenin bu maddesindeki suç daha önceki (89) 9 No.lu önerideki bilgisayar sabotajına karşılık gelmektedir. Maddenin amacı, bilgisayar verilerini kullanarak ya da onlara müdahale ederek telekomünikasyon olanakları da dahil bilgisayar sistemlerinin kullanımının engellenmesinin suç haline getirilmesidir. Korunan hukuki hak ise bilgisayar ve telekomünikasyon sistemlerinin uygun şekilde kullanılabilmesinin sağlanmasıdır.⁵¹⁵

Engelleme, bilgisayar sisteminin arzu edilen şekilde işlemesine veri yerleştirmek, veri göndermek, verilere zarar vermek, silmek, değiştirmek ya da verileri gizlemek yoluyla müdahalede bulunulması anlamındadır. Bununla birlikte, engelleme eyleminin suç teşkil edebilmesi için Sözleşme, yetkili kullanıcı ya da operatörün sistemi kullanmasını önemli ölçüde güçleştirecek kadar ciddi bir boyuta ulaşmış olmasını öngörmektedir. Bu konuda belirleyici olacak hususları kararlaştırmayı ise taraflara bırakmaktadır.⁵¹⁶

TCK'nın "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlıklı 244/1. maddesi ile Sözleşme'nin 4. maddesine bir paralellik sağlanmaya çalışıldığı görülmektedir.⁵¹⁷ Zira her ikisinde de korunan hukuki hakkın aynı olduğu değerlendirilmektedir. TCK'nın 244/1. maddesinde bir bilişim sisteminin işleyişinin

⁵¹³ Kurt, **a.g.e.**, s.161.

⁵¹⁴ Siber Suçlar Sözleşmesi Madde 5.

⁵¹⁵ Açıklayıcı Rapor, paragraf 65.

⁵¹⁶ Açıklayıcı Rapor, paragraf 66-67.

⁵¹⁷ Yazıcıoğlu, "Bilişim Suçları", s.73., Kurt, **a.g.e.**, s. 160., Dülger, **a.g.e.**, s.230., Öngören, **a.g.e.**, s.48.

engellenmesi veya bozulması suç olarak tanımlanmıştır. Suçun işlenme yöntemi ile ilgili herhangi bir kısıtlama bulunmamaktadır. Engelleme ve bozma filleri daha önceki bölümlerde belirtilen eylemlerden herhangi biri ile gerçekleştirilebilir. Sisteme virüs bulaştırılması vasıtasıyla sistem yavaşlatılabilir ya da işleyemez hale getirilebilir. Aynı şekilde yoğun e-posta bombardımanı nedeniyle işlem yükü artırılarak, sistemin kullanıcılara cevap veremeyecek hale gelmesi sağlanabilir.

Bilişim sisteminin bozulması ise tamamen çalışamaz hale gelmesi anlamındadır. Engelleme düzeltilebilir ya da giderilebilir bir durum iken, bozma fiilinde etki kalıcı olabilir. Bu kapsamda işletim sistemi çöktürülebilir, herhangi bir programın silinmesi, bozulması ya da kodlarının değiştirilmesi sonucu kendisinden beklenen belirli bir işlemi gerçekleştirememesi sağlanabilir.

Verilere müdahale ve sistemlere müdahale suçlarında belirtilen eylemler sayesinde Sözleşme'nin amacı ne olursa olsun bilişim sistemlerine ve bilişim sistemlerinde depolanan verilere karşı gerçekleştirilebilecek kötü maksatlı eylemlerin tümünü içermeye çalıştığı ve bu anlamda hâlihazırda işlenebilecek tüm suçların maddi unsurunu oluşturan filleri kapsadığı değerlendirilmektedir. Bu açıdan Sözleşme ile getirilen düzenlemenin suçla mücadelede etkili olacağı değerlendirilmektedir.

Sözleşmede siber terör konusuna değinilmemiş olmamasına rağmen, sistemlere müdahale eyleminin bilişim sistemleri ile kontrol edilen kritik altyapı tesislerine yapılması muhtemel eylemleri kapsadığı da ifade edilebilir. Dolayısıyla, Sözleşmenin sistemlere müdahaleyi suç haline getirmekle, doğrudan ifade edilmemekle birlikte siber terör eylemlerini kapsadığı da değerlendirilmektedir. TCK açısından bakıldığında ise verilere ve sistemlere müdahale ile ilgili düzenlemenin Sözleşme ile uyumlu olduğu ve Sözleşmede suç olarak tanımlanan tüm eylemlerin iç hukukta da suç haline getirilmiş olduğu görülmektedir.

(e) Madde 6-Cihazların Kötüye Kullanımı

Sözleşmenin cihazların kötüye kullanımı maddesinde tarafların, Sözleşmenin 2 ilâ 5. maddelerinde suç olarak düzenlenen eylemlerden herhangi birini gerçekleştirmek üzere tasarlanmış ya da dönüştürülmüş bir cihazın (bilgisayar programları dahil) ya da bir bilgisayar sisteminin bir parçasını veya tamamını erişilebilir kılacak parola, erişim kodu ve benzer verilerin üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı ya da başka surette elde edilebilir hale getirilmesini

suç haline getirecek gerekli yasal ve diğer düzenlemeleri yapmaları öngörülmektedir.⁵¹⁸

Sözleşme bu madde ile suça yönelik potansiyel tehlike yaratan eylemleri kaynağından yasaklamayı amaçlamaktadır. Bunun maksatla önceki maddelerde tanımlanan suçların işlenmesi amacıyla, belli cihazlar ya da erişim kodlarının yetkisiz ve kötü niyetle kullanılmasını suç haline getirmektedir. Siber suçların işlenmesi için standart olarak üretilen araç ve programlardan ziyade suç işlemek amacıyla üretilmiş ya da dönüştürülmüş araçlara ihtiyaç duyulmaktadır. Sözleşme bu talebe karşı oluşma eğiliminde olan karaborsayı ortadan kaldırarak suçu önlemeye çalışmaktadır.⁵¹⁹

Sözleşmeye göre “dağıtmak” verileri aktif bir şekilde başkalarına iletme, “kullanıma sunmak” ise online cihazları ağ üzerinden başkalarının kullanmasına imkân vermek anlamındadır. Bunun yanında hiper-bağlantılar (hyperlink) tanımlayarak, bu tür cihazlara erişim sağlanmasını da içermektedir. Bilgisayar programı ifadesi, verileri değiştirmek veya yok etmek için ya da bir sistemin işleyişine müdahale etmek için tasarlanmış veya dönüştürülmüş yazılımlardır.⁵²⁰ Madde böylece, virüs, Truva atı, ağ solucanları gibi daha önce bahsedilen kötü maksatlı yazılımların üretimini, dağıtımını ve kullanımını da suç haline getirmektedir.

Sözleşmeye göre suçun oluşabilmesi için bu araçların bulundurulması yeterli değildir. Suç işleme amacıyla kullanıma niyetinin olmasını da şart koşulmaktadır. Genel satışa sunulan ve suça karşılık vermek amacıyla kullanılabilecek cihazlar aynı zamanda suç işlemek amacıyla da kullanılabilmektedir. Sözleşme maddenin insanların bu tip araçlardan istifade etme haklarına engel teşkil edecek şekilde yorumlanmasından endişesi nedeniyle bu şartı getirmektedir.⁵²¹

Siber suçların artması ile birlikte kamusal ve özel kurumların kullandıkları sistemlerin ve bilgisayar ağlarının güvenliğinden emin olmaları ve bunu test etmeleri önem kazanmıştır. Yoğun teknoloji kullanan büyük şirketler, kendi güvenliklerini saldırganların teknik ve araçlarını taklit ederek test etmekte ve zayıf taraflarını gidermeye çalışmaktadır. Müşteriler ise hem İnternet üzerinden alışveriş esnasında sağlanan güvenliği, hem de ürünün güvenli olmasını, yeni ürün tercihlerinde

⁵¹⁸ Siber Suçlar Sözleşmesi Madde 6.

⁵¹⁹ Açıklayıcı Rapor, paragraf 71.

⁵²⁰ Açıklayıcı Rapor, paragraf 72.

⁵²¹ Açıklayıcı Rapor, paragraf 76.

aramaya başlamıştır.⁵²² Bu nedenle, suç işlemek için kullanılabilecek cihazların güvenliğin test edilebilmesi için iyi niyetle kullanılması bir zorunluluk haline gelmiştir. Sözleşmeye göre bu durumda suç işleme kastının bulunmaması ve eylemin haksız bir şekilde gerçekleştirilmemiş olmasından dolayı suç oluşmamaktadır.⁵²³

TCK'da ise bu konu önemli bir eksiklik olarak ortaya çıkmaktadır. Söz konusu şekilde cihaz üretimi veya yazılım üretimi, bulundurulması, satışı vb. fiiller hâlihazırda suç haline getirilmemiştir. Dolayısıyla Sözleşme bu anlamda suç araçlarını yasaklamak suretiyle suçu önlemeyi amaçlamaktadır ki bunun TCK'da yer bulmasının önemli olduğu değerlendirilmektedir.⁵²⁴

(2) Bilgisayarlarla İlişkili Suçlar

(a) Madde-7 Bilgisayarla İlişkili Sahtecilik

Sözleşme bu maddede, kasıtlı ve haksız biçimde yapılması durumunda hukuki açıdan orijinalmiş gibi değerlendirilmesi amacıyla, bilgisayar verilerine doğrudan okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, yeni veriler ilave etme, değiştirme, silme veya erişilemez kılma yoluyla orijinal verilerden farklı veriler meydana getirme fiilinin, suç olarak tanımlanmasını öngörmektedir.⁵²⁵

Maddenin amacı somut belgelerde yapılan sahtecilik fiiline paralel bir suçun, elektronik ortamdaki belgeler için de oluşturulmasıdır. Ceza hukukunun geleneksel sahtecilik eylemleri için öngördüğü belgedeki beyanların ve ifadelerin görsel olarak okunabilir olması gerekliliği bilgisayar verilerine uygulanamamaktadır. Maddede geçen “doğrudan okunabilir ve anlaşılabilir nitelikte olmasına bakılmaksızın” ifadesi ile bu açığın giderilmesi amaçlanmaktadır. Bilgisayarla ilişkili sahtecilikte verilerin izinsiz olarak değiştirilmesi ya da yeni veriler yaratılması doğrudan orijinal verilerin hukuki anlamda delil özelliğinin değiştirilmesi ile ilgilidir ve aldatmaya yöneliktir. Dolayısıyla, hukuki işlemlere konu olduğunda somut bir belge üzerinde yapılan sahtecilik eylemi ile aynı sonuçları doğurabilmektedir. Burada korunan hukuki yarar,

⁵²² “Effective Measures to Prevent and Control Computer-Related Crime: Report of The Secretary-General”, s.2, United Nations Economic and Social Council, 29 January 2002, (Çevrimiçi), <http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf>, 26 Mart 2007.

⁵²³ Açıklayıcı Rapor, paragraf 77.

⁵²⁴ Karagülmez, **Bilişim Suçları ve Soruşturma...**, s.309.

⁵²⁵ Siber Suçlar Sözleşmesi Madde 7.

hukuki işlemler açısından geçerliliği olan ve sonuç doğurabilecek elektronik verilerin güvenliğinin ve güvenilirliğinin korunmasıdır.⁵²⁶

Sözleşme açısından bu madde kapsamında bulunan veriler, hukuki işlemlerde kullanılabilen ve hukuki etkiler doğurabilen her türlü özel ya da resmi belgelerin eşdeğeridir. İzinsiz olarak doğru ya da yanlış verilerin ilave edilmesi sahte bir belgenin üretilmesi, verilerin değiştirilmesi, silinmesi ve erişilmez kılınması ise hakiki bir belgenin tahrif edilmesi ile aynı anlamı taşımaktadır.⁵²⁷

Sözleşmenin bu maddesinde suç olarak düzenlenen fiillerin, 4. maddedeki verilere müdahale suçu ile aynı olduğu görülmektedir. Ancak, bu maddede manevi unsur “hukuki açıdan orijinalmiş gibi değerlendirilmesi amacı”dır. Fail eğer bu amaç dışında farklı bir amaçla hareket ederse, bu durumda bilgisayarla ilişkili sahtecilik suçu yerine, 4. maddede belirtilen verilere müdahale suçu oluşmaktadır.

TCK’da Bilişim Alanında Suçlar başlığı altında doğrudan bilgisayarla ilişkili sahtecilik suçu tanımlanmamıştır. 244. maddenin 2. fıkrasında sistemdeki verileri bozma, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiilleri suç haline getirilmiştir. Görüldüğü üzere ifade edilen fiillerin tamamı, Sözleşmenin bilgisayarla ilişkili sahtecilik maddesi ile suç haline getirdiği fiillerdir. Ancak, TCK’da sahtecilik suçunun oluşması için manevi unsur ayrıca tanımlanmadığından, bu fiiller hukuki açıdan orijinalmiş gibi değerlendirilmesi amacı ile gerçekleştirilse bile bilgisayarla ilgili sahtecilik suçu değil; 244. maddede belirtilen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu oluşmaktadır. Bu suç için altı aydan üç yıla kadar hapis cezası öngörülmekte iken; TCK’nın somut belge ve mühürde sahtecilik ile ilgili maddelerinde ceza aralığı iki yıldan sekiz yıla kadar değişmektedir.⁵²⁸ Bu nedenle TCK’nın bilgisayarla ilişkili sahtecilik suçu açısından yetersiz kaldığı ve Sözleşme ile uyumlu olmadığı değerlendirilmektedir.

(b) Madde–8 Bilgisayarla İlişkili Dolandırıcılık

Sözleşme bu maddede tarafların, dolandırıcılık yoluyla kendine veya bir başkasına maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veri ekleme, değiştirme, silme ya da erişilmez kılma veya bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme fiilleriyle, bir başkasının

⁵²⁶ Açıklayıcı Rapor, paragraf 81., Sokullu-Akıncı, a.g.e., s.26.

⁵²⁷ Açıklayıcı Rapor paragraf 83, Sokullu-Akıncı, a.y.

⁵²⁸ Ayrıntılı Bilgi İçin Bkz. TCK Madde 202, 204 ve 205.

mülkiyetinin kaybına sebebiyet verme eyleminin, kasıtlı ve haksız yere yapılmasını suç olarak tanımlamalarını öngörmektedir.⁵²⁹

Teknolojinin getirileri sayesinde sanal bankacılık işlemlerinden, elektronik fon transferine, elektronik tahvillere ve kredi kartlarına, birçok soyut mal varlığı elektronik ortamda yönetilebilir olmuştur. Ancak, bu varlıklar zamanla geleneksel mülkiyet biçimlerinde olduğu gibi manipülasyon hedefi haline gelerek, ekonomik suçların işlenmesi için yeni fırsatlar yaratmıştır. Bu suçlar başlıca, bilgisayarlara yanlış verilerin girilmesi ile oluşan veri manipülasyonları, program manipülasyonları ve veri işleme sürecinde yapılan diğer müdahalelerdir. Dolayısıyla, Sözleşme bu madde ile mal varlığını yasa dışı biçimde nakletmek amacıyla, veri işleme sürecine yapılan kanunsuz manipülasyonları suç olarak düzenlemektedir.⁵³⁰

Sözleşme bilgisayarlarla ilgili dolandırıcılık suçunun işlenmesinde manipülasyon yapmak için gerçekleştirilebilecek tüm eylemleri kapsam dahiline alabilmeyi amaçlamış ve bu nedenle yerleştirme, silme, erişilmez kılma eylemlerine bilgisayar sisteminin ya da programının işleyişine müdahale etmeyi de eklemiştir. Burada açıklanan eylemler bir önceki maddedeki ile aynı anlamda kullanılmıştır. Sisteme ya da programa müdahale eylemi donanım manipülasyonunu, yazıcı çıktılarının erişilmez kılınmasını, veri kaydetme ya da veri akışına etkilemeyi veya programların komut işleme sürecinin değiştirilmesini kapsamaktadır.⁵³¹

Bilgisayarla ilişkili dolandırıcılık eylemleri birçok kategoriye içermektedir. Bunlar asılsız mali projeler veya ekonomik mal varlıklarına yönelik yalan ya da yanlış yönlendirme amaçlı teklifler olabilir. Bunun yanında kredi kartı dolandırıcılığı, elektronik posta dolandırıcılığı ya da banka dolandırıcılığı sayılabilir. Kısaca amaç dürüst olamayan yollarla ekonomik kazanç sağlamaktır. İnternet'te en tipik dolandırıcılık şekli borsa dolandırıcılığı ya da online bankacılık işlemleri esnasında yapılan dolandırıcılıktır. Şirketler ve bireyler, İnternet'i düşük fiyatlı az rağbet gören borsa kâğıtlarının değerini suni olarak yükseltmek için kullanabilmektedir. İstenmeyen postalar, elektronik gazeteler, mesaj panoları ve İnternet siteleri dolandırıcılık aracı olarak kullanılabilir.⁵³²

⁵²⁹ Siber Suçlar Sözleşmesi Madde 8.

⁵³⁰ Açıklayıcı Rapor, paragraf 86.

⁵³¹ Açıklayıcı Rapor, paragraf 87.

⁵³² Schjolberg, Hubbard, a.y.

Suçun oluşabilmesi için bir şahsın kendisine veya bir başkasına kazanç sağlamak niyetiyle hareket etmesi ve bu hareketi neticesinde bir başkasının malvarlığının kaybına sebep olması gerekmektedir. Bunun dışında yasalara uygun yaygın ticari eylemler, rekabet sayılabilecek faaliyetler hile ya da başka dürüst olmayan yollara başvurulmadığı için suç olarak değerlendirilmemektedir.⁵³³

TCK'da bilgisayarla ilişkili dolandırıcılık suçu, bilişim alanında suçlar başlığı altında doğrudan tanımlanmamıştır. Ancak, 244. maddenin 4. fıkrasında aynı maddenin 1. fıkrasında suç haline getirilen sistemini engelleme veya bozma fiili ve 2. fıkrasında suç haline getirilen verileri bozma, değiştirme, erişilmez kılma, veri yerleştirme, verileri başka bir yere gönderme fiillerinin, işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, hapis ve para cezası ile cezalandırılması öngörülmüştür. Dolayısıyla, doğrudan bir suç düzenlenmemiş olmasına karşın, Sözleşmenin bu maddesindeki paralel düzenlemenin mevcut olduğu görülmektedir.⁵³⁴

Bunun yanında TCK'nın Nitelikli Hırsızlık başlıklı 142. maddesinde hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi⁵³⁵ ve benzer şekilde TCK'nın Nitelikli Dolandırıcılık başlıklı 158. maddesinde dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi⁵³⁶ ağırlaştırıcı neden olarak düzenlenmiştir.

Son olarak ise TCK'nın Bilişim Alanında Suçlar bölümünde yer alan Banka ve Kredi Kartlarının Kötüye Kullanılması başlıklı 245. Maddesinde, başkasına ait banka veya kredi kartının her ne suretle olursa olsun ele geçirilmesi ve kullanılması, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka ve kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi, sahte üretilen veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanılması eylemleri suç olarak düzenlenmiştir.⁵³⁷

Dolayısıyla, Sözleşme'de bulunan bilgisayarlarla ilişkili sahtecilik suçunun TCK'da düzenlenmediği, dolandırıcılık suçunun ise ayrıntılı olarak düzenlendiği ifade edilebilir.

⁵³³ Açıklayıcı Rapor, paragraf 88-90.

⁵³⁴ Yazıcıoğlu, "Bilişim Suçları", s.73.

⁵³⁵ Bkz.: TCK Madde 142. paragraf 2/e.

⁵³⁶ Bkz.: TCK Madde 158. paragraf 1/f.

⁵³⁷ Bkz.: TCK Madde 245.

(3) İçerikle İlgili Suçlar

(a) Madde-9 Çocuk Pornografisine İlişkin Suçlar

Sözleşme içerikle ilişkili suç olarak, yalnızca neredeyse tüm üyelerin üzerinde anlaşabildiği çocuk pornografisini kabul etmiştir.⁵³⁸ Buna ilaveten Sözleşme taslağını hazırlayan komitede, ırkçı propagandanın bilgisayar sistemleri yoluyla dağıtımı gibi başka suçların da dahil edilmesi üzerine tartışılmıştır. Bu konunun da bir suç olarak Sözleşmeye dahil edilmesi yönünde güçlü bir destek olmasına rağmen, temsilcilerin bir kısmı böyle bir hükmün dahil edilmesi konusunda ifade özgürlüğü açısından kaygılı olduklarını belirtmişlerdir. Konunun karmaşıklığı göz önüne alınarak, Bilgisayar Sistemleri Aracılığıyla Irkçı ve Yabancı Düşmanlığı İçeren Eylemler Hakkında Ek bir protokol düzenlenmiştir.⁵³⁹

İnternet nispeten daha az risk taşıması, erişimi kolaylaştırması, tespit edilme, soruşturulma ve yakalanmayı güçleştirmesi nedeniyle, çocuk pornografisi içeren materyallerin dağıtılmasını kolaylaştırmaktadır. Bu nedenle, çocuk pornografisine yönelik talebin ve çocuklara yönelik istismarın artmasına katkıda bulunmaktadır. Ayrıca, İnternet kullanımı sayesinde çocuk pornografisine eğilimli insanlar kimliklerini açıklamadan çocuklarla temas kurabilmekte ve bazı durumlarda bu temas taciz, kaçırma veya tecavüz olaylarına dahi yol açmaktadır.⁵⁴⁰

Sözleşme bu maddesinde tarafların, bilgisayar sistemleri üzerinden dağıtmak amacıyla çocuk pornografisinin üretilmesi, bir bilgisayar sistemi üzerinden sunulması veya erişilebilir kılınması, dağıtılması ya da yayılması, bilgisayar sistemi üzerinden temin edilmesi, bir bilgisayar sistemi ya da veri depolama aygıtında bulundurulması eylemlerini, kasıtlı ve haksız bir biçimde gerçekleştirildiğinde iç hukukta suç olarak tanımlamalarını öngörmektedir.⁵⁴¹ Buna ilaveten çocuk pornografisi teriminin neyi ifade ettiği terimler bölümünde bulunmamasına rağmen, madde başlığı altında detaylı olarak açıklamıştır. Sözleşmeye göre çocuk pornografisi;

- Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı,

⁵³⁸ Gyula Zombori, "e + Finance + Crime a Report On Cyber-Crime and Money Laundering", 15 January 2001, (Çevrimiçi), http://www.yorku.ca/nathanson/Publications/e.htm#_Toc504182577, 09 Mart 2007.

⁵³⁹ Açıklayıcı Rapor, paragraf 35.

⁵⁴⁰ "Effective Measures to Prevent and Control Computer-Related Crime Report of The Secretary-General", s.6.

⁵⁴¹ Siber Suçlar Sözleşmesi Madde 9.

- Cinsel anlamda müstehcen bir eyleme reşit görünümünde olmayan bir kişinin katılımı,
- Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren görüntülerdir.

Sözleşme reşit olmayan kişi terimi ile 18 yaşından küçük olanları kastetmekle birlikte, taraflara 16 veya 17 yaşı sınır olarak belirleyebilme imkânı vermektedir. Ancak belirlenen sınır kesinlikle 16 yaşından daha küçük olamamaktadır.⁵⁴²

Sözleşme çocuk pornografisi ile mücadeleyi üretimden bulundurmaya kadar, tüm süreci kapsayacak şekilde suç saymayı amaçlamıştır. Çocuk pornografisi için oluşan talep ve arz karşılıklı olarak birbirini tetiklemektedir. Bu da İnternet'in sağladığı kolay erişim ve azalan yakalanma riskinden kaynaklanmaktadır. Sözleşme İnternet ortamında suçla mücadele etmek için hem talebi ve arzı hem de bunların tüm alt süreçlerini suç haline getirmiştir. Ancak sanatsal, tıbbi, bilimsel ya da benzer bir değeri olan malzemeler pornografik olmayan malzemeler kapsam dışında tutulmuştur.

Maddede suç olarak tanımlanan eylemler, İnternet siteleri oluşturmak, online bağlantılar kurmak veya hiper-bağlantılar aracılığıyla gerçekleştirilebileceği gibi, bu malzemeler bir bilgisayar sisteminde ya da CD-ROM, DVD, taşınabilir disk gibi veri depolama araçlarında bulundurulabilir.⁵⁴³

Sözleşme çocuk pornografisinin ne tür malzemeleri içerdiğine de açıklama getirmiştir. Buna göre, maddede belirtilen suçlara konu olan malzeme gerçek bir çocuğun, reşit olsa dahi reşit görünmeyen ve çocuk izlenimi veren bir kişinin ya da gerçekte bir çocuğu içermese de gerçekçi görünen ve bir çocuğun, cinsel olarak kötü muameleye uğramasının teşhirini, müstehcen bir eyleme katılımını gösteren pornografik görüntüleri kapsamaktadır. Bilgisayar yazılımları ve grafik programları sayesinde artık gerçekte çocuk kullanmadan da tamamen bilgisayar ortamında bu tür görüntü ve resimlerin yaratılması mümkündür. Dolayısıyla, Sözleşme tüm bu ihtimalleri kapsayabilmek amacıyla, çocuk kullanılmasını şart koşmamıştır. Bu nedenle bilgisayarda ya da elde üretilmiş animasyonlar, gerçek insanların görüntülerinin bilgisayar aracılığıyla çocuk izlenimi verecek şekilde değiştirilmesi ya

⁵⁴² A.y.

⁵⁴³ Açıklayıcı Rapor, paragraf 94-99.

da ne yöntemle olursa olsun kişide müstehcen eyleme maruz kalanın çocuk olduğu izlenimi yaratan tüm görüntüler dahil edilmiştir.⁵⁴⁴

Sözleşmenin gerçek çocuk içermeyen görüntüleri de suç kapsamına dahil etmesinin amacı, bir çocuğa gerçekten zarar verilmese bile, bu tür görüntülerin çocukları bu tür fiillere teşvik edebilme ya da istismar edilmelerine sebep olabilme ihtimalidir. Sözleşme bu tür görüntüleri suç kapsamına alarak, çocuklara kötü muameleye izin veren bir alt kültürün oluşmasını önlemeyi amaçlamaktadır. Bununla birlikte taraflara, temin ve bulundurma eylemlerinin suç sayılması ve çocuk görünümlü, ancak reşit kişilerin bulunduğu görüntülerin veya animasyonların suç unsuru sayılması konusunda hak saklı tutma imkânı verilmektedir.⁵⁴⁵

TCK'da ise Bilişim Alanında Suçlar bölümünde çocuk pornografisine yönelik bir düzenleme bulunmamaktadır. Bununla birlikte, TCK'nın Müstehcenlik başlıklı 226. maddesinde hem çocuklara müstehcen görüntü yazı vb. ürünlerin verilmesi, izletilmesi veya okunması gibi fiiller, hem de çocuk pornografisi üretimi, ülkeye sokulması, çoğaltılması, satılması, nakledilmesi, depolanması, ihracı, bulundurulması ve başkalarının kullanımına sunulması fiilleri suç olarak düzenlenmiştir.⁵⁴⁶

TCK'nın 226. maddesi, her türlü müstehcen içeriğin basın ve yayın yolu ile yayınlanmasını veya yayınlanmasına aracılık edilmesini suç haline getirmiştir. Ancak ülkemizde İnternet'in basın ve yayın organı olarak değerlendirilebileceğine dair açık bir düzenleme olmaması bu konuda bir boşluk yaratmaktadır. Uygulamada ise gerek ulusal gerekse uluslararası düzeyde İnternet üzerinden çocuk pornografisi ile mücadele edilmekte ve uluslararası işbirliğine gidilmektedir. Çocuk pornografisi bulundurulması eyleminde ise bilgisayar sistemleri ve diğer veri depolama

⁵⁴⁴ Açıklayıcı Rapor, paragraf 101.

⁵⁴⁵ Açıklayıcı Rapor, paragraf 102-106.

⁵⁴⁶ TCK 226. Madde "(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(4) Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(5) Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

aygıtlarında bu tür malzemenin bulundurulması 226. madde kapsamında suç oluşturan eylemi teşkil etmektedir.

226. maddede çocuk deyiminden ne anlaşılması gerektiği ayrıca belirtilmemiştir. TCK'nın tanımlar başlıklı 6. maddesinde "çocuk deyiminden; henüz on sekiz yaşını doldurmamış kişi" anlaşılır ifadesi yer almaktadır. Dolayısıyla 226. maddede aksi belirtilmediğinden çocuk ifadesinden on sekiz yaşını doldurmamış kişi anlaşılmalıdır. TCK'nın 226. maddesi 7. paragrafında madde hükümlerinin bilimsel eserlere uygulanamayacağı açıkça belirtilmiştir. Ancak sanatsal ve edebi değer gerekçesi ile dahi olsa çocuk pornografisine müsaade edilmemiştir.

TCK'da mevcut düzenleme ile genel anlamda çocuk pornografisinin engellenmesinin amaçlandığı açıkça anlaşılmaktadır. TCK'nın bilişim suçları ile ilgili 10. bölümünde çocuk pornografisine ilişkin bir suç bulunmamaktadır. Ayrıca, 226. madde çerçevesinde "bilişim sistemlerinin" kullanılması konusu ağırlaştırıcı bir neden olarak da düzenlenmemiştir. Bununla birlikte 5651 sayılı Kanun'un 8. maddesi kapsamında Telekomünikasyon İletişim Başkanlığı, yurt içi ve dışından yayın yapan ve TCK'da belirtilen "Çocukların Cinsel İstismarı (TCK 103/1)" ve "Müstehcenlik (TCK 226)" suçlarını oluşturduğu hususunda yeterli şüphe bulunan İnternet yayınlarının engellenmesine hakim, mahkeme ya da Cumhuriyet savcısı kararı olmadan re'sen karar verebilmektedir. Ayrıca, yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulması da düzenlenmiştir. Ancak, ne tür malzemelerin çocuk pornografisi olarak kabul edileceği veya çocuk içermeyen, ancak bu izlenimi veren gerçek ya da animasyon görüntülerin suç kapsamında olup olmadığı gibi konular ne TCK'da ne de 5651 sayılı Kanun'da açıkça belirtilmemiştir. Dolayısıyla, ulusal mevzuatta çocuk pornografisinin önlenmesine yönelik mevcut düzenlemenin Sözleşme ile karşılaştırıldığında yetersiz olduğu değerlendirilmektedir.

(b) Ek Protokol: Bilgisayar Sistemleri Aracılığıyla İrkçılık ve Yabancı Düşmanlığı

Daha öncede belirtildiği gibi ırkçı ve yabancı düşmanlığı içeren eylemlerin bilgisayar sistemleri aracılığıyla gerçekleştirilmesi hususunun, Sözleşmenin içerikle ilişkili suçlar bölümüne dahil edilmesi konusunda bir uzlaşmanın sağlanamaması nedeniyle, bu konuda Sözleşmeden ayrı ek bir protokol hazırlanarak 28 Ocak 2003

tarihinde imzaya açılmış ve 1 Mart 2006 tarihinde yürürlüğe girmiştir. Türkiye Siber Suçlar Sözleşmesinde olduğu gibi ek protokolü de henüz imzalamamıştır.⁵⁴⁷

İnternet'in sınır tanımayan niteliği, düşünce ve fikirlerin serbestçe yayılmasına imkân sağlamakla birlikte, bu imkân her zaman iyi amaçlarla kullanılmamaktadır. İnternet aynı zamanda ırkçı ve yabancı düşmanlığı içeren düşüncelerin desteklenmesi ve yayılması için etkili ve modern bir araç olarak da kullanılmaktadır. Protokol, İnternet'i bu maksatla kullanan kişileri yakalamak ve soruşturmak için uluslararası işbirliğinin kaçınılmaz olduğundan hareketle, suçlarda karşılıklı yardımlaşmayı en geniş, esnek ve modern bir tarzda mümkün kılmayı amaçlamaktadır. Protokolün amacı iki aşamalıdır. Birincisi İnternet ortamında ırkçılık ve yabancı düşmanlığına karşı mücadeleyi sağlayacak şekilde var olan ceza hukukunu uyumlu hale getirmek, ikincisi ise bu alanda uluslararası işbirliğini sağlamaktır. Böylece, iade, karşılıklı yardımlaşma veya çifte suçluluk gerekliliği gibi uluslararası işbirliğine yönelik faaliyetlerin kolaylaştırılması amaçlanmaktadır.⁵⁴⁸

Protokol suçun oluşabilmesi için Sözleşmeye paralel bir şekilde haksız bir şekilde yapılmasını öngörmektedir. Böylece, eylem her zaman cezalandırılabilir olmaktan çıkmaktadır. Suç oluşturan eylem, rıza, nefsi müdafaa, zaruret hali gibi klasik nedenlerle veya kanunun uygulanması, akademik ya da araştırma çalışmaları nedeniyle yasal ya da haklı görülebilmektedir. Buna ilaveten, suçun oluşabilmesi için eylem kasıtlı olmalıdır. Ancak, kasıt terimi ile neyin ifade edildiğinin kesinleştirilmesi taraflara bırakılmıştır. Örneğin içeriği kontrol etmek gibi bir sorumluluğu olmayan servis sağlayıcının bu öğeleri içeren bir İnternet sitesine erişim sağlaması veya ortam sağlaması kastın olduğu şeklinde yorumlanmamaktadır.⁵⁴⁹ Protokolde suç teşkil eden eylemler, dört ana başlık altında suç haline getirilmiştir.

I. Irkçı ve Yabancı Düşmanlığı İçeren Malzemelerin Bilgisayar Sistemleri Aracılığıyla Yayılması

Bu madde tarafların ırkçı ve yabancı düşmanlığı içeren malzemelerin bilgisayar sistemleri aracılığıyla aleni olarak yayılması veya elde edilebilir kılınması

⁵⁴⁷ Ayrıntılı Bilgi İçin Bkz.: Avrupa Konseyi Siber Suçlar Sözleşmesi'ne Ek Protokol, "Additional Protocol to the Convention on Cybercrime, Concerning The Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems ETS No.: 189", <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.

⁵⁴⁸ Ek Protokol Açıklayıcı Rapor, paragraf 3.

⁵⁴⁹ Ek Protokol Açıklayıcı Rapor, paragraf 24-25.

eylemlerini, haksız ve kasıtlı bir şekilde yapılması halinde kendi ulusal mevzuatlarında suç haline getirmelerini öngörmektedir.⁵⁵⁰

Maddede ifade edilen yaymak eylemi suç unsuru içeriğin başkalarına gönderilmesi anlamına gelmekte iken, elde edilebilir kılınması bu tür malzemenin bir İnternet sitesine yerleştirilmesi vb. şeklinde diğerlerinin online erişimine sunulmasıdır. Bu ifade aynı zamanda hiper-bağlantıların yaratılması veya derlenmesi yoluyla erişimin kolaylaştırılmasını da içermektedir.⁵⁵¹ Yayma eyleminde aktif bir hareket varlığından, elde edilebilir kılmada ise daha çok pasif bir eylemden söz edilebilir.

Maddede aleni bir tarzda ifadesinin kullanılması, kişiler arasındaki özel iletişim ya da ifadelerin kapsam dışında olduğunu açıkça ortaya koymaktadır. Bu tür iletişimin Avrupa İnsan Hakları ve Temel Özgürlükleri Sözleşmesinin 8. maddesi⁵⁵² kapsamında korunması hassasiyeti gerektirdiğinden, iletişimin özel ya da aleni olduğuna olayın tabi olduğu şartlara göre karar verilmesi gerekmektedir. Bu durumda, öncelikle gönderenin mesajı sadece önceden karar verdiği bir alıcıya gönderme niyetinin var olup olmadığının değerlendirilmesi gerekmektedir.⁵⁵³

Bunun dışında İnternet'in yaygın kullanım şekillerinden olan sohbet odaları, haber gurupları ya da tartışma gurupları gibi uygulamalar da ırkçı ve yabancı düşmanlığı içeren malzemelerin aleni şekilde yayılmasına imkân sağlamaktadır. Bu hallerde, malzeme herkesin erişebileceği nitelikte olarak değerlendirilmektedir. Hatta bu uygulamalarda erişim için şifre ya da yetkilendirme gerekse bile, bu şifrenin ya da yetkinin uygun kriterleri sağlayan herhangi birine verilmesi mümkün olduğundan aleni olarak yayma şeklinde değerlendirilmektedir.⁵⁵⁴

Protokol çok kısıtlı durumlarda olmak üzere hak saklı tutuma imkânı tanımaktadır. Hak saklı tutmak için öncelikle eyleme konu malzemenin nefret ve şiddet içermemesi sadece savunma, destekleme ya da teşvik içermesi gerekmektedir. Bu durumda etkili idarî ya da medenî yaptırımlar mevcut ise cezai sorumluluk öngörülmemektedir. Sadece, iç hukukta ifade özgürlüğü ile ilgili yasal

⁵⁵⁰ Ek Protokol Madde 3.

⁵⁵¹ Protokol Açıklayıcı Rapor, paragraf 28.

⁵⁵² Ayrıntılı Bilgi İçin Bkz.: Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Sözleşmesi Madde 8.
<http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

⁵⁵³ Ek Protokol Açıklayıcı Rapor, paragraf 29-30.

⁵⁵⁴ Ek Protokol Açıklayıcı Rapor, paragraf 31.

düzenlemeler nedeniyle, bu tip çözümler sağlayamayan taraf devletlere maddeyi tamamen uygulamama hakkı verilmektedir.⁵⁵⁵

II. Irkçı ve Yabancı Düşmanlığı Motivasyonlu Tehdit

Protokol, tarafların kasıtlı ve haksız şekilde yapıldığında, kişilerin ya da toplulukların, bir guruba ait olma, ırk, renk, soy, milli veya etnik köken, dini inanç, gibi özellikleri bahane edilerek, bilgisayar sistemleri aracılığıyla kendilerine yönelik ciddi bir suçun gerçekleştirileceği yönünde tehdit edilmelerini suç olarak düzenlemelerini öngörmektedir.⁵⁵⁶

Burada bahse konu tehdit, ciddi cezai bir suçun işleneceği yönünde olmalı ve yöneltildiği kişide korku yaratmalıdır. Bu tehdit kişisel güvenliğe yönelik olabileceği gibi mala zarar verme ya da akrabalara yönelik olabilir. Protokol, ciddi cezai suçların neler olduğunu taraflara bırakmıştır. Tehdidin aleni yapılması gibi bir husustan söz edilmemesi maddenin özel iletişimi de kapsadığını göstermektedir.⁵⁵⁷

III. Irkçı ve Yabancı Düşmanlığı Motivasyonlu Aşağılama

Bu madde de bir önceki ile paralel biçimde, aşağılama eyleminin taraflarca suç olarak düzenlenmesini öngörmektedir. Bahse konu aşağılama eylemi, bir şahsın şeref ve onurunu kıran saldırgan, küçümseyici ya da hakaret içeren davranışları ifade etmektedir. Tehdit suçunda olduğu gibi aşağılama fiili de maruz kalan kişinin bir guruba ait olmasıyla doğrudan ilgili olmalıdır, ancak özel iletişim aracılığıyla gerçekleştirilen aşağılamalar bu madde kapsamında değildir.⁵⁵⁸ Taraflar eylemin suç teşkil etmesi için kişi ya da gurubun aşağılamaya maruz kalma olasılığı yanında, bunun gerçekleşmesini de şart koşabilmektedir. Ayrıca, taraflara maddenin bir bölümü ya da tamamı için hak saklı tutma imkânı da verilmektedir.⁵⁵⁹

IV. Soykırım ya da İnsanlığa Karşı Suçların İnkârı, Önemsizleştirilmesi, Onaylanması veya Haklı Görülmesi

Protokolü hazırlayanlar İnternet'in bu amaçla kolaylıkla kullanılabilmesinden hareketle, soykırım ya da insanlığa karşı işlenen suçların bilgisayar sistemleri

⁵⁵⁵ Ek Protokol Madde 3, paragraf 3.

⁵⁵⁶ Ek Protokol Madde 4.

⁵⁵⁷ Ek Protokol Açıklayıcı Rapor, paragraf 34-35.

⁵⁵⁸ Ek Protokol Açıklayıcı Rapor, paragraf 36.

⁵⁵⁹ Ek Protokol Açıklayıcı Rapor, paragraf. 37-38.

aracılığıyla inkâr edilmesi, önemsizleştirilmesi, onaylanması veya haklı görülmesi eylemlerinin suç olarak düzenlenmesine karar vermiştir. Ancak, bu konudaki en önemli sorun, soykırım ve insanlık suçlarının belirlenmesidir. Protokol bu hususta çeşitli öneriler getirmektedir. Örneğin, Nuremberg Mahkemesi, Nazi yönetiminin 2. Dünya Savaşı sırasında Yahudilere karşı işlediği suçlar için soykırım kararı vermiştir. Bu karar bağlayıcı bir niteliktedir. Bunun yanında Eski Yugoslavya Yönetimine ve Ruanda'ya karşı kurulan Uluslararası Ceza Mahkemeleri ya da Kalıcı Uluslararası Ceza Mahkemesi kararlarının da bu kapsamda sayılabileceği belirtilmektedir. Protokol bu madde ile imza atan tarafların, yargı yetkisini tanıdıkları sürece, gelecekte teşkil edilebilecek mahkemelerin son ve bağlayıcı kararlarına başvurabilmelerine de izin vermektedir.⁵⁶⁰

Taraflar suçun oluşmasını ırk, renk, milliyet, etnik, köken vb. bahane edilerek kişi ya da bir topluluğa karşı kin ve nefreti, ayrımcılığı ya da şiddeti kışkırtmak amacıyla işlenmesi gibi başka şartlara bağlayabilmektedirler. Ayrıca, taraflar bu maddeyi kısmen ya da tamamen uygulamama hakkına da sahiptir.⁵⁶¹

Protokol kapsamında suç olarak düzenlenen fiiller, TCK'da ikinci kitap, üçüncü kısım, beşinci bölümde, Kamu Barışına Karşı Suçlar başlığı altında düzenlenmiş olmakla birlikte; bilişim sistemleri ile işlenmeleri hususuna yönelik bir ifade kullanılmamıştır. Bu suçlar; suç işlemeye tahrik (Madde 214), suçu ve suçluyu övme (Madde 215) , halkı kin ve düşmanlığa tahrik ve aşağılama (Madde 216) suçlarıdır. Protokol'ün suç olarak düzenlenmesini öngördüğü eylemler, yıkıcı ve bölücü faaliyetler ile İnternet ortamında mücadele etmek açısından önemli bir imkân sağlayabilir. Söz konusu sitelere Türkiye'den erişimi engellemek mümkün olmakla birlikte, sitelerin yayın yapmaya devam etmesi nedeniyle bir çözüm olmamakta ve bazı durumlarda bilgi edinme hakkı ve haberleşme özgürlüğüne ihlal teşkil etmektedir.⁵⁶² Bu nedenle, yıkıcı ve bölücü örgütlerin yurt dışından yayın yapan İnternet siteleri ile mücadelede, Türkiye'nin Protokole taraf olmasının fayda sağlayacağı değerlendirilmektedir.

Türkiye açısından ayrıca, Protokolün son maddesinin büyük önem taşıdığı değerlendirilmektedir. Türkiye'nin güncel sorunlarından bir tanesi de uluslararası

⁵⁶⁰ Protokol Açıklayıcı Rapor, paragraf. 40.

⁵⁶¹ Protokol Açıklayıcı Rapor, paragraf. 43.

⁵⁶² İstanbul 1. Sulh Ceza Mahkemesi'nin 2007/384 sayılı ve 06.03.2007 tarihli kararı gereği <http://www.youtube.com> sitesine erişim engellenmiştir. Sitenin adresini yazan kullanıcılar, "Bu siteye erişim engellenmiştir. !..." ifadesi ile karşılaşmıştır. Ancak kullanıcılar sitede bulunan ve suç teşkil etmeyen diğer içerikten de mahrum bırakılmış bilgi edinme hakkı ve haberleşme özgürlükleri kısıtlanmıştır.

alandaki sıklıkla ortaya atılan ve çeşitli konularda Türkiye'nin önüne bir engel olarak konulan sözde Ermeni soykırımı iddialarıdır. Birinci Dünya Savaşı sırasında Rusya, İngiltere, Almanya ve Fransa gibi batı devletleri tarafından kışkırtılan Ermenilerin bağımsız bir Ermenistan kurma çabaları, özellikle Van, Kars, Erzurum olmak üzere diğer Osmanlı vilayetlerinde de pek çok Türk'ün katledilmesine neden olmuştur.⁵⁶³ Osmanlı Devleti buna karşılık savaş sahasına yakın vilayetlerden başlayarak Ermeni vatandaşlarını tehciye tabi tutmuştur.⁵⁶⁴ Tehcir kararı, Dâhiliye Nazırı Talat Paşa'nın tezkere teklifi üzerine 30 Mayıs 1915 tarihinde Meclis-i Vükela'da kabul edilerek Dâhiliye, Harbiye ve Maliye Nezaretlerine uygulamaya yönelik bir yazının gönderilmesi ile resmen uygulanmaya başlanmıştır.⁵⁶⁵

Günümüzde hem Türk hem de Ermeni vatandaşların korunması amacıyla alınan tehcir kararı sonucunda yaşanan olaylar sözde Ermeni soykırımı, Ermeni komitelerinin kapatılıp yöneticilerinin tutuklandığı 24 Nisan 1915 tarihi⁵⁶⁶ ise sözde Ermeni soykırımının yıldönümü olarak dünya kamuoyuna kabul ettirilmeye çalışılmaktadır. İddiaların asıl amacı, Ermenilerin tanıtma, tanınma, tazminat ve toprak talebi ile sonlanacak "Dört T" planının gerçekleştirilmesidir.⁵⁶⁷ Devam etmekte olan Sözde Ermeni soykırımı iddialarına uluslararası kabul sağlama girişimleri ise planın ikinci safhasının uygulanmakta olduğunu göstermektedir.⁵⁶⁸

Hâlihazırda on beş ülke parlamentosu tarafından sözde Ermeni soykırımını tanıyan kararlar alınmıştır. Bu ülkelerin on ikisi ise Avrupa Konseyi üyesi ülkelerdir. Türkiye'nin uzun yıllardır karşı karşıya olduğu ve mücadele ettiği sözde Ermeni soykırımı iddiaları, Fransa ve İsviçre gibi ülkelerde kabul edilmiştir.⁵⁶⁹ Bu ülkelerde sözde soykırımın reddi, kabul edilmemesi cezai bir suç sayılmaktadır. Hâlihazırda bu ülkelerde bulundukları esnada bu suçu işleyen Türk vatandaşları, ulusal mahkemelerde yargılanarak cezalandırılabilir. ⁵⁷⁰

⁵⁶³ Yusuf Halaçoğlu, **Ermeni Tehciri**, 9.bs., İstanbul, Babıali Kültür, 2006. s.112.

⁵⁶⁴ **A.e.**, s.113.

⁵⁶⁵ **A.e.**, s.70.

⁵⁶⁶ Servet Avşar, "Ermeni Sorunu ve Türkiye", **Manas Üniversitesi Sosyal Bilimler Dergisi**, 2001, Yıl 1, No.1, s.70.

⁵⁶⁷ Zafer Özkan, **Tarihsel Akış İçerisinde Terörden Politikaya Ermeni Meselesi**, İstanbul. 2001., s.218. akt: Avşar, **a.g.e.**, s. 85.

⁵⁶⁸ Avşar, **a.g.e.**, s.85.

⁵⁶⁹ Özgür Yalçın, "Hangi Yüzle", (Çevrimiçi), <http://www.gazeteodtulu.com/yazilar.php?id=114>, 16 Mart 2007.

⁵⁷⁰ "İsviçre Perinçek'i mahkûm etti", 10 Mart 2007, Radikal, (Çevrimiçi), <http://www.radikal.com.tr/haber.php?haberno=215172>, 01 Nisan 2007.

Soykırım konusunda 1948 tarihli Birleşmiş Milletler Soykırımın Önlenmesi ve Cezalandırılması Sözleşmesi 1951 tarihinden itibaren uygulamaya girdiği ve hukuken geriye dönük uygulanabilirliği olmadığı için 1915 yılındaki bu olaylara uygulanabilmesi mümkün değildir.⁵⁷¹ Sözleşmenin 5. maddesine göre, soykırım suçunun işlenip işlenmediğine sadece yetkili mahkeme karar verebilmektedir. Bu mahkeme, soykırımın cereyan ettiği ülkenin mahkemesi, bu iddiaların yöneltildiği ülkenin mahkemesi veya bu amaçla kurulan bir uluslararası mahkeme olabilmektedir. Bir başka madde olan 9. madde'ye göre, taraflar herhangi bir olayla ilgili Lahey Adalet Divanı'nın görüşüne başvurabilirler.⁵⁷² Adalet Divanı'nın iki rolü bulunmaktadır. Birincisi ülkelerin Divan'a getirdikleri yasal ihtilafları uluslararası yasalara uygun olarak çözümlemek, ikincisi ise uluslararası organlar ve kurumların hukuksal konulardaki soruları ile ilgili tavsiye niteliğinde fikir vermektir.⁵⁷³ Dolayısıyla, Divan'ın kararları ülkeler açısından bağlayıcıdır. Hâlihazırda ne Türkiye, ne de Ermenistan konuyu Adalet Divanı'na taşımamıştır.

Türkiye'nin Protokol'ün bu maddesini kabul etmesi halinde, doğrudan sözde Ermeni soykırımının kabulü gibi bir anlam taşımayacağı ve Protokolün tarafların ancak yargı yetkisini tanıdıkları sürece uluslararası bir mahkemenin kararı ile bağlı olabileceklerini kabul ettiği açıktır. Ancak protokolün bu maddesinin kabulü ile Türkiye kaynaklı bir İnternet sitesinde sözde Ermeni soykırımı iddialarını inkâr eden bir açıklamanın ya da ifadenin, sözde soykırımı kabul eden bir ülkeden erişilebilir olması o ülke yasalarına göre suç oluşmasına neden olacaktır. Bu durum Türkiye'nin de bu maddeyi kabul etmiş olmasından dolayı "çifte suçluluk" şartı veya "yargıla ya da iade et"⁵⁷⁴ prensibi öne sürülerek, ulusal mevzuatta suç sayılmayan bir eylemden dolayı, Türk vatandaşlarının yargılanmasının talep edilmesine yol açabilecektir. Bu konunun bir benzeri, Alman ceza hukuku sisteminin, "potansiyel suç etkisi" doktrinini kullanarak, Kanada yasalarına uygun davranan, ancak Almanya'dan erişilebilen ve anti-Nazi kanununu ihlal eden servis operatörleri ve

⁵⁷¹ Yürürlüğe giriş tarihi ve imzalayan ülkeler için Bkz.: "http://untreaty.un.org/sample/EnglishInternetBible/partI/chapterIV/treaty1.htm".

⁵⁷² Sözleşme 9. Madde "Sözleşmeciler Devletler arasında, bu Sözleşmenin yorumlanması, uygulanması veya yerine getirilmesi ve ayrıca soykırım fiillerinden veya Üçüncü maddede belirtilen fiillerin her hangi birinden bir Devletin sorumluluğu ile ilgili olarak çıkan uyuşmazlıklar, uyuşmazlığın taraflarından birinin talebi üzerine Uluslararası Adalet Divanı önüne götürülür."

⁵⁷³ Adalet Divanı'nın kuruluş ve görevleri hakkında ayrıntılı bilgi için Bkz.: "http://www.icj-cij.org/icjwww/igeneralinformation/inotice.pdf".

⁵⁷⁴ "Yargıla ya da iade et" yani "aut dedere aut judicare" Latince bir hukuk özdeyişidir ve genellikle uluslararası hukukçular tarafından Evrensel Yetki ilkesinin bir alt kategorisi olarak kabul edilir. Bir ülkenin başka bir ülkeye karşı suç işlediği iddi edilen ve kendi sınırlarında bulunan bir faili, ilgili ülkeye iade etmesi veya kendisinin yargılaması anlamına gelmektedir.

içerik sunucuları üzerinde Almanya'nın yargı yetkisi olduğunu iddia etmesi olayında yaşanmaktadır.⁵⁷⁵

Bunun ötesinde Avrupa Konseyi ülkelerinin artan şekilde sözde Ermeni soykırımını kabul eden yasaları meclislerinde kabul etmeleri halinde, gelecekte Protokol'ün bu maddesinde geçen soykırım kapsamına sözde Ermeni soykırımının da dahil edilmesi talepleri ortaya çıkabilir. Bu durum, Türkiye'nin "de facto"⁵⁷⁶ şekilde soykırımı kabulüne yol açabilir. Bu kötümser tablo oluşmasa dahi Türkiye'nin bu konuda uluslararası baskılara maruz kalacağı ve İnternet ortamında işlenen suçlar nedeniyle büyük sıkıntılar yaşayabileceği değerlendirilmektedir. Sonuç olarak, Protokol imzalanırsa dahi hak saklı tutuma imkânı kullanılmalıdır.

(4) Telif haklarının ve benzer hakların ihlaline ilişkin suçlar (Madde 10)

Sözleşme bu maddede tarafların, kendi yasalarında tanımlandığı şekliyle telif haklarının ihlalini, Bern Sözleşmesi çerçevesindeki 24 Temmuz 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Telif Hakları Anlaşması uyarınca ve yine telif haklarına benzer hakların ihlalini, Oyuncuların, Fonogram Yapımcılarının ve Yayın Kuruluşlarının Korunması Hakkında Sözleşme (Roma Sözleşmesi), Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Oyunculuk ve Fonogramlar Anlaşması uyarınca, isteyerek, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla yapıldığında, ulusal mevzuatlarında cezaî bir suç olarak tanımlamalarını öngörmektedir.⁵⁷⁷

Gelişen teknoloji sayesinde fikir ve sanat eserlerinin çok hızlı bir şekilde ve büyük miktarlarda çoğaltılabilmesi, bunların korunmasını zorunlu kılmaktadır. Bilgisayar teknolojisinin yaygınlaşması geçmişte nispeten kısıtlı olan kopyalama imkânını artırmış, İnternet ise bu kopyaların yayımlanmasını inanılmaz derecede kolaylaştırmıştır. Dolayısıyla, telif haklarının İnternet ortamında korunması bir

⁵⁷⁵ Sieber, a.g.e., s.132.

⁵⁷⁶ De facto "gerçekte" ya da "uygulamada" anlamında kullanılan bir Latince deyiştir. "Kanuna göre" anlamında gelen de jure ile karşıt olarak sıkça kullanılır. Yasal bir durumu tartışırken de jure konu hakkında kanunların ne söylediğini, de facto ise gerçek hayatta uygulamanın nasıl olduğunu belirtir. (Bu uygulama yasal olabilir ya da olmayabilir.) De facto terimi ayrıca geçerli bir kanun ya da standartın olmadığı fakat genelleşmiş bir uygulamanın söz konusu olduğu durumu belirtmek için kullanılır. Ayrıntılı Bilgi İçin Bkz.: http://tr.wikipedia.org/wiki/De_facto.

⁵⁷⁷ Siber Suçlar Sözleşmesi Madde 10.

gereklilik halini almıştır.⁵⁷⁸ Sözleşme, bu madde ile telif haklarına yönelik ihlallerin bilgisayar sistemleri aracılığıyla işlenmesi fiilini suç haline getirmektedir.

Türk Hukukunda Yine Bilişim Alanında Suçlar bölümünde telif haklarına ilişkin bir düzenleme mevcut değildir. Ancak bu husus, 05.12.1951 tarih ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) ve bu kanunda değişiklik yapan 03.03.2003 tarih ve 5101 sayılı Kanun ile düzenlenmektedir.

Sözleşmede öngörülen düzenleme, FSEK ve değişiklikte ayrıntılı olarak ifade edilmiştir. 5101 sayılı Kanun'un 18. maddesi ile değişen 5846 sayılı Kanunun 72. maddesinde,⁵⁷⁹ bir eserin herhangi bir şekilde sahibinin izni olmadan işlenmesini, çoğaltılmasını ve yayılmasını suç olarak düzenlemiştir. Yine 5101 sayılı Kanun'un 25. maddesi ile 5846 sayılı Kanunun ek 4. maddesinde yapılan değişiklikle İSS'lerin yükümlülükleri de tespit edilmiştir.⁵⁸⁰

Türkiye aynı zamanda bu madde kapsamında atıfta bulunulan diğer uluslararası Sözleşmelere de taraftır. Türkiye, 1995 yılında, "4117 sayılı Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi'nin Kabulüne Dair Kanun" ile

⁵⁷⁸ Tamer Soysal, "İnternet Servis Sağlayıcıların Hukuki Sorumlulukları", **Türkiye Barolar Birliği Dergisi**, Yıl. 18, No.61, Kasım-Aralık 2005, s.331.

⁵⁷⁹ 5101 sayılı Kanun'un 18. maddesi ile değişen 5846 sayılı Kanunun 72. maddesi "1. Aralarında mevcut bir sözleşme olmasına rağmen bu sözleşme hükümlerine aykırı olarak bir eser veya işlenmelerinin kendi tarafından çoğaltılmış nüshalarını satan veya dağıtan kişiler hakkında, üç aydan iki yıla kadar hapis veya onmilyar liradan ellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden,

2. Hak sahibinin izni olmaksızın bir eseri ve çoğaltılmış nüshalarını, bu Kanunun 81 inci maddesinin yedinci fıkrasında sayılan yerlerde satan kişiler hakkında üç aydan iki yıla kadar hapis veya beşmilyar liradan ellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden,

3. Hak sahibinin izni olmaksızın;

a) Bir eseri herhangi bir şekilde işleyen,

b) Bir eseri herhangi bir şekilde çoğaltan,

c) Bir eseri herhangi bir şekilde yayan,

d) Bir eserin nüshalarını yasal veya yasal olmayan yollardan ülkeye sokan ve her ne şekilde olursa olsun ticaret konusu yapan,

e) Bir eseri topluma açık yerlerde gösteren veya temsil eden, bu gösterimi düzenleyen veya dijital iletim de dahil olmak üzere her nevi işaret, ses ve/veya görüntü iletimine yarayan araçlarla yayan veya yayımına aracılık eden, Kişiler hakkında iki yıldan dört yıla kadar hapis veya ellimilyar liradan yüzellimilyar liraya kadar ağır para cezasına veya zararın ağırlığı dikkate alınarak her ikisine birden hükümlenir."

⁵⁸⁰ 5101 sayılı Kanun'un 25. maddesi, "Dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlali halinde, hak sahiplerinin başvuruları üzerine ihlale konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlalin durdurulmasını ister. İhlalin devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlale devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir. İhlalin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır."

Bern Sözleşmesi'nin 1971'de Paris'te revize edilmiş metninin 1979 Paris Değişikliğini, 4116 sayılı kanun ile de Roma Sözleşmesi'ni kabul etmiştir. 26 Mart 1995 tarihinden beri Dünya Ticaret Örgütü(DTÖ)'nün üyesidir. TRIPS'i (Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Dünya Ticaret Örgütü Sözleşmesi'ni) 1995 yılında kabul etmiştir.⁵⁸¹ Türkiye ayrıca 12 Ocak 1976 tarihinden beri WIPO Sözleşmesine taraftır ve WIPO'nun üyesidir.⁵⁸²

b. Usul Hukuku

(1) Genel Hükümler

Siber Suçlar Sözleşmesi 14. maddesinde usul hukuku ile ilgili maddelerinin uygulanabileceği suçların kapsamını belirlemiştir. Buna göre ileriki bölümlerde daha detaylı açıklanacak olan 16 ilâ 21 maddeler arasında belirtilen düzenlemeler;

- Sözleşmenin 2–11. maddeleri arasında tanımlanan suçlar (bu suçlar, taraflar Sözleşmeyi kabul ettikleri için her bir tarafın ulusal düzenlemelerinde de suç sayılacaktır.),

- Bilgisayar sistemleri aracılığıyla işlenen diğer suçlar ve
- Elektronik ortamda delilleri olan klasik cezaî suçlar için geçerli olacaktır.⁵⁸³

Siber suçların işlenmesinde bilgisayar sistemleri ve İnternet'in sağladığı hız, faillerin tespit edilmesinde kolluk güçlerine büyük zorluklar yaratmaktadır. Buna ilaveten suça ait delillerin ve faile ait ipuçlarının elektronik ortamda bulunması, bunların çok kısa sürede değiştirilmelerine veya yok edilmelerine imkân sağlamaktadır. Bu nedenle, arama ve el koyma şeklindeki klasik usul hukuku önlemleri, siber suçlar söz konusu olduğunda delillerin özgün niteliğinin korunamaması veya kaybolması gibi sakıncalar doğurmaktadır. Sözleşme bu sakıncalardan yola çıkarak, usul hukukuna ait önlemleri bu bölümde siber suçlara ve elektronik ortamdaki delillere uygulanacak şekilde yeniden tanımlamaktadır.⁵⁸⁴

⁵⁸¹ T.C. Kültür ve Turizm Bakanlığı İnternet Sitesi, "http://www.kultur.gov.tr/TR/BelgeGoster.aspx?F6E10F8892433CFFFE5C29E16A7D38089C4DBFB16DD6A546". Sözleşme metinleri için ayrıca Bkz.: "http://www.wipo.int/portal/index.html.en".

⁵⁸² WIPO İnternet Sitesi, Ayrıca Türkiye'nin WIPO çatısı altında taraf olduğu tüm Sözleşmeler, Sözleşme metinleri ve üyelik bilgileri için Bkz.: "http://www.wipo.int/portal/index.html.en"

⁵⁸³ Siber Suçlar Sözleşmesi Madde 14.

⁵⁸⁴ Serap Keskin, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", İÜHFİM, C.LIX, No.1-2, 2001, s. 156.

Siber suçlarda mağdurun suç işlendikten nispeten uzun bir süre sonra suçtan haberdar olması ve suç türünün anlaşılmasının zaman gerektirmesi, öncelikle delil niteliğinde olabilecek verilerin hızla özgün haliyle korunmasını gerekli kılmaktadır. Suçun tam olarak anlaşılmasından sonra ise delil niteliğinde olabilecek korunan verilerin incelenmesi gerekmektedir. Sözleşme bu amaçla, öncelikle hızlı bir koruma rejimi daha sonrada korunan verilerin aranması ve el konulması için gerekli yetkileri tesis etmeyi amaçlamaktadır.⁵⁸⁵

Sözleşme, düzenlenen bu önlemlerin temel hak ve özgürlüklerin ihlal edilmesine yol açacak şekilde genel olarak suçlu avına çıkar tarzda uygulanmasına imkân vermemek için, usul hukukuna ait maddelerin yalnızca somut bir suça ve faile yönelik soruşturma ve kovuşturma dahilinde uygulanabilmesini öngörmektedir.⁵⁸⁶

(2) Madde 16-Depolanmış Bilgisayar Verilerinin Korunmasının Kolaylaştırılması

Sözleşme bu maddede tarafların, bir bilgisayar verisinin yok edilmesi veya değiştirilmesi hususunda makul şüphenin bulunması halinde, yetkili makamlarının bir bilgisayar sistemi tarafından depolanan ve trafik bilgilerini de içeren bilgisayar verisinin korunmasını süratle temin edecek talimatları vermesini veya söz konusu hususu buna benzer bir şekilde temin etmelerini sağlayacak yasal düzenlemeleri yapmalarını öngörmektedir. Tarafların bu hususun kişilere de uygulanmasını düzenlemeleri halinde, kişinin depolanan bilgisayar verisini, en fazla doksan gün olmak üzere, yetkili mercilerin içeriğinin açıklanmasını talep etmesine imkân verecek süre ile korumasını zorunlu kılacak yasal düzenlemeyi yapmalarını öngörmektedir. Taraflardan her biri koruma işlemini yapacak yetkilinin ya da şahsın, bu kararı ulusal yasalarda belirtilen süre boyunca gizli tutmasını sağlayacak yasal ve diğer düzenlemeleri de yapacaktır.⁵⁸⁷

Sözleşmenin 16. ve 17. maddelerinin, bilgisayar ağları üzerinden işlenen suçların kovuşturulmasında başarı elde etmek için çok yenilikçi ve önemli bir yetkiyi tanımladığı düşünülmektedir.⁵⁸⁸ Sözleşme bu şekilde, belirli bir suça yönelik soruşturmada, tarafların yetkili mercilerine soruşturma ile ilgili olabilecek depolanmış bilgisayar verilerinin süratle korunmasını sağlayacak yetkiyi vermeyi

⁵⁸⁵ A.y.

⁵⁸⁶ Açıklayıcı Rapor, paragraf 140, Keskin, a.g.e., s.157.

⁵⁸⁷ Siber Suçlar Sözleşmesi Madde 16.

⁵⁸⁸ Cangemi, a.g.e., s.168.

amaçlamaktadır.⁵⁸⁹ Depolanmış bilgisayar verilerinin hızlı biçimde korunması önlemi, gelecekte bu bilgisayar verileri üzerinde yapılacak arama ve el koyma önlemlerini gerçekleştirebilmek için alınmış bir koruma tedbiridir. Bu sayede korunan verilerin, değiştirilmeden, bozulmadan ve silinmeden muhafaza edilmesi ve gelecekte delil elde edilmek üzere özgün niteliğinin korunması amaçlanmaktadır.⁵⁹⁰

Sözleşmenin 16. ve 17. maddelerinde sözü edilen depolanmış bilgi, şimdiki zamanda yapılan ve halen iletilmekte olanlar değil; İSS'ler tarafından daha önceden toplanmış bilgilerdir.⁵⁹¹ Bu nedenle, bilgisayar verilerinin depolanması ve bilgisayar verilerinin korunması farklı anlamlar taşımaktadır. Koruma, zaten depolanmış biçimde var olan bilgisayar verilerinin mevcut halinin değişmesine ya da bozulmasına neden olacak her türlü eylemden uzak tutulmasıdır. Bununla birlikte, verilerin dondurulması, kendisinin ya da kopyalarının yasal kullanıcılar tarafından kullanılmasının engellenmesi anlamına gelmemektedir.⁵⁹²

Depolanan bilgisayar verilerinin korunmasının kolaylaştırılması taraflara rutin bir şekilde belli verileri toplamayan ve depolamayan servisleri kısıtlama zorunluluğu getirmemektedir. Aynı şekilde tarafların uluslararası işbirliği çerçevesinde istenmesi makul olmayan çok kısa ömürlü verilerin kaydedilmesini sağlayacak yeni teknik imkânlar tesis etmeleri de gerekmemektedir.⁵⁹³ Asıl amaç, bir suçla ilgili delil içermesi muhtemel verinin süratli biçimde korunması ve böylece işlenen bir siber suça ya da klasik bir suça ait bilgisayar ortamında bulunması muhtemel delillerin karartılmasını önlemektir.⁵⁹⁴

Maddede geçen "talimat vermek ya da buna benzer bir şekilde temin" ifadesi ile korumanın yalnızca adli ya da idari yollarla (kolluk güçleri ve savcı) değil; diğer yasal yollarla da yapılmasına imkân tanınması amaçlanmaktadır. Bazı ülkelerde koruma talimatı usul hukuku içerisinde yer almamakta ve veriler yalnızca arama ve el koyma ya da üretim talimatıyla korunabilmektedir. Bu ifade ile söz konusu ülkelere maddeyi bu şekilde uygulamaya sokma esnekliği sağlanmaya çalışılmaktadır. Yine de taraflara bilgisayar verilerinin hızlı bir şekilde korunmasını sağlayacak yetki ve

⁵⁸⁹ Açıklayıcı Rapor, paragraf 158.

⁵⁹⁰ Keskin, a.g.e., s.161.

⁵⁹¹ A.e., s. 162.

⁵⁹² Açıklayıcı Rapor, paragraf 159.

⁵⁹³ Açıklayıcı Rapor, paragraf 153.

⁵⁹⁴ Keskin, a.g.e., s. 164.

işlemleri tesis etmeleri önerilmektedir.⁵⁹⁵ Ülkemizde de düzenleme bu şekildedir ve usul hukukunda kişilere, İSS'lere veya benzeri veri depolayıcılara depolanmış bilgisayar verilerinin korunması talimatı verilmesini sağlayacak yasal düzenleme mevcut değildir. Ancak, ileriki bölümlerde daha detaylı açıklanacak olan CMK 134. madde ve Adli ve Önleme Aramaları Yönetmeliği 17. maddede düzenlenen el koyma ve yedekleme işlemlerinin, bilgisayar verilerinin korunması şeklinde yorumlanabileceği değerlendirilmektedir.

Sözleşme koruma talimatının İSS'ler veya benzeri veri depolayıcılarına da verilebilmesini içermektedir. Bu kapsamda, bir İSS'ye abonesi ya da kullanıcısı olan şüphelinin sisteminde muhafaza ettiği bilgisayar kütüklerini koruması talimatı verilebilmektedir. Yine CMK'nın 134. maddesinde bulunmamasına rağmen, Adli ve Önleme Aramaları Yönetmeliği 17. maddesinde yedekleme işleminin bilgisayar ağları ve diğer uzak bilgisayar kütükleri hakkında da uygulanabileceğinin⁵⁹⁶ belirtilmesi, bu şekilde değerlendirilebilir. Ancak, bilgisayar ağlarını ya da uzak bilgisayarda depolanan verileri kapsayan bir yedekleme işleminden önce süratli bir koruma talimatı büyük önem taşımaktadır. Aksi takdirde ağa bağlı uzak bir bilgisayarda bulunan ve bir suçla ilgili delil içermesi muhtemel veri yok edilerek delilin karartılabilir. Bir sonraki maddede daha detaylı bir şekilde açıklanacağı gibi ülkemizde 5651 sayılı Kanun ve ilgili yönetmeliklerle İSS'lere sadece kullanıcıların trafik bilgilerini belli bir süre ile depolama zorunluluğu getirilmektedir. Bunun dışında yer ve içerik sağlayıcılara, şüphelinin sisteminde muhafaza ettiği bilgisayar verilerini koruması talimatı verilmesi düzenlenmemiştir.

Sözleşme ile karşılaştırıldığında iç hukukta mevcut düzenlemenin korumadan ziyade sadece trafik bilgilerinin belli bir süre ile depolanmasına yönelik olduğu görülmektedir. Koruma ise arama ve el koyma ile gerçekleştirilmektedir. Siber suçlar söz konusu olduğunda savcının istemi ve hakim kararı için geçecek sürenin nispeten çok uzun olması ve bu süre içerisinde şahıslara, servis ve yer sağlayıcılara koruma talimatı verilememesi nedeniyle iç hukuktaki düzenlemenin yeterli olmadığı değerlendirilmektedir.

⁵⁹⁵ Açıklayıcı Rapor, paragraf 160.

⁵⁹⁶ Adli ve Önleme Aramaları Yönetmeliği Madde 17 "...Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında , sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır..."

(3) Madde 17-Trafik Bilgilerinin Korunmasının ve Kısmen Açıklanmasının Kolaylaştırılması

Trafik bilgilerinin korunmasının ve kısmen açıklanmasının kolaylaştırılması maddesinde sözleşme tarafların, korunan trafik bilgileri ile ilgili olarak, iletişime bir ya da daha fazla servis sağlayıcının dahil olmasına bakılmaksızın, trafik bilgilerinin süratle korunmasını kolaylaştıracak ve iletişime dahil olan servis sağlayıcılar ve iletişimin izlediği yolun tespit edilebilmesini sağlamaya yetecek miktarda trafik bilgisinin süratle açıklanmasına imkân verecek, yasal ve diğer düzenlemeleri yapmalarını öngörmektedir.⁵⁹⁷

Trafik bilgileri bir iletişimin en önemli unsurlarını ihtiva etmektedir. İletişimin kaynağını, varış noktasını, başlangıç ve bitiş zamanı, hizmet türü vb. trafik bilgilerini oluşturmaktadır. Bu nedenle, usulüne uygun olarak tutulmuş ve değiştirilme ihtimaline karşı korunmuş trafik verileri, belli bir suça yönelik soruşturma ve kovuşturmada failin, suç zamanının ve yerinin tespitinde ve failin yakalanmasında kolluk güçlerine büyük faydalar sağlamaktadır.⁵⁹⁸ Bununla birlikte, trafik bilgileri mevcut yasalar, teknik imkânlar ya da ticari nedenlerle çok kısa süre ile tutulan bilgilerdir. Bu nedenle, süratle korunmaları büyük önem taşımaktadır.⁵⁹⁹

Bir suçun aydınlatılması aşamasında trafik bilgileri sayesinde kolluk güçleri iletişimi mağdurdan geriye doğru takip etmek suretiyle faile ulaşma imkânı bulabilmektedir. Ancak çoğu zaman bilgilerin iletimine birden fazla İSS dahil olmaktadır. 17. Madde bu durumda dahi koruma talimatının, iletişime dahil olan İSS'lerin sayısına bakılmaksızın, tüm iletişim zincirinin yeniden bir araya getirilmesine olanak tanımasını amaçlamaktadır. Böylece, İSS'lerin sayısından bağımsız olarak haberleşmenin takip edilebilmesi garanti altına alınmak istenmektedir.⁶⁰⁰

İletişime dahil olan İSS'lerin birden fazla olması durumunda, her bir hizmet sağlayıcı iletişimin kendi sistemi üzerinden geçişi ile ilgili trafik bilgilerini üretmekte ve tutmaktadır. Bu nedenle, hiçbirinin elindeki trafik bilgisi tek başına iletişimin başlangıç ve bitiş noktasını tespit etmeye yarayacak kesin bilgiyi ihtiva

⁵⁹⁷ Siber Suçlar Sözleşmesi Madde 17.

⁵⁹⁸ Cevat Özel, M. Gökhan AHI, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", *Güncel Hukuk*, No.6, Haziran 2004, s.21.

⁵⁹⁹ Açıklayıcı Rapor, paragraf 166.

⁶⁰⁰ Cangemi, a.g.e., s.168.

etmeyebilir.⁶⁰¹ Bu durumda ceza soruşturması için önem taşıyan veriler herhangi bir İSS'de bulunabilmekte ve her bir İSS'nin elinde bulunan trafik bilgilerinin korunmasına ihtiyaç duyulmaktadır.⁶⁰² Sözleşme İSS'lere talimat verme yöntemini taraflara bırakmıştır. Taraflar, tek bir talimatla ya da her bir İSS'ye ayrı talimat verilmesi veya iletişim zinciri içerisinde İSS'lerin bir sonrakine talimatı iletmesi şeklinde düzenleme yapabilmektedir.⁶⁰³

Ancak, bir İSS'ye trafik bilgilerinin korunması için verilen talimat, söz konusu trafik bilgilerinin açıklanmasını gerektirmediği için, bu İSS'nin soruşturma ya da kovuşturma için yeterli bilgiye sahip olup olmadığı ve başka İSS'lerin iletişime dahil olup olmadığı bilinemeyecektir. Bu nedenle madde, İSS'nin iletişime dahil olan başka İSS'ler olup olmadığını ve iletişim güzergâhının belirlenmesine imkân verecek asgari trafik bilgisini kanun uygulayıcılara açıklamasını öngörmektedir.⁶⁰⁴

Ülkemizde ise İSS'lerin yükümlülükleri, 5651 sayılı Kanun ve Telekomünikasyon Kurumunun yayınladığı yönetmelik ile belirlenmiştir. 5651 sayılı Kanun'un 6. maddesine göre trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.⁶⁰⁵ Yönetmeliğe göre ise İSS olarak hizmet veren işletmeciler, en az altı ay süresince her bir kullanıcı için sisteme bağlı kalınan süre, trafik miktarı ve trafik yolu bilgilerini muhafaza etmek zorundadır.⁶⁰⁶ Diğer bir yönetmelikte ise işletmeci yani İSS'nin uyuşmazlık durumunda trafik bilgilerini mahkeme veya uyuşmazlığı çözmekle yetkili gerçek ve tüzel kişilere verebileceği ifade edilmiştir.⁶⁰⁷

⁶⁰¹ Açıklayıcı Rapor, paragraf 167.

⁶⁰² Keskin, a.g.e., s.166.

⁶⁰³ Açıklayıcı Rapor, paragraf 168.

⁶⁰⁴ Açıklayıcı Rapor, paragraf 169.

⁶⁰⁵ 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Madde 6: "(1) Erişim sağlayıcı; b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla..... yükümlüdür."

⁶⁰⁶ Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik Madde 5.4. "...İşletmeci, her bir kullanıcı için, kullanıcı tarafından sisteme bağlı kalınan süre, trafik miktarı ve trafik yolu bilgilerini en az 6 (altı) ay süreyle muhafaza etmekle yükümlüdür...", Bkz.: "http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/telekom-hiz-altyapi.pdf"

⁶⁰⁷ Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Madde 11 "...Trafik verisi; arabağlantı, faturalama veya benzeri anlaşmazlıkları çözmek amacıyla mahkeme veya uyuşmazlığı çözmekle yetkili gerçek ve tüzel kişilere bildirilebilir...", Bkz.: "http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/Kisisel_Bil_Yon_06_02_04.pdf".

Dolayısıyla ulusal mevzuatta, işlenen bir bilişim suçuna yönelik yürütülen bir soruşturmada suçun aydınlatılmasında büyük önem taşıyan trafik bilgilerinin İSS'ler tarafından korunması ve bunların kısmen açıklanması konusu 5651 sayılı Kanun ve ilgili yönetmeliklerle düzenlenmiştir. Ancak İSS'lerin bu konudaki yükümlülükleri yerine getirmemeleri durumunda cezaî bir yaptırım getirilmemiş ve idarî para cezası öngörülmüştür.⁶⁰⁸ Buna ilaveten iletişime birden fazla İSS'nin katılması durumunda, hangi yöntemin kullanılacağı konusunda da herhangi bir düzenleme bulunmamaktadır. Bu nedenle iç hukukta Sözleşmeye nazaran önemli eksikliklerin bulunduğu değerlendirilmektedir.

(4) Madde 18-Üretim Talimatı

Üretim talimatı maddesinde Sözleşme, tarafların yetkili mercilerine, kendi sınırları içerisinde bulunan bir kişiye mülkiyetinde veya kontrolünde bulunan bir bilgisayar sisteminde veya veri depolama aygıtında bulunan belirli bilgisayar verilerini vermesi ve yine sınırları içerisinde hizmet veren bir İSS'ye mülkiyetinde ya da kontrolünde bulunan hizmetlerle ilgili olmak üzere, abone bilgilerini vermesi talimatını verebilmeleri için gerekli olabilecek yasal ve diğer düzenlemeleri yapmalarını öngörmektedir. Maddede belirtilen abone bilgileri ifadesinden, İSS'ler tarafından bilgisayar verisi veya başka herhangi bir şekilde tutulan trafik ya da içerik bilgileri dışında kalan, abonenin kullandığı hizmet, teknik imkânlar, hizmet süresi, hizmet anlaşması gereği elde edilebilen abone kimliği, posta adresi, telefon ve diğer erişim numaraları, faturalandırma bilgileri ve iletişim cihazının tesis edildiği yer gibi aboneye ait diğer her türlü bilgi kastedilmektedir.⁶⁰⁹

Aslında üretim talimatı da depolanan bilgisayar verilerinin korunması ve trafik bilgilerinin kısmen açıklanmasında olduğu gibi kolluk güçlerine bir suça yönelik soruşturma aşamasında kolaylık sağlayacak bir uygulamadır. Ancak, burada dikkat edilmesi gereken husus üretim talimatının belirli olaylara ve kişilere yönelik olarak uygulanmasıdır. Suçlu avlamak için şahıslardan bilgisayar verilerini ya da İSS'lerden bir bölgedeki ya da hizmet verilen tüm abonelere ait bilgilerin istenmesi şeklinde icra edilmesi kastedilmemektedir. Zira bu tarz bir uygulama kişisel verilerin, temel hak ve özgürlüklerin korunması ile yine orantılılık ilkesine ters düşmektedir. Madde metninde, söz konusu ihtimalin ortadan kaldırılması ve keyfi uygulamalardan

⁶⁰⁸ 5651 sayılı Kanun Madde 6: "(3) Birinci fıkranın (b) ve (c) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir."

⁶⁰⁹ Siber Suçlar Sözleşmesi Sözleşme Madde 18.

kaçınılması için bu tarz düzenlemeler yapılamayacağı, üretim talimatının sözleşmenin 2. ilâ 11. maddelerinde belirtilen suçlara yönelik olarak ve belirli bir suçla ilgili soruşturma çerçevesinde verilebileceği belirtilmektedir.⁶¹⁰ Sözü edilen bilgisayar verileri ya da abone bilgileri ile hâlihazırda depolanmış olan bilgilerin üretimi kastedilmekte, geleceğe yönelik yeni bir kayıt oluşturulması amaçlanmamaktadır.⁶¹¹

Sözleşme ile getirilen bu usul mekanizmasının sıklıkla kanun uygulayıcılara ya da kolluğa yardım etmeye gönüllü, ancak sözleşmeleri ya da sözleşme dışı sebeplerle bunu yapamayan İSS'ler gibi üçüncü taraf yöneticilere kolaylık sağlayacağı düşünülmektedir.⁶¹² Üretim talimatı İSS'lerin ya da bireylerin verileri depolamış olduğu durumlarda uygulanabilir. Bazı İSS'ler hizmet verdikleri müşterilerin kayıtlarını tutmamaktadır. Bu nedenle, madde İSS'lere abonelere ait bilgileri tutması ya da bu bilgilerin doğruluğunu sağlaması yükümlülüğü getirdiği şeklinde yorumlanmamalıdır.⁶¹³

Mülkiyetinde olma ya da kontrolünde bulunma terimi ilgili verinin taraf devletin sınırları içerisinde fiziksel mülkiyet dahilinde bulunması veya üretilmesi istenen verinin kişinin fiziki mülkiyetinde olmadığı, ancak taraf devletin sınırları içerisinde kişinin üretimini serbestçe kontrol edebileceği durumlara karşılık gelmektedir. Örneğin uzak bir yer sağlayıcı tarafından sağlanan kişisel bir hesapta bulunan verinin üretimi bu kapsamdadır.⁶¹⁴

Suçla ilgili cezai bir soruşturma sürecinde abone bilgilerine başlıca iki durumda ihtiyaç duyulabilmektedir. Birincisi abone tarafından hangi hizmetlerin ve ilgili teknik araçların kullanıldığı ya da kullanılmakta olduğu örneğin kullanılan telefon hizmetinin çeşidi, telefon numarası ya da IP adresi tespit edilebilir. İkincisi ise IP adresi bilindiği zaman, ilgili şahsın kimliğini tespit etmeye yardımcı olması için abone bilgilerine ihtiyaç duyulmaktadır. Aboneye ait ticari bilgiler, fatura bilgileri ya da ödeme kayıtları da özellikle soruşturma bilgisayar dolandırıcılığı ya da diğer ekonomik suçları içerdiğinde cezai bir soruşturma ile alâkalı olabilir.⁶¹⁵

⁶¹⁰ Açıklayıcı Rapor, paragraf 174-182.

⁶¹¹ Açıklayıcı Rapor, paragraf 170.

⁶¹² Açıklayıcı Rapor, paragraf 171.

⁶¹³ Keskin, a.g.e., s.167.

⁶¹⁴ Açıklayıcı Rapor, paragraf 173.

⁶¹⁵ Açıklayıcı Rapor, paragraf 178.

Ülkemizde İSS'lere üretim talimatı verilmesi kapsamında değerlendirilebilecek düzenlemeyi içeren Ulaştırma Bakanlığı'nın Telekomünikasyon Hizmetleri Yönetmeliği⁶¹⁶ 26 Ağustos 2004 Tarih ve 25565 sayılı Resmi Gazete ile yürürlükten kaldırılmıştır.⁶¹⁷ Ancak, Adalet Bakanlığı'nın 14 Şubat 2007 tarihli Resmi Gazete'de yayınlanan ve Ceza Muhakemesi Kanunu çerçevesinde yapılacak iletişim, tespiti, dinlenmesi ve kayda alınmasını düzenleyen yönetmelikte İSS'lere istenmesi halinde "üretim" yapmaları zorunluluğu getirilmektedir.⁶¹⁸ Dolayısıyla, İSS'lerin üretim sorumlulukları açısından Sözleşmeye paralellik sağlanmıştır. Ancak, şahıslara üretim talimatı verilmesini sağlayacak bir düzenleme henüz mevcut değildir.

(5) Madde 19-Depolanmış Bilgisayar Verilerinin Aranması ve Bunlara El Konulması

Saklanan bilgisayar verilerinin aranması ve bunlara el konulması maddesinde Sözleşme tarafların, yetkili mercilerine ulusal sınırları içerisindeki bir bilgisayar sisteminde ya da bir parçasında ve bunların içerisinde depolanan bilgisayar verilerinde ve yine bilgisayar verilerinin depolanabileceği aygıtlarda arama yapma ve benzer şekilde erişim sağlama hususunda yetki verecek, gerekli yasal ve diğer düzenlemeleri yapmalarını öngörmektedir.

Taraflar yetkili mercilerinin, aranan verilerin kendi ulusal sınırları içinde bulunan ve ilk sistemden yasal olarak erişilebilen başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair gerekçeleri bulunduğu, arama ya da erişim işlemlerini bu sistemi de kapsayacak şekilde genişletebilmelerini ve erişilen verilere el konulması veya benzer şekilde korunmasını sağlamak üzere gerekli olabilecek yasal ve diğer düzenlemeleri yapmalarını da öngörmektedir. Bu kapsamda; bir bilgisayar sistemine, parçasına ya da veri depolama aygıtına el konulması veya benzer şekilde koruma altına alınması, bu bilgisayar verilerinin kopyalanarak alıkonulması, ilgili verilerin bütünlüğünün korunması ve erişilen bilgisayar sistemindeki verilerin silinmesi ya da erişilmez kılınması sağlanabilmelidir.

⁶¹⁶ Yönetmelik EK-3, Özel Şartlar "...(e) İnternet Servis Sağlayıcılığıyla (İSS) İlgili Yetki Belgelerine İlişkin Genel Hükümler "Kurum'ca talep edilmesi halinde; İSS'ler, kullanıcı sayısı, kullanıcı kimlikleri, sisteme bağlı kalınan süre ve iletilen bilgi miktarları ile ilgili trafik bilgileri verecektir.", (Çevrimiçi), <http://www.telkoder.org.tr/2-law/t-law01.doc>, 10 Ocak 2007.

⁶¹⁷ Bkz.: Resmi Gazete, http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/Resmi_Gazete_26.08.2004_2.pdf.

⁶¹⁸ Yönetmelik Madde 10 " (2) Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada Cumhuriyet savcıları veya mahkemeler tarafından; abone bilgileri, telefon numarası, elektronik cihaz bilgileri veya iletişim bağlantısının tespitine imkân veren kodu gibi iletişimin tespiti kapsamı dışındaki bilgiler işletmecilerden talep edilebilir. Bu tür istemler işletmeciler tarafından derhal yerine getirilir.". 14 Şubat 2004 tarih ve 26434 sayılı Resmi Gazete, (Çevrimiçi), 10 Mart 2004, "<http://rega.basbakanlik.gov.tr/eskiler/2007/02/20070214-11.htm>".

Ayrıca taraflar, yetkili mercilerine söz konusu bilgisayar sistemlerinin çalışması ya da verilerin korunması ile ilgili bilgi sahibi olan herhangi bir kimseye bu yetkilerin kullanılması esnasında gerekli bilgileri ve yardımı temin etme talimatını verebilecek yasal ve diğer düzenlemeleri de yapmalıdır.⁶¹⁹

Sözleşmenin bu maddesi ile elektronik olmayan geleneksel ortamdaki arama ve el koyma yöntemlerinin elektronik ortama uyumlu hale getirilmesi⁶²⁰ ve delil elde etmek amacıyla bilgisayarlarda depolanan verilerin aranması ve el konulması hususunda, tarafların iç hukuklarında modernleştirme ve uyumlaştırma sağlanması amaçlamaktadır. Yazılı belgeler veya dokümanların bulunduğu geleneksel arama ortamında arama faaliyeti maddi kayıtların aranması, incelenmesi ve el konulmasını faaliyetini içermektedir. Verilerin toplanması arama sırasında ve o anda mevcut olan verilere yönelik olarak gerçekleşir ve aramanın ön koşulu belli bir yerde yine belli bir cezai suça delil teşkil edecek verilerin var olduğuna inanmak için makul şüphenin bulunmasıdır.⁶²¹

Elektronik ortamda yapılan aramalar göz önüne alındığında geleneksel aramanın birçok özelliğinin devam ettiği görülmektedir. Verilerin toplanması arama sırasında ve o esnada mevcut olan verilere yönelik gerçekleştirilmektedir. Arama yapmak için gerekli ön koşul da değişmemektedir. Arama için belli bir suça yönelik delil niteliğinde veri elde edileceğine dair makul şüphenin bulunması gerekmektedir.⁶²²

Bilgisayar verileri elektromanyetik ortamda olmaları nedeniyle, fiziksel doküman yada deliller gibi el konulup götürülememektedir. Bu nedenle, verinin depolandığı fiziksel cihaza el konularak götürülmesi veya verinin yazıcı çıktısı gibi maddi bir kopyasının alınması ya da disket vb. bir cihaz üzerine maddi olmayan bir kopyasının alınması gerekmektedir. Kopya alınan durumlarda verinin bir kopyası bilgisayar sisteminde ya da depolama aygıtında kalmaya devam etmektedir. Sözleşme tarafların, bu şekilde kopya çıkarılmasına müsaade edecek düzenlemeyi yapmalarını öngörmektedir.⁶²³

⁶¹⁹ Siber Suçlar Sözleşmesi Madde 19.

⁶²⁰ Keskin, a.g.e., s.169.

⁶²¹ Açıklayıcı Rapor, paragraf 184-185.

⁶²² Açıklayıcı Rapor, paragraf 186.

⁶²³ Açıklayıcı Rapor, paragraf 187.

Bazen aranan veri CD-ROM, disket vb. bir veri depolama aygıtında bulunabileceği gibi, aranan bilgisayar sisteminden bağlanılabilen devletin sınırları içerisinde kalan diğer bir bilgisayar sistemi ya da depolama aygıtında bulunabilmektedir. Sözleşme, tarafların kanun uygulayıcı otoritelerine bu durumlarda erişim ve arama yetkisi tanımlarını istemektedir. Ancak bu madde, İnternet aracılığıyla ulaşılabilir olsa dahi başka bir devletin sınırları içerisinde depolanan verilerin aranmasına yetki vermemektedir.⁶²⁴ Sözleşme, hem bilgisayar sisteminin hem de yakınında bulunan ilgili tüm veri depolama aygıtlarının aranmasını kapsayıcı bir yetkilendirmeyi öngörmektedir. Arama ve el koyma yetkisinin genişletilmesi konusunu ise ulusal düzenlemelere bırakılmaktadır.⁶²⁵

Bazı durumlarda örneğin veriler kopyalanmalarının mümkün olmadığı nadir işletim sistemlerinde bulunuyorsa, veri taşıyıcısının tamamına el koymak kaçınılmaz olabilmektedir.⁶²⁶ Bilgisayar sistemlerinden elde edilen elektronik deliller parmak izi veya DNA delilleri gibi gözle görülmeyen ve ayrıntılı inceleme gerektiren gizli bir yapıya sahiptir.⁶²⁷ Bilgisayarda üzerine başka veriler yazılan bununla birlikte veri taşıyıcısında izleri kalmış eski veriler delil niteliği taşıyabilir ve bu şekilde gizli bir yapıdadır. Tekrar kazanılması için veri taşıyıcısının ayrıntılı şekilde incelenmesi gerekir. Sözleşme bu durumda da el koymayı kaçınılmaz olarak görmektedir.⁶²⁸

Bilgisayar ortamında bulunan deliller hassastır, kolayca değiştirilebilir, tahrip edilebilir ve yok edilebilir. Bu nedenle arama ve el koyma işleminde, arama tamamlandıktan sonra önemli olan husus delil özelliği taşıyan bilgisayar verilerinin soruşturma sonuçlanıncaya kadar korunmasıdır. Bu koruma işleminde, delil teşkil eden verilerin herhangi bir şekilde değiştirilmesi, silinmesi, taşınması veya erişilmez kılınması engellenmelidir.⁶²⁹

Sözleşmeye göre el koyma, veri ya da bilginin kaydedildiği fiziksel aygıtın götürülmesi veya verinin bir kopyasının alınmasıdır. Veriler maddi formda bulunmadığı için yetkili mercilerin verileri güven altına alması için ilave tedbirlere gerekir. Bunlar kopyalanan ya da taşınan verilerin sonradan el koyma anındaki haliyle geri elde edilebilmesi ve soruşturma süresince değişmeden muhafazasına

⁶²⁴ Cangemi, a.g.e., s.169.

⁶²⁵ Açıklayıcı Rapor, paragraf 194.

⁶²⁶ Açıklayıcı Rapor, paragraf 196.

⁶²⁷ Leyla Keser Berber, "Adli Bilişim", **Güncel Hukuk**, No. 6, Haziran 2004, s.19.

⁶²⁸ Açıklayıcı Rapor, paragraf 196.

⁶²⁹ Berber, a.y.

yönelik “verinin bütünlüğünün” veya “gözetim zincirinin” korunmasıdır. Böylece verilere el koyma ya da onları benzer şekilde güven altına alma, verileri kopyalamak yoluyla delil toplamak, ya da verileri kopyalamak ve daha sonra orijinal versiyonlarını erişilmez kılmak ya da taşımak yoluyla verileri müsadere etmek anlamındadır. El koymak, el konan verilerin nihai olarak silinmesi anlamına gelmemektedir.⁶³⁰

Verilerin erişilmez kılınması şifreleme ya da başka bir biçimde verilere erişimin engellenmesidir. Bu önlemin, virüs programları ya da bomba imalatıyla ilgili bilgiler, çocuk pornografisi veya yasadışı içerik olduğu durumlara uygulanması yararlı olabilir.⁶³¹

Bu madde ile aranan bilgisayar sistemi ile ilgili bilgi sahibi kişilere, işbirliği yapma talimatı verebilme yolunun yaratılmasını sağlanarak, arama yapmanın hem icra mercileri hem de bu durumdan etkilenen masum kişiler için daha etkili ve maliyet etkin bir hale getirilmesi amaçlanmaktadır. Bir sistem yöneticisini yasal olarak yardım etmeye zorlamak, yöneticinin sözleşmelerden kaynaklanan verileri açıklamamak ya da başka tür yükümlülüklerinden kurtulmasını da sağlayabilir.⁶³²

Ulusal mevzuatta bilgisayar verilerinin aranması ve el konulması hususu Ceza Muhakemesi Kanununun 134. maddesi ve Adli ve Önleme Aramaları Yönetmeliği 17. maddesinde düzenlenmiş ve “Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma” başlığı altında ifade edilmiştir.

Söz konusu düzenlemeye göre, bir suç dolayısıyla yapılan soruşturmada şüphelinin kullandığı bilgisayar, bilgisayar programları ile verilerde arama yapılmasına, verilerin kopyasının çıkarılmasına ve kayıtların çözülerek metin haline getirilmesine, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının isteği üzerine hakim tarafından karar verilmektedir.⁶³³ Burada “bir suç” ifadesi kapsamına hem elektronik ortamda delil bulunan klasik suçlar, hem de bilişim suçları girmektedir.⁶³⁴ Böylece Sözleşmede belirtilen arama ve el koyma tedbirinin, hâlihazırda mevcut olan ve belirli bir suça delil teşkil edecek verilerle ilgili olması şartı ile örtüşme sağlanmaktadır.

⁶³⁰ Açıklayıcı Rapor, paragraf 197-199.

⁶³¹ Açıklayıcı Rapor, paragraf 198.

⁶³² Açıklayıcı Rapor, paragraf 201.

⁶³³ CMK madde 134.

⁶³⁴ Ali Karagülmez, “Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular”, **Çağın Polisi Dergisi**, C.IV, S.46, Ekim 2005, s.9.

Söz konusu düzenleme bilgisayar sistemlerinde arama yapılmasına, verilerin aranmasına, kopyalarının çıkarılmasına ve el konulmasına olanak sağlamaktadır. Bilgisayar sistemine veya verilere şifre nedeniyle girilememesi veya gizlenmiş bilgilere ulaşılamaması durumunda çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için el konulabilmektedir. El koyma işleminde sistemdeki bütün verilerin yedeklemesi yapılmakta ve istemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline de verilmekte, bu husus tutanağa geçirilerek imza altına alınmaktadır. Tutanağın bir sureti de ilgililere verilmektedir. Burada yine Sözleşmeye paralel şekilde verilerin bütünlüğünün korunması ve soruşturma sonuçlanıncaya kadar, soruşturma ile ilgili delil niteliği taşıyabilecek verilerin değiştirilmesi, bozulması, erişilmez hale getirilmesi, silinmesi engellenmektedir. El koyma gerekçeleri detaylı şekilde açıklanmamış olmasına rağmen, bu husus da Sözleşmeye bir paralellik sağlanmaktadır.

Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilmektedir. Bu sayede şüpheli bilgisayar sistemini, programlarını veya verilerini kullanmaya devam edebilmektedir. Ancak tutanak altına alınarak yedeklenen verileri değiştirmesi bu aşamadan sonra bir anlam ifade etmemektedir. Ülkemizde uygulamada kolluk güçleri üç kopya çıkarmakta ve birini şüpheliye vermekte, biri incelenmekte bir diğeri ise uyuşmazlıkların giderilmesi için ayrı bir birimde koruma altına alınmaktadır. Burada da Sözleşme ile bir uyum görülmektedir. Ancak verilerin suç oluşturan içerik ya da virüs programı veya çocuk pornografisi gibi başlı başına suç unsuru ya da suç aracı olması durumunda erişilmez kılınması ve hatta kopyaları alındıktan sonra taşınması veya silinmesi gerekmektedir. Sözleşme, bu hususta bir düzenleme getirmesine rağmen, ulusal mevzuatımızda bu hususu kapsayıcı bir ifade yer almamasının bir eksiklik olduğu değerlendirilmektedir.

Sözleşme arama ve el koyma yetkisinin, İnternet vb. telekomünikasyon ağları ile yasal olarak erişilebilen diğer sistemler ya da bilgisayar sistemine doğrudan bağlı bulunan veya yakınında bulunan veri depolama aygıtları için de genişletilebileceğini öngörmekte ve uygulamayı ulusal mevzuatlara bırakmaktadır. CMK'nın 134. maddesinde bu konuda bir düzenleme bulunmaması nedeniyle bu maddenin İnternet ortamı için yetki sağlamadığı ifade edilebilir. Bununla birlikte, Adli ve Önleme Aramaları Yönetmeliğinin 17. maddesinde bulunan yedekleme işleminin

bilgisayar ağları ve diğer uzak bilgisayar kütükleri hakkında da uygulanabileceği⁶³⁵ şeklindeki ifade bu kapsamda değerlendirilebilir. Ancak, bilişim sistemlerinin yapısı ve bilgisayar sistemlerinin birbirlerine bağlanabilme özellikleri göz önüne alındığında bilgisayar verilerinin ağa bağlı başka bir sistemde saklanabilmesi büyük bir olasılıktır. Dolayısıyla tek cümle ile ifade edilen bu düzenlemenin yetersiz olduğu, arama ve el koyma yetkisinin İnternet üzerinden fail tarafından erişilebilen diğer sistemleri ve hizmetleri kapsayacak şekilde genişletilmesi hususunda sınırların mümkün olduğunca net çizilmesi, CMK 134. madde ve Arama Yönetmeliğinin 17. maddesinde buna imkân sağlayıcı yetkilerin düzenlenmesi gerektiği değerlendirilmektedir.

(6) Madde 20-Trafik Bilgilerinin Gerçek Zamanlı Olarak Toplanması

Sözleşmenin 20 ve 21. maddelerinde taraf devletlerin, iletişim bilgilerinin toplanması, İSS'lerin bu konuda işbirliği ve yardım sağlamaları, içerikle ilgili bilgilerin gerçek zamanlı olarak toplanması, kaydedilmesi, yetkili mercilerle işbirliğine gidilmesi ve bu tedbirin gizli tutulması konusunda gerekli yasal ve diğer düzenlemeleri yapmaları ile ilgili yükümlülükler ele alınmaktadır.⁶³⁶

Haberleşmeye müdahale etme kavramı genellikle geleneksel telekomünikasyon ağları ile ilgilidir. Bu ağlar, optik ya da klasik kablo altyapısını ve ilaveten bunların mobil telefon ve mikrodalga iletim sistemleri gibi kablosuz ağlarla bağlantılarını da ihtiva etmektedir. Günümüzde mobil haberleşme aynı zamanda uydu sistemleri üzerinden de gerçekleştirilmektedir. Bilgisayar ağları bağımsız olarak tesis edilmiş kablo altyapısı ile teşkil edilebileceği gibi, çoğunlukla küresel bir özelliğe sahip olmalarını da sağlayan telekomünikasyon altyapısı üzerinden sanal olarak oluşturulmaktadır. Böylece Sözleşmenin 1. maddesindeki "bilgisayar sistemi" tanımı cihazların ya da cihaz gruplarının hangi yöntemle irtibatlandırıldığını kısıtlamamaktadır. Bundan dolayı, madde 20 ve 21'de, bir bilgisayar sistemi aracılığıyla iletilen, başka bir bilgisayar sistemine ulaşmadan önce telekomünikasyon ağları aracılığıyla da iletilebilen belirli iletişim bilgileri ele alınmaktadır.⁶³⁷

⁶³⁵ Adli ve Önleme Aramaları Yönetmeliği Madde 17 "...Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır..."

⁶³⁶ Yener Ünver, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi", *İÜHFİM*, C. LIX, No.1-2, 2001, s.138.

⁶³⁷ Açıklayıcı Rapor, paragraf 206.

İçerikle ilgili bilgilere gerçek zamanlı olarak müdahale edilmesi hukukta sıklıkla ağır suçlar ya da suç kategorilerine yönelik cezai soruşturmalar için öngörülmektedir. Sözleşme bu suçları kendisi göstermemiş bu hususu ulusal mevzuatlara bırakmıştır.⁶³⁸ Bu suçların ulusal mevzuatlarda tanımlanması, sıklıkla tedbirin uygulanabileceği suçların liste halinde düzenlenmesi veya suça uygulanabilen azami hapis cezasına atıf yapılarak bu kategoriye dahil edilmesi şeklinde yapılmaktadır. 21 maddede de, taraflara içerik verilerine müdahale tedbirini, yalnızca ulusal mevzuatın belirlediği bir dizi ciddi suçla ilgili olarak tesis etmeleri zorunluluğu getirilmiştir.⁶³⁹

Trafik bilgilerinin toplanması ile ilgili olan 20. madde ise bu kadar kısıtlı değildir ve prensip olarak Sözleşmede belirtilen bütün cezaî suçlar için geçerlidir. Ancak tarafların, içerik verilerine müdahale önlemini uyguladıkları suçlardan daha sınırlı olmaması şartıyla, sadece hak saklı tutma imkânı verilen suçlarda ya da suç kategorilerinde hak saklı tutabileceği belirtilmiştir. Yani içerik bilgilerine müdahale edilebilen bir suç için, trafik bilgilerine müdahale etme önlemini saklı tutma hakkı kullanılamayacaktır.⁶⁴⁰ Böylece sözleşme saklı tutma hakkını kullanan tarafları, 20. maddeyi en geniş biçimde uygulayabilmeleri için yönlendirmektedir.⁶⁴¹

Sözleşme trafik bilgilerinin gerçek zamanlı olarak toplanması maddesinde, tarafların ulusal sınırları içerisinde yetkili mercilere, teknik olanaklar kullanarak bilgisayar sistemleri ile gerçekleştirilen belirli bir haberleşmeye ait trafik bilgilerini gerçek zamanlı olarak toplayacak veya kaydedecek yetkileri sağlayacak yasal ve diğer düzenlemeleri yapmalarını öngörmektedir. Aynı zamanda İSS'leri mevcut teknik imkânları çerçevesinde trafik bilgilerini toplamaya veya yetkili mercilere bu konuda yardım etmeye ve işbirliğine zorlamayı içermektedir. Yine taraflar İSS'lerin bu tedbiri gizli tutmasını sağlayacak yasal ve diğer düzenlemeleri de yapacaktır.⁶⁴²

Daha önceki usul hukukuna ilişkin maddeler bilgisayar verilerinin depolanmış olduğu, yani elde delil özelliği taşıyabilecek verilerin bulunduğu durumlarda uygulanabilen koruma yöntemleridir. Ancak, teknolojinin verdiği imkânlar sayesinde siber uzayda failler suçu işledikten sonra arkalarında bıraktıkları izleri silerek kaybolabilmekte ya da milisaniyeler içerisinde değiştirerek kolluk güçlerini

⁶³⁸ Keskin, a.g.e., s.158.

⁶³⁹ Açıklayıcı Rapor, paragraf 212.

⁶⁴⁰ Açıklayıcı Rapor, paragraf 213.

⁶⁴¹ Keskin, a.g.e., s.159.

⁶⁴² Siber Suçlar Sözleşmesi Madde 20.

yanıltabilmektedirler. Sonuçta geçmişe ait ya da depolanmış veri soruşturma anında mevcut olmayabilir veya değiştirilmiş olabilir.⁶⁴³ Bu nedenle, trafik bilgilerinin gerçek zamanlı olarak toplanması faile ulaşabilmek bakımından daha etkin bir yetki halini alabilmekte⁶⁴⁴ ve bazen failin tespit edilebilmesinin tek yolu iletişimin kaynağının iletişim devam ederken belirlenmesi olmaktadır.⁶⁴⁵

Maddeye göre ilgili trafik bilgileri tarafların ulusal sınırları içindeki belirli iletişimlerle ilgili olmalıdır. Trafik bilgilerinin toplanabildiği ya da kaydedilebildiği iletişimler açıkça belirlenmek zorundadır. Dolayısıyla, Sözleşmede büyük miktarlarda trafik verisinin genel amaçlı ve gelişigüzel bir biçimde toplanması öngörülmemekte ve buna izin verilmemektedir. Toplama yetkisini veren talimatlarda trafik verilerinin toplanabileceği iletişimler belirtilmek zorundadır.⁶⁴⁶

Sözleşmeye göre taraflar yetkili mercilerinin trafik bilgilerini teknik yöntemlerle toplama ve kaydetme imkânına sahip olmalarını sağlamak zorundadır.⁶⁴⁷ Madde bunun teknolojik olarak nasıl gerçekleştirileceği belirtilmemekte ve teknik açıdan hiçbir kısıtlama getirmemektedir.⁶⁴⁸ Yine taraflar yetkili mercilerin, İSS'leri trafik bilgilerini toplama ve kaydetmeye veya yardım ve işbirliğine zorlayabilmelerini sağlamalıdır. İSS'lerle ilgili bu zorunluluk, yalnızca İSS'lerin teknik imkânları çerçevesinde uygulanabilmektedir. Sözleşme İSS'lere yeni donanımlar temin etmeleri, uzman desteği almaları ya da masraf yaratacak şekilde sistemlerini yeniden düzenlemeleri zorunluluğu getirmemektedir. Madde İSS'lerin bu imkânlarını hâlihazırda bulunması durumunda ve kanun tarafından talep edildiğinde kullanmasını öngörmektedir.⁶⁴⁹

Bu önlem ulusal düzeyde uygulanacak olduğu için, ulusal sınırlar içindeki belirli iletişimlerin toplanması ve kaydedilmesi için geçerlidir. Dolayısıyla, pratik olarak, yükümlülükler genel olarak İSS'nin, başlıca faaliyetlerini yürüttüğü yer ya da merkez ofisi başka bir yerde olsa dahi, bu ulusal sınırlar içinde önlemleri gerçekleştirecek fiziksel altyapı ya da teçhizata sahip olduğu durumlar için de geçerlidir. Sözleşmenin amaçları açısından, iletişimde bulunan taraflardan biri (insan

⁶⁴³ Çeken, a.g.e., s.99.

⁶⁴⁴ Keskin, a.g.e., s.174.

⁶⁴⁵ "Cybercrime Laws, Prevention and Enforcement Capacity Builds", I-Ways, C.XXVI, No.3, 2003, s.120.

⁶⁴⁶ Açıklayıcı Rapor, paragraf 219.

⁶⁴⁷ Keskin, a.g.e., s.175.

⁶⁴⁸ Açıklayıcı Rapor, paragraf 220.

⁶⁴⁹ Açıklayıcı Rapor, paragraf 221.

ya da bilgisayar) belli bir taraf ülkenin ulusal sınırları içindeyse ya da iletişimin geçtiği bilgisayar ya da telekomünikasyon teçhizatı bu sınırlar içinde bulunuyorsa, söz konusu iletişimin ilgili tarafın ulusal sınırları içinde olduğu kabul edilmektedir.⁶⁵⁰

Trafik bilgilerinin anında toplanmasında tedbiri gizli olarak uygulandığı takdirde ceza soruşturmasında etkin olmaktadır. Bu nedenle Sözleşmede trafik verilerinin anında toplanması işleminin gizli yapılması öngörülmektedir. Bu çerçevede, müdahale, iletişimin taraflarının algılayamayacakları bir şekilde yürütülmelidir. Ayrıca, işbirliği yapan ya da yardım eden İSS'lere ve bilgisi bulunan çalışanlarına en azından soruşturma tamamlanıncaya kadar sır saklama yükümlülüğü getirecek yasal düzenleme yapılmalıdır.⁶⁵¹

Ulusal mevzuatımızda trafik bilgilerine gerçek zamanlı müdahale edilmesine yönelik mevcut düzenleme, iletişimin tespiti ile ilgili olduğundan müteakip madde çerçevesinde değerlendirilmiştir.

(7) Madde 21-İçerikle İlgili Bilgilere Müdahale Edilmesi

Sözleşmenin bu maddesi, tarafların iç hukuklarında kararlaştırılan bir seri ağır suçla ilgili olarak, yetkili mercilerine ulusal sınırları içinde, teknik olanaklar kullanarak bilgisayar sistemleri ile gerçekleştirilen belirli bir haberleşmeye ait içerik bilgilerini gerçek zamanlı olarak toplayacak veya kaydedecek yetkileri sağlayamaya yönelik yasal ve diğer düzenlemeleri yapmalarını öngörmektedir. Madde, İSS'lerin mevcut teknik imkânları çerçevesinde içerik bilgilerini toplamaya veya yetkili mercilere bu konuda yardım etmeye ve işbirliğine zorlanmasını da içermektedir. Yine taraflar, İSS'lerin bu tedbiri gizli tutmasını sağlayacak düzenlemeleri de yapacaktır.⁶⁵²

Bu maddede düzenlenen içerik bilgilerine müdahale tedbiri, telefon görüşmelerinin anında dinlenmesinin bilişim dünyasındaki biçimini oluşturmaktadır.⁶⁵³ Telefon konuşmaları ve benzeri telekomünikasyon vasıtalarına ait içerik bilgilerinin toplanması, iletişimin yasadışı bir nitelikte olup olmadığının (iletişimin suç teşkil eden tehdit veya yıldırma oluşturmaları, suç işlemeye yönelik komplolar, yalan beyanlar içermesi vb.) belirlenmesi ve işlenmiş ya da planlanan suçların delillerinin toplanması için gerekli bir tedbirdir. Bilgisayar iletişimleri de

⁶⁵⁰ Açıklayıcı Rapor, paragraf 222.

⁶⁵¹ Keskin, a.g.e., s.175.

⁶⁵² Siber Suçlar Sözleşmesi Madde 21.

⁶⁵³ Keskin, a.g.e., s.158.

benzer nitelikte suçlar teşkil edebilir ya da bunlara delil oluşturabilir. Bilgisayar suçlarının çoğunun işlenmesi, bir bilgisayar sistemine yasadışı erişim için gönderilen kodlar ya da bilgisayar virüslerinin dağıtımı gibi verilerin iletimi yoluyla gerçekleşir ve gönderilen mesajın içeriğine müdahale edilmeden, zararlı ve yasadışı nitelikte olduğunu belirlemek mümkün değildir.⁶⁵⁴

Suçun oluşumunu belirleyecek ve bunu önleyecek yetenekler olmadan kolluk, yalnızca zararın olduğu tamamlanmış suçları soruşturabilecektir. Bu nedenle, bilgisayar iletişimlerine ait içerik bilgilerine gerçek zamanlı müdahale, suçu önlemek açısından geleneksel iletişime müdahale etmek kadar, hatta belki daha da önemli bir hal almaktadır.⁶⁵⁵

"İçerik verileri" iletişimin içeriği, yani iletişimin anlamı ya da niyeti, ya da iletişim yoluyla iletilen mesaj ya da bilginin kendisidir. Trafik bilgileri dışında iletişime ait olarak iletilen her şey içerik verisini oluşturmaktadır.⁶⁵⁶

Bu maddede belirtilen çoğu unsur, 20. maddede belirtilenlerle özdeştir. Bu nedenle, yukarıda belirtilen, trafik bilgilerinin toplanması ve kaydedilmesi, işbirliği ve yardım yükümlülüğü ve gizlilik yükümlülüğü ile ilgili bütün değerlendirmeler içerik verilerine müdahale için de aynen geçerli olmaktadır. Ancak, içerik bilgilerine gerçek zamanlı olarak müdahale edilmesi için geçerli şart ve önlemler, trafik bilgilerinin gerçek zamanlı toplanması, depolanmış bilgisayar verilerinin aranması ve bunlara el konması, benzer şekilde verilere erişilmesi ya da güven altına alınması için geçerli olanlardan daha sıkı olabilir.⁶⁵⁷ Bunun nedeni, bu önlemin haberleşme özgürlüğüne ve özel yaşamın dokunulmazlığına en ağır müdahaleyi teşkil etmesidir.⁶⁵⁸ Bu nedenle, Sözleşmeyi hazırlayanlar bu konuda hassas davranmayı ve bir ihlâl yol açacak bağlayıcı ya da hükmedici bir ifade kullanmamayı tercih etmektedir.

Ulusal mevzuatta usul hukukunda birebir İnternet üzerinden yapılan iletişime ait trafik bilgilerinin gerçek zamanlı toplanması veya içerik bilgilerine müdahale edilmesine imkân veren veya bu hususu düzenleyen bir hüküm bulunmamaktadır. Ancak, telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi düzenlenmiştir. Dinlemeler bir suça

⁶⁵⁴ Keskin, a.g.e., s.176.

⁶⁵⁵ Açıklayıcı Rapor, paragraf 228.

⁶⁵⁶ Açıklayıcı Rapor, paragraf 229.

⁶⁵⁷ Açıklayıcı Rapor, paragraf 230-231.

⁶⁵⁸ Keskin, a.g.e., s.175.

ilişkin cezai soruşturma kapsamında başka yolla delil elde etme imkânı bulunmaması halinde ya da istihbarî ve önleyici amaçlı olarak iki şekilde yapılabilmektedir. İki Ceza Muhakemesi Kanununun 135. maddesinde işlenmiş ya da işlendiğine dair kuvvetli bir şüphe olan haller için düzenlenmiştir.

CMK'nın iletişimin tespiti, dinlenmesi ve kayda alınması başlıklı 135. maddesi uyarınca bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine yönelik kuvvetli şüphenin varlığı ve başka yollarla delil elde edilmesine imkân bulunmadığı durumlarda, hakim kararı ile gecikmesinde sakınca bulunan hallerde ise Cumhuriyet savcısının kararı ile şüpheli veya sanığın telekomünikasyon yolu ile iletişimi tespit edilebilmekte, dinlenebilmekte ve kayda alınabilmektedir. Aynı madde uyarınca sinyal bilgileri de değerlendirilebilmektedir. Burada önemli olan husus, bir suçun varlığı ya da buna yönelik kuvvetli şüphenin bulunmasıdır. Daha önce de belirtildiği gibi Sözleşmede de usul hükümleri belirli bir suça yönelik olarak uygulanmakta ve makul şüphe aranmaktadır.

İstihbarî veya önleyici amaçlı dinlemelerin ise usul hukukunda yasal dayanağı yoktur. Ancak, 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Selâhiyet Kanununun Ek 7. maddesi⁶⁵⁹, 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun Ek 5 inci maddesi ve 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun 6. maddesi bu kapsamda değerlendirilebilir. Ancak, AHİM kararları göz önüne alındığında bu maddeler kriterleri karşılamamaktadır.⁶⁶⁰

Gerek CMK'nın 135. maddesi, gerekse istihbarî ve önleyici amaçla iletişimin tespiti dinlenmesi ve kayda alınmasına ilişkin usul ve esaslar "Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının

⁶⁵⁹ Ek Madde 7-"...Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişini sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar.

Birinci fıkrada belirtilen görevlerin yerine getirilmesine yönelik olarak, 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250. maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir...", diğer kanunlarda da düzenleme benzer şekildedir.

⁶⁶⁰ Hamdi Ü. KARABEYOĞLU, "Açıklamalı Ceza Muhakemesi Kanunu", s.80. (Çevrimiçi), <http://www.ceza-bb.adalet.gov.tr/makale/127.doc>, 15 Kasım 2006,

Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik”te düzenlenmiştir.⁶⁶¹ Buna göre Emniyet, Jandarma ve Milli İstihbarat Teşkilatlarının yetki ve sorumluluklarını belirleyen kanunlarda belirtilen görevleri yerine getirmek üzere önleme veya istihbarî dinleme gerçekleştirilebilmektedir.

Bir suçun oluşmasından önce tespit, dinleme, kayda alma faaliyeti Emniyet, Jandarma veya Milli İstihbarat Teşkilatınca talep edilebilmekte ve suçun önlenmesine yönelik veya istihbarî amaçlı tedbir olarak tanımlanmaktadır. Önlemede suçun işlenmesinin önlenmesi amacıyla verilen hâkim kararları ile gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanı tarafından, Jandarma Genel Komutanı veya İstihbarat Başkanı tarafından verilen yazılı emirle, Anayasanın 2. maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak verilen hâkim kararları ile gecikmesinde sakınca bulunan hallerde Milli İstihbarat Teşkilatı Müsteşarı veya yardımcısı tarafından verilen yazılı emirle tek merkezden Telekomünikasyon İletişim Başkanlığı’nca yerine getirilmektedir.⁶⁶² Burada önemli olan nokta henüz suçun oluşmamış olmasıdır.

Telekomünikasyon terimi ile günümüzde kullanılan tüm iletişim yöntemleri kapsanmaya çalışılmakta, ses, görüntü, işaret, sembol ve elektrik sinyallerine dönüştürülebilen her türlü verinin yine kablo, telsiz, optik, elektromanyetik vb. her tür iletim yöntemi ile gönderilmesi ve alınması ifade edilmektedir. Buradan açık bir şekilde İnternet aracılığıyla yapılan iletişimin de bu madde kapsamında olduğu görülmektedir. Sinyal bilgileri ise Sözleşmede ifade edilen trafik bilgilerine karşılık gelmektedir. Tespit etme işlemi iletişimin içeriğine müdahale edilmeden yalnızca sanığın diğer kişilerle kurduğu iletişime ait aranan numaralar, yerleri ve kimlik bilgileri gibi bilgilerinin tespit edilmesine yöneliktir. Dinleme ve kayda almada ise

⁶⁶¹ Yönetmeliğin amacı 1. Maddesinde “...Bu Yönetmelik; a) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Selâhiyet Kanununun ek 7. maddesi, 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5 inci maddesi, 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun 6 ncı maddesi ile 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesi ile belirlenen çerçevede telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına ilişkin usul ve esasların belirlenmesi...” şeklinde ifade edilmektedir. Bkz.: (Çevrimiçi), <http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/yonetmelik-10-11-2005-sayi-25989.pdf>, 10 Aralık 2006.

⁶⁶² A.e., Yönetmelik Madde 17/a.

gerçekleştirilen konuşmalar ve diğer her türlü iletişim dinlenmekte ve kayda alınmakta diğer bir ifade ile içeriğe müdahale edilmektedir.⁶⁶³

Önemli bir nokta da gecikmesinde sakınca bulunan hal ifadesidir. Gecikmesinde sakınca bulunan hal derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması halini,⁶⁶⁴ ifade etmektedir. Bu husus özellikle siber suçlar açısından büyük önem taşımaktadır. Siber suçların doğası gereği çok küçük zaman dilimleri dahi büyük bir önem taşımakta, bir veya daha fazla suçun işlenmesi, suç izlerinin ya da delillerin yok edilerek suçun saniyeler içerisinde tamamlanabilmektedir. Aynı şekilde siber suçlarda gerçek zamanlı trafik bilgilerinin elde edilmesi suçluların yakalanması için büyük bir önem taşımaktadır. Hakim kararı almak için geçecek süre bu kapsamda değerlendirildiğinde çok uzun bir süreyi ifade etmektedir. Bu nedenle, gecikmesinde sakınca bulunan hal ifadesi ile bir istisna oluşturulması bilişim suçları ile mücadelede faydalı bir tedbir olmuştur.

Yine CMK 137. madde kapsamında telekomünikasyon (telekomünikasyon terimi yukarıda açıklandığı anlamdadır) hizmeti veren kurum ve kuruluşların yetkililerine içerikle ilgili bilgilere müdahale edilmesi hususunda yükümlülük getirilmiştir.⁶⁶⁵ Buna göre cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi tarafından yazılı olarak iletişimin tespiti, dinlenmesi veya kayda alınması işlemleri ve bu amaçla cihazların yerleştirilmesi talep edildiğinde, bu isteği derhal yerine getirmek mecburiyetindedirler. Aksi halde zor kullanılabilir. Bu husus Sözleşmede öngörülen İSS'leri mevcut teknik imkânları çerçevesinde, içerik bilgilerini toplamaya veya yetkili mercilere bu konuda yardım etmeye ve işbirliğine zorlama şartını da sağlar niteliktedir.

Ulusal mevzuatta Sözleşme ile en uyumlu düzenleme içerikle ilgili bilgilere müdahale tedbiri ile ilgili olanıdır. Daha önce belirtildiği gibi haberleşme özgürlüğü ve özel hayatın gizliliğine en büyük müdahale olarak görülen bu tedbir için ulusal mevzuatta da sınırlamalar getirilmiştir. Öncelikle iletişimin tespiti dışında kalan dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesi tedbirlerinin

⁶⁶³ A.e., Yönetmelik Madde 3/l.

⁶⁶⁴ A.e., Yönetmelik Madde 3/d.

⁶⁶⁵ CMK Madde 137 "135 inci maddeye göre verilecek karar gereğince Cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi, telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılmasını ve bu amaçla cihazların yerleştirilmesini yazılı olarak istediğinde, bu istem derhâl yerine getirilir; yerine getirilmemesi hâlinde zor kullanılabilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır."

uygulanabileceği suçlar sınırlandırılmıştır. Bu düzenleme Sözleşme ile paralel bir uygulamadır. İşlenmiş olan suçlar, CMK'nın 135/6. maddesinde sayılanlardan değilse, veriler bu suçların aydınlatılmasında kullanılamayacaktır.⁶⁶⁶ Buna ilaveten TCK'nın 220. maddesinin iki, yedi ve sekizinci fıkralarında yer alan suçların bir terör örgütünün faaliyeti kapsamında işlenmesi hâlinde bu suçlar için de iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi tedbirlerine başvurulabilmektedir.⁶⁶⁷

CMK 135. maddede kuvvetli şüphe aranmaktadır. Bu şüphe bir kimsenin mahkûm olmasını kuvvetle muhtemel hale getiren şüphedir. Ayrıca, tedbir ancak başka yolla delil elde edilememesi durumunda uygulanabilecektir. Arama ve el koyma tedbirlerinin uygulama imkânı varken telefon dinleme yoluyla delil elde etme yoluna gidilemeyecektir. Tedbire başvurulduğu sırada olayın başka şekilde aydınlatılmasının imkânsız olduğunun bilinmesi gerekir. Ancak bunun için başka bir tedbire başvurup da sonuç alamamak gerekmez. Başka tedbire başvurulamayacağı ihtimali yeterlidir. Yani mahkûmiyeti gerektirecek kuvvetli deliller var ise burada yine bu tedbir kullanılamayacaktır. Son olarak ise Sözleşmeye paralel bir şekilde soruşturmanın başarısı için tedbirin gizli tutulması düzenlenmiştir.⁶⁶⁸

Ancak önemli bir husus göz ardı edilmiştir. Sıradan telefonlara göre bilgisayar iletişimi farklı teknik ve yöntemler gerektirmekle beraber; temelde telekomünikasyon

⁶⁶⁶ “CMK 135/6: Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir:

a) Türk Ceza Kanununda yer alan; Göçmen kaçakçılığı ve insan ticareti (madde 79, 80), Kasten öldürme (madde 81, 82, 83), İşkence (madde 94, 95), Cinsel saldırı (birinci fıkra hariç, madde 102), Çocukların cinsel istismarı (madde 103), Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188), Parada sahtecilik (madde 197), Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, madde 220), Fuhuş (madde 227, fıkra 3), İhaleye fesat karıştırma (madde 235), Rüşvet (madde 252), Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282), Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315), Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları.

b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları.

c) Bankalar Kanununun 22. maddesinin (3) ve (4) numaralı fıkralarında tanımlanan zimmet suçu,

d) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.

e) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.

(7) Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz...”

⁶⁶⁷ Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, 14 Şubat 2004 tarih ve 26434 sayılı Resmi Gazete, 10 Mart 2004, (Çevrimiçi), <http://rega.basbakanlik.gov.tr/eskiler/2007/02/20070214-11.htm>”.

⁶⁶⁸ CMK Madde 135/5. “ bu madde hükümlerine göre alınan karar ve yapılan işlemler, tedbir süresince gizli tutulur.”

yoluyla iletişime dayanmaktadır. Bu nedenle, İnternet yoluyla yapılan iletişimlerde de CMK'nın 135. maddesi kapsamına girmektedir.⁶⁶⁹ Ayrıca, daha öncede belirtildiği üzere ilgili yönetmelikte bulunan telekomünikasyon tanımı da bunu destekler niteliktedir. Bu durumda, İnternet üzerinden gerçekleştirilen haberleşmelerin, tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi sadece CMK'nın 135/6. maddesinde belirtilen suçlar için mümkün olmakta ve dolayısıyla yalnızca bu suçlara yönelik olarak elektronik ortamdaki deliller elde edilebilmektedir. Ancak, 135/6. maddede sıralanan suçlar arasında bilişim suçlarını bulunmamaktadır. Bu nedenle, TCK'nın bilişim alanında suçlar başlığı altında düzenlenen suçlar ve diğer bilişim suçları için sadece iletişimin tespiti mümkün olurken, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi mümkün olmamaktadır.⁶⁷⁰ Yine bu kapsamda, Sözleşmede trafik bilgisi olarak ifade edilen sinyal bilgilerinin değerlendirilememesi ise Sözleşmenin 20. maddesinde belirtilen tedbirin iç hukukta bilişim suçları açısından uygulanmasının mümkün olmadığı anlamına gelmektedir.

Neticede ulusal mevzuatta, usul hukuku kapsamında İnternet üzerinden yapılan iletişimlerde içerikle ilgili bilgilere müdahale etmeyi sağlayacak düzenlemenin, Sözleşmeye oranla oldukça yetersiz kaldığı değerlendirilmektedir.

(8) Madde 22-Yargı Yetkisi

Sözleşmenin bu maddesinde taraf devletlerin, Sözleşmenin 2 ilâ 11. maddelerinde belirtilen suçlar hakkında yargılama yetkisini düzenlerken uymaları gereken ölçütler belirtilmektedir.⁶⁷¹ Buna göre taraf devletler suç kendi ulusal sınırları içerisinde, bayrağını taşıyan hareket halindeki bir gemide, yasaları uyarınca kayıtlı bir hava aracında gerçekleştirildiğinde ve yine bir vatandaşı tarafından fiilin suç sayıldığı bir başka yerde ya da herhangi bir ülkenin yargı yetkisine sahip olduğu sınırlar dışında işlenmesi hallerinde yargılanmasını sağlayacak, yasal ve diğer düzenlemeleri yapacaktır.⁶⁷²

Bilişim suçları göz önüne alındığında yargı yetkisi bakımından üç ihtimal mevcuttur. Bunlardan ilki failin ve mağdurun taraf devletin sınırları içerisinde bulunmasıdır. Bu durumda yargılama yetkisi açısından bir sorun doğmayacaktır. İkincisi failin yurt dışında mağdurun taraf devletin sınırları içerisinde bulunması,

⁶⁶⁹ Karagülmez, *Bilişim Suçları ve Soruşturma...*, s.297.

⁶⁷⁰ A.y.

⁶⁷¹ Keskin, *a.g.e.*, s.177.

⁶⁷² Siber Suçlar Sözleşmesi Madde 22.

üçüncüsü ise mağdurun yurt dışında failin taraf devletin sınırları içerisinde bulunmasıdır. Son iki durumda yetki ihtilafının çıkması kaçınılmazdır.⁶⁷³

Sözleşme mülkilik ve şahsilik ilkelerini tek başına kabul etmemektedir. Ancak, mülkilik ve şahsilik ilkelerinin ikisinin de çeşitli durumlarda uygulanmasını öngörmektedir. Sözleşmeye göre mülkilik ilkesine uygun olarak taraf devletler, failin kendi vatandaşı olmasına bakmasızın ulusal sınırları içerisinde işlenen suçlarla ilgili yargılama yetkilerini kullanacaklardır.⁶⁷⁴ Taraf devletler, gerçek ülkesi yanında bayrağını taşıyan gemi ya da o ülke adına kayıtlı uçak gibi varsayılan ülkesi sınırları içerisinde işlenen suçlarla ilgili de yargılama yetkisini kullanacaktır.⁶⁷⁵ İşlenen bir suçta fail veya mağdur ya da fail olmasa bile yalnızca mağdur bir ülke sınırları içinde ise mülkilik ilkesine uygun olarak suç, o ülkede işlenmiş kabul edilecektir.⁶⁷⁶

Sözleşmenin kabul ettiği bir diğer ilke ise şahsilik ilkesidir. Bu ilkeye göre bir ülkenin vatandaşına, dünyanın neresinde olursa olsun vatandaşı olduğu devletin hukuk kurallarının uygulanması gerekmektedir.⁶⁷⁷ Buna göre bir ülke vatandaşı, başka bir ülkenin sınırları içerisinde suç işlediği takdirde, eğer söz konusu fiil işlendiği ülkede de suç sayılıyor ise ya da suçun işlendiği yer hiçbir ülkenin yargı yetkisinin bulunmadığı bir yer ise kendi ülkesi tarafından yargılanacaktır.⁶⁷⁸

Sözleşme ayrıca taraf devletlere sadece varsayılan devlet sınırları içerisinde işlenen suçlar ve şahsilik ilkesi konusunda hak saklı tutma imkânı da tanımaktadır. Bununla birlikte mülkilik ilkesi gereğince ulusal sınırlar içerisinde yargı yetkisi konusunda hak saklı tutma öngörülmemektedir. Yine “yargıla ya da iade et” ilkesine uygun olarak herhangi bir taraf ülkenin bir faili uyruğu dolayısıyla iade etmeyi reddettiği ve failin kendi ulusal sınırları içerisinde bulunduğu durumlarda, yargı yetkisi tesis etmekle ilgili olarak herhangi bir hak saklı tutmasına izin verilmemektedir. Bu durumda ya faili kendisi yargılamalı ya da iade etmelidir.⁶⁷⁹

Sözleşme, bilgisayar sistemlerinin kullanılmasıyla işlenen suçlarda faillerin bir kısmı ya da tamamı üzerinde birden fazla taraf devletin yargı yetkisi iddia ettiği durumlar olacağını öngörmektedir. Bu nedenle örneğin çoğu virüs saldırıları,

⁶⁷³ Özel ve Ahi, a.g.e., s.23.

⁶⁷⁴ Çeken, a.g.e., s.106.

⁶⁷⁵ Keskin, a.g.e., s.177.

⁶⁷⁶ Açıklayıcı Rapor, paragraf 233., Keskin, a.g.e., s.177.

⁶⁷⁷ Temel Hukuk Bilgisi, s.61.

⁶⁷⁸ Keskin, a.g.e., s.177.

⁶⁷⁹ Açıklayıcı Rapor, paragraf 237.

sahtecilik ve telif hakları ihlali suçları İnternet üzerinden işlendiği ve farklı ülkelerdeki kurbanlar hedef olmasından hareketle, aynı çabaların tekrarlanmasının, tanıkların gereksiz yere rahatsız edilmesinin önüne geçmek ve kovuşturmanın etkinliğine ve adilliğine katkıda bulunmak amacıyla tarafların kovuşturma için en uygun yeri bulmak konusunda birbirleriyle istişare etmelerini öngörmektedir.⁶⁸⁰

Sonuç olarak yargılama yetkisinin düzenlenmesi, hem tarafların işbirliği yapmalarını, hem de yargı yetkisinin dışında kalacak boşluk alanlarının kapatılmasını ve böylece işlenen bir suçta failin boşluktan istifade ederek suçun cezasız kalmasının engellenmesi bakımından önemli ve yerinde bir düzenlemedir. Kısaca mülkilik ve şahsilik ilkesi sayesinde suç işleyen bir fail, taraf devletlerden herhangi birinin sınırları içerisinde ise mülkilik ilkesine ya da şahsilik ilkesinden birine göre, eğer taraf devletlerin ya da herhangi bir ülkenin yargı yetkisi dışında bir yerde ise şahsilik ilkesine uygun olarak yargılabilecektir. Ancak suçun işlendiği ülkenin taraf devlet olmaması ya da mağdurun herhangi bir taraf devlet failin ise olmaması durumunda yine problem yaşanacaktır. Aslında sözleşmenin neden mümkün olduğunca çok sayıda devletin taraf olmasını amaçladığı da açıkça anlaşılmaktadır.

Türk hukukunda da düzenleme aynıdır.⁶⁸¹ TCK 8. maddesine⁶⁸² göre Türkiye’de işlenen suçlara yönelik olarak, Türk kanunlarının uygulanacağı belirtilmekte ve suçun kısmen ya da tamamen Türkiye’de işlenmesi veya neticenin Türkiye’de gerçekleşmesi durumunda suç Türkiye’de işlenmiş kabul edilmektedir. Fail olmasa dahi mağdur ulusal sınırlarda içinde ise suç Türkiye’de işlenmiş kabul edilmektedir ki bu düzenleme Sözleşmede belirtilen mülkilik ilkesinin aynısıdır.

Yine TCK’ya göre varsayılan ülke sınırları içerisinde işlenen suçlarda da Sözleşme ile paralel olarak yargı yetkisi düzenlenmiştir. Buna ilaveten TCK madde

⁶⁸⁰ Açıklayıcı Rapor, paragraf 239.

⁶⁸¹ Keskin, a.g.e., s.177.

⁶⁸² TCK Madde 8 “...(1) Türkiye’de işlenen suçlar hakkında Türk kanunları uygulanır. Failin kısmen veya tamamen Türkiye’de işlenmesi veya neticenin Türkiye’de gerçekleşmesi halinde suç, Türkiye’de işlenmiş sayılır.

(2) Suç;

a) Türk kara ve hava sahaları ile Türk karasularında,

b) Açık denizde ve bunun üzerindeki hava sahasında, Türk deniz ve hava araçlarında veya bu araçlarla,

c) Türk deniz ve hava savaş araçlarında veya bu araçlarla,

d) Türkiye’nin kıt’a sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı, işlendiğinde Türkiye’de işlenmiş sayılır...”

11, 12 ve 13'te vatandaş tarafından yurt dışında ve yabancılar tarafından işlenen suçlarla ilgili düzenlemeler Sözleşme ile birebir aynıdır.⁶⁸³

3. ULUSLARARASI İŞBİRLİĞİ

a. Genel İlkeler

Günümüzde küresel çaptaki telefon altyapısı üzerine kurulmuş olan İnternet'i kullanarak dünyanın herhangi bir yerinden, bir telefon bağlantısı ile yine dünyanın herhangi bir yerindeki bilgisayar sistemine erişmek mümkün hale gelmiştir. Bu sayededir ki bilgisayar suçları da siber uzayın sanal özelliğini edinmiş ve ülke sınırlarından ve zamandan bağımsız bir hal almıştır. Kablosuz sistemlerin ve uydu teknolojisinin yaygınlaşması ile yer kavramı, bilgisayar sistemlerinin haftanın her günü ve günün her saati erişim imkânı sağlayan yapısı ile de zaman kavramı önemini yitirmiştir. Dolayısıyla, siber suçlar, uluslararası bir nitelik kazanarak, bu suçları önlemeye ya da azaltmaya çalışan ülkeler için büyük güçlükler ortaya çıkarmaya başlamıştır.⁶⁸⁴ Uluslararası bilgisayar ağları, siber suçlarla mücadelede uluslararası işbirliğini kaçınılmaz hale getirmiştir.⁶⁸⁵

Uluslararası bilgisayar ağlarında iletilen bilgilerin miktarı, bunların içeriklerinin kontrol edilmesini imkânsız kılmakta ve toplumsal açıdan özel hayatın gizliliğinin ihlal edilmesine yol açması nedeniyle de tepki ile karşılanmaktadır. Bu nedenle, ulusal düzeyde oluşturulacak çözüm yöntemlerinin başarısızlıkla sonuçlanma ihtimali bulunmaktadır. Siber suçlarla mücadelenin ülkeler tarafından ulusal bazda bağımsız düzenlemeler yoluyla yapılmasının "siber suç cennetleri"nin oluşmasına, hepsinden önemlisi İnternetin temel getirisi olan bilginin serbest dolaşımının engellenmesine ve ülkeler için pazar kısıtlamalarına yol açması muhtemeldir. Bu nedenle siber suçlara uluslararası boyutta yaklaşmak ve çözüm bulmaya çalışmak diğer suç alanları ile karşılaştırıldığında daha fazla önem kazanmaktadır.⁶⁸⁶

Daha önce de belirtildiği gibi elektronik ortamdaki deliller, klasik suçlardaki delillere nazaran, bozulmaya, silinmeye veya değiştirilmeye çok müsaittir. Suçla ilgili bir kovuşturmanın birden fazla ülkeyi ilgilendirdiği durumlarda, soruşturma makamları yabancı meslektaşları ile işbirliği ve koordinasyon yapmaya ihtiyaç

⁶⁸³ Ayrıntılı bilgi için Bkz.: TCK'nın 11, 12 ve 13. maddeleri.

⁶⁸⁴ Garbys, a.g.e., s.23.

⁶⁸⁵ Sieber, a.g.e., s.32.

⁶⁸⁶ A.y.

duyacakları için ilave problemler ortaya çıkmaktadır. Bir suça ilişkin işe yarar delillerin toplanması, bazı ülkelerce bilgilerin yeterli süre ile ya da hiç tutulmaması nedeniyle daha karışık bir hal almaktadır. Bu durumda, yabancı makamların soruşturmayı devam ettirmesini veya işbirliği yapmasını sağlamak çoğunlukla kayda değer bir zaman ve çaba gerektirmektedir. Suçu aydınlatacak bir delil elde edildiği zaman ise bu delilin toplanması ile korunması eşit oranda önem taşıyacaktır. Elektronik delillerin özelliğinden dolayı, uygun adli yöntemler uygulanmadığında delillerin geçerliliği sağlanamayacaktır.⁶⁸⁷

Sözleşme uluslararası işbirliğinin, maddi ceza hukuku bölümünde belirtilen ve taraf ülkeleri suç olarak düzenlemesi zorunlu olan fiiller ve bilgisayar sistemleri ile ilgili diğer cezaî suçlar için geçerli olmasını öngörmektedir. Bununla birlikte herhangi bir klasik cezai suça ait delillerin elektronik ortamda bulunması durumunda da işbirliği geçerlidir. Diğer bir ifade ile bilgisayar sistemleri ya da bilgisayar sistemlerine karşı işlenen tüm suçlar veya cinayet, işkence vb. klasik suçlarda da elektronik ortamda delil bulunması halinde uluslararası işbirliği hükümleri uygulanabilmektedir. Ancak Madde 24 (İade), 33 (Trafik bilgilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma) ve 34'ün (İçerikle ilgili bilgilere müdahale edilmesi konusunda yardımlaşma) tarafların bu önlemlerin uygulamasında farklı bir kapsam benimsemelerine de izin verilmektedir.⁶⁸⁸

Sözleşme bu bölümde uluslararası işbirliğine yönelik hükümler getirmekle birlikte, taraflar arasında daha önceden yapılmış çok taraflı ya da iki taraflı diğer işbirliği anlaşmaları bulunmaktadır. Bu nedenle Sözleşmenin işbirliği hükümlerinin, taraflar arasında daha önceden yapılmış hukuki yardımlaşma ve iade ile ilgili uluslararası sözleşmelerin hükümlerinin, taraflar arasındaki karşılıklı sözleşmelerin ve ulusal mevzuatın uluslararası işbirliğiyle bağlantılı ilgili hükümlerinin yerine geçmeyeceği şeklindeki genel ilke açıkça ortaya konulmuştur. Sözleşmenin işbirliğine yönelik çok taraflı ya da iki taraflı diğer anlaşmaları ortadan kaldıran ya da onlara üstünlük sağlayan bir niteliği olmadığı belirtilmiştir.

(1) Madde 24-İade

Sözleşmeye göre iade ile ilgili yükümlülükler, yalnızca 2 ilâ 11. maddelerde belirtilen suçlar ve bu suçların her iki taraf ülke için en az bir yıllık özgürlükten

⁶⁸⁷ Garbys, a.g.e., s.29.

⁶⁸⁸ Açıklayıcı Rapor, paragraf 243.

mahrum bırakma ile cezalandırılabilir olması durumunda geçerlidir.⁶⁸⁹ Sözleşme suçları tanımlamasına ve taraf devletlerin her birinin ulusal hukuklarında suç olarak düzenlemesini öngörmesine rağmen uygulanacak cezalara ilişkin hükümler getirmemiştir. Taraf ülkeler bazı suçlar için bir yıldan daha kısa azami hapis cezaları belirleyebilirler. Dolayısıyla 2 ilâ 11. maddelerde belirtilen fillerin her zaman iadeye konu olması, Sözleşmeyi hazırlayanlar tarafından da uygun görülmemiştir.⁶⁹⁰

Bununla birlikte bir eşik cezanın getirilmesi kararlaştırılmış ve daha öce yapılan Sözleşmelerle uyum sağlanabilmesi açısından “Avrupa İade Sözleşmesi”nin (ETS No. 24)⁶⁹¹ 2. maddesinde öngörüldüğü gibi iadeye konu olan suç için azami cezanın en az bir yıl hapis olması şeklinde genel bir şart getirilmesi üzerinde anlaşılmıştır. Bir suç için verilecek ceza yasalarla öngörülen azami sınırın altında olabileceğinden, Sözleşme bir suçun iadeye konu olabilmesi için verilen gerçek cezanın değil, yasal olarak verilebilecek azami sürenin göz önüne alınmasını kararlaştırmıştır.⁶⁹²

Sözleşmede belirtilen bir yıllık ceza eşğine karşılık taraflar arasında hâlihazırda yürürlükte bulunan iki ya da çok taraflı iade anlaşmalarında farklı bir ceza eşği öngörülmesi durumunda bu anlaşmalarda öngörülen eşik geçerli olacaktır. Taraflar kendi aralarında hâlihazırda mevcut ve gelecekte yapacakları iade anlaşmalarına maddenin 1. paragrafı çerçevesinde tanımlanan cezai suçları da dahil edeceklerdir. Ancak, bu durum her iade talebinin karşılanacağı şeklinde değil, bu suçlar için kişilerin iade imkânının mevcut olması gerektiği anlamına gelmektedir.⁶⁹³

İade talep edilen bir ülke talep eden ülke ile arasında bir iade anlaşması bulunmaması veya mevcut anlaşmaların Sözleşmede belirtilen suçları kapsamaması nedeniyle iade talebini yerine getiremeyebilir. Bu durumda Sözleşme zorunluluk olmamak kaydıyla, iade talep edilen tarafın Sözleşmeyi iade için yasal dayanak olarak kullanabileceğini belirtmektedir. Yine taraflardan biri iade işlemini iade anlaşmalarına değil genel bir yasal plana bağlamış olabilir. Bu durumda,

⁶⁸⁹ Siber Suçlar Sözleşmesi Madde 24.

⁶⁹⁰ Açıklayıcı Rapor, paragraf 245.

⁶⁹¹ Söz konusu Sözleşme ve Ek Protokolleri Türkiye tarafından 13 Aralık 1957 tarihinde imzalanmıştır. Ayrıntılı bilgi için Bkz.: <http://conventions.coe.int/Treaty/en/Treaties/Html/024.htm>.

⁶⁹² Açıklayıcı Rapor, paragraf 245.

⁶⁹³ Açıklayıcı Rapor, paragraf 246-247.

Sözleşme taraf devletin iadenin mümkün olduğu suçlara 1. paragrafta tanımlanan suçların da dahil edilmesini şart koşmuştur.⁶⁹⁴

Sözleşme 24/5. maddede, iade talep edilen tarafın eğer talep eden tarafın geçerli anlaşma ve yasalardaki bütün hüküm ve şartların yerine getirildiği konusunda tatmin olmamışsa iade talebini geri çevirebileceğini belirtmektedir. Bu husus, işbirliğinin taraflar arasında yürürlükte bulunan geçerli uluslararası araçların, karşılıklı düzenlemelerin ya da ulusal yasaların hükümleri uyarınca gerçekleştirilmesi gerekliliği ilkesi için diğer bir örnektir.⁶⁹⁵ Avrupa İade Sözleşmesi'nin 3. Maddesinde, suçun siyasi nitelikli olduğuna ya da iade talebinin kişiyi, başka şeylerin dışında, ırk, din, milliyet veya siyasi görüşü nedeniyle kovuşturmak ya da cezalandırmak amacıyla yapıldığına karar verildiğinde iadenin reddedileceğinin belirtilmiş olması, bu hususa bir örnektir.⁶⁹⁶

Siber suçların geneline bakıldığında, failerin sıklıkla diğer ülkelerdeki kişilere karşı suç işlemeyi tercih ettiği görülmektedir. Bu durum her ülkenin bu şekilde işlenen bir suçu kovuşturmaya ya da suçluyu mağdurun yaşadığı ülkeye iade edecek düzenlemeye sahip olmaması durumunda, bu ülkeyi suçlular için korunaklı bir suç cenneti haline getirmektedir.⁶⁹⁷ Bu şekilde suçlular ve suç için oluşması muhtemel boşlukları kapatmak amacıyla Sözleşmenin iade ile ilgili olarak düzenlediği bir başka husus ise "yargıla ya da iade et" ilkesidir. Genellikle birçok ülke kendi vatandaşları ile ilgili olarak başka bir ülkede işledikleri suçtan dolayı yapılan iade talebini geri çevirmekte ve yerel merciler gerekli kovuşturma işlemlerini yapmaya zorlanmazlarsa, başka ülkede işlenen suçlar cezasız kalabilmektedir. Sözleşme söz konusu ilke ile herhangi bir taraf ülkenin iade talebini failin vatandaşı olması nedeniyle geri çevirmesi durumunda, iade talep eden ülkenin isteği üzerine, kovuşturulmak üzere vakayı kendi ülkesindeki ilgili mercilere sevk etmek zorundadır. İade talebi reddedilen taraf vakanın yerel soruşturma ve takibat için sevkini talep etmezse, talebin yapıldığı taraf kendiliğinden hukuki işlem yapmak zorunda değildir. Buna ilaveten, iade talebi yapılmadıysa ya da iade uyruk dışındaki nedenlerden geri çevrildiyse, talebin yapıldığı tarafın vakayı ulusal kovuşturmaya sevk etmesi için bir yükümlülük getirilmemektedir.⁶⁹⁸

⁶⁹⁴ Sözleşme Madde 24/3-4.

⁶⁹⁵ Çeken, a.g.e., s.115.

⁶⁹⁶ Açıklayıcı Rapor, paragraf 250.

⁶⁹⁷ "Cybercrime Laws, Prevention and Enforcement Capacity Builds", s.121.

⁶⁹⁸ Açıklayıcı Rapor, paragraf 251.

İç hukukumuzda bir Türk vatandaşının yurt dışında suç işlemesi durumunda ya da bir yabancıların Türkiye’de ya da yurt dışında Türkiye aleyhine suç işlemesi durumunda geçerli olacak uygulama TCK’nın 9, 10, 11, 12 ve 13. maddelerinde ayrıntılı olarak düzenlenmiştir. İadeye ilişkin hükümler ise TCK Madde 18’de⁶⁹⁹ Geri verme başlığı altında düzenlenmiştir. Mevcut ulusal düzenlemenin Türkiye’nin zaten taraf olması nedeniyle, Sözleşme’nin uygulanmasında esas alınması öngörülen Avrupa İade Sözleşmesine, paralel olduğu, dolayısıyla Sözleşmenin iadeye yönelik hükümleri ile de bağdaştığı görülmektedir.

(2) Madde 25-Yardımlaşmaya İlişkin Genel İlkeler

Yardımlaşmayla ilgili genel ilkeler, 23. maddede belirtildiği şekilde mümkün olan en geniş biçimde, hem bilgisayar sistemleri ve verileriyle bağlantılı suçlar hem de bir cezai suçun elektronik ortamdaki delillerinin toplanması için geçerlidir.⁷⁰⁰ Sözleşme tarafların yardımlaşmayı hâlihazırda geçerli olan yardımlaşma anlaşmaları, yasaları ve düzenlemeleri çerçevesinde yürütmelerini öngörmektedir. Ancak, tarafların mevcut düzenlemeleri bu tür hükümler içermiyorsa yardımlaşmanın sağlanabilmesi için Sözleşme ile öngörülen yasal düzenlemeleri yapacaktır.⁷⁰¹

Sözleşme acil durumlarda taraflar arasında yardım taleplerinin ve cevaplarının süratli biçimde iletebilmesini amaçlamaktadır. Bu nedenle, taraflara acil işbirliği taleplerini yazılı, mühürlü evrakların iletilmesi gibi geleneksel yöntemler yerine, daha hızlı yöntemlerle yapma yetkisi verilmekte ve cevap verilirken de aynı yöntemin kullanılması şart koşulmaktadır. Ayrıca yardım talep edilen tarafa sonradan geleneksel yöntemlerle resmi bir onay gönderilmesini isteme hakkı da sağlanmaktadır. Faks ve e-posta adreslerinin listelenmesi bu yeterliliğin göstergesidir. Taraflar yardımlaşma esnasında gerçekleştirecekleri iletişimin

⁶⁹⁹ TCK Madde 18. “...(1) Yabancı bir ülkede işlenen veya işlendiği iddia edilen bir suç nedeniyle hakkında ceza kovuşturması başlatılan veya mahkumiyet kararı verilmiş olan bir yabancı, talep üzerine, kovuşturmanın yapılabilmesi veya hükmedilen cezanın infazı amacıyla geri verilebilir. Ancak, geri verme talebine esas teşkil eden fiil;

a) Türk kanunlarına göre suç değilse,

b) Düşünce suçu veya...

(2) Uluslararası ceza Divanına taraf olmanın gerektirdiği yükümlülükler hariç olmak üzere, vatandaş suç sebebiyle yabancı bir ülkeye verilemez...”

⁷⁰⁰ Açıklayıcı Rapor, paragraf 253.

⁷⁰¹ Açıklayıcı Rapor, paragraf 254-255.

doğruluğu ve güvenliğinin sağlanması için gerekli olabilecek koruma yöntemlerine karar verebilmektedir.⁷⁰²

Sözleşmede düzenlenen bir diğer husus yardımlaşmanın geçerli yardımlaşma anlaşmalarının ve ulusal yasaların hükümlerine tabi olduğudur. Kısaca talebin yapıldığı taraf ülkedeki ulusal bir vaka için geçerli olan temel şartlar yerine getirilmedikçe, talebi yapan taraf adına arama ve el koyma gibi müdahaleci önlemler gerçekleştirilememektedir. Taraflar hukuki yardımlaşma yoluyla el konan ve ilgili tarafa sağlanan eşyalarla ilgili olarak, kişilerin haklarının korunmasını da güvence altına alabilmektedir.⁷⁰³

Sözleşmede düzenlenen diğer iki önemli husus taraflar arasında geçerli bir yardımlaşma anlaşması olmadığı durum ve çifte suçluluk halidir. Taraflar arasında yardımlaşma anlaşması veya eşdeğer bir düzenleme bulunmadığı durumlarda, taleplerin uygulanması için talebin yapıldığı tarafın ulusal mevzuatındaki uluslararası işbirliği ile ilgili hükümlerin yerine Sözleşmenin 27. maddesinde bulunan hükümler geçerli olmaktadır. Çifte suçlulukta ise talebin yapıldığı taraf yardım için çifte suçluluğu şart olarak ileri sürdüğünde, suça konu fiili yardım talep eden tarafın yasalarında başka bir suç kategorisine yerleştiriliyor ya da suçu adlandırmak için farklı bir terminoloji kullanıyor olsa bile, çifte suçluluğun geçerli olduğu kabul edilmektedir.⁷⁰⁴

(3) Madde 26-Anında İletilen Bilgiler

Bir ülkenin, bir diğer ülkenin herhangi bir suça yönelik soruşturmasında yardımcı olabileceğine inandığı çok değerli bilgilere sahip olması ve soruşturmayı yürüten tarafın bu bilginin varlığından haberdar olmaması durumuyla giderek daha fazla karşılaşılacaktır. Sözleşme, taraflara var olan bilgiyi talep edilmeksizin, yardımı olacağı düşünülen ülkeye aktarma yetkisi vermektedir. Bu düzenleme, yasaları gereği talep edilmediği sürece bu tarz bilgileri, diğer ülkelere aktaramayan ülkelerin yardımlaşma yapabilmelerine zemin sağlamaktadır. Bu nedenle, siber suçlarla mücadele açısından oldukça faydalı görülmektedir.⁷⁰⁵

⁷⁰² Açıklayıcı Rapor, paragraf 256.

⁷⁰³ Açıklayıcı Rapor, paragraf 257-258.

⁷⁰⁴ Açıklayıcı Rapor, paragraf 259.

⁷⁰⁵ Çeken, a.g.e., s.116.

Bununla birlikte tarafların bilgiyi diğer tarafa anında iletmek gibi bir yükümlülükleri bulunmamaktadır. Bu konuda durumun gerektirdiği şartlar ışığında takdir haklarını kullanabileceklerdir.⁷⁰⁶ Bilginin ifşa edilmesi, bilgiyi veren ülkenin önemli çıkarlarını tehlikeye sokabilir, bilgi toplama yönteminin açığa çıkmasına neden olabilir ya da bir suç örgütü ile ilgili soruşturmanın gizliliğini ihlal edebilir. Sözleşme bu gibi durumlarda bilgiyi ifşa eden tarafın çeşitli şartlar ileri sürülebilmesini öngörmektedir. Bilgiyi alan tarafın, örneğin bilginin kamuya açık bir duruşmada delil olarak kullanılması şeklinde gizlilik şartına uymayacağını anlaşılmaması durumunda, bunu karşı tarafa bildirmesi gerekmektedir. Bu durumda karşı taraf bilgiyi vermeme seçeneğine sahip olacaktır. Bununla birlikte, bilgiyi alan taraf şartı kabul etmişse sözünde durmalıdır.⁷⁰⁷

Sözleşmenin bu maddesi, Suçlardan Elde Edilen Kazançların Aklanma, Aranma, El Konma ve Müsaderesiyle İlgili Konvansiyon'un (ETS No. 141) 10. Maddesi ve Yolsuzlukla İlgili Ceza Hukuku Konvansiyonu'nun (ETS No. 173) 28 Maddesi gibi geçmiş Avrupa Konseyi araçlarındaki hükümlerden türetilmiştir.⁷⁰⁸ Türkiye bu konvansiyonların ilkinde 27 Eylül 2001 tarihinde⁷⁰⁹, diğerine ise 27 Ocak 2001 tarihinde⁷¹⁰ taraf olmuştur.

(4) Madde 27-Uluslararası Anlaşmaların Olmadığı Durumlarda Gelen Yardım Taleplerine İlişkin Usuller

Sözleşme bu maddede yardımlaşmanın, taraflar arasında hâlihazırda var olan tek taraflı veya karşılıklı yardımlaşma anlaşmaları ile yürütülmesi genel ilkesini pekiştirmektedir. Bu gibi düzenlemeler bulunmadığı takdirde, yardımlaşmayı düzenleyen ulusal yasalar yerine, bu maddenin hükümlerinin uygulanması öngörülmektedir. Sözleşmede, ayrı bir yardımlaşma rejimi oluşturulmak yerine, mevcut yardımlaşma anlaşmalarının esas alınması tercih edilmiştir. Böylece, tarafların bilinen araç ve düzenlemeleri kullanmaları suretiyle, birbirine karşıt rejimlerin tesis edilmesinden doğacak karışıklığın engellenmesi amaçlanmaktadır.⁷¹¹

⁷⁰⁶ Açıklayıcı Rapor, paragraf 260.

⁷⁰⁷ Açıklayıcı Rapor, paragraf 261.

⁷⁰⁸ Açıklayıcı Rapor, paragraf 260.

⁷⁰⁹ Ayrıntılı bilgi için Bkz.: <http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm>

⁷¹⁰ Ayrıntılı bilgi için Bkz.: <http://conventions.coe.int/Treaty/en/Treaties/Html/173.htm>

⁷¹¹ Açıklayıcı Rapor, paragraf 262.

Sözleşmenin bu maddesinde belirtilen yardımlaşma biçimlerinin çoğu Avrupa Cezai Konularda Yardımlaşma Konvansiyonu (ETS No. 30) ve Protokolü (ETS No. 99)'nden alınmıştır.⁷¹² Dolayısıyla Sözleşmede yardımlaşmanın taraflarca söz konusu sözleşmeye göre yürütülmeye devam edileceği belirtilmiştir. Bununla birlikte Sözleşme'deki hükümler, taraflar arasında mevcut ikili ya da çok taraflı anlaşmalara üstünlük sağlamamaktadır. Taraflardan Sözleşmenin yardımlaşmaya dayalı hükümlerini uygulamak istemedikleri takdirde, mevcut yardımlaşma anlaşmalarını siber suçlara da uygulanacak şekilde geliştirmeleri istenmektedir. Bu durum gelecekte yapılacak tek taraflı ya da karşılıklı yardımlaşma anlaşmaları için de geçerlidir.⁷¹³

Sözleşme yardımlaşmanın nasıl yapılacağına dair tarafların ulusal mevzuatlarına yönelik herhangi bir hüküm getirmemektedir. Örneğin, yapılacak olan talebin şekli ve içeriği, tanık ifadelerinin nerede alınacağı, resmi ya da ticari kayıtların sağlanması, tanıkların nakledilme yöntemi gibi konularda hüküm içermemektedir. Sözleşmenin daha önce incelenen 25. maddesinde, bu bölümde açıkça belirtilen durumlar dışında, bu tür yardım sağlanması ile ilgili belirli konuların yardım talebinde bulunan tarafın ulusal mevzuatına göre düzenleneceği belirtilmiştir.⁷¹⁴

Sözleşme siber suçlarla mücadelede çok önemli bir husus olan süratli tepkinin sağlanması amacıyla, tarafların cezai konularda yardımlaşmanın modern araçlarından biri olarak görülen merkezi yetkili merciler kurmalarını öngörmektedir. Bu sayede hem diplomatik kanallara göre daha hızlı olunacağı, hem de yardımlaşma ile ilgili gelen ve giden taleplerin titizlikle takip edilmesinin sağlanacağı değerlendirilmiştir.⁷¹⁵

Yardımlaşma ile ilgili konuların en önemlisi çoğu zaman elde edilen delilin, yardım talep eden ülkenin yasalarına göre kabul edilebilirliğinin sağlanması, yani yasalara uygun olarak elde edilmesidir. Aksi takdirde, delil mahkemede

⁷¹² Avrupa Cezai Konularda Yardımlaşma Konvansiyonu (ETS No. 30) Türkiye tarafından 23 Ekim 1959 tarihinde ve Protokolü (ETS No. 99) ise 04 Şubat 1986 tarihinde imzalanmıştır.

Ayrıntılı Bilgi İçin Bkz.: "<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CM=8&DF=3/13/2007&CL=ENG>", "<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=099&CM=8&DF=3/13/2007&CL=ENG>".

⁷¹³ Açıklayıcı Rapor. paragraf 263.

⁷¹⁴ Açıklayıcı Rapor. paragraf 264.

⁷¹⁵ Açıklayıcı Rapor, paragraf 265.

kullanılamamaktadır.⁷¹⁶ Bunu sağlamak için Sözleşme, talepte bulunulan ülkenin yasalarına aykırı olmadığı sürece uygulamanın talebi yapan tarafın belirlediği usullere göre yapılmasını şart koşmuştur. Bu hususun yalnızca teknik usul şartlarıyla ilgili olduğu, temel usul korumalarıyla ilgili olmadığına altı özellikle çizilmektedir. Örneğin, talebi yapan tarafın usul kanunları çerçevesinde tanık ifadelerinin yeminli olarak anılması şartı olabilir. Bu durumda talebin yapıldığı taraf kendi usul kanunlarında böyle bir düzenleme olmasa dahi tanık ifadesini yeminli olarak almalıdır.

Sözleşme taraf devletlere yardım taleplerini belirli durumlarda reddetme olanağı da tanımıştır. Yardım talep edilen devletin egemenliğine, güvenliğe, kamu düzenine ve diğer temel çıkarlarına zarar gelmesi ya da siyasi bir suç veya siyasi bir suçla bağlantılı bir suç olarak görüldüğü durumlarda yardımlaşma talebi reddedilebilir. Ancak, bu durumda dahi sözleşme bu ret gerekçelerinin daha önce de belirtilen “mümkün olan en geniş biçimde işbirliği” ilkesini engellemeyecek şekilde dar tutulmasını istemektedir. Bu gerekçeler, dışında veri koruma gerekçeleri de yardımlaşma talebinin reddedilmesine neden olabilir. Bu durumda da yardımlaşmanın sağlanabilmesi için veri koruma ilkelerinin geniş, kategorik ya da sistematik bir uygulamasını benimsemek engellenmelidir.⁷¹⁷ Yardımlaşma amacıyla talep eden tarafa sağlanan veriler gizli ya da kişisel veriler olabilir ve bunların yalnızca talep edildiği amaç için kullanılması, korunması ve saklanmasına gerek kalmadığı zaman süratle yok edilmesi gerekebilir. Dolayısıyla talep eden tarafın bunları sağlayacak düzenlemelerinin talep edilen tarafa nazaran farklı yöntemler olması yardımlaşma talebinin reddedilmesi için başlı başına gerekçe olmamalıdır. Burada yeri gelmişken çok kısa bir şekilde Türkiye’de TCK’da belirtilen birkaç madde haricinde, ne kişisel verilerin korunması ne de ulusal bilgi güvenliği konusunda detaylı bir düzenleme ya da ayrı bir kanunun hâlihazırda bulunmadığını belirtmek gerekir. Bu durumun yardımlaşma talepleri konusunda Türkiye’nin önüne engeller çıkarması muhtemeldir.

Bunun yanında yardım taleplerinin derhal karşılanmasının talebin yapıldığı taraftaki bir soruşturma ve kovuşturma açısından olumsuz etkiler yaratma olasılığı bulunabilir. Bu durumda yardım talep edilen taraf, yardımı reddetmek yerine bir

⁷¹⁶ Ayrıntılı Bilgi İçin Bkz.: CMK. Madde 206 Delillerin Ortaya Konulması ve Reddi “... Ortaya konulması istenen bir delil aşağıda yazılı hallerde reddolunur:

- a) Delil, kanuna aykırı olarak elde edilmişse,
- b) Delil ile ispat.....”

⁷¹⁷ Açıklayıcı Rapor, paragraf 268.

takım koşullar tamamlanıncaya kadar yardımı erteleyebilmektedir. Ancak, reddetme veya erteleme sebebi talep eden tarafa bildirilmelidir. Böylece, talep eden tarafın talebini karşılanabilecek tarzda yeniden yapılandırması sağlanabilir.⁷¹⁸ Daha sonraki taleplerinde, karşı tarafın bu maddeyi nasıl yorumladığını anlayarak, talebini başlangıçta karşılanacak şekilde gerçekleştirmesi ve yardımlaşmanın etkinliğinin artırılması sağlanabilir.⁷¹⁹

Benzer şekilde, yardım talebinin konusunun, talebi yapan taraf açısından çok hassas bir konu olması veya zamanından önce kamuya açıklanmasının kötü sonuçlar yaratması mümkün olabilir. Sözleşme, talepte bulunan tarafa, talebin ve içeriğinin gizli tutulması isteme etme hakkı sağlamaktadır. Ancak, bu gizliliğin bizzat talebin gerçekleştirilmesini imkânsız kılması da mümkün olabilir. Yardım talebinin karşılanabilmesi için mahkeme kararı ya da delili elinde bulunduran kişilerin talepten haberdar edilmesi gerekebilir. Bu gibi durumlarda talep ifşa olacaktır. Bu nedenle Sözleşme, talebi yapan tarafın talebi geri çekme ya da değiştirme konusunda karar verebilmesi için bundan haberdar edilmesini öngörmektedir.⁷²⁰

Sözleşmenin tesis edilmesini öngördüğü yetkili merciler yardımlaşma amacıyla doğrudan haberleşebileceklerdir. Bununla birlikte acil hallerde, yardımlaşma talepleri hakim ve savcılar arasında doğrudan yapılabilecektir. Bu tarz bir yardımlaşmada talebi yapan hakim veya savcı, karşı tarafın yetkili merciine iletmek üzere talebin bir kopyasını kendi yetkili merciine de gönderecektir. Yardım talebinde bulunan taraf, talebin yetki sınırlarını aşması ve üçüncü tarafları ilgilendirmesi durumunda, talebi üçüncü tarafın yetkili merciine iletmek ve talebi yapan tarafın yetkili mercilerini bu iletim konusunda bilgilendirmek zorundadır.⁷²¹

(5) Madde 28-Kullanımda Gizlilik ve Sınırlama

Kullanımda gizlilik ve sınırlama ile ilgili düzenleme bir önceki maddede belirtildiği gibi bu konu ile ilgili taraflar arasında iki ya da çok taraflı anlaşmaların bulunmadığı durumlarda geçerlidir. Yürürlükte böyle bir anlaşma bulunduğu takdirde ve taraflar aksine bir karar almadıkları sürece, bu madde hükümleri yerine mevcut anlaşma hükümleri uygulanacaktır.

⁷¹⁸ Çeken, a.g.e., s.118.

⁷¹⁹ Açıklayıcı Rapor, paragraf 272.

⁷²⁰ Açıklayıcı Rapor, paragraf 273.

⁷²¹ Açıklayıcı Rapor, paragraf 274.

Sözleşme yardımlaşma talep edilen tarafın, bilgi ya da materyallerin hassas olduğunu durumlarda, bunların kullanımının yardımın sağlanma gerekçesiyle sınırlı tutulmasını ya da talebi yapan tarafın icra görevlilerinin dışında kimseye açıklanmamasını sağlamak amacıyla sınırlamalar getirmesine imkân vermektedir. Bu sınırlamalara veri güvenliği de içermektedir.⁷²² Dolayısıyla yardım talep eden taraf, bilgi güvenliği kapsamında kendisine sağlanan verilerin herhangi bir şekilde başkalarının eline geçmesini engelleyecek güvenlik tedbirlerini de almak zorundadır.

Sözleşmeye göre yardımlaşma talep edilen taraf, bu talebin yerine getirilmesi için iki tür şart ileri sürebilmektedir. Birincisinde talep edilen taraf, talep eden tarafın kendisinden istenen şartlara uymasının mümkün olmadığı durumlarda (örneğin gizli bir bilgi kaynağının açıklanmaması gibi), sağlanan bilginin gizli tutulmasını isteyebilmektedir. İkincisinde ise bilgi ve materyallerin sağlanmasını, isteğin yapılmasına neden olan soruşturma ve kovuşturma dışında kullanılmaması şartına bağlayabilmektedir.⁷²³

Bu nedenle, talepte bulunan taraf eğer bilgiyi sağlayan tarafın şartlarını yerine getiremiyorsa, bilgiyi sağlayan tarafın bilgiyi sağlamama seçeneğini kullanabilmesi için bunu bildirmelidir. Aksi halde şartları kabul etmişse buna uygun olarak davranmak ve şartları yerine getirmek zorundadır. Bunun yanında bilgiyi sağlayan taraf, talep eden tarafa bilgiyi kullanım biçimini açıklama şartı da getirebilmektedir.⁷²⁴

Sözleşme bu düzenleme ile yardımlaşma ile taraflara getirilen yükümlülüklerin arzu edilen fayda ile orantılı olmasını amaçlamaktadır. Yardımlaşma ile bir tarafa fayda sağlanırken, yardım eden tarafın çıkarlarının zarar görmesi ihtimali her zaman bulunmaktadır. Bu durumda yardımın mecburi olması gibi bir yükümlülüğün getirilemeyeceği açıktır. Dolayısıyla Sözleşme, yardımlaşma için taraflara bu gibi durumlarda şart koşabilmeyi ve tarafların sağlayacakları faydalar arasında denge kurmayı amaçlamaktadır. Örneğin bir taraf devletin uzun süredir gizli olarak yürüttüğü bir kovuşturmada elde edilen bilgilerin, talep üzerine başka bir tarafa sağlanması ve bu bilgilerin kamuoyuna açık bir davada kullanılarak ifşa edilmesi durumunda, yardımlaşma fayda sağlamak yerine zarara neden olabilecektir.

Görüldüğü üzere Sözleşme var olan düzenlemelerin yerine yenisini tesis etme ve yürürlükten kaldırma tarzında zorlayıcı bir üslubu ve yöntemi kullanmak yerine,

⁷²² Açıklayıcı Rapor, paragraf 275.

⁷²³ Açıklayıcı Rapor, paragraf 277-278.

⁷²⁴ Açıklayıcı Rapor, paragraf 279-280.

tarafların var olan alışlageldik ikili ya da çok taraflı sözleşmeleri kullanmalarına imkân sağlamaktadır. Taraflar arasında uygulanan bir düzenlemenin bulunmaması durumunda boşluğu doldurabilmek için taraflara bir araç sunmaktadır. Ayrıca yardım taleplerinin karşılanması konusunda mutlak bir zorunluluk getirmemekte, özellikle güvenlik konusunda hem talepte bulunan hem de bulunulan tarafa gizlilik ve sınırlama getirme hakkı tanımaktadır. Bu şekli ile Sözleşmenin uluslararası işbirliğinin genel ilkeleri çerçevesinde güvenlik hassasiyetlerini göz önünde bulundurduğu değerlendirilmektedir.

b. Özel Hükümler

Bu kısmın amacı siber suçlar ve elektronik biçimdeki delillerin söz konusu klasik suçlarda, daha önceki bölümlerde belirtilen uluslararası alanda güçlüklerin giderilmesi, birlikte ve etkin bir şekilde eyleme geçilebilmesi için gerekli belirli mekanizmaları sağlamaktır.

Bu bölümde Sözleşme usul hukukuna ilişkin olarak ulusal düzeyde alınacak önlemlerin, uluslararası düzeyde de alınmasını öngörmekte ve buna yönelik hükümleri düzenlemektedir.

(1) Madde 29-Depolanmış Bilgisayar Verilerinin Korunmasının Kolaylaştırılması

Bu madde usul hukukuna yönelik ulusal düzeyde yapılması öngörülen düzenlemelerin sağladığı mekanizmanın uluslararası düzeyde de tesis edilmesini öngörmektedir. Bu sayede her bir taraf devlete kendi sınırları ve yargı yetkisi dışında olsa da başka bir taraf devletin sınırları içerisindeki bir bilgisayar sisteminde saklanan verilerin hızlı bir şekilde korunmasını sağlayacak yasal imkân verilmektedir. Burada amaç yine ileride yapılacak bir kovuşturma ile ilgili, faile ulaşılmasını sağlayabilecek veya delil olarak kullanılacak verilerin yardımlaşma için gerekli işlemler gerçekleştirilinceye kadar değişmeden, bozulmadan ve silinmeden korunmasını sağlamaktır.⁷²⁵

Bilgisayar verilerinin daha önce de bahsedilen hassas özellikleri ve bazı durumlarda çok kısa süreli olarak saklanmaları gerekliliğinin ortaya çıkardığı

⁷²⁵ Açıklayıcı Rapor, paragraf 282.

güçlükler nedeniyle, koruma klasik yardımlaşma faaliyetlerine nazaran çok daha hızlı yürütülmesi gereken sınırlı ve geçici bir önlemdir.⁷²⁶

Bu önlem sıradan yardımlaşma uygulamalarına nazaran çok daha hızlı olmasına ilaveten en az müdahaleci olma avantajına da sahiptir. Bunun nedeni koruma talebinin, korunan bilgilerin yardımlaşma görevlileri tarafından koruyucusundan alınmasını gerektirmemesidir. Tam ifşa ölçütleri yerine getirilmeden önce herhangi bir devlet görevlisi verilerin içeriğine erişememekte ve bu sayede verilerin ilgili olduğu şahsın gizliliği ihlal edilmemektedir.⁷²⁷

Koruma önlemin mümkün olduğunca hızlı uygulanması gerektiğinden yola çıkarak, talep süratle iletilebilecek ve mümkün olduğunca açık, kısa bir şekilde gerekli özet bilgileri ihtiva edecek şekilde hazırlanmalıdır. Bunun yanında talep eden taraf korunan verilerin üretiminin yapılabilmesi için koruma talebini müteakip bir karşılıklı yardımlaşma isteğinde bulunacağı garantisini vermelidir.⁷²⁸ Bunun, Sözleşmenin koruma önlemini daha öncede belirtildiği gibi sınırlı ve geçici bir önlem olarak kabul etmesinden kaynaklandığı ve lüzumsuz koruma talepleri neticesinde ortaya çıkacak gereksiz işlem yoğunluğun engellenmesi amacını taşıdığı değerlendirilmektedir.

Sözleşme koruma önleminin uygulanması için çifte suçluluk şartının gerekçe olarak aranamayacağını belirtmektedir. Koruma hususunda çifte suçluluğun uygulanması aslında engelleyici bir tavidir. Birincisi modern yardımlaşma uygulamalarında, arama ve el koyma, iletişimin dinlenmesi gibi en müdahaleci yöntemler dışında kalanların tamamı için çifte suçluluğun kaldırılması yönünde bir eğilim bulunmaktadır. Dolayısıyla yukarıda da açıklandığı üzere müdahaleci bir nitelik taşımayan, korunan verilerin içeriğine müdahale edilmesine olanak tanımayan, sadece koruyucunun zaten mülkiyetinde bulunan bilgileri korumaya devam etmesini öngören koruma önleminde çifte suçluluğu öne sürmek mantıklı olmayacaktır. İkinci olarak, uygulamada çifte suçluluğun varlığının kesin olarak belirlenebilmesi amacıyla gerekli açıklamaları sağlamak için geçecek süre çoğunlukla çok uzun bir süre olacaktır. Bu süre içerisinde veriler hızla korunmaz ise suçun niteliği anlaşılincaya kadar ilgili veriler çoktan bozulmuş, değiştirilmiş ya da silinmiş olacak ve veriler geri elde edilemeyeceğinden fail de asla yakalanamayacaktır.

⁷²⁶ A.y.

⁷²⁷ Açıklayıcı Rapor, paragraf 283.

⁷²⁸ Açıklayıcı Rapor, paragraf 284.

Sözleşme çifte suçluluk konusunda getirdiği düzenlemeye rağmen taraflara hakkın sınırlı bir biçimde saklı tutulması imkânını tanımıştır. Buna göre tarafların öncelikle üretime yönelik yardım taleplerine cevap vermek için çifte suçluluğu şart koşuyor olmaları gerekmektedir. Bu durumda ifşa zamanında çifte suçluluk şartının karşılanmayacağına inanmak için nedenleri de mevcutsa korumanın önkoşulu olarak çifte suçluluğu şart koşma hakkını saklı tutabilmektedirler. Taraflar bu şartı sadece Konvansiyonda tanımlananlar dışındaki suçlarla ilgili olarak getirebilirler.⁷²⁹

Bununla birlikte taraflar Sözleşmeyi imzalamış olduklarından ve Sözleşmenin 2 ilâ 11. maddelerinde belirtilen suçların her biri tarafından suç kabul edilmiş olmasından dolayı çifte suçluluk şartının otomatik olarak sağlandığı kabul edilmektedir.⁷³⁰

Sözleşme taraf devletlerin koruma taleplerini, devletin egemenliğine, güvenliğe, kamu düzenine ve diğer temel çıkarlarına zarar gelmesi ya da siyasi bir suç veya siyasi bir suçla bağlantılı bir suç olarak görüldüğü durumlarda reddedebilmelerini öngörmektedir. Bununla birlikte korumanın bilişim suçlarının önlenmesi hususunda en temel önlem olmasından dolayı başka bir gerekçe ile reddedilemeyecektir.

Bazen korumanın talep edildiği taraf verilerin koruyucusunun talepte bulunan tarafın soruşturmasının gizliliğini tehdit edebileceğini ya da başka bir şekilde zarar verebileceğini fark edebilir (örneğin koruyucu durumundaki hizmet sağlayıcının bir suç örgütü ya da bizzat soruşturmanın hedefi tarafından kontrol edildiği durumlarda). Böyle bir durumda koruma talep edilen taraf, koruma talebinin yaratacağı riski almayı veya üretim ya da arama ve el koyma gibi karşılıklı yardımlaşmanın daha müdahaleci fakat güvenli şeklini isteme seçeneğini değerlendirebilmesi için koruma talebinde bulunan tarafı haberdar etmelidir.⁷³¹

Saklanan verilerin korunması bilişim suçlarıyla ve delilleri elektronik ortamda bulunan geleneksel suçlarla mücadelede büyük önem taşımaktadır. Bir suçun aydınlatılmasında ilk önce ve en hızlı şekilde yapılacak işlem saklanan verilerin korunmasıdır. Koruma önlemi özellikle uluslararası yardımlaşmada büyük bir hassasiyetle ele alınması gereken ve yardımlaşmanın temelini oluşturan önlemdir. Bir bilişim suçunda koruma önlemini acilen uygulamadan diğer yardımlaşma

⁷²⁹ Açıklayıcı Rapor, paragraf 286.

⁷³⁰ Çeken, a.g.e., s.120.

⁷³¹ Açıklayıcı Rapor, paragraf 288.

tedbirlerini uygulamak bir sonuç getirmeyecektir. Saklanan veriler eğer korunmamış ise muhtemelen arama ve el koyma için yardım talebinde bulunulsa bile bir sonuç alınamayacaktır. Bu nedenle Sözleşmenin bu önlemi düzenlemesi ve hak saklı tutulabilecek halleri sınırlandırması suçla mücadeleyle yönelik etkili bir düzenleme oluşturmaktadır.

(2) Madde 30-Korunan Trafik Bilgilerinin Açıklanması İşleminin Kolaylaştırılması

Sözleşme bu maddedeki tarafların ulusal hukukunda trafik verilerinin kısmen açıklanması hususunda yapılması öngörülen düzenlemede belirtilen yetkilerin, uluslararası düzeyde de tesis edilmesini amaçlamaktadır. Daha önceki bölümlerde açıklandığı gibi bir iletişime dahil olan servis sağlayıcıların sayısının birden fazla olabileceği gibi farklı ülkelerde bulunan servis sağlayıcılar üzerinden iletişimin gerçekleştirilmiş olması ihtimali oldukça yüksektir. Bu durumda herhangi bir taraf ülke kendi yargı yetkisi dahilindeki sınırlar içerisinde işlenen bir suçla ilgili olarak başka bir taraf ülkeden bu ülkenin yargı yetkisi dahilinde bulunan sınırlar içerisindeki bilişim sistemlerinde saklanan trafik bilgilerini korumasını isteyebilir. Bu durumda Sözleşme talebin yapıldığı tarafın trafik verilerinin korunması için gerekli olabilecek her türlü önlemi almasını öngörmektedir.⁷³²

Diğer yandan talebin yapıldığı taraf korunan trafik bilgilerinden iletişimin üçüncü bir taraf ülkeden ya da talebi yapan ülkeden kaynaklandığını keşfedebilir. Bu durumda, yapan tarafa diğer ülkedeki hizmet sağlayıcının kimliğini ve bu ülkeden yapılan iletişimin izlediği yolu belirlemeye yetecek miktarda trafik verisini hızlı bir biçimde sunmak zorundadır. İletimin üçüncü bir ülkeden gelmesi durumunda talebi yapan taraf bu sayede bu ülkeye aynı şekilde koruma talebinde bulunabilecektir. Diğer durumda iletim talebi yapan tarafın kendisine geri dönmüşse, talebi yapan taraf ulusal düzenlemelere uygun olarak gerekli tedbirleri alabilecektir.⁷³³

Bu madde de, Sözleşme kapsamındaki suçlarda trafik bilgilerinin suçluların tespiti ya da kritik delillerin konumunun tespiti açısından taşıdığı olağanüstü önem nedeniyle, yardımlaşma talebinin devletin egemenliğine, güvenliğe, kamu düzenine ve diğer temel çıkarlarına zarar gelmesi ya da siyasi bir suç veya siyasi bir suçla

⁷³² Açıklayıcı Rapor, paragraf 290.

⁷³³ Açıklayıcı Rapor, paragraf 290.

bağlantılı bir suç olarak görüldüğü durumlar haricinde reddedilemeyeceğini öngörmektedir.⁷³⁴

Daha öncede belirtildiği gibi trafik bilgilerini önemli kılan husus, bu bilgiler sayesinde iletişimin kaynağına kadar ulaşılmasının mümkün olmasıdır. Bu da bir bilişim suçunda trafik bilgilerinin geriye doğru takip edilmesi suretiyle failin tespit edilmesine ve yakalanmasına olanak vermektedir. Dolayısıyla Sözleşmede öngörülen düzenleme özellikle bilişim suçlarının uluslararası niteliği göz önüne alındığında suçla mücadelede hayati bir gereksinimi karşılamaktadır.

(3) Madde 31-Depolanmış Bilgisayar Verilerine Erişilmesine İlişkin Yardımlaşma

Depolanmış bilgisayar verilerine erişilmesine ilişkin yardımlaşma maddesi ulusal düzeydeki uygulamayla eşdeğer bir şekilde, her bir taraf devletin başka bir taraf devletin yararına, kendi yargı yetkisinde bulunan sınırlar içerisindeki bilgisayar sistemleri aracılığıyla depolanan verileri aramasına, el koymasına ya da benzer şekilde koruma altına almasına ve ifşa etmesine imkân sağlamaktadır.⁷³⁵

Bununla birlikte söz konusu yardımlaşma, cezai suçlarla ilgili yardımlaşmayı düzenleyen uygulanabilir anlaşmalar, düzenlemeler ve ulusal yasalar uyarınca gerçekleştirilmelidir. Sözleşme, ilgili verilerin özellikle silinme ya da değiştirilmeye karşı hassas olduğu durumlarda ya da mevcut sözleşmelerin imkân tanıması halinde yardımlaşmanın hızlı bir biçimde gerçekleştirilmesini öngörmektedir.⁷³⁶

(4) Madde 32-Depolanmış Bilgisayar Verilerine İzinli Şekilde ya da Bu Verilerin Halka Açık Olduğu Durumlarda Sınır Ötesinden Erişim Sağlamak

Sözleşmenin bu maddesinde iki farklı erişim yönteminden bahsedilmektedir. Birincisi verilerin herkesin ulaşımına açık olduğu durumdur. İkincisi ise başka bir taraf devletin sınırları içerisindeki bilgisayar sistemlerinde depolanan, ancak herkese açık olmayan verilere, kendi sınırları içerisinde bulunan bir bilgisayar sistemi ile erişimdir. İkinci yöntemde verilere erişimin, yasalar uyarınca bu verileri talep eden tarafa vermeye yetkili kişinin rızası alınarak ve yasal olarak yapılması gerekmektedir. Sözleşme verileri ifşa etmeye "yasalar uyarınca yetkili" kişinin kim

⁷³⁴ Açıklayıcı Rapor, paragraf 291.

⁷³⁵ Açıklayıcı Rapor, paragraf 292.

⁷³⁶ Açıklayıcı Rapor, paragraf 292.

olduğunun, koşullara göre ve durum için geçerli yasaya bağlı olarak farklılık gösterebileceğinden bahsetmektedir.⁷³⁷

Maddede dikkat çeken önemli bir husus yetkili kişinin rızasının yasalara uygun olarak alınmasıdır. Rıza alınmasına rağmen, kişinin verileri ifşa edilmesi yasalara aykırı ise ve bunun farkında değilse ya da rıza yasalara uygun bir şekilde alınmadıysa örneğin zorla, tehdit veya korkutma ile alındıysa, bu durumda söz konusu erişim bu madde kapsamında değerlendirilemeyecektir. Dolayısıyla sınır ötesi erişimin Sözleşme'nin en hassas düzenleme alanlarından birini teşkil ettiği değerlendirilmektedir.

Aslında şu ana kadar incelenen maddeler arasında üzerinde önemle durulması gereken madde olmasına rağmen Sözleşme bu maddeyi sadece iki paragrafta açıklamak suretiyle geçiştirmiştir. İncelendiğinde sınır ötesi erişimi düzenleyen bu maddenin tarafların egemenlik haklarına en büyük müdahaleyi içermesi nedeniyle özel bir niteliğe sahip olduğu görülmektedir. Buraya kadar incelenen maddelerde en çok dikkat çekilen nokta, kişisel hayatın gizliliğine müdahalenin en az seviyede ve orantılı olması gerekliliği iken, burada müdahale tarafların egemenliklerine yöneliktir. Ancak, Sözleşme zaten konunun hassasiyetine binaen bu konuyu fazla detaylı bir düzenlemeye gitmemeyi uygun bulmuştur. Sözleşmenin hazırlık safhasında konu uzun süre tartışılmıştır. Sözleşmenin hazırlanması esnasında tek taraflı erişiminin kabul edilebilir olduğu ve olmadığı durumlar detaylı olarak ele alınmıştır. Sonuçta bu konunun henüz kapsamlı bir şekilde genel kurallara bağlanarak düzenlenemeyeceği kararlaştırılmıştır. Sözleşmeyi hazırlayanlar bu konuda sadece herkesin tek taraflı erişimi kabul ettiği durumların belirtilmesi ile yetinilmesine karar vermişlerdir.

İlk durumda herkese açık verilere erişim konusu herhangi bir sorun teşkil etmeyecektir. İkinci durum ise yetkilendirilmiş kişi ya da kimin yetkili sayılacağı ve hangi bilgilerin bir taraf devletin talep etmesi durumunda verilebileceği gibi hususların ulusal yasalarla detaylı olarak belirlenmesi gerekmektedir. Özellikle yetkili kişiden talep edilen verilerin ulusal güvenlik açısından değerlendirilmesi ne dereceye kadar doğru yapılabilecektir. Türkiye açısından değerlendirdiğimizde ise yukarıdaki çekincelerin geçerli olduğu görülmektedir. Zira ülkemizde ne kişisel verilerin korunması ne de ulusal bilgi güvenliği konusunda düzenleme bulunmamaktadır. Hâlihazırda Kişisel Verilerin Korunması Yasa Tasarısı, Ulusal Bilgi Güvenliği Yasa

⁷³⁷ Açıklayıcı Rapor, paragraf 294.

Tasarısı ve Devlet Sırrı Yasa Tasarısı hazırlanmış olmakla birlikte henüz kabul edilmemiştir.

**(5) Madde 33-Trafik Bilgilerinin Gerçek Zamanlı Olarak Toplanması
Konusunda Yardımlaşma**

Trafik bilgilerinin siber suçlar söz konusu olduğunda failin tespit edilmesi hususunda geriye doğru izleme imkânı vermesi nedeniyle çok önemli olduğuna daha önceki bölümlerde değinilmiştir. Yine gerek teknik nedenler ve gerekse taraf ülkelerin yasal düzenlemeleri çerçevesinde trafik bilgilerinin depolanamaması veya çok kısa süre ile tutulabilmesi, kolluk güçlerinin siber suçlarla mücadelede çok önemli olarak değerlendirilen bir araçtan yoksun kalmasına neden olmaktadır. Bu konu suçun özellikle sınır aşan bir niteliği bulunduğu durumlarda daha da büyük bir önem taşımaktadır. Sözleşme bu madde kapsamında, bir taraf devletin diğer bir taraf devlet yararına, kendi yargı yetkisindeki sınırlar içerisindeki bilgisayar sistemleri ile iletilen bir iletişime ait trafik verilerini gerçek zamanlı olarak toplamasına imkân sağlamaktadır.⁷³⁸

Sözleşme bu maddede de yardımlaşmanın yürütülmesi konusunda yeni bir düzenleme ortaya koymayarak, daha önceki maddelerde belirtildiği gibi yardımlaşmanın mevcut ikili ve çok taraflı yardımlaşma anlaşmaları ve düzenlemeleri çerçevesinde yürütülmesini öngörmüştür.⁷³⁹

Trafik bilgilerinin gerçek zamanlı olarak toplanması arama ve el koyma önlemlerine göre daha az müdahaleci olarak değerlendirildiğinden bu konuda birçok ülke geniş çaplı yardımlaşma sağlamaktadır. Bununla birlikte bazı ülkeler daha dar bir yaklaşım tarzı sergilemektedirler. Sözleşme bu nedenle taraflara bu maddenin ulusal düzeydeki eşiti olan 14 madde 3. paragraftakine benzer şekilde, uygulanacağı suçların kapsamını madde 23'te (Uluslararası işbirliğine ilişkin genel ilkeler) belirtilenlerden daha dar bir suç grubuyla sınırlamalarına izin vermiştir. Ancak bu sınırlama, en azından aynı önlemin uygulanabileceği ulusal suçlardan daha dar olmayacaktır.⁷⁴⁰

•

⁷³⁸ Siber Suçlar Sözleşmesi Madde 33.

⁷³⁹ Açıklayıcı Rapor, paragraf. 295.

⁷⁴⁰ Açıklayıcı Rapor, paragraf. 296.

(6) Madde 34-İçerikle İlgili Verilere Müdahale Edilmesi Konusunda Yardımlaşma

Maddenin özel hayata müdahale edici niteliği yüzünden, içerik verilerine müdahale için yardımlaşma sağlama yükümlülüğü sınırlandırılmıştır. Yardım Tarafların geçerli anlaşma ve yasalarının izin verdiği ölçüde sağlanacaktır. İçerik verilerine müdahale konusunda işbirliğinin sağlanması yardımlaşma uygulamasının yeni şekillenmekte olan bir alanı olduğu için yardım sağlama yükümlülüğünün kapsamı ve sınırları konusunda mevcut yardımlaşma rejimlerine ve ulusal yasalara uyulmasına karar verilmiştir.

(7) Madde 35-24/7 Ağı

Bilgisayar sistemleri kullanılarak gerçekleştirilen suçlarla etkili bir şekilde mücadele edilmesi ve elektronik ortamda bulunan delillerin zamanında elde edilmesi hızlı bir biçimde harekete geçilmesini gerektirmektedir. Klasik suçlarda olduğu gibi siber suçlarında işlenmesi beklenen bir zaman dilimi bulunmamaktadır. Ayrıca İnternet'in ve dolayısıyla siber suçların zamandan ve mekândan bağımsız niteliği, dünyanın herhangi bir yerinde basılacak bir tuşla, çok uzak bir noktada birden çok suçun aynı anda işlenmesine neden olabilmektedir. Bundan dolayı her bir tarafın diğer tarafa her an süratli bir şekilde yardımlaşma talebini iletebilmesi ve buna cevap alabilmesi için diğer tarafta talebini her an iletebileceği bir irtibat noktasının bulunması hayati bir önem taşımaktadır.

Sözleşme bu maddede yukarıdaki gerekçelerle her bir taraf devletin haftanın her günü ve günün her saati görev yapacak şekilde bir irtibat noktası tesis etmesini şart koşturmaktadır. Sözleşmeyi hazırlayanlara göre böyle bir ağın tesisi, Sözleşme tarafından kolluk güçlerinin bilgisayar suçları ya da bilgisayar yardımıyla işlenen suçlarla etkili bir şekilde mücadele etmesini sağlamak üzere getirilen en önemli düzenlemelerden biridir.⁷⁴¹

Teşkil edilen merkez, teknik tavsiye, verilerin korunması, delillerin toplanması, şüphelinin yerinin tespit edilmesi, gayri resmi ya da resmi işbirliği sağlamak için gereken gerekli ön koşullar hakkında yardımlaşma talep eden tarafa danışmanlık yapılması faaliyetlerini doğrudan yerine getirecek veya kolaylaştıracaktır.⁷⁴²

⁷⁴¹ Açıklayıcı Rapor, paragraf 298.

⁷⁴² Açıklayıcı Rapor, paragraf 299.

TASNİF DIŐI

Bunun yanı sıra merkezin en gelişmiş ve yeterli miktarda teçhizatla donatılması ve ağ ekibini oluşturan personelin bilgisayar suçları ve bilgisayarla bağlantılı suçlar ile bunlara nasıl etkin bir biçimde karşılık verileceği konusunda gerekli eğitimi almış olması da şart koşulmaktadır.⁷⁴³

⁷⁴³ Açıklayıcı Rapor, paragraf 301.

BEŞİNCİ BÖLÜM

SONUÇ VE DEĞERLENDİRME

SONUÇ VE DEĞERLENDİRME

Bilgisayar ve iletişim teknolojisinde yaşanan devrimin ortak sonucu olan ve insanlığa bugüne kadar hayal dahi edilemeyecek olanaklar sunan İnternet, sanayi toplumundan bilgi toplumuna geçişin de itici gücü olmuştur. İnternet'in gelişimi ve artan kullanıcı sayısı ile birlikte, gerçek dünyaya paralel, ancak sınırlardan, mesafelerden ve kurallardan muaf yeni bir dünya oluşmuştur. Bu dünya "siber uzay" olarak adlandırılmıştır. Siber uzayda insanlık öyle inanılmaz bir rahatlık, konfor ve özgürlüğe kavuşmuştur ki, sırasıyla bireyler, ticari hizmetler, özel sektör, sosyal ilişkiler ve en sonunda devlet bu ortama taşınmıştır. Ancak, siber uzayın imkânları aynı zamanda suçu ve suçluları da cezpt etmiştir. Bu durum, bir taraftan bilinen suçların işlenmesi için yeni yöntemlerin ortaya çıkmasına neden olurken, diğer taraftan yeni suç çeşitlerini doğurmuştur.

Günümüzde insanoğlunun yüzlerce yılda oluşturduğu modern hukuk sistemi, nispeten yeni ortaya çıkan ancak kısa sürede oldukça büyük boyutlara ulaşan siber suçlar ile etkin bir şekilde mücadele etmekte yetersiz kalmaktadır. İnsanlık tarihin başlangıcına geri dönmüş gibidir. İyinin ve kötünün bir arada bulunduğu, ancak kötüyü sınırlandıracak yeterli ve etkin hukuksal araçların bulunmadığı bir dünyada, suçla mücadele edilmeye çalışılmaktadır. Kötünün kendisini ustaca gizleyebildiği ve anonimlik maskesinin arkasına saklandığı siber uzayda, iyi ile kötü birbirinden kesin olarak ayırt edilememektedir. Bu nedenle suçu önlemeye yönelik çabaların bir kısmı, temel hak ve özgürlüklerin kısıtlandığı gerekçesiyle tepkilere yol açmaktadır.

Bilişim teknolojisi çok hızlı gelişen ve değişen bir olgudur. Her geçen gün yeni gelişmeler yaşanmaktadır. Buna bağlı olarak hukuksal alt yapının da ortaya çıkan yeni durumlara hızla uyum sağlayacak şekilde esnek, ancak fazla yoruma yer bırakmayacak kadar net ve açık olması gerekmektedir. İnsanoğlunun etrafındaki dünya hızla değişirken ve teknoloji bunda belirleyici olurken, bu dünyayı düzenleyen hukuk normlarının durağan kalması düşünülemez. Ancak, değişimin ve gelişimin süreklilik gösterdiği siber uzayı, kapsamlı olarak düzenleyecek hukuki mevzuatın bir anda oluşturulması da mümkün değildir. Bu nedenle, başlangıçta hukuki düzenlemelerin eksikleri nedeniyle, suçla mücadelede yetersiz kalması normal karşılanmalı ve zaman içerisinde bu eksiklikler giderilmeye çalışılmalıdır.

Siber suçlarla mücadelede karşılaşılan en büyük problem, küresel olarak değerlendirildiğinde İnternet'in sınır tanımayan, ülkelerin coğrafi ve yargısal sınırlarından muaf olan yapısıdır. Bu durum, siber suçların büyük çoğunluğunun uluslararası bir özellik göstermesine ve suçlu ile mağdurun farklı ülkelerde bulunmasına neden olmaktadır. Buna siber suçlarla mücadelede karşılaşılan teknik ve yasal güçlükler de eklendiğinde, bu suçlarla etkin şekilde mücadele edilmesi, ancak uluslararası işbirliği ve yardımlaşma ile mümkün olabilmektedir.

Ulusal güvenlik açısından ele alındığında, çalışmanın konusu olan Siber Suçlar Sözleşmesi'nin iki yönü bulunduğu değerlendirilmektedir. Gün geçtikçe artan ve daha ciddi sonuçlar doğuran siber suçların ulusal güvenliği tehdit edecek boyutlara ulaştığı ve bir ulusal güvenlik meselesi haline geldiği ifade edilebilir. Bu nedenle, siber suçlarla mücadeleye katkıda bulunacak düzenlemeler, doğrudan ulusal güvenliğin sağlanması ve korunmasına da katkı sağlayacaktır. Dolayısıyla, Sözleşmenin bilgi, bilişim alt yapısı ve bilgi edinme hakkına yönelik suçları önlemedeki ve toplumun zararlı bilgiden korunmasını sağlamadaki etkinliği; diğer bir ifadeyle ulusal güvenlik meselesi haline gelen siber suçların önlenmesi konusundaki yeterliliği, Sözleşmenin ulusal güvenliğe etkisinin ilk yönünü oluşturmaktadır.

Sözleşme uluslararası işbirliği kapsamında karşılıklı yardımlaşma için, taraf devletler arasında süratli bilgi alışverişini, içerik bilgilerine müdahaleyi ve hatta sınır ötesi erişimi öngörmektedir. Bu durum, tarafların yardımlaşma esnasında ulusal bilgi güvenliğini tehlikeye sokacak müdahale, bilgi paylaşımı ve erişim faaliyetlerine müsaade etmemesini önemli hale getirmektedir. Bunun için özellikle ulusal bilgi güvenliğine yönelik önlemlerin, tarafların iç hukuklarında düzenlenmesi, bu konuda yetki ve sorumlulukları düzenleyen hukuki alt yapının tesis edilmiş olması gerekmektedir. Dolayısıyla Sözleşmenin kabulü halinde, Türkiye'ye uluslararası işbirliği kapsamında getireceği yükümlülüklerin ulusal bilgi güvenliği açısından oluşturması muhtemel risk, ulusal güvenliğe etkisinin ikinci yönünü oluşturmaktadır.

İlk yönü ile ele alındığında, Sözleşmenin siber suçlarla mücadelede etkin bir düzenleme olabilmesi için dört hususu sağlaması gerektiği ifade edilebilir. Bunlardan ilki suçta ve cezada kanunilik ilkesi gereğince, Sözleşmenin maddi ceza hukuku bölümünde suç teşkil eden fiillerin ve suç yöntemlerinin tamamının kapsanmasıdır. İkincisi, bu yeni suç türleri ve suç işleme yöntemlerinin kovuşturulmasına uygun yeni usullerin belirlenmesi ve kolluğun en az suçlular kadar hızlı tepki vermesine olanak sağlanmasıdır. Üçüncüsü, suçla mücadelede başta İSS'ler olmak üzere İnternet sükjelerinin görev ve sorumluluklarının belirlenmesidir. Sonuncusu ise suçla

mücadele ederken, İnternet'in özünde yer alan bilgi edinme, düşünce ve ifadeleri yayma özgürlüğü kapsamında temel hak ve özgürlüklere saygılı olunmasıdır.

Siber Suçlar Sözleşmesi, bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar ve bilgisayarla ilişkili suçlar ana başlığı altında düzenlenen suçlar ile hâlihazırda var olan siber suç türleri ve yöntemlerinin tamamını kapsayan bir nitelik sergilemektedir. Suçun ilk aşaması olan yetkisiz erişiminden dahil kötü maksatlı tüm fiiller suç haline getirilmiştir. Özellikle kötü niyetle kullanılabilecek belli cihazlar ya da yazılımların suç haline getirilmesi, suç aletlerinin ve suça yönelik potansiyel tehlike yaratan eylemlerin kaynağından yasaklamasını sağlamaktadır. Bu durum Sözleşmeyi, yalnızca tamamlanmış suçların cezalandırılmasını sağlayan pasif bir araç olmaktan çıkararak, suçun önlenmesini sağlayan aktif bir araç haline getirmektedir. Ayrıca, suç olarak kabul edilen fiillere daha sonra gelişen duruma göre yenilerinin eklenmesine de imkân tanınacak şekilde kaleme alınmıştır. Bu yönü ile Sözleşmenin, siber suçlarla mücadelede, dolayısıyla bilgi güvenliğinin sağlanması ve bilişim altyapısının korunmasında etkin bir araç özelliği sergilediği değerlendirilmektedir.

Toplumun zararlı bilgiden korunması kapsamında ise Sözleşmenin özellikle çocuk pornografisi ile uluslararası alanda mücadele edilebilmesine büyük katkı sağlayacağı değerlendirilmektedir. Ancak, Türkiye'nin mevcut güvenlik sorunları göz önüne alındığında, İnternet'in yıkıcı ve bölücü örgütler tarafından kullanılmasının engellenmesi daha büyük bir önem taşımaktadır. Özellikle, Türkiye'de faaliyet gösteren terör örgütleri lehine propaganda yapan, adam devşirmeyi amaçlayan, doğrudan toplumda kin, nefret ve şiddeti teşvik eden yurt dışı kaynaklı İnternet sitelerinin yayınlarının durdurulması konusunda güçlükler bulunmaktadır. Hâlihazırda bu tür sitelere Türkiye'den erişimi engellemek mümkün olsa dahi yayının yapıldığı ülke ve dünyanın diğer yerlerinden erişilebilmesi bu tedbiri etkin olmaktan uzaklaştırmaktadır. Bu nedenle, Ek Protokol'ün suç olarak düzenlenmesini öngördüğü fiillerin, İnternet ortamında yıkıcı ve bölücü faaliyetler ile mücadele açısından olumlu katkı sağlayacağı değerlendirilmektedir.

Bununla birlikte içerik açısından zararlı olarak değerlendirilebilecek İnternet sitelerinin tamamı, doğrudan terör örgütleri lehine propaganda yapmamaktadır. Bazı İnternet siteleri yıkıcı ve bölücü faaliyetler yürüten örgütlerin, eylemlerini dayandırdıkları siyasi görüşlerin sözcülüğünü yapmak veya bu eylemlere siyasi bir anlam kazandırmak amacıyla, fikri mücadele yürütmeye çalışmaktadır. Bu durum,

İnternet'in siyasi bir baskı aracı olarak kullanılması anlamına gelmektedir. Bu tür siteler her ne kadar düşünce ve ifade özgürlüğü içerisinde hareket ediyor gibi görünseler de laik düzeni, mevcut rejimi ve ulusal devlet yapısını tehdit eden düşünceleri yaymak suretiyle, ulusal güvenlik açısından tehdit teşkil etmektedirler. Bu noktada ulusal güvenlik kavramı ile düşünce ve ifade özgürlüğü çakışmaktadır. Avrupa Konseyi Siber Suçlar Sözleşmesinin giriş bölümünde, Sözleşme kapsamında suç olarak değerlendirilen eylemlere yönelik ceza sorumluluklarının düzenlenmesinde, AİHS'nin gereklerine uyulması gerektiği belirtilmiştir. AİHM'in ulusal güvenlik karşısında düşünce ve ifade özgürlüğünü ele alan kararlarında, açık ve yakın bir tehlike bulunmadığı sürece, ulusal güvenlik nedeniyle düşünce ve ifade özgürlüğünün kısıtlanması ihlal olarak kabul ettiği görülmektedir. Bu husus göz önüne alındığında, Sözleşmenin bu tür İnternet sitelerinin engellenmesinde Türkiye'ye ilave bir yarar sağlamayacağı değerlendirilmektedir. Sözleşmenin hazırlanış sürecinde bilgisayar sistemleri aracılığıyla ırkçı ve yabancı düşmanlığına yönelik eylemlerin suç haline getirilmesi konusunda yaşanan tartışmalar nedeniyle, bir ek protokol oluşturulması, Sözleşmenin bu konudaki sorunlara çözüm getirmek konusun bir iddiası bulunmadığı şeklinde değerlendirilebilir.

Türkiye'nin güncel sorunlarından biri de uluslararası alanda sıkça karşılaşılan sözde Ermeni soykırımı iddialarıdır. Siber Suçlar Sözleşmesini hazırlayan Avrupa Konseyi'ne üye ülkelerin de aralarında bulunduğu birçok ülke parlamentosu tarafından, sözde soykırım iddiaları kabul edilmiştir. Ek Protokol kapsamında soykırım ve insanlığa karşı suçların inkârı, önemsizleştirilmesi, haklı görülmesi suç haline getirilmektedir. İnkârı suç sayılacak soykırım suçlarının tarafların, yargı yetkisini tanıdıkları sürece gelecekte teşkil edilebilecek mahkemelerin son ve bağlayıcı kararları ile hâlihazırdaki Uluslararası Ceza Mahkemesi kararları ile belirlenmesi öngörülmektedir. Avrupa Konseyi ülkelerinin çoğunluğunun, sözde Ermeni soykırımını kabul eden yasaları meclislerinde kabul etmeleri halinde, gelecekte sözde Ermeni soykırımı iddialarının da inkârı suç sayılan soykırımlar kapsamında değerlendirilmesi konusunda ortak görüş oluşabilir. Türkiye'nin günümüz itibarıyla Protokolün ilgili maddesini kabul etmesi, gelecekte bu ihtimalin gerçekleşmesi durumunda, İnternet aracılığıyla gerçekleştirilen inkâr fiilleri için Protokole taraf olması nedeniyle iade talepleri ile karşılaşması sonucunu doğurabilir. Bu hususun, uluslararası alanda Türkiye üzerinden baskı oluşturmak amacıyla, bir araç olarak kullanılabileceği değerlendirilmektedir.

Sözleşme, klasik usul hukukunun siber suçlar söz konusu olduğunda yetersiz ve yavaş kalan uygulamalarını, bu suç türlerine uygun hale getirmiştir. Siber uzaya uygun şekilde arama ve el koyma; diğer ifade ile erişim ve kopyalama, depolanmış verilerin korunması, trafik bilgilerine ve içerik bilgilerine müdahale gibi yetkileri tanımlamıştır. Depolanmış bilgisayar verilerinin hızlı bir biçimde korunması, trafik bilgilerinin İSS'ler tarafından belli bir süre ile depolanması, trafik bilgilerinin gerçek zamanlı olarak toplanması ve içerikle ilgili bilgilere müdahale edilmesine yönelik düzenleme, suçla mücadelede siber suçların işlenme hızı, elektronik ortamda bulunan delillerin hassasiyeti gibi hususların neden olduğu güçlükleri en aza indirecek uygun tedbirlerdir. Bir başka ifade ile Sözleşme usul hukukunu siber uzayla uyumlu hale getirmektedir. Bu açıdan, Sözleşmenin çalışmanın başında ortaya konulan, suçla mücadelede yaşanan yasal ve teknik güçlükleri en aza indirebileceği, bu sayede kolluğun en az suçlular kadar hızlı tepki vermesine imkân sağlayacağı ve Türkiye açısından ulusal mevzuatın Sözleşmeye uygun hale getirilmesinin, ulusal seviyede siber suçlarla mücadeleye önemli katkılar sağlayacağı değerlendirilmektedir.

Sözleşme yargılama yetkilerini düzenlemek suretiyle, yargı yetkisinin dışında kalacak boşlukları kapatmaktadır. Böylece, işlenen bir suçta failin yargı yetkisi boşluğundan istifade ederek, cezadan kurtulmasını engellenmek bakımından etkili bir düzenleme getirmektedir. Mülkilik ve şahsılık ilkesinin bir arada kullanılması suretiyle suç işleyen bir fail, taraf devletlerden herhangi birinin sınırları içerisinde ise mülkilik ilkesine ya da şahsılık ilkesinden birine göre, eğer taraf devletlerin ya da herhangi bir ülkenin yargı yetkisi dışında bir yerde ise şahsılık ilkesine uygun olarak yargılanabilmektedir.

Sözleşme öncelikle siber suçları belirleyerek, bu suçların taraf devletlerin tamamı tarafından suç olarak kabul edilmesini sağlamaktadır. Böylece iadeye konu olan eylemin talep eden ve talep edilen taraf ülkelerin her ikisinde de suç olması gerekliliğini ifade eden "çifte suçluluk" ilkesinden kaynaklanan işbirliği ile ilgili güçlüğü ortadan kaldırmaktadır. Bu sayede Sözleşme'de tanımlanan suçlardan herhangi birinin yine taraf devletlerin herhangi birinin sınırları içerisinde veya sınırları dışında bir vatandaş tarafından, taraf devletlerden birine ya da vatandaşına karşı gerçekleştirilmesi durumunda cezalandırılması mümkün olmaktadır. Buna ilaveten taraf devletlerin usul hukuku düzenlemelerinin uyumlu hale getirilmesi, taraf devletlerin her birinde suçluların takip edilebilmesi, yakalanabilmesi ve yasalara uygun delil elde edilebilmesine olanak tanımaktadır. Taraf ülkelerin her birinde

depolanan bilgisayar verilerinin sratle korunabilmesi, trafik bilgilerinin İSS'ler tarafından belirli sreyle saklanması, trafik ve ierik bilgilerine mdahale edilebilmesi suuların takibi esnasında soruřturma zincirinin kopmasını engellemektedir. Suun iřlenmesi esnasında iletiřime dahil olan İSS'lerin ve lkelerin sayısından bağımsız olarak faile ulařılması mmkn olabilmektedir. Ayrıca Szleřme'nin iřbirlięinin sratle saęlanması imkn tanıyan dzenlemeleri, elektronik ortamdaki su delilleri yok olmadan, hızlı bir řekilde yardımlařma ve koordinasyon saęlanmasını mmkn kılmaktadır. Szleřmenin yargılama yetkisi, karřılıklı yardımlařma ve suuların iadesi gibi konulardaki hkmlerinin, uluslararası iřbirlięi konusunda karřılařılan gkleri byk oranda ortadan kaldıracabilecek nitelikte olduęu deęerlendirilmektedir.

Ancak, siber sularla mcadele iin yalnızca suların tanımlanması ve buna uygun usul hukukunun oluřturulması yeterli deęildir. İnternet sjelerinin siber uzayda denetimin saęlanması aısından sorumluluklarının ve grevlerinin belirlenmesi de nem tařımaktadır. Szleřmenin etkin bir ara olabilmesi iin nc olarak bu hususu saęlaması gerektięi ifade edilebilir. Szleřme, İSS'lere trafik bilgilerinin belli bir sre ile depolanması, depolanan trafik bilgilerinin korunması, gerektięinde trafik ve ierik bilgilerinin gerek zamanlı olarak toplanması ve abone bilgilerinin retilmesi hususunda koluęa yardım etme ykmllę getirmektedir. Bununla birlikte, İSS'lere, yeni donanımlar temin etmeleri, uzman desteęi almaları ya da masraf yaratacak řekilde sistemlerini yeniden dzenlemeleri konusunda zorunluluk getirilmemektedir. Bu imknların hlihazırda bulunması durumunda ve kanun tarafından talep edildięinde kullanılması ngrlmektedir. Taraf devletlere rutin bir řekilde trafik ya da abone bilgileri gibi belli verileri toplamayan ve depolamayan servisleri kısıtlama zorunluluęu da getirilmemektedir. Bu ykmllkler yalnızca teknik aıdan, bu imkna sahip olan İSS'ler iin uygulanmaktadır. Siber suların aydınlatılması konusunda İSS'ler tarafından depolanan bilgilerin nemi ve IP adresinden yola ıkarak hedeften geriye doęru gerekleřtirilen soruřturma teknięi gz nne alındıęında, birden fazla İSS'nin dahil olduęu bir suta, zincirin halkalarını oluřturan herhangi bir İSS'nin trafik bilgilerini depolamaması suun aydınlatılmasını olduka gleřtirecektir. Bu durum uluslararası sularda daha ciddi bir problem oluřturabilecektir. Dolayısıyla, ilk bakıřta Szleřmenin olumlu taraflarından biri olarak grlebilecek bu durumun, aslında Szleřmenin yaptırım gc ve pratikte sula mcadele aısından bir zafiyet olduęu deęerlendirilmektedir.

Türkiye açısından değerlendirildiğinde ise Telekomünikasyon Kurumu'nun yayınladığı yönetmelikte İSS olarak hizmet veren işletmecilere, en az altı ay süresince her bir kullanıcı için sisteme bağlı kalınan süre, trafik miktarı ve trafik yolu bilgilerini muhafaza etme zorunluluğu getirilmektedir. Dolayısıyla, yönetmeliğin uygulandığı kabul edilirse, Türkiye'de Sözleşme'nin öngördüğü 90 günlük süre hususunda teknik açıdan bir problem olmadığı değerlendirilebilir. Ancak, hem yönetmelikte hem de 5651 sayılı Kanun'da uygun işlem yapmayan İSS'ler için yaptırım olarak, yalnızca idari para cezasını öngörülmektedir. Dolayısıyla, Türkiye'de İSS'lere tam anlamıyla cezaî sorumluluk getiren bir düzenleme bulunmamaktadır. Buna ilaveten Türkiye'de hâlihazırda, İnternet'in ulusal düzeyde denetimine yönelik yasal düzenlenmelerin tamamlanmamış olmasının, iç hukukta yasal dayanak olmaması nedeniyle, uluslararası işbirliği çerçevesinde gelecek yardım taleplerine karşılık verilememesine neden olacağı ve bunun Türkiye'yi uluslararası alanda zora sokacağı değerlendirilmektedir.

Sözleşmede eksik bırakılan çok önemli bir husus da, İnternet hizmetinin toplu olarak verildiği mekânlarda ve özellikle İnternet kafelerde, İnternet kullanımının kayıt altına alınması konusunda işletmecilere ya da sistem yöneticilerine sorumluluk getirilmemesidir. İnternet kafelerden işlenen siber suçların oranı ve bu suçlarda faillerin bulunmasında yaşanan güçlükler dikkate alındığında, kullanıcıların kimliği, kullanım süresi, log bilgilerinin kayıt altına alınması suçla mücadelede kilit rol oynamaktadır. Bu eksiklik uluslararası suçlarda işbirliği yapmaktan kaçınan ya da yargıya veya iade et ilkesini uygulamak istemeyen taraf devletlerin, İSS'lerin teknik imkânsızlıkları ya da suçun İnternet kafeden işlendiği mazeretinin arkasına sığınmasını sağlayabilir. Bu durumun, Sözleşmenin uluslararası alanda ciddiyetini, uygulanabilirliğini ve etkinliğini olumsuz yönde etkilediği değerlendirilmektedir.

Sözleşme ile öngörülen düzenlemelerin, hukuk devleti ilkeleri doğrultusunda temel hak ve özgürlüklere saygılı olması gerektiği hususunda ise, Sözleşmenin suçla mücadele için öngördüğü müdahaleci yöntemler ile temel hak ve özgürlükler arasında uygun dengenin sağlanması için büyük bir özen sergilendiği görülmektedir. Sözleşme bir taraftan kolluğa depolanmış bilgilerin aranması, el konması, trafik bilgilerinin gerçek zamanlı olarak toplanması ve içerikle ilgili bilgilere müdahale edilmesi gibi yetkiler sağlarken; diğer taraftan bu yetkilerin temel hak ve özgürlüklerin ihlaline yol açacak biçimde, genel olarak suçlu avına çıkar tarzda uygulanmasına imkân vermemektedir. Bu yetkiler yalnızca somut bir suç ve faile yönelik soruşturma ve kovuşturma dahilinde uygulanabilmektedir.

Sözleşme'nin kabulünün, Türkiye'ye getireceği yükümlülüklerin ulusal güvenliğe etkileri kapsamında ise özellikle karşılıklı yardımlaşma çerçevesinde diğer taraf devletlerin talep ettikleri bilgilerin sağlanması ve depolanmış bilgisayar verilerine sınır ötesinden erişim imkânı verilmesinin ulusal bilgi güvenliği açısından oluşturabileceği tehdit ön plana çıkmaktadır. Bilginin ifşa edilmesi, bilgiyi veren ülkenin önemli çıkarlarını tehlikeye sokabilir, bilgi toplama yönteminin açığa çıkmasına neden olabilir ya da bir suç örgütü ile ilgili soruşturmanın gizliliğini ihlal edebilir. Sözleşme bu gibi durumlarda, tarafların bilginin ifşa edilmesi için çeşitli şartlar ileri sürülebilmesini öngörmekte ve yardım taleplerini belirli durumlarda reddetme olanağı da tanımaktadır. Yardım talep edilen devletin egemenliğine, güvenliğe, kamu düzenine ve diğer temel çıkarlarına zarar gelmesi durumunda yardımlaşma talebi reddedilebilmektedir. Bu açıdan Sözleşmenin taraf devletlerin güvenliklerini tehlikeye atmalarına sebep olacak bir yükümlülük getirmediği değerlendirilmektedir.

Ancak, özellikle Sözleşmenin depolanmış bilgisayar verilerine sınır ötesinden erişim sağlanması ile ilgili maddesi bu açıdan önem taşımaktadır. Bu maddeye göre sınır ötesi erişim için iki yöntem ya da iki koşul bulunmaktadır. Birincisi verilerin herkesin ulaşımına açık olduğu durumdur. İkincisi ise herkese açık olmayan verilere erişimdir. İkinci yöntemde verilere erişim, ancak verilerin depolandığı ülke yasaları uyarınca bu verileri talep eden tarafa vermeye yetkili kişinin rızası alınarak mümkün olabilmektedir. Sınır ötesi erişimi düzenleyen bu madde tarafların egemenlik haklarına en büyük müdahaleyi içermesi nedeniyle özel bir niteliğe sahiptir. Ulusal ve uluslararası seviyedeki diğer usul hukuku maddeleri kişisel hayatın gizliliğine müdahale mahiyetinde iken, burada müdahale tarafların egemenliklerine yöneliktir. Sözleşme ayrıca bu maddede taraflara hak saklı tutma imkânı da vermemektedir.

Sözleşme, yardım taleplerinin ve cevaplarının süratle gerçekleştirilebilmesi için geleneksel yardımlaşma yöntemleri yerine, ilgili mercilerin doğrudan iletişime geçmelerine olanak sağlayan süratli yöntemleri ve tesis etmektedir. Bu nedenle, yardım taleplerinin ulaştırılacağı makamların, bunların yetki ve sorumluluklarının ve bilgi güvenliği ilkelerinin detaylı biçimde düzenlenmiş olması, hem Sözleşme ile amaçlanan süratli yardımlaşmanın gerçekleştirilmesi hem de ulusal güvenliğin ihlal edilmemesi için zorunludur. Sözleşmede tarafları zor durumda bırakacak bir yükümlülük getirilmemesine rağmen; iç hukuktaki eksiklikten kaynaklanan bir hassasiyet ortaya çıkmaktadır. Türkiye'de "Devlet Sırrı Kanunu", "Kişisel Verilerin Korunması Hakkında Kanun" ve "Ulusal Bilgi Güvenliği Kanunu" gibi ulusal bilgi

güvenliği konusunda büyük önem taşıyan hukuksal alt yapının henüz tesis edilmemiş olması ve kimlerin, hangi bilgileri, hangi koşullar altında diğer ülke makamlarına verebileceği konusunda ortaya çıkması muhtemel belirsizlik nedeniyle, özellikle sınır ötesi erişime imkân sağlanmasının ulusal bilgi güvenliği açısından olumsuz sonuçlar doğurabileceği değerlendirilmektedir.

Sözleşme genel olarak birçok düzenlemeyi ulusal mevzuata bırakmakta ve tarafların bazı konularda hak saklı tutmalarına imkân tanımaktadır. Böylece katı ve hükmedici bir çerçeve çizmemeye özen göstermektedir. Uluslararası işbirliği, karşılıklı yardımlaşma ve iade gibi konularda yeni usuller getirilmemektedir. Sözleşme, bu alanlarda var olan Avrupa Konseyi Sözleşmelerinin uygulanması öngörmektedir. Buna ilaveten, Sözleşme hükümlerinin taraflar arasında mevcut karşılıklı sözleşmelerin ve ulusal mevzuatın uluslararası işbirliği ile ilgili hükümlerinin yerine geçmeyeceği genel ilke olarak ortaya konulmaktadır. Sözleşme bu haliyle var olan uluslararası çok taraflı ve ikili anlaşmalar karşısında ikincil bir araç özelliği taşımaktadır.

Türkiye Sözleşmenin uluslararası işbirliği ve karşılıklı yardımlaşmada öncelik tanıdığı diğer Avrupa Konseyi Sözleşmelerinin ve telif hakları konusunda Sözleşmede atıf yapılan uluslararası anlaşmaların tümüne zaten taraftır. Ayrıca Sözleşme metninin hazırlanması sürecinde istifade edilen diğer Avrupa Konseyi Sözleşmelerini de imzalamıştır. Siber Suçlar Sözleşmesi ile karşılaştırıldığında Türkiye'nin hâlihazırdaki hukuki mevzuatı büyük paralellik sergilemektedir. Cihazların kötüye kullanılması, elektromanyetik dinleme ve bilgisayarla ilgili sahtecilik suçları haricinde, Sözleşmenin 2-11. maddelerinde de suç haline getirilen eylemlerin tamamı TCK'da bilişim alanında suçlar başlığı altında düzenlenmiştir. Hırsızlık ve dolandırıcılık suçlarının bilişim sistemleri kullanılarak gerçekleştirilmesi ise nitelikli hırsızlık ve dolandırıcılık olarak düzenlenmiştir. Bu nedenle, siber suçlarla mücadele için Türkiye'nin kısa sürede iç hukukta gerekli düzenlemeyi tamamlayabileceği değerlendirilmektedir.

Sözleşme mümkün olan en geniş katılımı sağlamayı amaçlamaktadır. Avrupa Suç Sorunları Komitesi (CDPC), Kasım 1996 yılında siber suçlarla mücadele etmek üzere uzmanlardan oluşan bir komite kurma kararı aldığı anda bu kararını, siber suçlarla mücadele için tavsiye kararından daha çok maddi ceza hukuku, usul hukuku ve uluslararası ceza hukuku usullerine dayanan, Sözleşme tarzında yükümlülük getiren bir hukuki araca başvurulması gerektiği sonucuna dayandırmıştır. Sözleşmenin gerek maddi ve usul hukuku, gerekse uluslararası

işbirliği açısından teorik olarak siber suçlarla mücadelede etkili bir araç özelliği gösterdiği ifade edilebilir. Ancak, mümkün olan en geniş katılımı sağlamak amacıyla, hem uluslararası işbirliği ile ilgili bazı konularda kesin hükümler ortaya koyamamasının, hem de İSS'lere ve diğer İnternet sùjelerine sorumluluk getirmedeki çekingenliğinin, Sözleşme'nin CDPC'nin başta belirlediği yükümlölük getiren hukuki bir araç olma amacından yoksun kalmasına neden olduđu ve uluslararası işbirliği alanında uygulamada beklenen faydayı gösteremeyeceđi ifade edilebilir. Bununla birlikte gelecekte bilişim sistemlerine olan bağımlılıđın artması ve daha fazla insanın ve ülkenin bu suçlardan etkilenmesi nedeniyle, İnternet'in denetlenmesi konusundaki çekincelerin azalacağı ve uluslararası işbirliği ihtiyacının artacağı, dolayısıyla zamanla Sözleşme'nin eksikliklerinin giderilerek uluslararası alanda da etkin bir araç haline geleceđi değerlendirilmektedir. Bu durumda Türkiye'nin kurucu üyesi olduđu Avrupa Konseyi'nin siber uzayı düzenlemeye yönelik gelecekteki çalışmalarının dışında kalarak Sözleşme'ye sonradan taraf olması yerine, bu düzenlemelere etki edebilecek şekilde süratle çalışmalara dahil olması büyük önem taşımaktadır. Bu sayede Türkiye'nin siber uzayda kendi menfaatlerini koruyabileceđi, en azından olumsuz etkide bulunabilecek düzenlemeleri önleme imkânına sahip olabileceđi ve bunun da Türkiye açısından fayda sağlayacağı değerlendirilmektedir.

Bu değerlendirmeler ışığında; Türkiye'nin, özellikle İnternet sùjelerinin cezaî yükümlölüklerini, e-devlet sürecinde kurumlar arasındaki güvenlik standartlarını tesis etmeyi, kişisel verilerin korunması, devlet sırrı ve bilgi güvenliğine yönelik hâlihazırda taslak halde bulunan kanunları kabul etmeyi, usul hukuku ile ilgili yetkileri tesis etmeyi ve İnternet'in ulusal düzeyde denetimine yönelik yasal düzenlenmeleri süratle gerçekleştirmeyi müteakip, Sözleşmeye ve 6. maddedeki hak saklı tutma imkânını kullanmak suretiyle Ek Protokole taraf olmasının uygun olacağı sonucuna varılmıştır.

ALTINCI BÖLÜM

KAYNAKÇA

“ABD ve Avrupa, Aldı Başını Gidiyor”, Haziran 2006, Bilişim Dünyası. 11 Nisan 2007 <<http://www.bilisimdunyasi.net.tr/yazi.asp?sayi=4&yazi=355>>.

“A Brief History of The Internet”, Internet Society (ISOC) İnternet Sayfası. 12 Nisan 2007 <<http://www.isoc.org/internet/history/brief.shtml>>.

ACQUISTI, Alessandro ve diğerleri. “Is There a Cost to Privacy Breaches? An Event Study”. 25 Mart 2007 <<http://weis2006.econinfosec.org/docs/40.pdf>>.

“Additional Protocol to the Convention on Cybercrime, Concerning The Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems”. Council of Europe. 10 Ekim 2006 <<http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>>.

AKMAN, Toygar. **Sibernetik: Dünü, Bugünü, Yarını**, İstanbul, Kaknüs Yay., 2003.

AKOLAŞ, Arzu. “Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları”. 10 Şubat 2007 <http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler%5CD.Arzu%20AKOLA%C5%9E%5C29-43+.pdf>.

AKYILDIZ, Fulya. “Bilgi Toplumu Yönetim Anlayışı’nın Gerçekleşebilmesi İçin Zorunlu Bir Hak: Bilgi Edinme Hakkı”, 3. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi (Osman Gazi Üni. İktisadi ve İdari Bilimler Fakültesi, Eskişehir, 25-26 Kasım 2004). 20 Mart 2007 <<http://libf.ogu.edu.tr/kongre/bildiriler/11-01.pdf>>.

ALFORD, Lionel D. “Cyberwarfare: Protecting Military Systems” **Acquisition Review Quarterly**, Spring 2000, 100-120.

ALKİM, B. Emre. “Bilmediğiniz 10 Büyük Tehlike”, **CHIP Dergisi**, Ocak 2007, 160-164.

ALKİN, K. ve C. GÜRLESEL, “Dünya Ekonomisine Yönelik Global Tehditler; Dünya da Güvenlik ve Tehdit Kavramının Evrimi ve Global Güvenlik İçinde Ulusal Güvenlik Perspektifi”, **İstanbul Ticaret Üniversitesi Dergisi**, 3, 6, 2004, 9-34.

AnaBritannica Genel Kültür Ansiklopedisi, 15.bs., IV, X, XIX, Ana Yayıncılık, 2004.

ARKUN, M. Ender. "Türkiye İçin Bir Enformasyon Politikasının Ana Öğeleri Neler Olmalı?", **Bilgi Dünyası**, IV, 2, 2003, 175-191.

ATICI, B. ve Ç. GÜMÜŞ, "Sanal Ortamda Gerçek Tehditler: Siber Terör", **Polis Dergisi**, 9, 37, Ekim-Kasım-Aralık 2003, 57-66.

"ATO İnternet Kumarhaneleri Raporu", ATO İnternet Sayfası. 29 Mart 2007 <<http://www.atonet.org.tr/turkce/bulten/bulten.php3?sira=281>>.

AVŞAR, Servet. "Ermeni Sorunu ve Türkiye", **Manas Üniversitesi Sosyal Bilimler Dergisi**, I, 1, 2001, 57-89.

AYTAÇ, Osman. "Siber Terör", Terör Okulu Eğitim Programında sunulan bildirisi, (Bahçeşehir Üniversitesi, İstanbul, 09 Aralık 2006).

BAL, Mehmet. **Modern Devlet ve Güvenlik**, İstanbul, IQ Kültür Sanat Yayınları, 2003.

BALDWIN, David A. "Güvenlik Kavramı", **Avrasya Dosyası**, Ankara, ASAM Yayınları, IX, 2, Yaz 2003, 5-35.

Başbakanlıkta Bulunan Kanun Tasarıları. Adalet Bakanlığı İnternet Sayfası. 12 Şubat 2007 <<http://www.kgm.adalet.gov.tr/basbakanliktabulunanlar.htm>>.

BECENİ, Yasin. "Siber Uzayda Mahremiyet", Mart 2004, Türkiye 2. Bilişim Şurası İnternet Sayfası. 08 Kasım 2006 <http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf>.

BEYLİ, Ceylin. "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler". 30 Mart 2007 <http://www.bilisimsurasi.org.tr/hukuk/docs/tbs_kisisel_veri_ceylin_beyli_gorus1.pdf>.

BİLGİN, Pınar. "Individual and Societal Dimensions of Security", **International Studies Review**, V, 2, 2003, 203-222.

BOASE, Jeffrey ve diğerleri. "The Strength of Internet Ties", **PEW İnternet & American Life Project**, Washington, 2006.

BOLLINGER, C. ve G. STONE, "Dialogue", **Eternally Vigilant: Free Speech in the Modern Era**, L. C. BOLLINGER, G. R. STONE (Ed.), The University of Chicago Press, 2002, 1-31.

BOSCH, Olivia. "Teknoloji ve Uluslararası Güvenlik Stratejileri", Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, 61-76.

BOWMAN, Gerald. "Physical Security for Mission-Critical Facilities and Data Centers", **Information Security Management Handbook**, 5. bs., H. F. TIPTON, M. KRAUSE (Ed.), Auerbach Publication, 2006, 641-662.

BRENNER, Susan W. "Distributed Security: A New Model of Law Enforcement", **Journal of Internet Law**, VIII, 5, Nov 2004, 8-25.

Büyük Larousse Sözlük ve Ansiklopedi, III, XVII, Gelişim Yayınları, 1986.

BUZAN, Barry ve diğerleri. **Security: A New Framework of Analysis**, London, Lynne Rienner, 1998.

CANGEMI, Daniele. "Procedural Law Provisions of The Council of Europe Convention on Cybercrime", **International Review of Law Computers & Technology**, XVIII, 2, July 2004, 165-172.

CASHELL, Brian ve diğerleri. "The Economic Impact of Cyber-Attacks", **CRS Report for Congress**, April 1, 2004. 09 Mart 2007 <http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf>.

CENTEL, Nur ve diğerleri. **Karşılaştırmalı-Tablolu Yeni Türk Ceza Kanunu, Ceza Muhakemesi Kanunu, Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun ve İlgili Mevzuat**, 6.bs., İstanbul, Beta Yay., 2006.

Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, 14 Şubat 2004 tarih ve 26434 sayılı Resmi Gazete. 10 Mart 2004 <<http://rega.basbakanlik.gov.tr/eskiler/2007/02/20070214-11.htm>>.

Code of Federal Regulations. 28 CFR. Section 0.85 on Judicial Administration, FBI. 24 Aralık 2006 <http://www.fbi.gov/publications/terror/terror2000_2001.htm>.

COLLIN, Barry C. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", 11th Annual International Symposium on Criminal Justice Issues. 07 Şubat 2007 <<http://afgen.com/terrorism1.html>>.

"Internet History", Computer History Museum İnternet Sayfası. 12 Nisan 2007 <http://www.computerhistory.org/exhibits/internet_history/index.shtml>.

"Convention for the Protection of Human Rights and Fundamental Freedoms", Council of Europe. 12 Şubat 2007 <<http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>>.

"Convention on Cybercrime", Council of Europe. 10 Ekim 2006 <<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>>.

"Council of Europe Convention on the Prevention of Terrorism", Council of Europe. 13 Ocak 2007 <<http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm>>.

CORDESMAN, A. ve J. CORDESMAN, **Cyber-Threats, Information Welfare, and Critical Infrastructure Protection: Defending the U.S. Homeland**, Connecticut, Praeger, 2001.

"Cybercrime Laws, Prevention and Enforcement Capacity Builds", **I-Ways**, XXVI, 3, 2003, 117-123.

ÇEÇEN, Anıl. "Türkiye'nin Güvenliği", **Uluslararası Çatışma Alanları ve Türkiye'nin Güvenliği**, G. KONA (Der.), İstanbul, IQKültür Sanat, 2005, 107-126.

ÇEKEN, Hüseyin. "Council of Europe's Convention 2001 on Cybercrimes and Turkey", İstanbul, Marmara Üniversitesi Avrupa Topluluğu Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2003.

"Çalışma Grubu 4, E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları", Çalışma/Belgeleme Grupları 2. Ara Değerlendirme Raporu, TBD Kamu-BİB Bilişim Platformu VIII (Antalya 25-28 Mayıs 2005).

DAĞI, İhsan. "İnternet Türkiye'de ve Dünyada Demokrasiye Neler Kattı?", International Policy Fellowships. 24 Mart 2007 <<http://www.policy.hu/dagi/leftmenu/files/edevlet.pdf>>.

DASTYCH, David. "Another Watergate? Promisgate: World's Longest Spy Scandal Still Glossed Over", January 31, 2006, Canada Free Press. 12 Mart 2007 <<http://www.canadafreepress.com/2006/dastych013106.htm>>.

DEDEOĞLU, Beril. **Uluslararası Güvenlik ve Strateji**, İstanbul, Derin Yayınları, 2003.

DEĞİRMENCI, Olgun. "Bilişim Suçları", İstanbul, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2002.

DEMİRTAŞ, Erkan. "İnsan Hakları Avrupa Sözleşmesinin 8. Maddesi ve İlgili Yargı Kararları", Ocak 2004, Adalet Bakanlığı İnternet Sayfası. 29 Ocak 2006 <<http://www.inhak-bb.adalet.gov.tr/aihs/madde8.htm>>.

DENNING, Dorothy E. "Cyberterrorism", 23 May 2000, Gergetown University. 20 Ekim 2006 <<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>>.

Department of Defense Education Activity Internal Physical Security. Department of Defense. DoDEA Regulation 4700.2. 24 Aralık 2006 <http://www.dodea.edu/foia/iod/pdf/4700_2.pdf>.

DODGE, M. ve R. KITCHIN, **Mapping Cyberspace**, London, Routledge, 2001.

DONNELLY, Chris. "Küreselleşme Bağlamında NATO ve Avrupa Birliğinin Gelecekteki Roller", Küreselleşme ve Uluslararası Güvenlik, Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, 129-142.

DURAN, Mustafa. "AIHS 11. Madde Dernek Kurma ve Toplantı Özgürlüğü", Adalet Bakanlığı İnternet Sayfası. 29 Ocak 2006 <<http://www.inhakbb.adalet.gov.tr/aihs/madde11.htm>>.

DÜLGER, Volkan M. **Bilişim Suçları**, Ankara, Sekçin, 2004.

EDAPPAGATH, Ajmal. "Cyber-Laws and Enforcements to Optimize Benefits of ICT", **I-Ways**, XXVII, 3/4, 2004, 167-173.

"Economic Crime Survey 2001: European Report". 26 Mart 2007 <http://www.pwc.com/gx/eng/cfr/gecs/pwc_2001_europe_crimesurvey.pdf>.

"E-Dönüşüm Türkiye Projesi 2003-2004 KDEP Uygulama Sonuçları ve 2005 Eylem Planı", Eylül 2005. Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi. 04 Nisan 2007 <http://www.bilgitoplumu.gov.tr/yayin/KDEPUygulamaSonuclari_2005EylemPlani.pdf>.

"Elektromanyetik Dinleme ve Güvenlik (EDG)", 12 Mayıs 2001, Olympos Security İnternet Sayfası. 15 Nisan 2007 <http://www.olympos.org/article/articleview/278/1/10/elektromanyetik_dinleme_ve_guvenlik_edg>.

"Encryption: Impact on Law Enforcement", June 3, 1999, FBI. 21 Mart 2007
<<http://sion.quickie.net/en60399.pdf>>.

Encyclopedia Of New Media:An Essential Reference To Communication And Technology, S. JONES (Ed.), USA, Sage Publications, 2003.

ERBSCHLOE, Michael. **Implementing Homeland Security for Enterprise IT**, Burlington, MA: Digital Press, 2004.

ERDOĞAN, M. Zafer. "Hakimlerin Tarafsızlığı", Adalet Dergisi. 2 Haziran 2007.
<http://www.yayin.adalet.gov.tr/dergi/18_sayi.htm>.

ERKUL, R. Erdem. "Dünyada Kamu Yönetimindeki Dönüşüm ve Türkiye'de Kamu Yönetimi Öğretimine Yansımaları", II. Kamu Yönetimi Forumu (Beytepe, Ankara, 7-8 Ekim 2004). 22 Aralık 2006 <<http://www.digitaldevlet.net/edevlet.pdf>>.

ERSANEL, Nedret. **Siber İstihbarat**, Ankara, ASAM, 2001.

ERSOY, Eren. "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", Akademik Bilişim 2006 + BilgiTek IV (Pamukkale Üniversitesi, Denizli, 9-11 Şubat 2006). 04 Nisan 2007 <<http://ab.org.tr/ab06/bildiri/6.doc>>.

"E-Ticaret", Eylül 2006, Bursa Ekonomi Bursa Sanayi ve Ticaret Odası Aylık Yayın Organı. 11 Nisan 2007 <<http://www.bursaekonomi.com.tr/default.asp?page=newsopen.asp&opennews=470&qmshow=223>>.

"Explanatory Report", Council of Europe. 10 Ekim 2006 <<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>>.

From Gutenberg to The Internet: A Source Book on The History of Information Technology, J. M. NORMAN (Ed.), California, Historyofscience.com, 2005.

FULLER, Charlie. "The Community of Cyberspace", **Cyber Crime**, 2003, 9-21.

FULLER, Charlie. "Law Enforcement and Security", **Cyber Crime**, 2003, 77-89.

GABRYS, Ed. "The International Dimensions of Cyber-Crime, Part 1." **Information Systems Security**, XI, 4, September-October 2002, 21-32.

Gambling Act 2005, <<http://www.opsi.gov.uk/acts/acts2005/20050019.htm>>.

GERE, Charlie. **Digital Culture**, London, Reaktion Books, 2002.

GERSTENFELD, Phyllis B ve diğerleri. "Hate Online: A Content Analysis of Extremist Internet Sites", **Analyses of Social Issues and Public Policy**, III, 1, 2003, 29-44.

GIBSON, R. ve S. ERLE, **Google Maps Hacks**, U.S.A., O'Reilly Media Inc., 2006.

GOLDMAN, Emily O. "Introduction: Security in the Information Technology Age", **National Security in the Information Age**, Emily O. GOLDMAN (Ed.), London Portland, Frank Cass, 2004, 1-12.

GORDON, S. ve R. FORD, "Cyber Terrorism?", Symantec. 12 Kasım 2006 <<http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>>.

GRABOSKY, Peter. "Cyber Crime and Information Warfare", Australian Institute of Criminology. 08 Kasım 2006 <<http://www.aic.gov.au/conferences/transnational/grabosky.pdf>>.

"Hacking Techniques", High Tech Crime Brief, Australian Institute of Criminology, 2005.

HAKYEMEZ, Y. Şevki. "Demokratik Ülkelerde Milli Güvenlik Politikalarının Belirlenmesi ve Türkiye", **AÜEHFD**, VII, 3-4, Aralık 2003, 285-308.

HALAÇOĞLU, Yusuf. **Ermeni Tehciri**, 9.bs., İstanbul, Babıali Kültür, 2006.

HELMBRECHT, Udo. "Economic Dimension in Cyber Security". 26 Mart 2007 <http://www.bsi.bund.de/bsi/reden/2006_08_18_Erice.pdf>.

HILDRETH, Steven A. "Cyberwarfare", **CRS Report for Congress**, June 19, 2001. 07 Kasım 2006 <<http://www.fas.org/irp/crs/RL30735.pdf>>.

Internet Explorer and Outlook Express 6.0, Australia, Software Publications, 2002.

"Internet Usage In Europe", Internet World Stats. 12 Nisan 2007 <<http://www.internetworldstats.com/stats4.htm#europe>>.

İÇEL, Kayıhan. "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İÜHFM**, LIX, 1-2, 2001, 3-10.

İnsan Hakları, Ankara, Matus Basımevi, 2006.

JUHNKE, Deborah H. "Cyber Terrorism or Cyber Crime". 29 Aralık 2006 <<http://www.forensics.com/pdf/Cyber.pdf>>.

KAHRAMAN, Faruk. "CRM (Customer Relationship Management)". 04 Nisan 2007 <<http://tech-strategy.org/Manuel/CRM-Nedir-Ne-Degildir.pdf>>.

KARABEYOĞLU, Hamdi Ü. "Açıklamalı Ceza Muhakemesi Kanunu", Adalet Bakanlığı İnternet Sayfası. 15 Kasım 2006 <<http://www.cezabb.adalet.gov.tr/makale/127.doc>>.

KARAGÜLMEZ, Ali. **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, Ankara, Seçkin, 2005.

KARAGÜLMEZ, Ali. "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", **Çağın Polisi Dergisi**, IV, 46, Ekim 2005, 7-11.

KAYA, Mine. "Avrupa İnsan Hakları Sözleşmesinde Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı", Adalet Bakanlığı İnternet Sayfası. 29 Ocak 2006 <<http://www.inhak-bb.adalet.gov.tr/aihs/madde8.htm>>.

KESER BERBER, Leyla. "Adli Bilişim", **Güncel Hukuk**, 6, Haziran 2004, 19-20.

KESKİN, Serap. "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", **İÜHFM**, LIX, 1-2, 2001, 155-180.

KIEFER, Kimberly ve diğerleri. **Information Security: A Legal, Business, and Technical Hand Book**, U.S.A., American Bar Association, 2004.

KIZZA, Joseph M. **Computer Network Security**, USA, Springer Science+Business Media Inc., 2005.

KİPER, Mahmut. "Teknoloji Transfer Mekanizmaları ve Bu Kapsamda Üniversite Sanayi İşbirliği", **TMMOB 50. Yıl Yayınları....Teknoloji**, M. KİPER (Ed.), Ankara, Kozan Ofset, 2004.

KUZU, Burhan. "Düşünceleri Açıklama Özgürlüğü Alanında Geldiğimiz Nokta", **İÜHFM**, LIX, 1-2, 2001, 247-334.

KÖNİ, Hasan. "Ekonomik Güvenlik ve Uluslararası İlişkiler ve Türkiye", **Uluslararası Çatışma Alanları ve Türkiye'nin Güvenliği**, G. KONA (Der.), İstanbul, IQ Kültür Sanat Yayıncılık, 2005, 391-400.

KYKER, Keith. **Wading the World Wide Web: Internet Activities for Beginners**, U.S.A., y.y., 1998.

LAMPSON, Butler W. "Computer Security in the Real World". 28 Aralık 2006 <<http://www.acsac.org/invited-essay/essays/2000-lampson.pdf>>.

LARISA, Paul. "When Cyber Hacktivism Meets Cyberterrorism.", Jan. 2001. 11 Kasım 2006 <<http://rr.sans.org/hackers/terrorism.php>>.

LEWIS, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", December 2002, **Center for Strategic & International Studies**. 23 Kasım 2006 <http://www.csis.org/media/csis/pubs/021101_risks_of_cyberterror.pdf>.

LEWIS, James A. "Cyber Terror: Missing in Action", **Knowledge, Technology & Policy**, XVI, 2, Summer 2003, 34-41.

LIPSON, Howard F. **Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues**, Pittsburgh, Carnegie Mellon University, 2002.

MACOVEI, Monica. "İfade Özgürlüğü AIHS'nin 10. Maddesi'nin Uygulanmasına İlişkin Kılavuz", **İnsan Hakları El Kitapları, No. 2**, Adalet Bakanlığı İnternet Sayfası. 29 Ocak 2006 <<http://www.inhak-bb.adalet.gov.tr/aihs/madde10.htm>>.

MACZ, Mad. **Internet Underground: The Way of the Hacker**, U.S.A., PageFree Publishing Inc., 2002.

MAIWALD, Eric. **Fundamentals of Network Security**, U.S.A., McGraw-Hill , 2004.

"Main lines of the Convention", Council of Europe. 10 Ocak 2007 <http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/e_lignesconv.asp>.

MANGO, Andrew. "Küreselleşme Bağlamında Medyai Bilgi Harekatı ve Uluslararası Güvenlik", Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, 113-120.

MANION, M. ve A. GOODRUM, "Terrorism or Civil Disobedience: Toward a Hactivist Ethic", **Internet Security: Hacking, Counterhacking & Society**, K. E. HIMMA (Ed.), U.S.A., Jones and Barlett Publishers Inc., 2007, 61-72.

MERKOW, M. ve J. BREITHAUPT, **Computer Security Assurance Using The Common Criteria**, Canada, Thomson Delmar Learning, 2005.

METİN, Zafer. "Çağdaş Gelişme Eğilimleri Işığında Siber Suçlar ve Güvenlik Kuramı", İstanbul, İstanbul Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, 2003.

Microsoft Encarta 2006. Elektronik Sözlük

Milli Güvenlik Siyaseti ve Stratejisi, İstanbul, Harp Akademileri Komutanlığı Yayınları, 1996.

NAGPAL, Rohas. "Cyber Terrorism in the Context of Globalization", September 2002, **II World Congress on Informatics and Law (Spain) Tebliği**. 29 Aralık 2006 <<http://www.ieid.org/congreso/ponencias/Nagpal,%20Rohas.pdf>>.

NAGPAL, Rohas. "Tools and Techniques of Cyber Crime", 2004, Asian Scholl of Cyber Law. 10 Aralık 2006 <http://www.asianlaws.org/cyberlaw/library/cc/cc_tt.htm>.

NASHERI, Hedieh. **Economic Espionage and Industrial Spying**, U.S.A., Cambridge University Press, 2005.

NATHWANI, Niraj. "Atlantic Divide on Fight Against Racist Websites". 20 Şubat 2007 <http://eumc.europa.eu/eumc/index.php?fuseaction=content.dsp_cat_content&catid=3e3e6e32a2316&contentid=3e3e8aedef03d5>.

NESADURAI, Helen. "Introduction: Economic Security, Globalization and Governance", **The Pacific Review**, XVII, 4, 2004, 459-484.

NIE, Norman ve diğerleri. "Internet Use, Interpersonal Relations, and Sociability", **The Internet in Everyday Life**, B. WELLMAN, C. HAYTHORNTHWAITTE (Ed.), Blackwell Publishers Ltd., 2002, 215-243.

NOHUTÇU, A. ve D. DEMİREL, "E-Devlet:Genel Bir Çerçeve ve Teorik Bir Yaklaşım". 04 Nisan 2007 <http://www.nvi.gov.tr/attached/NVI/makale/e-devlet-genel_cerceve.pdf>.

OKIN, J.R. **The Internet Revolution: The not for Dummies Guide to the History, Technology, and Use of the Internet**, Maine, Ironbound Press, 2005.

ÖZCAN, Mehmet. "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu", Turkish Weekly. 01 Temmuz 2006 <<http://www.turkishweekly.net/turkce/makale.php?id=87>>.

ÖZEL, C. ve M. AHL, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", **Güncel Hukuk**, 6, Haziran 2004, 21-23.

PASTOR-SATORRAS, R. ve A. VESPIGNANI, **Evolution and Structure of The Internet: A Statistical Physics Approach**, Cambridge, Cambridge Univesity Press, 2004.

PATHAK, Jagdish. **Information Technology Auditing: An Evolving Agenda**, Berlin, Springer-Verlag, 2005.

POCAR, Fausto. "New Challenges for International Rules Against Cyber-Crime" **European Journal on Criminal Policy & Research**, X, 1, 2004, 27-37.

"Philippine Officials Charge Alleged 'Love Bug' Virus Creator", June 29, 2000, CNN. 14 Mart 2007 <<http://archives.cnn.com/2000/TECH/computing/06/29/philippines.lovebug.02/index.htm>>.

POCAR, Fausto. "New Challenges For International Rules Against Cyber-Crime", **European Journal on Criminal Policy & Research**, X, 1, 2004. 27-37.

RIEM, Anthony. "To Catch a Cyber Thief: Tracing Internet Crime", **The In House Lawyer**, March 2007, 43-46.

ROBERTS, P. A. ve S. CHALLINOR, "IP Address Management", **Carrier Scale IP Networks: Designing and Operating Internet Networks**, P. WILLIS (Ed.), London, The Institution of Electrical Engineers, 2001, 217-225.

ROBINSON, John P. ve diğerleri. "The Internet and Other Uses of Time", **The Internet in Everyday Life**, B. WELLMAN, C. HAYTHORNTHWAITE (Ed.), Blackwell Publishers Ltd., 2002, 244-262.

ROLLINS, J. ve C. WILSON, "Terrorist Capabilities for Cyberattack: Overview and Policy Issue", **CRS Report for Congress**, October 20, 2005. 27 Kasım 2006 <<http://www.usembassy.it/pdf/other/RL33123.pdf>>.

RUSSELL, Deborah. ve G.T. GANGEMI, **Computer Security Basics**, U.S.A., O'Reilly&Associates Inc., 1992.

SAĞSAN, Mustafa. "Bilgi Teknolojileri Güvenliği: Ulusal Bilginin Korunmasına Pragmatik Bir Yaklaşım ve Türkiye Perspektifi", **Stratejik Analiz**, II, 22, Şubat 2002, 74-81.

SAĞSAN, Mustafa. "Akıllı Toplum Olma Yolunda Ulusal Bilgi Stratejisi ve Bilgi Ortaklığı", **Stratejik Analiz**, II, 18, Ekim 2001, 87-93.

SALOMON, David. **Foundations of Computer Security**, U.S.A., Springer-Verlag London Ltd., 2006.

SANDIKLI, A. ve G. YİVCİGER, TASAM Siber Terörizm Raporu, Stratejik Rapor No:2.

SCHJOLBERG, Stein. "Computer-Related Offences", A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime (15-17 September 2004, Council of Europe, Strasbourg, France). 09 Mart 2007 <<http://www.cybercrimelaw.net/documents/Strasbourg.pdf>>.

SCHJOLBERG, S. ve A. HUBBARD, "Harmonizing National Legal Approaches on Cybercrime", ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 28 June – 1 July 2005), ITU, 2005.

Security and Development, R. PICCIOTTO, R. WEAIVING (Ed.), New York, Routledge, 2006.

SEPER, Jerry. "Software Likely in Hands of Terrorist (Promis/Inslaw)", Washington Times, 14 June 2001. 12 Mart 2007 <<http://www.freerepublic.com/forum/a3b28933d7f22.htm>>.

SHAFFER, Howard J. "Internet Gambling & Addiction", January 16, 2004. 29 Mart 2007 <<http://www.divisiononaddictions.org/html/publications/shafferinternetgambling.pdf>>.

SHINDER, Debra L. **Scene of the Cybercrime: Computer Forensics Handbook**, USA, Syngress Publication, 2002.

SIEBER, Ulrich. "Legal Aspects of Computer-Related Crime in The Information Society-Comcrime Study". 10 Kasım 2006 <<http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc>>.

SINROD, J. Eric ve W. P. REILLY, "Cyber-Crimes: A Practical Approach to The Application of Federal Computer Crime Laws", **Santa Clara Computer And High Technology Law Journal**, XVI, 2, May 2000, 1-53.

Siber Suçlar Sözleşmesi'ne Ek Protokol, "Additional Protocol to the Convention on Cybercrime, Concerning The Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems ETS No.: 189".
<<http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>>.

SJURSEN, Helene. "Security and Defence", ARENA. 24 Şubat 2007
<http://www.arena.uio.no/publications/wp03_10.pdf>.

SMITH, Russell G. ve diğerleri. **Cyber Criminals on Trial**, Australia, Cambridge University Press, 2004.

Symantec Internet Security Threat Report:Trends For July–December 06, XI, Mart 2007.

Symantec EMEA Internet Security Threat Report:Trends For July–December 06, XI, Mart 2007.

SOKULLU-AKINCI, Füsün. "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", **İÜHFİM**, LIX, 1-2, 2001, 11-38.

SOLOMON, M. G., M. CHAPPLE, **Information Security Illuminated**, U.S.A., Jones and Barlett Publishers, 2005.

SOYSAL, Tamer. "İnternet Servis Sağlayıcıların Hukuki Sorumlulukları", **Türkiye Barolar Birliği Dergisi**, 18, 61, Kasım-Aralık 2005, 304-340.

"SPSS Veri Madenciliği Çözümleri", SPSS İnternet sayfası. 04 Nisan 2007
<<http://www.spss.com.tr/Web%20link/6-Veri%20Madenciligi.pdf>>.

STERN, Maria. **Naming Security-Constructing Identity**, New York, Manchester University Press, 2006.

ŞAHİN, Ali ve diğerleri. "Türkiye'de Demokrasiden E-Demokrasiye Geçiş Süreci ve Karşılaşılan Sorunlar", 3. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi (Osman Gazi Üni. İktisadi ve İdari Bilimler Fakültesi, Eskişehir, 25-26 Kasım 2004). 24 Mart 2007
<<http://iibf.ogu.edu.tr/kongre/bildiriler/06-02.pdf>>.

ŞEHİTOĞLU, Onur. “Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Mücadelenin Hukuksal ve Güvenlik Boyutu”, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2005.

T.C. Ulaştırma Bakanlığı Haberleşme Genel Müdürlüğü İnternet Sayfası. 10 Ocak 2007 <<http://www.ubak.gov.tr/tr/hgm/mevcut.htm>>.

Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik, <<http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/telekom-hiz-altyapi.pdf>>.

Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, <http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/Kisisel_Bil_Yon_06_02_04.pdf>.

Temel Hukuk Bilgisi, Y. ATAR, S. KARAHAN (Ed.), Konya, Mimoza, 2006.

TERASHIMA, Nobuyoshi. **Intelligent Communication Systems**, USA, Academic Press, 2002.

Terörle Mücadele Kanunu, 1991, <<http://www.mevzuat.adalet.gov.tr>>.

The U.S. History Highway: A Guide to Internet Resources, D. A. TRINKLE, S. A. MERRIMAN (Ed.), New York, M. E. Sharpe Inc., 2002.

THOMAS, Timothy L. “Al Qaeda and The Internet: The Danger of Cyberplanning”, 2003. 27 Kasım 2006. <<http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf>>.

TIEFENBRUN, Susan. “A Semiotic Approach to a Legal Definition of Terrorism”, **ILSA Journal of International & Comparative Law**, IX, 357-402.

TİMUR, Necdet. “Ulusal Güvenlik”, **Uluslararası Çatışma Alanları ve Türkiye’nin Güvenliği**, G. KONA (Der.), İstanbul, IQKültür Sanat, 2005, 557-563.

TUNA, Gülgün. **Küresel Ekonomik ve Sosyal Tehditler, Yeni Güvenlik**, Ankara, Nobel, 2003.

TURGUT, Reşat. “Küreselleşmenin Askerî Boyutları ve Güvenlik Stratejilerine Etkileri”, Küreselleşme ve Uluslararası Güvenlik, Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, 41-44.

TULUNAY, E. ve F. SARI, “Kamu Kurum ve Kuruluşları ile Özel Kurum ve Kuruluşların, Bilgi Teknolojisi Alanında Ulusal Güvenlik Politikası Doğrultusunda Yönlendirilmeleri.” Konulu bildiri”, 07 Şubat 2007 <<http://www.harpak.tsk.mil.tr/duyurular/SEMPOZYUM/09%20Prof%20Dr%20Ersin%20TULUNAY.DOC>>.

“Türk Ceza Kanunu Madde Gerekçeleri”, Adalet Bakanlığı İnternet sitesi, 10 Aralık 2006, <<http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc>>.

Türkçe Sözlük, 9.bs., Türk Dil Kurumu, Ankara, 1998.

“Türkiye İnternet’te Saldırı Şampiyonu”, BTDünyası İnternet sayfası. 22 Mart 2007 <http://www.btdunyasi.net/index.php?module=news&news_id=3556&cat_id=1,09>.

UÇKAN, Özgür. “E-Devlet, E-Demokrasi ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü”, Stradigma. 30 Mart 2007 <http://www.stradigma.com/turkce/haziran2003/print_09.html>.

UĞURLU, Hakan. “Küreselleşme ve Ulusal Güvenlik (1990 Sonrası)”, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2005.

“ULAKBİM’in Tarihçesi”, TUBİTAK ULAKBİM İnternet Sayfası. 12 Nisan 2007 <<http://www.ulakbim.gov.tr/hakkinda/tarihce/>>.

“Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı”, 01 Mart 2007, Türkiye Bilişim Derneği. 05 Mart 2007 <http://www.tbd.org.tr/genel/bizden_detay.php?kod=245&tipi=5&sube=>>.

“Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi”, Kasım 2004, TUBİTAK. 04 Nisan 2007 <http://vizyon2023.tubitak.gov.tr/Strateji_Belgesi-V211.pdf>.

“Effective Measures to Prevent and Control Computer-Related Crime: Report of The Secretary-General”, 29 January 2002, United Nations Economic and Social Council. 26 Mart 2007 <<http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf>>.

Unlawful Internet Gambling Enforcement Act in October 2006, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr412p1.109.pdf

U.S. Departman of Justice İnternet sayfası. 29 Aralık 2006 <<http://www.cybercrimes.net/Terrorism/ct.html>>.

ÜNERİ, Mert. “e-Dönüşüm Türkiye Bilgi Güvenliği Projeleri”. 04 Nisan 2007 <http://www.bilgitoplumu.gov.tr/duyuru/lcraKurulu/20070123_IK_XX_UEKAE_BILGI_GUVENLIGI.pdf>.

ÜNVER, Yener. “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısı’nın İnternet Açısından Değerlendirilmesi”, **İÜHFM**, LIX, 1-2, 2001, 51-153.

WÆVER, Ole ve diğerleri. **Identity, Migration and The New Security Agenda in Europe**, New York, St. Martin’s Press, 1993.

WALLANDER, Celeste A ve diğerleri. “Introduction”, **Imperfect Unions: Security Institution over Time and Space**, H. HAFTENDORN, R. KEOHANE, C. WALLANDER (Ed.), New York, Oxford University Press, 1999, 1-18.

WHINE, Michael. “The Far Right on the Internet”, **The Governance of Cyberspace**, B. D. LOADER (Ed.), New York, Routledge, 1997, 209-227.

WHITTAKER, Jason. **The Cyberspace Handbook**, Oxon, Routledge, 2004.

WILSON, Clay. “Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress”, **CRS Report for Congress**, October 17, 2003. 27 Kasım 2006 <<http://www.fas.org /irp/crs/RL32114.pdf>>.

WIPO İnternet Sitesi, Türkiye’nin WIPO çatısı altında taraf olduğu tüm Sözleşmeler, Sözleşme metinleri ve üyelik bilgileri, “<http://www.wipo.int/portal/index.html.en>”

WORTLEY, R. ve S. SMALLBONE, “Child Pornography on the Internet”, **Problem-Oriented Guides for Police Problem-Specific Guides Series Guide No. 41**, U.S. Department of Justice, 2006.

VOGLER, John. “Küreselleşmenin Çevresel Boyutları ve Güvenlik Stratejilerine Etkileri”, Küreselleşme ve Uluslararası Güvenlik, Birinci Uluslararası Sempozyum Bildirileri (İstanbul, 29-30 Mayıs 2003), Ankara, SAREM, 2003, 45-60.

YALÇIN, Cemal. “Sosyolojik Bir Bakış Açısıyla İnternet”, **C.Ü. Sosyal Bilimler Dergisi**, XXVII, 1, Mayıs 2003, 77-89.

YALÇIN, Özgür. "Hangi Yüzle". GAZETE ODTÜLÜ. 16 Mart 2007 <<http://www.gazeteodtulu.com/yazilar.php?id=114>>.

YAZICIOĞLU, R. Yılmaz. **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle**, İstanbul, Alfa, 1997.

YAZICIOĞLU, Yılmaz. "Bilişim Suçları", **Bilişim Teknolojisi Hukuku Gündemi 2004-2005**, İstanbul, Bilgi Üniversitesi, 2006, 65-75.

YENİDÜNYA, A. C. ve O. DEĞİRMENÇİ. **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal, 2003.

Yeni Dünya Stratejileri ve Kilit Ülke Türkiye, A. KULEBLİ (Ed.), Ankara, TUSAM MET-VAK Yay., t.y.

YILDIRIM, Hakan ve diğerleri. **"Her Şeyi e-leştirdik"**, 2.bs., Ankara, Macar Yayıncılık, 2003.

YILMAZ, A. ve S. GÜNAYERGÜN, "Türkiye'de Şehir Asayiş Suçları: Dağılışı ve Başlıca Özellikleri", Milli Eğitim Bakanlığı. 28 Mart 2007 <<http://yayim.meb.gov.tr/dergiler/170/170/ali%20yilmaz.pdf>>.

YÜCEL, İ. Hakkı. "Bilim-Teknoloji Politikaları ve 21 Yüzyılın Toplumu", 1997. 07 Ocak 2007 <<http://ekutup.dpt.gov.tr/bilim/yucelih/biltek.html>>.

"Y2K bug", **Britannica Concise Encyclopedia**. 27 Mart 2007 <<http://concise.britannica.com/ebc/article-9383056/Y2K-bug>>.

ZOMBORI, Gyula. "e + Finance + Crime a Report On Cyber-Crime and Money Laundering", 15 January 2001. 09 Mart 2007 <http://www.yorku.ca/nathanson/Publications/e.htm#_Toc504182577>.