T.C.

Radyo ve Televizyon Üst Kurulu

BİLGİ GÜVENLİĞİ UYGULAMALARI VE ÇÖZÜM ÖNERİLERİ

ÜST KURUL UZMANLIK TEZİ

Seyda MENTEŞ

ANKARA

KASIM / 2018

T.C.

Radyo ve Televizyon Üst Kurulu

BİLGİ GÜVENLİĞİ UYGULAMALARI VE ÇÖZÜM ÖNERİLERİ

ÜST KURUL UZMANLIK TEZİ

Seyda MENTEŞ

DANIŞMAN

ÜST KURUL UZMANI Şahin AY

ANKARA

KASIM / 2018

RADYO VE TELEVİZYON ÜST KURULU BAŞKANLIĞINA

Bu çalışma, Tez Değerlendirme Komisyonu tarafından oy birliği/oy çokluğu ile Uzmanlık Tezi olarak kabul edilmiştir.

	Adı Soyadı	İmza
Başkan	: Doç. Dr. Hamit ERSOY Üst Kurul Üyesi	
Üye	: Hikmet İNCE Üst Kurul Başkan Yardımcısı	
Üye	: İlker ILGIN Üst Kurul Başkan Yardımcısı	
Üye	: Dr. Yaşar UĞURLU İzleme ve Değerlendirme Dai. Bşk. V.	
Üye	: Şahin AY Üst Kurul Uzmanı	

ONAY
... / ... / 2018

Prof. Dr. İlhan YERLİKAYA
Üst Kurul Başkanı

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI

Radyo ve Televizyon Üst Kurulu Uzman Yardımcılığı Giriş ve Yeterlik Sınavları ile Uzmanlığa Atanma, Yetiştirilme, Görev, Yetki ve Çalışma Usul ve Esasları Hakkında Yönetmeliğin 19'uncu maddesinin 4'üncü fıkrasına istinaden çıkartılan Radyo ve Televizyon Üst Kurulu Tez Hazırlama Yönergesi' ne uygun olarak hazırlamış olduğum uzmanlık tezi ilişikte sunulmuştur.

Bu uzmanlık tezindeki bütün bilgileri akademik kurallara ve etik davranış ilkelerine uygun olarak toplayıp sunduğumu; ayrıca, bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi beyan ederim.

Bilgilerinizi ve gereğini arz ederim.

… / 11 / 2018
Seyda MENTEŞ
Üst Kurul Uzman Yardımcısı
Uzmanlık Tezinin Adı: Bilgi Güvenliği Uygulamaları ve Çözüm Önerileri

EK:

1- Tez (2 Adet)
2- CD (1 Adet)

Tezi Teslim Alan
Daire Başkanı

... / 11 / 2018

TEŞEKKÜR

"Bilgi Güvenliği Uygulamaları ve Çözüm Önerileri" isimli bu tezin hazırlanması sürecinde öncelikle Üst Kurul Başkanı Sayın Prof. Dr. İlhan YERLİKAYA'ya, Üst Kurul üyelerine ve tez değerlendirme komisyonu üyelerine teşekkürlerimi sunarım.

Tez çalışmamda yoğun çalışma temposuna rağmen desteğini esirgemeyen, çalışmaya her türlü bilgi ve tecrübesini aktaran tez danışmanım Üst Kurul Uzmanı Sayın Şahin AY'a teşekkürü bir borç bilirim.

Tez çalışmam boyunca hoşgörüsüyle çalışma şartlarımı kolaylaştıran Daire Başkan Vekilim Sayın Yasin YİĞİT, Daire Başkan Yardımcım Sayın Ali SARI ve birlikte çalıştığım değerli mesai arkadaşlarıma teşekkürlerimi sunarım.

Çalışmaya başladığım ilk günden itibaren manevi desteğini sürekli üzerimde hissettiğim, bana her konuda destek olan sevgili eşim Asiye MENTEŞ'e ve tez sürecinde dünyaya gelerek hayatımızı renklendiren canım oğlum Ömer Alp'e sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

TEŞEKKÜR I

İÇİNDEKİLER II

KISALTMALAR VI

ŞEKİLLER LİSTESİ XI

TABLOLAR LİSTESİ XII

GİRİŞ 1

BİRİNCİ BÖLÜM 7

BİLGİ GÜVENLİĞİ İLE İLGİLİ KAVRAMLAR 7

1.1. BİLGİ KAVRAMI 7

1.2. BİLGİ GÜVENLİĞİ 10

1.3. BİLGİ GÜVENLİĞİNİN UNSURLARI 11

1.3.1. Gizlilik 13

1.3.2. Bütünlük 14

1.3.3. Erişilebilirlik 15

1.3.4. Diğer Unsurlar 16

1.4. BİLGİ GÜVENLİĞİNİN TARİHSEL GEÇMİŞİ 17

1.5. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) 20

1.5.1. ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı 22

1.5.2. COBIT 24

1.5.3. ITIL 26

1.5.4. PCI DSS 27

1.5.5. HIPAA 27

İKİNCİ BÖLÜM 29

SİBER GÜVENLİK VE SİBER SALDIRI TÜRLERİ 29

2.1. SİBER KAVRAMI 29

2.2. SİBER UZAY 30

2.3. SİBER GÜVENLİK 32

2.4. SİBER SALDIRI 34

2.5. SİBER SALDIRI TÜRLERİ 36

2.5.1. Kötücül Yazılımlar 36

2.5.1.1. Virüsler 38

2.5.1.2. Solucanlar (Worm) 39

2.5.1.3. Truva Atları (Trojen) 39

2.5.1.4. Tuş Kaydedici (Keylogger) 40

2.5.1.5. Şebeke Trafiğinin Dinlenmesi (Sniffing) 41

2.5.1.6. IP Aldatmacası (IP Spoofing) 41

2.5.1.7. BOTNET Ağları 42

2.5.2. Oltalama (Phishing) 43

2.5.3. Rootkit 44

2.5.4. DDoS (Hizmet Dışı Bırakma) Saldırıları 45

2.5.5. Ransomware (Fidye Yazılımı) 47

2.6. SOSYAL MÜHENDİSLİK 49

2.6.1. Sosyal Mühendislik Saldırı Yöntemleri 50

2.7. SİBER ZORBALIK 53

ÜÇÜNCÜ BÖLÜM 58

ULUSLARARASI ALANDA SİBER GÜVENLİK 58

3.1. ULUSLARARASI SİBER GÜVENLİK FAALİYETLERİ 58

3.1.1. Avrupa Birliği (AB) 59

3.1.2. Kuzey Atlantik Antlaşması Örgütü (NATO) 60

3.1.3. Birleşmiş Milletler (BM) 62

3.2. ÜLKELER 66
3.2.1. Amerika Birleşik Devletleri 66
3.2.2. Çin Halk Cumhuriyeti 68
3.2.3. Rusya Federasyonu 69
3.2.4. İran 70
3.2.5. İngiltere 71
3.2.6. İsrail 73
3.2.7. Almanya 75
3.2.8. Fransa 76

3.3. ULUSLARARASI ALANDA GERÇEKLEŞEN BÜYÜK SİBER SALDIRILAR 78
3.3.1. Stuxnet 78
3.3.2. Duqu 82
3.3.3. Flame 83
3.3.4. Gauss 85
3.3.5. Estonya Siber Saldırıları 85
3.3.6. WannaCry Fidye Yazılımı 87
3.3.7. Sony Pictures Şirketine Yönelik Saldırılar 90

DÖRDÜNCÜ BÖLÜM 92

TÜRKİYE'DE BİLGİ TOPLUMUNA DÖNÜŞÜM SÜRECİ VE SİBER GÜVENLİK ALANINDA YAPILAN ÇALIŞMALAR 92

4.1. BİLGİ TOPLUMUNA DÖNÜŞÜM SÜRECİ 93
4.1.1. Bilişim ve Ekonomik Modernizasyon Raporu 93
4.1.2. Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) 93
4.1.3. Elektronik Ticaret Koordinasyon Kurulu 96
4.1.4. e-Türkiye Projesi 96
4.1.5. e-Dönüşüm Türkiye Projesi 97
4.1.6. 2003-2004 Kısa Dönem Eylem Planı 99
4.1.7. 2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı 99
4.1.8. 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı 103

4.2. TÜRKİYE'DE SİBER GÜVENLİK ÇALIŞMALARI 104
4.2.1. Türkiye'de Siber Güvenlik Faaliyetlerinde Bulunan Kurumlar 107
4.2.1.1. Siber Güvenlik Enstitüsü 107
4.2.1.2. Siber Suçlarla Mücadele Daire Başkanlığı 108
4.2.1.3. TSK Siber Savunma Merkezi Komutanlığı 109
4.2.1.4. Siber Güvenlik Kurulu 109
4.2.1.5. USOM ve SOME'ler 111
4.2.1.6. Türkiye Bilişim Derneği 114
4.2.1.7. Bilgi Güvenliği Derneği 116
4.2.2. Ulusal Siber Güvenlik Stratejileri 117
4.2.2.1. Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı 117
4.2.2.2. Ulusal Siber Güvenlik Stratejisi 2016-2019 Eylem Planı 118
4.2.3. KamuNet Projesi 122
4.3. YASAL DÜZENLEMELER 123
4.3.1. 5237 Sayılı TCK'da Bilişim Suçlarına Yönelik Düzenlemeler 123
4.3.2. 5809 Sayılı Elektronik ve Haberleşme Kanunu 127
4.4.3. 5070 Sayılı Elektronik İmza Kanunu 128
4.4.4. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 128
4.4.5. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu 129
4.4.6. 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) 129
4.4. 2017 GCI RAPORUNDA TÜRKİYE'NİN DURUMU 130
SONUÇ VE DEĞERLENDİRME 134
KAYNAKÇA 140
ÖZET 151
ABSTRACT 152
ÖZGEÇMİŞ 153

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AET	Advanced Evasion Techniques (Gelişmiş Saldırı Yöntemleri)
a.g.b	Adı Geçen Belge
a.g.e	Adı Geçen Eser
a.g.k	Adı Geçen Kitap
a.g.m	Adı Geçen Makale
a.g.p	Adı Geçen Plan
a.g.r.	Adı Geçen Rapor
a.g.t	Adı Geçen Tez
ANSSI	Agence Nationale de la Sécurite des Systémes d'Information (Fransız Ağ ve Bilgi Güvenliği Teşkilatı)
AR-GE	Araştırma Geliştirme
ARPA	Advanced Research Projects Agency (Gelişmiş Savunma Araştırma Projeleri Birimi)
ARPANET	Advanced Research Projects Agency Network (Gelişmiş Savunma Araştırma Projeleri Dairesi Ağı)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGE	Bilişim Sistemleri Güvenliği Enstitüsü
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİLGEM	Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BSI	British Standards Institute (İngiliz Standartlar Enstitüsü)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BTYK	Bilim ve Teknoloji Yüksek Kurulu
C4I	Command, Control, Communications, Computers and Intelligence (Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat)

CCDCOE	Cooperative Cyber Defence Centre of Excellence (Müşterek Siber Savunma Mükemmeliyet Merkezi)
IRCERT	Iran Computer Emergency Response Team (İran Bilgisayar Acil Müdahale Ekibi)
CGSD	Cyber and Government Security Directorate (Siber ve Devlet Güvenliği Direktörlüğü)
CIA	Central Intelligence Agency (Merkezi İstihbarat Teşkilatı)
CIWIN	Critical Infrastructure Warning Information Network (Kritik Altyapı Uyarı Bilgi Ağı)
COBIT	Control Objectives for Information and Related Technology (Bilgi ve İlgili Teknolojilerine İlişkin Kontrol Hedefleri)
DDoS	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DGSE	Direction Générale de la Sécurite Extérieure (Fransa Dış Güvenlik Teşkilatı)
DGSI	Direction Générale de la Sécurite Intérieure (Fransa İç Güvenlik Teşkilatı)
DHS	Department of Homeland Security (Amerika İç Güvenlik Bakanlığı)
DPT	Devlet Planlama Teşkilatı
EC³	European Cybercrıme Centre (Avrupa Siber Suç Merkezi)
EGM	Emniyet Genel Müdürlüğü
ENIAC	Electronic Numerical Integrator And Computer (Elektronik Sayısal Entegreli Hesaplayıcı)
ENISA	European Union Agency for Network and Information Security (Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı)
EPCIP	The European Programme for Critical Infrastructure Protection (Avrupa Kritik Altyapıları Koruma Programı)
EPDK	Enerji Piyasası Düzenleme Kurumu
ETKK	Elektronik Ticaret Koordinasyon Kurulu
FATA	İran Siber Polis Birimi
FBI	Federal Bureau of Investigation (Federal Soruşturma Bürosu)
FTP	File Transfer Protocol (Dosya Aktarım Protokolü)

GCA	Global Cybersecurity Agenda (Küresel Siber Güvenlik Gündemi)
GCI	Global Cybersecurity Index (Küresel Siber Güvenlik Raporu)
GOP	Guardians of Peace (Barış Muhafızları - Hacker Grubu)
GSM	Global System for Mobile Communications (Küresel Mobil Haberleşme Sistemi)
HIPAA	Health Insurance Portability and Accountability Act (Amerikan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu)
HLEG	High Level Experts Group (Yüksek Seviyeli Uzmanlar Grubu)
IEC	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
IMPACT	International Multilateral Partnership Against Cyber Threats (Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği)
INCB	Israel National Cyber Bureau (İsrail Ulusal Siber Bürosu)
IP	Internet Protocol (İnternet Protokolü)
IRGC	The Islamic Revolutionary Guard Corps (İran Devrim Muhafızları Ordusu)
ISACA	Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Derneği)
ISO	International Organization for Standardization (Uluslararası Standardizasyon Teşkilatı)
ITGI	IT Governance Institute (Bilgi Teknolojileri Yönetim Enstitüsü)
ITIL	Information Technologies Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
KamuNet	Kamu Sanal Ağı
KDEP	Kısa Dönem Eylen Planı
KOBİ	Küçük ve Orta Ölçekli İşletmeler
KVKK	Kişisel Verilerin Korunması Kanunu

MASAK	Mali Suçları Araştırma Kurulu
MEBS	Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri
MGK	Milli Güvenlik Kurulu
MİT	Milli İstihbarat Teşkilatı
NATO	North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
NCIRC	NATO Computer Incident Response Capability (NATO Bilgisayar Olaylarına Müdahale Yeteneği)
NCSC	National Cyber Security Centre (Ulusal Siber Güvenlik Merkezi)
NCT	National Cybernetics Taskforce (Milli Sibernetik Görev Gücü)
NIST	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NSA	National Security Agency (Ulusal Güvenlik Ajansı)
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information de la Communication (Bilişim Teknolojileri ile İlgili Suçlarla Mücadele Dairesi)
PCI DSS	Payment Card Data Security Standard (Kartlı Ödeme Endüstrisi Veri Güvenliği Standardı)
PDOI	Passive Defence Organization of Iran (İran Pasif Savunma Teşkilatı)
PLA	Public Liberation Army (Çin Halk Kurtuluş Ordusu)
PLC	Programmable Logic Controller (Programlanabilir Mantıksal Denetleyici)
PUKÖ	Planla – Uygula – Kontrol Et – Önlem Al
SCADA	Supervisory Control and Data Acqusition (Kapsamlı ve Entegre Veri Tabanlı Kontrol ve İzleme Sistemi)
SGE	Siber Güvenlik Enstitüsü
SİSAMER	Siber Savunma Harekât Merkezi
SOME	Siber Olaylara Müdahale Ekibi
SPK	Sermaye Piyasası Kurulu

SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
TCK	Türk Ceza Kanunu
TCMB	Türkiye Cumhuriyet Merkez Bankası
TDK	Türk Dil Kurumu
TİB	Telekomünikasyon İletişim Kurumu
TSE	Türk Standartları Enstitüsü
TSK	Türk Silahlı Kuvvetleri
TTGV	Türkiye Teknoloji Geliştirme Vakfı
TUENA	Türkiye Ulusal Enformasyon Altyapısı Ana Planı
TÜBA	Türkiye Bilimler Akademisi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB	Ulaştırma Denizcilik ve Haberleşme Bakanlığı
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UNGA	United Nations General Assembly (Birleşmiş Milletler Genel Kurulu)
UNSC	United Nations Security Council (Birleşmiş Milletler Güvenlik Konseyi)
USB	Universal Serial Bus
USCYBERCOM	United States Cyber Command (Birleşik Devletler Siber Komutanlığı)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
Wi-Fi	Wireless Fidelity (Kablosuz Bağlantı Alanı)

ŞEKİLLER LİSTESİ

Şekil 1.1 Bilgi Piramidi 8
Şekil 1.2 McCumber Bilgi Güvenliği Modeli 11
Şekil 1.3 Solomon CIA Üçgeni 12
Şekil 1.4 Bilgi Güvenliğinin Diğer Unsurları 16
Şekil 1.5 BGYS Süreçlerinde Uygulanan PUKÖ Modeli 23
Şekil 1.6 COBIT Süreçleri 25
Şekil 2.1 Anlık Küresel Siber Saldırı Haritası 35
Şekil 2.2 Dünya Geneli ve Türkiye Zararlı Yazılım Bulaşma Oranları 37
Şekil 2.3 Dünya Geneli Anlık DDOS Saldırıları Haritası 46
Şekil 2.4 Yıllara Göre Dünya Geneli Fidye Yazılımı Bulaşma Oranı 48
Şekil 2.5 Fidye Yazılımından Etkilenen Ülkelerin Dağılımı 48
Şekil 2.6 Sosyal Mühendislik Saldırılarının Aşamaları 50
Şekil 3.1 Küresel Siber Güvenliğin Beş Ana Unsuru 63
Şekil 3.2 Ülkelerin Siber Savunma Kapasitelerine İlişkin Harita 65
Şekil 3.3 Stuxnet'ten Etkilenen Ülkelerin Küresel Dağılımı (İlk 14 Ülke) 82
Şekil 3.4 WannaCry Saldırılarından Etkilenen Ülkelerin Dağılımı 89
Şekil 4.1 Bilgi Toplumu Stratejisi Eylem Planının Eksenlere Göre Başarı Oranı 102
Şekil 4.2 Ulusal Siber Olaylara Müdahale Organizasyonu 112
Şekil 4.3 SGE Organizasyon Şeması 108
Şekil 4.4 Kritik Altyapı Sektörleri 120

TABLOLAR LİSTESİ

Tablo 1 Çevrimiçi Taciz Türlerine İlişkin Veriler _____ 54
Tablo 2 TUENA Çalışmalarına Dair Rakamlar _____ 95
Tablo 3 Yedi Eksende Gerçekleştirilmesi Planlanan Eylem Sayıları _____ 101
Tablo 4 Sektörel SOME Kurulacak Kurumlar _____ 113
Tablo 5 GCI 2017 Raporunda Ülkemizin Siber Güvenlik Alanındaki Durumu __ 131

GİRİŞ

İnsan, geçmişten günümüze içgüdüsel olarak değerli gördüğü her şeyi koruma çabası içinde olmuştur. Yaşamın her alanında ihtiyaç duyulan bilgi de, insanlarca korumaya değer görülen varlıkların başında olagelmiştir. İnsanların hayatta kalabilmelerinde, düşüncelerinin şekillenmesinde ve gelişim süreçlerinde en önemli etken olan bilginin korunması için her dönemde zamanın şartlarına göre çeşitli önlemler alınmıştır.

Yazının icadından önceki dönemlerde bilginin sonraki dönemlere aktarılması belli oranda mümkün olabilmiştir. Yazının icadı, elde edilen bilgilerin sonraki dönemlere daha iyi aktarılabilmesi bakımından bir dönüm noktası olmuştur. Yazı her ne kadar bilginin aktarımına imkân tanımış olsa da; bilginin izinsiz olarak ele geçirilebilmesi ya da içeriğinin izinsiz değiştirilebilmesi problemlerini de beraberinde getirmiştir. O dönemlerden itibaren bilgi güvenliğini sağlamak amacıyla çeşitli işaretler, semboller ve şifreler kullanılmaya başlanmıştır.

İlk başlarda yazılı materyallerin korunması ile başlayan bilginin korunma süreci; günümüze doğru geldikçe fikirlerin, eserlerin ve buluşların korunmasını sağlamak amacıyla ortaya çıkan kanunlarla sağlanmaya çalışılmıştır.

1990'lı yıllara kadar arşiv ortamlarında fiziksel olarak saklanan bilgiler, bu yıllardan itibaren internet ve bilgi teknolojileri altyapılarının yaygınlaşmasıyla birlikte sanal ortamlara aktarılarak saklanmaya başlamıştır.

2000'li yıllara gelindiğinde tüm dünyayı saran internet ve bilişim ağları insanların hayatını kolaylaştırarak, insanların teknolojiye bağımlı hale gelmesine

sebep olmuştur. Teknolojik gelişmeler bilginin tek bir kaynaktan milyonlarca noktaya çok kısa sürede iletilebilmesini, verilerin sayısal ortamlarda saklanabilmesini ve bu verilere istenilen anda istenilen yerden ulaşılabilmesini mümkün kılmaya başlamıştır.

Günümüzde bankacılık, finans, sağlık, eğitim, su yönetimi, enerji, gıda, e-devlet, e-ticaret ve bulut bilişim hizmetleri gibi birçok kamu ve özel sektör hizmeti devletler tarafından kritik altyapı sektörleri olarak kabul edilmiştir. Bu sektörlerde sunulan hizmetlerin bilişim sistemleri altyapıları kullanılarak sanal ortama aktarılması; sunulan hizmetlerin hızını arttırmış, maliyetleri düşürmüş ve hizmetlerin şeffaflığını arttırmıştır.

Kritik altyapı sektörlerinde sunulan hizmetlerin çeşitlenmesine bağlı olarak her geçen gün artan veri trafiği ve kullanıcı sayısındaki artış ile birlikte bilgi güvenliği ihlalleri de artış göstermeye başlamıştır. Günden güne artan ve güçlenen tehditler sahip olunan bilgilerin istenilen anda erişilebilir ve analiz edilebilir olmasını gerektirmektedir. Siber ortamda birçok tehdide açık hale gelen bilginin zarar görmeden saklanması, iletilmesi ve sunulan hizmetlerin kesintiye uğramaması için bilgi güvenliğinin sağlanması kritik öneme sahiptir. Bu nedenle bilgi güvenliği alanında alınan tedbirler devletler, kurumlar ve bireyler için önemli hale gelmiştir.

Birçok olumsuz eylemin gerçekleştirilebilmesi için uygun bir altyapı sunan küresel internet ağı, örgütlü sınır ötesi siber saldırıların kolaylıkla gerçekleştirilebilmesine imkân tanımaktadır. Siber saldırılar saldırganın yeteneklerini ispatlama, maddi ve manevi menfaat sağlama, bireylere ya da devletlere ait gizli bilgileri ele geçirme gibi amaçlarla gerçekleştirilmektedir.

Bilgi çağı olarak kabul edilen çağımızda ülkelerin gelişmişliklerinin ve zenginliklerinin en önemli göstergesi, sahip oldukları bilgi miktarı ve bilgili insan kaynağıdır. Ülkelerin teknolojileri geliştikçe sahip oldukları bilgi artmakta; sahip oldukları bilgi arttıkça da teknolojileri gelişmektedir. Bilgi güvenliği adına teknolojinin gelişmesi hem fırsat hem de tehdit oluşturmaktadır.

Devletlere ait teknik, askeri ve ekonomik bilgiler; şirketlere ait borç ve alacak bilgileri, üniversitelere ait AR-GE çalışmalarına ilişkin bilgiler, bireylere ait kişisel bilgiler ve üst düzey yöneticilere ait sağlık verileri gizlidir ve gizlilikleri ihlal edilmeden gerekli koruyucu tedbirleri almak önem arz etmektedir.

Günümüzde neredeyse tüm devletler başta ekonomik ve askeri alan olmak üzere, birçok alanda rekabet edebilmenin tek yolunun bilişim sistemlerini etkin bir şekilde kullanabilmek ve bu sistemleri milli imkânlarla üretebilmek olduğunu düşünmektedirler. Bu amaçla Türkiye de dâhil birçok devlet Ulusal Siber Güvenlik Stratejilerini bu yönde hazırlayarak, bilişim sektörünü destekleyici çeşitli yatırım programlarını devreye almışlardır.

Amaç

Bu tez çalışması kapsamında yapılan araştırmalar, çalışmalar ve değerlendirmeler sonucunda;

- Siber ortamda bilgi güvenliğinin önemine dikkat çekilmesi,
- Gün geçtikçe bireyler, kurumlar ve devletler için daha tehlikeli hale gelen siber saldırı türleri ile uluslararası alanda gerçekleştirilen büyük siber saldırı olayları ve sonuçlarının ele alınması,
- Türkiye'de bilgi güvenliği ve siber güvenlik alanında yapılan çalışmaların eksik yönlerinin tespit edilmesi,
- AB, BM ve NATO gibi uluslararası kuruluşlar ile bazı dünya ülkelerinin siber güvenlik faaliyetlerinin incelenerek, ülkemizin siber uzayda tehditlerle etkin bir şekilde mücadele edilebilmesine yönelik birtakım çözüm önerilerinin sunulması,

- Köle bilgisayar sayısının çok fazla olduğu ülkemizde, siber uzayda bilgi güvenliğinin sağlanması için bireylerde ve kurumlarda farkındalığın arttırılmasına yönelik çözüm önerilerinin sunulması amaçlanmaktadır.

Önem

Bilginin ve BİT sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaya yönelik faaliyetlerin önem kazandığı günümüzde siber ortamda bilgi güvenliği kavramı yalnızca devletler için değil; kurumlar ve bireyler için de önemli bir mesele haline gelmiştir. Bu nedenle siber uzayda bilgi güvenliği alanında güncel çalışmaların ele alındığı bu tez çalışması; ülkemiz, kurumumuz ve bireyler açısından siber güvenlik farkındalığı oluşturacağı için önem arz etmektedir.

Yöntem

Tez çalışmasının hazırlanma sürecinde kaynak tarama yönteminden faydalanılmıştır. Bu yöntem kapsamında belirlenen çalışma konusu ile ilgili güncel ve geçmiş çalışmalar araştırılarak, araştırmanın tarihsel bir perspektife oturtulması amaçlanmıştır.

Kapsam, Sınırlılıklar ve Varsayımlar

Bu çalışmada günümüzde bilgi güvenliğine yönelik birçok uygulama ve standart bulunmasına rağmen, yalnızca siber uzaydaki bilgi güvenliği faaliyetleri ele alınmıştır.

Uluslararası alanda devletleri, şirketleri ve insanları büyük maddi zararlara uğratarak en çok ses getiren (Stuxnet, Estonya Siber Saldırıları, Sony Pictures şirketine yönelik siber saldırılar ve WannaCry fidye yazılımı vb.) siber saldırılar ele alınmıştır.

Siber güvenlik alanında yapılan çalışmalardan somut sonuçların alındığı özellikle 2000'li yıllardan itibaren yapılan çalışmalar ele alınmıştır. Birçok ülkenin

siber uzayda bilgi güvenliği faaliyetleri bulunmasına rağmen, bu tezde siber güvenlik faaliyetleriyle ön plana çıkan ABD, İsrail, İran, İngiltere, Çin ve Rusya gibi ülkeler seçilmiştir. Ayrıca ülkelerin yanı sıra siber güvenlik çalışmalarıyla uluslararası alanda kabul görmüş NATO, BM ve AB gibi çok uluslu örgütlerin faaliyetleri de ele alınmıştır.

Tez çalışmasında ele alınan konularla alakalı mümkün olan en güncel kaynaklar seçilmiş, seçilen tüm kaynakların doğruluğu ve bilimsel etik kurallara uygunluğu varsayılmıştır.

Verilerin Toplanması ve Analizi

Ön tarama aşamasında konu ile ilgili daha önce yapılan çalışmalar incelenerek tezin bölümleri ve konu başlıkları belirlenmiştir. Ardından detaylı tarama aşamasına geçilerek;

- Türkiye'de konu ile ilgili çalışmalarıyla ön plana çıkan Kalkınma Bakanlığı, BTK, TÜBİTAK gibi kurum ve kuruluşların çalışmaları,
- Uluslararası alanda dikkat çekici çalışmalar ortaya koyan AB, BM ve NATO gibi çok uluslu kuruluşların ve bazı devletlerin çalışmaları,
- Konu ile ilgili faaliyetlerde bulunan bazı özel şirketlerin çalışmaları,
- Konu hakkında yayımlanan ulusal ve uluslararası raporlar, makaleler ve istatistiki bilgiler incelenmiştir.

Maddeler halinde belirtilen tüm kaynakların yanı sıra akademik tez çalışmaları, araştırmalar, web siteleri, kitaplar, konferanslar gibi çeşitli kaynaklardan güncel ve önemli veriler elde edilmiştir. Tezin yazım sürecinde elde edilen tüm veriler bilimsel ve etik kurallara uygun olarak aktarılmıştır.

Bu kapsamda, dört bölümden oluşan "Bilgi Güvenliği Uygulamaları ve Çözüm Önerileri" isimli bu tez çalışmasının birinci bölümünde bilgi güvenliği tanımlanarak bilgi güvenliği unsurları, bilgi güvenliğinin tarihsel geçmişi ve en yaygın kullanılan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ayrıntılı olarak ele alınmıştır. Ayrıca uluslararası alanda kabul görmüş COBIT, ITIL, PCI DSS ve HIPAA bilgi güvenliği yönetim sistemleri hakkında da detaylı bilgi verilmiştir.

Tezin ikinci bölümünde günümüzde bilgi güvenliği ihlallerinin en fazla gerçekleştiği mecra olan siber ortama ilişkin temel kavramlar, siber ortamda gerçekleşebilecek olan siber saldırı türleri ve bu saldırılara karşı alınabilecek önlemlerden bahsedilmiştir.

Üçüncü bölümde uluslararası alanda bilgi güvenliği ve siber güvenlik alanındaki çalışmalarıyla dikkat çeken NATO, AB ve BM gibi uluslararası kuruluşlar ile bazı ülkelerin faaliyetleri hakkında bilgi verilmiştir. Ayrıca devletleri büyük savaşların eşiğine getiren, ekonomik olarak ciddi zararlara yol açan uluslararası alanda gerçekleşen büyük siber saldırılar ve bilgi güvenliği ihlallerinden örnek olaylar seçilerek, bu olaylar hakkında ayrıntılı bilgiler verilmiştir.

Tezin dördüncü bölümünde Türkiye'nin bilgi toplumuna dönüşüm süreciyle ilgili olarak somut adımların atıldığı 1990'lı yılların başından itibaren yapılan çalışmalar ve bu çalışmaların sonuçları ele alınmıştır. Yine aynı bölümde Türkiye'nin Ulusal Siber Güvenlik Stratejisi ile Türkiye'de bu alanda kurulan kurum ve kuruluşlardan bahsedilmiştir. Ayrıca Türkiye'nin bilgi güvenliği ve siber güvenlik alanlarında yasal altyapısı hakkında ayrıntılı bilgiler verilmiştir.

Sonuç ve değerlendirme bölümünde, ülkemizin siber güvenlik altyapısını güçlendirmek ve toplumda siber güvenlik farkındalığını oluşturmaya yönelik birtakım öneri ve değerlendirmelerde bulunulmuştur.

BİRİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ İLE İLGİLİ KAVRAMLAR

1.1. BİLGİ KAVRAMI

Bilgi, insanlığın başlangıcından itibaren yaşamın her alanında ihtiyaç duyulan en önemli unsur olmuştur. İnsanların hayatta kalabilmeleri, gelişimleri, düşünce ve davranışlarının şekillenmesi gibi süreçlerde önemli bir unsur olan bilginin yüzyıllardan beri pek çok bilim insanı tarafından tanımlaması yapılmış olsa da henüz ortak bir tanım üzerinde mutabık kalınamamıştır.

Bilgi, birçok konuda olduğu gibi ilk başlarda felsefe biliminin ilgi alanında yer almıştır. Zamanla birçok yeni bilim dalının ortaya çıkmasıyla tüm alanların konusu haline gelmiştir. Her alan kendi beklentilerini veya özelliklerini karşılayacak şekilde bilgiye farklı tanımlamalar yapmıştır. Tanımların alanlara göre birbirinden farklılık göstermesi, yapılan tanımın yanlış olduğunu değil; bilginin anlam genişliğini ve tanımlanan alanda bilgiye bakışın farklı olduğunu göstermektedir.[1]

Türk Dil Kurumu (TDK) sözlüğünde bilgi:

İsim bağlamında "*İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat*", genel anlamda "*Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf*" ve "*İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf*", felsefi bağlamda "*Genel olarak ve ilk sezi durumunda zihnin*

[1] Özenç Uçak, Nazan (2010), "*Bilgi: Çok Yüzlü Bir Kavram*", Türk Kütüphaneciliği, Sayı: 24, No: 4, s. 705-706.

kavradığı temel düşünceler", bilişim bağlamında "*Kurallardan yararlanarak kişinin veriye yönelttiği anlam*" şeklinde tanımlanmaktadır.[2]

TDK tanımlarından yola çıkarak tanımlanacak olursa; öğrenme, araştırma, tecrübe veya gözlem yoluyla elde edilen gerçek veya ilkelerin bütününe bilgi denir.



Şekil 1.1 Bilgi Piramidi

Bilgi çağında ilerlemek, bir piramidin en altından en üstüne doğru tırmanmaya benzetilebilir. Şekil 1.1'de yer alan bilgi piramidinin en alt basamağından en üst basamağına doğru ilerledikçe sırasıyla; veri, bilgi, öz bilgi ve hikmet yer almaktadır. Aşağıdan yukarı doğru çıkıldıkça sahip olunan şeyin değeri artarken, miktarı azalmaktadır. Bilgi piramidinde bir üst basamağa çıkmak daha zordur ve daha fazla emek istemektedir.[3]

[2] http://www.tdk.gov.tr (29.03.2018)
[3] Canbek, Gürol ve Sağıroğlu, Şeref (2006) "*Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme*", Gazi Üniversitesi Politeknik Dergisi, Cilt: 9 Sayı: 3 s. 165- 166.

Veri: Birbiriyle ilişkisi kurulmamış bilinenlere veri denir. Veri, hamdır ve işlenmesi gerekmektedir; ilişkili olduğu konu ya da olay ile bağdaştırılmadan tek başına bir anlam ifade etmemektedir. Bilgi ve iletişim teknolojileri (BİT) bağlamında veri; sayısal ortamlarda bulunan, taşınan sinyaller ve/veya bit[4] dizeleri olarak ifade edilmektedir.[5]

Bilgi: Verilerin belli bir anlam ifade edecek şekilde işlenmiş haline bilgi denir. Sayısal ortamda veri üzerinde yapılan mantığa dayalı dönüşümler, formüller, ilişkiler, varsayımlar, basitleştirmeler gibi işlemlerin sonucunda bilgi ortaya çıkmaktadır. Sayısal ortamlarda bilgi, 0 ve 1'lerden oluşan bit dizelerinin çıktılarıdır. Bu yüzden 0 ve 1'lerden oluşan çeşitli algoritmalar[6] yazılarak ve bunlar arasında çeşitli ilişkiler kurularak bilgi elde edilmektedir.

Öz Bilgi: Öğrenme, tecrübe edinme ya da iç gözlemler sonucunda elde edilen bilginin, gerçeklerin veya doğruların anlaşılması ve farkında olunmasına öz bilgi denir.[7] Öz bilgi bir şeyin ne (know-what), nasıl (know-how), neden (know-why) ve kim (know-who) olduğunu bilmek üzere toplam dört sınıftan oluşmaktadır.[8]

Hikmet (Bilgelik): Varlık, bilgi ve değerler üzerine tam ve bütün bir bilginin ortaya çıkması ya da insanın böyle bir bilgiye sahip olabilecek ölçüde olgunluğa erişmesi halidir.[9] Hikmet, kişinin bir alanda elde ettiği tecrübe ve bilginin uzun yıllarca yoğrulması sonucu oluşan bir olgudur.

---

[4] **Bit:** Bir bilgisayarın veri boyutunda işleyebileceği en küçük ve temel birimdir. Bilgisayar içinde karakterler ikilik sayı sisteminde 8 haneli bir sayıyla ifade edilir. Bu sayının her bir basamağına 1 Bit denir.

[5] *Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme*, a.g.m. s. 166.

[6] **Algoritma:** Belli bir problemi çözmek veya belirli bir amaca ulaşmak için tasarlanan yol. Matematikte ve bilgisayar biliminde bir işi yapmak için tanımlanan, bir başlangıç durumundan başladığında, açıkça belirlenmiş bir son durumunda sonlanan, sonlu işlemler kümesidir.

[7] *Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme,* a.g.m. s. 166.

[8] Güngör Murat, *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, Kalkınma Bakanlığı Uzmanlık Tezi, 2015, s. 6.

[9] Sarı, Emre (2016), "Geçmişten Günümüze Felsefe*",* Nokta E-Book Publishing Kitap Yayınları, s. 23.

Bilgi piramidinde yer alan en alt basamaktan en üst basamağa kadar bilginin tüm seviyeleri değerlidir. Çünkü her bir basamak zamanla ve edinilen tecrübeler sonucunda olgunlaşmaktadır. Ayrıca bir alt basamak, bir üst basamağın temelini oluşturmaktadır. Bu yüzden bilgi güvenliğinin sağlanması adına her tecrübeden ve bilgiden faydalanmak, beklenmedik tehlikelere karşı reaksiyon geliştirebilmek için önem arz etmektedir.

1.2. BİLGİ GÜVENLİĞİ

Bilgi ve iletişim teknolojileri sağlık, eğitim, bankacılık, finans, ulaştırma, enerji, e-ticaret, e-devlet hizmetleri ve daha birçok sektörde yaygınlaşarak günlük hayatımızda daha fazla yer edinmeye başlamıştır. Her alanda artan bilgi kaynaklarının korunması; kişiler, kurumlar ve devletler için önemli bir problem haline gelmiştir.

Bilgi ve bilgi sistemlerinin izinsiz erişim, izinsiz kullanım, ifşa edilme, tahrip edilme, yok edilme gibi tehditlerden korunmasına yönelik; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak adına yapılan tüm işlemlere bilgi güvenliği denir.[10]

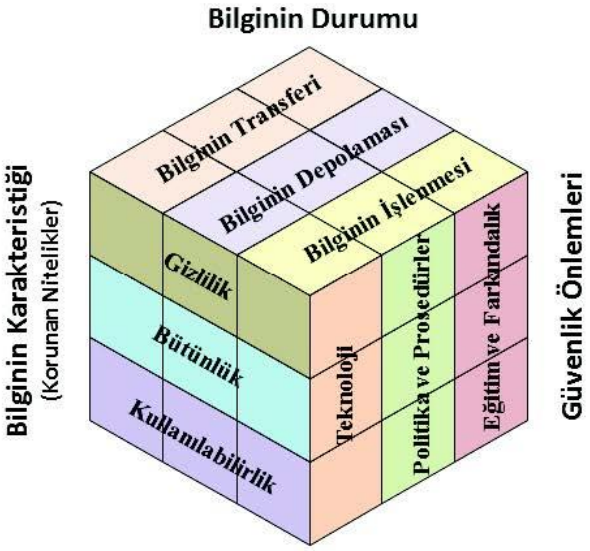
Başka bir ifadeyle; fiziksel, elektronik veya diğer ortamlarda bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğünün bozulmaması ve izinsiz erişimlerden korunması için güvenli bir bilgi işleme platformu oluşturma çabalarının tümüne bilgi güvenliği denir.[11]

[10] Henkoğlu, Tülay (2015), "*Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi*", Hacettepe Üniversitesi Doktora Tezi, s. 26.
[11] http://www.cagataycebi.com/security/bilgi_guvenligi.pdf (03.04.2018)

1.3. BİLGİ GÜVENLİĞİNİN UNSURLARI

Bilgi güvenliğini sağlamak amacıyla yapılan çalışmaların başarıya ulaşabilmesi için sadece bilgi güvenliği politikalarının oluşturulması yeterli değildir. Ortaya konan bilgi güvenliği politikalarının uygulama sürecinde, politikaların tüm yönleriyle değerlendirilmiş olması gerekmektedir.

Uluslararası alanda devletler tarafından ilk başta askeri alanda olmak üzere, zamanla birçok kritik altyapı sektöründe bilgi güvenliğini sağlamak amacıyla çeşitli politikalar geliştirilmiştir. Gelişen teknoloji ve artan tehditlere göre kimi politikalar yürürlükten kalkmış, kimileri ise uzun yıllar öncesinden günümüze kadar gelebilmişlerdir.[12]



Şekil 1.2 McCumber Bilgi Güvenliği Modeli[13]

Şekil 1.2'de yer alan ve 1991 yılında McCumber tarafından geliştirilen bilgi güvenliği modeli uluslararası alanda kabul görmüş en yaygın modeldir. Model, bilgi güvenliğinin tüm yönleriyle uygulanabileceği en uygun modeldir. McCumber

[12] Henkoğlu, Türkay ve Yılmaz, Bülent (2013), "*Avrupa Birliği (AB) Bilgi Güvenliği Politikaları-European Union (EU) Information Security Policies*", Türk Kütüphaneciliği Hakemli Yazılar, s. 453.
[13] a.g.m. s. 454.

oluşturduğu modelde bilginin boyutlarını bilginin durumu, bilginin karakteristiği ve alınabilecek güvenlik önlemleri olmak üzere üç farklı gruba ayırmıştır. Böylece bilgi güvenliği uygulamalarında en çok üzerinde durulan gizlilik, bütünlük ve erişilebilirlik unsurlarının yanı sıra süreci yöneten insan faktörü ve uygulanan bilgi güvenliği politikalarının da önemine değinilmiştir.[14]

Üzerinden yıllar geçmiş olmasına rağmen hala önemini koruyan model uluslararası alanda birçok devlet, şirket, kurum ve kuruluşun bilgi güvenliği politikalarının omurgasını oluşturmaktadır. Bunlardan en önemlileri; NIST (Ulusal Standartlar ve Teknoloji Enstitüsü), ENISA (Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı), NATO (Kuzey Atlantik Antlaşması Örgütü) ve BM (Birleşmiş Milletler) gibi kuruluşlardır.



Şekil 1.3 Solomon CIA Üçgeni

Solomon da Şekil 1.3'de yer alan "CIA (Confidentiality-Integrity-Availability) Triad" adını verdiği üçgende bilgi güvenliğinin; gizlilik, bütünlük ve erişilebilirlik

[14] a.g.m. s. 454.

faktörlerinden meydana geldiğini belirtmektedir. Solomon, güvenlik sektöründe konunun uzmanları tarafından bilgi güvenliği çalışmalarında en fazla önemsenen ve birbirinden bağımsız olarak düşünülemeyen bu unsurların iyi tasarlanmış bir sistemin köşe taşlarını oluşturduğunu ifade etmektedir.[15]

1.3.1. Gizlilik

Genel anlamda gizlilik, bilgi veya kaynakların gizlenmesidir. Bilgi güvenliğinde ise; bilgi teknolojileri ve haberleşme sistemleri üzerinden gerçekleşen veri trafiğinin veya bu sistemler üzerinde depolanan verilerin yetkisiz erişimlere karşı korunmasıdır.

Bilginin korunma ihtiyacı devlet kurumları, savunma ve sanayi gibi kritik öneme sahip alanlarda bilgi ve iletişim teknolojilerinin yaygın olarak kullanılmaya başlamasıyla ortaya çıkmıştır. Bilgi güvenliği ve gizlilikle ilgili ilk somut çalışmalar "*bilmesi gereken (need to know)*" ilkesiyle askeri alanda yapılmıştır. Bu ilke bir organizasyon içinde yer alan personelin sadece görev ve sorumluluk sınırları içerisindeki bilgiye erişebilmesini, görev ve sorumluluğu dışındaki bilgilere erişememesini ifade etmektedir. Daha sonraları devlet kurumları ve özel sektör kuruluşları tarafından da benimsenmiş olan bu ilke güvenlik politikalarının en önemli halkasını oluşturmaktadır.

Günümüzde devletlerin, kurumların ve hatta bireylerin en büyük problemi sahip olunan gizli bilgilerin yetkisiz erişimler sonucunda ifşa olmasıdır. Bu bağlamda bilginin gizliliğini sağlamak adına günümüzde başvurulan en yaygın ve etkili yöntem, kriptografidir. Kriptografi, bilgilerin depolanması ve iletilmesi sırasında şifrelenerek yetkisiz kişilerin erişiminden korunmasını sağlayan kodlama sistemidir.[16] Kriptografi

[15] Solomon, Michael G. ve Cahapple, Mike (2005), "*Introducing Computer and Network Security*", Jones and Barlett Publishers, Chapter 1, s. 2-3.
[16] Bishop, Matt (2005), "*Introduction to Computer Security"*, Pearson Education, Inc., Boston., s. 2. http://iips.icci.edu.iq/images/exam/Introduction-to-Computer-Security-pdf-DONE.pdf - (03.04.2018)

yöntemiyle şifrelenen sistemlere ya da verilere yetkisiz erişimlerin önüne büyük oranda geçilebilmektedir.

1.3.2. Bütünlük

Bilgi işlem sistemlerinde bilginin içeriği bozulmadan veya değiştirilmeden iletilebilmesi ve saklanabilmesine bilgi bütünlüğü denmektedir. Bir diğer ifadeyle bilginin yetkisiz erişimle içeriğinin değiştirilmesinin, kopyalanmasının veya tahrip edilmesinin engellenmesi denmektedir.

Bütünlük mekanizmaları; önleme mekanizmaları ve algılama mekanizmaları olarak ikiye ayrılmaktadır. Önleme mekanizmaları yetkisiz veri değiştirme teşebbüslerini önceden algılayıp engel olarak bilgi bütünlüğünü korurken; algılama mekanizmaları ise veriye yetkisiz şekilde ulaşılmasını veya yetkisiz şekilde içeriğinin değiştirilmesini tespit etmektedir. Algılama mekanizmaları bütünlüğün ihlaline mâni olmaz; yalnızca verilerin bütünlüğünün bozulduğunu ve verilerin artık güvenli olmadığını bildirmektedir.[17]

Bütünlük ve gizlilik birbirinden çok farklıdır. Gizlilik, bilginin ifşa edilip edilmediği ile alakalıyken; bütünlük, bilginin doğruluğu ve güvenilirliği ile alakalıdır. Verilerin kaynağı (nasıl veya kimden elde edildiği), alıcıya gelmeden önce güvenilir olup olmadığı ve alıcıya iletildikten sonra güvenilirliğinin sağlanıp sağlanmadığı bilgi bütünlüğünü etkilemektedir.

Kötü niyetli yazılımların veya kullanıcıların yanı sıra, sistemsel bozukluklar da bilgi bütünlüğü için tehdit oluşturabilmektedir. Bunun için yetkilendirme yöntemleri (kullanıcı adı, şifre, parmak izi vb.) ve kimlik doğrulama mekanizmaları iyi belirlenerek, her kullanıcıya ihtiyacı kadar yetki verilmelidir. Kurumlar bilgi güvenliği

[17] "*Introduction to Computer Security",* a.g.k. s. 3.

bütçelerinin önemli bir kısmını bilgi bütünlüğünü korumaya ayırmaktadırlar.[18] Çünkü bütünlüğü bozulan bilginin mahremiyeti ve güvenliği kalmamıştır.

1.3.3. Erişilebilirlik

Bilgi işlem sistemlerinde kullanıcının ihtiyaç duyduğu içeriğe/bilgiye istediği anda ve kendisine tanımlanan yetkiler/izinler dâhilinde ulaşabilmesine ve bu verileri kullanabilmesine erişilebilirlik denir. Bilgi işlem sistemlerinin devamlılığının sağlanması anlamında erişilebilir olmaları kritik öneme sahiptir. Bilişim sistemlerinden kendilerinden beklenen iş ve işlemleri tam, eksiksiz ve zamanında yapmaları beklenmektedir. Erişilebilirlik, sistemleri içeriden ve dışarıdan gelebilecek tehditlere karşı korumayı amaçlamaktadır. Böylelikle kullanıcılar erişim yetkileri dâhilinde olan verilere güvenli bir şekilde ulaşabileceklerdir.

Bir sistemin aktif olarak çalışabilmesinin yanında istendiği anda erişilebilir olması, sistem yöneticilerine farklı sorumluluklar yüklemektedir. Özellikle veri depolama sistemlerinin kullanıcının ihtiyaç duyduğu veriye istediği anda erişim olanağı verebilmesi bakımından veri yedekleme işleminin düzenli olarak yapılması gerekmektedir.[19]

Sistemlerde gizliliğin çok fazla ön planda tutulması, verilerin erişilebilirliğine engel olabilmektedir. Bu durum erişilemeyen bilginin kullanılamaz olduğunu göstermekte; böylelikle kullanılamayan bilgi de bir anlam ifade etmemektedir. Erişilebilirliğin ön planda tutulduğu sistemlerde ise gizlilik ve bütünlük problemleriyle karşılaşılabilmektedir. Tüm sistemlerde bu üç temel güvenlik unsurunun birlikte ve dengeli bir şekilde sağlanması önem arz etmektedir.

[18] "*Introduction to Computer Security",* a.g.k. s. 3.
[19] "*Avrupa Birliği (AB) Bilgi Güvenliği Politikaları-European Union (EU) Information Security Policies*" a.g.m. s. 455.

1.3.4. Diğer Unsurlar

Zamanla McCumber ve Solomon tarafından ortaya koyulan temel unsurlara ek olarak yeni bilgi güvenliği unsurları türetilmiştir. Bunlar, bir nevi temel unsurların detaylandırılması sonucunda ortaya çıkmıştır. Bu unsurlardan bazıları Şekil 1.4'de yer alan güvenilirlik, inkâr edememe, kimlik sınaması, yetkilendirme ve izlenebilirliktir.[20]



Şekil 1.4 Bilgi Güvenliğinin Diğer Unsurları

Güvenilirlik: Bir sistemden beklenen davranış ile çalışması sonucu elde edilen sonuçların tutarlı olmasıdır. Yani sistemin beklendiği gibi çalışmasıdır. Sistemin güvenilirliği tutarlılık olarak da ifade edilebilir.

İnkâr Edememe: Veri haberleşmesinin gerçekleştiği iki sistemde, gönderici ve alıcı arasında iletim sürecinde meydana gelebilecek sorunları ortadan kaldırmayı ya da minimuma indirmeyi amaçlayan bilgi güvenliği unsurudur. Özellikle gerçek zamanlı

[20] https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/ (03.04.2018)

haberleşmenin önem arz ettiği finans, sağlık ve askeri alanlardaki haberleşme sistemleri için vazgeçilmez bir unsurdur.

Kimlik Sınaması: Kullanıcının bir sisteme giriş yapabilmesi veya ulaşabilmesi esnasında kimliğinin doğrulanmasıdır. Günümüzde neredeyse tüm sistemlerde kullanıcılar; kullanıcı adı ve parola doğrulamasına tabi tutulmaktadırlar. Böylelikle yetkisiz kişiler veya cihazlar sistem dışında tutularak güvenlik sağlanmaya çalışılmaktadır.

Yetkilendirme: Güvenlik sınamalarından (kullanıcı adı, şifre vb.) geçerek sisteme erişebilen kullanıcının yetkileri dâhilinde içeriğe erişebilmesinin kontrol altında tutulmasıdır. Örneğin; tüm iş ve işlemlerin tek bir sistem üzerinden yapıldığı banka şubesinde gişe görevlisi memur ile banka müdürünün yetkileri farklıdır. Banka müdürüne daha fazla yetkinin/iznin tanımlandığı sistemde gişe görevlisi memurun yetkileri daha kısıtlıdır.

İzlenebilirlik: BİT altyapılarının kullanıldığı organizasyonlarda bir problemle karşılaşıldığında geçmişe dönük kayıtların incelenmesi problemlerin tespiti ve çözümlenebilmesi konusunda oldukça önem arz etmektedir. Sistemde yer alan tüm kullanıcıların yaptığı iş ve işlemler (e-posta kayıtları, iş yeri giriş-çıkış zamanları, telefon görüşme kayıtları vb.) güvenlik nedeniyle kayıt altına tutularak, bir problemle karşılaşılması durumunda problemin tespiti veya çözümlenebilmesi için incelenmektedir.[21]

1.4. BİLGİ GÜVENLİĞİNİN TARİHSEL GEÇMİŞİ

İnsanlar yaşamları boyunca elde ettikleri bilgileri güvende tutabilme çabası içerisinde olmuşlardır. Yazının icadına kadar edinilen bilgiler sonraki nesillere çok

[21] Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June s. 306-308.

sağlıklı bir şekilde aktarılamamıştır. Yazının icadı, bilginin sonraki nesillere aktarılabilmesi bakımından bir dönüm noktası olmuştur. Çünkü yazının icadı; bilgilerin kaydedilmesine ve fiziksel olarak muhafaza edilmesine imkân tanımaya başlamıştır. Yazı, ne kadar bilgilerin kaydedilebilmesine katkıda bulunmuş olsa da zaman içerisinde bilginin izinsiz ele geçirilebilmesi ve içeriğinin değiştirilebilmesi gibi güvenlik sorunlarını da beraberinde getirmiştir. İnsanlar da bilgi güvenliğini sağlama noktasında zamanın şartlarına göre çeşitli güvenlik önlemleri almışlardır.

Günümüze yaklaştıkça, özellikle II. Dünya Savaşı'ndan sonraki yıllarda bilim ve teknolojide hızlı bir ilerleme olmuştur. Bu gelişmelerden en önemlisi de 1946 yılında Amerikan ordusunun top atışları hesaplamalarına yardımcı olmak için geliştirilen Türkçe anlamı "*elektronik sayısal entegreli hesaplayıcı*" olan ilk dijital bilgisayar ENIAC (Electronic Numerical Integrator And Computer) olmuştur.[22]

1962 yılında çok sayıda bilgisayar kullanıcısının birbirleriyle haberleşmesini öngören ağ çalışmaları sonucunda; Birleşik Devletler Savunma Bakanlığına bağlı Gelişmiş Araştırma Projeleri Dairesi (Advanced Research Projects Agency - ARPA) tarafından geliştirilen ve dünyanın ilk paket dağıtım ağı "Gelişmiş Araştırma Projeleri Dairesi Ağı (Advanced Research Projects Agency Network – ARPANET)" ortaya çıkmıştır. ARPANET günümüzde kullanmakta olduğumuz internetin temelini oluşturmaktadır.

ARPANET üzerinden ilk e-posta 1971 yılında gönderilmiştir. 1973 yılına gelindiğinde sadece e-postalar ARPANET trafiğinin %75'ini oluşturmuştur. Sisteme 1973 yılında ARPANET üzerinden dosya aktarımına izin veren FTP (File Transfer Protocol) protokolü tanımlanmış ve bu yıldan itibaren bilgisayar ağları arasında dosya aktarımı da gerçekleştirilmeye başlanmıştır.[23] ARPANET'in yaygın olarak kullanılmaya başlaması veri haberleşmesini daha hızlı hale getirirken, elektronik

[22] https://tr.wikipedia.org/wiki/ENIAC (13.09.2017)
[23] https://tr.wikipedia.org/wiki/ARPANET (13.09.2017)

ortamda transfer edilen bilginin bütünlüğüne yönelik endişeleri de beraberinde getirmiştir.

1970'li yıllardan itibaren teknolojideki hızlı ilerlemeye bağlı olarak bilgi güvenliğinin kapsamına bilgisayar sistemleri de dâhil olmuştur. Bu yıllarda bilgi güvenliği konusunda askeri amaçlı verilerin gizliliğini ve kontrolünü sağlamak üzere ilk çalışmalar yapılmaya başlanmıştır. Yine bu dönemde askeri bilgiler gizlilik derecelerine göre sınıflandırılmış ve bu sınıflandırma derecelerine göre bilgilerin korunmasına yönelik güvenlik stratejileri geliştirilmiştir. Ardından 1980'li yıllara gelindiğinde ticari alanda bilginin bütünlüğünün sağlanmasına yönelik endişelerin artması sonucunda, bilgi güvenliğinin ticari boyutu da önem kazanmaya başlamıştır.[24]

1990'lı yıllara kadar bilgiler kâğıtlara yazılarak arşivlerde saklanıyorken; 1990'lı yılardan itibaren internet ve bilgisayar sistemlerinin yaygın olarak kullanılmaya başlamasıyla birlikte elektronik ortamlarda depolanmaya başlamıştır. Günden güne gelişen teknoloji ve internet ağı; dev arşivlerde saklanan devasa miktarda bilginin çok küçük ortamlarda saklanabilmesine ve kullanıcıların söz konusu bilgilere kısa sürede ulaşabilmelerine imkân sağlamaya başlamıştır.[25]

Yine 1990'lı yıllarda bilişim sitemleri ve bilgisayar ağlarının yaygınlaşmasına bağlı olarak artan tehditler sonucunda bilgi güvenliğini sağlama konusunda farklı bilgi güvenliği modelleri ortaya koyulmuştur. Bu modellerden en önemlisi ve yaygın olanı "*Bilgi Güvenliği Unsurları*" başlığı altında önceki bölümde ayrıntılı bir şekilde ele alınan McCumber Bilgi Güvenliği Modeli'dir.

2000'li yıllara gelindiğinde devasa boyutlara ulaşan veri miktarı ve artan veri trafiği güvenlik sorunlarını daha da önemli hale getirmiştir. Bu döneme kadar yalnızca

[24] "*Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi*", a.g.t. s. 25-26.
[25] Çetinkaya, Mehtap (2008), "*Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması*", Akademik Bilişim 2008, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak-01 Şubat 2008, s. 510.

devletlerin ve kurumların güvenliğini ön planda tutan bir bilgi güvenliği politikası izlenmekte iken; dünya genelinde özellikle 2000'li yıllarda insanlar tarafından internet ve sosyal medya kullanımının yaygınlaşması sonucunda kişisel verilerin güvenliği de önem kazanmaya başlamıştır.

Günümüzde yaygın olarak kullanılmakta olan internet ve bilgisayar ağları bilişim suçlarının işlenmesi için en önemli altyapıyı sunmaktadır. Son yıllarda sanal ortamda kişisel verilerin gizliliği, bütünlüğü ve erişilebilirliğine yönelik yapılan saldırılarda ciddi artışlar yaşanmıştır. Bilgi toplumuna dönüşüm sürecinde birçok devlet kişisel verilere yönelik artan saldırılara karşın teknik ve hukuki altyapılarını oluşturarak çeşitli önlemler almışlardır.[26]

1.5. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Kurumların sahip oldukları hassas ve gizli bilgilerin güvenliğini sağlamak için gereken önlemlerin belli bir program dâhilinde alındığı; bilgi güvenliği uygulamalarının daha etkin ve belli bir sistematiğe uygun olarak yapılması, bilgi güvenliği sürecine insan faktörünün de dâhil olduğu sisteme bilgi güvenliği yönetim sistemi (BGYS) denir.[27]

Etkin bir bilgi güvenliğinin sağlanması için gerekli önlemler yerinde ve zamanında alınmalıdır. Bilgi güvenliği yönetim standartları ile bilgi güvenliği uygulamalarının sürekliliği, kaynakların verimli bir şekilde kullanılması ve güvenlik uygulamalarının geliştirilmesi hedeflenmektedir.[28]

---

[26] "*Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi",* a.g.t. s. 26.

[27] http://www.isokalitebelgesi.com/bilgi-nedir-bilgi-guvenligi-nedir-bilgi-guvenligi-yonetim-sistemi-nedir (05.04.2018)

[28] Boğa Uğur (2011) "*Bilişim Suçlarıyla Mücadele Yöntemleri"*, Radyo ve Televizyon Üst Kurulu Uzmanlık Tezi, Ankara, s. 65-66.

1995 yılında İngiliz Standartlar Enstitüsü (British Standards Institute - BSI) tarafından BİT sistemlerinde kullanılan yazılım ve donanımların güvenlik açıklarının izlenmesi, güvenlik yönetimi sürecine dâhil olan insan faktörünün kontrolü ve üst düzey bilgi güvenliği yönetiminin sağlanması amacıyla yapılan çalışmalar sonucunda BS-7799 standart ailesinin ilk kısmı BS7799-1 yayımlanmıştır. Standardın ikinci kısmı olan BS7799-2 ise 1999 yılında yayımlanmıştır.

2000 yılında Uluslararası Standardizasyon Teşkilatı (International Organization for Standardization - ISO) tarafından daha önce BSI'nın yayımlamış olduğu BS7799-1 standardı, üzerinde çeşitli düzenlemeler yapılarak ISO/IEC 17799 adıyla dünyaya ilan edilmiştir. Böylece ISO/IEC 17799 standardı uluslararası alanda kabul gören bir standart haline gelmiştir. ISO/IEC 17799, 2005 yılında üzerinde yapılan düzeltme çalışmaları sonucunda ISO/IEC 17799:2005 adıyla yeniden yayımlanmıştır. Ayrıca 2005 yılında BS7799-2 standardı üzerinde yapılan çeşitli ekleme ve düzeltme çalışmaları sonucunda ISO/IEC:27001 standardı yayımlanmıştır.[29]

Türkiye'de bilgi güvenliği standartları ile ilgili çalışmalar ve bilgi güvenliği belgelendirme faaliyetleri Türk Standartları Enstitüsü (TSE) tarafından yürütülmektedir. TSE, ISO tarafından yayımlanan standartları Türkçeleştirerek ve Türkiye'nin gereksinimleri doğrultusunda yeniden düzenleyerek yayımlamaktadır.

Günümüzde bilgi güvenliği yönetiminde uluslararası alanda kabul görmüş en yaygın standart, Uluslararası Standardizasyon Teşkilatı/Elektroteknik Komisyonu (ISO/IEC) tarafından hazırlanan ISO 27001 standardıdır. Bu bölümde ISO 27001 standardının yanı sıra BİT uygulamalarında yaygın olarak kullanılan,

- Bilgi ve İlgili Teknolojilerine İlişkin Kontrol Hedefleri (Control Objectives for Information and Related Technology - COBIT),

[29] Vural, Yılmaz ve Sağıroğlu, Şeref (2008), "*Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme*", Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi Cilt 23, No 2, s. 511.

- Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technologies Infrastructure Library - ITIL),

- Kartlı Ödeme Endüstrisi Veri Güvenliği Standardı (Payment Card Data Security Standard - PCI DSS),

- Sağlık alanında Amerikan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu (Health Insurance Portability and Accountability Act - HIPAA)

gibi bilgi güvenliği yönetim standartları ele alınmaktadır.

1.5.1. ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı

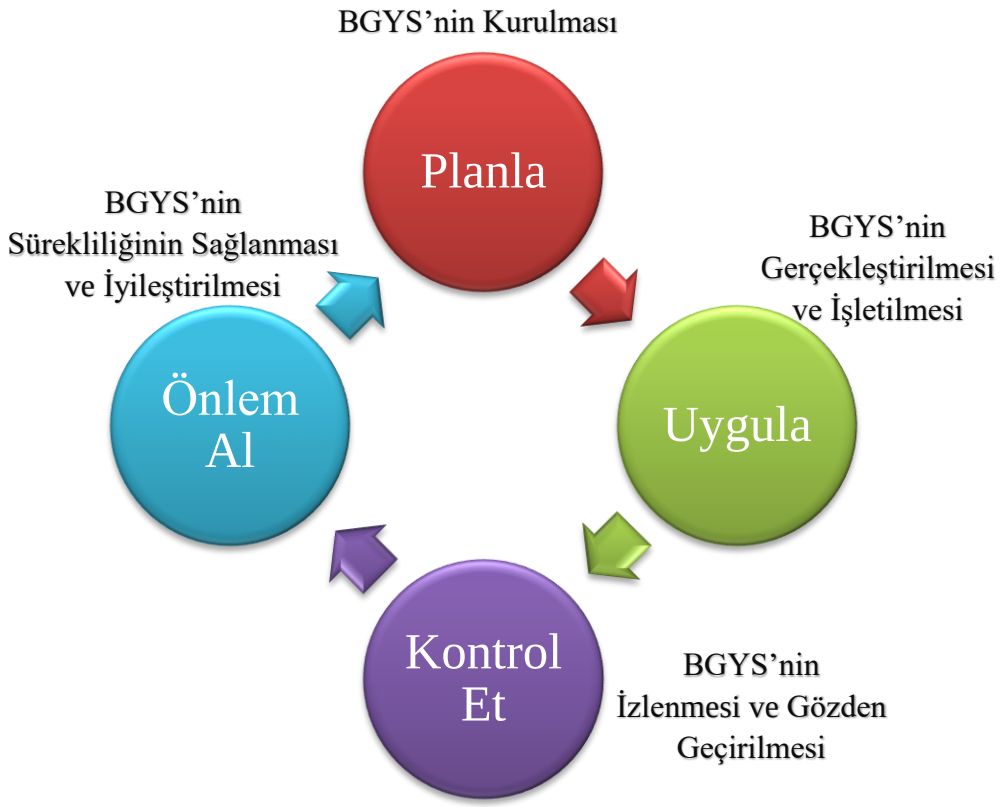
ISO/IEC 27001, ISO ve IEC tarafından hazırlanan Bilgi Güvenliği Yönetim Sistemi standardıdır. İlk sürümü 2005 yılının Ekim ayında yayımlanmıştır. En son sürümü 2013 yılı Eylül ayında yayımlandıktan sonra, ISO/IEC 27001:2005 yürürlükten kalkmıştır. ISO/IEC 27001:2013, bilgi güvenliği risklerinin yönetimi konusunda uluslararası alanda kabul görmüş en yaygın uygulamadır.[30]

ISO/IEC 27001 standardı, Bilgi Güvenliği Yönetim Sisteminin kurulum ve belgelendirilme süreçlerinin tamamını kapsayan bir standarttır. Bu standart BGYS'nin tüm iş riskleri bağlamında kurulması, izlenmesi, sürdürülebilirliğinin sağlanması ve iyileştirilmesi süreçleri için gereken tüm adımları kapsamaktadır.

TSE tarafından en son ISO/IEC 27001:2013'ün Türkçe sürümü olan TS ISO/IEC 27001:2013 standardı yayımlanmıştır. Standardın adı tam olarak "ISO/IEC 27001:2013 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler" olarak geçmektedir. [31]

[30] http://www.iso27001security.com/html/27001.html (06.04.2018)
[31] "*Bilişim Suçlarıyla Mücadele Yöntemleri"* a.g.t. s. 78.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Şekil 1.5'de yer alan PUKÖ (Planla – Uygula – Kontrol Et – Önlem Al) Modeli ile yürütülmektedir. PUKÖ döngüsünde ISO/IEC 27001'in kurulum, izleme, sürdürme ve iyileştirme süreçleri yer almaktadır.[32]



Şekil 1.5 BGYS Süreçlerinde Uygulanan PUKÖ Modeli

Planla: BGYS'nin politikası, amaçları, hedefleri, süreçleri ve prosedürlerinin geliştirildiği adımdır.

Uygula: Planlama sürecinde geliştirilen politika, amaç, süreç ve prosedürlerin uygulamaya geçirilerek işletildiği adımdır.

[32] Önel, Dinçer ve Dinçkan, Ali (2007), "*Bilgi Güvenliği Yönetim Sistemi Kurulumu*", TÜBİTAK UEKAE, s. 8-9.

Kontrol Et: BGYS sürecinde uygulamaya geçirilen adımlara ilişkin performans değerlendirilmeleri ve ölçümlerin yapıldığı; yapılan ölçüm ve değerlendirmelerden elde edilen sonuçların rapor edildiği adımdır.

Önlem Al: BGYS sürecinde performans değerlendirme ve ölçüm sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirildiği adımdır.

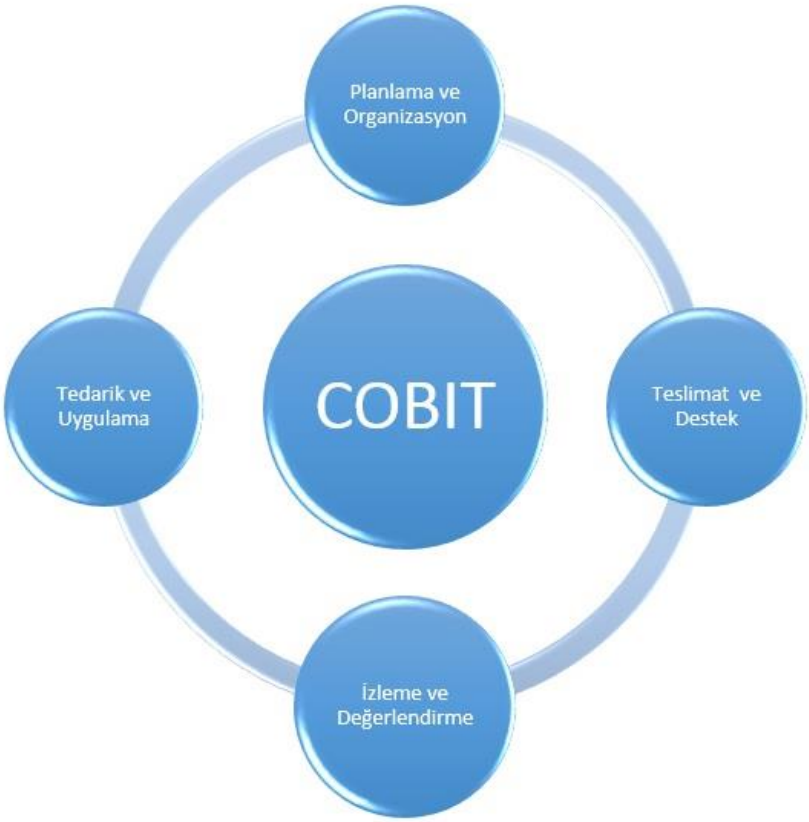
ISO/IEC 27001 bilgi güvenliği yönetim sistemi başlangıç ve bitiş zamanı olan bir proje gibi düşünülmemelidir. BGYS sürekli devam eden bir döngüdür.[33] BGYS sürecinin sağlıklı bir şekilde yürütülebilmesi için PUKÖ döngüsünde yer alan tüm adımlar birbiriyle uyum içinde olmalıdırlar.

1.5.2. COBIT

Bilgi ve İlgili Teknolojilerine İlişkin Kontrol Hedefleri *(The Control Objectives For Information and Related Technology - COBIT)*, en yaygın kullanılan BİT uygulamalarından birisidir. Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association - ISACA) ile Bilgi Teknolojileri Yönetim Enstitüsü (IT Governance Institute - ITGI) tarafından 1996 yılında yayımlanmıştır.[34]

Misyonu; "araştırma, geliştirme, ilan ve yetkili tanıtmak, güncellik, uluslararası alanda kabul görmüş genel bilgi teknolojileri kontrol hedeflerinin iş yöneticileri ve denetçiler tarafından kullanılmasıdır." COBIT BİT sistemlerinde meydana gelen problemlere çözüm sunmayıp; BİT sistemlerini anlamada ve sahip olunan verilerin korunması için gerekli güvenlik ve kontrol seviyelerini belirlemede rehberlik etmektedir. Bu yüzden yöneticiler, denetçiler ve kullanıcılar tarafından çokça tercih edilmektedir.

[33] "*Bilgi Güvenliği Yönetim Sistemi Kurulumu*" a.g.e. s. 9.
[34] "*Bilişim Suçlarıyla Mücadele Yöntemleri"* a.g.t. s. 66.



Şekil 1.6 COBIT Süreçleri

COBIT'te 34 üst düzey işlem mevcuttur. İşlemlerin de kapsadığı 210 tane kontrol hedefi vardır. Kontrol hedefleri kısaca dört ana kategoriye ayrılırlar. Bunlar Şekil 1.6'daki gibi Tedarik ve Uygulama, Planlama ve Organizasyon, Hizmet Sağlama ve Destek, İzleme ve Değerlendirmedir.[35]

- **Planlama ve Organizasyon:** Kuruluşun stratejik BİT planı ile bilgi mimarisinin tanımlandığı ve teknolojik yönünün belirlendiği basamaktır. Ayrıca bu süreçte insan kaynakları (İK) yönetimi, kalite yönetimi, proje yönetimi ve risk değerlendirmesi planları yapılmaktadır.

- **Tedarik ve Uygulama:** Kuruluşun BİT gereksinimlerinin belirlenerek ihtiyaç duyulan teknolojinin tedarik edilme süreçlerinin yanı sıra, BİT sistemi

[35] http://www.isaca.org/education/upcoming-events/documents/intro-cobit5.pdf (30.10.2017)

bileşenlerinin ömrünü uzatabilmek adına bir bakım planının oluşturulması süreçlerini kapsayan basamaktır.

- **Hizmet Sağlanması ve Destek:** Hizmet sürekliliğinin güvenli bir şekilde sağlanması, BİT sistemlerinin etkili ve yeterli düzeyde işletilmesini sağlayan destek süreçlerini (sistem güvenliği, kullanıcı eğitimi vb.) de içeren basamaktır.

- **İzleme ve Değerlendirme:** Daha önceden belirlenen stratejilere göre tasarlanan BİT sisteminin beklentilere ne ölçüde cevap verdiğinin ele alındığı basamaktır. Ayrıca BİT sisteminin iç ve dış denetçilerce denetiminin sağlanarak ilgili yasal mevzuat ve yönetmeliklere uyumluluğu bu basamakta sağlanmaktadır.[36]

1.5.3. ITIL

Bilgi Teknolojisi Altyapı Kütüphanesi (*Information Technology Infrastructure Library-ITIL*), BİT sistemlerini en iyi şekilde yönetebilmek amacıyla 1987 yılında İngiltere Ticaret Bakanlığı tarafından geliştirilmiş bir altyapıdır.

Müşteri, tedarikçi, BİT bölümü ve kullanıcılar arasında başarılı bir iletişim kurulmasını hedefleyen ITIL'ın 2007 yılında yayımlanan üçüncü sürümü ile birlikte bir adet giriş kitabıyla birlikte 5 temel kitabı yayımlanmıştır. Uluslararası alanda BİT servislerinin yönetimi konusunda kabul görmüş olan ITIL'ın uygulama alanı günden güne genişlemektedir. Özellikle ISO 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Standardı ile uygulama alanı genişleyen ITIL son yıllarda ülkemizde de yaygınlaşmaya başlamıştır.[37]

[36] https://tr.wikipedia.org/wiki/Cobit (30.10.2017)
[37] https://tr.wikipedia.org/wiki/Bilgi_Teknolojisi_Altyapı_Kütüphanesi (19.04.2018)

1.5.4. PCI DSS

Kartlı Ödeme Endüstrisi Veri Güvenliği Standardı (*Payment Card Industry Data Security Standard-PCI DSS*) kredi kartının üretilmesi, kullanıcıya iletilmesi ve muhafaza edilmesi aşamalarında kart sahibinin verilerini korumak için belirlenmiş olan teknik ve operasyonel gereklilikleri içeren bilgi güvenliği yönetim sistemi standardıdır.

Standardın şartları PCI Güvenlik Standartları Konseyi tarafından belirlenmektedir. Konseyin üyeleri arasında American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. gibi uluslararası bankacılık ve finans şirketleri bulunmaktadır. Kartlı ödeme sistemlerini kullanan ve müşterilerine bu alanda hizmet sunan tüm kuruluşların uyması gereken uluslararası bir standarttır.[38]

1.5.5. HIPAA

Amerikan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Kanunu (*Health Insurance Portability and Accountability Act-HIPAA*), 1996 yılında Amerikan Kongresi tarafından kabul edilen ulusal sağlık standartları ve sağlık verilerinin korunması konularını içeren bir kanundur. Dünya genelinde sağlık sektöründe referans bir güvenlik standardı olarak kullanılmaktadır. HIPAA standartları idari, fiziksel ve teknik tedbirler olmak üzere üç başlıkta sınıflandırılmaktadır.

İdari tedbirler bölümünde sağlık sistemlerinde konu ile ilgili idari sorumlular ve organizasyon içerisinde uyulması gereken prosedürler tanımlanmaktadır. Yine bu bölümde elektronik ortamlarda yer alan bilgiler seviyelendirilerek organizasyon içinde kimlerin hangi içeriklere erişebileceği tanımlanmaktadır. Ayrıca acil durumlar ve acil durumlarda yapılacaklar da bu bölümde yer almaktadır.

[38] https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf (31.10.2017)

Fiziksel tedbirler kısmında sağlık verilerinin yer aldığı ortamlara (otomasyon, veritabanı vb.) erişimlerin belli prosedürlere göre yapılması ve içeriklere erişimlerin kontrol edilmesi konuları yer almaktadır.

Teknik tedbirler kısmında BİT altyapılarını kullanarak sağlık verilerinin gizlilik, güvenlik ve bütünlüğünün korunması ile verilere yetkisiz erişimlerin engellenmesi konuları ele alınmaktadır.[39]

[39] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (04.11.2017)

İKİNCİ BÖLÜM

SİBER GÜVENLİK VE SİBER SALDIRI TÜRLERİ

BİT sistemleri ve internet altyapısının gelişmesiyle birlikte finans, ticaret, eğitim, basın, enerji, sağlık, ulaşım ve haberleşme gibi birçok kritik altyapı hizmeti siber ortama aktarılmıştır. Siber uzayda zamanla ortaya çıkan zararlı yazılımlar BİT sistemleri ve kritik altyapıların güvenliğini tehdit eder hale gelmiştir. Bunun sonucunda siber güvenlik kavramı gün geçtikçe bireyler, kurumlar ve devletler için önem arz etmeye başlamıştır. Bu bölümde siber güvenliğe ilişkin temel kavramlardan, kritik altyapılara ciddi zararlar veren siber saldırılardan ve doğrudan bireylere yönelik gerçekleştirilen siber saldırı türü olan siber zorbalıktan bahsedilmektedir.

2.1. SİBER KAVRAMI

Siber terimi sibernetik kelimesinin kökeninden gelmektedir. Sibernetik kelimesi ilk olarak 1948 yılında Amerikalı bilim insanı Norbert Wiener'ın "Cybernetics" isimli kitabında kullanılmıştır. Sibernetik, Yunanca "Kubernetes" ve Latince "Gobernare" kökeninden gelmektedir. Her iki kelime de bulundukları dilde sevk ve idare anlamına gelmektedir. Sibernetik; canlılarda ve makinelerde kontrol, iletişim ve işleyişi inceleyen bilim dalıdır.[40] Ayrıca TDK sözlüğünde *"güdüm bilimi"* olarak da ifade edilmektedir. [41]

[40] https://www.turkcebilgi.com/sibernetik - (22.04.2018)
[41] http://www.tdk.gov.tr - (08.11.2017)

Bilişim bağlamında siber; internete ait olan, sanal gerçeklik veya bilgisayar ağları ile ilgili olan şeklinde tanımlanabilir. Siber sözcüğü bir kavramın önüne ek şeklinde gelerek kullanılmaktadır. Siber ortam, siber güvenlik, siber uzay, siber tehdit, siber terör, siber savaş, siber casusluk, siber fidyecilik ve siber silah kavramları bunlardan bazılarıdır.

2.2. SİBER UZAY

İnternet bir dönem sanal ortam, "sanal âlem" veya "siber âlem" olarak adlandırılmıştır. Günümüzde sıklıkla internet ortamını ifade etmek için kullanılan siber uzay (cyberspace) kavramı ilk olarak Kanadalı ünlü bilimkurgu yazarı William Gibson'ın 1982 yılında yayımlanan "Burning Chrome" adlı romanında kullanılmıştır. Daha sonra yine aynı yazarın 1984 yılında yayımlanan bir bilgisayar korsanının "Matrix" adlı bilgisayar sistemine sızarken yaşadıklarını anlatan "Neuromancer" adlı romanında kullanılmıştır. William Gibson'ın kitabında siber uzay;

> "*...her ulustan milyonlarca yasal kullanıcının, matematiksel kavramları öğrenen çocukların, her gün yaşadığı anlaşmalı yanılsama. İnsan sistemindeki her bir bilgisayarın kayıtlarından yansıtılan verilerin grafiksel sunumu. Kavranamayacak bir karmaşıklık. Zihnin uzaysızlığında; ışık çizgileri, öbekler ve takımyıldızlar şeklinde düzenlenen veriler…* "[42]

şeklinde ifade edilmiştir.

2000'li yıllardan itibaren siber uzayın çok hızlı gelişme göstermesiyle birlikte siber uzay kavramına ilişkin yeni tanımlar ortaya çıkmıştır. Siber uzay, ABD (Amerika Birleşik Devletleri) Savunma Bakanlığı'nın 2010 yılında yaptığı tanımda;

> "*İnternet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve kontrol birimlerini içeren, birbirine karşılıklı olarak bağımlı olan, bilgi teknolojileri altyapıları tarafından oluşturulan küresel alandır.*"

[42] *William GIBSON,Neuromancer, 1984 (aktaran:* Keleştemur, Atalay (2015), *Siber İstihbarat*, Level Kitap Umuttepe Yayınları, İstanbul s. 133*)*

şeklinde ifade edilmiştir.

NATO 2011 yılında yapmış olduğu tanımda siber uzay kavramını bütünsel bir bakış açısıyla ele almış ve siber uzayı;

> "*Bilgisayar ve bilgisayar ağlarının ortaya çıkardığı, insanlar ve bilgisayarların bir arada bulunduğu ve çevrimiçi faaliyetlerin tamamını kapsayan sayısal dünyadır.*"

şeklinde ifade etmiştir.

NATO yaptığı tanımda siber uzayın sadece bilgisayar ve BİT sistemlerinden ibaret olmadığını, bu sistemleri yöneten insanların da siber uzayın bir parçası olduğunu ifade etmiştir. Bu bağlamda siber savaşçı, siber terörist, siber ordu ve siber güvenlik uzmanı gibi insan kaynaklı üyelerin de siber uzayda önemli bir yeri vardır. [43]

Tanımlardan da anlaşılacağı üzere siber uzay birbirine bağlı iletişim sistemlerinden meydana gelmektedir. İnternet, siber uzayın önemli bir kısmını oluşturmaktadır. Siber uzayı yalnızca internet ortamına indirgemek doğru bir yaklaşım değildir. İnternet ortamının yanı sıra donanım sistemleri, yazılım sistemleri, mobil ağlar, telsiz sitemleri, hava trafik ağları, BİT altyapılarını kullanan intranet[44] ağları da siber uzayın diğer elemanlarıdır.

İletişim ağlarının birbirine bağlanmasıyla siber uzay çok hızlı bir şekilde büyüme göstermiştir. Siber uzay iletişim ortamlarının birbirlerine uzaktan erişimin mümkün olduğu bir ortamdır. Bu ortam üzerinde, aralarında binlerce kilometre mesafe bulunan iki nokta arasında iletişime geçebilmek mümkündür.

[43] Keleştemur, Atalay (2015), *Siber İstihbarat*, Level Kitap Umuttepe Yayınları, İstanbul s. 132-133.
[44] **İntranet:** Sadece belirli bir kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı bir ağdır.

Siber uzay uluslararası ilişkilerde kara, deniz, hava ve uzay olarak bilinen dört fiziksel boyuta insanlar tarafından eklenen beşinci boyuttur. Siber uzay NATO tarafından ilk kez 2016 Varşova Zirvesi'nde operasyonel bir alan olarak tanınmıştır. Siber uzay dört fiziksel boyuttan keskin bir şekilde farklılaşmasına karşın, belirtilen dört boyutla karmaşık bir ilişkiye sahiptir.[45]

2.3. SİBER GÜVENLİK

Siber güvenliğin uluslararası alanda kabul görmüş birçok tanımı bulunmaktadır.

BİT şirketi Cisco siber güvenlik kavramını;

> *"Siber uzayı oluşturan bilişim sistemlerinin gizlilik, bütünlük ve erişilebilirliğini korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin bütünü…"*

olarak ifade etmektedir.

Uluslararası Standartlar Teşkilatı ISO siber güvenlik ya da siber uzay güvenliği kavramını;

> *"Bilginin siber uzayda gizlilik, bütünlük ve erişilebilirliğinin korunması şeklinde ifade etmektedir. Ayrıca siber uzayı; teknolojik cihazlar ve birbirine bağlı ağlar vasıtasıyla, internet üzerinde insan, yazılım ve hizmetlerin birbiriyle etkileşim içerisinde olduğu fiziksel olmayan karmaşık bir yapı…"*

olarak ifade etmektedir. [46]

---

[45] Kasapoglu, Can (2017), *Cyber Security: Understanding The Fifth Domain*, EDAM Cyber Policy Paper Series 2017/1 s. 2.

[46] http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf (12.12.2017)

Türkiye'de siber güvenlik faaliyetlerini yürütmekten sorumlu kurum olan Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB) ise Ulusal Siber Güvenlik Stratejisi'nde siber güvenlik kavramını;

> *"Siber saldırılara karşı alınan tedbirler bütünü… Kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullandığı araçlar, geliştirilen politika ve uygulamalar; yazılı belgeler, elektronik ortam dokümanları, etkinlikler, eğitimler ve bilişim alanında kullanılan güvenlik teknolojilerinin tamamı…"*

olarak ifade etmektedir.[47]

Tüm tanımlardan yola çıkarak siber güvenlik ifade edilecek olursa;

Siber uzaydaki verilerin ve ağların tehditlere veya yetkisiz erişimlere karşı gizlilik, bütünlük veya erişilebilirliğini korumak amacıyla alınan bir dizi tedbire siber güvenlik denir.

Devletlerin kritik altyapılarını ve mahrem bilgilerini ciddi anlamda tehdit eden siber saldırı türlerine karşı savunma mekanizmalarının geliştirilmesi, ülkelerin ulusal güvenlikleri için kritik öneme sahiptir. Son yıllarda birçok ülke siber güvenlik faaliyetlerini arttırarak BİT altyapılarını güçlendirmiş ve nitelikli insan kaynağının arttırılmasına yönelik eğitim faaliyetlerini arttırmışlardır. Ülkeler tüm bu faaliyetlerin yürütülmesi sırasında uluslararası işbirliğine de önem vermişlerdir.

2015 yılında siber suçların dünya genelindeki maliyeti 3 trilyon Amerikan Doları olmuştur. Çeşitli siber güvenlik toplulukları ve konu ile ilgili uzman kişilerin ortak tahminlerine göre 2021 yılında siber suçların dünyaya maliyeti 6 trilyon

[47] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2015), "*2016-2019 Ulusal Siber Güvenlik Stratejisi*", s. 8.

Amerikan Doları olacaktır.[48] Rakamlar siber güvenliğin önümüzdeki yıllarda daha da önem kazanacağını göstermektedir.

2.4. SİBER SALDIRI

Siber uzaydaki imkânların kullanılarak BİT altyapılarına yönelik yapılan tüm kötü niyetli eylemlere siber saldırı denir.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı[49] (UDHB) Ulusal Siber Güvenlik Stratejisi'nde siber saldırı kavramını,

> *"Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler…"*

olarak ifade etmektedir.[50]

Çoğunlukla siber korsanlar tarafından gerçekleştirilen siber saldırılar, bunun dışında bazı devletlerin siber orduları tarafından da gerçekleştirilebilmektedir. Siber saldırı türleri ve yöntemleri gün geçtikçe artış göstermektedir. Bu da en temel güvenlik önlemlerini dahi karmaşık hale getirmiştir. Günümüzde AET (Advanced Evasion Techniques) adı verilen gelişmiş saldırı yöntemlerine karşı, savunma amaçlı gelişmiş güvenlik sistemlerini kullanmak zorunlu hale gelmiştir.

Siber uzayda yer alan yazılım, donanım ve BİT sistemleri gibi altyapılar siber saldırıların hedefinde yer almaktadır. Siyasi nedenler, dini nedenler, ekonomik

[48] https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html (12.12.2017)
[49] 10.07.2018 tarihli ve 1 sayılı Cumhurbaşkanlığı Kararnamesi ile görev ve yetkileri yeniden düzenlenerek adı "Ulaştırma ve Kalkınma Bakanlığı" olarak değiştirilmiştir. (Resmi Gazete 30474)
[50] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2015), "*2016-2019 Ulusal Siber Güvenlik Stratejisi*", s. 8.

nedenler, intikam alma güdüsü ya da merak duygusu gibi çeşitli sebeplerle siber saldırılar gerçekleştirilebilmektedir. Siber saldırılar bir ideolojiyi dayatma, bilgi hırsızlığı, hedef sistemi çökerterek kullanılamaz hale getirme gibi amaçlar taşıyabilmektedir.[51]

Siber saldırıların temelde aktif ve pasif olmak üzere iki tipi vardır. Aktif saldırılar hedef bilgiyi ele geçirmek, sisteme zarar vermek ya da sistemi kullanılamaz hale getirmek gibi faaliyetler; pasif saldırılar ise sisteme zarar vermeden, sistem üzerindeki veri trafiğinin izlenmesine yönelik faaliyetlerdir.

Siber saldırının etkileri de hedefe göre değişiklik gösterebilmektedir. Kimi siber saldırıların etkileri sistemi yavaşlatma veya sistemi devre dışı bırakma olabiliyorken; bazı saldırıların yangın, sel, patlama hatta can kayıpları gibi daha ağır etkileri olabilmektedir.[52]



Şekil 2.1 Anlık Küresel Siber Saldırı Haritası[53]

[51] *Siber İstihbarat*, a.g.k. s. 287.
[52] a.g.k s. 288.
[53] https://cybermap.kaspersky.com/ (18.05.2018)

Günümüzde saldırganlar tarafından dünyanın farklı yerlerine anlık olarak binlerce siber saldırı gerçekleştirilmektedir. Şekil 2.1'de görüleceği üzere dünyada internet ağının yaygınlaşmasına bağlı olarak ülkeler arasındaki sınırlar kalkmış, bir noktadan çok uzaklardaki bir noktaya siber saldırı düzenlemek mümkün hale gelmiştir.

2.5. SİBER SALDIRI TÜRLERİ

Siber uzayda bilgisayar ve haberleşme ağlarına yapılabilecek çok fazla sayıda saldırı çeşidi vardır. Örneğin sosyal mühendislik yöntemleri, kötü amaçlı yazılımlar, oltalama (phishing) ve DDoS (Distributed Denial of Service) atakları en yaygın kullanılan siber saldırı yöntemleridir.

Siber saldırı düzenlenmeden önce saldırıda bulunulacak sistemin ya da kişinin zayıf ve güçlü yönleri siber saldırganlar tarafından belirlenmektedir. Ardından tespit edilen zafiyete ve saldırının amacına göre belirlenen şekilde siber saldırı gerçekleştirilmektedir. Genellikle birçok sisteme sızmak ya da kullanılamaz hale getirmek için insan zafiyetlerinden yararlanılmaktadır. Çünkü bir BİT sisteminde en zayıf halka insan faktörüdür.

Bu bölümde sitemlere sızmak, çalışamaz hale getirmek ya da sistemleri izlemek maksadıyla gerçekleştirilen siber saldırı türleri ele alınmaktadır.

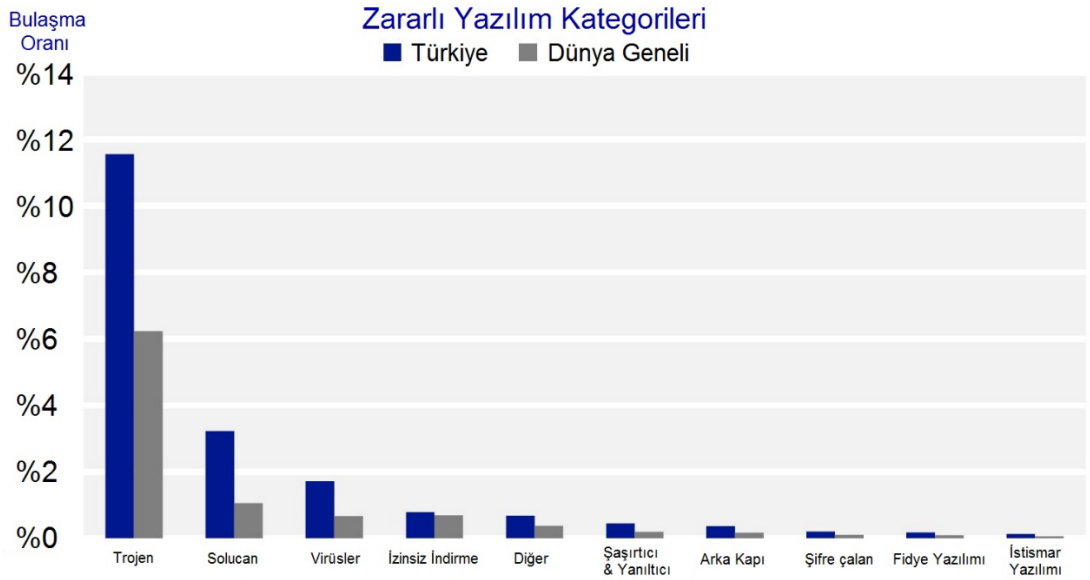
2.5.1. Kötücül Yazılımlar

Bir bilişim sistemine bulaşarak sisteme zarar veren ya da sistemi izinsiz izleyen/dinleyen kötü niyetli yazılımlara kötücül yazılım denir. Kötücül yazılımlar; kullanıcıların bilgisi olmadan sisteme uzaktan erişebilme, içerikleri izleyebilme veya

değiştirilebilme, sistemden dışarıya bilgi gönderebilme gibi yeteneklere sahip olabilmektedirler.[54]

İnternet üzerinden gerçekleştirilen saldırılardan en yaygın olanı ağ tabanlı saldırılardır. Küresel internet ağının günden güne büyümesiyle birlikte, internet üzerinden sunulan hizmetler ve interneti kullanan insan sayısı sürekli artış göstermiştir. Yaygınlaşan ve hızlanan internet ağı da saldırganlara kötücül faaliyetlerin gerçekleştirilebilmek için önemli bir altyapı sunmuştur.

Kötü niyetli yazılımlar içine yerleştikleri cihazın veya sistemin yavaşlamasına, çalışamaz hale gelmesine hatta cihazların kötü niyetli bilişim korsanları tarafından uzaktan kontrol edilebilmesine imkân sağlayabilmektedirler. 2000'li yıllardan önce yalnızca bilgisayarları tehdit eden zararlı yazılımlar, günümüzde özellikle internete bağlanabilen akıllı cihazlar başta olmak üzere tüm teknolojik cihazları ve ağları tehdit eder hale gelmiştir. Siber dünyada virüs, worm (solucan), trojen (truva atı), tuş kaydedici (keylogger), casus yazılım (spyware) olarak adlandırılan yazılımlar kötü niyetli yazılımlara örnek olarak verilebilir.



Şekil 2.2 Dünya Geneli ve Türkiye Zararlı Yazılım Bulaşma Oranları[55]

[54] http://virusler.info.tr/kotucul-yazilim/ (12.03.2018)
[55] Microsoft Security Intelligence Report – *Volume 22 (January-March 2017)* s. 4.

Microsoft tarafından 2017 yılı mart ayı içerisinde yayımlanan rapora göre dünya genelinde ve Türkiye'de zararlı yazılım bulaşmış bilgisayarların oranı Şekil 2.2'de yer almaktadır. Bu oran dünya genelinde %8,1 iken, Türkiye'de %14,1'dir. Oranlardan da anlaşılacağı üzere Türkiye'deki zararlı yazılımların oranı dünya ortalamasının oldukça üzerindedir.[56]

2.5.1.1. Virüsler

Teknolojinin günümüzdeki kadar gelişmediği ve insan hayatına bugünkü kadar ortak olmadığı dönemlerde canlı organizmaları tehdit eden biyolojik virüs; ancak elektron mikroskobu ile görülebilen, kendi başına yaşamını sürdüremeyen, konak bir canlının üzerinde yaşayan ve çoğalan, hastalık yapıcı, parazit şeklinde tanımlanmaktaydı.

Teknolojinin gelişmesiyle birlikte insan hayatının vazgeçilmezleri haline gelen teknolojik cihazlar da aynı canlı organizmaların maruz kaldığı gibi birtakım tehditlere maruz kalmaya başlamışlardır. TDK sözlüğünde bilişim sistemlerini tehdit eden virüs; "*veri girişi yoluyla yüklenen, sistemin veya programların bozulmasına, veri kaybına veya olağan dışı çalışmasına neden olan yazılım*" olarak tanımlanmaktadır.[57]

İlk olarak bilgisayarlarda ortaya çıkan ve "virüs" adı verilen zararlı yazılımlar biyolojik virüs ile hemen hemen aynı mantıkta çalışmaktadır. Virüsler birtakım yazılım, donanım (USB bellek, diskler vb.), bilişim ağı veya dosyayı konak olarak kullanmak suretiyle, cihazlar veya ağlar arasında kendilerini kopyalayabilmektedirler. Siber saldırılarda yaygın olarak kullanılmakta olan virüsler hedef cihazdan veya sistemden kritik verileri elde edebilecekleri gibi bu verileri ortadan da kaldırabilmektedirler.[58]

---

[56] a.g.r. s. 4.
[57] http://www.tdk.gov.tr (11.11.2017)
[58] Gürkaynak, Muharrem ve İren, Âdem Ali (2011) *"Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler"* Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi C.16, S.2, s. 273.

2.5.1.2. Solucanlar (Worm)

Kendisini bir bilgisayardan diğerine kopyalamak üzere tasarlanmış zararlı yazılım türüdür. Virüs, yayılabilmek için kullanıcının kendisini bilerek veya bilmeyerek diğer bilgisayarlara göndermesini beklerken; solucanlar böyle bir şeye ihtiyaç duymadan kontrolsüz bir şekilde çoğalarak, farklı bilgisayarlara ulaşmaya çalışmaktadırlar. Ayrıca solucanlar kendilerini sayısız kez kopyalayabilmektedirler.

Genellikle e-posta ile gönderilen ekler, web siteleri ve ağ üzerinden paylaşılan dosyaları kullanarak yayılım göstermektedirler. Özellikle ağ kaynakları solucanların hızla çoğalabilmelerine ve birçok bilgisayara ulaşabilmelerine olanak sağlayan ortamlardır. Solucanlar tarafından ele geçirilen sistemlerde kullanıcının e-posta adres listeleri gibi veri kaynakları hedeftedir. Böylelikle adres listesinden daha fazla kullanıcıya ulaşarak çoğalmak mümkün olmaktadır.

Sayısız kez çoğalabilme özelliğine sahip olan solucanlar, çoğalırlarken kullanıcının bant genişliklerini ve ağ kaynaklarını kullanmaktadırlar. Bu durum da ağların kilitlenmesine, e posta sunucularının aşırı yüklenmesine veya web ortamlarına erişim sürelerini arttırmaktadır.[59]

2.5.1.3. Truva Atları (Trojen)

Truva atı, virüs ve solucanlar gibi bilgisayarlar için tehdit oluşturan zararlı yazılımlardan birisidir. İsmi Eski Yunan'da Truva şehrinin çöküşüne neden olan aldatıcı tahta bir at olan Truva'dan gelmektedir. Genellikle yararlı gibi gözüken kullanıcının çalıştırması ile aktif hale gelen yazılımlardır.

Truva atları virüs ve solucanlardan farklı olarak hedef sistem üzerinde açıklar (delikler) bırakarak, bilgisayarları savunmasız hale getirmektedirler. Truva atları

[59] http://bidb.itu.edu.tr (12.11.2017)

bilgisayarların kötü niyetli kişilerce izlenmesine, içeriklerin değiştirilebilmesine ve kötü niyetli saldırılarda kullanılabilmesine olanak sağlamaktadırlar.

Truva atlarının iki türlü yayılma yöntemi vardır. Birincisi, bilindik bir programın (popüler bilgisayar oyunları veya programlar) bilgisayar korsanı tarafından tahribata uğratılmak suretiyle içine zararlı yazılımın yerleştirilmesi ile kullanıcılara bulaştırıldığı yöntemdir. Diğer yayılma şeklinde ise, bilgisayar korsanı tarafından zararlı bir yazılım üretilir. Üretilen bu zararlı yazılım sahte e-posta veya bağlantı adresi ile kullanıcıya ulaştırılır. Bu zararlı bağlantıya kullanıcı tarafından tıklanması durumunda, zararlı yazılım aktif hale gelerek bulaşma gerçekleşmektedir.

Truva atları virüs ve solucanlar gibi kendi başlarına harekete geçememektedirler. Yazılımın bulaşması; genellikle kullanıcının sahte linklere tıklaması veya bilgisayara lisanssız yazılımlar kurulması gibi işlemler sonucunda gerçekleşmektedir.[60]

2.5.1.4. Tuş Kaydedici (Keylogger)

Bilgisayarlara veya mobil cihazlara bulaşarak klavyeden yazılan her şeyi kaydeden yazılımlardır. Yazılımın amacı klavyede basılan tuşları sürekli kaydedip, bunları bir metin dizisi haline getirerek saldırgana iletmektir. Özellikle siber istihbaratçılarca sıkça kullanılan bir casusluk yöntemidir. Tuş dinleyici zararlı yazılımlar gömülü olarak donanımlar üzerinde olabileceği gibi, sonradan yüklenen bir bilgisayar programı ya da mobil uygulama şeklinde de olabilmektedir. Özellikle donanım üzerinde bulunan tuş dinleyiciler donanıma gizlendiği için BİT uzmanları tarafından bile çoğu zaman zor tespit edilmektedir.

Bu tür yazılımlar genellikle kullanıcı adı, şifre, kredi kartı bilgileri vb. gibi kişisel bilgileri ele geçirmeyi hedefleyen yazılımlardır. Gelişen teknoloji ve internet

[60] https://en.wikipedia.org/wiki/Trojan_horse_(computing) (12.11.2017)

hızının artmasıyla birlikte tuş dinleyici yazılımların yetenekleri de artmıştır. Günümüzde tuş dinleme yazılımları, bilinen özelliklerine ek olarak yerleştiği cihazın kamera veya mikrofonlarına erişim sağlayarak ses ve görüntü de elde edebilmekte; internet ağı aracılığıyla bu verileri saldırgana anlık olarak gönderebilmektedir.[61]

2.5.1.5. Şebeke Trafiğinin Dinlenmesi (Sniffing)

Türkçe anlamı koklamak olan "*sniffing"*, bir ağ üzerindeki veri trafiğini izleyerek içeriğini okumaktır. Bu işlem "*sniffer*" adı verilen zararlı yazılımlarla gerçekleştirilmektedir. Bu yöntem, siber saldırganlara izledikleri ağ trafiği üzerinden kullanıcılara ait şifreleri ve e-posta trafiği gibi gizli verileri izinsiz bir şekilde ele geçirebilmelerine imkân sağlamaktadır. Bu yöntemden korunmak için ağda bulunan bilgisayarlar arasındaki bağlantıların şifrelenmesi gerekmektedir. Şifrelenmiş veri paketleri ağın dinlenmesini engelleyemez; ancak ele geçirilen paketler kriptolandığı (şifrelendiği) için içeriklerine ulaşılamamaktadır.

Sniffing yöntemi ağ yöneticileri tarafından da yaygın olarak kullanılan bir yöntemdir. Ağ yöneticileri bu yöntem ile ağda bir sorun olup olmadığını ya da verilerin şifreli olarak iletilip iletilmediğini de kontrol edilebilmektedirler.[62]

2.5.1.6. IP Aldatmacası (IP Spoofing)

Bilgisayar ağlarında ve internet ağı üzerinden gerçekleşen veri haberleşmesinde kullanılan temel protokol İnternet Protokolü (IP)'dür. IP adresi, internet ağını kullanan bir cihazı diğer cihazlardan ayıran bir kimliktir. Bir bilgisayar bu protokol üzerinden farklı bir bilgisayara bağlandığında karşı tarafa kimliğini bildirmektedir. IP aldatmacası ya da IP spoofing olarak da bilinen saldırı türünde,

[61] Siber İstihbarat a.g.k. s. 224-225.
[62] Öğün, Mehmet Nesip ve Kaya, Adem (2013), "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri Dergisi*, Yıl: 9, Sayı: 18, s. 160.

saldırı yapan bilgisayarın IP adresi farklıymış gibi gösterilmekte ya da gizlenmektedir. Sahte IP adresinden bir paket alan bilgisayar genellikle paketin kimden geldiğini bilemez ya da göndericiyi sorgulamaz.

IP aldatmacası saldırganların kimliklerini gizledikleri önemli bir yöntemdir. Özellikle hizmet dışı bırakma (DDoS) saldırılarında sıkça kullanılmaktadır. Bunun dışında IP adresine dayalı kimlik doğrulama sistemlerinde de hedef bilgisayarı aldatmak maksadıyla kullanılabilmektedir.[63]

2.5.1.7. BOTNET Ağları

İnternete bağlı binlerce hatta milyonlarca cihazın (bilgisayar, tablet, telefon vb.) kötü bir amaç için bir araya geldiği, genellikle tek bir merkezden yönetilen zararlı ağlara BOTNET denir. BOTNET'e dâhil olan cihazların kullanıcıları, güvenlik yazılımı veya donanımı (güvenlik duvarı, antivirüs vb) kullanmadıkları için çoğu zaman bu zararlı ağa dâhil olduklarının farkında olmamaktadırlar.

İnternet ortamında gezinirken temel korumadan yoksun cihazlar ile zararlı bir linke tıklanması ya da zararlı bir içeriğin cihaza indirilmesi sonucunda BOTNET ağına dâhil olunmaktadır. Eğer tıklanan link zararlı yazılım (rootkit, trojen vb.) barındırıyor ise bu zararlı yazılım otomatik olarak cihazın işletim sisteminde bir arka kapı (back door) oluşturmaktadır. Cihaz oluşturulan arka kapı sayesinde BOTNET'in yönetim merkeziyle bağlantı kurar hale gelir ve böylelikle zararlı ağa dâhil olmaktadır.[64]

BOTNET ağları, siber saldırganların saldırı kapasitesini ciddi oranda arttırarak hedef sistemin kolaylıkla ele geçirilebilmesini sağlamaktadır. Çoğunlukla "hizmet dışı bırakma saldırıları" olarak adlandırılan DDOS saldırılarında kullanılan BOTNET ler;

[63] Siber İstihbarat a.g.k. s. 299-300.
[64] Atluri, Anoop Chowdary ve Tran, Vinh (2017), "Botnets Threat Analysis and Detection", *Springer International Publishing AG 2017/ I. Traoré et al. (eds.), Information Security Practices, DOI 10.1007/978-3-319-48947-6_2*, s. 7. (www.springer.com – 15.10.2018)

kredi kartı dolandırıcılığı ve veri hırsızlığı gibi kötü amaçlı faaliyetler için de kullanılabilmektedir.

BOTNET ağına dâhil olan cihazların dağınık bir yapıda olması, ağda bulunan cihazların internet erişiminin durdurulmasının imkânsız olması ve ağların yöneticilerine ulaşabilmenin çok zor olması gibi sebeplerden dolayı BOTNET saldırıları engellenememektedir.[65]

BOTNET ağlarına dâhil olmamak için yapılabilecek işlemler;

- İnternete bağlı tüm cihazlarda güncel antivirüs yazılımı kullanılmalıdır.
- Tanıdık kişilerden ya da kurumlardan gelen e-postalara dahi şüphe ile yaklaşılmalı ve iyice incelenmeden açılmamalıdır.
- Sosyal medyada paylaşılan her linke ya da dosya uzantılarına (.rar, .exe, .zip, .bat, .scr vb.) tıklanmamalıdır.
- Dosya paylaşım sitelerinden (4Shared, FilesTube, Hotfile, FileServe vb.) indirilen dosyalara dikkat edilmelidir.
- Lisanslı yazılımlar dışında yazılım kullanılmamalı ve yazılımlar sürekli güncel tutulmalıdır.[66]

2.5.2. Oltalama (Phishing)

Oltalama (phishing), siber uzayda yaygın olarak kullanılan bir kimlik hırsızlığı türüdür. Bu yöntemle sahte internet adresi ya da e-posta adresleri kullanılarak kimlik bilgilerinin, şifrelerin ve kredi kartı bilgilerinin yasadışı bir şekilde ele geçirilmesi hedeflenmektedir.

[65] http://siberest.com.tr/botnet-nedir/ (15.10.2018)
[66] http://www.mugla.pol.tr/fethiye/Sayfalar/Botnet-Nedir.aspx (15.10.2018)

Kullanıcıdan, güvenilir bir kaynaktan (banka, devlet kurumu, iş yeri, aile bireyi vb.) gönderilmiş gibi görünen sahte e-postada yer alan linke tıklaması istenmektedir. Linke tıklayan kullanıcı sahte bir internet adresine yönlendirilerek, bu sahte sitede kişisel bilgilerini girmesi veya zararlı bir yazılım yüklemesi istenebilmektedir.[67]

Oltalama saldırılarının hedefinde çoğunlukla finans sektörü yer almaktadır. Özellikle büyük bankaların müşterilerine yönelik gerçekleştirilen saldırılarda birçok kişi ve kurum dolandırılarak milyonlarca lira zarara uğratılmaktadır.

2.5.3. Rootkit

İşletim sistemini yanıltmayı başararak, sistemin yönetimini ele geçirmeye yarayan zararlı yazılımlara Rootkit denmektedir. Rootkitlerin üç temel hedefi bulunmaktadır:

- **Çalıştır:** Rootkitler, sızmayı başardıkları hedef sistemde hiçbir kısıtlamaya uğramaksızın çalışmayı hedeflemektedirler. Yaygın olarak kullanılan Windows İşletim Sistemi de dâhil olmak üzere birçok işletim sisteminde, sistemde yüklü olan yazılımların Erişim Kontrol Listeleri (Access Control Lists - ACL) bulunmaktadır. Rootkitler uygulamaların ACL listelerinde yer alan açıklardan yararlanarak ya da sosyal mühendislik yöntemleriyle sisteme bir şekilde sızmayı başararak herhangi bir kısıtlamaya tabi olmazlar.

- **Gizle:** Rootkitler sızdıkları sistemde diğer zararsız uygulamalar gibi güvenlik taramalarına takılmadan kendilerini gizlemeyi hedeflemektedirler.

- **Eylem:** Rootkitlerin sızdıkları sistemde kendilerine tanımlanmış birtakım görevleri vardır. Rootkitler, geliştiricisi tarafından hedef sistemden veri veya

[67] Yıldız, Mithat (2014) *"Siber Suçlar ve Kurum Güvenliği"* Ulaştırma Denizcilik ve Haberleşme Bakanlığı Denizcilik Uzmanlık Tezi, s. 37-38.

bant genişliği çalmak, ya da sisteme zararlı bir yazılım yüklemek gibi amaçlarla üretilmektedirler.[68]

Rootkitler bulaştıkları sistemlerde fark edilmedikleri için; sisteme uzaktan izinsiz erişim sağlanması, zararlı sitelere yönlendirilme, zararlı yazılımların kurulması gibi zararlı faaliyetleri gerçekleştirebilmektedirler. Rootkitlerden korunmak için kullanılan işletim sisteminin lisanslı ve güncel olması önemlidir, ancak yalnızca bu yeterli değildir. Ayrıca sistemde yüklü olan tüm uygulamaların da lisanslı ve güncel olması gerekmektedir. Çünkü rootkitler sistemde kullanılan uygulamalardan yalnızca bir tanesinde bulunan güvenlik açığından faydalanarak tüm sistemi ele geçirebilmektedir.

2.5.4. DDoS (Hizmet Dışı Bırakma) Saldırıları

DDoS (Distributed Denial of Service) yani hizmet dışı bırakma saldırıları çevrimiçi hizmet veren bir uygulama veya bir sistemin çalışmasını engellemek amacıyla yapılan siber saldırılardır. DDoS saldırılarında hedef sistemin bant genişliğinin tamamı kullanılarak sistem meşgul edilmektedir. Böylelikle sistem kullanıcılara cevap veremez hale gelmektedir.[69]

İlk başlarda tek bir kaynaktan bir hedefe doğru hizmet engelleme amacıyla ortaya çıkan bu saldırılar, zamanla şiddetini arttırarak bir sistemin birçok kaynak tarafından hedef alınmasıyla gerçekleştirilen ve daha tehlikeli olabilen DDoS saldırıları adını almıştır. Günümüzde bu tarz saldırılar daha önceden zararlı yazılımlarla ele geçirilmiş köle bilgisayarlar tarafından gerçekleştirilmektedir.

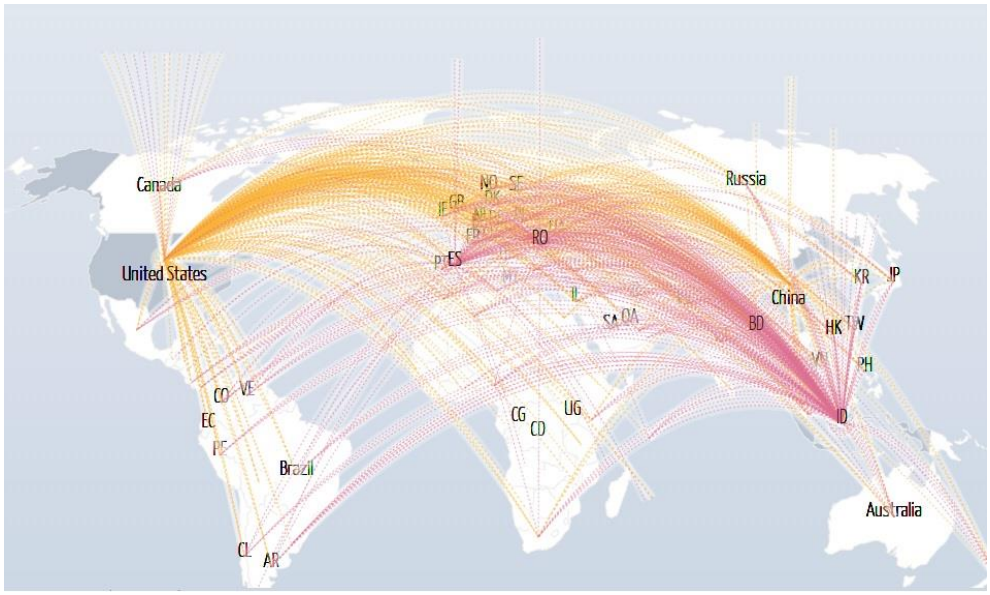
---

[68] Symantec, (2012), *"Rootkits"*, s. 1-2. (https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/rootkits-12-en.pdf - 16.10.2018)

[69] Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT) (2014) *"DDos El Kitabı"* Bilgi Teknolojileri ve İletişim Kurumu-Telekomünikasyon İletişim Başkanlığı, s. 3.

DDoS saldırıları sistemlerin erişilebilirliğini engellemeye yönelik saldırılardır. Her sistem kurulum aşamasında; hizmet verilecek kullanıcı sayısı, hat kapasitesi ve anlık istek sayısı gibi parametreler için belli değerler öngörülerek, bu değerlerin biraz üstünde yükü karşılayabilecek şekilde tasarlanmaktadır. DDoS saldırılarında ise bir sistemin kaldırabileceği yükün çok üzerinde kullanıcı ve anlık istek sayısı sistemi meşgul etmektedir. Bunun sonucunda sistem yavaşlamakta veya ulaşılamaz hale gelmektedir. [70]

Dünyada her an farklı yoğunluk ve hacimde DDoS saldırıları düzenlenmektedir. Bu saldırılar; örgütlü bir şekilde ve belli bir plan dâhilinde düzenlenmeleri durumunda hedef sisteme ciddi zararlar verebilmektedir. Şekil 2.3'de dünya genelinde anlık olarak gerçekleşen DDoS saldırı trafiği yer almaktadır. Haritadaki gibi bir sistemin birçok kaynak tarafından hedef alındığı saldırılarda, hedef sistem hizmet veremez hale gelmektedir.



Şekil 2.3 Dünya Geneli Anlık DDOS Saldırıları Haritası[71]

Verisign adlı BİT hizmetleri sunan şirketin 2017 yılı 1. Çeyrek DDoS raporuna göre, bu dönemde gerçekleşen DDoS saldırı sayısı 2016 yılı 4. Çeyreğinde gerçekleşen

[70] Altundal, Ömer Faruk (2012) *"DDoS nedir, ne değildir?"* Siber Güvenlik Derneği, s. 4-7.
[71] http://www.digitalattackmap.com (10.05. 2018)

saldırı sayısına göre %23 oranında azalmıştır. Ancak saldırı sayısı azalmış olmasına karşın saldırıların şiddetleri bir önceki yıla göre %26 oranında artmıştır. Yine aynı raporda en çok hedeflenen üç sektör %58 ile BİT sektörü, %28 ile finans sektörü ve %6 ile medya sektörü olmuştur. Sonuçlar saldırıların bir önceki yıla göre hacim, hız ve karmaşıklığında belirgin bir artışın meydana geldiğini ortaya koymaktadır.[72]

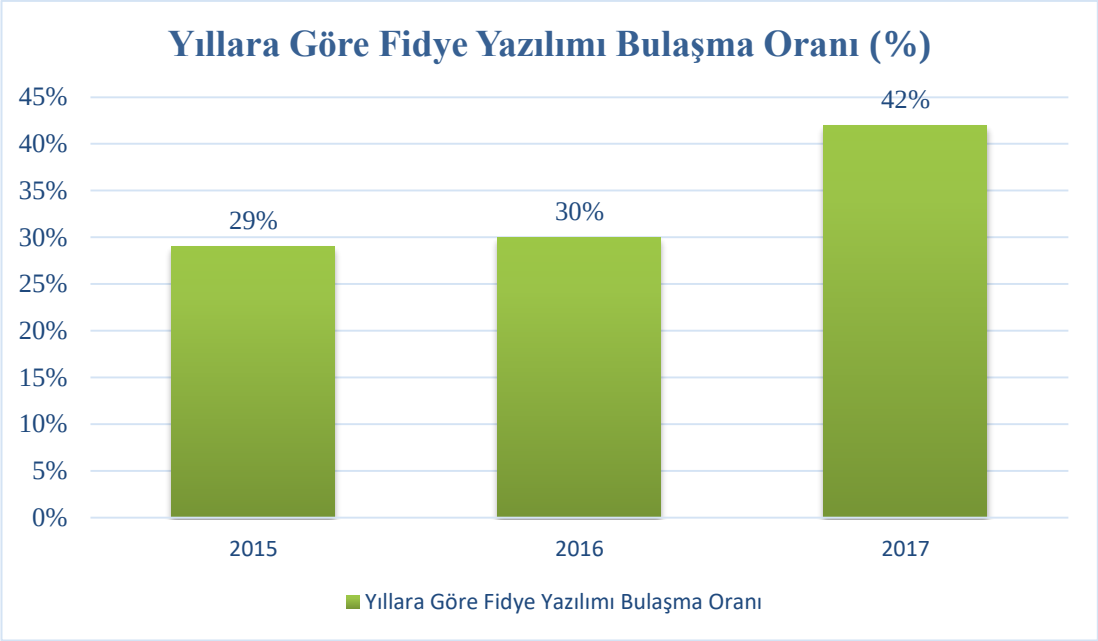
Aynı şirketin 2017 yılı 2. Çeyrek DDoS raporuna göre, DDoS saldırıları ile en çok hedeflenen sektörün %52 ile BİT sektörü olmuş; BİT sektörünü %31 ile finans sektörü ve %13 ile e-ticaret sektörü takip etmiştir.[73]

2.5.5. Ransomware (Fidye Yazılımı)

Bulaştıkları bilgisayarlarda kullanıcı dosyalarını şifreleyerek erişilemez ve kullanılamaz hale getirerek; ardından şifrenin kırılabilmesi için para talep eden zararlı yazılımlardır.[74] Bu tür yazılımlar fidye yazılımları olarak da bilinmektedir.

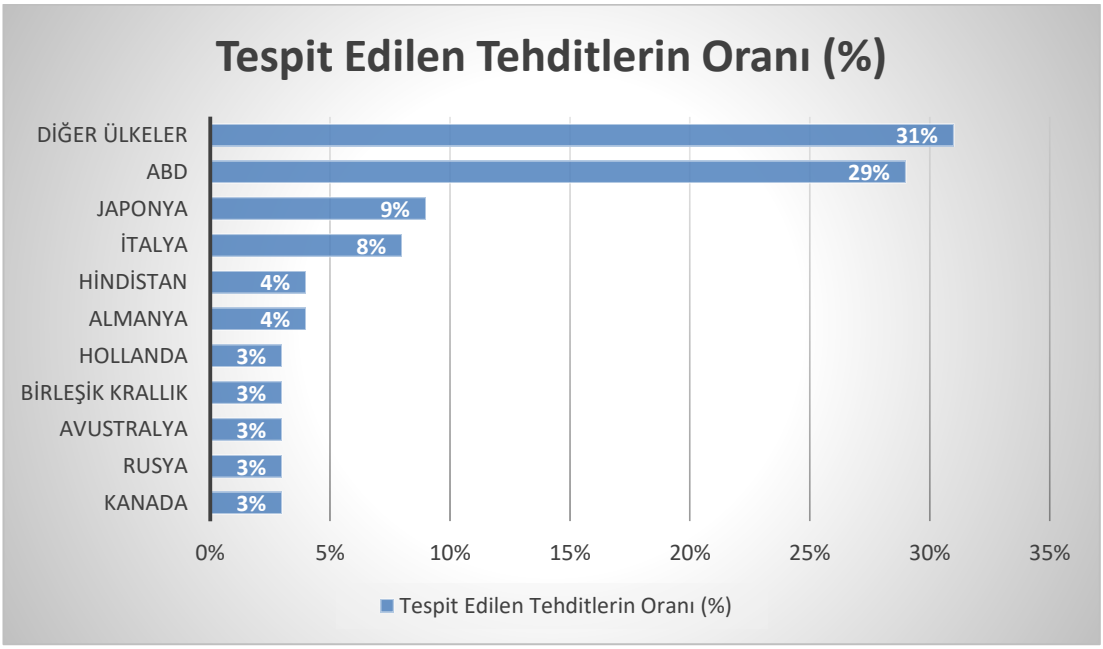
Fidye yazılımları genellikle bir e-posta mesajına eklenerek, oltalama yöntemiyle sistemlere sızmaktadırlar. Kurumsal firmalardan gönderilen bir e-fatura bildirimi gibi gönderilen sahte e-posta mesajlarının, gerçeğinin birebir kopyası olması nedeniyle ilk bakışta fark edilmesi oldukça zordur. Eğer şifrelenen verilerin veya sistemin yedekleri mevcut değilse; kullanıcılar, içeriklere yeniden erişim sağlayabilmek için istenen ücreti ödemek zorunda kalmaktadırlar.

[72] https://www.verisign.com/assets/infographic-ddos-trends-Q12017_tr_TR.pdf (23.04.2018)
[73] https://www.verisign.com/assets/infographic-ddos-trends-Q22017_tr_TR.pdf (23.04.2018)
[74] http://www.vodafone.com.tr/VodafoneHakkinda/zararli-yazilimlar.php (15.11.2017)



Şekil 2.4 Yıllara Göre Dünya Geneli Fidye Yazılımı Bulaşma Oranı

Symantec şirketi tarafından yayımlanan Şekil 2.4'de yer alan rapora göre çoğunluğunu ticari işletmelerin oluşturduğu kuruluşlardan fidye yazılımların saldırısına uğrayanların oranı 2015 yılında %29 ve 2016 yılında %30 iken bu oran 2017 yılında %42'ye yükselmiştir.



Şekil 2.5 Fidye Yazılımından Etkilenen Ülkelerin Dağılımı [75]

[75] O'brien, Dick (2017) "Internet Security Threat Report – Ransomware 2017" Symantec, s. 7.

Şekil 2.5'de yer alan 2017 yılı verilerine göre saldırılardan en fazla etkilenen ülke ABD'dir. ABD'yi Japonya, İtalya, Hindistan, Almanya, Hollanda, İngiltere, Avustralya, Rusya ve Kanada takip etmektedir.[76]

2.6. SOSYAL MÜHENDİSLİK

Bilişim sistemlerinde verilerin korunması ve sistem güvenliğinin sağlanması yalnızca teknik imkânlarla mümkün olmamaktadır. Çünkü en iyi korunan sistemlerde bile güvenlik zincirinin halkalarından birisi de insan unsurudur. İnsan davranışları, insanın duygusal durumuna göre zaman zaman farklılıklar gösterebileceği için bu durum güvenlik zafiyetlerine sebep olabilmektedir. İnsan bu yüzden güvenlik zincirlerinin en zayıf halkası konumunda bulunmaktadır. İnsanın zafiyetlerinden yararlanarak bunu istismar etme düşüncesi sonucunda, sosyal mühendislik kavramı ortaya çıkmıştır. Sosyal mühendislik, insanların zafiyetlerinden faydalanarak gizli/önemli bilgilere ve ağ sistemlerine yetkisiz erişim sağlama yöntemlerinin tamamıdır.[77]

Sosyal mühendislik yöntemi düşük teknoloji ve düşük maliyet gerektiren bir yöntem olduğu için saldırganlar tarafından yaygın olarak kullanılan bir yöntemdir. Bilgi sistemlerinde güvenliğin sağlanması konusu büyük oranda insanlara bağlıdır. En gelişmiş güvenlik sistemlerinin kullanıldığı bilişim sistemlerinde dahi insan zafiyetlerinden yararlanılarak kullanıcı ve parola bilgilerinin ele geçirilmesi halinde, kullanılan güvenlik sistemlerinin bir önemi kalmamaktadır.[78]

[76] a.g.e s. 4-7.
[77] Gündüz, M. Zekeriya ve Daş, Resul (2017), "Sosyal Mühendislik ve Korunma Yolları", *CyberMag Dergisi*, Sayı 18, s. 14-15.
[78] a.g.e. s. 15-16.



Şekil 2.6 Sosyal Mühendislik Saldırılarının Aşamaları

Bir sosyal mühendislik saldırısı Şekil 2.6'da yer alan döngüdeki gibi gerçekleşmektedir. Saldırının her bir adımı sosyal mühendisler tarafından belli bir düzen içinde gerçekleştirilmektedir. Öncelikle belirlenen hedef hakkında kritik bilgiler toplanarak hedefin zafiyetleri belirlenir. Belirlenen zafiyetlerden faydalanılarak saldırı işlemi gerçekleşir. Sosyal mühendis, saldırı hedeflerinin başarıya ulaşması sonucu kendisini ele verebilecek saldırı kanıtlarını ortadan kaldırır.[79]

2.6.1. Sosyal Mühendislik Saldırı Yöntemleri

Sosyal mühendislik ile kişiler, kurumlar ve devletlere ait önem arz eden verilerin ele geçirilmesi, kişisel veya kurumsal verilerin silinmesi veya içeriğinin değiştirilmesi, ilgili kişi veya kurumların itibarının zedelenmesi, sistemlere zararlı programlar yüklenerek veri trafiğinin izlenmesi veya yönetilmesi gibi olaylar mümkün

[79] a.g.e. s. 16.

olabilmektedir. Sosyal mühendislik saldırıları kullanılan yöntem bakımından insan tabanlı ve teknoloji(bilgisayar) tabanlı olmak üzere ikiye ayrılmaktadır.[80]

- **İnsan Tabanlı (Human Based)**

İnsan tabanlı sosyal mühendislikte insanlarla bire bir etkileşim söz konusudur. Bu tür sosyal mühendislikte, sosyal mühendis tarafından bilginin doğrudan elde edilmesi amaçlanmaktadır. Sosyal mühendisler insan tabanlı sosyal mühendisliği farklı şekillerde kullanabilmektedirler. En yaygın kullanılan yöntemlerden bazıları aşağıda açıklanmaktadır.

- **Kişiliğe Bürünme (Impersonation):** Bu yöntemde sosyal mühendis bir kurumun çalışanı veya sistem üzerinde erişim yetkilerine sahip bir kullanıcı gibi davranır. Böylelikle kurum çalışanı, güvenlik görevlisi veya taşeron firma yetkilisi gibi ortama fiziksel olarak erişim sağlayabilmektedir.

- **Önemli Bir Kullanıcı Gibi Davranmak (Important User):** Sosyal mühendisin kritik verilere ve bilgi işlem sistemlerine erişebilmek için üst düzey bir yetkili gibi davranmasıdır. Alt kademede çalışan personel çoğunlukla kendilerinin üstü konumunda olan yöneticilerin dediklerini sorgulamadan yerine getirmektedirler.

- **Üçüncü Taraf Olmak (Third Party Authorization):** Sosyal mühendisin bilgi işlem sistemlerine erişim sağlamak için yetkili bir kişiden izin almış gibi davranmasıdır. Bu yöntem yetkili kişilere teyit için ulaşılamayacağı durumlarda kullanılan bir yöntemdir.

- **Yardım Masası (Help Desk):** Yaygın olarak kullanılan sosyal mühendislik yöntemlerinden birisidir. Bu yöntemde sosyal mühendis, kurban olarak seçtiği kullanıcıya teknik destek sunmak üzere arandığını ve kullanıcıdan verdiği talimatları yerine getirmesini istemektedir.

[80] a.g.e. s. 19.

- **Sinsice Gözetleme veya Dinleme (Shoulder Surfing):** Klavyeden bilgi giren bir kullanıcının şifre bilgilerini sinsice izlemek suretiyle elde etmek ya da kritik bir toplantıda konuşulanları izinsiz dinleyerek ele geçirmek amacıyla başvurulan sosyal mühendislik yöntemidir.

- **Çöp Dalışı (Dumpster Diving):** Önem arz eden bilgileri elde etmek amacıyla hedefin çöp kutusunun gizlice karıştırılmasıdır.

- **Telefon Oltalaması (Vishing):** İngilizce voice (ses) ve phishing (oltalama) kelimelerinden türeyen "Vishing", bir oltalama türüdür. Oltalamada seçilen kurbana sahte bir e-posta içerisinde gönderilen link yerine bir telefon numarası yer almaktadır. Bu telefon numarasının aranarak bilgilerin güncelleştirilmesi istenir ve böylelikle kullanıcının bilgileri ele geçirilmektedir.[81]

- **Bilgisayar Tabanlı (Computer Based)**

İstenen bilgilerin elde edilebilmesi için zararlı bilgisayar yazılımlarının veya teknik cihazların kullanıldığı sosyal mühendislik türüdür. Bu sosyal mühendislik türünde kurban ile doğrudan iletişim söz konusu değildir. En yaygın olarak kullanılan iki yöntemi vardır.

- **Sazan Avlama (Oltalama):** Saldırganlar bu yöntemde gizli bilgileri ele geçirmek üzere gerçek ve bilindik bir sistem kimliğine bürünmektedirler. Bilindik bir firmanın ya da kurumun web sitesinin aynısı tasarlanarak; kullanıcının e-posta adresine gönderilen link ile bu sahte siteye bağlanması sağlanmaktadır. Sahte sitede kullanıcının bilgilerinin güncellenmesi ya da teyit edilmesi gibi sahte amaçlarla, kullanıcıdan kişisel verilerini girmesi istenmektedir. İlk bakışta söz konusu siteyi gerçeğinden ayırt edemeyen kullanıcı, kendisinden istenen verileri girerek saldırganların tuzağına düşmektedir.

[81] a.g.e. s. 17-18.

- **Çevrimiçi Dolandırıcılık (Online Fraud):** Sosyal mühendis tarafından hedef seçilen kurbana ekinde sahte yazılım bulunan bir e-posta yollanmasıdır. Ekteki yazılım klavye dinleyen yazılım (keylogger), cihazın kamerasına ya da mikrofonuna erişim sağlayan zararlı yazılım, virüs, trojen (Truva atı) veya worm (solucan) zararlı yazılımları olabilmektedir.[82]

Sosyal mühendislik saldırılarında kullanılan donanımlar basit ve etkili olmalarının yanında, kolayca temin edilebilen donanımlardır. Böylelikle saldırıların kolaylıkla yapılabilmesi mümkün hale gelmektedir.[83]

Sosyal mühendisler kurbanlarını kolaylıkla tuzağa düşürebilmek için saldırılarında çok konuşulan güncel olayları veya tartışmaları (deprem, savaş söylentileri), sahte haber sitelerini, uzun zamandır beklenen bir ürün veya hizmet ile ilgili tanıtımı, ünlü kişilerle ilgili asılsız haberleri, telefon ile dolandırıcılığı, bazı sosyal medya numaraları gibi çeşitli yanıltıcı yöntemler kullanmaktadırlar.[84]

Türkiye'de 2015 yılında sosyal mühendislik yöntemlerini kullanarak telefon üzerinden kendilerini polis, hâkim, savcı olarak tanıtan dolandırıcılar kurbanlarından kayda geçen 40 milyon TL civarında telefon dolandırıcılığı gerçekleştirmişlerdir. Gerçek rakamın bu rakamın çok üzerinde olduğu düşünülmektedir.[85]

2.7. SİBER ZORBALIK

Siber ortamda bilişim teknolojilerini kullanarak bir bireye ya da bir gruba karşı kasıtlı olarak yapılan aşağılama, korkutma, iftira, tehdit ve taciz gibi rahatsız edici

[82] a.g.e. s. 18.
[83] http://www.bilgimikoruyorum.org.tr/?b323_sosyal_muhendislikte_kullanilan_saldiri_yontemleri (24.12.2017)
[84] https://www.trendmicro.com.tr/media/resource_lib/social/5-reasons-why-social-engineering-tricks-work-tr.pdf - (24.12.2017)
[85] http://www.hurriyet.com.tr/telefonla-dolandiricilara-milyonlarca-lira-kaptirdik-37247480 (23.05.2018)

eylemlerin tümüne siber zorbalık denmektedir.[86] Teknolojinin amacı dışında kullanılması sonucu ortaya çıkan siber zorbalık, ilk olarak Amerika ve Kanada'da ortaya çıkmış olsa da son 10 yılda dünyanın her yerine salgın gibi yayılarak küresel bir tehdit haline gelmiştir. Günden güne artan siber zorbalık eylemleri fiziksel ve ruhsal anlamda başta çocuklara ve gençlere olmak üzere ciddi zararlar vermektedir.[87]

Amerikalı Pew Research şirketi tarafından yapılan, 4228 yetişkin Amerikalının katıldığı Çevrimiçi Taciz 2017 Raporu Anketi'ne göre; her 10 Amerikan vatandaşından 4'ünün siber ortamda en az bir kez çevrimiçi tacize uğramış olduğunu ve insanların %62'sinin siber zorbalığı bir tehdit olarak gördüklerini ortaya koymaktadır. Aynı şirketin 2014 yılında yaptığı bir önceki ankete göre siber zorbalık eylemleri 2017 yılına gelindiğinde %14 artış göstermiştir.

Tablo 1 Çevrimiçi Taciz Türlerine İlişkin Veriler

Taciz Türü	Oran
Çevrimiçi Lakap Takma	%27
Birisini Mahcup Etme Çabaları	%22
Fiziksel Tehditler	%10
Sinsice Takip (Stalklama)	%7
Sürekli Taciz	%7
Cinsel Taciz	%6

Ankete katılan vatandaşların karşılaştığı siber zorbalık tacizlerinin oransal dağılımı yukarıdaki Tablo 1'de yer almaktadır. Sonuçlara göre *Çevrimiçi Lakap Takma* %27 ile ilk sırada yer almakta olup bu taciz türünü %22 ile *Birisini Mahcup Etme Çabaları* ve %10 ile *Fiziksel Tehditler* takip etmektedir. Katılımcılardan %41'i siber zorbalığa maruz kaldığını, %18'si ise cinsel taciz ve takip gibi şiddetli tacize maruz kaldıklarını belirtmişlerdir. Ankete katılan yetişkinlerden %66'sı ise başkalarına yönelik gerçekleştirilen siber zorbalık eylemlerine tanıklık ettiklerini bildirmişlerdir. Ayrıca raporda, çevrimiçi platformların birçoğunda bu tarz eylemlerin

[86] http://www.samsung.com/tr/sosyal-sorumluluk/siber-zorba-olma/ (26.12.2017)
[87] http://www.haberturk.com/yasam/haber/1522728-can-almaya-baslayan-siber-zorbalik-cagin-sorunu-olmaya-aday (26.12.2017)

gerçekleştiği; özellikle Facebook, Twitter, Snapchat ve Instagram gibi sosyal mecraların bu tarz eylemler için uygun bir zemin oluşturduğu ortaya konmuştur.[88]

Çevrimiçi ortamlarda kullanıcılar çok farklı şekillerde siber zorbalığa maruz kalabilmektedirler. En yaygın karşılaşılan siber zorbalık türleri;

- Mobil cihazlar ile bireylerin izinsizce görüntülerinin çekilerek sosyal medya platformlarında paylaşılması,
- Sosyal medya platformlarında kullanıcılara küçük düşürücü, şiddet içerikli, taciz edici veya tehdit edici iletilerin gönderilmesi,
- Bir kişinin kimlik bilgileri veya özel hayatına dair gizli bilgileri sosyal medyada paylaşılması,
- İnternet ortamında özel veya tüzel kişiliklerin itibarlarını zedeleyici, karalayıcı asılsız dedikoduların paylaşılması,
- Bir kişinin tüm sosyal medya hesaplarını ısrarlı bir şekilde takibe alınması,
- Bir kişi hakkında karalayıcı propagandalar yapılarak sosyal medyada ve gerçek hayatta dışlanmasının sağlanması gibidir.[89]

Ülkemizde Kocaeli Üniversitesi ile TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu)'ın iş birliği ile öğrenciler arasında yapılan siber zorbalık araştırması çok çarpıcı sonuçlar ortaya koymuştur.

- Araştırmaya katılan öğrencilerin Facebook hesabı olanların oranı %90'dır.
- Öğrenciler arasında sözlü olarak siber zorbalığa maruz kalma oranı %11,64 iken siber zorbalık yaptığını belirtenlerin oranı ise %10,13'tür.

[88] Duggan, Maeve (2017) *"Online Harassment 2017 Report"* Pew Research Center www.pewresearch.org , s. 1-7.
[89] http://www.hurriyet.com.tr/siber-zorbaliga-yuzde-20-maruz-kaliyor-40664423 (27.12.2017)

- Araştırmaya katılan öğrencilerden sosyal medyada tanımadığı kişiler ile konuşanların oranı %56,5'tir.

- Katılımcı kız öğrencilerin %16'sı, erkek öğrencilerin ise %30,5'i uğradıkları siber zorbalığa karşılık vermeyi doğru bulmaktadır.

- Siber uzayda en az bir kez sözlü tacize uğradığını belirtenlerin oranı %25,4'tür.

- Siber zorbalığa maruz kalmaları durumunda bunu okul arkadaşımla paylaşırım diyenlerin oranı %41, ailemle paylaşırım diyenlerin oranı %37 ve öğretmenlerimle paylaşırım diyenlerin oranı ise %15 olmuştur.[90]

Günümüzde çocuklar ve gençler arasında artan sosyal medya bağımlılığı ve çevrimiçi oyun bağımlılığı siber zorbalık olaylarının da artışını beraberinde getirmektedir. Özellikle ergenlik dönemlerinde özgüveni gelişmeyen bireylerin siber zorbalık eylemlerinden olumsuz etkilenme ihtimalleri yüksektir.

Çocuklara ve gençlere psikolojik anlamda ciddi zararlar veren siber zorbalık intiharlara da sebep olabilmektedir. 2013 yılında ABD'nin Florida eyaletinde meydana gelen 12 yaşındaki Rebecca Ann Sedwick isimli genç kızın intiharıyla sonuçlanan olay intihar vakalarının en çarpıcı örneklerinden birisidir. Genç kız, telefonunda bulunan mesajlaşma uygulamasında adını '*Ölü Kız*' olarak değiştirdikten sonra iki arkadaşına '*Sonsuza dek hoşçakalın…*' mesajı atmıştır. Ardından evinin yakınında bulunan terk edilmiş bir binaya giderek, kendisini yüksekten aşağı bırakarak yaşamına son vermiştir.

Rebecca'nın ölümünün ardından polisin yaptığı araştırma, genç kızın son 1 yıl içerisinde 15 kız arkadaşı tarafından internet ortamından '*Ölmelisin!*', '*Neden intihar etmiyorsun?*' gibi mesajlarla baskı altına alındığını ve bunun sonucunda depresyona girerek intihara sürüklendiğini ortaya koymuştur. Olaydan sonra genç kızın annesi kızının her zaman güler yüzlü bir kişilik takındığını ve hiçbir zaman olayın

[90] https://www.cnnturk.com/teknoloji/siber-zorba-olma-farkina-var-hareketi-basladi (27.12.2017)

ciddiyetinin farkına varamadığını belirtmiştir. Bu olay; gençlerin siber ortamdan kolaylıkla baskı ve aşağılanmalara maruz kalarak depresyona girebileceklerini ve hatta en önemlisi de en yakınları olan ailelerinin bile bu vahim durumdan haberdar olamadıklarını göstermektedir.[91]

[91] http://www.milliyet.com.tr/abd-yi-karistiran-intihar/dunya/detay/1763540/default.htm (28.12.2017)

ÜÇÜNCÜ BÖLÜM

ULUSLARARASI ALANDA SİBER GÜVENLİK

Ülkelere ait BİT altyapılarının yaygınlaşması, internetin küresel bir altyapı olarak tüm dünyayı sarması ve bireylerin bu sistemleri yoğun olarak kullanması; ülkeleri ve bireyleri geri dönülemez bir şekilde bu sistemlere bağımlı hale getirmiştir. Siber uzayda artan tehditler ve kapsamlı siber saldırılar ülkelerin ulusal güvenlikleri için ciddi anlamda tehdit oluşturmaya başlamıştır. Birçok siber saldırıda ülkelere ait kritik altyapılar ciddi zarar görmüş, ülkeler büyük savaşların eşiğine gelmişlerdir.

Tüm bu gelişmelerin sonucunda her ülkenin kendine ait bir Bilgi Güvenliği Politikası ve Ulusal Siber Güvenlik Stratejisine sahip olması zorunlu hale gelmiştir. Bütün devletler yaygınlaşan BİT sistemleri ve internet kullanımıyla beraber; sahip oldukları kritik altyapıları korumak, nitelikli siber güvenlik personeli yetiştirmek, vatandaşlarını siber tehditlere karşı bilinçlendirmek gibi amaçlarla siber güvenlik stratejilerini hazırlayarak bu alanda çeşitli faaliyetlerde bulunmaktadırlar.

Bu bölümde siber güvenlik stratejileri, eğitim çalışmaları ve uluslararası iş birliği faaliyetleri ile ön plana çıkan dünya ülkeleri ile NATO, BM ve AB gibi bazı uluslararası kuruluşların bu alanda yaptıkları faaliyetler ele alınmaktadır.

3.1. ULUSLARARASI SİBER GÜVENLİK FAALİYETLERİ

Siber uzayda günden güne artan ve güçlenen tehditler, ülkelerin bu alanda iş birliği yapmalarını zorunlu hale getirmiştir. Tehditlerle etkin bir şekilde mücadele

edebilmek için uluslararası kuruluşlar bu alandaki faaliyetlerini yoğunlaştırarak eylem planlarını hazırlamışlardır. Bu başlık altında siber güvenlik ve bilgi güvenliğine ilişkin çalışmalarıyla dikkat çeken Avrupa Birliği, NATO ve BM gibi uluslararası kuruluşların çalışmaları ele alınmaktadır.

3.1.1. Avrupa Birliği (AB)

AB kritik altyapıların diğer devletler ya da terör saldırılarına karşı korunmasına yönelik tebliğini 2004 yılında yayımlamıştır. Tebliğde kritik altyapılar; "kesintiye uğraması ya da zarar görmesi durumunda vatandaşların sağlıkları, güvenlikleri ve ekonomik durumları üzerinde veya üye devletlerin etkin ve verimli bir şekilde işleyişi üzerinde olumsuz etkiler oluşturabilecek fiziksel altyapılar, bilişim sistemleri ve hizmetler" olarak tanımlanmıştır.[92] Tebliğe göre enerji sistemleri, haberleşme, bankacılık, finans, ulaşım ağları, sağlık, gıda, su, tehlikeli madde taşımacılığı ve hükümetlere ait bilişim sitemleri kritik altyapı sektörleri kapsamına alınmıştır.[93]

2006 yılında Avrupa Kritik Altyapıları Koruma Programı (The European Programme for Critical Infrastructure Protection-EPCIP) hazırlanmıştır. Söz konusu Program ile kritik altyapıların korunması, tehditlerin tespit edilmesi, gerekli önlemlerin alınarak hasar ve saldırı olasılıklarının asgari düzeyde tutulması hedeflenmiştir.[94] 2008 yılında EPCIP programının uygulamasını kolaylaştırmak için Kritik Altyapı Uyarı Bilgi Ağı (Critical Infrastructure Warning Information Network-CIWIN) oluşturulmuştur.[95]

[92] Commıssıon Of The European Communıtıes (2004), *Critical Infrastructure Protection in the fight against terrorism*, s. 10. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (01.05.2018)
[93] a.g.b. s.4.
[94] http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/epcip_presentation_/epcip_presentation_en.pdf (01.05.2018)
[95] https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (01.05.2018)

Avrupa Komisyonu 2010 yılında ağ ve bilgi güvenliğini sağlamak, olası tehditleri tespit etmek ve önlemek için "Avrupa İçin Sayısal Gündem" projesini hayata geçirmiştir. Proje kapsamında kritik altyapı sektörlerinin büyük kısmının işletmesini yürüten özel sektör de siber güvenlik çalışmalarına dâhil edilmiştir.

2010 yılında AB ve NATO tarafından ortak düzenlenen Lizbon Zirvesi'nde siber olaylara hızlı bir şekilde müdahale edilebilmesi için bir merkez kurulmasına karar verilmiştir. Alınan karar kapsamında 11 Ocak 2013 tarihinde Europol bünyesinde Avrupa Siber Suç Merkezi (European Cybercrıme Centre - EC^3) kurulmuştur. 2011 yılında AB bünyesindeki kurumların bilgisayar olaylarına acil müdahalede bulunabilmek amacıyla Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Team, CERT-EU) oluşturulmuştur.[96]

AB'nin siber güvenlik faaliyetlerini yürüten bir diğer teşkilat, 2004 yılında kurulan Avrupa Ağ Güvenliği ve Bilgi Güvenliği Teşkilatı (European Network and Information Security Agency - ENISA)'dır. ENISA, çalışmalarına aktif olarak 2005 yılında başlamıştır. Teşkilat AB sınırları içerisindeki haberleşme ağlarının kurulması, siber güvenliğin sağlanması ve ilgili personelin eğitilmesi hususlarında çalışmalarını sürdürmektedir. ENISA tarafından AB'ye üye ülkelerin diğer devletler ya da terörist gruplarca yapılacak siber saldırılara karşı güçlü bir savunmaya sahip olabilmeleri amacıyla belirli aralıklarla siber güvenlik tatbikatları düzenlenmektedir.[97]

3.1.2. Kuzey Atlantik Antlaşması Örgütü (NATO)

NATO 21. yüzyıl başlarına kadar kara, hava, deniz ve uzay olmak üzere dört farklı operasyonel alanda faaliyetlerini sürdürmüştür. 1999 yılında Kosova krizinin patlak verdiği dönemde Sırp hackerlar[98] tarafından NATO web sitesine siber saldırı

[96] *Siber Saldırılar- Siber Savaşlar ve Etkileri*, a.g.t. s. 56-57.
[97] *Siber İstihbarat,* a.g.k. s. 192.
[98] **Hacker:** Bilgisayar korsanı.

düzenlenmiştir. Saldırının ardından NATO tarafından siber uzay savaşın beşinci boyutu olarak tanımlanmış ve siber güvenlik alanında çalışmalara başlanmıştır.

2002 yılında üye ülkelerin katılımıyla Prag'da düzenlenen zirvede NATO üyesi devletlerin siber savunma ve bilgisayar olaylarına müdahale yeteneklerinin geliştirilmesi ile ilgili konular görüşülmüştür. 2006 Riga Zirvesi'nde siber saldırılar yeniden ele alınarak, NATO'nun siber uzayda alacağı karşı önlemlerin daha kapsamlı ve yeni bir bakış açısıyla ele alınması vurgulanmıştır.[99]

İttifak bünyesinde yer alan Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability - NCIRC) NATO sitelerine tek bir merkezden 24 saat boyunca siber savunma desteği sağlayarak, NATO ağlarını siber ortamdaki tehditlere karşı korumaktadır. NCIRC sistem yöneticileri ve kullanıcılara siber ortamdaki önemli olayları raporlayarak ilgili birimlerde farkındalık oluşturmaktadır. Ayrıca NATO ve müttefik ağlarını korumak için Acil Müdahale Ekipleri (Rapid Reaction Teams) de NCIRC içinde sürekli göreve hazır halde bulunmaktadır.

NATO ve 29 müttefiki arasında siber saldırıları önleme, savunma kabiliyetinin geliştirilmesi, saldırılara etkin bir şekilde karşılık verilebilmesi ve karşılıklı bilgi alışverişinin sağlanması hususunda mutabakat zaptı imzalanmıştır. Her yıl düzenlenen Siber Koalisyon Tatbikatları gibi ortak çalışmalar ile siber savunma unsurları ve görüşlerinin tüm ittifak uygulamalarına entegre edilmesi amaçlamaktadır. NATO tüm bu çalışmaların yanı sıra siber güvenlik eğitimi ve AR-GE çalışmalarını da yürütmektedir.[100]

2007 yılında Baltık ülkesi Estonya'nın başkenti Tallinn meydanında yer alan Bronz Asker Anıtı'nın kaldırılması[101] üzerine, ülke yoğun siber saldırılara maruz

[99] a.g.k s. 193.
[100] Fact Sheet, (2016), NATO s. 1. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, (02.05.2018)
[101] Bronz Asker Anıtı'nın kaldırılması olayına ilişkin ayrıntılı bilgi *"Uluslararası Alanda Gerçekleşen Büyük Siber Saldırılar/Estonya Siber Saldırıları"* bölümünde ayrıntılı olarak ele alıncaktır.

kalmıştır. Bu olayın ardından 2008 Bükreş Zirvesi'nde siber savunma konusunda iş birliğinin önemine değinilerek, bu alanda faaliyet yürütecek yeni bir birimin kurulması kararı alınmıştır. Alınan karar üzerine 14 Mayıs 2008 tarihinde Estonya'nın başkenti Tallinn'de Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence - CCDCOE) kurulmuştur. CCDCOE, siber savunma konusunda müttefik ülkelere eğitim ve danışmalık desteği sunmasının yanı sıra birlik bünyesinde siber güvenlik alanında AR-GE çalışmalarını yürütmektedir.

İtalya'nın Latina şehrinde bulunan NATO İletişim ve Bilgi Sistemleri Okulu, NATO üyesi ülkeler ile diğer ülkelerin ilgili personellerine NATO'nun bilişim ve güvenlik sistemlerinin işleyişi ve bakımı ile ilgili eğitim programları düzenlemektedir. Ayrıca Almanya'nın Oberammergau şehrindeki NATO Okulu ve İtalya'nın Roma şehrindeki NATO Savunma Koleji de NATO operasyonları, stratejileri ve politikalarını destekleyici benzer eğitim faaliyetlerini yürütmektedir.[102]

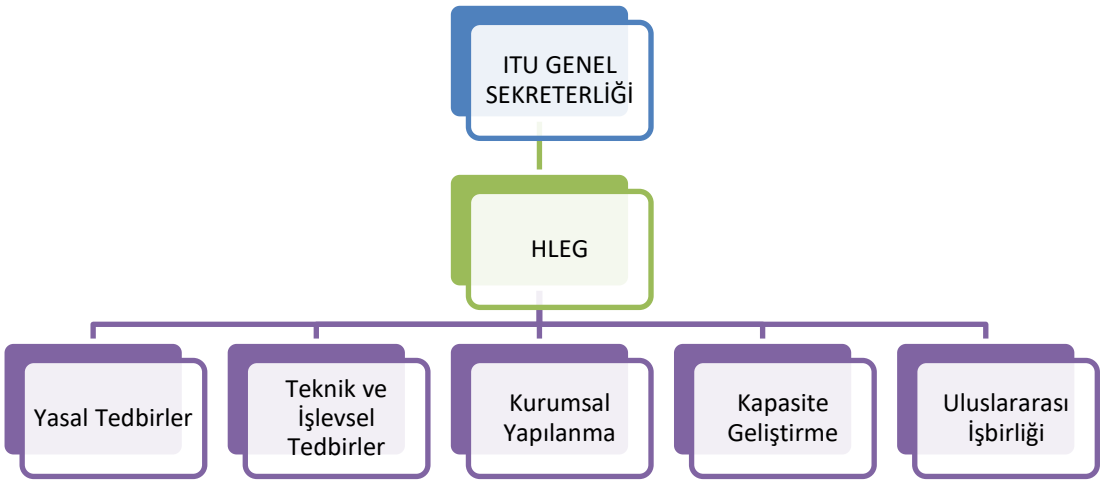
3.1.3. Birleşmiş Milletler (BM)

BM'nin siber güvenliğe ilişkin faaliyetleri, BM bünyesinde yer alan hükümetler arası birçok organ tarafından ele alınmaktadır. BM bünyesinde tüm organlar bir konu hakkında karar alabilir, ancak nihai kararlar çoğunlukla Birleşmiş Milletler Genel Kurulu (United Nations General Assembly - UNGA) ve Birleşmiş Milletler Güvenlik Konseyi (United Nations Security Council - UNSC) tarafından gerçekleştirilen oylama sonucunda alınmaktadır. UNSC tarafından kabul edilen kararlar dışındaki kararlar üye devletler için tavsiye niteliğinde olup, yasal bağlayıcılığı bulunmamaktadır. Günümüze kadar siber güvenlik sorunlarına ilişkin kararlar yalnızca UNGA'da alınmıştır.

[102] Fact Sheet, (2016), NATO s. 2.

Siber güvenliğin farklı yönleriyle ilgili taslak kararlar, BM'nin altı ana komitesinden üçü (Silahsızlanma ve Uluslararası Güvenlik Komitesi; Ekonomik ve Mali Komite; Sosyal, İnsani ve Kültürel Komite) tarafından UNGA'ya iletilmiştir.[103]

BM'nin BİT faaliyetlerinin yürütmekten sorumlu alt birimi Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU) 2001 yılında düzenlenen Dünya Bilgi Toplumu Zirvesi'nin ardından yürütmekte olduğu telekomünikasyon faaliyetlerinin yanında siber güvenlik alanında da etkin olarak çalışmalara başlamıştır.[104] Ekim 2007'de üye devletlere siber güvenlik alanında stratejik öneriler geliştirmede ITU Genel Sekreterliğine yardımcı olmak amacıyla Yüksek Seviyeli Uzmanlar Grubu (High Level Experts Group - HLEG) kurulmuştur.[105] HLEG'in üyeleri farklı ülkelerden tüm kamu kurum ve kuruluşları, özel sektör, araştırma merkezleri, uluslararası kuruluşlar ve üniversitelerde siber güvenlik hususunda alanında uzman kişilerden oluşmaktadır.[106]



Şekil 3.1 Küresel Siber Güvenliğin Beş Ana Unsuru

[103] https://ccdcoe.org/un.html - 17.10.2018
[104] https://www.itu.int/en/action/cybersecurity/Pages/default.aspx - 17.10.2018
[105] https://www.itu.int/itunews/manager/display.asp?lang=en&year=2008&issue=06&ipage=05&ext=html – 17.10.2018
[106] http://www.cybersecuritygateway.org/pdf/Members%20of%20the%20ITU%20High%20Level%20Experts%20Group.pdf – 17.10.2018

2007 yılında HLEG uzmanlarının çalışmaları sonucunda, bilgi toplumunda güven ve bilgi güvenliğinin sağlanmasına yönelik uluslararası işbirliğinin nasıl sağlanacağına ilişkin bir yol haritası sunan Küresel Siber Güvenlik Gündemi (Global Cybersecurity Agenda - GCA) yayımlanmıştır. Söz konusu stratejik güvenlik raporunda, küresel siber güvenliğin beş ana unsuru belirtilmiştir. Bu unsurlar Şekil 3.1 'de yer almaktadır.[107]

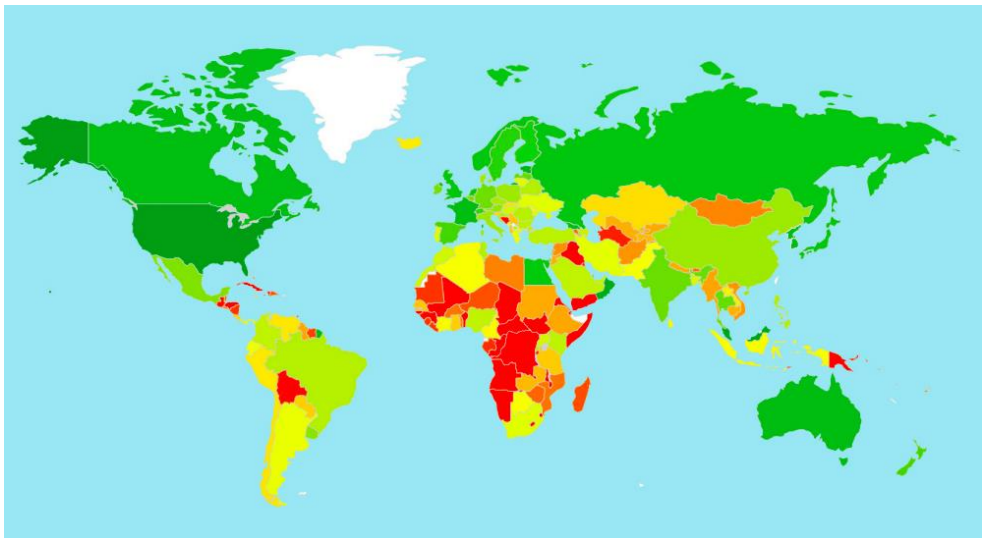
ITU tarafından 2008 yılında çevrimiçi alanda çocukların korunmasının küresel bir sorun olduğu ve bu sorunun çözümünün küresel bir yaklaşım gerektirdiği vurgulanmıştır. Bu kapsamda Kasım 2008'de Çocuk Çevrimiçi Koruma (Child Online Protection - COP) girişimini başlatmıştır. COP girişimi çocukların çevrimiçi ortamlarda güvenliğine ilişkin stratejilerini hazırlarken 2007 yılında yayımlanan Küresel Siber Güvenlik Gündeminde yer alan belirtilen beş ana unsuru esas almaktadır.[108]

ITU, merkezi Malezya'nın Cyberjaya şehrinde bulunan kamu ve özel sektör girişimi olan Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (International Multilateral Partnership Against Cyber Threats - IMPACT) adlı kuruluş ile 2011 yılında Uluslararası Bilgi Toplumu Zirvesinde iş birliği anlaşması imzalamıştır. IMPACT bu anlaşmanın ardından ITU'nun siber güvenlik alanında resmi danışmanlık birimi unvanını almıştır.

IMPACT, ülkelerin küresel siber tehditlerle başa çıkma yeteneklerini geliştirmek üzere ITU üyesi 193 ülkeye siber güvenlik alanında uzmanlık, eğitim ve danışmanlık hizmeti vermektedir. Tüm bu çalışmalar ile siber güvenlik alanında teknik, yasal ve politik yönlerin geliştirilerek; uluslararası iş birliğinin güçlendirilmesi hedeflenmektedir.[109]

[107] International Telecommunication Union, (2017), *Global Cybersecurity Agenda*, s. 2-3.
[108] https://www.itu.int/en/cop/Pages/about_cop.aspx - 17.10.2018
[109] https://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf , (13.05.2018)

ITU tarafından ilki 2015, ikincisi 2017 yılında yayımlanan Küresel Siber Güvenlik Raporunda (Global Cybersecurity Index – GCI) devletlerin siber saldırılara karşı savunma kapasitelerine ilişkin durumları açıklanmıştır. Bu rapor ile ülkelere ait siber savunma kapasitesinin ölçümünün yanı sıra üye devletlerin siber güvenlik farkındalığının arttırılması amaçlanmaktadır. GCI ölçümlerinde GCA'da belirlenen yasal, teknik, kurumsal, kapasite geliştirme ve uluslararası iş birliğine yönelik faaliyetler referans alınmaktadır.



Şekil 3.2 Ülkelerin Siber Savunma Kapasitelerine İlişkin Harita

Yine 2017 GCI raporunda dünya ülkelerinin siber güvenlik savunma kapasitelerini gösterir harita Şekil 3.2'de yer almaktadır. Siber savunma kapasitesi en yüksek ülkeler koyu yeşil renge boyalı ülkelerdir. Ardından sırasıyla yeşil, sarı ve turuncu ülkeler gelmektedir. Siber savunma kapasitesi en düşük ülke ise koyu kırmızı renkle gösterilmektedir.[110]

[110] a.g.r. s. 13.

3.2. ÜLKELER

Uluslararası kuruluşların yanı sıra birçok ülke kendi ihtiyaçları doğrultusunda bilgi güvenliği ve siber güvenlik stratejilerini hazırlamışlardır. Bu bölümde siber güvenlik faaliyetleri ile ön plana çıkan bazı ülkelerin bu alanda yaptıkları çalışmalar ele alınmaktadır.

3.2.1. Amerika Birleşik Devletleri

ABD 1990'lı yıllardan itibaren siber güvenlik çalışmaları üzerine yoğunlaşmaya başlamıştır. İlk olarak Şubat 2003'de "Sayısal Ortamın Güvenliği İçin Ulusal Strateji" adlı siber güvenlik stratejisi yayımlanmıştır. Söz konusu güvenlik stratejisi artan güvenlik gereksinimlerine göre 2009 yılında güncellenerek yeniden yayımlanmıştır.[111]

Siber güvenlik faaliyetlerine ilişkin sorumluluklar; İç Güvenlik Bakanlığı (Department of Homeland Security - DHS), Federal Soruşturma Bürosu (Federal Bureau of Investigation - FBI), Birleşik Devletler Siber Komutanlığı (USCYBERCOM) ve Ulusal Güvenlik Ajansı (National Security Agency-NSA) arasında dağıtılmıştır. ABD adına gerçekleştirilen siber saldırı operasyonlarının çoğu, Siber Komutanlık ve Merkezi İstihbarat Teşkilatı (Central Intelligence Agency - CIA) tarafından koordineli olarak gerçekleştirilmektedir.

İç Güvenlik Bakanlığı'nın siber alanda birincil sorumluluğu; ülke içindeki siber savunma faaliyetlerini yürütmektir. İç Güvenlik Bakanlığı, ABD'nin siber uzayda çıkarlarını korumak için kamuoyu, özel sektör ve uluslararası kuruluşlarla iş birliği içinde çalışmalarını sürdürmektedir.[112]

[111] *Siber İstihbarat* a.g.k. s. 178.
[112] Cybersecurity and Cyberwarfare a.g.e. s.21-22.

USCYBERCOM, ABD Savunma Bakanlığı'nın siber savunma gücünün arttırılması ve ordunun siber uzayda caydırıcılığının güçlendirilmesi amacıyla kurulmuştur. İkincil ordu olarak tanımlanan USCYBERCOM'un başında bir general bulunmaktadır. Birim dört temel amaca odaklanmıştır. Bunlar; Savunma Bakanlığı'na ait ağlar, sistemler ve bilgi kaynaklarının korunması, siber uzayda ABD'nin çıkarlarının korunması, askeri operasyonlara entegre siber yeteneklerin geliştirilmesi ve olası siber saldırılara karşı acil eylem planlarının hazırlanmasıdır.[113]

ABD'nin 88 ülkede 4 bin askeri üstte, 15 bin iletişim ağı ve 7 milyonu aşkın bilgisayarı bulunmaktadır. Söz konusu ağların ve sistemlerin siber uzayda savunulabilmesi ve koordinasyonunun sağlanabilmesi amacıyla USCYBERCOM bünyesinde 5 bine yakın personel istihdam edilmiştir. Ayrıca komutanlık dışında da yaklaşık 100 bin personel USCYBERCOM'a destek vermektedir.[114]

FBI, ülke içerisindeki siber olayların araştırılması ve engellenmesinden sorumludur. Siber uzayda elde ettiği istihbaratları yetkili kurum ve kuruluşlarla paylaşmakla yükümlüdür. Ayrıca siber güvenlik alanında İç Güvenlik Bakanlığı'na bilgi ve destek sunmaktadır.[115]

Son yıllarda ABD Yönetimi devlet kurumlarına yönelik giderek artan siber saldırılarla mücadele edebilmek için siber güvenlik yatırımlarını her yıl arttırmaktadır. Obama Yönetimi tarafından federal kurumların siber güvenlik kapasitelerini güçlendirmek için 2016 yılı mali bütçesinden 14 milyar Dolar, 2017 yılı mali bütçesinden 19 milyar Dolar kaynak ayrılmıştır.[116]

---

[113] *"Fact Sheet: The Department of Defense (DoD) Cyber Strategy" (2015)*, USA Department of Defense, s.1-2.
[114] *Siber İstihbarat* a.g.k. s. 179.
[115] *Siber İstihbarat* a.g.k. s. 184-185.
[116] http://www.hurriyet.com.tr/abd-rusyaya-karsi-muttefikleri-icin-milyarlar-harcayacak-40052448 (11.01.2018)

3.2.2. Çin Halk Cumhuriyeti

Çin, 1990'lı yıllardan itibaren siber istihbarat faaliyetlerine yoğunlaşarak siber savaş ile ilgili birçok proje geliştirmiştir. Çalışmalar kapsamında ülkenin internet altyapısına büyük yatırımlar yapılarak, internet altyapısı koruma altına alınmıştır. Çin, vatandaşları arasından seçerek yetiştirdiği birçok siber savaşçıyı farklı hacker grupları altında örgütlemiştir. Böylelikle; dünyada meydana gelen Çin kaynaklı siber saldırıların, devletten bağımsız olarak gerçekleşen siber saldırılarmış gibi servis edilmesi amaçlanmaktadır.

Çin, özellikle ABD menşeli yazılım ve donanımlardan uzak kalarak, kendi yazılım ve donanım sitemlerini geliştirmektedir. ABD'nin kritik altyapılarına birçok kez sızmayı başaran Çin, saldırılar sonucunda ciddi istihbarat elde etmiştir. Çin, mevcut siber gücüyle bir siber savaşa ne kadar hazır olduğunu tüm dünyaya kanıtlamış durumdadır. Ülkede yaklaşık 250 tane hacker grubu olduğu tahmin edilmektedir.

Çin, siber alanda savunmadan ziyade saldırıya yönelik bir strateji izlemektedir. Çin ve Tayvan arasındaki siyasi gerilime ABD'nin müdahil olma teşebbüsleri sonucunda, ABD'ye yönelik ülkenin elektrik şebekesini çökertebilecek güce sahip olduğunu kanıtlar nitelikte bazı saldırılarda bulunmuştur. İnterneti aktif şekilde bir propaganda aracı olarak kullanan ülke, internet ortamında yanıltıcı pek çok veri yayımlamaktadır. Böylelikle asılsız iddialarla çeşitli algı operasyonları yürütmektedir.

Çin ordusu da siber alanda başta ABD olmak üzere diğer ülkelerle mücadele edebilmek için siber alanda teknik kapasitesini ve personelinin eğitim seviyesini arttırmaya yönelik faaliyetlerde bulunmaktadır.[117] Çin, 2011 yılında 30 kişiden oluşan Mavi Ordu adlı bir orduya sahip olduğunu tüm dünyaya duyurmuştur. Mavi Ordu'nun görevi Çin Halk Kurtuluş Ordusu'nun (PLA) internet ağlarını dış tehditlerden

[117] *Siber İstihbarat*, a.g.k. s. 185-186.

korumak olarak belirtilmiştir. Mavi Ordu PLA'da görevli asker ve subaylar ile çeşitli üniversitelerin öğrencilerinden oluşmaktadır.[118]

3.2.3. Rusya Federasyonu

Soğuk Savaş döneminde nükleer teknolojinin geliştirilmesine yoğunlaşan Rusya, 1990'lı yılların sonuna doğru siber savaş alanında faaliyetlerini arttırmıştır. İlk olarak Federal Bilgi ve İletişim Kurumu (The Federal Agency for Government Communications and Information – FAPSI) tarafından 1997 yılında bilgi savaşlarının dört bileşeni; komuta ve kontrol merkezlerinin yok edilmesi, bilgi ve iletişim teknolojilerine elektromanyetik saldırı, istihbarat toplama ve bilgisayar sistemlerinin tahrip edilmesi olarak belirlenmiştir.

2003 yılında FAPSI bünyesinde kriptoloji, kod kırma ve virüs geliştirme işlemlerinden sorumlu olan Federal Güvenlik Servisi kurulmuştur. Ayrıca sektör temsilcileri ve üniversiteler ile siber yeteneklerin araştırılması ve geliştirilmesi konusunda güçlü iş birlikleri kurulmuştur.

Rusya Federasyonu, 2010 yılının şubat ayında ulusal çıkarları ve müttefiklerinin çıkarlarını korumak için siyasi ve bilgilendirici araçların kullanımını ortaya koyan yeni askeri ilkelerini yayımlamıştır. Yayımlanan ilkeler askeri ve askeri olmayan yeteneklerin kullanımını bütünleşik bir şekilde ele alarak, modern askeri çatışmaların karakteristik özelliklerini ortaya koymaktadır. İlkelerde ayrıca devletlerarası artan bilgi savaşlarının öneminden ve devletlere verebileceği zararların boyutlarından bahsedilmektedir. Askeri güç kullanmadan siyasi hedeflere ulaşmak için önceden elde edilen kritik bilgilerin devletlere sağlayacağı avantajlara ve ileride

[118] "Çin "süper gizli ordusunu" açıkladı", Sabah, 2011. (http://www.hurriyet.com.tr/gundem/cin-super-gizli-ordusunu-acikladi-17884879 , (15.03.2018)

meydana gelebilecek askeri bir çatışmada elde edilen kritik verilerin önemine değinilmiştir.[119]

Rusya son yıllarda milli işletim sistemi ve antivirüs gibi projeleri ile dikkat çekmektedir. Ayrıca ülkenin BİT altyapısını tamamen millileştirmek için AR-GE faaliyetlerine de önem verilmektedir. Ülke, siber uzayda artan tehditlerle etkin bir şekilde mücadele edebilmek amacıyla hükümetle bağlantısı olmayan hacker grupları ile de iş birliği içinde bulunmaktadır.[120]

3.2.4. İran

İran'ın siber güvenlik faaliyetleri ordu içerisinde yer alan İran Pasif Savunma Teşkilatı (Passive Defence Organization of Iran-PDOI) isimli birim ile koordineli yürütülmektedir. Bütçesinin yaklaşık 76 milyon dolar olduğu tahmin edilen 2400 personelli PDOI, İran Devrim Muhafızları Ordusu'nun *(*The Islamic Revolutionary Guard Corps- IRGC) siber savaş gücünü oluşturmaktadır.[121]

2011 yılında ana görevi sosyal medya sitelerini ve interneti takibe almak olan İran Siber Polis Birimi (The Iranian Cyber Police Unit-FATA) kurulmuştur. FATA ayrıca İran'ın nükleer programına ciddi zararlar veren Stuxnet saldırısından sonra ülkenin web savunmasını güçlendirmeye yönelik çalışmaları da yürütmektedir.[122]

İran'ın sahip olduğu siber güç, ülkenin iç ve dış siyasetine yön vermek amacıyla etkin bir şekilde kullanılmaktadır. Ülke siber kapasitesi bakımından dünyanın ilk 10 ülkesi arasında yer almaktadır. Ülkenin siber güce düzenli olarak yatırım yapması, özellikle yurtdışı siber kapasitesinin ciddi artışına sebep olmuştur.

---

[119] Lewis, James A. ve Timlin, Katrina (2011) *"Cybersecurity and Cyberwarfare"* The Center for Strategic and International Studies, s. 19.
[120] *Siber İstihbarat*, a.g.k. s. 187.
[121] https://www.military.com/defensetech/2008/09/23/iranian-cyber-warfare-threat-assessment (15.12.2017)
[122] http://www.dw.com/tr/iran-siber-polis-ordusu-kurdu/a-14782649 (15.12.2017)

İran'ın siber faaliyetlerin artmasında iki önemli olay etkili olmuştur. Birinci olay; 2009 seçimlerinden sonra binlerce eğitimli gencin internet ve sosyal medya üzerinden organize olarak rejime yönelik eleştirel faaliyetlerde bulunmaları sonucunda, rejim sanal siyasi alanı kontrol altına almak amacıyla yeni düzenlemeler yapmıştır. Bu olay Yeşil Hareket olarak da bilinmektedir. İkinci olay ise 2010 yılında Natanz ve Buşehr nükleer tesislerine yönelik gerçekleştirilen ve uluslararası alanda büyük ses getiren Stuxnet saldırısıdır.[123] Bu saldırının ardından İran siber savunma ve saldırı gücüne ciddi yatırımlar yaparak siber kapasitesini arttırmıştır.[124]

3.2.5. İngiltere

İngiltere, en güncel ve en kapsamlı siber güvenlik stratejisi olan 2016-2021 Siber Güvenlik Stratejisini 2016 yılında yayımlamıştır. Bu stratejide güvenliğe yönelik üç yönlü bir yaklaşım yer almaktadır. Bunlar; riskleri azaltmak, fırsatları değerlendirmek ve siber olaylara tepkileri geliştirmektir. Strateji belgesinde siber ortamdaki risklerin azaltılmasının; güvenlik açıklarının azaltılması ve siber olayların etkilerinin hafifletilmesi ile sağlanabileceği ifade edilmektedir.

İngiltere siber ortamın güvenliğine yönelik istihbarat toplama, devlet güvenlik politikalarını geliştirme ve olası tehditlere yönelik savunma faaliyetlerine büyük önem vermektedir. Ulusal Siber Güvenlik Stratejisinde siber tehditlere karşı etkin bir mücadelenin; bilgi ve farkındalığın arttırılması, güvenlik politikalarının geliştirilmesi, konu ile ilgili yönetişim ve karar alma mekanizmalarının iyileştirilmesi, teknik altyapı ve insan kaynağının iyileştirilmesi ile sağlanabileceğinden bahsedilmektedir.[125] 2010 Ulusal Siber Güvenlik Stratejisinde, ülkenin siber ortamına diğer devletler tarafından

[123] Stuxnet Saldırısı *"Uluslararası Alanda Gerçekleşen Büyük Siber Saldırılar"* bölümünde ayrıntılı olarak ele alınacaktır.
[124] https://www.timeturk.com/iran-in-uluslararasi-silahi-siber-saldirilar/haber-93495 (15.12.2017)
[125] *National Cyber Security Strategy of the United Kingdom* 2016-2021, UK Office of Cyber Security, s. 9-15.

veya küresel çapta meydana gelebilecek bir siber saldırının ulusal güvenliğe en büyük tehdidi oluşturacağı vurgulanmıştır.[126]

Ülkenin siber ortamda bilgi kaynağını korumak ve ülkeye ait kritik altyapıların güvenliğini sağlamak üzere bazı kurumlar veya birimler kurulmuştur. Bu birimlerden, Ulusal Siber Güvenlik Merkezi (National Cyber Security Centre - NCSC) hem saldırı hem de savunma amaçlı siber yeteneklerin geliştirilmesinden sorumlu olan birimdir. Bu birimin temel görevi hükümete ait BİT sistemlerinin sürekli izlenerek sorunsuz bir şekilde çalışmasını sağlamak ve muhtemel siber saldırılara karşı savunma mekanizmaları geliştirmektir.[127]

Hükümet ofisi bünyesinde yer alan Siber ve Devlet Güvenliği Direktörlüğü (Cyber and Government Security Directorate - CGSD) hükümetin 2016-2021 Milli Siber Güvenlik Programını yönetmektedir. Bu birim temel olarak siber güvenlik eğitimi, siber tehditlere karşı farkındalık oluşturulması ve uluslararası iş birliği gibi konulara odaklı olarak çalışmalarını yürütmektedir. CGSD çalışmalarını Ulusal Siber Güvenlik Merkezi ve Savunma Bakanlığı gibi kritik birimlerle koordineli olarak yürütmektedir.[128]

İngiltere siber alanda ekonomik ve güvenlik çıkarlarını korumak üzere yaptığı güvenlik yatırımlarının yanında AB, NATO, BM ve müttefikleri ile hem ikili hem de çok taraflı iş birliği içerisindedir. Ayrıca İskoçya, Galler ve Kuzey İrlanda yönetimleri ile birlikte Birleşik Krallık sınırları içerisinde yer alan bireylerin, kurum ve kuruluşların internet ortamında güvenliklerini sağlamak için özel ve kamu sektörüyle ortak çalışmalar yürütmektedir.

İngiltere sahip olduğu tecrübeler ve endüstrinin imkânlarını kullanarak İngiltere ağlarının siber kapasitelerini güçlendirmek adına aktif siber savunma

[126] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, UK Prime Minister's Office, 2010, s.27.
[127] *Cyber Security Strategy of the United Kingdom* 2016-2021 a.g.e s.9-10.
[128] https://www.gov.uk/government/policies/cyber-security (06.01.2018)

önlemleri geliştirmekte ve bunları uygulamaya geçirmektedir. Alınan tedbirler arasında en yaygın oltalama saldırılarının minimize edilmesi, kötü niyetli IP adreslerinin filtrelenmesi ve çevrimiçi kötü etkinlikleri engelleme gibi temel önlemler yer almaktadır.

İngiltere Hükümeti himayesinde okullarda, üniversitelerde ve kamu/özel tüm iş çevrelerinde siber güvenlik bilincini oluşturmak üzere eğitim programları düzenlenmektedir. Devletin 2016-2021 Ulusal Siber Güvenlik Stratejisinde, en modern siber güvenlik ürünlerin üretimini ve yeni siber güvenlik şirketlerinin kurulmasını teşvik etmek amacıyla iki yeni siber yenilikçilik merkezinin kurulması planları yer almaktadır ve devlet bu proje kapsamında 165 milyon Sterlin Savunma ve Siber Yenilikçilik Fonu ayırmıştır. Ayrıca İngiltere Hükümeti 2016-2021 Ulusal Siber Güvenlik Stratejisi kapsamında savunma ve güvenlik alanlarında yenilikçi üretimleri teşvik etmek amacıyla ülkenin siber güvenliğini iyileştirmek için 5 yıl içerisinde toplamda 1,9 milyar Sterlin yatırım yapmayı planlamaktadır.[129]

3.2.6. İsrail

İsrail Devleti son yıllarda siber alanda güvenliği sağlamak adına ciddi gelişmeler kaydetmiştir. Hükümet tarafından 2002 yılında Ulusal Bilgi Güvenliği Otoritesi kurularak siber alandaki tehditler ve bu tehditlerle sistematik bir şekilde mücadele edilmesi gerekliliği vurgulanmıştır. Bu yıllardan itibaren siber güvenlik teknolojilerinin geliştirilmesi ve siber uzay aktivitelerinin arttırılması yönünde çalışmalar hızlandırılmıştır.[130]

İsrail'in ulusal siber savunma faaliyetlerinden dört birim sorumludur. Bunlar Unit 8200 (Birim 8200), Shin Bet, C4I Kolordusu ve Milli Sibernetik Görev Gücü (National Cybernetics Taskforce - NCT)' dür.

[129] *National Cyber Security Strategy of the United Kingdom 2016-2021*, a.g.p. s. 10.
[130] Siboni, Gabi ve Assaf, Ofer (2016) "*Guidelines for a National Cyber Strategy"*, Institute for National Security Studies, Memorandum No. 153, s. 11-15.

Unit 8200, İsrail ordusuna bağlı personeli sivil memurlar ve askeri personelden oluşan birimdir. Unit 8200, faaliyetlerini siber savaşın üç alanına odaklı olarak yürütmektedir. Bunlar; siber alanda istihbarat toplama, siber tehditlere karşı savunma ve saldırı faaliyetleridir. Ülkede sinyal istihbaratı ve şifre çözme işlemleri bu birim tarafından gerçekleştirilmektedir.

1990'lı yılların sonlarından itibaren siber ortamda hükümet sistemleri, ulusal kritik altyapılar ve finansal verilerin korunması bir iç istihbarat birimi olan Shin Bet'in sorumluluğunda olmuştur.

C4I (Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat) Kolordusu haberleşme ve siber savunma kabiliyetlerinin örgütlenmesinden sorumlu birimdir. Askeri ağları siber saldırılardan korumaktan sorumludur.

2009 yılında askeri istihbarat birimleri ve C4I arasındaki iş birliğini geliştirmek için üst düzey bir istihbarat görevlisi "Matzov" olarak bilinen Şifreleme ve Bilgi Güvenliği Merkezi'ne atanmıştır. Matzov, siber ortamda İsrail için tehdit oluşturabilecek devletlerin veya hacker grupların siber saldırı yetenekleri ve sahip oldukları teknolojik imkanlar hakkında istihbarat toplamakla görevli birimdir. Matzov ayrıca İsrail Savunma Kuvvetleri, Shin Bet ve MOSSAD ağlarını şifreleyen kodların yazılımından sorumludur. Ayrıca C4I Kolordusu bünyesinde güvenlik duvarlarını ve şifreleme sistemlerinin güvenliğini ve dayanıklılığını test eden ekipler yer almaktadır.

2011 yılında kamu ve özel sektöre ait kritik ağları hacker gruplarının saldırıları veya diğer siber casusluk faaliyetlerine karşı korumak amacıyla NCT kurulmuştur. NCT üniversitelerde siber güvenlik üzerine araştırma/geliştirme çalışmalarını ve siber güvenlik alanında öğrencilerin yetiştirilmesi faaliyetlerini desteklemektedir.[131] 2012 yılında siber ortamdaki etkinlikleri geliştirmek ve düzenlemek amacıyla İsrail Ulusal Siber Bürosu (Israel National Cyber Bureau-INCB) kurulmuştur.[132]

[131] Cybersecurity and Cyberwarfare a.g.e. s.14-15.
[132] Guidelines for a National Cyber Strategy a.g.e. s.11.

İsrail'de bulunan yüksek teknoloji üreten firmaların %20'si siber güvenlik alanında faaliyetlerini sürdürmektedirler. Başbakanlık Ulusal Siber Güvenlik Bürosu verilerine göre İsrailli firmalar 2014 yılında 6 milyar Dolar tutarında siber güvenlik çözümü ihraç etmişlerdir. İsrail'in Pazar payı toplamda 71,7 milyar Dolarlık küresel siber güvenlik pazarının %8'ini oluşturmaktadır.[133]

3.2.7. Almanya

2015 yılında kabul edilen Siber Güvenlik Yasası, siber suçların önlenebilmesi ve kritik altyapıların güvenliğinin sağlanması adına birçok önemli değişiklikler getirmiştir. Su, enerji, finans, ulaşım, telekom ve sağlık sektörlerinde faaliyet gösteren binlerce kamu ve özel sektör kuruluşları bu değişikliklerden etkilenmiştir. Bu yasa ile tüm kurum ve kuruluşlar için kritik altyapıların güvenliğini sağlamak üzere minimum bilgi güvenliği standartlarına uymak zorunlu hale gelmiştir. Aksi takdirde, söz konusu düzenleme yükümlülere 100 bin Avroya kadar cezalar öngörmektedir.

Ülkede polis güçlerinin siber suçlarla mücadele noktasında yetersiz kaldığı düşünüldüğü için, Siber Güvenlik Yasası ile polislere yeni yetkiler tanımlanmıştır. Bu yasanın verdiği yetkilerle birlikte emniyetin alt birimlerinden birisi olan Kriminal Soruşturma Bürosu en basit siber suçlardan karmaşık siber casusluk operasyonlarına kadar geniş bir alanda operasyon yapabilme yetkilerine sahip olmuştur. Yasa maddelerinden birisi telekom şirketlerine müşterilerine ait veri trafiği bilgilerini 6 ay saklama zorunluluğu getirmektedir. Çeşitli sivil toplum kuruluşlarınca eleştirilerin odağında yer alan bu maddenin özel hayatın gizliliğini ihlal ettiğine inanılmaktadır. Telekom şirketlerince saklanan verilerin istenildiği takdirde polislere verilmesi gerekmektedir. Ayrıca yasaya göre telekom şirketleri müşterilerine ait telefon ve internet hesaplarının istismar edilmesi durumunda müşterilerini uyarmakla yükümlüdürler.[134]

---

[133] http://www.itrade.gov.il/turkey/israil-siber-guvenlikte-kuresel-pazar-payinin-8ine-sahip/ (09.01.2018)

[134] Almanya'nın Yeni Siber Güvenlik Yasası Can Yakacak, https://siberbulten.com/strateji-guvenlik/2040/ (23.01.2018)

3.2.8. Fransa

Fransa'da son yıllarda gerçekleşen büyük terör saldırılarının ardından kritik altyapıların güvenliğinin sağlanması ve siber uzayda etkin bir şekilde istihbarat toplanabilmesi amacıyla ilgili birimlerin nitelikli personel sayısı arttırılmıştır. 2008 yılında yayımlanan Savunma ve Milli Güvenlik Belgesi'nde ülkede siber güvenlik faaliyetlerinin etkin bir şekilde yürütülebilmesi, birimler arasında koordinasyonun sağlanabilmesi ve siber saldırılara karşı savunma kapasitelerinin geliştirilmesi adına yeni birimlerin kurulmasına karar verilmiştir.[135]

Özellikle ülkede yaşanan terör saldırılarının ardından siber istihbarat faaliyetleri büyük önem kazanmıştır. Bu kapsamda, 2009 yılında Fransız Ağ ve Bilgi Güvenliği Teşkilatı (Agence Nationale de la Sécurite des Systémes d'Information - ANSSI) kurulmuştur. ANSSI'nın görevi devlete ait haberleşme ağlarına yapılan saldırıları tespit etmek ve bu saldırıları bertaraf etmektir. ANSSI devlete ait kritik altyapıların siber güvenlik sistemlerinin kurulması ve geliştirilmesi hususlarında da ilgili kurumlara desteklerini sunmaktadır.

ANSSI'nın yanı sıra Savunma Bakanlığı bünyesinde yer alan Dış Güvenlik Teşkilatı (Direction Générale de la Sécurite Extérieure – DGSE) ve İç Güvenlik Teşkilatı (Direction Générale de la Sécurite Intérieure – DGSI) ile siber istihbarat faaliyetleri konusunda ortak hareket etmektedir.[136]

Siber güvenlik alanında faaliyet gösteren bir diğer birim, İçişleri Bakanlığı bünyesinde adli polis birimine bağlı olarak faaliyet gösteren Bilişim Teknolojileri ile İlgili Suçlarla Mücadele Dairesi (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information de la Communication - OCLCTIC)'dir. OCLCTIC

[135] *Siber İstihbarat* a.g.k. s. 190.
[136] *Siber İstihbarat* a.g.k. s. 191.

bilişim teknolojileri altyapıları kullanılarak işlenen suçların tespit edilerek, suçlara en hızlı şekilde müdahale etmek üzere kurulmuş kolluk kuvvetidir.[137]

Fransa'nın ilk siber güvenlik stratejisi, ülkenin ekonomi ve maliye bakanlıklarına casusluk amacıyla düzenlenen bir siber saldırının ardından 2011 yılında yayımlanmıştır.[138] Siber ortamda tehditlerin artması ve ülkenin kritik altyapılarına yönelik saldırıların yoğunlaşması üzerine, ülkenin Siber Güvenlik Stratejisi daha kapsamlı hale getirilerek 2015 yılında Ulusal Dijital Güvenlik Stratejisi yayımlanmıştır. Bu strateji belgesinde devletin siber uzaydaki hedefleri 5 madde ile ifade edilmiştir.[139]

Bu maddeler:

1. Fransa'nın düşünce ve ifade özgürlüğünün yanı sıra, ülkenin kritik altyapılarının güvenliğini sağlamak,

2. Vatandaşların ve işletmelerin dijital yaşamlarını korumak ve siber suçlarla etkin bir şekilde mücadele etmek,

3. Dijital güvenlik için gerekli eğitim ve öğretim faaliyetlerini yürütmek,

4. Dijital teknolojiye güven veren bir ortamın gelişimine katkıda bulunmak,

5. Avrupa dijital stratejik özerkliğinin ortaya çıkması için Avrupa Birliği'ne üye devletler arasındaki iş birliğinin arttırılmasını teşvik etmek, bu sayede daha güvenli ve Fransa'nın değerlerine saygılı bir siber uzayın uzun vadeli garantörü olmaktır.

[137] Meral Mehmet, (2008), *Siber Savunma: Ülkeler ve Stratejiler*, 3. Uluslararası Katılımlı Bilgi Güvenliği Ve Kriptoloji Konferansı Bildiriler Kitabı s. 259.
[138] *French National Digital Security Strategy*, (2015), s. 7. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (11.05.2018)
[139] a.g.b. s. 9.

Fransa'da siber suçlar Ceza Kanunu'nun (Code Pénal) 226. ve 323. maddeleri uyarınca cezalandırılmaktadır. Ülkede siber haberleşme alanı Posta ve Elektronik Haberleşme Kanunu (Code des Postes et des Communications Electroniques) ile düzenlenmektedir.[140]

Hem NATO hem de AB üyesi olan Fransa siber güvenlik alanında uluslararası iş birliğine önem vererek NATO ve AB üyesi devletlerle müşterek siber güvenlik tatbikatlarına katılmaktadır.

3.3. ULUSLARARASI ALANDA GERÇEKLEŞEN BÜYÜK SİBER SALDIRILAR

Devletler BİT sistemlerine artan bağımlılıkla birlikte kara, deniz, hava ve uzayın ardından rekabet alanlarını siber uzaya taşımışlardır. Günümüzde devletler arasındaki savaşlar soyut bir ortam olan siber uzayda gerçekleşmektedir. Ülkeler arasındaki çıkar çatışmaları, siber saldırılar sonucunda güçlü devletin zayıf olanı saf dışı bırakmasıyla sonuçlanmaktadır.

Bu başlık altında dünyanın çeşitli ülkelerine yönelik gerçekleştirilen ve saldırıya maruz kalan ülkelerin altyapılarına ciddi zararlar veren büyük siber saldırılar sebepleriyle ve sonuçlarıyla ele alınmaktadır.

3.3.1. Stuxnet

Stuxnet ilk tespit edildiğinde bunun, basit bir virüs çeşidi ya da solucan değil; yetenekleriyle çığır açan bir zararlı yazılım olduğu anlaşılmıştır. Bu zararlı yazılım amaçladığı hedef bakımından daha önceden bilinen virüsler veya zararlı yazılımlardan çok farklı olmuştur. Stuxnet'ten önceki virüsler, çoğunlukla insanları taciz etmek veya

[140] *Siber Savunma: Ülkeler ve Stratejiler,* a.g.k. s. 259.

banka kartı bilgilerini ele geçirmek amacıyla kullanılmıştır. Ancak bir virüsün binalara zarar verebileceği, dev makineleri çalışamaz hale getirebileceği ya da insanları öldürebileceği hususları ilk kez Stuxnet ile ortaya çıkmıştır.

İran'ın Natanz ve Buşehr nükleer santrallerinin reaktörlerine ve reaktörlere bağlı makinelere zarar veren Stuxnet, İran'ın nükleer programını sabote etmek için geliştirilmiştir. Windows işletim sisteminde yer alan dört tane sıfır gün açığından[141] faydalanarak yayılan virüs Siemens'in S7 300 SCADA (Supervisory Control and Data Acqusition) sisteminin parçalarını hedef almıştır.

Kapsamlı ve entegre bir veri tabanlı kontrol ve izleme sistemi olan SCADA sistemleri, sanayi sektöründe makinelerin davranışlarını kontrol eden PLC (Programmable Logic Controller) adı verilen unsurları denetlemektedirler. Nükleer santralde de kullanılan bu sistemler Stuxnet'in hedefinde yer almışlardır. Nükleer reaktörleri kontrol eden PLC'leri ele geçirerek reaktörlerin basıncını arttırabilme, enerji boru hatlarındaki akışı durdurabilme yeteneğine sahip olan bu virüs; sistemi kontrol eden operatörlere de sistemin sorunsuz bir şekilde faaliyetlerine devam ettiği bilgisini vererek problemlerin son ana kadar fark edilebilmesine engel olmuştur.

Stuxnet sistemlere sızmak için sahte bir güvenlik sertifikası kullanmamıştır. Antivirüs programlarını yanıltıcı birçok özelliğe sahip bu kapsamlı virüs, dünyanın en güvenilir firmalarından birisi olan Realtek firmasının güvenlik sertifikalarını kullanarak sistemleri yanıltmayı başarmıştır. Bu dikkat çekici özelliklerinden dolayı Stuxnet, o güne kadar keşfedilen en zararlı ve en karmaşık virüs olmuştur.[142]

Konunun uzmanları tarafından incelenen virüs yazılımının karmaşık yapısı, virüsün farklı alanlardan uzman kişilerce uzun zamanlar ve büyük bütçeler harcanarak geliştirildiğini ortaya koymuştur. Bir USB (Universal Serial Bus) bellek aracılığıyla

[141] **Sıfır gün açığı**: Bir sistem üzerinde ilk kez saldırgan tarafından keşfedilip, henüz açığa çıkmamış güvenlik açıklarıdır.
[142] http://www.tuicakademi.org/stuxnet-virusu-iran-a-nasil-etki-etti/ (09.02.2018)

İran'ın yüksek güvenlikli Natanz nükleer tesisine sızmayı başaran virüs, öncelikle ağ içerisinde Siemens S7 300 yazılımını taramıştır. Tarama sonucu bulduğu Siemens S7 300 yazılımının kodlarını değiştirerek PLC'lere beklenmedik komutlar vermeye başlamıştır. Böylelikle çok sayıda santrifüjün[143] arızalanmasına sebep olmuştur. Santrifüjlerin çalışmasını denetleyen PLC'ler devre dışı bırakılmış; ardından kontrolden çıkarak hızla dönen makineler parçalanmıştır.

Santrifüjlerin onarılarak yeniden devreye alınması uzun zaman almıştır. Bu saldırının İran'ın nükleer faaliyetlerini en az 2 yıl geriye götürdüğü ve ülkeyi milyonlarca Dolar zarara uğrattığı düşünülmektedir.[144]

Saldırı sonrası İran başlarda gizlice yürüttüğü, sonraları da açıktan yürüttüğü nükleer programını zorunlu olarak durdurmuştur. Çünkü ilk olarak görevli Rus uzmanın bilgisayarına bulaşan virüs, kısa sürede ülkenin nükleer programı çalışmalarının yürütüldüğü 30 bin bilgisayara da sızmayı başarmıştır. Bunun sonucunda devlet gizli bilgilerin ifşa edildiği gerekçesiyle tüm nükleer faaliyetlerini askıya almıştır.

Stuxnet, İsrail istihbarat teşkilatı MOSSAD ile bağlantılı Debka adlı haber sitesinin iddiasına göre Amerikan istihbarat teşkilatı CIA ve İsrail istihbarat teşkilatı MOSSAD'ın İran'ın nükleer programını sabote etmek üzere ortaklaşa geliştirmiş oldukları bir siber silah olduğu belirtilmiştir. Çünkü iki ülkenin gizli servislerinin siber savaş birimleri tarafından geliştirildiği düşünülen virüsün büyük oranda İran'ın nükleer programını hedef almış olması bu ihtimali güçlendirmektedir.[145]

---

[143] Uranyum elementinin nükleer reaktörlerde kullanılabilmesi için zenginleştirilmesi gerekmektedir. Santrifüj cihazları ile zenginleştirilen Uranyum elementi nükleer reaktörlerde kullanılabilecek hale gelmektedir.

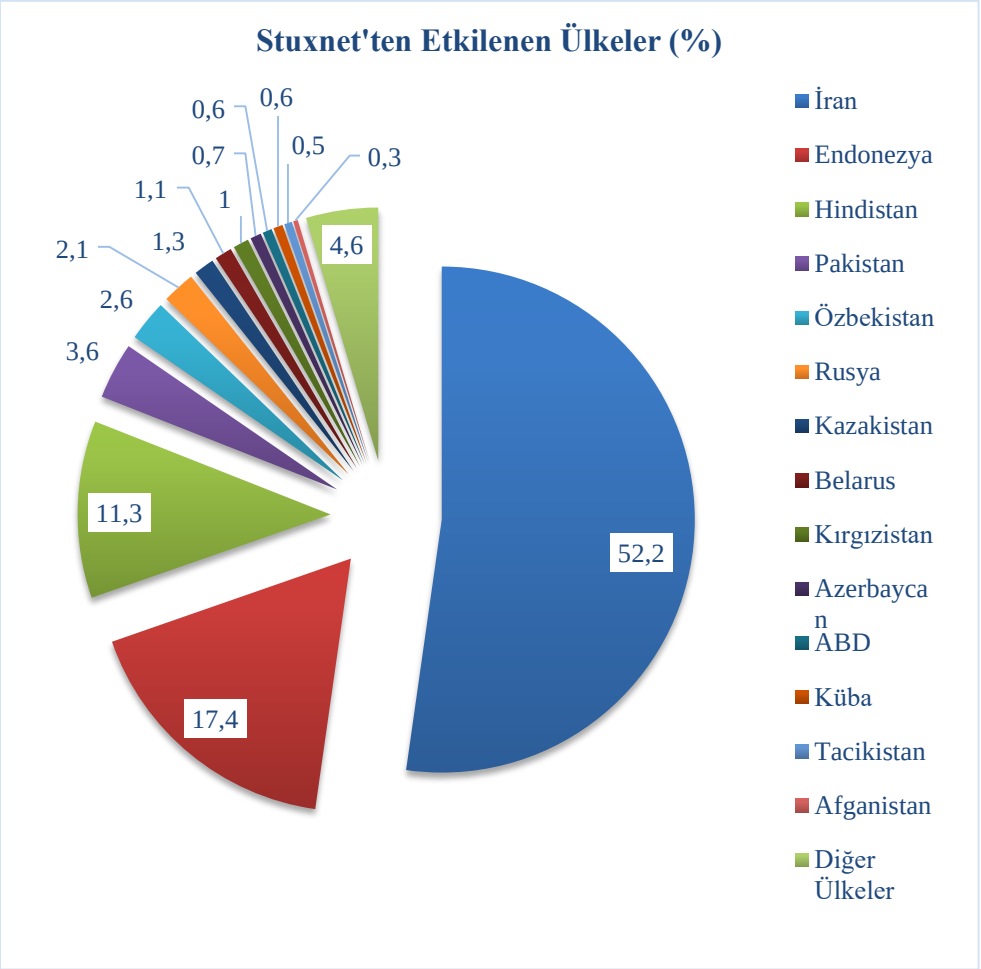
[144] Kara Mahruze, (2013), *Siber Saldırılar- Siber Savaşlar ve Etkileri*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, s. 43-44.

[145] *MOSSAD-CIA virüsü İran'ı Vurdu*, 2010, Vatan Dış Haberler http://www.gazetevatan.com/mossad-cia-virusu-iran-i-vurdu-331204-dunya/ (10.02.2018)

ABD'li New York Times Gazetesi haberinde, İsrail'in Stuxnet'i kendi sınırları içerisinde yer alan Negev Çölü'ndeki Dimona Nükleer tesisinde test ettiğini belirtmiştir. Ayrıca istihbarat kaynaklarına dayandırılan haberde İsrail ve Amerika'nın ortaklaşa yürüttüğü çalışmalara Almanya ve İngiltere'nin de isteyerek ya da istemeyerek destek sağladığı ifade edilmiştir.[146]

Dünya genelinde 130.000 bilgisayarın Stuxnet virüsünden etkilendiği düşünülmektedir.[147] 2010 yılının haziran ayında ortaya çıkan virüs büyük oranda İran'ı etkilemiştir. Ancak, dünya genelinde çok hızlı bir şekilde yayılarak başta Asya ülkeleri olmak üzere birçok ülkeyi olumsuz etkilemiştir. 2010 yılında eylül ayı itibariyle dünya genelinde virüs bulaşmış bilgisayarların ülkelere göre istatistiki dağılımı Şekil 3.3'de yer almaktadır.

[146] *İran'ı Vuran Virüs İsrail'de Üretilmiş,* 2011, Haberturk, http://www.haberturk.com/haber/haber/592070-irani-vuran-virus-israilde-uretilmis - (10.02.2018)
[147] Siber İstihbarat a.g.e. s. 150.



Şekil 3.3 Stuxnet'ten Etkilenen Ülkelerin Küresel Dağılımı (İlk 14 Ülke)

Grafikten de anlaşılacağı üzere Asya ülkeleri Stuxnet'ten etkilenen bilgisayarların sayısı bakımından ilk sırada yer almaktadır. İran, Stuxnet'in en geniş yayılım gösterdiği ülkeler arasında ilk sırada yer almaktadır.[148]

3.3.2. Duqu

Stuxnet virüsünden bir yıl sonra ortaya çıkan virüstür. Eylül 2011'de Budapeşte Teknoloji ve Ekonomi Üniversitesi'nde Kriptografi ve Sistem Güvenliği

[148] *Stuxnet Under The Microscope Revision 1.1*, ESET, 2010, s. 15-16. https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf - (10.02.2018)

Laboratuvarlarında yapılan çalışmalar sonucunda keşfedilmiştir. Bulaştığı bilgisayarlarda "DQ" adlı dosyalar ürettiği için bu adı almıştır.[149] Bu virüsün endüstriyel sistemler hakkında istihbarat toplamak amacıyla Stuxnet'ten önce oluşturulduğu düşünülmektedir.

Duqu'nun Stuxnet ile büyük benzerlikler taşıyor olması dikkat çekicidir. İki virüs arasındaki benzerlikler, ikisinin de aynı yazılımcılar tarafından üretildiği ya da Duqu'yu üreten yazılımcıların Stuxnet'ten esinlendikleri ihtimallerini güçlendirmektedir. İki virüsün en önemli ortak özelliği, SCADA adı verilen endüstriyel kontrol ve izleme sistemlerini hedef almış olmalarıdır. Hem Stuxnet hem de Duqu sistemlere sızmak için güvenilir firmaların güvenlik sertifikalarını kullanmışlardır. Ayrıca sıfırıncı gün açıklarını kullanarak ağ içerisinde yayılmışlardır. Yine iki virüs yoğun olarak İran'da görülmüştür.

Duqu'yu, Stuxnet'ten ayıran bazı özellikler de vardır. Stuxnet sızdığı SCADA sitemini yanıltmak suretiyle sisteme zarar vermeyi amaçlamaktadır. Duqu ise sızdığı SCADA sitemi ile ilgili kritik verileri toplamak amacıyla tasarlanmıştır. Bu virüs sisteme hiç zarar vermeden sistemi izleme görevini yürütmektedir. Duqu, daha sonra gerçekleştirilmesi planlanan muhtemel saldırılar için sistemin zafiyetlerini tespit ederek bunları yazılımcısına raporlama görevini yürütmektedir. Ayrıca virüs sızdığı sistemden 36 gün sonra kendini silmektedir. Böylelikle sisteme zarar verilmeden, izinsiz bir şekilde sistemin zayıf ve güçlü yönleri tespit edilebilmektedir.[150]

3.3.3. Flame

Mayıs 2012'de keşfedilen, Stuxnet'ten 20 kat daha güçlü olan virüstür. Rus güvenlik firması Kaspersky tarafından keşfedilmiştir. Siber savaşın önemli

[149] Meral Mustafa, "*Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi"*, Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul, 2015, s. 76. (https://tez.yok.gov.tr - Tez No: 398413 – 17.10.2018)
[150] *Siber Saldırılar- Siber Savaşlar ve Etkileri* a.g.e s.34-35.

silahlarından biri olan Flame virüsünün Stuxnet ile bağlantıları olduğu düşünülmektedir. Flame'in en önemli özelliği kendisini sürekli güncellemesi ve antivirüs programlarına takılmamasıdır. Bir zararlı yazılıma göre boyutunun oldukça büyük olması (20 MB) daha önce keşfedilen Stuxnet ve Duqu virüslerinden daha üstün ve farklı bir yapısının bulunduğunu göstermektedir.[151]

İran Bilgisayar Acil Müdahale Ekibi (Iran Computer Emergency Response Team - IRCERT) yaptığı bir duyuruda, Flame virüsünün bulaştığı bilgisayarlarda tüm sesli aramaları, ekran görüntülerini ve klavye hareketlerini kaydedebildiğini, Arapça ve İbranice metinleri analiz edebildiği belirtmiştir. Virüs, sızdığı bilgisayarların Bluetooth özelliklerini açarak yeni cihazlarla bağlantı kurmayı denemektedir. Bağlanmayı başardığı bilgisayarlardan ve mobil cihazlardan veri toplayabilen virüs Orta Doğu'da birçok ülkede tespit edilmiştir. Bu ülkeler arasında yine ilk sırada İran yer almaktadır. İran'da yer alan birçok petrol ve doğalgaz şirketi bu virüsten olumsuz etkilenmişlerdir.[152]

Budapeşte üniversitesi bünyesinde yer alan ve bilgisayar virüslerini inceleyen Crysys Laboratuvarı raporunda, virüs üzerinde yapılan teknik analizler sonucunda virüsün çok yüksek bir bütçe ve teknik altyapıya sahip bir devlet kurumu tarafından alanında uzman kişilerce üretildiğini belirtmiştir. Virüsün sızdığı sitemlerden elde ettiği verileri sistematik bir şekilde işliyor olması ve verileri sızdırabilmek için sistemin Wi-Fi, mikrofon, USB sürücüler, klavye, mikrofon, monitör, depolama cihazlarını kullanabiliyor olması virüsü o güne kadar keşfedilen tüm virüslerden farklı kılmaktadır.[153]

[151] Siber İstihbarat a.g.e. s. 150.
[152] *Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi* a.g.e. s.76.
[153]Ortadoğu'yu Alarma Geçiren Virüs: Flame, 2012, NTV, https://www.ntv.com.tr/turkiye/ortadoguyu-alarma-geciren-virus-flame,8X_pXRhHnkCbotEqgKFsLw (10.02.2018)

3.3.4. Gauss

Stuxnet, Duqu ve Flame adlı virüsler gibi hedefinde Ortadoğu olan bir virüstür. Yalnız bu üç virüsten farklı olarak İran'ın nükleer programı ve enerji altyapısını hedeflememiştir. Bu virüs, Lüban'daki bankalar ağırlıklı olmak üzere bölgedeki bankaların müşterilerinin kimlik bilgileri ve hesaplarındaki paraları çalmayı hedeflemiştir. Lübnan'da 1660, İsrail'de 483 ve Filistin'de 261 banka hesabı ele geçirilmiştir.

Kaspersky şirketi yaptığı açıklamada, Gauss yazılımının daha önce ortaya çıkarılan Stuxnet, Duqu ve Flame virüsleriyle benzerlik taşıdığını ifade etmiştir.[154]

3.3.5. Estonya Siber Saldırıları

ABD'de 11 Eylül 2001 tarihinde gerçekleşen terör saldırılarından sonra milli güvenlik kavramı devletlerin gündem maddeleri arasında ilk sıraya yerleşmiştir. Bu terör saldırıları sonucunda uluslararası alanda milli güvenlik ve tehdit kavramları yeniden tanımlanmaya başlamıştır.

Saldırıların ardından en çok tartışılan konular arasında NATO üyesi ülkelerden birisine karşı gerçekleşebilecek muhtemel "Dijital Felaket" senaryosu olmuştur. NATO üyesi herhangi bir devlete karşı gerçekleşebilecek siber saldırı milli güvenlikle ilişkilendirilmiş ve birçok NATO üyesi devlet kendi siber güvenlik stratejilerini belirlemişlerdir. Ulusal güvenlik belgelerine eklenen siber güvenlik stratejileri sürekli güncellenerek kapsamlı hale getirilmeye devam etmiştir.

NATO üyesi devletlere karşı gerçekleşen siber saldırı örneklerinden en dikkat çekici olanı 2007 yılında Baltık ülkesi Estonya'ya karşı gerçekleştirilen siber

[154] 'Hırsız' Virüs Alarmı, 2012, Hürriyet, http://www.hurriyet.com.tr/hirsiz-virus-alarmi-21197087 - (10.02.2018)

saldırılardır. Söz konusu saldırılar Estonya Hükümeti'nin İkinci Dünya Savaşından sonra başkent Tallinn meydanına dikilen Bronz Asker Anıtı'nı kaldırma kararı sonrası başlamıştır. Estonya'ya yönelik olarak gerçekleştirilen siber saldırıların ayrıntılarından bahsetmeden önce ülkenin siyasi geçmişinden bahsetmekte fayda vardır. Zira söz konusu siber saldırıların ülkenin siyasi geçmişiyle yakından ilgili olduğu düşünülmektedir.

Estonya 1991 yılında SSCB (Sovyet Sosyalist Cumhuriyetler Birliği)'nin dağılması sonucu bağımsızlığını ilan eden bir Baltık ülkesidir. Ülkenin bağımsızlığını ilan ettiği yıllarda halkın yarısının en basitinden telefon erişimleri bile yoktu. Bu yıllardan itibaren Estonya Hükümeti devletin içinde bulunduğu teknik yetersizlikleri göz önünde bulundurarak BİT sistemleri ve telekomünikasyon alanlarında yeni yatırımlar yapmıştır. Devlet yaptığı yatırımlar ve AR-GE teşvikleriyle teknik altyapısını güçlendirerek birçok yeniliğe imza atmıştır. Örneğin; dünyada seçmenlere ilk kez elektronik oy kullanabilme imkânı 2005 yılı seçimlerinde Estonya'da sunulmuştur. Bu yıllarda halkın en az %60'lık kesimi günlük iş ve işlemlerini gerçekleştirmek üzere internet kullanmak zorundaydılar. 2005 yılında bile bankacılık işlemlerinin %96'sı internet bankacılığı üzerinden gerçekleştirilmekteydi. Bu özelliklerinden dolayı "Avrupa'nın en dijital ülkesi" olmakla ün yapan devletin dijital altyapısı savunma yönünden zayıf kalmaktaydı. [155]

Estonya Parlamentosu tarafından baskıcı Sovyet dönemini simgelediği gerekçesiyle Bronz Asker Anıtı'nın 27 Nisan 2007'de kaldırılması, ülkede bulunan Rus azınlığının ayaklanmasına sebep olmuştur. Ülke nüfusunun yaklaşık %25'ini oluşturan Rus azınlıkların protesto gösterileri sırasında 1 kişi ölmüş, 100 kişi yaralanmış, 1.300 kişi de tutuklanmıştır. Rus Hükümeti anıtın kaldırılmasının Estonya'yı Nazi işgalinden kurtarırken ölen Sovyet askerlerine saygısızlık olarak nitelemiş ve olayı kınamıştır.

[155] Yazıcı, Merve (2015). "İlk Modern Siber-Atak: Estonya", (http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ (11.02.2018)

Anıtın kaldırılmasının ertesi gününde ülkeye yönelik yoğun siber saldırılar düzenlenmeye başlamıştır. Saldırılar sonucu Estonya Cumhurbaşkanlığı, parlamento, siyasi partiler, bakanlıklar, bankalar ve diğer birçok kurum veya işletmenin internet siteleri hedef alınmıştır. Saldırıların ardından aşırı yüklenmelere dayanamayarak kullanıcılara cevap veremeyen sitelerin çökmesi sonucu ülkenin dış dünya ile bağlantısı kesilme noktasına gelmiştir. Ülkede birçok hizmete günlerce erişim sağlanamamıştır. Saldırıların ülkeye vermiş olduğu zarar tam olarak belirlenememiştir.

Estonya Savunma Bakanlığı'ndan yapılan açıklamalara göre, saldırıların birçok ülkeden yönetildiğini ancak bazı saldırılarda Rus devletine ait izlere rastlandığı açıkça belirtilmiştir. Saldırılarla başa çıkamayan ülke, saldırıları milli güvenliğine yönelik bir saldırı olarak nitelemiş ve NATO ile AB'den yardım istemiştir. Olayların ardından açıklama yapan Kremlin sözcüsü Dimitri Peskov, Estonya'nın Rusya'ya yönelik iddialarını gerçek dışı olarak niteleyerek olaylardan Rusya'nın sorumlu tutulamayacağını belirtmiştir.[156]

Estonya örneği uluslararası alanda siber saldırıların hangi durumlarda savaş sebebi sayılabileceği, devletlerin siber saldırıları nasıl algılamaları gerektiği konularının tartışılmaya başlamasına neden olmuştur. Bu olaydan sonra birçok devlet siber savunma stratejilerini yeni muhtemel tehditlere göre güncellemişlerdir. Bu sonuçlarından dolayı Estonya siber saldırıları ülkeler ve iş birliği örgütleri için bir dönüm noktası niteliğindedir.

3.3.6. WannaCry Fidye Yazılımı

Mayıs 2017'de ortaya çıkan son yılların en zararlı fidye yazılımı olan Wannacry adlı virüs, dünya genelinde aralarında Türkiye'nin de bulunduğu 150 ülkede

[156] "Estonya'ya siber saldırı" (http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml (12.02.2018)

200 binden fazla bilgisayarı olumsuz etkilemiştir. Virüs bilgisayarlardaki verileri şifreleyerek kurbanlardan şifrelerin kırılması karşılığında ortalama 300$ fidye istemiştir. Bu rakam önceki yıllarda meydana gelen benzer saldırılarda talep edilen fidye miktarlarına kıyasla daha düşük bir rakam olmuştur.[157]

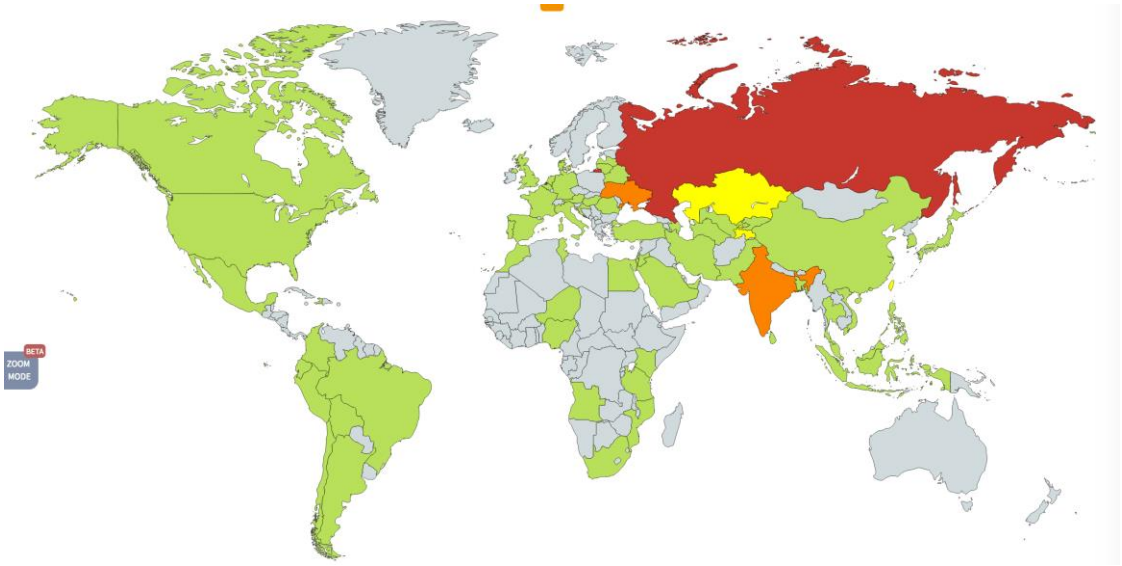
Basında çıkan haberlere göre kötü niyetli yazılım ilk olarak Rusya'da görülmüş, ancak daha önce benzeri görülmemiş bir şekilde çok hızlı bir şekilde tüm dünyada yayılmıştır. Saldırganlar eski bir sürüm olmasına rağmen, dünyada hala milyonlarca kullanıcısı olan Windows XP işletim sistemlerindeki bilindik bir açıktan faydalanarak sistemlere sızmayı başarmışlardır. Microsoft 2014 yılında Windows XP sürümlerine sağladığı güvenlik desteğini durdurmuş olmasına rağmen, Wannacry saldırılarından etkilenen Windows XP kullanıcıları için bir acil güvenlik destek paketi yayınlamıştır.[158]

WannaCry virüsünün ABD'nin istihbarat servisi NSA tarafından geliştirilen bir virüsten türetildiği tahmin edilmektedir. NSA tarafından geliştirilen virüsün ortaya çıktığı dönemde, birçok güvenlik uzmanı bu virüs aracılığıyla yeni fidye yazılımlarının ortaya çıkabileceğini öngörmüşler fakat bunun önüne geçilememiştir.

Virüsten Türkiye'de bulunan bilgisayarların da olumsuz etkilenmesi üzerine Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı Ömer Fatih SAYAN Twitter hesabı üzerinden aşağıdaki uyarı mesajını paylaşmıştır:

> "*Ülkemizin Siber Güvenlik Merkezi USOM ön alma operasyonlarına devam etmektedir. Dünyada yayılan Wcry zararlısından korunmak için Windows sistemleri ve antivirüsleri güncelleyin! Sistemlerinizi taratmayı ihmal etmeyin.*" (SAYAN, 2017)

[157] Güvenlik yazılımları şirketi Symantec verilerine göre 2016 yılında bilinen tüm saldırılarda istenen ortalama fidye miktarı 1.007$ olmuştur.
[158] Richter, Felix (2017) "*200,000+ Systems Affected by WannaCry Ransomware Attack*" (https://www.statista.com/chart/9399/wannacry-cyber-attack-in-numbers/ , 13.02.2018 tarihinde erişildi.)



Şekil 3.4 WannaCry Saldırılarından Etkilenen Ülkelerin Dağılımı[159]

Şekil 3.4'de Kaspersky Lab tarafından açıklanan ve dünya genelinde WannaCry virüsünden etkilenen ülkelere ait haritada, saldırıdan en fazla etkilenen ülkeler kırmızı renge boyalı ülkeler olmuştur. Ardından sırasıyla turuncu ve sarı boyalı ülkeler gelmektedir. Diğer ülkelerle kıyaslandığında daha az etkilenen ülkeler ise yeşil renge boyalı ülkeler olmuştur.

Saldırılardan en çok zarar gören ülkelerden birisinin Rusya olduğu belirtilmiştir. Ülkede içişleri bakanlığı, sağlık bakanlığı, devlet demiryolları şirketi, GSM operatörü MegaFon ve bazı bankaların etkilendiği bildirilmiştir.

İspanya'da aralarında enerji şirketi Iberdrola, devlet şirketi Gas Natural ve Telekom şirketi Telefonica'nın da bulunduğu birçok kuruluş virüsten etkilenmiştir.

İngiltere ve İskoçya'da Ulusal Sağlık Sisteminin çökmesi sonucu birçok sağlık kuruluşu hizmet veremez hale gelmiş, ameliyatlar yapılamamış ve acil vakalar dışında sağlık hizmetleri aksamıştır.

[159] Kaspersky Lab Küresel Araştırma & Analiz Ekibi, (2017) (https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (13.02.2018)

Fransa'da otomotiv şirketi Renault, Portekiz'in geneline telekom hizmeti sunan Telecom, ABD'li taşıma şirketi FedEx de virüsten etkilenen şirketlerden bazılarıdır.

Yalnızca Windows işletim sistemlerine bulaşan bu virüsten korunmak için, antivirüs ve işletim sistemleri sürekli güncel tutulmalıdır. Ayrıca gelen şüpheli e-postalar açılmamalı veya e-postalarda gönderilen şüpheli linklere tıklanmamalıdır. Çünkü virüsün en yaygın bulaşma yöntemi oltalama saldırılarıdır.[160]

3.3.7. Sony Pictures Şirketine Yönelik Saldırılar

24 Kasım 2014 tarihinde kendilerini Guardians of Peace (GOP) olarak tanıtan bir hacker grubu Sony Pictures adlı film şirketinin sistemine sızmışlardır. Saldırı sonucu şirket ile ilgili birçok önemli veriyi internetten yayınlamışlardır. Veriler arasında Sony Pictures şirketinin çalışanları ile aileleri hakkındaki kişisel veriler, çalışanların e-postaları, maaşları ve sigorta bilgileri ile gösterime girmemiş dört tane film yer almaktadır. Saldırganlar verileri ele geçirdikten sonra Sony şirketinin bilgisayar altyapısını silmek üzere programlanmış Shamoon adlı zararlı yazılımı çalıştırarak sisteme ciddi zararlar vermişlerdir.

GOP adlı hacker grubu Sony'den Kuzey Kore lideri Kim Jong Un'a suikast düzenlenmesini konu alan "The Interview" adlı komedi filminin yayınlanmamasını talep etmiş, eğer yayınlanması durumunda sinema salonlarına terör saldırıları düzenleneceği tehdidinde bulunmuştur. Tehditler üzerine Sony, filmi gösterime sokmaktan vazgeçerek filmin sınırlı bir kısmını daha sonra dijital ortamdan yayınlamıştır. Saldırıların ardından Amerikan istihbarat teşkilatı FBI yetkilileri yaptıkları incelemeler sonucunda, saldırıda kullanılan yazılımların ve teknik altyapıların Kuzey Kore tarafından finanse edildiğini açıklamışlardır. Ancak Kuzey Kore bu iddiaları reddetmiştir. [161]

[160] 5 soruda Türkiye'yi de etkileyen fidye yazılımı 'WannaCry' (2017), (http://www.bbc.com/turkce/haberler-39906717 (13.02.2018)
[161] (https://en.wikipedia.org/wiki/Sony_Pictures_hack (14.02.2018)

Saldırganlar Sony'nin taleplerini yerini getirmemesi durumunda birçok önemli veriyi daha yayınlayacaklarını ve ele geçirdikleri verilerin toplam boyutunun 11 Terabayt büyüklüğünde olduğunu açıklamışlardır.[162]

[162] http://www.hurriyet.com.tr/teknoloji/sony-hacklendi-vizyona-girmeyen-filmler-torrente-dustu-27691925 (14.05.2018)

DÖRDÜNCÜ BÖLÜM

TÜRKİYE'DE BİLGİ TOPLUMUNA DÖNÜŞÜM SÜRECİ VE SİBER GÜVENLİK ALANINDA YAPILAN ÇALIŞMALAR

Tüm dünyada 1990'lı yılların özellikle ortalarından itibaren bilgi toplumuna dönüşüm adımları atılmaya başlanmıştır. Bu yıllarda Türkiye'de de bilgi toplumuna dönüşüm konusunda uluslararası koordinasyona yönelik çalışmalar ile uluslararası araştırmalar yapılarak; konu hakkında çeşitli raporlar, projeler ve eylem planları hazırlanmıştır. Ayrıca yapılan tüm bu faaliyetlerin başarıya ulaşabilmesi için mevzuat altyapısının güçlendirilmesine yönelik çalışmalar da yapılmıştır.

Türkiye'de bilgi toplumuna dönüşüm sürecinde kamuda ve özel sektörde sunulan birçok hizmet, toplumda internet kullanımının da yaygınlaşmasıyla birlikte elektronik ortama aktarılmıştır. Sunulan hizmetlerin maliyetleri düşmüş, kısa zamanda daha fazla kişiye hizmet sunulabilmiş; ancak siber uzayda artan tehditlere bağlı olarak ülkenin ihtiyaçlarına göre bilgi güvenliği politikası ve siber güvenlik stratejilerinin hazırlanıp uygulanması zorunlu hale gelmiştir.

Bu bölümde Türkiye'nin bilgi toplumuna dönüşüm süreci kronolojik sıraya göre ele alınmaktadır. Ayrıca bilgi güvenliği ve siber güvenlik alanında kurulan kurumlar, mevzuat altyapısı ve Ulusal Siber Güvenlik Stratejilerinden ayrıntılı bir şekilde bahsedilmektedir.

4.1. BİLGİ TOPLUMUNA DÖNÜŞÜM SÜRECİ

İlk olarak 1993 yılında Dünya Bankası ve Türkiye'nin iş birliğinde Bilişim ve Ekonomik Modernizasyon Raporunun (1993) hazırlanmasıyla başlayan süreç TUENA Planı (1999), e-Türkiye Projesi (1998), e-Dönüşüm Türkiye Projesi (2003) ve Bilgi Toplumu Stratejisi Eylem Planları ile devam etmiştir.

2002 yılına kadar ortaya konan çalışmalar genel itibariyle birbirinden bağımsız, ülkemizin öncelikli ihtiyaçları gözetilmeden, yalnızca kurumsal öncelik ve ihtiyaçlar ön planda tutularak hazırlanmıştır. Ayrıca ülkenin içinde bulunduğu siyasi ve ekonomik istikrarsızlıklardan dolayı uygulama imkânı bulamayan çalışmalardan hedeflenen sonuçlar alınamamıştır.

4.1.1. Bilişim ve Ekonomik Modernizasyon Raporu

1993 yılında Türkiye ve Dünya Bankası iş birliğinde "Bilişim ve Ekonomik Modernizasyon Raporu" hazırlanarak yayımlanmıştır. Raporda Türkiye'nin bilgi toplumuna dönüşüm sürecine yönelik bilgisayar kullanımı, yazılım pazarı, bilgi ekonomisinde insan kaynağı, iletişim ağları ve yasal altyapıların hazırlanması gibi alanlarda tespitlere yer verilerek bir eylem planı hazırlanmıştır. Ancak Türkiye ile Dünya Bankası arasında kredi konusunda mutabakat sağlanamamış ve raporda yer alan öneriler hayata geçirilememiştir.[163]

4.1.2. Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA)

1995 yılında Türkiye Bilimler Akademisi (TÜBA), TÜBİTAK ve Türkiye Teknoloji Geliştirme Vakfı (TTGV) tarafından oluşturulan Bilim-Teknoloji-Sanayi Politikaları Platformu Enformatik Çalışma Grubu tarafından bir rapor hazırlanmıştır.

[163] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (19.04.2018)

Raporda dünyada enformatik sektörünün kazandığı stratejik önem ile Türkiye'nin bilgi sistemleri altyapısının karşı karşıya kaldığı tehditlere dikkat çekilerek, konu hakkında ulusal bir ana planın hazırlanmasının önemi vurgulanmıştır. Söz konusu rapor yaklaşık 2000 kişi ve kuruluşa gönderilmiştir. Raporda uluslararası alanda enformatik sektörünün kazandığı öneme dikkat çekilerek, ulusal bilgi sistemleri altyapısının oluşturulması hususuna bir ana plan çerçevesinde yaklaşım sergilenmesi gerektiği vurgulanmıştır.

Milli Güvenlik Kurulu (MGK) Genel Sekreterliği konunun önemine istinaden 23 Ocak 1996 tarihinde çeşitli kamu kuruluşlarının temsilcilerini toplantıya çağırmıştır. Toplantının ardından konunun Master Plan çerçevesinde ele alınması gerekliliği vurgulanarak şu görüşlere yer verilmiştir;

- Yeni teknolojik gelişmelerin beraberinde getireceği yasal yükümlülüklerden kurtulmanın, bu teknolojilerin ülkeye girmesini ve yaygınlaşmasını engelleyerek olmayacağı,

- Dünya ekonomisinin şekillenmesinde en kritik rolü üstlenen teknolojinin, benzer şekilde yasaların ve uluslararası hukukun şekillenmesinde de önemli bir role sahip olduğu,

- Bilgi teknolojileri alanında söz sahibi olan devletlerin, geleceğin bilgi toplumu ekonomisinin yanında hukuki alanda da söz sahibi olacakları,

- Teknolojinin gelişmesine bağlı olarak yapılacak olan düzenlemelerde ulusal çıkarların gözetilmesi gerekliliği,

- İnternetin ulusal bilgi sistemleri altyapısının başlangıcı olarak kabul edilmesi ve bu alanda daha sonra geliştirilecek benzer ek altyapıların inşasının da bir Master Plan dâhilinde ele alınması gerekliliği ifade edilmiştir.[164]

[164] *Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) Sonuç Raporu*, (1999), Ulaştırma Bakanlığı, s. 3.

1999 yılında Ulaştırma Bakanlığı ile TÜBİTAK'ın birlikte yürüttüğü çalışmalar sonucunda TUENA hazırlanmıştır.

Tablo 2 TUENA Çalışmalarına Dair Rakamlar

TÜRKİYE ULUSAL ENFORMASYON ALTYAPISI (TUENA) ANAPLAN ÇALIŞMALARININ ENVANTERİ	Sayı
Hazırlanan Raporların Toplam Sayfa Sayısı	3397
Alt İş Paketi Raporları Sayısı	10
Uzman ve Akademisyenlerin Yazdığı Çalışma Belgesi Raporları Sayısı	42
Proje Ofisi ve Tam Zamanlı Çalışan Sayısı	14
Ulaştırma Bakanlığının Proje Yürütme Grubu Üye Sayısı	9
TÜBİTAK Proje Yönlendirme Kurulu Üye Sayısı	14
Bilgi Toplumu 2010 Toplantısı Katılımcı Sayısı (4-5 Temmuz 1998-Antalya)	88
Bilgi Toplumu 2010-Ulusal Katkı Payı ve Araçlar Toplantısı (21-22 Kasım 1998-Antalya) Katılımcı Sayısı	94
Oluşturulan Çalışma Grupları	14
Türkiye'yi Temsil Eden (Toplam nüfusun %65'ini oluşturan kent nüfusu) Hanehalkı Saha Anketi	1
Mülakatlar yoluyla görüşü alınan özel ve kamu kurumlarının sayısı	200
Çalışılan Uzman Sayısı	42

Tablo 2'den de görüleceği üzere 3397 sayfadan oluşan sonuç raporu 79 kişilik uzman kadronun, 14 ayrı çalışma grubunda, 200 kamu-özel sektör görüşü ve bir hane halkı anket sonucu derlenerek ortaya çıkmıştır.[165] TUENA Sonuç Raporunda Türkiye'nin bilgi politikalarının belirlenmesi amacıyla bilgi teknolojileri altyapı kullanımı, bu alanda yapılan düzenlemeler ve eğilimler bağlamında uluslararası alandaki genel eğilimler, Türkiye'deki konu ile ilgili mevcut durum, geleceğe yönelik vizyon ve hedefler ile kurumsal yapılanma önerileri ortaya koyulmuştur.[166]

Birçok kamu kurum ve kuruluşunun katkılarıyla hazırlanan TUENA, ülkemizde bilgi toplumuna dönüşüm konusunda ilk defa kapsamlı bir bakış açısı ortaya konmuştur. Ayrıca ulusal bilgi güvenliğinin sağlanması için bilgi güvenliği duvarının oluşturulması gerekliliğine ilk kez bu raporda yer verilmiştir.[167]

[165] *Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) Sonuç Raporu,* s. 6.
[166] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (20.04.2018)
[167] *Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) Sonuç Raporu,* s. 69.

4.1.3. Elektronik Ticaret Koordinasyon Kurulu

1998 yılında Bilim ve Teknoloji Yüksek Kurulu (BTYK) kararı kapsamında, Dış Ticaret Müsteşarlığının koordinatörlüğünde Türkiye'de e-ticaretin yaygınlaştırılması amacıyla Elektronik Ticaret Koordinasyon Kurulu (ETKK) kurulmuştur. Kurul bünyesinde hukuk, teknik ve finans alanlarında çalışma grupları oluşturulmuştur. Çalışma grupları ülkemizde e-ticaretin yaygınlaştırılması ve geliştirilmesine yönelik hazırladıkları raporlar ile bu alanda çeşitli öneriler ortaya koymuşlardır. Kurul, 2002/20 Başbakanlık Genelgesi ile "e-Türkiye" ile ilgili çalışmalar kapsamında yetkilerinin Devlet Bakanlığı ve Başbakan Yardımcılığına devredildiği döneme kadar faaliyetlerini sürdürmüştür.[168]

4.1.4. e-Türkiye Projesi

Başbakanlığın 19.03.1998 tarih ve 1998/13 sayılı genelgesi ile kamu bilgisayar ağları konusunda yapılan faaliyetlerin değerlendirilmesi, koordinasyonu, izlenmesi ve finansmanı gibi konularda karşılaşılan sorunların aşılması amacıyla Başbakanlık Müsteşarının başkanlığında kamu kurum ve kuruluşlarının katılımıyla Kamu-Net Üst Kurulu ve Kamu-Net Teknik Kurulu oluşturulmuştur. Kurulun faaliyetleri kapsamında 1998 yılında Kamu Bilgisayar Ağları Konferansı düzenlenmiş ve bir eylem planı önerisi ortaya konmuştur. 2002/20 Başbakanlık Genelgesi ile "e-Türkiye" çalışmalarının başlamasıyla faaliyetleri sona ermiştir.[169]

23-24 Mart 2000 tarihlerinde Lizbon'da düzenlenen Avrupa Konseyi toplantısında 15 AB üyesi ülkenin devlet başkanları, AB bölgesinin gelecek 10 yıllık eylem planında dünyanın en rekabetçi ve en dinamik bilgi tabanlı ekonomisi haline gelmesini hedef olarak belirlenmiştir. Hazırlanan eylem planı Haziran 2001'de

[168] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (21.04.2018)
[169] (http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/avrupa-icin-sayisal-gundem/eavrupa/ (27.02.2018)

Göteborg'da düzenlenen Avrupa Konseyi toplantısında kabul edilerek "e-Avrupa+" girişimi resmen yürürlüğe girmiştir.[170]

09.10.2001 tarihli ve 352 sayılı Başbakanlık Genelgesi ile e-Avrupa+ Eylem Planı ülkemize uyarlanarak e-Türkiye girişimi başlatılmıştır. Bu kapsamda ilgili bakanlıklar, Genelkurmay Başkanlığı ile ilgili kamu kurum ve kuruluşları koordinesinde 13 adet çalışma grubu oluşturulmuş ve çalışmalar sonucunda taslak eylem planı hazırlanmıştır. Ancak e-Türkiye girişimi o dönemdeki siyasi ve ekonomik istikrarsızlıklardan dolayı uygulama imkânı bulamamış; e-Dönüşüm Türkiye Projesinin ilanı ile son bulmuştur.[171]

4.1.5. e-Dönüşüm Türkiye Projesi

58. Türkiye Cumhuriyeti Hükümeti tarafından ilan edilen Acil Eylem Planı'nda yer alan e-Dönüşüm Türkiye Projesi ülkemizin bilgi toplumuna dönüşümü hususunda önemli bir adım olmuştur. Projenin koordinasyonu ile ilgili olarak Devlet Planlama Teşkilatı (DPT)[172] görevlendirilmiştir. Projenin amaçları, kurumsal yapısı ve uygulama esasları 27.02.2003 tarihli 2003/12 sayılı Başbakanlık Genelgesi ile yayımlanmıştır.

e-Dönüşüm Türkiye Projesi'nin koordine edilmesi, kamu kurum ve kuruluşlarının BİT yatırımları arasında eşgüdüm sağlanması ve Türkiye'nin bilgi toplumuna dönüşümü yolunda atılacak adımlara ilişkin stratejilerin belirlenmesi amacıyla 2003 yılında DPT bünyesinde Bilgi Toplumu Dairesi Başkanlığı kurulmuştur.[173]

---

[170] (http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/avrupa-icin-sayisal-gundem/eavrupa/ (27.02.2018)

[171] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (21.04.2018)

[172] Devlet Planlama Teşkilatı 2011 yılında yeniden organize edilmiş ve o yıldan itibaren Kalkınma Bakanlığı olarak çalışmalarını sürdürmektedir.

[173] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (21.04.2018)

Proje ile;

- Bilgi ve iletişim teknolojileri politikaları ve mevzuatının, öncelikle Avrupa Birliği müktesebatı çerçevesinde gözden geçirilerek yeniden düzenlenmesi, bu konuda e-Europe + kapsamında aday ülkeler için öngörülen eylem planının ülkemize uyarlanması,

- Vatandaşın, BİT sistemleri yardımıyla kamusal alandaki karar alma süreçlerine katılımını sağlayacak mekanizmaların geliştirilmesi,

- Kamu idaresinin şeffaf ve hesap verebilir hale getirilmesine katkıda bulunması,

- Kamu hizmetlerinin sunumunda BİT sistemlerinden azami ölçüde yararlanılarak, iyi yönetişim ilkelerinin hayata geçirilmesine katkıda bulunması,

- BİT sistemlerinin kullanımının yaygınlaştırılması,
- BİT alanında kaynak israfını azaltmak amacıyla; kamunun mükerrerlik arz eden veya örtüşen ilgili yatırım projelerinin bütünleştirilmesi, izlenmesi, değerlendirilmesi ve yatırımcı kamu kuruluşları arasında gerekli koordinasyonun sağlanması,

- Sektördeki özel sektör faaliyetlerine yukarıdaki ilkeler ışığında yol gösterilmesi hedeflenmiştir.

e-Dönüşüm Türkiye Projesi'nin yürütülmesinde daha önce yapılan çalışmalardan ve bilgi birikimlerinden faydalanılmıştır. Önceki çalışmalarda yer alan çalışma grupları yeniden düzenlenerek daha aktif ve verimli bir şekilde çalışmaları sağlanmıştır.[174]

[174] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (21.04.2018)

4.1.6. 2003-2004 Kısa Dönem Eylem Planı

2003-2004 Kısa Dönem Eylen Planı (KDEP), e-Dönüşüm Türkiye Projesi kapsamında bir Eylem Planı olarak kısa sürede hazırlanmış; 04.12.2003 tarih ve 2003/48 sayılı Başbakanlık Genelgesi ile "e-Dönüşüm Türkiye Projesi 2003-2004 Kısa Dönem Eylem Planı" olarak yürürlüğe girmiştir.

Yine 2003-2004 KDEP kapsamında yapılan çalışmaların tamamlanmasıyla orta vadeli programın hazırlanacağı zamana kadar bir yıllık 2005 Eylem Planı hazırlanarak uygulamaya konulmuştur.[175]

4.1.7. 2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı

2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı Türkiye'nin dünyadaki konu ile ilgili gelişmelere paralel olarak bilgi toplumuna dönüşüm hedeflerini gerçekleştirmek üzere çalışmalarını orta vadeli bir programa bağladığı temel bir politika metni olarak kabul edilmiştir. Yüksek Planlama Kurulu'nun 2006/38 sayılı kararı ile 28.07.2006 tarihinde yürürlüğe girmiştir.

Söz konusu strateji ile, BİT sistemlerinin toplumun tüm kesimlerine yayılması sonucunda oluşturulacak ağ etkisi üzerinden sonuç almayı hedefleyen bir yaklaşım ortaya konmuştur. 2006-2010 Bilgi Toplumu Stratejisi ile kamu kurumları, özel sektör, vatandaşlar ve BİT sektörünü kapsayan 4 aktör grubu belirlenmiş; yine bu gruplara yönelik 7 temel stratejik öncelik alanı belirlenmiştir.[176]

[175] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (21.04.2018)
[176] Bilgi Toplumu Stratejisi (2006-2010), Devlet Planlama Teşkilatı, 2006, s. 20-21.

Bu 7 temel alan ve amaçları:

- **Sosyal Dönüşüm**: Vatandaşların günlük ve iş hayatlarında BİT altyapılarını etkin olarak kullanmaları ile ekonomik ve sosyal faydanın arttırılması amaçlanmıştır.

- **Bilgi ve İletişim Teknolojilerinin İş Dünyasına Nüfuzu**: KOBİ'lerin (Küçük ve Orta Ölçekli İşletmeler) bilgisayarı ve interneti etkin kullanımının arttırılması, faaliyetlerini elektronik ortama taşıyarak e-ticaret yapmalarının teşvik edilmesi amaçlanmıştır. Ayrıca stratejik öneme sahip sektör ve bölgelere yönelik bilgi ve iletişim teknolojileri ihtiyaçlarının belirlenerek, bu ihtiyaçların karşılanmasına yönelik verimlilik programlarının hayata geçirilmesi amaçlanmıştır.

- **Vatandaş Odaklı Hizmet Dönüşümü**: Kamu hizmetlerinin BİT altyapılarının yardımıyla, kullanımı yoğun ve getirisi yüksek olan hizmetlerden başlanarak elektronik ortama aktarılması amaçlanmıştır. Ayrıca iş süreçlerinin kullanıcıların ihtiyaçlarına göre yeniden yapılandırılarak, kamu hizmetlerinin sunumunda etkinliğin sağlanması amaçlanmıştır.

- **Kamu Yönetiminde Modernizasyon:** BİT altyapıları yardımıyla vatandaş memnuniyeti ve verimliliği öncelikli olarak gözeten, ülke koşullarına uygun örgüt ve süreç yapılanmalarına sahip bir e-devlet yapısının hayata geçirilmesi amaçlanmıştır.

- **Küresel Rekabetçi Bilgi Teknolojileri Sektörü**: BİT alanında proje odaklı hizmetler ve kamu-özel sektör iş birliğiyle sektör yetkinliklerinin geliştirilerek yurtdışı pazarlarına açılım, paket yazılımda ise rekabet avantajının daha yüksek olduğu sektörel çözümlere odaklanılması amaçlanmıştır.

- **Rekabetçi, Yaygın ve Ucuz İletişim Altyapı ve Hizmetleri:** İletişim altyapı ve hizmetlerinin geliştirilmesi, kullanımının yaygınlaştırılması için telekomünikasyon sektöründe sunulan hizmet ve altyapılarda etkin rekabet ortamının tesis edilmesi gerekmektedir. Böylelikle hızlı, güvenli, kaliteli ve sürekli iletişim hizmetlerinin uygun maliyetlerle sunulmasının yanında yeni teknolojilere dayalı telekomünikasyon altyapılarının kurulması için uygun ortamın oluşturulması amaçlanmıştır.

- **AR-GE ve Yenilikçiliğin Geliştirilmesi:** Uluslararası pazarlarda talebin sürekli arttığı, yenilikçi ve yüksek katma değerli bir sektör olan BİT sektöründe AR-GE faaliyetlerine öncelik verilerek bu alanda yapılan yenilikçi çalışmaların desteklenmesi amaçlanmıştır. Ayrıca, tüm bu yenilikçi faaliyetlerin gerçekleştirilmesi sürecinde mevcut BİT altyapılarından azami ölçüde faydalanılması amaçlanmıştır.[177]

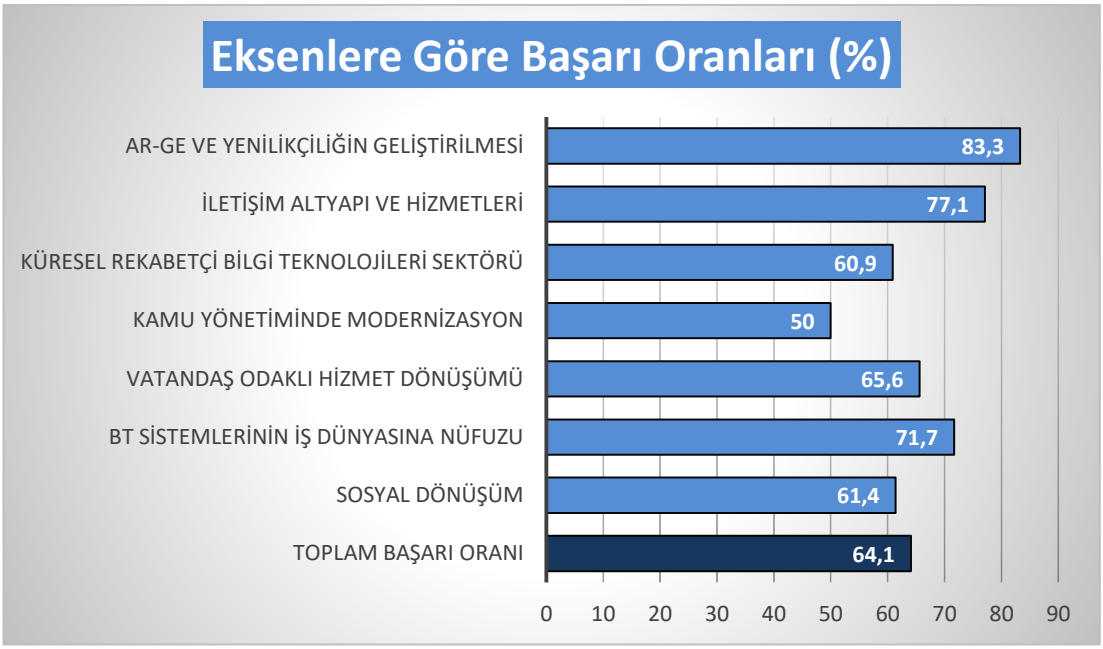
Tablo 3 Yedi Eksende Gerçekleştirilmesi Planlanan Eylem Sayıları

Eksenler	Eylem Sayısı
Sosyal Dönüşüm	14
Bilgi ve İletişim Teknolojilerinin İş Dünyasına Nüfuzu	12
Vatandaş Odaklı Hizmet Dönüşümü	41
Kamu Yönetiminde Modernizasyon	21
Küresel Rekabetçi Bilgi Teknolojileri Sektörü	13
Rekabetçi, Yaygın ve Ucuz İletişim Altyapı ve Hizmetleri	7
AR-GE ve Yenilikçiliğin Geliştirilmesi	3
TOPLAM	111

2006-2010 Bilgi Toplumu Stratejisi Tablo 3'de belirtilen 7 eksende, 38 kamu kurumunun sorumlu olduğu, 111 eylemin hayata geçirileceği, 36 tanesi temel gösterge olmak üzere toplamda 117 gösterge ile gelişmelerin takip edildiği ve 2,9 milyar TL harcamanın öngörüldüğü kapsamlı bir program olarak ortaya konulmuştur.[178]

[177] Bilgi Toplumu Stratejisi (2006-2010), Devlet Planlama Teşkilatı, 2006, s. 20-21. (http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf (11.03.2018)

[178] Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010) Nihai Değerlendirme Raporu, Kalkınma Bakanlığı, 2013, s. 8. (http://www.bilgitoplumu.gov.tr/Documents/1/Diger/BTS_VE_EYLEM_PLANI_NIHAI_DEGERLENDIRME_RAPORU.pdf (11.03.2018)



Şekil 4.1 Bilgi Toplumu Stratejisi Eylem Planının Eksenlere Göre Başarı Oranı

Kalkınma Bakanlığınca söz konusu planın uygulanmasından sorumlu kuruluşların katkılarıyla Mayıs 2008-Mart 2010 döneminde 5 tane değerlendirme raporu ve Mart 2013'de sonuç raporu yayımlanmıştır. Bilgi Toplumu Strateji Eylem Planı'nda Haziran 2012 itibariyle toplamda %64,1 başarı elde edilmiştir. Belirlenen 7 eksende elde edilen başarı oranları sayısal olarak Şekil 4.1'de yer almaktadır.[179]

Daha önce yayımlanan 2003/48 ve 2007/7 sayılı Başbakanlık Genelgeleri kapsamında kurumlar arası iş birliğinin sağlanması, ortak ilke ve standartların uygulanması, bilgi toplumuna dönüşüm sürecinde Bilgi Toplumu Stratejisinin etkin bir şekilde uygulanabilmesi amacıyla e-Dönüşüm Türkiye İcra Kurulu, Dönüşüm Liderleri Kurulu ve Danışma Kurulu oluşturularak çalışmalarına başlamışlardır.[180]

[179] a.g.r. s. 7-9.
[180] http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (21.04.2018)

4.1.8. 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı

2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı konu ile ilgili o güne kadar yayımlanmış en kapsamlı belgedir. Söz konusu strateji istihdam ve büyüme odaklı olarak, sekiz ana eksende hazırlanarak yürürlüğe girmiştir. Planın odak ve kapsamları belirlenirken;

- Türkiye'nin bilgi toplumu alanında kat ettiği mesafe ve bu alanda devam eden ihtiyaçları,
- Türkiye'nin temel sorunları ve önünde yer alan fırsatlar,
- 2014-2018 dönemini kapsayan Onuncu Kalkınma Planı,
- Ulusal, bölgesel ve tematik politika belgeleri,
- AB'nin Avrupa İçin Sayısal Gündem (Digital Agenda for Europe) Girişimi ve diğer uluslararası politika tercihleri,

olmak üzere beş ana unsur belirleyici olmuştur.

2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı'nın eksenleri:

1) Bilgi Teknolojileri Sektörü
2) Genişbant Altyapısı ve Sektörel Rekabet
3) Nitelikli İnsan Kaynağı ve İstihdam
4) Bilgi ve İletişim Teknolojilerinin Topluma Nüfuzu
5) Bilgi Güvenliği ve Kullanıcı Güveni*
6) Bilgi ve İletişim Teknolojileri Destekli Yenilikçi Çözümler
7) İnternet Girişimciliği ve e-Ticaret
8) Kamu Hizmetlerinde Kullanıcı Odaklılık ve Etkinlik[181]

[181] 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Kalkınma Bakanlığı, 2015 s. 15. http://www.bilgitoplumustratejisi.org/tr (13.03.2018)

2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Onuncu Kalkınma Planı'nda tanımlanan bilgi toplumu politika ve hedeflerinin detaylandırıldığı; bu politikaların uygulanmasına yönelik strateji ve eylemlerin belirlendiği bir politika belgesi niteliği taşımaktadır. [182]

Strateji ve Eylem Planı'nın "Bilgi Güvenliği ve Kullanıcı Güveni" ekseninde bilgi toplumuna dönüşümün sağlıklı bir şekilde sağlanabilmesi için; bilgi güvenliğinin sağlanması ve kullanıcı güveninin arttırılması temel amaç olarak belirtilmiştir. Bu kapsamda ulusal bilgi güvenliğinin sağlanması ve kişisel verilerin korunmasına yönelik yasal altyapının oluşturulması, siber suçlarla mücadelenin bütüncül olarak ele alınması ve güvenli internet uygulamalarında eğitim ve farkındalık faaliyetlerine ağırlık verilmesi hususlarının önemine değinilmiştir.

Plan kapsamında ulusal bilgi güvenliğine yönelik yasal, idari ve teknik altyapılar oluşturulacaktır. Böylelikle hem kamu hem de özel sektöre ait bilgi sistemleri ve kritik altyapıların denetlenmesi, standardizasyonu ve koordinasyonuna yönelik yetki ve sorumluluklar kanunla düzenlenecek ve bu alanda kurumsal bir yapı oluşturulacaktır. Kritik bilgi sistemlerinin muhtemel saldırılara karşı korunması için gerekli önlemler alınarak, bilgi güvenliği farkındalığının kurumsal ve bireysel düzeyde oluşmasını sağlayacak bilinçlendirme faaliyetleri yürütülecektir. Ayrıca ulusal bilgi güvenliğini sağlamak adına uluslararası iş birliklerine önem verilerek mevcut strateji ve eylem planı ülkemizin ihtiyaçları doğrultusunda güncellenecektir.[183]

4.2. TÜRKİYE'DE SİBER GÜVENLİK ÇALIŞMALARI

Ülkelerin kalkınmasına önemli katkı sağlayan BİT altyapıları, toplumların ve ekonomilerin göz ardı edilemez unsurları haline gelmiştir. Ülkemizde de kamu kurum ve kuruluşları, özel sektör ve vatandaşların yanı sıra; enerji hatları, su kaynakları,

[182] 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, a.g.p. s. 15.
[183] 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, a.g.p. s. 70-71.

ulaşım, haberleşme, finans, gıda ve sağlık hizmetleri gibi kritik altyapılarda BİT sitemleri yaygın olarak kullanılmaktadır. BİT sistemleri ve internet kullanımının yaygınlaşması ile birlikte siber ortamın tüm unsurları birbirine bağlı hale gelmiştir. Bu durum da siber güvenlik risklerini beraberinde getirmiştir.

Ülkemizde de BİT sistemlerine olan ihtiyacın günden güne artmasıyla birlikte, söz konusu sistemlerin güvenliğinin sağlanması ülkemizin ulusal güvenliği için önemli hale gelmiştir.[184] Siber ortamdaki tehditlerden ülkemizi korumak için yasal düzenlemeler yapılmış, mevcut kurumlara yeni yetkiler verilmiş, yeni kurumlar kurulmuş ve çeşitli projeler hayata geçirilmiştir. Her geçen gün devletin ve sivil toplum kuruluşlarının destekleriyle yürütülen projelerle yeni siber güvenlik uzmanları yetiştirilmekte, yetiştirilen uzmanlar kamu ve özel sektörün önemli kademelerinde görev almaktadırlar.

Türkiye'de siber güvenlik alanında UDHB, BTK, TÜBİTAK, TSK Siber Savunma Merkezi Başkanlığı ve Siber Güvenlik Kurulu konu ile ilgili çalışmaları yürütmektedirler. Bu kurumlar dışında çeşitli sivil toplum kuruluşları da siber güvenlik ile ilgili çalıştaylar düzenleyerek siber uzayda yer alan tehditler konusunda internet ve BİT sistemi kullanıcılarını bilinçlendirme faaliyetlerinde bulunmaktadırlar.[185]

Ülkemizde 2009 yılında, siber savunma ve sanal ortam güvenliği politika esaslarını belirlemek üzere TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) koordinatörlüğünde ilgili kamu kurum ve kuruluşlarının temsilcilerinden oluşan bir çalışma grubu oluşturulmuştur. Çalışma grubu konu ile ilgili çalışmalarını 30 Ocak 2009 tarihinde tamamlayarak "Ulusal Sanal Ortam Güvenlik Politikası" belgesini hazırlamıştır. Çalışma grubunda yer alan kamu kurum ve kuruluşları şunlardır:

[184] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2016), *"2016-2019 Ulusal Siber Güvenlik Stratejisi"*, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (19.02.2018)
[185] Siber İstihbarat a.g.e. s. 171-172.

- Cumhurbaşkanlığı
- Başbakanlık
- Dışişleri Bakanlığı
- Adalet Bakanlığı
- Milli Savunma Bakanlığı
- Ulaştırma Bakanlığı
- İçişleri Bakanlığı
- Maliye Bakanlığı
- Genelkurmay Başkanlığı
- Devlet Planlama Teşkilatı Müsteşarlığı
- Hazine Müsteşarlığı
- Dış Ticaret Müsteşarlığı
- Türkiye Cumhuriyet Merkez Bankası (TCMB)
- Milli Güvenlik Kurulu Genel Sekreterliği
- Milli İstihbarat Teşkilatı (MİT) Müsteşarlığı
- Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)
- Emniyet Genel Müdürlüğü
- Bilgi Teknolojileri ve İletişim Kurumu (BTK)
- TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

Ulusal Sanal Ortam Güvenlik Politikası "Temel İlkeler", "Tehditler ve Açıklıklar", "Sanal Ortam Güvenlik Adımları" olmak üzere 3 ana başlıktan oluşmaktadır.[186] Söz konusu belge ülkemizde siber güvenlik alanında ilk resmi belgedir.

2010 yılında Genelkurmay Başkanlığı'nın önerisi doğrultusunda "siber terörizm" kavramı Milli Güvenlik Siyaset Belgesi'ne eklenmiştir.[187]

[186] BTK, (2009), *"Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler"* s. 25-26. , (https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf (21.02.2018)

[187] (http://www.haberturk.com/gundem/haber/557436-siber-teror-kirmizi-kitapta (22.02.2018)

Siber Güvenlik alanında AR-GE çalışmalarının daha etkin yürütülebilmesi 2012 yılında TÜBİTAK BİLGEM (Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi)'e bağlı Siber Güvenlik Enstitüsü kurulmuştur.[188]

Üniversitelerde siber güvenlik alanında yüksek lisans ve doktora düzeyinde akademik çalışmaların yürütülebilmesi amacı ile yeni birimler oluşturulmuştur.

4.2.1. Türkiye'de Siber Güvenlik Faaliyetlerinde Bulunan Kurumlar

Türkiye'de ulusal siber güvenlik faaliyetleri TÜBİTAK, Ulaştırma ve Kalkınma Bakanlığı, Emniyet Genel Müdürlüğü, Türk Silahlı Kuvvetleri gibi kamu kurumlarının yanı sıra başta Bilgi Güvenliği Derneği ve Türkiye Bilişim Derneği olmak üzere çeşitli sivil toplum kuruluşlarınca yürütülmektedir. Bu bölümde siber güvenlik alanında kurulan kurumlar ve kuruluşlar ele alınmaktadır.

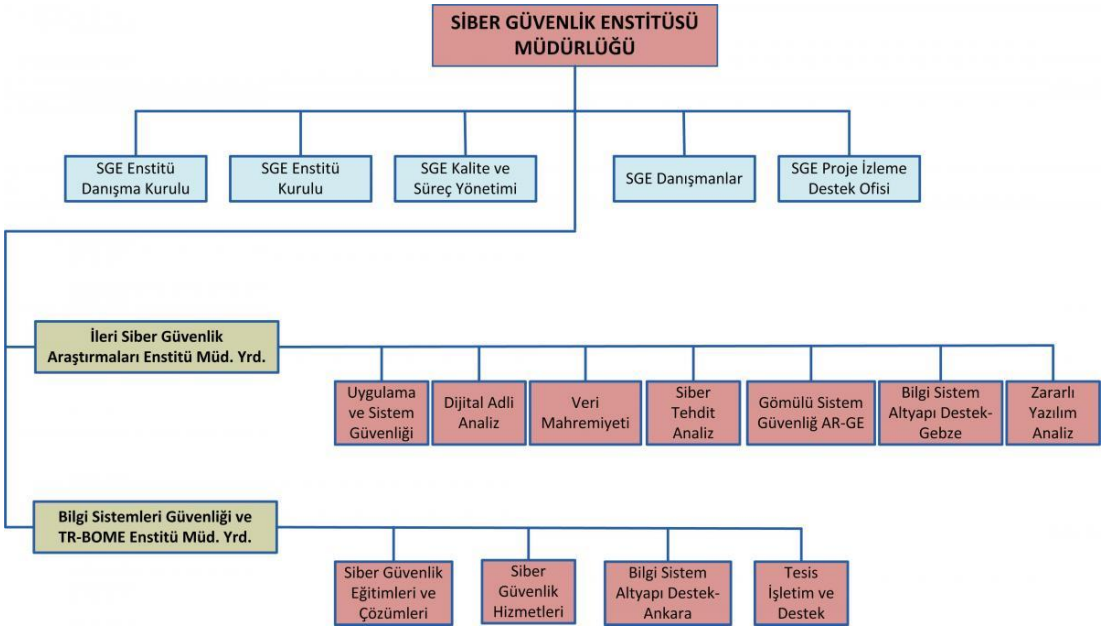
4.2.1.1. Siber Güvenlik Enstitüsü

1997 yılında TÜBİTAK UEKAE'nin alt birimi olarak Bilişim Sistemleri Güvenliği Enstitüsü (BGE) adıyla çalışmalarına başlamıştır. 2012 yılından itibaren TÜBİTAK BİLGEM bünyesinde Siber Güvenlik Enstitüsü (SGE) adıyla ayrı bir enstitü olarak faaliyetlerine devam etmektedir.

Siber Güvenlik Enstitüsü'nün faaliyetleri üç başlık altında toplanabilir:

- İleri Düzey Siber Güvenlik AR-GE Çalışmaları
- Siber Güvenlik Strateji Belirleme Çalışmaları
- Kurumlara (askeri, kamu, özel sektör) Yönelik Siber Güvenlik Çözüm Projeleri

[188] (http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi (22.02.2018)



Şekil 4.2 SGE Organizasyon Şeması

Kuruma ait organizasyon şeması Şekil 4.2'de yer almaktadır. Siber Güvenlik Enstitüsü Müdürlüğü bünyesinde İleri Siber Güvenlik Araştırmaları Enstitü Müdür Yardımcılığı ile Bilgi Sistemleri Güvenliği ve TR-BOME Enstitü Müdür Yardımcılığı adlı iki ana birim siber güvenlik faaliyetlerini yürütmektedir.[189]

4.2.1.2. Siber Suçlarla Mücadele Daire Başkanlığı

Emniyet Genel Müdürlüğü (EGM) bünyesinde BİT altyapıları kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren ilgili daire başkanlıkları ve taşra teşkilatındaki birimler dağınık yapıda bulunmaktaydı. Tüm bu birimlerin tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla etkin ve verimli bir mücadelenin yürütülebilmesi amacıyla 2011/2025 sayılı Bakanlar Kurulu kararı ile EGM bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur.

[189] http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi (22.02.2018)

28.03.2013 tarihli Bakanlık Oluruna istinaden Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nın adı Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir.[190] Bu birim bünyesinde şifre kırma, sinyal istihbaratı, internet ortamındaki içeriklerin analizi ve takibi gibi faaliyetler yürütülmektedir.

4.2.1.3. TSK Siber Savunma Merkezi Komutanlığı

Türk Silahlı Kuvvetleri kara, deniz, hava ve uzay harekât alanlarının ardından siber ortamda da harekât kapasitesini arttırmak amacıyla 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur. Siber Savunma Merkezi Başkanlığının görev ve sorumluluğu Türk Silahlı Kuvvetleri bünyesinde kullanılan bilişim sistemlerinin siber tehditlere karşı korunmasıdır. Başkanlık UDHB, TÜBİTAK ve çeşitli üniversiteler ile iş birliği içerisinde faaliyetlerini yürütmektedir. Ayrıca NATO ile de ulusal ve uluslararası alanda ortaklaşa faaliyetlerde bulunmaktadır.[191]

TSK'ya ait BİT sistemlerinin siber güvenliğini sağlamada kullanılan yazılımların milli imkânlarla geliştirilmesi ve TSK bünyesinde gerçekleştirilen siber güvenlik faaliyetlerinin tek bir yerden koordine edilmesi amacıyla Siber Savunma Harekât Merkezi kurulması faaliyetleri Savunma Sanayi Müsteşarlığınca yürütülmektedir. Siber Savunma Harekât Merkezi (SİSAMER)'nin kurulumu tamamlanmış olup, yazılım geliştirme faaliyetlerinin de 2018 yılı ilk yarısı itibariyle tamamlanması hedeflenmektedir.[192]

4.2.1.4. Siber Güvenlik Kurulu

Bakanlar Kurulunun 11.06.2012 tarihli ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin

[190] http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx - (21.05.2018)
[191] Siber İstihbarat a.g.e. s. 177.
[192] https://www.ssm.gov.tr/website/contentlist.aspx?PageID=1083&LangID=1 (21.02.2018)

Kararı", 20.12.2012 tarihli ve 28447 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Siber Güvenlik Kurulu; Bakanlar Kurulunun söz konusu kararı kapsamında kurulmuştur.[193]

05.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen "Ek Madde 1" ile Siber Güvenlik Kurulu'nun amacı, görevleri ve üyeleri düzenlenmiştir.

Kurulun kanunda kuruluş amacı; "*Türkiye'nin kritik altyapıları başta olmak üzere kişiler ve kurumlar için siber güvenlikle ilgili alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak*" olarak belirtilmiştir.

Ulaştırma Denizcilik ve Haberleşme Bakanı'nın başkanlığında toplanan kurul;

- İlgili bakanlıkların müsteşarları,
- Millî İstihbarat Teşkilâtı (MİT) müsteşarı,
- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri (MEBS) Başkanı,
- BTK Başkanı,
- TÜBİTAK Başkanı,
- Mali Suçları Araştırma Kurulu (MASAK) Başkanı,
- Telekomünikasyon İletişim Kurumu (TİB) Başkanı[194]
- Ulaştırma Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlıklar ve kamu kurumlarının üst düzey yöneticilerinden meydana gelmektedir. [195]

UDHB Binali Yıldırım başkanlığında ilk kez toplanan kurul; 21.12.2012 tarihli ilk toplantısında "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" ile "Siber Güvenlik Kurulunun Görevleri, Çalışma Usul ve Esasları Yönergesi" kabul

[193] http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (15.02.2018)
[194] TİB, 671 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname'ye göre 15 Ağustos 2016'da kapatılarak görev ve yetkileri Bilgi Teknolojileri ve İletişim Kurumuna aktarılmıştır.
[195] http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm (15.02.2018)

edilmiştir. Kurulun ikinci toplantısı 20.06.2013 tarihinde gerçekleşmiştir. Bu toplantıda Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) kurulduğu ve 15 Mayıs 2013 tarihinden itibaren faaliyetlerine başladığı açıklanmıştır. Kurulun üçüncü toplantısı 19.12.2013 tarihinde gerçekleşmiştir.[196] Dördüncü toplantısı 10.02.2016 tarihinde gerçekleştirilmiştir.[197]

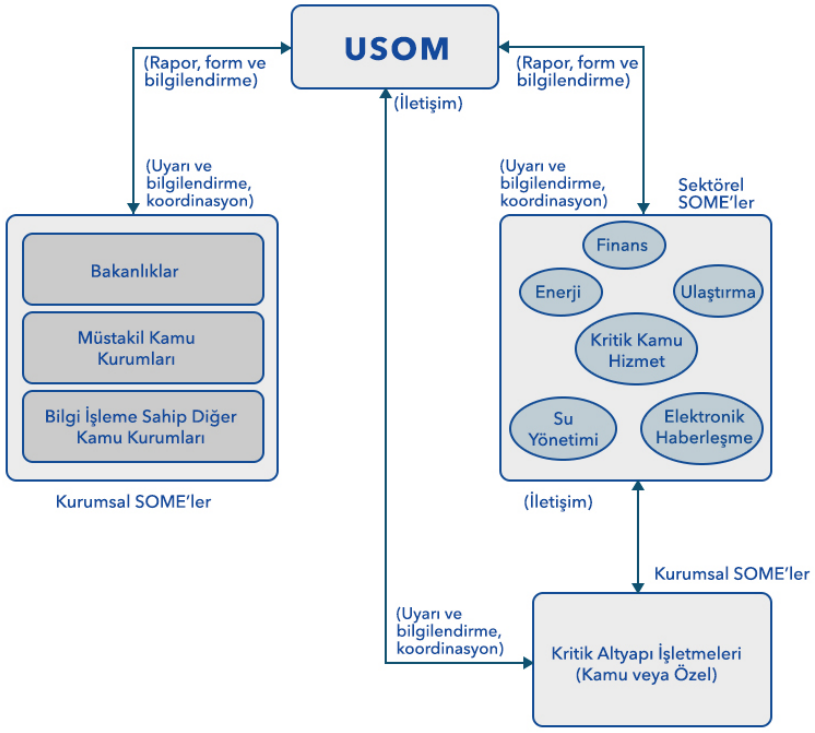
Ek Madde 1 kapsamında Siber Güvenlik Kurulunun sekretaryasını yapmak, ilgili faaliyetlerin koordinasyonunu sağlamak, siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı arttırma gibi tüm çalışmalar Haberleşme Genel Müdürlüğünce yürütülmüştür. Ancak 09.07.2018 tarihli ve 703 sayılı Kanun Hükmünde Kararname (KHK) kapsamında Haberleşme Genel Müdürlüğü bünyesinde yürütülen siber güvenlik kurulu sekretarya işlemleri kaldırılarak, icra kurulu iptal edilmiştir.[198] Siber Güvenlik Kurulunun yetkilerinin önümüzdeki günlerde Cumhurbaşkanlığınca belirlenecek olan merci ya da kurula devredileceği beklenmektedir.[199]

4.2.1.5. USOM ve SOME'ler

Ulusal Siber Olaylara Müdahale Merkezi (kısaca USOM veya TR-CERT), Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı'nın 4.3 numaralı maddesi uyarınca BTK bünyesinde kurulmuştur. USOM; siber uzayda ortaya çıkan tehditlerin hızla tespit edilmesi, tespit edilen tehditlerin etkilerini minimuma indirmek veya tamamen ortadan kaldırmaya yönelik önlemlerin geliştirilmesini amaçlamaktadır. Ayrıca kurum ve kuruluşların siber olaylara müdahale yeteneklerinin geliştirilmesine yönelik çalışmaları yürütmektedir.

[196] https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK-KURULU (15.02.2018)
[197] https://www.btk.gov.tr/tr-TR/Kurumdan-Haberler/Siber-Guvenlik-Kurulu-Toplandi (15.02.2018)
[198] http://ticaretgazetesi.com.tr/siber-guvenlik-icin-kararname-bekliyoruz (02.11.2018)
[199] 703 sayılı KHK, (2018), T.C. Resmi Gazete, 30473, 09/07/2018.

USOM, Ülkemize yönelik olası siber tehditlere karşın 7/24 çalışma prensibiyle faaliyetlerini yürütmektedir. USOM kurumsal ve sektörel Siber Olaylara Müdahale Ekipleri (SOME)'nin koordinasyonunu sağlamaktadır. Ayrıca SOME'lere yönelik bilgilendirme ve bilinçlendirme faaliyetlerini yürütmektedir. USOM ve kurumsal SOME'ler siber olaylarla mücadele çalışmalarını kolluk kuvvetleri ile koordineli bir şekilde yürütmektedirler. USOM Türkiye'nin uluslararası alanda siber olaylar konusunda temas noktası olması sebebiyle, eşdeğer yabancı kuruluşlarla yakın iş birliği içerisinde faaliyetlerini yürütmektedir.[200]



Şekil 4.3 Ulusal Siber Olaylara Müdahale Organizasyonu

Siber Güvenlik Stratejisi 2013-2014 Eylem Planı'na göre kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (SOME)'nin kurulması öngörülmüştür. Şekil 4.3'de yer alan organizasyon şemasından da görüldüğü üzere,

[200] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2013), "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*", s. 8.
http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf (17.02.2018)

USOM'a bağlı olarak faaliyetlerini yürütmekte olan sektörel ve kurumsal SOME'ler yer almaktadır.

Kurumsal SOME'ler bakanlıklar, müstakil kamu kurumları ve kritik altyapı işletmecileri (kamu veya özel) bünyesinde oluşturulmaktadır. Kurumsal SOME'ler faaliyetlerini yürütürken USOM ve diğer Kurumsal SOME'lerle birlikte koordinasyon ve iletişim halinde bulunmaktadırlar.

Şekil 4.3'de yer alan;

- **Uyarı ve bilgilendirme**: Siber olaylar öncesi USOM tarafından hazırlanan duyuru, uyarı, bülten gibi bilgileri,
- **Koordinasyon**: Siber olay sırasında; USOM, kurumsal SOME ve sektörel SOME arasında sağlanan koordinasyonu,
- **İletişim**: Siber olayın öncesinde, esnasında ve sonrasında USOM ve/veya Kurumsal SOME'nin bağlı olduğu sektörel SOME tarafından talep edilen rapor, form veya bilgilendirmeyi belirtmektedir.[201]

Tablo 4 Sektörel SOME Kurulacak Kurumlar

Kritik Altyapı Sektörü	SOME Kurulacak Kurum
Enerji	EPDK
Finans	SPK, BDDK
Elektronik Haberleşme	BTK
Su Yönetimi	Orman ve Su İşleri Bakanlığı
Ulaştırma	• Karayolu Düzenleme Genel Müdürlüğü • Demiryolu Düzenleme Genel Müdürlüğü • Deniz ve İç sular Düzenleme Genel Müdürlüğü • Sivil Havacılık Genel Müdürlüğü • Tehlikeli Mal ve Kombine Taşımacılık Düzenleme Genel Müdürlüğü
Kritik Kamu Hizmetleri	• İçişleri Bakanlığı • Adalet Bakanlığı • Maliye Bakanlığı • Çevre ve Şehircilik Bakanlığı • Çalışma ve Sosyal Güvenlik Bakanlığı • Gıda, Tarım ve Hayvancılık Bakanlığı • Sağlık Bakanlığı

[201] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2014), "*Kurumsal SOME Kurulum Rehberi"*, s. 10-12. http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf (23.02.2018)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 5 numaralı maddesi kapsamında Siber Güvenlik Kurulu'nca enerji, finans, ulaştırma, elektronik haberleşme, kritik kamu hizmetleri ve su yönetimi ülkemizin kritik altyapı sektörleri olarak belirlenmiştir. Plana göre her altyapı sektörü için sektörel SOME'ler kurulmuştur. Sektörlere göre SOME kurulacak kurumlar Tablo 4'de yer almaktadır.

Sektörel SOME'ler sorumlu oldukları sektörün siber güvenlik faaliyetlerinin koordinasyonundan, düzenlenmesinden ve yetkileri varsa denetlenmesinden sorumludurlar. Sektörel SOME'ler faaliyetlerini yürütürlerken USOM ve diğer Kurumsal SOME'lerle birlikte koordinasyon ve iletişim halinde bulunmaktadırlar.[202]

4.2.1.6. Türkiye Bilişim Derneği

Türkiye Bilişim Derneği (TBD) 1971 yılında bilişim alanında uzman kişilerce ülkemizde "Bilişim Kültürünü" toplumun tüm kesimlerine yaymayı hedefleyen bir sivil toplum kuruluşudur. Ülkemizin BİT altyapıları ile ilk tanışmaya başladığı dönemde kurulan dernek, bilişim alanında kurulmuş en köklü sivil toplum kuruluşudur. Bakanlar Kurulu kararıyla 7 Mart 1994 tarihinde kamu yararına çalışan destek statüsünü kazanmıştır.

Derneğin kuruluş amaçları:

- Türkiye BİT sitemlerinin verimli bir biçimde kullanımının arttırılması, gelişmesi ve çağdaş standartlarda tutulmasına yardımcı olmak,
- Bilişim alanında çalışan kişileri bir araya toplayarak, mesleki gelişim ve dayanışma ortamları sağlamak,
- Bilişim sektöründe nitelikli ve verimli insan gücünün geliştirilmesine katkı sağlamak,

[202] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2014), "*Sektörel SOME Kurulum Rehberi"*, s. 14-15. (http://www.udhb.gov.tr/doc/siberg/Sektorel_SOME_Reh.docx) - (23.02.2018)

- Bilişim alanında standartlar, eğitim, yasal altyapı, çalışma koşulları gibi konularda işbirliğini sağlamak,
- Bilişim konusunda bilimsel AR-GE çalışmaları ile donanım ve yazılım sistemlerinin üretim faaliyetlerini desteklemek,
- Bilişim alanında kamusal faydanın ön planda tutulduğu politika ve kararların oluşmasını sağlamak,
- Bilgi toplumu olma yönündeki bilincin ülke genelinde yayılmasını sağlamak,
- Bilişim alanında ortaya çıkan toplumsal sorunlara çözüm önerileri sunmak,
- İnsan odaklı ve toplumun yararına faaliyetlerde bulunmaktır.

TBD, amaçları doğrultusunda çalışma grupları kurarak bilişim alanında güncel ve geleceğe yönelik çalışmalar yapmaktadır. Düzenlediği ulusal ve uluslararası seminer, kurultay, konferans, meslek içi eğitimler vb. etkinliklerle; hazırladığı teknik ve bilimsel yayınlarla; bilişim ile ilgili dünyada yaşanan gelişmeleri yakından izleyerek bilişim kültürünü topluma yaymak üzere çeşitli faaliyetlerde bulunmaktadır. Ayrıca bilişim ile ilgili her türlü uygulama ve yasal düzenlemede görüş belirten TBD, diğer sivil toplum kuruluşları ile işbirliği faaliyetlerini de sürdürmektedir.

TBD bünyesinde 1976 yılında "TBD Birinci Ulusal Bilişim Kurultayı" adıyla düzenlenen bilişim etkinliği, bu alanda düzenlenen ilk bilimsel toplantı niteliği taşımaktadır. TBD tarafından düzenlenen bilişim etkinlikleri günümüzde çok katılımlı uluslararası bir boyuta ulaşmıştır.[203]

TBD bünyesinde aktif olarak faaliyet yürüten 7 tane çalışma grubu bulunmaktadır. Tüm çalışma grupları bilişim bağlamında kendi alanlarında faaliyetlerini yürütmektedirler. Bu çalışma grupları:

- Kamu BİB (Bilgi İşlem Birimleri) Çalışma Grubu
- Hukuk Çalışma Grubu
- Türk Dünyası Ortak Bilişim Terimleri Çalışma Grubu

[203] https://www.tbd.org.tr/kurumsal/tanitim/ (12.11.2018)

- Bilişimde Özenli Türkçe Çalışma Grubu
- Türk Dünyası Bilgi Teknolojileri Çalışma Grubu
- Bilişim Kentleri Çalışma Grubudur.[204]

TBD'nin toplamda 13 ilde ve birçok üniversitede temsilcilikleri bulunmaktadır. 2018 yılı verilerine göre derneğin toplamda 12.000'in üzerinde üyesi bulunmaktadır.[205]

4.2.1.7. Bilgi Güvenliği Derneği

Bilgi Güvenliği Derneği (BGD) 2007 yılında kamu ve özel sektör yöneticileri ile akademisyenlerden oluşan, alanında uzman kişiler tarafından kurulmuştur. Merkezi Ankara'da bulunmaktadır.

Derneğin kuruluş amaçları:

- Bilgi güvenliği ve siber güvenlik konusunda toplumun tüm kesimlerinin bilgi ve bilinç düzeyini arttırmak,
- Konu hakkındaki teknolojik gelişmeleri yakından takip etmek,
- Milli siber güvenlik teknolojilerinin geliştirilmesine katkı sağlamak,
- Bireysel, kurumsal ve ulusal düzeydeki güvenlik riskleri konusunda farkındalık oluşturmaktır.[206]

BGD yurtiçinde başta kamu ve özel sektör kuruluşları, üniversiteler ve çeşitli sivil toplum kuruluşları olmak üzere tüm paydaşlarla işbirliği içerisinde bilgi güvenliği mevzuatının hazırlanması ve geliştirilmesinde aktif olarak rol oynamaktadır. Ulusal Siber Güvenlik Stratejisinin hazırlanması ve 2012/3842 sayılı Bakanlar Kurulu kararının alınmasında önemli görevler üstlenmiştir. Ayrıca yurtiçinde düzenlediği

[204] https://www.tbd.org.tr (12.11.2018)
[205] https://www.tbd.org.tr/kurumsal/tanitim/ (12.11.2018)
[206] https://www.bilgiguvenligi.org.tr/hakkimizda/tuzuk/ (02.11.2018)

sempozyum, çalıştay, konferans ve eğitimler; yayımladığı rapor ve dokümanlarla toplumsal siber güvenlik farkındalığının arttırılmasına katkı sağlamaktadır.

BGD yurtiçi faaliyetlerinin yanı sıra uluslararası alanda da ITU ve ENISA ile işbirliği faaliyetlerinde bulunmaktadır. BGD, ISCTURKEY (Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı - Türkiye) konferanslarının ülkemizde düzenlenmesine öncülük etmektedir. Ayrıca ENISA bünyesinde her yıl ekim ayında düzenlenen "Avrupa Siber Güvenlik Ayı" platformuna dâhil olmuştur. Bu kapsamda her yıl ekim ayı içerisinde toplumsal siber güvenlik farkındalığının arttırılmasına yönelik çeşitli etkinlikler düzenlemektedir.[207]

4.2.2. Ulusal Siber Güvenlik Stratejileri

2013 yılında kabul edilerek yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Türkiye'nin ilk siber güvenlik stratejisi ve eylem planı niteliği taşımaktadır. Gelişen BİT sistemleri, siber uzayda artan tehditler ve 2013 yılında yayımlanan strateji planındaki eksiklikler göz önünde bulundurularak Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı kabul edilerek yürürlüğe girmiştir.

Bu bölümde yayımlanan sırasıyla 2013-2014 ve 2016-2019 Ulusal Siber Güvenlik Stratejileri ayrıntılı olarak ele alınmaktadır.

4.2.2.1. Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı

Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı; Siber Güvenlik Kurulu'nun 21.12.2012 tarihinde gerçekleştirilen toplantısında kabul edilmiş ve Bakanlar Kurulunun 20.06.2013 tarihli ve 28683 sayılı kararı ile Resmî Gazetede yayımlanarak yürürlüğe girmiştir. İlgili Bakanlar Kurulu kararı gereğince hazırlanan

[207] https://www.bilgiguvenligi.org.tr/bgd-genc/ (02.11.2018)

eylem planında, 2013-2014 döneminde yapılması planlanan çalışmalar ile eğitim ve farkındalık faaliyetlerine ilişkin planlar yer almaktadır.[208]

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı;

- Kamu kurum ve kuruluşlarında BİT altyapıları ile sağlanan her türlü hizmetin sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ve özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin minimum düzeyde kalmasına, muhtemel bir siber saldırı sonrası sistemlerin normal çalışmasına devam edebilmesine yönelik siber güvenlik eylemlerinin belirlenmesine ve meydana gelen siber suçun adli makamlar ve kolluk kuvvetlerince etkin bir şekilde araştırılması ve soruşturulmasının sağlanmasına yönelik bir siber güvenlik alt yapısı oluşturmaktır.[209]

4.2.2.2. Ulusal Siber Güvenlik Stratejisi 2016-2019 Eylem Planı

Gelişen BİT sistemleri, siber uzayda artan tehditler, 2013-2014 dönemi eylem planındaki eksiklikler ve edinilen tecrübeler doğrultusunda UDHB tarafından ulusal siber güvenlik stratejisinin güncellenerek 2016-2019 dönemini kapsayan yeni bir eylem planının hazırlanmasına gereksinim duyulmuştur. Bu kapsamda 2013-2014 dönemi eylem planının uygulamasından sorumlu kuruluşlar ile ilgili kurumlar arasında 10 Mart-7 Nisan 2015 tarihleri arasında yedi tane değerlendirme toplantısı yapılmıştır. Toplantılarda daha önceki eylem planında yer alan hedeflere ulaşma oranları, uygulamalarda karşılaşılan güçlükler ve ileriye yönelik gerçekleştirilmesi hedeflenen faaliyetler ayrıntılı olarak ele alınmıştır.

[208] https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Siber-Guvenlik-Stratejisi-ve-Eylem-Plani - (20.02.2018)
[209] *"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"* a.g.p. s. 10.

Toplantıların ardından kamu kurumları, sivil toplum örgütleri, kritik altyapı işletmeleri, üniversiteler ve bilişim sektöründen 73 kurum ve kuruluştan oluşan toplam 126 temsilcinin katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. İki gün süren platform çalışmaları kapsamında Türkiye'nin siber güvenlik alanında güçlü ve zayıf yönleri ele alınarak stratejik hedefleri ve gerçekleştirilmesi gereken eylemler belirlenmiştir.

2016-2019 dönemi eylem planı hazırlanırken ülke içinde paydaşlarla gerçekleştirilen çalışmalara ek olarak Amerika, Asya ve Avrupa ülkelerinin mevcut siber güvenlik stratejileri incelenmiş, ülkelerin siber güvenlik alanında kapsam, hedefler, öncelikler, AR-GE koordinasyonu, kamu-özel sektör iş birliği, eğitim gibi başlıklarda ortaya koyduğu çalışmalar değerlendirilmiştir. Tüm bu kapsamlı araştırma, inceleme ve değerlendirme çalışmaları sonucunda 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmıştır.

Ulusal Siber Güvenlik Stratejisinde;

- Kritik altyapılar: İşlediği verilerin gizliliği, bütünlüğü ve erişilebilirliği bozulduğunda can kaybına, büyük çaplı ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına sebep olabilecek bilişim sistemlerini barındıran alt yapıları,

- Kritik altyapı sektörleri: Şekil 4.4'de görüldüğü üzere elektronik ve haberleşme, ulaştırma, enerji, su yönetimi, kritik kamu hizmetleri, gıda, bankacılık ve finans sektörleri kritik altyapı sektörlerini oluşturmaktadır.



Şekil 4.4 Kritik Altyapı Sektörleri

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ana amacı; siber güvenliğin ulusal güvenlikten ayrı düşünülemeyecek bir kavram olduğu anlayışının tüm kesimlerde yerleştirilmesi, ulusal siber uzayda bulunan sistem ve paydaşların güvenliğini sağlamak üzere idari ve teknik tedbirlerin alınmasını sağlayacak yetkinlik ve bilincin kazanılmasıdır.

Ulusal Siber Güvenlik Stratejisi gelişen teknoloji, değişen koşullar ve gereksinimler göz önünde bulundurularak, kamu ve özel sektörden gelen talepler doğrultusunda güncellenecek olup, ulaşılamayan hedefler bir sonraki eylem planına aktarılacaktır.[210]

[210] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2015), "*2016-2019 Ulusal Siber Güvenlik Stratejisi*", s. 6-10. http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (20.02.2018)

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda gerçekleştirilmesi planlanan stratejik eylemler beş ana başlık altında gruplandırılmıştır.[211] Bunlar:

- **Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması**: Bu stratejik eylem maddesi ile; devleti, milli ekonomiyi, kritik altyapıları ve toplumun genelini etkileyebilecek tehditlerin azaltılmasına veya tamamen ortadan kaldırılmasına yönelik gerçekleştirilebilecek eylemler planlanmaktadır.

- **Siber Suçlarla Mücadele**: Bu stratejik eylem maddesi ile kurumları ve bireyleri etkileyerek, çoğunlukla maddi kayıplara yol açan tehditlerin azaltılmasına veya tamamen ortadan kaldırılmasına yönelik gerçekleştirilebilecek eylemler planlanmaktadır.

- **Farkındalık ve İnsan Kaynağı Geliştirme**: Bu stratejik eylem maddesi ile; bilgi ve iletişim teknolojilerini kullanan vatandaşlardan kurum ve şirket yöneticilerine kadar toplumun tüm kesimlerine kadar siber güvenlik kültürünün kazandırılmasına yönelik gerçekleştirilebilecek eylemler ile nitelikli siber güvenlik uzmanlarının yetiştirilebilmesine yönelik eylemler planlanmaktadır.

- **Siber Güvenlik Ekosisteminin Geliştirilmesi**: Bu stratejik eylem maddesi ile; kamu, özel sektör, sivil toplum kuruluşları ve diğer paydaşların katkılarıyla mevzuat ve teknoloji altyapıları bağlamında ülkenin gereksinimlerinin belirlenmesi ve yapılan çalışmaların uygulamaya konulmasına yönelik gerçekleştirilebilecek eylemler planlanmaktadır.

- **Siber Güvenliğin Milli Güvenliğe Entegrasyonu**: Bu stratejik eylem maddesi ile; devleti, milli ekonomiyi, kritik altyapıları ve toplumun genelini etkileyebilecek, iyi organize olmuş tehdit unsurları tarafından

[211] a.g.b. s. 15.

gerçekleştirilebilecek kasıtlı saldırıların ülkemize verebileceği zararların azaltılması veya tamamen ortadan kaldırılmasına yönelik gerçekleştirilebilecek eylemler planlanmaktadır.[212]

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kamu bilişim sistemleri ile kamu ve özel sektöre ait kritik altyapıların yanı sıra küçük ve orta ölçekli sanayi kuruluşları, tüm özel ve tüzel kişilerin de dâhil edildiği ulusal siber uzayın tüm unsurlarını kapsayan kapsamlı bir strateji belgesi niteliği taşımaktadır.

4.2.3. KamuNet Projesi

Siber Güvenlik Kurulu kararları kapsamında "Kamu Kurum ve Kuruluşlarının KamuNet'e Dâhil Edilmesi" konulu 2016/28 sayılı başbakanlık genelgesi yayımlanmıştır. KamuNet (Kamu Sanal Ağı) kamu kurum ve kuruluşlarının daha güvenli bir ağ üzerinden hızlı bir şekilde veri haberleşmesi gerçekleştirebilmelerine imkân tanımaktadır. Projenin çalışmaları UDHB ile Türk Telekom arasında imzalanan iş birliği protokolüne göre yürütülmektedir.

KamuNet internet ortamına kapalı, fiziksel ve siber saldırılara karşı risklerin azaltıldığı güvenli bir sanal ağdır. KamuNet Projesi ile kamu kurumları arası veri iletişiminde standardın sağlanması, e-Devlet hizmetlerinin güvenli bir şekilde sunulması, ortak veri merkezlerinin oluşturulması ve hâlihazırda kullanılan bulut hizmetlerinin internete kapalı güvenli bir ortamdan gerçekleştirilmesi amaçlanmaktadır.[213]

[212] a.g.b. s. 15.
[213] http://www.udhb.gov.tr/doc/siberg/KamuNetgenelgesi.pdf (17.02.2018)

4.3. YASAL DÜZENLEMELER

İnternet altyapısının gelişmesiyle birlikte birçok kritik altyapı hizmetine erişim kolaylaşmış ve sunulan hizmetlerin hızı artmıştır. Ancak siber ortamda günden güne artan tehditler güvelik problemlerini de beraberinde getirmiştir. Ülkemizde siber ortamda bilgi güvenliğini sağlamak amacıyla alınan birçok güvenlik önleminin yanı sıra mevzuatta da birtakım düzenlemeler yapılmıştır.

4.3.1. 5237 Sayılı TCK'da Bilişim Suçlarına Yönelik Düzenlemeler

Bilişim suçları, Türk Hukuk Sistemi'nde 1990'lı yıllardan itibaren yapılan düzenlemelerle yasal boyut kazanmaya başlamıştır. İlk olarak 765 sayılı Türk Ceza Kanunu'na (TCK) "Bilişim Alanında Suçlar" adlı bir bap eklenerek 6 Haziran 1991 tarihinde yürürlüğe girmiştir.

2000'li yıllara gelindiğinde bilişim sistemlerinin yaygınlaşması, bilgisayar ve internet kullanımının artması, bankacılık ve finans hizmetlerinin dijital ortama aktarılması sonucu mevcut TCK'daki eksiklikler göz önünde bulundurularak 26.09.2004 tarihli ve 5237 sayılı TCK kabul edilmiştir. Bilişim suçları 5237 sayılı TCK'da "Bilişim Alanında Suçlar" başlığı altında (Madde 243-246) ve "Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında (Madde 135, 136 ve 138) ele alınmıştır. Kanunun bahsedilen maddeleri ile düzenlenen suçlar özellikle bilişim sistemleri aracılığıyla işlenebilen, bilişim sistemleri dışında işlenebilme imkânı kısıtlı olan suçlardır.[214]

[214] Boğa Uğur, Bilişim Suçlarıyla Mücadele Yöntemleri, Radyo ve Televizyon Üst Kurulu Uzmanlık Tezi, 2011, Ankara, s. 73.

Bilişim suçları ile ilgili kanun maddelerini ele alacak olursak:

TCK Madde 243:

> *"(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.*
> *(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.*
> *(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."*

Birinci fıkrada herhangi bir bilişim sitemine yetkisiz veya izinsiz şekilde erişim sağlanması durumunda bir yıla kadar hapis cezası verileceğinden bahsedilmektedir. Yani eylemin suç sayılması için sisteme zarar verilmesi ya da veri hırsızlığı yapılması gerekmemektedir. Bilişim sistemine her ne sebeple erişim sağlanırsa sağlansın, bu eylem suç olarak kabul edilmektedir.

İkinci fıkrada suçun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi durumunda birinci fıkrada belirtilen cezanın yarı oranda indirilebileceğinden bahsedilmiştir ancak, burada bedeli karşılığında yararlanılabilen sistemler açıkça ifade edilmemiştir.

Üçüncü fıkrada izinsiz erişim sağlanan bilişim sisteminin verilerinin yok edilmesi veya içeriğinin değiştirilmesi durumunda birinci fıkrada yer alan cezanın ağırlaştırılacağı ifade edilmektedir.

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 adlî para cezasına hükmolunur."

Kanun maddesinin birinci ve ikinci fıkrasında bir bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi gibi eylemlerin suç teşkil ettiğinden ve bu suçlar için öngörülen cezalardan bahsedilmiştir. Belirtilen suç tanımlarıyla bilişim sistemlerinin sadece soyut unsurlarını oluşturan veriler ve yazılımlar koruma altına alınmamış; aynı zamanda bilişim sistemlerinin somut unsurlarını oluşturan donanım sistemleri de koruma altına alınmıştır.[215]

Üçüncü fıkrada, birinci ve ikinci fıkrada belirtilen ve suç teşkil eden eylemlerin bankacılık ve finans kurumlarına veya bir kamu kurum veya kuruluşuna ait sistemlere karşı işlenmesi durumunda cezaların ağırlaştırılacağı ifade edilmiştir. Dördüncü fıkrada, birinci ve ikinci fıkrada belirtilen suç teşkil eden eylemlerin kişinin kendisi veya başkasının yararına haksız çıkar sağlaması suç olarak tanımlanmıştır.

TCK Madde 245:

"*(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.*
(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır."

Kanun maddesinin birinci ve ikinci fıkrasında başkasına ait bir banka veya kredi kartının her ne şekilde olursa olsun ele geçirilmesi, kullanılması veya

[215] a.g.t. s. 76-77.

kullandırılması sonucu kişinin kendisine veya başkasına yarar sağlanması durumu suç olarak kabul edilmiştir.

TCK Madde 246:

> "*(1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*"

Bu maddede 243, 244 ve 245. maddelerde düzenlenen suçlarla ilgili tüzel kişiler hakkında uygulanacak güvenlik tedbirleri ortak olarak ele alınmıştır. Bu maddeyle birlikte tüzel kişilerin önceki üç maddede tanımlanan suçları işleyerek haksız menfaat sağlamaları durumunda tüzel kişiler hakkında bunlara özgü uygulanacak güvenlik tedbirleri hüküm altına alınmıştır.

TCK Madde 135:

> "*(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.*
> *(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.*"

Bu maddeyle her türlü kişisel verinin hukuka aykırı şekilde kaydedilmesi suç olarak kabul edilmiştir.

TCK Madde 136:

> "*(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.*"

Bu maddeyle hukuka aykırı olarak kişisel verilerin bir başkasına verilmesi, yayılması veya ele geçirilmesi suç olarak kabul edilmiştir. Söz konusu hukuka aykırı

eylemlerin hangi yollarla ya da hangi ortamlarda yapılacağı belirtilmediği için kanun maddesi kapsayıcı niteliktedir. Böylelikle kişisel verilerin gizliliğinin en çok istismar edildiği internet ortamındaki hukuksuz eylemler kanun maddesiyle suç olarak hüküm altına alınmıştır.

TCK Madde 138:

> "*(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.*"

Günümüzde birçok hizmetin BİT altyapıları kullanılarak sunulduğu kamuda ve özel sektörde vatandaşlara ait elde edilen verilerin kanunun öngördüğü süre boyunca yasal olarak saklanması ve sürenin bitiminde söz konusu verilerin yok edilmesi zorunludur. Belirtilen süre içerisinde verilerin yok edilmemesi durumunda sorumluların görevlerini yerine getirmeyerek suç işledikleri hüküm altına alınmıştır.

Yukarıda belirtilen maddeler dışında nitelikli hırsızlık (Madde 142/2-e), dolandırıcılık (Madde 158/1-f), müstehcenlik (Madde 226), haberleşmenin engellenmesi (Madde 124), haberleşmenin gizliliğini ihlal (Madde 132), kişiler arasındaki konuşmanın dinlenmesi veya kayda alınması (Madde 133) ve hakaret (Madde 125) gibi suçların bilişim sistemleri vasıtasıyla işlenmesi de bilişim suçu olarak nitelendirilmiştir.[216]

4.3.2. 5809 Sayılı Elektronik ve Haberleşme Kanunu

5809 Sayılı Elektronik ve Haberleşme Kanunu 10.11.2008 tarihli ve 27050 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Elektronik ve Haberleşme Kanununun 4'üncü maddesinde yer alan ilkelerin (I) bendinde elektronik ve

[216] Güngör Murat, Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, Kalkınma Bakanlığı Uzmanlık Tezi, 2015, s. 99.

haberleşme hizmetlerinin sunulması ve bu hususta yapılacak düzenlemelerde "*Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi.*" hüküm altına alınmıştır.[217] Aynı kanunun 12'nci maddesinde işletmecilerin hak ve yükümlülükleri düzenlenmiştir. Bu kanun maddesinde işletmecilere (Madde 12/2-d) "*Kişisel veri ve gizliliğin korunması.*" hususunun sağlanması görevi verilmiştir. Böylelikle elektronik ve haberleşme hizmetlerinin sunulmasında kişisel verilerin ve gizliliğin korunması hususları hüküm altına alınmıştır.[218]

4.4.3. 5070 Sayılı Elektronik İmza Kanunu

5070 sayılı Elektronik İmza Kanunu 23.01.2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Kanunda tanımlanan şekliyle elektronik imza; "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi*" ifade etmektedir. Elektronik imzanın güvenliği, imza sahibinin imza doğrulama verisi ve kimlik bilgilerini birbirine bağlayan elektronik sertifika ile sağlanmaktadır. Böylelikle bir bilginin; bütünlüğü bozulmadan, tarafların kimlik doğrulaması gerçekleştirilerek gönderici ve alıcı arasında iletimi gerçekleştirilmektedir. 5070 sayılı Elektronik İmza Kanunu ile elektronik imzanın hukukî yapısı, elektronik sertifika hizmet sağlayıcılarının faaliyetleri ve her alanda elektronik imzanın kullanımı ile ilgili işlemler düzenlenmektedir.[219]

4.4.4. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 23.05.2007 tarihli ve 26530 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Bu kanunla

[217] a.g.t. s. 99.
[218] 5809 Sayılı Elektronik Haberleşme Kanunu, (2008), T.C. Resmi Gazete, 27050, 10/11/2008.
[219] 5070 Sayılı Elektronik İmza Kanunu (2004), T.C. Resmi Gazete, 25355, 23/1/2004.

Türk hukukunda ilk kez internet ortamına düzenleme getirilmiştir.[220] Bu kanunda içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen çeşitli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin usul ve esaslar düzenlenmektedir.

4.4.5. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanununun 72'nci maddesi[221], bir bilgisayar programının hukuka aykırı bir şekilde çoğaltılmasının önüne geçmek amacıyla oluşturulan programların etkisiz kılınmasına yönelik program ve teknik donanımları üreten, satan ve kişisel amacı dışında kullananlara yönelik birtakım düzenlemeleri içermektedir.

4.4.6. 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

6698 Sayılı Kişisel Verilerin Korunması Kanunu 07.04.2016 tarihli ve 29677 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. KVKK, kişisel verilerin işlenmesi[222] hususunda başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen tüzel ve özel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektedir. KVKK'nın 19 uncu maddesi kapsamında kişisel verilerin korunması hususunda kanunda verilen görevleri yerine getirmek üzere kamu tüzel kişiliğine sahip Kişisel Verileri Koruma Kurumu kurulmuştur.

---

[220] BOĞA, s. 81.

[221] **Madde 72 - (Değişik: 23/1/2008-5728/139 md.):** *Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır.*

[222] **KVKK Madde 3-(d)** *Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*dir.

4.4. 2017 GCI RAPORUNDA TÜRKİYE'NİN DURUMU

ITU tarafından ülkelerin siber güvenlik kapasitelerini ölçen GCI (Global Cybersecurity Index – Küresel Siber Güvenlik Endeksi) raporunun ilki 2015 yılında yayınlanmıştır. GCI raporunun ikincisi ve en güncel olanı ise 2017 yılında yayınlanmıştır.

Raporda ülkeler, siber güvenlik alanında faaliyetleri bakımından üç kategoriye ayrılmaktadırlar. Kırmızı kategoride yer alan devletler siber güvenlik alanında henüz çalışmalara başlamamış veya çalışmaları yetersiz olan ülkeleri; sarı kategoride yer alan ülkeler siber güvenlik alanında çalışmalarına başlamış ve bu alanda gelişim göstermekte olan ülkeleri; yeşil kategoride yer alan ülkeler ise siber güvenlik alanında iyi durumda olan ülkeleri belirtmektedir.[223]

GCI raporu, GCA (Global Cybersecurity Agenda)'da belirlenen siber güvenliğin 5 temel unsuru ve bu unsurların alt başlıklarında yer alan 25 göstergeye göre oluşturulmuştur. Ülkemizin küresel siber güvenlik endeksindeki maddelere göre gelişim seviyeleri Tablo 5'de yer almaktadır. Tabloda 25 alt göstergeye göre ülkemizin durumu ayrı ayrı gösterilmiş; yine beş temel unsura göre genel durum da ayrıca gösterilmektedir.[224]

[223] International Telecommunication Union, (2007), *Global Cybersecurity Agenda*, s. 13-15.
[224] a.g.r. , s. 5.

Tablo 5 GCI 2017 Raporunda Ülkemizin Siber Güvenlik Alanındaki Durumu[225] (Kırmızı: Kötü, Sarı: Orta, Yeşil: İyi)

GÜVENLİK MADDELERİ	KATEGORİ
Siber Suçlara Yönelik Mevzuat	
Siber Güvenlik Mevzuatı	
Siber Güvenlik Eğitimi	
KANUNİ TEDBİRLER (GENEL)	
Ulusal SOME	
Kurumsal SOME	
Sektörel SOME	
Kurumsal Standartlar	
Mesleki Standartlar	
Çocukların Korunmasına Yönelik Tedbirler	
TEKNİK TEDBİRLER (GENEL)	
Ulusal Siber Güvenlik Stratejisi	
Siber Güvenlikten Sorumlu Birim	
Siber Güvenlik Kriterleri	
KURUMSAL YAPILANMA (GENEL)	
Standardizasyon Kuruluşları	
İyi Siber Güvenlik Uygulamaları	
AR-GE Programlarına Destek	
Toplumsal Farkındalık Kampanyaları	
Mesleki Eğitim Kursları	
Milli Eğitim Programları ve Müfredat	
Teşvik Mekanizmaları	
Yerli ve Milli Üretim	
KAPASİTE GELİŞTİRME (GENEL)	
İkili Anlaşmalar	
Çok Taraflı Anlaşmalar	
Uluslararası Katılım	
Kamu-Özel Sektör İşbirliği	
Kurumlar Arası İşbirliği	
İŞBİRLİĞİ VE KOORDİNASYON (GENEL)	
KÜRESEL SİBER GÜVENLİK ENDEKSİ TÜRKİYE'NİN GENEL DURUMU	

Kanuni Tedbirler: Kanuni tedbirler kategorisinde 3 başlık altında ülkelerin siber güvenliğe yönelik yasal çalışmalarının durumu ölçülmektedir. Ülkemiz siber suçlar ve siber güvenliğe yönelik mevzuat çalışmalarında yeşil kategoride yer almaktadır. Ancak siber güvenlik eğitiminde yeterli gelişimi gösteremediği için, kırmızı

[225] a.g.r. s. 37.

kategoride yer almaktadır. Genel kanuni tedbirler anlamında ise sarı kategoride yer almaktadır; bu da ülkemizin bu alanda gelişmekte olan ülkeler arasında yer aldığını göstermektedir.

Teknik Tedbirler: Teknik tedbirler kategorisinde 5 başlık altında ülkelerin siber güvenliğe yönelik teknik çalışmalarının durumu ölçülmektedir. Ülkemiz ulusal, kurumsal ve sektörel SOME'lerin kurulmasına yönelik çalışmalar, kurumsal güvenlik standartlarının belirlenmesi ve çocukların siber ortamda korunmasına yönelik çalışmalarda yeşil kategoride yer almaktadır. Ancak siber güvenlik sektörüne yönelik mesleki standartlar konusunda kırmızı kategoride yer almaktadır. Ülkemiz, genel teknik tedbirler anlamında yeşil kategoride yer almaktadır. Alt başlıklardan bir tanesinin bile kırmızı kategoride yer alması; diğer iyi çalışmaları da olumsuz etkileyebileceği için, bu konudaki eksikliklerin de hızlıca giderilmesi önem arz etmektedir.

Kurumsal Yapılanma: Kurumsal yapılanma kategorisinde 3 başlık altında ülkelerin siber güvenlik alanında kurumsal yapılanmalarına yönelik çalışmalarının durumu ölçülmektedir. Ülkemiz bir ulusal siber güvenlik stratejisinin olması ve ulusal siber güvenlikten sorumlu birimin belirlenmiş olması sebebiyle yeşil kategoride yer almaktadır. Ancak ülkemiz ulusal siber güvenlik kriterlerinin belirlenmesi hususunda sarı kategoride yer almasına karşın; kurumsal yapılanmaya ilişkin çalışmalarda genel olarak yeşil kategoride yer almaktadır.

Kapasite Geliştirme: Kapasite geliştirme kategorisinde 8 başlık altında ülkelerin siber güvenlik kapasitelerinin durumu ölçülmektedir. Ülkemiz, siber güvenlik standardizasyon kuruluşlarının kurulması, toplumsal siber güvenlik farkındalık kampanyaları, mesleki eğitim kursları ve siber güvenlik teşvik mekanizmalarının hayata geçirilmesi çalışmalarında yeşil kategoride yer almaktadır. AR-GE programlarına devlet desteği, milli eğitim programlarında siber güvenliğe yer verilmesi ve milli siber güvenlik ürünlerinin üretilmesi çalışmalarında ise sarı kategoride yer almaktadır. Kapasite geliştirme hususunda, yalnızca iyi siber güvenlik

uygulamaları alanında kırmızı kategoride yer almaktadır. Ülkemiz, ulusal siber güvenlik kapasitesinin geliştirilmesine yönelik çalışmalarda genel olarak sarı kategoride yer almaktadır.

İşbirliği ve Koordinasyon: İşbirliği ve koordinasyon kategorisinde 5 başlık altında ülkelerin siber güvenlik alanında uluslararası işbirliği ve koordinasyon çalışmalarının durumu ölçülmektedir. Ülkemiz ikili ve çokuluslu siber güvenlik anlaşmaları, kamu-özel sektör işbirliği ve kurumlar arası işbirliği çalışmalarında kırmızı kategoride yer almaktadır. Bu kategoride yalnızca uluslararası siber güvenlik çalışmalarına katılım hususunda yeşil kategoride yer almaktadır. Tabloda görüldüğü üzere işbirliği ve koordinasyon, ülkemizin en yetersiz olduğu kategoridir.

Ülkemiz Küresel Siber Güvenlik Endeksi'nde 1 üzerinden 0.581 puanla tüm ITU üyesi ülkelerin yer aldığı listede 43'üncü sırasında yer almaktadır.[226] Ülkemiz sahip olduğu puan ve sıralamaya göre bu listede gelişim göstermekte olan ülkelerin bulunduğu sarı kategoride yer almaktadır. Raporda ülkemizin siber güvenlik eğitimi, mesleki standartlar, iyi siber güvenlik uygulamaları, devletlerarası anlaşmalar ve kamu-özel sektör işbirliği alanlarında yetersiz olduğu görülmektedir.

[226]a.g.r. s. 57.

SONUÇ VE DEĞERLENDİRME

İlk başlarda askeri amaçlı olarak geliştirilen internet ve bilgisayar ağlarının 1995 yılından itibaren tüm dünyada kullanıcılar arasında yaygınlaşmaya başlamasıyla birlikte veriler elektronik ortama aktarılmıştır. 2000'li yıllardan itibaren dünya genelinde insanların büyük bir bölümü internet altyapısı üzerinden birbiriyle bağlantı kurabilir hale gelmiştir. Özellikle mobil cihazların yaygınlaşması ve mobil cihazların bağlantı hızlarındaki artışa bağlı olarak siber ortamdaki veri trafiğinin yarıdan fazlası mobil cihazlar üzerinden gerçekleşmeye başlamıştır.

Bilişim sistemlerinin yaygınlaşması, günden güne artan veri haberleşme hızı ve sanal ortamın depolama kapasitesindeki artışa bağlı olarak; bankacılık, finans, sağlık, eğitim, ulaşım, e-devlet, e-ticaret ve bulut bilişim hizmetleri internet ortamından sunulmaya başlanmıştır. İnternet ortamından sunulan hizmetler, insanların ve devletlerin işini kolaylaştırmasının yanında birçok riski de beraberinde getirmiştir.

2016 yılı verilerine göre siber ortamda birbirine bağlı cihaz sayısı sadece OECD ülkelerinde 1 milyarı aşmış durumdadır. Bu sayının 2022 yılında 14 milyarı aşacağı tahmin edilmektedir.[227] Bu durum, her geçen gün artan sayıda ve çeşitlilikte tehdide maruz kalan siber ortamdaki bilgilerin güvenliğini sağlamak için devletler, kurumlar ve bireylere yeni sorumluluklar yüklemektedir.

Son yıllarda birçok devletin yansıra NATO, BM, AB, ITU, OECD gibi çok uluslu topluluklar siber güvenlik stratejileri ve bu konudaki eylem planlarını hazırlayarak, söz konusu strateji ve planları uygulamaya geçirmişlerdir. Siber uzay NATO tarafından kara, hava, deniz ve uzayın ardından beşinci operasyonel alan olarak

[227] http://www.milliyet.com.tr/34-ulusal-bilisim-kurultayi-ankara-yerelhaber-2478735/ (08.06.2018)

tanımlanmıştır. NATO siber uzayı operasyonel bir alan olarak tanımlamasının ardından bu konudaki çalışmalarına hız vererek müttefiklerini bilinçlendirme faaliyetlerine ağırlık vermiştir.

Siber uzay, tehdidin ne zaman ve nereden geleceğini kestirmenin zor olduğu soyut bir ortamdır. Devletlerin siber uzayda her geçen gün artan ve çeşitlenen tehditlerle tek başlarına mücadele edebilmeleri oldukça zordur. Bu yüzden siber tehditlerle etkin bir şekilde mücadele edebilmek için uluslararası iş birliği şarttır.

2013 yılında NATO, AB ve bazı devletlerin siber güvenlik stratejileri incelenerek Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı hazırlanarak yürürlüğe girmiştir. Siber uzayda artan tehditler ve edinilen tecrübeler doğrultusunda, mevcut stratejide çeşitli güncellemeler yapılarak Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı hazırlanarak yürürlüğe girmiştir. Ulusal Siber Güvenlik Stratejisinde elektronik ve haberleşme, ulaştırma, enerji, su yönetimi, kritik kamu hizmetleri, bankacılık ve finans Türkiye'nin kritik altyapı sektörleri olarak belirlenmiştir.

Türkiye jeopolitik konumu gereği yer altı kaynakları bakımından zengin, aynı zamanda da siyasi istikrarsızlıkların en fazla olduğu ülkelerle komşudur. Türkiye, askeri alanda alması gereken güvenlik tedbirlerinin yanı sıra siber güvenlik altyapısının güçlendirilmesine yönelik de birtakım tedbirler almak zorundadır. Sınırlarda Türkiye'ye yönelik olası tehditleri bertaraf etmek için kullanılan silah sistemleri ne kadar önemliyse; örneğin Borsa İstanbul (BIST) bilişim altyapısında yer alan bir firewall (güvenlik duvarı) cihazı da siber uzaydaki tehditleri bertaraf etmek adına en az sınırdaki silah sistemleri kadar önemlidir.

2017 yılında ITU tarafından ülkelerin siber güvenlik alanında yasal, teknik, kurumsal, uluslararası iş birliği gibi faaliyetleri ile ilgili ölçümlerin yapıldığı Küresel

Siber Güvenlik Endeksi'nde Türkiye 43'üncü sırada yer almaktadır.[228] 3.5 trilyon dolarlık dünya siber güvenlik pazarında Türkiye'nin payı sadece %1'dir.[229] 2017 verilerine göre dünyanın en büyük 17'nci ekonomisi konumunda olan Türkiye, siber güvenlik pazar payında bu rakamın oldukça gerisinde kalmaktadır.

Türkiye'de kritik altyapılar da dâhil olmak üzere tüm bilişim sistemlerinde %97 oranında yabancı menşeli yazılım kullanılmaktadır.[230] Rakamlar da göstermektedir ki siber güvenlik sektöründe kullanılan yerli ve milli yazılımların oranı çok azdır.

Türkiye en fazla siber saldırı gerçekleştiren ve en fazla siber saldırıya uğrayan devletler sıralamasında dünyada ilk 10'da yer almaktadır.[231] Bunun en önemli sebebi ülkemizde yaygın olan köle bilgisayar ağlarıdır. Ülkemizde lisanssız yazılım kullanımının yaygın olması ve internete bağlı cihazlarda antivirüs programı kullanım oranının düşük olması; tüm bu cihazları siber uzaydaki tehditlere açık hale getirmektedir.

Siber ortamda tam anlamıyla güvenliği sağlamak için bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunması gerekmektedir. Bu sürece dâhil olan insan faktörü, güvenlik zincirinin en zayıf halkasını oluşturmaktadır. Bir sistemde en son teknoloji ile donatılmış güvenlik ürünleri dahi kullanılsa; insanın zafiyet göstermesi durumunda, kullanılan güvenlik ürünlerinin pek bir önemi kalmamaktadır.

Dünya genelinde sosyal medya kullanıcıların toplam nüfusa oranı %37 iken, Türkiye'de aktif sosyal medya kullanıcıları ülke nüfusun %60'ını oluşturmaktadır.[232]

---

[228] International Telecommunication Union, (2017), *Global Cybersecurity Index 2017*, ITU, s. 57.
[229] CyberMag Dergisi (2017), Sayı 18, s. 7.
[230] http://www.iha.com.tr/haber-siber-guvenlik-pazarinin-yuzde-97si-yabancilarda-619115/ (08.06.2018)
[231] https://www.aa.com.tr/tr/turkiye/kamu-bilisimcileri-siber-guvenligi-tartisacak/1096284 (08.06.2018)
[232] http://www.dijitalajanslar.com/internet-ve-sosyal-medya-kullanici-istatistikleri-2017/ (08.06.2018)

Siber risklerin en fazla barındığı ve yayılım gösterdiği mecralar olan sosyal medya uygulamalarının kullanımına ilişkin toplumun bilinçlendirilmesi çok önemlidir.

ÖNERİLER

Uluslararası İşbirliği

Ülkemiz, NATO bünyesinde siber güvenlik faaliyetleri yürütmekte olan Siber Güvenlik Mükemmeliyet Merkezi benzeri ortak siber güç oluşumları içinde aktif olarak yer almalıdır. Konunun uzmanlarının yer aldığı ortak AR-GE çalışmalarında edinilen tecrübeler ülkemize aktarılmalıdır.

Dünyanın birçok ülkesinden üst düzey siber güvenlik uzmanlarından oluşan ITU bünyesinde bulunan Yüksek Seviyeli Uzmanlar Grubu'nda ülkemizin üyesi bulunmamaktadır. Ülkemiz bu gruba dâhil olarak dünyada siber güvenlik alanındaki en güncel çalışmaları yakından takip etmelidir.

Ülkemizin, ITU tarafından yayınlanan 2017 Küresel Siber Güvenlik Endeksi'nde uluslararası alanda siber güvenlik konusunda devletlerarası ikili ve çoklu işbirliği faaliyetlerinde geride kaldığı görülmektedir. Siber güvenlik konusunda uluslararası alanda iyi durumda olan dost ülkelerle ikili ve çoklu işbirliğini arttırmaya yönelik faaliyetlere ağırlık verilmelidir.

Nitelikli İnsan Kaynağı, Yerli ve Milli Siber Güvenlik Ürünleri

Sürdürülebilir bir bilgi güvenliği ve siber güvenliğin sağlanabilmesi için kullanılan tüm yazılımların yerli ve milli olması önem arz etmektedir. Başta kamu bilişim sitemleri altyapısı ve kritik altyapı sektörlerinde kullanılan yazılımların yerli ve millilik oranının arttırılması gerekmektedir.

Siber güvenlik alanında nitelikli insan kaynağı yetiştirilmesi ve milli siber güvenlik ürünlerinin geliştirilmesi için, devlet tarafından çeşitli teşvik programları hazırlanarak bu alanda yapılan AR-GE çalışmaları desteklenmelidir.

Kritik Altyapı Sektörleri ve Sektörler Arası İşbirliği

Kritik altyapı sektörleri görev alanlarına göre sınıflandırılarak, sektöre özel güvenlik stratejileri belirlenmesi gerekmektedir. Çünkü her sektörün sahip olduğu sistemler ve varlıklar diğerlerinden farklılık göstermektedir. Sektöre özel hazırlanan yol haritaları ilgili birimlerce takip edilerek, durum bilgisi düzenli olarak yöneticilere raporlanmalıdır.

Başta kritik altyapı sektörleri olmak üzere tüm kamu ve özel sektör BİT sistemlerinin güvenliğini sağlamaya yönelik çalışmalarda uluslararası standartlar göz önünde bulundurularak, sektörler arası iş birliğine önem verilmelidir.

KamuNet Projesi

Kamu kurum ve kuruluşlarının veri haberleşmesinin internete kapalı bir sanal ağ üzerinden siber güvenlik risklerinin minimize edilerek sağlanmasına olanak sağlayacak KamuNET Projesi çalışmalarına hız verilerek, tüm kamu kurum ve kuruluşları ile kritik altyapı sektörlerinin en kısa zamanda bu güvenli ağa dâhil edilmesi Türkiye'nin ulusal güvenliği açısından kritik öneme sahiptir.

Ulusal Siber Güvenlik Stratejisi

Ulusal Siber Güvenlik Stratejisi gelişen güvenlik teknolojileri ve artan siber tehditlere bağlı olarak sürekli güncel tutulmalıdır. Kapsamlı ve geniş katılımlı bir siber güvenlik stratejisi hazırlanabilmesi için sürece kamu, özel sektör ve üniversitelerin temsilcileri de dâhil edilmelidir.

Toplumsal Siber Güvenlik Farkındalığı

Vatandaş, kamu ve özel sektör kurumlarının tamamını kapsayan siber güvenlik farkındalık programları oluşturularak toplumun bilinçlendirilmesi gerekmektedir. RTÜK ve BTK kurumlarının iş birliğinde siber güvenlik, siber zorbalık, bilinçli sosyal medya kullanımı gibi konularda hazırlanacak kamu spotlarının toplumda siber güvenlik farkındalığının oluşturulmasına katkısı olacaktır.

Eğitim ve Müfredat

Ülkemizde siber güvenliğe yönelik eğitimler büyük oranda yükseköğretim seviyesinde verilmektedir. Toplumumuzda siber güvenlik kültürünün oluşması, yerli ve milli yazılımların geliştirilebilmesi için; Güney Kore gibi ülkeler örnek alınarak "Siber Güvenlik Farkındalığı" ve "Kodlama" derslerinin zorunlu hale getirilerek ilkokuldan itibaren müfredata girmesi gerekmektedir.

Yasal Altyapı

Siber ortamda işlenen suçların yöntemi, çeşitliliği ve etkilediği kitle günden güne artış göstermektedir. Bu sebeple ülkemizde bilgi güvenliği ihlalleri ve siber uzayda işlenen suçlara ilişkin yasal altyapı yeniden gözden geçirilmelidir. Siber güvenliğin sağlanması ve siber suçların önlenebilmesi için uluslararası alanda yapılan yasal çalışmalar da göz önünde bulundurularak; kapsamlı ve güncel bir yasal altyapının oluşturulması önem arz etmektedir.

KAYNAKÇA

Altundal, Ömer Faruk (2012), *DDoS nedir, ne değildir?*, Siber Güvenlik Derneği Yayını, Ankara.

Atluri, Anoop Chowdary ve Tran, Vinh (2017), "Botnets Threat Analysis and Detection", *Springer International Publishing AG 2017/ I. Traoré et al. (eds.), Information Security Practices.* https://www.springer.com/gp (15.10.2018)

Bishop, Matt (2005), "*Introduction to Computer Security"*, Pearson Education, Inc., Boston. http://iips.icci.edu.iq/images/exam/Introduction-to-Computer-Security-pdf-DONE.pdf (03.04.2018)

Boğa, Uğur (2011), *Bilişim Suçlarıyla Mücadele Yöntemleri*, Radyo ve Televizyon Üst Kurulu Uzmanlık Tezi, Ankara.

Canbek, Gürol ve Sağıroğlu, Şeref (2006), "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Gazi Üniversitesi Politeknik Dergisi*, Cilt: 9 Sayı: 3 s. 165- 174.

Commıssıon Of The European Communıtıes (2004), *Critical Infrastructure Protection in the fight against terrorism*, EC, Brussels. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (01.05.2018)

Çetinkaya, Mehtap (2008), "Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması", *Akademik Bilişim 2008*, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak-01 Şubat 2008.

Devlet Planlama Teşkilatı (2006), *Bilgi Toplumu Stratejisi (2006-2010),* DPT, Ankara. (http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf (11.03.2018)

Duggan Maeve, Smit Aaron ve Caiazza Tom (2017), *Online Harassment 2017 Report*, Pew Research Center. http://www.pewinternet.org/2017/07/11/online-harassment-2017/ (15.05.2018)

Matrosov, Aleksandr, Rodionov, Eugene, Harley, David ve Malcho, Juraj (2010), *Stuxnet Under The Microscope Revision 1.1*, ESET https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf - (10.02.2018)

French National Digital Security Strategy (2015). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (11.05.2018)

Güngör, Murat (2015), *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, Uzmanlık Tezi, Kalkınma Bakanlığı, Ankara.

Gündüz, M. Zekeriya ve Daş, Resul (2017), "Sosyal Mühendislik ve Korunma Yolları", *CyberMag Dergisi,* Sayı 18.

Gürkaynak, Muharrem ve İren, Adem Ali (2011) *"*Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler*" Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* Cilt: 16, Sayı: 2, s. 263-279.

Henkoğlu, Tülay (2015), "*Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi*", Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi, Ankara.

Henkoğlu, Türkay ve Yılmaz, Bülent (2013), "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", *Türk Kütüphaneciliği 27, 3 Hakemli Yazılar*, s. 451-471.

International Multilateral Partnership Against Cyber Threats (2011), *IMPACT Activities (2008-2011),* IMPACT, Cyberjaya. https://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf (13.05.2018)

International Telecommunication Union (2007), *Global Cybersecurity Agenda,* ITU, Geneva.

International Telecommunication Union, (2017), *Global Cybersecurity Index 2017,* ITU, Geneva.

Kalkınma Bakanlığı (2013), *Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010) Nihai Değerlendirme Raporu*, Kalkınma Bakanlığı, Ankara.

Kalkınma Bakanlığı (2015), *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı*, Kalkınma Bakanlığı, Ankara.

Kara Mahruze, (2013), *Siber Saldırılar - Siber Savaşlar ve Etkileri*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul.

Kasapoglu, Can (2017), "Cyber Security: Understanding The Fifth Domain", *EDAM Cyber Policy Paper Series* 2017/1.

Keleştemur, Atalay (2015), *Siber İstihbarat*, Level Kitap Umuttepe Yayınları, İstanbul.

Lewis, James A. ve Timlin, Katrina (2011) *"Cybersecurity and Cyberwarfare"* The Center for Strategic and International Studies.

Maconachy W. Victor, Schou Corey D. , Ragsdale Daniel ve Welch Don (2001), *A Model for Information Assurance: An Integrated Approach,* Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 Haziran.

Meral Mehmet (2008), *Siber Savunma: Ülkeler ve Stratejiler*, 3. Uluslararası Katılımlı Bilgi Güvenliği Ve Kriptoloji Konferansı Bildiriler Kitabı s. 257-262.

Meral Mustafa, (2015), *Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi*, Harp Akademileri Stratejik Araştırmalar Enstitüsü Yüksek Lisans Tezi, İstanbul.

Microsoft Security Intelligence Report (2017), *Volume 22 (January-March 2017),* Microsoft.

North Atlantic Treaty Organization (2016), *Fact Sheet*, Public Diplomacy Division (PDD) – Press & Media Section NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf (05.05.2018)

O'brien, Dick (2017) *Internet Security Threat Report – Ransomware 2017*, Symantec.

Öğün, Mehmet Nesip ve Kaya, Adem (2013), "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri Dergisi*, Yıl: 9, Sayı: 18, s. 145-181.

Önel, Dinçer ve Dinçkan, Ali (2007), *Bilgi Güvenliği Yönetim Sistemi Kurulumu*, TÜBİTAK UEKAE, Kocaeli.

Özenç Uçak, Nazan (2010), "Bilgi: Çok Yüzlü Bir Kavram", *Türk Kütüphaneciliği*, Sayı: 24, No: 4, s. 705-722.

Richter, Felix (2017) "*200,000+ Systems Affected by WannaCry Ransomware Attack*" https://www.statista.com/chart/9399/wannacry-cyber-attack-in-numbers/ (12.02.2018)

Sarı, Emre (2016), *Geçmişten Günümüze Felsefe*, Nokta E-Book Publishing Kitap Yayınları, Antalya.

Siboni, Gabi ve Assaf, Ofer (2016) "*Guidelines for a National Cyber Strategy"*, Institute for National Security Studies, Memorandum No. 153.

Solomon, Michael G. ve Cahapple, Mike (2005), *Introducing Computer and Network Security*, Jones and Barlett Publishers.

Symantec, (2012), *"Rootkits"*. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/rootkits-12-en.pdf (16.10.2018)

UK Office of Cyber Security (2016), *National Cyber Security Strategy of the United Kingdom 2016-2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (15.04.2018)

UK Prime Minister's Office (2010), *Strong Britain in an Age of Uncertainty: The National Security Strategy*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (16.04.2018)

Ulaştırma Bakanlığı (1999), *Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) Sonuç Raporu*, Ulaştırma Bakanlığı, Ankara.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2015), *2016-2019 Ulusal Siber Güvenlik Stratejisi*, UDHB, Ankara. http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (20.02.2018)

Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2013), *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, UDHB, Ankara. (http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf (17.02.2018)

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2014), *Kurumsal SOME Kurulum Rehberi*, UDHB, Ankara. http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf (23.02.2018)

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2014), *Sektörel SOME Kurulum Rehberi*, UDHB, Ankara. http://www.udhb.gov.tr/doc/siberg/Sektorel_SOME_Reh.docx (23.02.2018)

Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT) (2014), *DDos El Kitabı*, BTK-TİB, Ankara.

USA Department of Defense (2015), *Fact Sheet: The Department of Defense (DoD) Cyber Strategy*.

https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf (15.04.2018)

Vural, Yılmaz ve Sağıroğlu, Şeref (2008), "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi* Cilt 23, No. 2, s. 507-522.

Yıldız, Mithat (2014), *Siber Suçlar ve Kurum Güvenliği,* Ulaştırma Denizcilik ve Haberleşme Bakanlığı Yayımlanmış Denizcilik Uzmanlık Tezi, Ankara.

5809 Sayılı Elektronik Haberleşme Kanunu, (2008), T.C. Resmi Gazete, 27050, 10/11/2008.

5070 Sayılı Elektronik İmza Kanunu (2004), T.C. Resmi Gazete, 25355, 23/1/2004.

İNTERNET SİTELERİ

http://www.tdk.gov.tr (29.03.2018)

http://www.siber.pol.tr/Sayfalar/hakkimizda.aspx (21.05.2018)

http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi (22.02.2018)

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (02.05.2018)

https://www.ria.ee/x-tee/fact/#eng (12.02.2018)

http://www.iha.com.tr/haber-siber-guvenlik-pazarinin-yuzde-97si-yabancilarda-619115/ (08.06.2018)

http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/epcip_presentation_/epcip_presentation_en.pdf (01.05.2018)

http://www.hurriyet.com.tr/gundem/cin-super-gizli-ordusunu-acikladi-17884879 (15.03.2018)

https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Siber-Guvenlik-Stratejisi-ve-Eylem-Plani (20.02.2018)

http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ (11.02.2018)

http://www.tuicakademi.org/stuxnet-virusu-iran-a-nasil-etki-etti/ (09.02.2018)

https://www.military.com/defensetech/2008/09/23/iranian-cyber-warfare-threat-assessment (15.12.2017)

https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (13.02.2018)

http://www.bbc.com/turkce/haberler-39906717 (13.02.2018)

https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (01.05.2018)

http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/avrupa-icin-sayisal-gundem/eavrupa/ (27.02.2018)

http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml (12.02.2018)

http://www.dw.com/tr/iran-siber-polis-ordusu-kurdu/a-14782649 (15.12.2017)

https://www.timeturk.com/iran-in-uluslararasi-silahi-siber-saldirilar/haber-93495 (15.12.2017)

https://www.gov.uk/government/policies/cyber-security (06.01.2018)

http://www.itrade.gov.il/turkey/israil-siber-guvenlikte-kuresel-pazar-payinin-8ine-sahip/ (09.01.2018)

https://siberbulten.com/strateji-guvenlik/2040/ (23.01.2018)

http://www.cagataycebi.com/security/bilgi_guvenligi.pdf (03.04.2018)

https://www.ntv.com.tr/turkiye/ortadoguyu-alarma-geciren-virus-flame,8X_pXRhHnkCbotEqgKFsLw (10.02.2018)

http://www.haberturk.com/gundem/haber/557436-siber-teror-kirmizi-kitapta (22.02.2018)

http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi (22.02.2018)

http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (15.02.2018)

http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm (15.02.2018)

https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK-KURULU (15.02.2018)

https://www.btk.gov.tr/tr-TR/Kurumdan-Haberler/Siber-Guvenlik-Kurulu-Toplandi (15.02.2018)

http://www.hurriyet.com.tr/hirsiz-virus-alarmi-21197087 (10.02.2018)

https://www.ssm.gov.tr/website/contentlist.aspx?PageID=1083&LangID=1 (21.02.2018)

https://ccdcoe.org/un.html (17.10.2018)

https://www.itu.int/en/action/cybersecurity/Pages/default.aspx (17.10.2018)

https://www.itu.int/itunews/manager/display.asp?lang=en&year=2008&issue=06&ipage=05&ext=html (17.10.2018)

http://www.cybersecuritygateway.org/pdf/Members%20of%20the%20ITU%20High%20Level%20Experts%20Group.pdf (17.10.2018)

https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/ (03.04.2018)

http://www.gazetevatan.com/mossad-cia-virusu-iran-i-vurdu-331204-dunya/ (10.02.2018)

https://www.itu.int/en/cop/Pages/about_cop.aspx (17.10.2018)

http://www.haberturk.com/haber/haber/592070-irani-vuran-virus-israilde-uretilmis (10.02.2018)

https://tr.wikipedia.org/wiki/ENIAC (13.09.2017)

https://tr.wikipedia.org/wiki/ARPANET (13.09.2017)

http://www.isokalitebelgesi.com/bilgi-nedir-bilgi-guvenligi-nedir-bilgi-guvenligi-yonetim-sistemi-nedir (05.04.2018)

http://www.iso27001security.com/html/27001.html (06.04.2018)

http://www.hurriyet.com.tr/abd-rusyaya-karsi-muttefikleri-icin-milyarlar-harcayacak-40052448 (11.01.2018)

http://www.isaca.org/education/upcoming-events/documents/intro-cobit5.pdf (30.10.2017)

http://siberest.com.tr/botnet-nedir/ (15.10.2018)

http://www.mugla.pol.tr/fethiye/Sayfalar/Botnet-Nedir.aspx (15.10.2018)

http://www.udhb.gov.tr/doc/siberg/KamuNetgenelgesi.pdf (17.02.2018)

https://en.wikipedia.org/wiki/Sony_Pictures_hack (14.02.2018)

http://www.hurriyet.com.tr/teknoloji/sony-hacklendi-vizyona-girmeyen-filmler-torrente-dustu-27691925 (14.05.2018)

http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (19.04.2018)

http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ (20.04.2018)

https://tr.wikipedia.org/wiki/Cobit (30.10.2017)

https://tr.wikipedia.org/wiki/Bilgi_Teknolojisi_Altyapı_Kütüphanesi (19.04.2018)

https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf (31.10.2017)

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (04.11.2017)

https://www.turkcebilgi.com/sibernetik (22.04.2018)

http://www.tdk.gov.tr - (08.11.2017)

http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf (12.12.2017)

https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html (12.12.2017)

http://bidb.itu.edu.tr (12.11.2017)

https://en.wikipedia.org/wiki/Trojan_horse_(computing) (12.11.2017)

http://www.bilgimikoruyorum.org.tr/?b323_sosyal_muhendislikte_kullanilan_saldiri_yontemleri (24.12.2017)

https://www.trendmicro.com.tr/media/resource_lib/social/5-reasons-why-social-engineering-tricks-work-tr.pdf (24.12.2017)

http://www.hurriyet.com.tr/telefonla-dolandiricilara-milyonlarca-lira-kaptirdik-37247480 (24.12.2017)

http://www.samsung.com/tr/sosyal-sorumluluk/siber-zorba-olma/ (26.12.2017)

http://www.haberturk.com/yasam/haber/1522728-can-almaya-baslayan-siber-zorbalik-cagin-sorunu-olmaya-aday (26.12.2017)

https://www.verisign.com/assets/infographic-ddos-trends-Q12017_tr_TR.pdf (23.04.2018)

http://www.milliyet.com.tr/34-ulusal-bilisim-kurultayi-ankara-yerelhaber-2478735/ (08.06.2018)

https://www.verisign.com/assets/infographic-ddos-trends-Q22017_tr_TR.pdf (23.04.2018)

http://www.vodafone.com.tr/VodafoneHakkinda/zararli-yazilimlar.php (15.11.2017)

http://www.hurriyet.com.tr/siber-zorbaliga-yuzde-20-maruz-kaliyor-40664423 (27.12.2017)

https://www.cnnturk.com/teknoloji/siber-zorba-olma-farkina-var-hareketi-basladi (27.12.2017)

http://www.milliyet.com.tr/abd-yi-karistiran-intihar/dunya/detay/1763540/default.htm (28.12.2017)

https://www.tbd.org.tr/kurumsal/tanitim/ (12.11.2018)

ÖZET

Toplumların internet altyapısı ve bilişim sistemlerine bağımlılıkları günden güne artmaktadır. Teknolojinin gelişmesi ve internet bağlantı hızlarının artışına bağlı olarak sunulan birçok hizmet ve önemli bilgi sanal ortama aktarılmıştır. Özellikle 2000'li yıllardan itibaren sanal ortamda sunulan hizmetlerin ve bu ortamda saklanan verilerin güvenliği bireyler, kurumlar ve devletler için önemli hale gelmiştir.

Bu tez çalışmasında; siber uzayda artan tehdit ve risklere dikkat çekilerek, uluslararası alanda gerçekleştirilen büyük siber saldırılar ve veri hırsızlığı olaylarından bahsedilmiştir. Uluslararası alanda bilgi güvenliği ve siber güvenlik çalışmalarıyla ön plana çıkan NATO, AB ve BM gibi uluslararası kuruluşlar ile bazı devletlerin bu alanlardaki faaliyetleri incelenmiştir. Ardından Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve bu alanda yapılan faaliyetler incelenerek, değerlendirmelerde bulunulmuştur.

Yapılan araştırmalar ve incelemeler sonucunda Türkiye'de bilgi güvenliği ve siber güvenlik alanında yapılan çalışmaların eksiklikleri saptanmış; bundan sonra bu alanda yapılabilecek çalışmalara ilişkin çeşitli önerilerde bulunulmuştur.

ARŞİV Kayıt Bilgileri

Tezin Adı	Bilgi Güvenliği Uygulamaları ve Çözüm Önerileri
Tezin Yazarı	Seyda MENTEŞ
Tezin Danışmanı	Şahin AY
Tezin Konumu	Uzmanlık Tezi
Tezin Tarihi	Kasım 2018
Tezin Alanı	Bilişim Sistemleri Güvenliği
Tezin Yeri	RTÜK – ANKARA
Anahtar Kelimeler	Siber Güvenlik, Bilgi Güvenliği, Türkiye'de Bilgi Güvenliği, Ulusal Siber Güvenlik Stratejisi

ABSTRACT

The dependence of societies on internet infrastructure and information systems is increasing day by day. Due to the development of technology and the increase in internet connection speeds, many services and important information have been transferred to virtual environment. Especially since 2000, the services provided in the virtual environment and the security of the data stored in this environment have become important for individuals, institutions and states.

In this thesis study; has been drawn attention to the increasing threats and risks in cyberspace, and the phenomena of massive cyber attacks and data thefts on the international scene have been mentioned. International organizations such as NATO, the EU and the United Nations (UN), as well as some governments' activities in this area, which are at the forefront of information security and cyber security work on the international scene, have been examined. Following Turkey's National Cyber Security Strategy and assessing the activities carried out in this area have been made in evaluation.

Research and analysis results in information security and the lack of studies in the field of cyber security in Turkey detected; various suggestions have been made about the work that can be done in this area from now on.

Key Words: Cyber Security, Information Security, Information Security in Turkey, National Cyber Security Strategy

ÖZGEÇMİŞ

Seyda MENTEŞ, 1991 yılında Muğla ili, Fethiye ilçesinde doğdu. İlköğrenimini Fethiye Merkez Atatürk İlköğretim Okulu'nda, ortaöğrenimini ise Fethiye Mehmet Erdoğan Anadolu Lisesi'nde tamamladı. 2014 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümü'nü, 2016 yılında da Anadolu Üniversitesi Kamu Yönetimi Bölümü'nü bitirdi. 2014-2015 yılları arasında özel sektörde mühendis olarak çalıştı. 2015 yılı Nisan ayında Radyo ve Televizyon Üst Kurulu'nda Üst Kurul Uzman Yardımcısı olarak göreve başladı.

2017 yılında başlamış olduğu Eskişehir Osmangazi Üniversitesi İşletme Bölümü'nde yüksek lisans eğitimine devam etmektedir. İyi derecede İngilizce bilen MENTEŞ, evli ve 1 çocuk babasıdır.