T.C
Radyo ve Televizyon Üst Kurulu

İNGİLTERE VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKA YAKLAŞIMLARININ KARŞILAŞTIRILMASI

UZMANLIK TEZİ

Sena NEZGİTLİ

ANKARA

HAZİRAN / 2021

T.C
Radyo ve Televizyon Üst Kurulu

İNGİLTERE VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKA YAKLAŞIMLARININ KARŞILAŞTIRILMASI

UZMANLIK TEZİ

Sena NEZGİTLİ

DANIŞMAN
Üst Kurul Uzmanı Uğur BOĞA

ANKARA

HAZİRAN / 2021

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	:	
Üye	:	
Üye	:	
Üye	:	
Üye	:	

ONAY

…./…./2021

Ebubekir ŞAHİN

Üst Kurul Başkanı

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI

Radyo ve Televizyon Üst Kurulunda görev yapan Üst Kurul Uzman Yardımcısı olarak, Radyo ve Televizyon Üst Kurulu Tez Hazırlama Yönergesi'ne uygun şekilde hazırlamış olduğum uzmanlık tezi ilişikte sunulmuştur.

Bu uzmanlık tezindeki bütün bilgilerin 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.

/08/2021
Sena NEZGİTLİ
Üst Kurul Uzman Yardımcısı

Uzmanlık Tezinin Adı:

İngiltere ve Türkiye'nin Siber Güvenlik Politika Yaklaşımlarının Karşılaştırılması

EK:
1- TEZ (6 adet)
2- CD (1 Adet)

Tezi Teslim Alan
Daire Başkanı

Tarih : /08/ 2021

F. İnci ÖZKAN

TEŞEKKÜR

"İngiltere ve Türkiye'nin Siber Güvenlik Politika Yaklaşımlarının Karşılaştırılması" isimli bu tezin hazırlanması sürecinde öncelikle Üst Kurul Başkanı Sayın Ebubekir ŞAHİN ve Üst Kurul Üyelerine teşekkürlerimi sunarım.

Bu tezin hazırlanmasında önerileriyle bana destek veren tez danışmanım Sayın Uğur BOĞA'ya, çalışmalarım esnasında yardımlarını esirgemeyen Daire Başkanım Fatma ÇELİKER'e, Türkiye'de uluslararası siber güvenlik çalışmaları ile tanınmış olan Prof. Dr. Nezir AKYEŞİLMEN hocama, yardımlarını esirgemeyen ve bana akademik çalışmalarımda öncülük eden çok kıymetli hocam Doç. Dr. Recep BENZER'e teşekkürü borç bilirim.

Bu tez döneminde bana her konuda destek veren değerli annem Etfal NEZGİTLİ'ye, sevgili babam Yavuz NEZGİTLİ'ye hep arkamda duran canım ablalarım Rabia NEZGİTLİ, Saliha NEZGİTLİ ve Lamia NEZGİTLİ ile canım yeğenlerim Asım Furkan ŞEKER ve Eslem Büşra ŞEKER'e sevgilerini sundukları için sonsuz teşekkür ederim.

İÇİNDEKİLER

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI I

TEŞEKKÜR II

İÇİNDEKİLER III

KISALTMALAR VI

TABLO VE ŞEKİLLER XI

GİRİŞ 1

Çalışmanın Konusu 3
Çalışmanın Soruları 4
Çalışmanın Amacı 4
Çalışmanın Önemi 5
Çalışmanın Yöntemi 5
Çalışmanın Kapsamı ve Sınırlılıkları 6
Çalışmanın Varsayımları 6
Çalışma Kapsamında Veri Toplanması ve Analizi 6

BİRİNCİ BÖLÜM 7

SİBER KAVRAMI, SİBER SALDIRI TÜRLERİ VE SİBER SALDIRININ TARİHSEL GELİŞİMİ 7

1.1. SİBER KAVRAM VE ORTAK TANIMLAR 7
1.1.1. Siber Kavramı 8
1.1.2. Siber Kavram ile İlgili Ortak Tanımlar 9
1.1.2.1. Siber Varlık 9
1.1.2.2. Siber Uzay 10
1.1.2.3. Siber Olay 11
1.2. SİBER SALDIRI 12
1.2.1. Siber Saldırı Nedir? 12
1.2.2. Siber Saldırı ile İlgili Ortak Kavramlar 14
1.2.2.1. Siber Suç 14
1.2.2.2. Siber Savaş 18
1.2.2.3. Siber Casusluk 19
1.2.2.4. Siber Silah 20
1.2.2.5. Siber Tehdit 20
1.2.2.6. Siber Risk 21
1.2.2.7. Siber Zorbalık 22
1.2.2.8. Siber Terör 24
1.3. SİBER SALDIRI TÜRLERİ 25
1.3.1. Bilişim Sistemlerine Yönelik Siber Saldırı Türleri 26
1.3.1.1. Kötücül Yazılımlar (Malicious Software) 26
1.3.1.1.1.Virüsler 27
1.3.1.1.1.1. Solucanlar (Worm) 28
1.3.1.1.1.2. Bukalemunlar 29

1.3.1.1.1.3. Tavşanlar 30
1.3.1.1.1.4. Mantık Bombası 30
1.3.1.1.2. Truva Atları (Trojen Horses) 30
1.3.1.1.3. Tuş Kaydediciler (Keyloggers) 31
1.3.1.1.4. Arka kapılar (Back Doors) 32
1.3.1.1.5. Koklayıcı (Sniffer) 33
1.3.1.1.6. Kök Kullanıcı Takımları (Rootkits) 33
1.3.1.1.7. Casus Yazılım (Spyware) 34
1.3.1.1.8. Fidye Yazılım (Ransomware) 34
1.3.2. Bilişim Altyapısı ve Bilişim Ağına Yönelik Siber Saldırı Türleri 35
1.3.2.1. DNS ve ARP Zehirlenmesi 35
1.3.2.2. Oltalama (Phishing) 36
1.3.2.3. Sosyal Mühendislik 37
1.3.2.4. Hizmet Dışı Bırakma (DoS) 38
1.3.2.5. Ortadaki Adam (Man in The Middle) Saldırıları 40
1.3.2.6. Siteler Arası Betik Çalıştırma (XSS) 40
1.3.3. Bilişim Sistemi Uygulamalarına Yapılan Siber Saldırı Türleri 41
1.3.3.1. Parola Saldırısı (Password Attack) 41
1.3.3.2. Kripto Krikosu (Crypto Jacking) 42
1.3.3.3. Sıfır Gün İstismarı (Zero Day Exploit) 42
1.3.3.4. SQL (Structured Query Language) Enjeksiyon 42
1.4. SİBER SALDIRININ TARİHSEL GELİŞİMİ 43

İKİNCİ BÖLÜM 47

SİBER GÜVENLİK TÜRLERİ, AMACI VE SİBER GÜVENLİĞİN TARİHSEL GELİŞİMİ 47

2.1 SİBER GÜVENLİK 47
2.1.1. Siber Güvenlik Nedir? 47
2.1.2. Siber Güvenlik ile İlgili Kavramlar 48
2.1.2.1. Bilgi Güvenliği 48
2.1.2.2. Ulusal Siber Güvenlik 49
2.1.2.3. Siber Caydırıcılık 49
2.1.2.4. Parola Güvenliği 50
2.1.2.5. Kritik Altyapıların Güvenliği 50
2.2. Siber Güvenliğin Amacı: CIA Modeli 51
2.3. SİBER GÜVENLİĞİ SAĞLAMA YÖNTEMLERİ 53
2.3.1. Anti virüs 53
2.3.2. IDS/IPS (Saldırı Tespit Etme ve Önleme Sistemleri) 53
2.3.3. Güvenlik Duvarı (Firewall) 54
2.3.4. NAC (Sistem Ağ Erişimi) 55
2.3.5. Web ve E-mail Gateway 56
2.3.6. Honeypot (Bal küpü) 57
2.3.7. SIEM (Güvenlik Bilgi ve Olay Yönetimi) 58
2.3.8. URL Filtreleme 58

2.3.9. WAF (Web Uygulama Güvenlik Duvarı) 59
2.3.10. Anti DDOS 59
2.3.11. VPN (Sanal Özel Ağ) 60
2.4. SİBER GÜVENLİĞİN TARİHSEL GELİŞİMİ 61

ÜÇÜNCÜ BÖLÜM 64

İNGİLTERE VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASININ KARŞILAŞTIRILMASI 64

3.1. ITU SİBER GÜVENLİK ENDEKSİNİN TARİHİ 64
3.2. İNGİLTERE VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRILMASI 67
3.2.1. Yasal Düzenlemeler (Legal Measures) 67
3.2.2. Kurumsal Yapılanma (Organizational Measures) 72
3.2.3. Teknik Çerçeve (Technical Measures) 76
3.2.4. Kapasite Geliştirme (Capacity Building) 82
3.2.5. Uluslararası İşbirliği (Cooperation) 85
3.3. DİJİTAL DÖNÜŞÜM OFİSİ VE BİLGİ GÜVENLİĞİ DERNEĞİ'NİN YÜRÜTTÜĞÜ SİBER GÜVENLİK FAALİYETLERİ 91

SONUÇ VE ÖNERİLER 95

KAYNAKÇA 103

ÖZET 125

ABSTRACT 127

ÖZGEÇMİŞ 128

KISALTMALAR

a.g.e.	Adı geçen eser
a.g.k.	Adı geçen kanun
a.g.m.	Adı geçen makale
a.g.r.	Adı geçen rapor
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ACM	Association for Computing Machinery (Bilgi İşlem Makineleri Derneği)
AGİT	Avrupa Güvenlik ve İşbirliği Teşkilatı
AIDS	Acquired Immune Deficiency Syndrome (Kazanılmış Bağışıklık Yetersizliği Sendromu)
ALERT	Applied Learning for Emergency Response Team (Acil Müdahâle Ekibi için Uygulamalı Öğrenme)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
ASSS	Avrupa Siber Suçlar Sözleşmesi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BSI	British Standarts Institute (İngiltere Standartlar Enstitüsü)
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
C	Cilt
CCDCOE	Cooperative Cyber Defence Centre of Excellence (Müşterek Siber Savunma Mükemmeliyet Merkezi)
CEOP	Child Abuse and Online Protection Command (Çocuk İstismarı ve Çevrimiçi Koruma Komutanlığı)
CERT	Computer Emergency Response Team (Bilgisayar Acil Müdahâle Ekibi)
CESG	National Technical Authority for Information Assurance (Ulusal Bilgi Güvencesi Teknik Kurumu)

CFAA	Computer Fraud and Abuse Act (Bilgisayar Dolandırıcılığı ve Kötüye Kullanma Yasası)
CIA	Confidentiality Integrity Availability (Gizlilik Bütünlük Erişilebilirlik)
CIRT	Computer Incident Response Team (Bilgisayar Olay Müdahâle Ekibi)
CISP	Cyber Security Information Sharing Partnership (Siber Güvenlik Bilgi Paylaşım Ortaklığı)
CRS	Congressional Research Service (Kongre Araştırma Servisi)
CSIRT	Computer Security Incident Response Team (Bilgisayar Güvenliği Olay Müdahâle Ekibi)
DDoS	Distributed Denial of Service (Dağıtık Servis Dışı Bırakma)
DNS	Domain Name System (Alan Adı Sistemi)
DoS	Denial of Service (Servis Dışı Bırakma)
DPA	Data Protection Act (Veri Koruma Yasası)
EARN	European Academic Research Network (Avrupa Akademik Araştırma Ağı)
ENISA	European Network and Information Security Agency (Avrupa Ağ ve Bilgi Güvenliği Ajansı)
e-posta	Elektronik posta
GCA	Global Cybersecurity Agenda (Küresel Siber Güvenlik Gündemi)
GCI	Global Cybersecurity Index (Küresel Siber Güvenlik Endeksi)
GDPR	General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
HLEG	High Level Experts' Group (Üst Düzey Uzmanlar Grubu)
HPE	Hewlett Packard Enterprise
HTML	HyperText Markup Language (Hiper Metin İşaretleme Dili)
HTTP	Hyper Text Transfer Protocol (Hiper Metin Aktarım Protokolü)
IBM	International Business Machines (Uluslararası İş Makineleri)
ICO	Information Commissioner's Office (Bilgi Komisyonu Ofisi)
ICSE	International Cyber Shield Exercise (Uluslararası Siber Kalkan Tatbikatı)
IDS	Intrusion Detection System (Saldırı Tespit Sistemleri)
IEC	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)

IEEE	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IGF	Internet Governance Form (İnternet Yönetişim Formu)
IISP	Institute of Information Security Professionals (Bilgi Güvenliği Uzmanları Enstitüsü)
IMPACT	International Multilateral Partnership Against Cyber Threats (Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık)
IoT	Internet of Things (Nesnelerin İnterneti)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention System (Saldırı Önleme Sistemleri)
ISO	International Organization for Standardization (Uluslararası Standartlar Teşkilatı)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
IWF	İnternet Watch Foundation (İnternet İzleme Kurumu)
KVKK	Kişisel Verileri Koruma Kanunu
MAC	Media Acess Control (Ortam Erişim Yönetimi)
MITM	Man in The Middle (Ortadaki Adam)
NAC	Network Access Control (Ağ Erişim Kontrolü)
NASA	National Aeronautics and Space Administration (Ulusal Havacılık ve Uzay Dairesi)
NATO	North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
NCSC	National Cyber Security Center (Ulusal Siber Güvenlik Merkezi)
NIS	Network and Information Security (Ağ ve Bilgi Güvenliği)
NISR	Network and Information Security Regulation (Ağ ve Bilgi Güvenliği Yönetmeliği)
No	Numara
NSCR	National Security Capability Review (Ulusal Güvenlik Yeteneği İncelenmesi)
NSS	National Security Strategy (Ulusal Güvenlik Stratejisi)
NTT	Nippon Telegraph and Telephone (Nippon Telgraf ve Telefon)

NVC	National Volunteer Participant (Ulusal Gönüllü Katılımcı)
OCSIA	Office of Cyber Security and Information Assurance (Siber Güvenlik ve Bilgi Güvencesi Ofisi)
Ofcom	Office of Communications (İletişim Ofisi)
PLC	Programmable Logic Controller (Programlanabilir Mantıksal Denetleyiciler)
R&D	Research and Development (Araştırma ve Geliştirme)
RA	Royal Assert (Kraliyet Onayı)
RG	Resmî Gazete
RISCS	Research Institute for Sociotechnical Cyber Security (Siber Güvenlik Bilim Araştırma Enstitüsü)
RSA	Rivest-Shamir-Adleman
RTÜK	Radyo ve Televizyon Üst Kurulu
s.	Sayfa
S.	Sayı
SCADA	Supervisory Control and Data Acquisition (Merkez Kontrol ve Veri Toplama Merkezi)
SIEM	Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)
SOME	Siber Olaylara Müdahâle Ekibi
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSL	Secure Socket Layer (Güvenli Yuva Katmanı)
STK	Sivil Toplum Kuruluşları
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
TSE	Türk Standartları Enstitüsü
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜHİD	Türkiye Halkla İlişkiler Derneği
UAB	Ulaştırma ve Altyapı Bakanlığı
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
URL	Uniform Resource Locator (Standart Kaynak Bulucu)
USOM	Ulusal Siber Olaylara Müdahâle Merkezi

VPN	Virtual Private Network (Sanal Özel Ağ)
WAF	Web Application Firewall (Web Uygulama Güvenlik Duvarı)
WSIS	World Summit on the Information Society (Dünya Bilgi Toplumu Zirvesi)
XSS	Cross-site Scripting (Siteler Arası Betik Çalıştırma)

TABLO VE ŞEKİLLER

ŞEKİLLER

Şekil 1.1 2008-2018 Haziran Ayını Kapsayan Toplam İnternet Kullanım Rakamları 7
Şekil 1.2 İnternette 1 Dakikada Neler Oluyor 2020……..... 8
Şekil 1.3 NTT'ye göre 2013 Yılında Ülke Başına Düşen Siber Olayların Haritası... 11
Şekil 1.4 Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi……... 14
Şekil 1.5 Siber Suçların Ülkelerin GSYİH'na Göre Maliyet Oranları..…… 17
Şekil 1.6 1990-2011 Siber Suçlara göre Toplam Dava Dosya Sayısı…… 18
Şekil 1.7 Siber Zorbalığa Maruz Kalan Ülkeler…… 23
Şekil 1.8 Ipsos'un 28 Ülkeyi Kapsayan Siber Zorbalık Farkındalık Araştırması….. 23
Şekil 1.9 Kötücül Yazılımların Oranları…… 28
Şekil 1.10 Klavye Tablolama Yöntemi…….. 31
Şekil 1.11 İnternet Bankacılığına Girişteki Sanal Klavye Örneği……. 32
Şekil 1.12 Arka Kapıların Çalışma Prensibi…….. 32
Şekil 1.13 Normal ve Arp Zehirlenmesine Maruz Kalmış Ağ Trafiği……...36
Şekil 1.14 Sosyal Mühendislik Yaşam Döngüsü……... 38
Şekil 1.15 DDoS Saldırı Mimarisi…… 39
Şekil 1.16 MITM Saldırısı…… 40
Şekil 1.17 XSS Çalışma Prensibi……... 41
Şekil 1.18 SQL Enjeksiyon Yaşam Döngüsü…… 43
Şekil 1.19 Siber Saldırıların Getirdiği Mali Zararla……...……46
Şekil 2.1 Türkiye için Belirlenen Kritik Altyapılar……... 51
Şekil 2.2 Siber Güvenliğin Amacı: CIA Modeli…… 52
Şekil 2.3 IDS/IPS Mimarisi……54
Şekil 2.4 Güvenlik Duvarı Çalışma Şeması……... 55
Şekil 2.5 Gateway Çalışma Prensibi…….. 56
Şekil 2.6 Honeypot Çalışma Prensibi…… 57
Şekil 2.7 WAF Akış Şeması……...59
Şekil 2.8 VPN Çalışma Prensibi…… 60
Şekil 3.1 HLEG Küresel Strateji Raporundaki Siber Güvenliğin Beş Ana Unsuru...66
Şekil 3.2 Türkiye Siber Güvenlik Yönetişim Modeli……74

Şekil 3.3 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı Haritası……... 75
Şekil 3.4 Ulusal Siber Güvenlik Organizasyon Şeması……..79
Şekil 3.5 Küresel Ölçekte Ülkelerin Siber Güvenlik Taahhütleri…….. 90
Şekil 3.6 Küresel Ölçekte Ülkelerin Siber Güvenlik Taahhütleri Isı Haritası……90

TABLOLAR

Tablo 1.1 Klasik Terör ve Siber Terör Farkı……..25
Tablo 1.2 2013-2014 Kötücül Yazılımın Hedefi Olan Ülkeler……..27
Tablo 3.1 2017 GCI Türkiye-İngiltere Yasal Düzenlemedeki Durumları…… 71
Tablo 3.2 2017 GCI Türkiye-İngiltere Kurumsal Yapılanma Durumları……... 76
Tablo 3.3 2017 GCI Türkiye-İngiltere Teknik Düzenleme Durumları……..82
Tablo 3.4 2017 GCI Türkiye-İngiltere Kapasite Geliştirme Durumları…….85
Tablo 3.5 2017 GCI Türkiye-İngiltere İşbirliği Durumları……89
Tablo 3.6 GCI Dünya Sıralamasına göre Türkiye ve İngiltere…… 89

GİRİŞ

İnsanlık varoluşundan bugüne kadar kendini güvende hissetmek için kendini ve çevresini koruma ihtiyacı duymuştur. Bu güvenlik ihtiyacı, yaşam döngüsü ve insanlığın gelişimine göre kimi zaman yırtıcı hayvanlara kimi zaman deprem, sel, yangın vb. doğal afetlere karşı olmuştur. Ancak çağın ilerlemesi ile beraber ortaya çıkan yeni gelişmeler güvenlik konusunda dönüşümler geçirerek farklı boyutlar kazanmıştır. Bu dönüşümler de insanın güvende kalma olgusunu değiştirmiş ancak bu duyguyu yok etmemiştir. İnsanlığın yeni şeyler keşfetmesi ve dünyaya kendisinden bir şeyler katma düşüncesi, onu farklı güvenlik alanlarına yöneltmiştir. Günümüzde hiçbir insan yabani bir hayvandan kendini koruma ihtiyacı hissetmemektedir. Fakat içinde bulunduğumuz durum ve teknoloji itibari ile her insan banka hesabının güvenliğinden veya telefonunun çalınmasından büyük endişe duymaktadır. Kısacası insanlığın varoluşundan bu zamana kadar elbette ki güvenlikle alakalı riskler değişmiştir ancak insanlığın güvenlik sorunu hâlâ devam etmektedir ve bu sorun zaman ilerledikçe önem arz etmektedir.

Günümüz dünyası, teknoloji ile beraber hızlı bir dönüşüm içerisindedir. Teknolojinin her alana girmesi ve gelişim göstermesi kaçınılmazdır. Bu durum gerek bireysel gerek ulusal ve hatta uluslararası alanda en önemli eğilimlerden biri olmuştur. Bu ilerleme sağlıktan eğitime, bankacılıktan enerji sektörüne, inovasyon hizmetlerinden kültürel aktivitelere kadar her alana nüfuz etmiş durumdadır. İlerleme ve gelişimler bazen insanların takip edemeyeceği kadar hızlı olabilmektedir. Bu konuda genel eğilim her ne kadar yeni gelişmeleri takip etmek ve sunulan bu teknolojiyi kullanmak gibi düşünülse bile asıl olan teknolojiyi güvenli kullanmak olmalıdır. Çünkü teknolojinin sadece ilerlemesi önemli değildir. Teknoloji ancak güvenle ilerleyerek insanlığa hizmet edebilir.

2020 yılı itibari ile dünyayı etkisi altına alan Kovid-19 virüsü ile beraber sosyal mesafenin korunması hususunda alışveriş, eğitim, evden çalışma uygulamaları, seminer ve konferanslar gibi birçok durum çevrimiçi gerçekleştirilmektedir. Bu hususta artık teknoloji ve bu teknolojiyi oluşturan her türlü donanım ve yazılım ekipmanları hayatın vazgeçilmezi olmuştur. Bu nedenle bu ekipmanlarda aranacak en önemli kriter güvenlik prensibi olmalıdır. Örneğin, bireysel güvenlik ele alındığında, artık akıllı telefonlar insan hayatı için bir vazgeçilmez unsurdur. İçinde birçok şifre ve fotoğraf gibi hayati verileri taşıdığı düşünülürse bu kitle iletişim aracının güvenli bir sistem altyapısına sahip olması önemlidir. Ülke güvenliği ele alındığında, devletlerin vatandaşları için sundukları enerji, su, elektronik-haberleşme, bankacılık ve finans gibi kritik altyapı hizmetleri mevcuttur. Teknoloji ilerlemesi ile bu sistemlerin korunma ihtiyacı ortaya çıkmıştır. Bu altyapılarda yaşanacak güvenlik sıkıntıları, o ülkenin maddi kaybı ile beraber küresel dünyada prestij kaybına da neden olur ve o ülkeyi dış politikada güvenilmez kılabilir. Bu durum siber güvenlik kavramını ortaya çıkarmıştır ve Uluslararası Telekomünikasyon Birliği (ITU) tarafından siber güvenlik, sanal ortamı kapsayan kurum, kuruluş ve kullanıcılara ait varlık oluşturan bilgileri koruma hedefiyle kullanılan yöntem, politika, kavram, kılavuz, risk yönetim ve yaklaşımları, faaliyet, eğitim, en iyi uygulama deneyimi ve kullanılan teknolojilerin tamamı[1] olarak açıklamıştır. Bu güvenlik hedefi üç kriterden oluşur ve bunlar; gizlilik, bütünlük ve kullanılabilirliktir.

Etkili bir siber güvenlik için olmuş ve olması muhtemel saldırılara karşı devletler siber güvenlik politikası belirlemelidir. Etkili bir siber güvenlik politikasının temelini halkı bilinçlendirme çalışmaları oluşturmaktadır. Bilinçlendirme hareketi çeşitli kanallar kullanılarak yapılabilir. Türkiye için yapılan bilinçlendirme çalışmalarına örnek olarak T.C. İçişleri Bakanlığı 5. Uluslararası Siber Suçlar Çalıştayı[2], Bilgi Teknolojileri ve İletişim Kurumu'nun geleceğin beyaz şapkalı

[1] https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets (03.10.2020)
[2] https://www.icisleri.gov.tr/5-uluslararasi-siber-suclar-calistayi (05.07.2020)

hackerlarını yetiştirmek için düzenlediği "*Hacker Kampı*"[3], Ticaret Bakanlığının internet ve telefon dolandırıcılığına dair yayınladığı kamu spotu[4] verilebilir.

Çalışmanın Konusu

Günümüze kadar geçen süreçte yapılan siber saldırılar ve oluşturduğu tehditler karşısında Türkiye ve İngiltere'nin siber güvenlik politika süreçleri değişiklik göstermiş ve teknolojiye uyum gösterme çabası içerisinde olmuşlardır. Bu süreç çok yönlü ve karmaşık bir durumdadır. İşte bu yüzden üç ana bölümden oluşan "İngiltere ve Türkiye'nin Siber Güvenlik Politika Yaklaşımlarının Karşılaştırılması" adlı çalışmada bu karmaşık ve çok yönlü süreç analiz edilmektedir.

Çalışmanın birinci bölümünde, siber güvenlik ve siber saldırının ortaya çıkardığı "*siber kavramı*" ele alınarak siber saldırı ve türleri istatistiksel veriler ışığında göz önüne serilecektir. Ayrıca siber saldırı ve siber saldırı ile ortaya çıkan kavramlar açıklanarak konu hakkında oluşabilecek kavram kargaşasının önüne geçilecektir.

İkinci bölümde, siber güvenliğin ne olduğu, nasıl ortaya çıktığı ve tarihsel süreci ile beraber gelişimi ele alınacaktır. Siber güvenlik kavramları analiz edilerek siber güvenliğin nasıl sağlanacağı ve uygulama yöntemleri incelenecektir. Ayrıca siber güvenliğin önemi, CIA modeli ile açıklanacaktır.

Çalışmanın temelini oluşturan üçüncü bölümde ise Türkiye ve İngiltere'nin siber güvenlik politikaları konusunda dünya sıralamasında nerede oldukları hakkında yasal düzenlemeler, kurumsal altyapı, teknik çerçeve, kapasite geliştirme ve

[3] http://etkinlik.btk.gov.tr/etkinlik/detay/btk_hacker_kamp/ (05.07.2020)
[4] https://www.ticaret.gov.tr/video-galeri/kamu-spotu (05.07.2020)

uluslararası işbirliğini içine alan kapsamlı bir karşılaştırma yöntemi ortaya konarak bu kapsamda her iki ülke için de siber güvenlik analizi yapılacaktır.

Çalışmanın sonuç kısmında, tüm bölümlerde yapılan çalışmalar için değerlendirme yapılarak Türkiye'nin siber güvenlik politikaları için öneri ve değerlendirmeler verilecektir. Yapılan bu öneri ve değerlendirmelerin sonucunda, bu çalışmanın gelecek yıllar için siber güvenlik alanında yapılacak diğer çalışmalara örnek teşkil etmesi düşünülmektedir. Ortaya çıkan siber tehdidin oluşturduğu tehlike ve riskler karşısında iki ülke için siber güvenlik farkındalık durumu ele alınacaktır.

Çalışmanın Soruları

Bu çalışmanın ana sorusu "Türkiye ve İngiltere'nin siber güvenlik politikaları nelerdir?" olacaktır. Bu kapsamda ana soruyu destekleyen bazı yan sorular da mevcuttur. Bunlara örnek olarak; "siber güvenlik nedir?", "siber güvenlik hangi parametrelerle ölçülür?", "Türkiye ve İngiltere dünyanın siber güvenlik sıralamasında kaçıncı ülkelerdir?" gibi sorular verilebilir.

Çalışmanın Amacı

Bu çalışmanın temel amacı, Türkiye ve İngiltere'yi siber güvenlik politikaları açısından karşılaştırıp Türkiye'nin ulusal siber güvenlik konusunda yapılması gerekenleri belirlemektir. Bununla birlikte ulusal siber güvenlik kapasitesi ve RTÜK'ün kurumsal siber güvenlik yapılanması arasındaki ilişkinin incelenmesi de amaçlanmaktadır. Bu çalışma, literatüre konu hakkında yapılan çalışmalara ilave olarak yeni bir soluk getirecektir.

Çalışmanın Önemi

Ülkeler, uluslararası anlamda siber saldırıların son zamanlardaki artışı ile beraber maddi ve manevi birçok kaybın yanı sıra ülke düzenlerini koruyamaması gibi ciddi risklerle karşı karşıya kalmaktadır. Bu tehditlerin sürekli olarak değişmesi ve kendi içindeki dinamizm ile güvenlik tarafının da bu tehditlere ayak uydurarak kendini sürekli yenilemesi gereklidir. Bu çalışma, uluslararası siber güvenliğin temelini oluşturan bilinçlendirme ve farkındalık konusunda yeni bir bakış açısı kazandıracaktır. Uluslararası siber güvenliği tehdit edebilecek ve taşıdığı riskler bakımından bazı koşullarda geri dönüşü olmayan siber saldırılar için alınması gereken önlemlerin bilinçlendirme faaliyetlerine katkı sağlayacağı düşünülmektedir.

Çalışmanın Yöntemi

Bu çalışmada, kaynak tarama (Review) yöntemi kullanılmıştır. Bilindiği üzere kaynak tarama yöntemi; akademik nitelikteki konu hakkında yapılan araştırma için konunun daha önce ele alınıp alınmadığı ve ayrıca konu ele alındıysa nasıl ele alındığını ortaya koyan bir yöntemdir[5]. Bilgi ve belgelere erişim, konu hakkındaki basılı kaynaklar, çeşitli indeksler (Google Akademik, Science World Index, Acarindex, Academic Research Index), bilimsel veri tabanları (Scopus, IEEE Explore, Academia, ACM Digital Library, ITU, Wiley Online Library, Science Direct), yayımlanmış tezler ayrıca yayınlanmış makaleler ve kurumsal web siteleri incelenerek elde edilmiştir. İlgili veriler çalışmanın amacına aykırı olmadan çalışmanın doğrultusunda bilimsel etik kurallara uygun biçimde aktarılmıştır. Belirlenen yöntem doğrultusunda ITU tarafından üye ülkelere gönderilen anket uygulamasıyla ülkelerin siber güvenlik sıralamalarının belirlendiği modelleme kullanılmıştır. Bu modellemede, uygulanan anket sonucuna göre üye ülkeler verdikleri cevaplarla puanlandırılıp sıralamaya sokulmuştur. İngiltere ve Türkiye bu sıralamaya göre kıyaslanarak ülkemizin mevcut siber güvenlik kapasitesi belirlenmiştir.

[5] https://www.akademikkaynak.com/literatur-taramasi-nedir-ve-nasil-yapilir.html (06.07.2021)

Çalışmanın Kapsamı ve Sınırlılıkları

Bu çalışmada, siber güvenlik kavramı uluslararası güvenliği anlamaya katkı sağlayacağı düşünülerek incelenmiştir. Bu hususta öncelik Türkiye ve İngiltere'nin siber güvenlik yaklaşımlarına verilmiştir. Ülke güvenliğini tehdit eden siber saldırı ve siber saldırı türleri de ele alınmıştır. Bu süreçte siber saldırı türlerinin oldukça fazla olması ve benzer yöntemleri kullanmalarından dolayı belirli bir kısmına bu çalışmada yer verilmemiştir. Siber güvenlik ile ilgili çeşitli ulusal ve uluslararası mevzuatlar çalışma kapsamında incelenmiştir.

Çalışmanın Varsayımları

Bu çalışmanın araştırmasına geçilmeden önce bulunulan varsayımlar: Uluslararası alanda Türkiye uluslararası iş birliğe daha açık ve uluslararası alanda İngiltere Türkiye'ye göre daha kapsamlı siber güvenlik politikasına sahip olduğu düşüncesidir. Bu iki varsayım çalışmanın tamamlanması ile sonuç bölümünde doğru veya yanlış oldukları yorumlanarak ifade edilecektir.

Çalışma Kapsamında Veri Toplanması ve Analizi

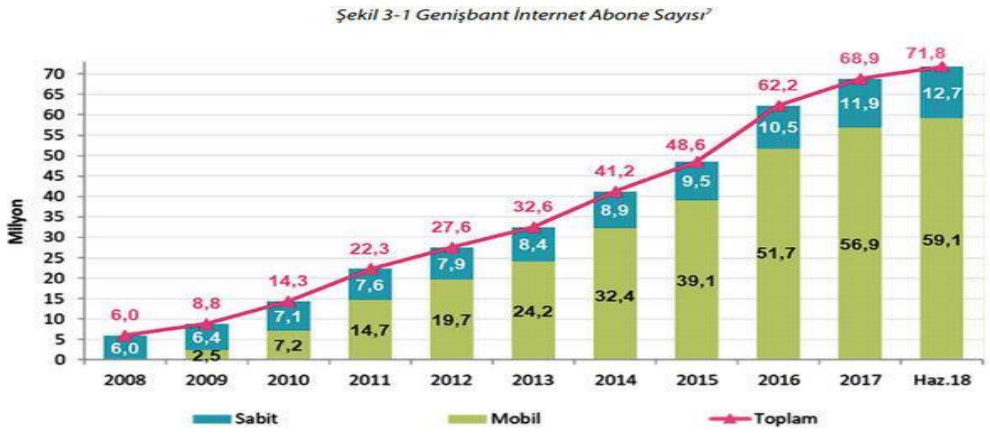
Bu çalışmada, veriler; kaynak tarama yöntemi ile beraber ITU'nun yayınladığı 2015, 2017 ve 2018 siber güvenlik endeksi kapsamında elde edilmiştir. Öncelikle bu yöntem için anahtar kelimeler kullanılarak çeşitli basılı kaynaklar, bilimsel veri tabanları, uluslararası anlaşmalar ve siber uzayın kapsam alanına giren direktifler toplanmıştır. ITU 2015, 2017 ve 2018 yıllarında yayınlanan endeks konusunda Türkiye'nin yaptığı siber güvenlik çalışmalarında incelenen veriler analiz edilmiştir. Bununla beraber özellikle Bilgi Güvenliği Derneği başta olmak üzere Ulaştırma Bakanlığı, TÜBİTAK gibi çeşitli kurum ve sivil toplum kuruluşlarından elde edilen bilgiler de bu endekslerin anlaşılması konusunda çok büyük katkı sağlamıştır.

BİRİNCİ BÖLÜM

SİBER KAVRAMI, SİBER SALDIRI TÜRLERİ VE SİBER SALDIRININ TARİHSEL GELİŞİMİ

1.1. SİBER KAVRAM VE ORTAK TANIMLAR

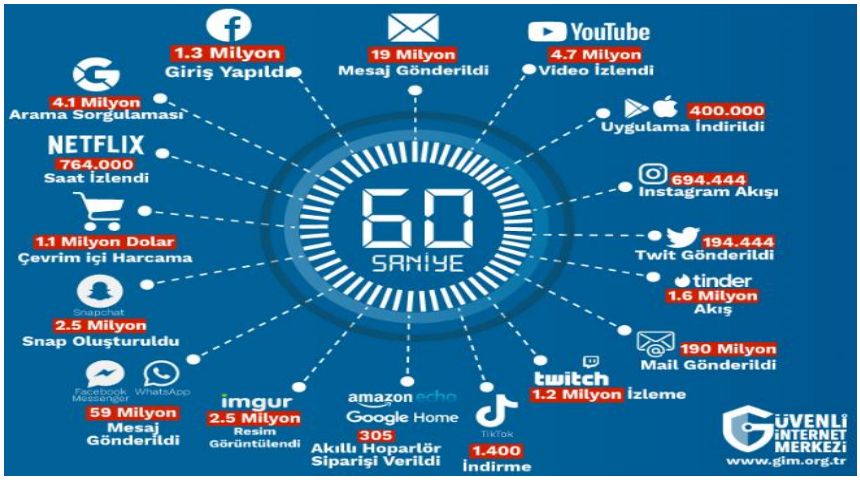
Siber kavram, günlük yaşamda internetin kullanımı ile beraber sıklıkla duyulmaya başlanmıştır. Şekil 1.1'de 2008 ile 2018 Haziran ayını kapsayan Türkiye'deki sabit ve mobil internet kullanımı görülmektedir.



Şekil 1.1 2008-2018 Haziran Ayını Kapsayan Toplam İnternet Kullanım Rakamları[6]

İnternet ve mobil internet kullanımının artması ile internette bir dakika içerisinde neler olduğu ve buna bağlı olarak oluşan yoğun veri trafiği Şekil 1.2'de görülmektedir.

[6] https://www.haberturk.com/turkiye-internet-kullanim-istatistiklerinde-son-durum-ne-2171017-ekonomi (15.07.2020)



Şekil 1.2 İnternette 1 Dakikada Neler Oluyor 2020 Yılı[7]

Bu büyük veri trafiği internetin küresel bir güç olduğunu göstermektedir. Bu küresel güç, siber kavramı ortaya çıkartmıştır. Siber kavramı anlamak, bu çalışma için önemlidir.

1.1.1. Siber Kavramı

Siber kavramının kökeni Fransızcada "*cybernétique*" olarak adlandırılan sibernetik kelimesinden meydana gelmektedir. İngilizcede "*cyber*" olarak bilinen bu kelime, Türkçeye "siber" kelimesi olarak geçmiştir[8]. Sibernetik kelimesi Türk Dil Kurumu sözlüğünde "*güdüm bilimi*" olarak ifade edilmiştir[9]. Literatürde de "*siber"* kelimesinin tanımları mevcuttur. Siber kelimesi, bilgisayar veya bilgisayar ağları ile ilgili olan kavram ve içerikleri tanımlamak için kullanılır[10] . Bu kavramın geçmişi eskiye dayanmamaktadır ve internetin hayatımıza girmesi ile ortaya çıkmıştır. Siber kelimesi, ilk kez Norbert Wiener'ın *Cybernetics* adlı romanında kullanılmıştır[11]. Bu

[7] https://www.guvenliweb.org.tr/galeri-detay/internette-1-dakikada-neler-oluyor (15.07.2020)
[8] Ceylan Daban, "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", *Cyberpolitik Journal*, S: 1, No: 1, 2016, s.81.
[9] https://sozluk.gov.tr/ (17.07.2020)
[10] Hakan Hekim ve Başıbüyük, Oğuzhan, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, Sayı: 4, No: 2, 2013, s. 136.
[11] Münevver Alıcı, "Siber Uzayda Sosyal Medya ve Gözetim: Facebook Örneği", *Cyberpolitik Journal*, Sayı: 4, No: 8, 2019, s. 187.

kavramın kapsam alanı geniş olduğundan ortak bir tanım yapmak mümkün değildir. Ancak siber kavramının iki temel özelliği mevcuttur. Birincisi tıpkı internet gibi bilgisayar ve bilgisayar sistemleri arasındaki fiziksel ortam, ikincisi bu fiziksel ortamın dışında oluşan sanal ortamdır[12].

1.1.2. Siber Kavram ile İlgili Ortak Tanımlar

Siber kavramını oluşturan kavramlar; siber varlık, siber uzay ve siber olaydır. Bunlar siber saldırı ve siber güvenlik için önemlidir ve bu kavramların anlaşılması çalışmanın da anlaşılmasını sağlayacaktır.

1.1.2.1. Siber Varlık

Siber varlık hakkında literatürde birçok tanım mevcuttur. Adır'a göre siber varlık, siber ortamın içinde yer alan her türlü bilgi, belge, yazılım, donanım ve veri tabanı kayıtları gibi birçok varlığı kapsamı[13] olarak tanımlamıştır. Bilgi Güvenliği Derneği tarafından çıkarılan "*Siber Güvenlik ve Savunma Kitabı"*nda siber varlık, siber ortam içinde bulunan ve kapsamı içine giren her türlü doküman, veri, yazılım ve donanım olarak belirtilmiştir[14]. Bu iki tanıma bakılarak siber varlık kısaca: Siber ortamda bulunabilecek her türlü fiziksel ve sanal ekipmanlar şeklinde ifade edilebilir. Bu ekipmanlar yazılım, veri, bilgi gibi soyut niteliğe sahip olabileceği gibi belge ve doküman gibi somut niteliğe de sahip olabilir. Çünkü siber dünya, sanal ve fiziksel ortamın birleşimidir.

[12] Şeyma Kızılay, "Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası", *International Journal of Economics Administrative and Social Sciences,* Sayı: 3, No: 1, 2020, s. 34.
[13] Arif Emre Adır, "Kurumlar için Siber Güvenlik Laboratuvarı Altyapısının Oluşturulması", Yüksek Lisans Tezi, Konya, 2019, s. 5.
[14] Şeref Sağıroğlu, Alkan, Mustafa, Samet, Refik Ulutaş, Güzin ve diğ., *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Grafiker Yayınları, Ankara, 2018, s. 24.

1.1.2.2. Siber Uzay

Siber uzay, insan yaşamında en, boy, yükseklik ve zaman boyutunun dışındaki bir boyutta var olur. Çünkü siber uzay, sanal ve gerçek arasında insanlığa kapı açar. Siber uzay, bu kapsamıyla beşinci boyutu ifade etmektedir [15] ki bu da insanın gerçekten sanala geçişi olarak düşünülebilir. Siber uzay oluşumu, fiziksel olarak her türlü donanım, iletişim ağlarında bulunan santral, uydu, bilgisayar, modem vb. ekipmanlar olurken sanal olarak oluşturulan sohbetler, her türlü veri paylaşımı, veri depolama alanlarını da kapsamaktadır[16]. Siber uzay, sadece verileri saklayan bilgisayarları kapsamaz buna ilaveten veri akışı sağlayan sistem ile beraber alt yapıyı birleştiren sanal ve fiziksel ortamlar bütünüdür[17]. Bu yüzden siber uzayın hem kavramı hem de kapsam alanı oldukça geniştir. Kısaca, insanların birbirleriyle hızlı ve etkili iletişim kurmak amacıyla internet altyapısı kullanarak kendi oluşturduğu geniş bağlantı alanıdır. Siber uzay kavramına 1984 yılında yayınlanan William Gibson'ın *Neuromancer* adlı kitabında da yer verilmiştir[18].

Kurumsal olarak siber uzay kavramı Ulaştırma Denizcilik ve Haberleşme Bakanlığının yayınladığı 2016-2019 Ulusal Siber Güvenlik Stratejisine göre dünya ile beraber uzaya yayılmış olan bilişim sistemleri ve bu bilişim sistemlerini birbirine bağlayan ağlardan oluşan veya bu ağlardan bağımsız bilgi sistemlerinden oluşan dijital bir ortam olarak ifade edilebilir[19].

---

[15] Ali Nadi Ünal ve Yarman, Bekir Sıddık Binboğa, "Millî Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü", *7th International Conference On Information Security and Cryptology*, İstanbul, 2014, s. 278.

[16] Bülent Akkuş, "Yeni Dünyanın Babil Kulesi (?): Özne-Bilgi-İktidar İlişkisi Bağlamında Siber Uzay ve Özgür Bilgi Sorunsalı Üzerine", *Ankara Üniversitesi SBF Dergisi,* Cilt: 71, No: 4, 2016, s. 1161.

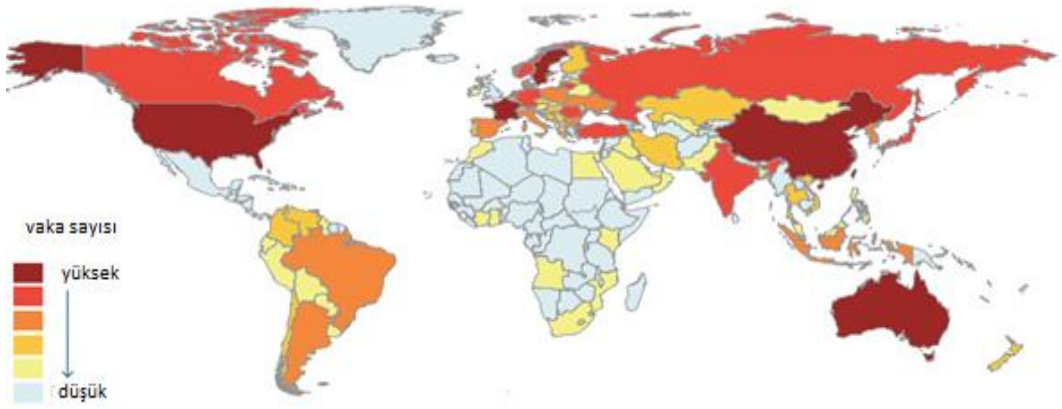
[17] İbrahim Kurnaz, "Siber Güvenlik ve İlintili Kavramsal Çerçeve" *Cyberpolitik Journal*, S: 1, No: 1, 2016, s. 61.

[18] Osman Girgin, "Siber Uzay'da Üstünlük Mücadelesi; Amerika Birleşik Devletleri ve Rusya Federasyonu", *Academic Review of Humanities and Social Sciences,* S: 3, No: 1, 2020, s. 38.

[19] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi*, 2016, s. 8.

1.1.2.3. Siber Olay

Siber olay adından da anlaşılacağı üzere siber varlıklarla beraber siber uzayda gerçekleşen olayların tamamıdır. Siber olayın içinde birçok bilişim altyapısı mevcuttur. Siber uzayda yer alan siber varlıkların etkilendiği, zarar gördüğü hatta bozulduğu ve bunlara ek olarak değişik şekilde bu varlıklar üzerinde işlem yapılabildiği ortamların tümüne verilen addır[20]. Başka bir ifade ile siber olay, siber uzaya ait olan yazılım, donanım, sistem ve her türlü cihazı kapsayan ve bunların zarar gördüğü veya etkilendiği tüm durumlara verilen olayları kapsamaktadır[21]. Bu konuda olumsuz siber olay yaşanmaması adına aralarında Türkiye'nin de yer aldığı birçok ülke Siber Olaylara Müdahâle Merkezi (USOM) ile beraber Ulusal Siber Olaylara Müdahâle Ekibi (SOME) kurmuştur. USOM koordinasyonundaki SOME'ler stratejik hedefler ve güvenlik prensipleri ile beraber millî güvenliğe yardımcı olurlar. Tüm ülkeler siber olaylara az veya çok maruz kalabilirler. Nippon Telegraph and Telephone Corporation olarak bilinen Japonya telekomünikasyon şirketlerinden biri olan NTT[22] tarafından 2013 yılında gerçekleşen ülke bazlı siber olayların dünya genelindeki yoğunluğu Şekil 1.3'te verilmiştir.



Şekil 1.3 NTT'ye göre 2013 Yılında Ülke Başına Düşen Siber Olayların Haritası[23]

[20] Ş. Sağıroğlu, M. Alkan, R. Samet, G. Ulutaş ve diğ. ,2018, s. 24.
[21] A. E. Adır, 2019, s. 5.
[22] https://www.ntt.co.jp/index_e.html (25.07.2020)
[23] Maarten Gehem, Usanov, Artur, Frinking, Erik ve Rademaker, Michel, *Assessing Cyber Security: A Meta Analysis of Threats, Trends, and Responses to Cyber Attacks*, The Hague Centre For Strategic Studies, 2015, s. 37.

1.2. SİBER SALDIRI

1.2.1. Siber Saldırı Nedir?

Çalışmanın bu bölümünde çalışmanın hemen hemen her yerinde karşılaşılacak siber saldırı ve siber saldırının kapsadığı siber suç, siber savaş, siber tehdit ve siber risk gibi terimlerin kavramsal çerçevede çeşitli tanımları yapılacaktır. Tanımların daha iyi anlaşılması için örnekler ve istatistiksel verilere yer verilecektir. Siber saldırının, ortaya çıktığı ilk günden bu yana birçok kurum, kuruluş, uluslararası organizasyon ve hatta basın yayın organları tarafından tanımı yapılmıştır. Bu çalışma kapsamında bu kavram için tek bir tanım vermek doğru değildir.

Gazete tanımlarına bakılırsa: Millîyet Gazetesi *"Siber Saldırı nedir, nasıl olur? Siber Saldırı mı var, korunma yolları nelerdir?"* başlıklı haber içeriğinde "*Bilgisayar ve internet alanında uzmanlaşmış hacker diye tabir edilen hack veya hacker gruplarının banka, polis, jandarma, devlet, şahıs, firma vb. sitelere veya bilgisayarlara zarar vermek amacı ile yaptıkları saldırıya siber saldırı denir*."[24] şeklinde tanımlarken, Hürriyet Gazetesi *"Siber saldırı ne demek? İnternet siber saldırıdan mı çöktü?"* başlıklı haber içeriğinde siber saldırıyı, *"Siber saldırı ise DDOS başta olmak üzere farklı yollarla internet üzerinden yapılan saldırılara deniyor*. "[25] şeklinde tanımlamıştır. Suha Onay ise Dia Blog sitesindeki "*Siber Saldırı Nedir? Siber Saldırılardan Nasıl Korunulur?*" adlı yazısında siber saldırıyı bilişim alanında uzman kişilerin devlet, emniyet teşkilatı, banka veya bireylere zarar vermek için yapılan bilgisayar sistemlerindeki elektronik saldırılar[26] olarak tanımlamaktadır.

[24] https://www.millîyet.com.tr/gundem/siber-saldiri-nedir-nasil-olur-siber-saldiri-mi-var-korunma-yollari-nelerdir-6126736/ (26.07.2020)

[25] https://www.hurriyet.com.tr/teknoloji/siber-saldiri-ne-demek-internet-siber-saldiridan-mi-coktu-41424233/ (27.07.2020)

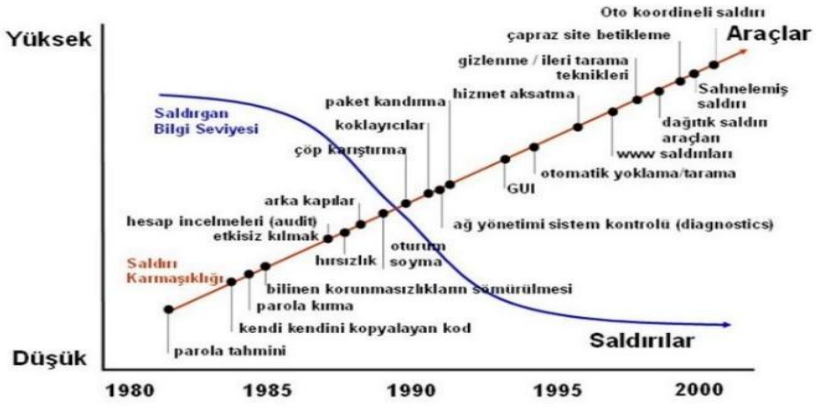
[26] https://www.dia.com.tr/siber-saldiri-nedir-siber-saldirilardan-nasil-korunulur/ (01.08.2020)

Bazı kurumların yaptığı tanımlara bakılırsa: UDHB'nin 2016-2019 Ulusal Siber Güvenlik Strateji Eylem Planı'nda "*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 işlemlerdir*."[27] şeklinde tanımlanırken, TBMM İnternet Komisyonu'nda "*hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar*"[28] olarak tanımlanmıştır.

Uluslararası alanda, Amerika Birleşik Devletleri Ulusal Araştırma Konseyi'nin 2009 yılında yaptığı çalışmada "*Ağlar, bilgisayar sistemleri veya bilgiyi ve bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler*"[29] olarak tanımlanmaktadır. Tüm tanımlamalardan yola çıkarak siber saldırı bilişim sistemlerine ve bilişim altyapısına sahip kişi, kurum veya ülkelerin mevcut sistemlerine onların rızası olmadan kişi veya kişi grupları tarafından yapılan her türlü zarar verici faaliyettir.

1980'lerden başlayarak 2000'li yıllara ilerledikçe siber saldırı araçlarının yetenekleri artarken saldırıyı yapan kişilerin bilgi seviyesindeki düşüş Şekil 1.4'te görülmektedir. Bunun sonucunda, saldırganın yapacağı ve yöneteceği süreci teknolojik araçlar üstlenmiştir.

[27] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s.8.
[28] Mustafa Alkan, "Siber Güvenlik ve Siber Savaşlar Sunumu", Siber Güvenlik Siber Savaşlar TBMM Internet Komisyonu, 2012, s. 7.
[29] Peter W. Singer ve Friedman, Alman, *Siber Güvenlik ve Siber Savaş*, (Çev. Ali Atav), Buzdağı Yayınları, Ankara, 2015, s. 182.



Şekil 1.4 Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi[30]

1.2.2. Siber Saldırı ile İlgili Ortak Kavramlar

1.2.2.1. Siber Suç

Siber suça geçmeden önce suçun tanımına bakılırsa suç, "yasalara aykırı davranış"[31] olarak tanımlanmaktadır. Siber suç da kavramsal çerçevede hem birçok tanıma hem de birçok terime karşılık gelmektedir. Siber suç için "bilişim suçu", "dijital suç", "elektronik suç", "bilgisayar suçu" ve "ileri teknoloji suçları" kavramları da kullanılabilir. Yani siber suçun kapsadığı kavramlar çeşitlilik göstermektedir. Bu kavramlar arasında siber suç ve bilişim suçu ön plana çıkmaktadır ve diğerlerine göre daha kapsamlıdır. Ancak bilişim suçu ve siber suçun hangisinin daha kapsayıcı olduğuna dair literatürde farklı görüşler mevcuttur. Bir yanda bilişim suçunun siber suçu kapsadığı yani siber suçun bilişim suçunun alt kategorisi[32] olduğu düşüncesi hâkimken diğer yandan da siber suçun bilgisayar ve teknolojiye dair işlenen tüm bilişim suçlarını kapsadığı[33] düşüncesi hâkimdir. Bu nedenle çalışmanın temelini

[30] Gürol Canbek ve Sağıroğlu, Şeref, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, Cilt: 9, Sayı: 3, 2006, s.169.
[31] https://sozluk.gov.tr/ (04.08.2020)
[32] Mehmet Emin Artuk, Gökcen, Ahmet, Yenidünya, Caner, *Ceza Hukuku Özel Hükümler*, Turhan Kitapevi, 11. Baskı, Ankara, 2011.
[33] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime*, Anderson Publishing, 2010.

oluşturan siber kelimesi ve bunun kavramlarından biri olan siber suçun tanımlarına bakılırsa tıpkı siber saldırı gibi birçok tanımlama yapmak mümkündür.

Emniyet Genel Müdürlüğü siber suçu, bilişim sistemi ile yürütülen bilişim sistemi güvenliğini ve bu sisteme bağlı olan veri ile kullanıcıları esas alan suçlar[34] olarak tanımlamıştır. Uluslararası alanda Avrupa Ekonomik Topluluğu 1983 yılında bilişim suçu terimini "*bilgileri otomatik olarak işleme tabi tutan yahut verilerin nakline yarayan bir sisteme karşı veya sistem ile gayri kanuni, ahlak dışı ve yetkisiz gerçekleştirilen her türlü davranıştır.*"[35] şeklinde ifade etmiştir. Görsel-işitsel medya aracı olan Millîyet Gazetesi "*Siber Suç Nedir?*" konu başlıklı haberinde siber suçun diğer suçlardan farklı olarak bilişim sistemi olmadan işlenemeyeceği[36] ifadesini vurgulamıştır.

Hukuki boyutu düşünüldüğünde ise; ABD'de Federal Ceza Kanunu'nun 1030. maddesinde, "*ABD hükümetine zarar vermek veya başka bir ülkeye yarar sağlamak amacıyla savunma ve dış işlerine ait tasnif edilmiş ve gizlilik dereceli bilgiye izinsiz olarak erişmek, finansal bir kurumun finans kayıtlarına veya tüketici bilgilerine ulaşmak veya bunları kullanmak amacıyla bir bilgisayara hukuka aykırı olarak girmek cezalandırılan bir fiil olarak düzenlenmiştir. Ayrıca devlet kurum veya teşkilatlarınca veya hükümet tarafından kullanılan bir bilgisayara yetkisiz erişmek de suçtur*."[37] ifadesine yer verilmiştir. İngiltere'de 29 Ağustos 1990 tarihinde yürürlüğe giren "Computer Misuse Act (Bilgisayarı Kötüye Kullanma Yasası)"de ise "*başka suçların işlenmesini kolaylaştırmak veya yardımcı olmak amacıyla bilgisayarlara yetkisiz olarak erişim ve bilgisayarlarda saklı tutulan program veya verilerin yetkisiz olarak değiştirilmesi fiilleri suç olarak düzenlenmiştir.*"[38] ifadesi kullanılmıştır.

---

[34] https://www.egm.gov.tr/siber/sibersucnedir#/ (08.08.2020)
[35] Cahit Aliusta ve Benzer, Recep (2018), "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dâhil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, S: 4, No:2, s. 36.
[36] https://www.millîyet.com.tr/siber-suc-nedir--molatik-12976/ (10.08.2020)
[37] Susan W. Brenner, "State Cybercrime Legislation in the United States of America: A Survey", Richmond Journal of Law and Technology Cilt: 7, S: 3, No: 4, 2001, s. 2.
[38] Olgun Değirmenci, *Bilişim Suçları*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2002, s. 158.

Tüm bu tanımlamalar doğrultusunda siber suç, bilişim sistemine yetkisiz erişim sağlayan kişi veya kişi topluluğu olarak bu sistemdeki verileri etkileyecek biçimde her türlü değişim ve yok etme gibi zararlı faaliyetlerde bulunma çabasıdır. Suçu işleyen kişi veya kişiler bunu herhangi bir kişi, kurum veya ülkeye yönelik yapabilir. Bu kişi veya kişilerin hedefleri insan olabileceği gibi mal varlığı ve maddi çıkarlar da olabilir. Bu hususta TCK, ABD Federal Ceza Kanunu ve İngiltere'nin Bilgisayarı Kötüye Kullanma Yasası ile siber suçun farkına varılarak bunun üzerine yaptırım oluşturmak ve teknoloji kullanılarak işlenen suçlar için caydırıcılık amaçlanmıştır. Siber suçlar çok çeşitli olabilir ve bilişimin olduğu her sektör ve alan içinde boy gösterebilir. TCK'da bilişim suçları şunlardır:

- *Bilişim sistemine girme suçu* (TCK m.243),
- *Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu* (TCK m.244),
- *Banka kartları veya kredi kartlarının kötüye kullanılması suçu* (TCK m.245),
- *Yasak cihaz veya program kullanma suçu* (TCK m.245/a)[39]

Siber suçların işlenme şekli üç ana başlıkta incelenebilir. Bunlar:

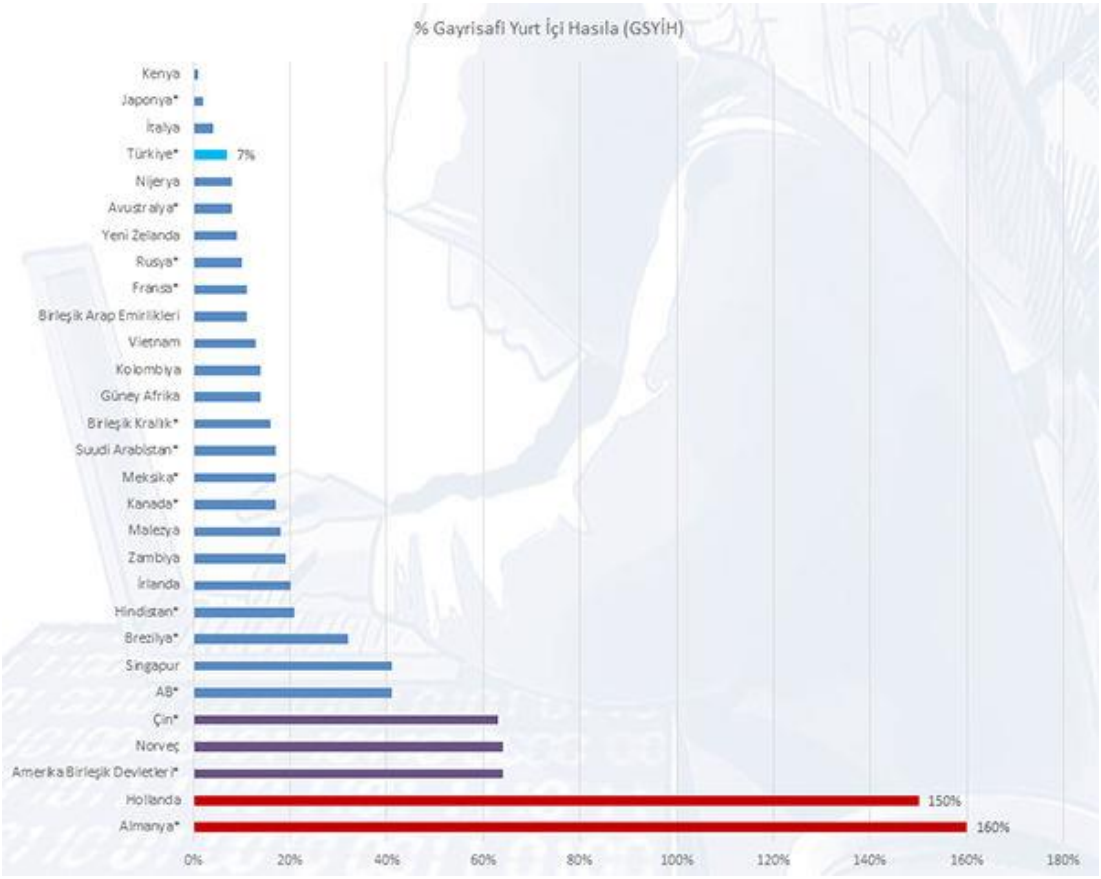
- Hedef olarak bilişim sistemlerini hedef alan suçlardır. Bilişim sisteminin hedeflenmesindeki erişim yetkisi olan kişinin sisteme erişimini engellemek, mevcut olarak işlemekte olan servisi devre dışı bırakmak ve bu durumdan faydalanarak sistem verilerine zarar vermek istenir.

- Doğrudan bilişim sistemine yetkisiz erişimden ziyade bu suçlar bilişim sistemleri ile bağlantılı suçlardır. En sık görülen yöntemler kredi kartı ve banka kartı dolandırıcılığı şeklinde olur. Aynı zamanda bu suçlara telif hakları ihlali gibi suçlar da eklenmelidir. Günümüzde telif hakları kapsamına, üretilen yazılım kodları da girmektedir. Bu nedenle sadece yayınlanan bir makale, üretilen bir müzik değil teknoloji ile üretilen yazılım, yeni bir cihaz vb. birçok durumda siber suçun işlenme nedenini oluşturur.

[39] TCK, 2004, s. 66-67.

- Bilişim sistemlerini kullanarak yapılan suçlar oldukça yaygındır. Bunlar sosyal medya üzerinden yapılan hakaret, kara para aklama, yürütülen terör faaliyetleri de örnek olarak verilebilir.

Ülkelerin gayrisafi yurt içi hasılasına göre siber suç maliyetleri Şekil 1.5'te görülmektedir. Buna göre Türkiye %7 oranla 4. sırada yer alırken İngiltere'nin %20 oranla 14. sırada yer aldığı görülmektedir.

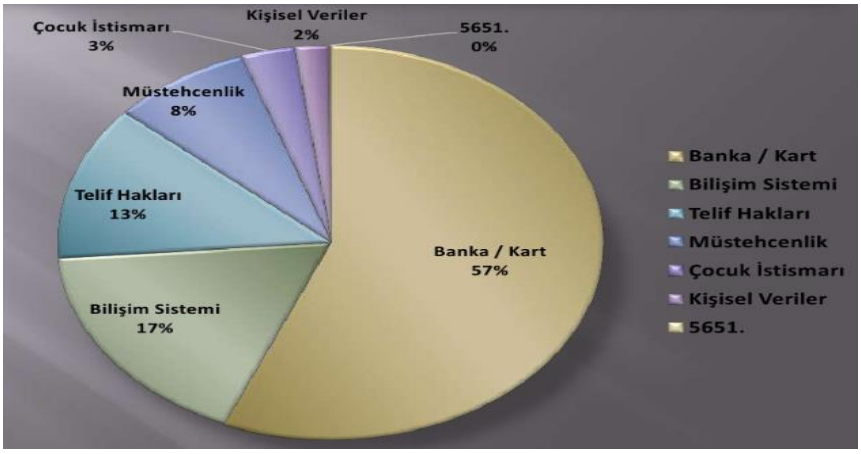


Şekil 1.5 Siber Suçların Ülkelerin GSYİH'na Göre Maliyet Oranları[40]

Türkiye için 1990 ve 2011 yılları arasında işlenen siber suç dağılımı Şekil 1.6'da görülmektedir. Bu grafiğe göre, banka ve kredi kartı dolandırıcılığı birinci

[40] https://www.kbd.org.tr/kategori/yazilar/66721/siber-guvenlik-pazari-bas-donduruyor (01.07.2021)

sıradadır. Bu hususta ülkede hizmet veren banka ve finans sektörleri uyarılmalı ve siber güvenlik önlemlerini arttırmalıdır.



Şekil 1.6 1990-2011 Siber Suçlara göre Toplam Dava Dosya Sayısı[41]

1.2.2.2. Siber Savaş

Siber savaş, bir ülkeyi hedef alan veya bir ulusla devam eden savaş kapsamında bir ülkenin diğer ülkeye karşı sahip olduğu askeri ve sivil her türlü bilişim sistemi ve altyapısını bozma, erişilmez kılma veya imha etme gibi yıkıcı etkilerle sonuçlanacak zarar verme işlemidir[42]. Bu zarar verme sürecinde ülkelerin kendini koruması için aldığı tedbir ve süreçler de siber savaşa dâhildir. Yani siber savaş, bir devletin başka devletin bilişim ağına sızma girişimidir[43]. 2001 CRS Raporu'nda siber savaş, düşmanın aynı eylemi yapma durumunu reddederek, siber uzaya ait olan bilişim ağlarını savunma veya bu bilişim ağlarına saldırılarını içeren türlü durumlar[44] olarak ifade edilmiştir. Coleman ise bu terim için, düşmanına ekonomik zarar verme ve düşmanın savunmasını bozmak amacıyla illegal faaliyetlerle bilgi ve iletişim

[41] Çığır İlbaş ve Av. Köksal, Mehmet Ali, "Türkiye'nin Siber Suç Haritası 1990-2011 Sunumu", 2011, s. 6.
[42] Gökhan Bayraktar," Siber Savaş ve Ulusal Güvenlik Stratejisi", *Yeniyüzyıl Yayınları*, İstanbul, 2015, s. 48.
[43] Vahit Güntay, "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi*, S: 6, No: 2, 2017, s. 81-108.
[44] Steven A. Hildreth, "Cyberfare Warfare 11", *Congressional Research Service Report for Congress No. Rl30735*, 2001, s.1.

altyapılarına ait olan bilgisayar ve ağlara yapılan saldırılar[45] şeklinde tanımlamıştır. Literatürdeki başka bir tanım ise çeşitli dönemleri kapsamakla beraber politik ve askeri çıkarları hedefleyerek düşmana ait olan bilişim altyapısı, sistemi veya bunun yürütüldüğü süreçleri erişilmez kılarak sekteye uğratacak ve bunları kendi menfaatleri doğrultusunda kullanarak karşı tarafın bu faaliyetler için önlem almasını engelleyerek benzer faaliyetlere de kendi için karşı koyma sürecidir[46]. Siber savaş, dijital yollarla sürdürülen savaş taktiğine ek olarak altyapıyı kullanılmaz hâle getirme, bilgi edinme gibi kavramları da kapsamaktadır[47].

Siber savaşta gerçek hedefi belirlemek güçtür. Siber ortam zaman ve mekândan bağımsız olarak internet altyapısını kullandığı için savaş her an her yerden gerçekleşebilir ve bu yüzden kontrol edilmesi neredeyse imkânsızdır. Ayrıca faaliyet gösterilen alanda iz bırakmayan yollar seçildiğinden neye ve kime karşı savunma geliştirileceği problemi nedeniyle normal savaşa göre farklı strateji belirlenmesi gerekir.

1.2.2.3. Siber Casusluk

Siber casusluk siber savaşın olmazsa olmaz bileşenlerinden biridir. İyi bir siber savaş stratejisi için iyi bir siber casusluk şarttır. Çünkü siber kaynağa giden gizli bilgiler elde edilmedikçe iyi bir siber savaş yürütülemez. Yani siber casusluk bilişim sistemine izinsiz girmek suretiyle hedeften veri elde etme veya veriyi manipüle etme anlamını taşır[48]. Başka bir ifade ile siber casusluk, siber savaşın gerektirdiği ölçüde düşman tarafın bilgi ve iletişim altyapısına girerek kendi çıkarları doğrultusunda elde edilen bilgi yığınıdır. Siber casusluk yönteminde en etkili yollardan biri sosyal

[45] Kevin Coleman, "The Cyber Arms Race Has Begun", *CSO online*, 2008, s. 1.
[46] Çalışma Grubu 4, "E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları", *Türkiye Bilişim Derneği*, 2006, s.5
[47] Şeyda Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, S: 71, No: 1, 2013, s. 1181.
[48] Ersin Çahmutoğlu, "Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi", *Analytical Politics*, S:1, No:1, 2020, s. 68.

mühendisliktir. Burada güvenliğin en zayıf halkası kabul edilen insan saldırı risklerine açıktır[49] ve siber savaşta kullanılması oldukça muhtemeldir.

1.2.2.4. Siber Silah

Siber savaşın bir diğer elemanı da siber silahlardır. Siber silah, etki alanına giren düşük ve yüksek potansiyelli programlar ve yazılımlar olarak nitelendirilebilir[50]. Düşük ve yüksek etkiden kastedilen sisteme verilen zarardır. Malware gibi sisteme girebilen ancak sistemi ele geçirme potansiyeli olmayanlar yazılımlar düşük etki gösterirken, sistem içine girip o sistemi kontrol edebilenler ise yüksek etkili sınıfında yer alır. Rid ve McBurney siber savaşı, yapı ve sistemler ile beraber canlılara fiziksel, psikolojik veya işlevsel zarar veren bilgisayar kodları[51] olarak tanımlamıştır. Sağıroğlu siber savaşı, sanal ortamdaki gerek savunma gerek de saldırı için kullanılan araçlar[52] olarak tanımlamıştır. Yani siber silah, tasarımı ve kullanımı gereği kişilerin yaralanmasına veya ölümüne yol açan siber savaş araçlarıdır[53]. Kısacası saldırı yeteneğini taşıyan ve bu potansiyelle zarar da verebilecek yazılım ve yazılımı oluşturan kod parçalarıdır.

1.2.2.5. Siber Tehdit

Siber tehdit, siber uzayda gerçekleşebilecek siber savaş veya siber saldırı olduktan sonra meydana gelebilecek zararlı durumlardır. Yani siber tehdit, bilginin temel unsurunu oluşturan verinin bozulması, yetkisiz kişilerce erişilmesi, elde edilen bu verilerin ifşa edilmesi gibi potansiyel sorunları barındıran durumdur. Siber uzayda meydana gelebilecek insan eli ile oluşturulan ve yazılımsal açıklar sayesinde var olan bilgi veya bilgilerin niteliğinin değiştirilmesi, bu bilgilere zarar verilmesi gibi

[49] Samet Oğuz, Ceyhan, E. Burak ve Sağıroğlu, Şeref, "Teknolojinin Casuslukta Kullanılması ve Karşı Önlemler", *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC Turkey),* 2015, s. 2.
[50] Thomas Rid ve Mcburney, Peter, "Cyber-Weapons", *Rusi Journal*, 2012, S: 157, No: 1, s. 6.
[51] A.g.m., s.7.
[52] Ş.Sağıroğlu, M. Alkan, R. Samet, G. Ulutaş ve diğ., 2018, s. 25.
[53] https://www.cyberdefensemagazine.com/nato-and-definition-rules-for-cyber-warfare/ (12.08.2020)

oluşabilecek etkilerdir[54]. USOM siber tehdidi, zararlı sonuçlara neden olabilecek muhtemel saldırı veya buna açık durumlar[55] olarak ifade etmiştir. Siber tehditlerin oluşmasını sağlayan üç durum mevcuttur. Bunları anlamak oluşacak siber tehditleri kavramak için çok önemlidir. Bunlar:

- İnternet tasarımındaki var olan açıklar (internet sistemlerinin açık ve şifresiz olması)
- Donanım ve yazılım hataları
- İletişim, enerji vb. kritik altyapıları barındıran sistemlere çevrimiçi erişim[56]dir.

Siber tehditlerin kendine has özellikleri mevcuttur. Yani bir siber tehdidin oluşabilmesi için belirli koşulların olması gerekir. Bunlardan en sık karşılaşılan yedi örnek incelendiğinde bunların:

- Perakende veri saldırıları
- Mobil güvenlik ve akıllı telefon güvenlik açığı tehditleri
- Kimlik avı saldırıları ve sosyal mühendislik
- Kimlik hırsızlığı
- Sağlık sektörü verilerine yapılan saldırılar
- Çocukların sapıklar tarafından hedeflenmesi
- Bankalara yönelik saldırılar[57] olduğu görülmektedir.

1.2.2.6. Siber Risk

Siber risk konusunda literatürde tanımlama mevcut değildir. Kurumsal olarak bakıldığında USOM, siber saldırı sonucunda oluşabilecek muhtemel sonuçlar[58] olarak

[54] Mehmet Bilge Kağan Önaçan ve Atan, Hasan, "Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği, *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, S: 17, No: 1, 2016, s. 14.
[55] Ulusal Siber Olaylara Müdahâle Merkezi, *Siber Güvenliğe İlişkin Temel Bilgiler,* USOM, Ankara, 2014, s.7
[56] Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", *Internetional Journal of Multidisciplinary Studies and Innovative Technologies,* S: 1, No: 1, 2017, s. 25.
[57] https://www.kaspersky.com.tr/resource-center/threats/top-7-cyberthreats (13.08.2020)
[58] Ulusal Siber Olaylara Müdahâle Merkezi, 2014, s.7.

ifade ederken benzer şekilde UDHB tarafından hazırlanan 2016-2019 Ulusal Siber Güvenlik Stratejisinde, tehditlerin bir veya daha çok bilgi varlığındaki açıklıktan faydalanarak zarar verme gücü[59] şeklinde ifade edilmiştir. Kısacası siber risk, siber savaş veya siber saldırının olma potansiyeline karşı oluşacak zararlardır. Böyle düşünüldüğünde her ülke için siber risk her zaman mevcuttur. Bu konuda, güçlü savunma için iyi bir siber risk analizi yapmak önemlidir. Siber risk analizi, daha önce olan veya olabileceği varsayılan kuvvetle muhtemel siber saldırı ve siber savaş için oluşturulacak bir yol haritasıdır. Burada riskler ortaya konularak nasıl bir siber güvenlik stratejisi belirleneceği analiz edilir.

1.2.2.7. Siber Zorbalık

Fiziksel zorbalıkla benzerlik gösterse bile siber zorbalık, sanal ortam kullanılarak yapılan zorbalık türüdür. Bu zorbalık için elektronik zorbalık ve sanal zorbalık gibi ifadeler de literatürde kullanılmaktadır. Belsey siber zorbalığı, bilgi ve iletişim teknolojileri aracılığıyla bir kişi veya grubun karşı tarafa kasıtlı, tekrarlı ve düşmanca davranışları barındıran zarar verme davranışı[60] olarak açıklamıştır. Siber zorbalık, sanal ortamda karşıdaki kişi veya kişi grubunu küçük düşürecek, aşağılayacak ve kişilik haklarına zarar verecek biçimde iletişime geçme durumudur.

Ipsos'un Siber Zorbalık Araştırmasına göre Şekil 1.7'de de görüldüğü gibi Peru, Arjantin, Meksika ülkelerinde yaşayan insanların siber zorbalığa maruz kalma oranları oldukça yüksektir. Türkiye tabloda 12. sırada yer alırken İngiltere 5. sırada yer almaktadır. Bu durum, ülkenin siber zorbalık konusunda ciddi bir çalışma yapması gerektiğini göstermektedir.

[59] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 7.
[60] http://www.cyberbullying.ca (15.08.2020)

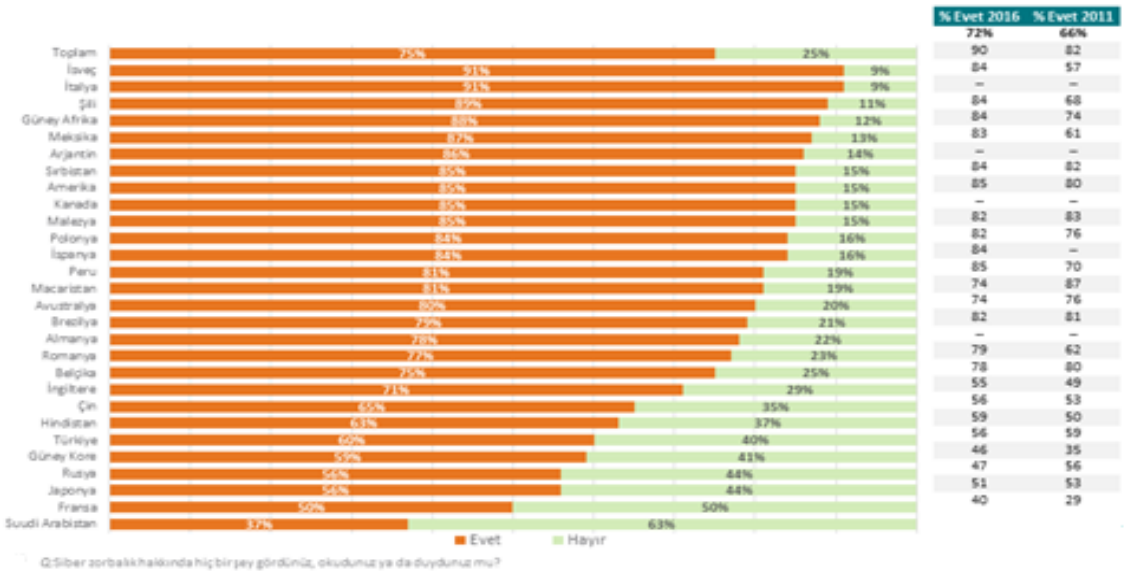
Not: Grafikte sadece N=100 den büyük ülkeler tasvir edilmiştir.

	Toplam	Arjantin	Brezilya	Kanada	Çin	İngiltere	Hindistan	Malezya	Meksika	Peru	Suudi Arabistan	Güney Afrika	Türkiye	Amerika
Sosyal Ağlar	65%	74%	70%	68%	23%	69%	66%	71%	73%	80%	56%	66%	60%	67%
Mobil	45%	48%	32%	34%	58%	36%	44%	57%	61%	51%	37%	47%	43%	46%
Online Mesajlar	38%	43%	28%	41%	57%	44%	47%	33%	40%	31%	28%	43%	36%	42%
Online Sohbet Odaları	34%	42%	28%	24%	53%	20%	50%	31%	28%	39%	42%	25%	33%	33%
Email	19%	10%	10%	14%	25%	16%	44%	23%	22%	19%	23%	13%	18%	30%
Diğer Web Siteler	14%	21%	15%	8%	8%	13%	16%	19%	25%	27%	20%	8%	10%	8%
Diğer	6%	8%	6%	4%	1%	6%	5%	9%	14%	12%	4%	9%	6%	3%

Q: Siber zorbalık yapayan çocuklar taciz olaylarını nasıl yapıyor. (Sadece çocuk sahibi olan veya kendi ailesi içinde siber zorbalığa maruz kalmış ebeveynler)

Şekil 1.7 Siber Zorbalığa Maruz Kalan Ülkeler[61]

Yine aynı araştırma kapsamında 2011 yılında siber zorbalık kavram bilinirliği %66 iken 2016 yılında bu oranın %72 olduğu Şekil 1.8'de görülmektedir. Bu da siber zorbalık kavram bilinirliğinin arttığını göstermektedir.



Şekil 1.8 Ipsos'un 28 Ülkeyi Kapsayan Siber Zorbalık Farkındalık Araştırması[62]

[61] Ipsos, *Cyberbullying A Global Advisor Survey Report*, 2018, s. 7.
[62] A.g.r., s. 2.

Siber zorbalık gençler arasında sık görülmektedir. Siber zorbalığı, kişinin genellikle yakın çevresine, okul ve sınıf arkadaşlarına yapma eğilimi vardır. Bunun nedenleri:

- Bulunulan ortamda lider olma isteği,
- Sosyal medya platformlarında yaptıkları siber zorbalık paylaşımları ile takipçi toplama düşüncesi,
- Popülarite,
- Yaşadıkları psikolojik ve duygusal boşluğu doldurma isteği gibi durumlardır.

1.2.2.8. Siber Terör

Bu kavramın uluslararası kapsamda bulunan ortak bir tanımı olmamakla beraber siber terör için, siber alan kullanılarak yürütülen her türlü terör eylemidir. Konu hakkında literatürde az sayıda çalışma mevcuttur ve siber terör, kişi veya toplumun can ve mal güvenliğini tehdit ederek zarar veren etkiler ile sonuçlanabilecek sosyal ağ, sayısal platformlar gibi siber ortam kullanılarak gerçekleştirilen saldırılar[63] şeklinde tanımlanmıştır. Atıcı ve Gümüş'e göre siber terörizm "*Bilişim sistemleri doğrultusunda, elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan, kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler*[64]" şeklinde tanımlanmıştır. Siber terör ve siber terörizm kavramlarına ilaveten siber terörist kavramı da açıklanması gereken bir konudur. Siber terör faaliyetlerini işleyen buna yardım ve yataklık eden bunun için gerekli sanal ortamı hazırlayan ve ayrıca bilişim altyapısını kuran kişi veya kişi gruplarına da siber terörist denmektedir. Siber terör, normal terör faaliyetleri ile her ne kadar benzerlik gösterse de aslında bu iki kavramın birçok farkları mevcuttur ve bu farklar Tablo 1.1'de açıkça görülmektedir.

[63] Süreyya Atasever, Özçelik, İlker ve Sağıroğlu, Şeref, "Siber Terör ve DDoS", *Journal of Natural and Applied Sciences*, S: 23, No: 1, 2019, s. 228.
[64] Bünyamin Atıcı, Gümüş, Çetin, "Sanal Ortamda Gerçek Tehditler: Siber Terör", *Polis Dergisi*, S: 37, 2003, s. 57.

Tablo 1.1 Klasik Terör ve Siber Terör Farkı[65]

	Klasik Terör	Siber Terör
Amaç Bakımından	Siyasal rejime ve topluma mesaj için terörizm bir aracıdır.	Yapılan eylemler ile toplumu, devleti veya hedef alınan organizasyona zarar verme, maddi kayba uğratmak için terörizm bir amaçtır.
Karşılaşılan Risk	Eylemi gerçekleştiren kişi ya da grup yaşamsal risk üstlenir.	Herhangi bir yaşamsal risk olmaksızın etkili saldırı
Etki Alanı	Saldırının yapıldığı bölge ile sınırlı	Ulusal, uluslararası boyutlarda etkili olabilecek saldırılar
Propaganda	Bölgesel	Küresel
Denetim	Terörü kontrol altında tutmak, izlemek ve yok etmek kısmi anlamda mümkün	Siber saldırıları belirlemek, saldırganları tespit etmek ve yok etmek neredeyse imkânsız
Kullanılan Araçlar	Silah, bomba gibi fiziksel saldırı araçları	Yazılım, virüs, e-bomba gibi sanal saldırı araçları
Uygulanacak Ceza	Suçun niteliğine göre uygulanacak ceza belli	Suçun niteliğindeki hukuki boşluklar nedeniyle belirsiz

1.3. SİBER SALDIRI TÜRLERİ

Oldukça sık karşılaşılan bu saldırılar literatürde çeşitli şekilde sınıflandırılmaktadır. Bu sınıflandırma, suçun hedef kitlesi, suçun nasıl işlendiği ve bilişim sistemini nasıl etkilediği gibi nedenlere bağlıdır. Dünya çapında yaklaşık yirmi beş siber saldırı türü mevcuttur. Etki alan kapsamı ve saldırı için kullanılan araçlar değişse de siber saldırıların ortak amacı, etkili bir saldırı gerçekleştirerek karşı tarafa zarar vermektir. Bu nedenle saldırı türlerinin bilinmesi önemlidir. Yapılan siber saldırı sonucunda etkili bir siber güvenlik stratejisi belirlenebilir. Saldırılarda ilk olarak zarar verilecek hedef kitle belirlenir. Bu hedef kitlelere göre saldırılar üç gruba ayrılabilir. Bunlar:

- Bireyleri hedef alan saldırılar,
- Herhangi bir mal varlığı veya mülkiyete yönelik saldırılar,
- Kurum ve kuruluşlara yönelik saldırılardır[66].

[65] Oğuz Kara, Aydın, Üzeyir ve Oğuz, Ahmet, "Ağ Ekonomisinin Karanlık Yüzü: Siber Terör", *V. Uluslararası Bilgi, Ekonomi ve Yönetim Kongresi,* C: 2, 2016, s. 157-158.
[66] H. Thomas Milhorn, "Cybercrime How to Avoid Becoming A Victim", *Universal Publishers,* Florida, 2007, s. 1-3.

Siber saldırılar bazen tek bir olay ile sınırlı kalırken bazen aynı saldırının birden çok yerde gerçekleştirilmesi ile olur. Bu konuda tek bir saldırı olabileceği gibi aynı saldırı biçimleri ile başka kurbanlar seçilerek seri bir saldırı zinciri de oluşturulabilir. Siber saldırı çeşitleri *bilişim sistemlerine yönelik, bilişim altyapısı ve bilişim ağına yönelik ve bilişim sistemi uygulamalarına yapılan* siber saldırı türleri olmak üzere üç ana başlıkta değerlendirilebilir.

1.3.1. Bilişim Sistemlerine Yönelik Siber Saldırı Türleri

1.3.1.1. Kötücül Yazılımlar (Malicious Software)

İngilizcesi *malicious software (zararlı yazılım)* olan ve kısaca *malware* diye adlandırılan kötücül yazılımlar bir sisteme veya bir cihaza yetkisiz erişim yoluyla uzaktan yönetme, bilgiyi ifşa etme, bilgiye sızma gibi kötü amaçlar için üretilmiş kod parçalarıdır[67]. Bulaştığı bilgisayar ağındaki makinelere zarar vererek çalışmalarını engelleyen ve istenmeyen yazılımlardır[68]. Başka bir deyişle kötücül yazılım bilişim sistemi ağına veya bilişim sistemine doğrudan bulaşarak bu sistem içinde bulunan bilgisayar, sunucu vb. cihazların hizmet verme kapasitesini engelleme amacıyla üretilen kötü amaçlı kod parçalarıdır. Kötücül yazılımlar kapsam alanı olarak çeşitlilik gösterir. Kötücül yazılımlar sistemlere verdiği hasar, bulaşma yolları ve etki alanına giren cihazlar olarak farklı zarar verme durumları ve farklı adlandırmalar ile bilinir. Bunlardan en sık karşılaşılanlar; virüs, solucan, truva atı, istenmeyen e-posta, tuş kaydedici, arka kapı, koklayıcı, kök kullanıcı takımları, casus ve fidye yazılımlarıdır. Farklı türleri de mevcuttur olabilir ancak literatürde sıkça karşılaşılan örnekleri bunlardır.

[67] Anıl Utku ve Doğru, İbrahim Alper, "Android Kötücül Yazılımlar için İzin Tabanlı Tespit Sistemi" *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, S: 32, No: 4, 2017, s. 1016.
[68] Gürol Canbek, *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme,* Gazi Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara, 2005, s. 13.

Microsoft tarafından yayınlanan Güvenlik İstihbarat Raporu (Microsoft Security Intelligence Report)'na göre kötücül yazılımların 2013 ve 2014'ün 1. ve 2. çeyreğindeki değişim oranları Tablo 1.2'de görülmektedir. Türkiye 4. sırada yer alırken İngiltere 10. sırada yer almaktadır. Yani bu iki ülke de kötücül yazılımlara maruz kalan ülkelerin başında gelmektedir.

Tablo 1.2 2013-2014 Kötücül Yazılımın Hedefi Olan Ülkeler[69]

	Ülke/Bölge	3Q13	4Q13	1Q14	2Q14
1	ABD	16.7 %	13.0 %	13.0 %	12.3 %
2	Brezilya	43.1 %	36.8 %	34.0 %	30.5 %
3	Rusya	31.7 %	28.9 %	28.7 %	26.4 %
4	Türkiye	41.3 %	45.5 %	45.7 %	40.5 %
5	Fransa	24.2 %	23.0 %	20.2 %	16.8 %
6	Hindistan	51.0 %	47.1 %	50.5 %	41.7 %
7	Meksika	39.8 %	36.7 %	38.6 %	32.1 %
8	Almanya	18.1 %	14.8 %	13.6 %	13.5 %
9	İtalya	28.3 %	26.1 %	25.5 %	20.4 %
10	İngiltere	18.2 %	14.5 %	13.5 %	13.3 %
	Dünya çapında	20.21%	21.58%	21.3 %	19.1 %

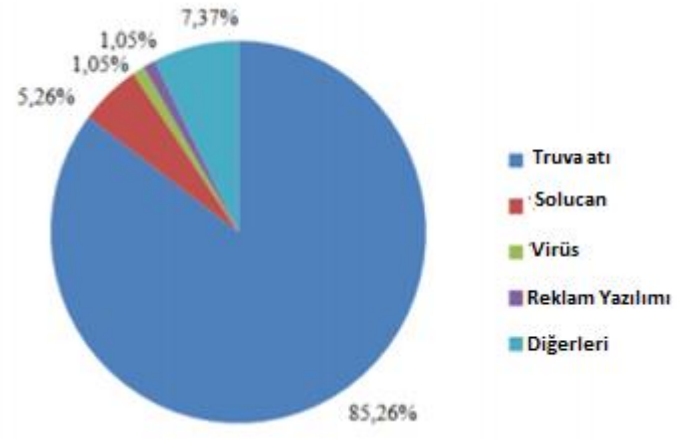
1.3.1.11.1. Virüsler

Virüs kelimesini ilk kullanan kişi 1983 yılında Fred COHEN'dir. 1984'te bu kelimeyi akademiye kazandırmıştır. Virüsler, kötücül yazılım denilince akla en sık gelen ve diğer türlere göre bilinirliği dünya çapında oldukça fazla olan kötücül yazılım türünden birisidir. Virüslerin kendi başlarına çoğalabilme yetenekleri mevcuttur ve bu çoğalma sonucu oluşan kopyalarıyla beraber farklı bilişim sistemlerine ulaşıp sistemleri kötü yönde etkileyebilen kod parçalarıdır. Yani virüsler, kendi kendine çoğalabilen ve içinde bulunduğu sistem dışında oluşturdukları kopyalarının da ulaştığı sistemlere olumsuz etki yapan siber saldırı türüdür şeklinde tanımlanabilir. Virüsler girdikleri sistemi işlevsiz hâle getirirler. Temel görevleri, kendilerini kopyalayıp arttırarak sistemi kısa sürede ele geçirmeleridir. Bunun sonucunda temel olarak

[69] Microsoft, *Microsoft Security Intelligence Report*, C: 17, 2015, s. 65.

virüslerin iki olumsuz etkisi ön plana çıkar. Birincisi yerleştiği sistemi etkisiz kılarak sistemi iş yapamaz hâle getirmek, ikincisi ise sistem için kritik sayılabilecek dosyaları imha ederek sistemde aksamalara yol açmaktır. Bu iki amaç doğrultusunda virüslerle yapılan saldırıların ne kadar kritik olduğunu ifade etmek adına örnek olarak; radyo frekans sisteminde sinyal bozma, kıtalararası balistik füze kullanımı, nükleer bomba patlatarak elektromanyetik dalga oluşturup uyduları bozma[70] verilebilir. Çok fazla virüs çeşidi mevcuttur ancak en yaygın virüs çeşitleri solucanlar, bukalemunlar, tavşanlar ve mantık bombasıdır.

Şekil 1.9'da kötücül yazılımların içinde virüsün kullanım oranı verilmiştir. Truva atları kötücül yazılım olarak kullanılan en yüksek siber saldırı türü olurken virüsler bu alanda üçüncü sırada yer almaktadır.



Şekil 1.9 Kötücül Yazılımların Oranları[71]

1.3.1.1.1.1. Solucanlar (Worm)

Siber saldırı konusunda etkili olarak kullanılan kötücül yazılımlardan biri de solucanlardır. Bunlar İngilizcede *worm* olarak adlandırılırlar ve etki alanları oldukça

[70] Aşkın İnci Sökmen, "Yeni Savaş Alanı: Uzay", *Security of the Future,* 2020, s. 94.
[71] Fanny Lalonde Levesque, Nsiempba, Jude, Fernandez, Jose M., Chiasson, Sonia, Somayaji, Anil, "A Clinical Study of Risk Factors Related to Malware Infections" *In Proceedings of The 2013 Acm Sıgsac Conference On Computer and Communications Security*, 2013, s. 101.

geniştir. Literatürde bazen ağ solucanları (network worms) olarak da adlandırılırlar. Virüsün bir çeşidi olan solucanlar tıpkı virüs gibi kendi kendilerini kopyalayabilirler. Ayrıca solucanlar girdikleri sistemde kendi kendilerine çalışarak başka bilişim sistemine ağ aracılığıyla geçebilirler. Ancak virüsten farklı olarak sisteme zarar vermek gibi bir amaç gütmezler. Ancak diğer sistemlere girdiklerinde virüs gibi davranıp sistemi bozmaya çalışabilirler. Çalışma mantığı olarak virüsten ayrılırlar ve solucanlar bağımsız çalışan virüsler sistem içindeki dosya ve programları kendilerine bağlayıp çalışırlar[72]. Kısacası solucanlar, kullanıcı müdahâlesinden bağımsız olarak kendiliğinden çalışabilen aynı zamanda kendini kopyalayarak çoğaltabilen ve çalıştırabilen ve buna ek olarak eğer ağa bağlı başka bir sistem mevcut ise burada da kendini kopyalayabilen bilgisayar programıdır[73].

1.3.1.1.1.2. Bukalemunlar

Bukalemunlar da tıpkı solucanlar gibi virüslerin alt kollarından biridir. Bukalemunlar adını bukalemun hayvanının kendini korumak için ortama göre renk değiştirme prensibine benzerliği nedeniyle almıştır. Bu saldırı türü, sisteme aldatma yoluyla sızarak sisteme ters düşmeden sistem içinde uyumlu çalışıyormuş gibi görünse de sistem içine girmeleri ile gerçek amaçları su yüzüne çıkar ve daha sonra tıpkı diğer kötücül yazılımlar gibi kötü amaçlı faaliyetlere hizmet ederler. Kullanıcı sayısı fazla olan sistemlerde kullanıcı bilgilerini taklit ederek kendisini gizli dosyaya kaydedip normal programmış gibi çalıştıktan sonra sistemin kendini kapatması ile asıl hizmet ettiği kişiye uyarı vererek gizlice kullanıcı bilgilerini kaydettiği dosyayı saldırgana ileten yazılımlardır[74].

---

[72] https://www.sonsuzteknoloji.com/virus-ve-solucan-arasindaki-fark-nedir/ (19.08.2020)

[73] Sacit Yılmaz, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *Barolar Birliği Dergisi*, S: 92, 2011, s. 75.

[74] Dilek Yüksel Civelek, *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, Devlet Planlama Teşkilatı, Uzmanlık Tezi, Ankara, 2011, s. 38.

1.3.1.1.1.3. Tavşanlar

Bu adı tavşan gibi hızlı çoğaldıklarından alırlar. Sistemi manipüle etmeye çalışırlar ve sistem işlemcisine kapasitesinden daha fazla komut göndererek hizmet aksamasına neden olurlar. Kısacası sisteme fazla yüklenerek sistem işlevselliğini bozarlar.

1.3.1.1.1.4. Mantık Bombası

Virüslerin bir çeşidi olan mantık bombaları ancak istenilen şartlar yerine geldiğinde tetiklenip aktif olurlar. Bu yönüyle diğer virüs çeşitlerinden ayrılırlar. Yani bunlar belirli bir zaman ve koşul meydana geldiğinde[75] sistemde etki gösterirler. Bu hususta saldırganın belirlediği koşullar gerçekleşince sistemdeki dosyaları silebilir ve bununla beraber tüm sistemin çökmesine neden olabilecek zararlı faaliyetler yürütebilirler. Kısaca mantık bombaları belirli programlar içine özel olarak yerleştirilen kod ve yazılımların genel adıdır. Dünya çapında en iyi örneği Çernobil patlamasına neden olan mantık bombalardır. Bunlar Çernobil virüsü olarak da adlandırılır.

1.3.1.1.2. Truva Atları (Trojen Horses)

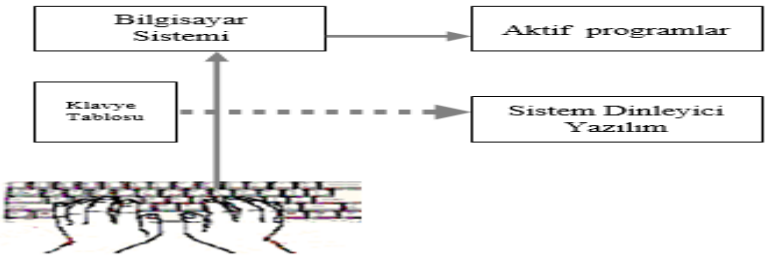
Truva atları bu ismi savaş taktiğinden almıştır. Tıpkı Truva atının düşman alanına girdikten sonra kendi askerlerinin düşman topraklarını işgal etmesi gibi Truva atları da sistemler için yararlı ve yasal gibi görünerek şüphe uyandırmadan sistemleri arka planda uzaktan yönetmeyi amaçlarlar[76]. Bunu arka kapıları açarak yaparlar. Saldırgan Truva atı sayesinde sistemde bulunan cihazlarla bir "Bot" yani "zombi" ağı oluşturarak sistemdeki bu cihazları kendisine köle yaptıktan sonra her türlü hassas içeriğe erişip yönetebilir. Botnet robot ve network kelimelerinin birleşmesiyle oluşan

[75] Vahit Güntay, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", *Güvenlik Stratejileri Dergisi*, S: 14, No: 27, 2018, s. 83.
[76] Murat Güngör, *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, T.C. Kalkınma Bakanlığı, Uzmanlık Tezi, Ankara, 2015, s. 49.

melez bir sözcüktür[77] ve sistemde Truva atlarının verdiği komutları yaparlar. Bunu arka tarafta sistem güvenliğini tehlikeye atarak ve sistemde bulunan verilerin bütünlüğünü tehlikeye sokarak yaparlar. Asıl hizmet ettiği botnet'in sahibidir.

1.3.1.1.3. Tuş Kaydediciler (Keyloggers)

Literatürde klavye dinleme olarak da adlandırılan tuş kaydediciler İngilizcede keylogger olarak adlandırılmaktadır. Çalışma mantıkları kişi, kurum veya kuruluşlarda bulunan ve bilgisayar klavyesine veya tuş takımına sahip birçok elektronik cihaz içinde basılan tuşları hafızasına alarak kaydeden ve bunun sonucunda amacı saldırgana hizmet etmek olan yazılım türüdür. Tarihi eski olmamakla birlikte her geçen gün bu saldırı türü yaygınlaşmaktadır ve özellikle finans sektörü için oldukça büyük bir tehlike arz etmektedir. Çünkü basılan her tuş bir veridir. Şekil 1.10'da tuş kaydedicisi, kullanıcının bastığı tuşu klavye tablosuna kaydetmektedir.



Şekil 1.10 Klavye Tablolama Yöntemi[78]

Bu açıdan sisteme girişlerde kişileri korumanın en temel yolu Şekil 1.11'deki gibi sanal klavye kullanımı olmalıdır.

[77] https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks (20.08.2020)
[78] Meriç Say ve Sağıroğlu, Şeref, "Bilgisayar Veri Güvenliği Üzerine Bir İnceleme: Klavye Dinleme Sistemleri", s. 3.



Şekil 1.11 İnternet Bankacılığına Girişteki Sanal Klavye Örneği[79]

1.3.1.1.4. Arka kapılar (Back Doors)

Arka kapılar, sistemsel açıkları kullanmanın en iyi yöntemlerinden biridir. Arka kapılar İngilizce "*back doors*" kelimesine karşılık gelmektedir. Amaç, sistem açıklarını bularak sisteme bu yolla sızma girişimidir. Saldırı kısmının en kritik noktası, sistem açıklarını bularak bu sisteme nasıl erişebileceğini anlamaktır. Kısacası arka kapılar, sistemde normal analizlerle elde edilemeyecek bilgilerin yasa dışı faaliyetlerle erişilerek kimlik denetim sürecinin atlanması veya o sisteme uzaktan erişim yöntemine verilen durumların tamamını oluşturan kötücül yazılımlardır. Arka kapılar sistem açığı tespit ettiklerinde açıktan emin olmak için sistemin tüm giriş portları saldırgan tarafından taranır. Çalışma mantığı olarak arka kapılar Şekil 1.12'de görülmektedir.



Şekil 1.12 Arka Kapıların Çalışma Prensibi[80]

[79] https://esube.albaraka.com.tr/ (25.08.2020)
[80] Mehmet Emin Arslan, "Siber Güvenlik ve Siber Saldırı Türleri", 2016 s. 6.

1.3.1.1.5. Koklayıcı (Sniffer)

Literatürde şebeke trafiği dinlenmesi olarak da karşılaşılan koklayıcılar, İngilizce "*sniffer*" kelimesinden gelmektedir ve yapılan işleme sniffing yani koklama adı verilmektedir. Koklayıcılar veri yolunu keserler ve ağ üzerindeki paketleri tutup içerik okuyabilirler. Koklayıcının temel amacı, cihaz ve ağ arasındaki bilgi trafiğini şebeke içine girerek dinlemektir. Trafikteki elde edilen veriler yakalanır ve saklanır. Bunu, şifreleme açığı bulunan ağ trafiğinde yaparlar. Toplanan veriler, gönderilmiş e-postalar, veri transferinde aktarılan her türlü görüntü, ses ve video olabilir.

1.3.1.1.6. Kök Kullanıcı Takımları (Rootkits)

Saldırı yöntemlerinden yeni duyulan ama etkili olan türlerden biridir. İngilizcede "*rootkits"* olarak bilinirler ve en tehlikelisi çekirdek rootkitleridir. Bunlar en yüksek ayrıcalık düzeyinde çalıştıkları ve kurbanın kaynaklarına sınırsız erişime sahip olmaları nedeniyle bilgisayar sistemleri için çok ciddi bir tehdit oluştururlar. Bunlar işletim sistemlerine çekirdek modülü olarak kurulduktan sonra sistemi bozan yazılımlardır. Sisteme sürekli zarar veremezler ve sistemin kapanması ile etkilerini kaybederler. Kök kullanıcı takımları, siber saldırı gerçekleştiren kişi için işletim sistemindeki verileri gizlice değiştiren kötücül yazılımlardır[81]. Kök kullanıcılar, tuş kaydedici olarak bilinen keyloggerları da gizleyerek birçok gizli bilgiye yetkisiz ulaşabilir ve ayrıca sisteme arka kapılar da kurabilir. Anti virüs, güvenlik duvarı gibi kritik güvenlik elemanları da devre dışı bırakabilir[82] ve bu özellikleri dolayısıyla birden çok işlevi kendisini sistemde gizleyerek yerine getirir. Bunun tespiti için çekirdek içindeki kök kullanıcı savunması, bir kök kullanıcı saldırısından

[81] Bickford, Jeffrey, O'Hare, Ryan, Baliga, Arati, Gnapathy, Vinod, Iftode, Liviu, "Rootkits on smart phones: attacks, implications and opportunities", *Proceedings of the eleventh workshop on mobile computing systems and applications*, 2010, s.49.

[82] Baliga, Arati, Kamat, Pandurang ve Iftode, Liviu, "Lurking in the shadows: Identifying systemic threats to kernel data." *2007 IEEE Symposium on Security and Privacy (SP'07)* IEEE, 2007, s. 246.

sonra çekirdek için olabilecek kök kullanıcıların tespit edilmesini inceler[83]. Bunun sonucunda sistemi korumak adına, son yıllarda işletim sistemine kötü amaçlı kod enjeksiyonu engelleme konusunda bu yöntemle önemli yol kat edilmiştir[84].

1.3.1.1.7. Casus Yazılım (Spyware)

Casus yazılım konusunda; kötücül yazılımın bir alt kategorisi olduğu[85] ve casus yazılımın kötücül yazılım türlerinden ayrı değerlendirilmesi gerektiği düşünceleri mevcuttur. Casus yazılım, sistemdeki verileri toplayarak bilgileri sistem dışıyla paylaşan yazılım türüdür.

1.3.1.1.8. Fidye Yazılım (Ransomware)

Mantık olarak zararlı yazılımlar gibi davranan fidye yazılımların zararlı yazılımlardan farkı, eriştiği sistem içinde kullanıcıya ait verileri şifreleyerek kullanıcının verilerine tekrar erişebilmesi için fidye talep eden kötücül yazılım türüdür. Bu yazılımlar içlerinde güçlü şifreleme algoritmaları barındırarak bulaştıkları sistem verilerini şifreler ve asıl kullanıcının kendi verilerine ulaşmasını engeller. Burada istenen fidye miktarı ödendikten sonra bu verilere sadece kullanıcı kendisine verilen özel anahtar ile erişebilir. Yani fidye yazılımlar, bulaştıkları sistemi tamamen veya etki alanına giren verileri şifreleyip dosyalara erişimi engelledikten sonra erişim şartı olarak fidye talep eden yazılımlardır[86]. Bu yönüyle diğer kötücül yazılımlardan ayrılırlar.

---

[83] Riley, Ryan, Jiang, Xuxiian ve Xu, Dongyan, "Guest-Transparent Prevention of Kernel Rootkits with Vmm-Based Memory Shadowing" *International Workshop on Recent Advances in Intrusion Detection,* Springer, Berlin, Heidelberg, 2008, s. 1.

[84] Li, Jinku, Wang, Zhi, Jiang, Xuxian, Grace, Mike ve Bahram, Sina "Defeating Return-Oriented Rootkits with" Return-Less" Kernels, *Proceedings of The 5th European Conference on Computer Systems*, 2010, s. 200.

[85] Gürol Canbek ve Sağıroğlu, Şeref, "Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler", *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, S: 23, No: 1, 2008, s. 165.

[86] İlker Kara, "Teslacrypt Fidye Yazılım Virüsünün Tespiti, Teknik Analizi ve Çözümü", *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, S: 2, No: 2, 2018, s. 88.

1.3.2. Bilişim Altyapısı ve Bilişim Ağına Yönelik Siber Saldırı Türleri

Burada bilişim altyapısını ve bilişim ağını hedef alan saldırılar ön plana çıkmaktadır. Zayıf bilişim ağları siber saldırganlar için açık bir hedef hâlindedir. Bu hedeflere ulaşmak kimi zaman bir ağ açığı olsa da bazen de etkin şifrelemenin olmamasından kaynaklanır.

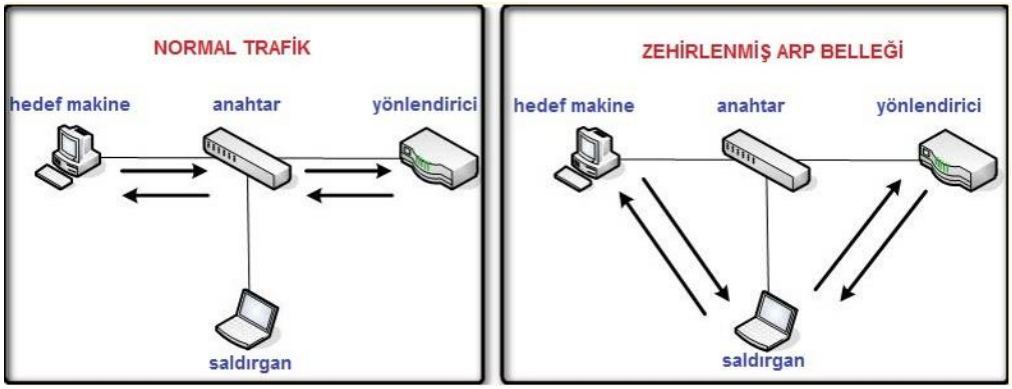
1.3.2.1. DNS ve ARP Zehirlenmesi

DNS İngilizce "*Domain Name System"* kelimelerinin kısaltmasından oluşan alan adlandırma sistemi olarak bilinir. Ağ üzerinden aranan anahtar kelimeleri ağ sisteminin anlayabileceği IP (Internet Protocol) adreslerine çevirir. Her aranan kelimeyi karşılayan bir IP adresi mevcuttur. Örneğin arama motoruna "8.8.8.8." IP adresi yazıldığında bunu karşılık gelen site Google'ın ana sayfası olacaktır. DNS çevirici bir işlem görmektedir. ARP ingilizce "*Adress Resolution Protocol"* olarak bilinen adres çözümleme protokolüdür ve kısaca IP adresine sahip cihazların fiziksel adresinin öğrenilmesini sağlar. Fiziksel adres MAC (Media Acess Control) yani *ortam erişim yönetimi* adresidir ve 48 bitli 12 haneden oluşan 16'lık tabanda oluşturulurlar[87]. DNS zehirlenmesi, DNS sunucusunun önbellek bilgilerini değiştirerek sunucu isminin yanlış IP adresine gönderilmesine neden olur, bu da saldırganın trafiği istediği bir cihaza yönlendirilmesini sağlar ve trafik buradan ilerler. Bu durum sonucunda saldırgan, yapacağı saldırıları masum kullanıcının cihazı üzerinden yapar[88]. ARP zehirlenmesi ise çalışma prensibi olarak DNS zehirlenmesine benzerdir. ARP zehirlenmesi, ağda bulunan ve dolanan verilerin ARP ön belleğinin değiştirilmesiyle beraber yetkisiz kişiye yönlendirilmesi ile elde edilmesidir. Veri alışverişinin iki hedef arasında yapılması yerine veri gönderen kaynaktan çıkar, hedefe ulaşmak yerine önce dinleyiciye gider ve daha sonra hedefe ulaşır. Bu, aktarılan tüm verilerin elde edilmesi

[87] https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/arp-(adres-%C3%A7%C3%B6z%C3%BCmleme-protokol%C3%BC) (02.09.2020).

[88] Gözde Karataş, Akbulut, Akhan, Zaim ve Abdül Halim, "Mobil Cihazlarda Güvenlik–Tehditler ve Temel Stratejiler", *Istanbul Commerce University Journal of Scienc,* S: 15, No: 30, 2016, s. 61.

anlamına gelir. Başka bir ifade ile IP adresine karşılık sahte bir MAC adresi oluşturularak saldırganın ağ trafiğini kendine yönlendirmesi[89] olarak düşünülebilir. Şekil 1.13'te olması gereken bir ağ trafiği ve ARP zehirlenmesine maruz kalan ağ trafiği görülmektedir.



Şekil 1.13 Normal ve Arp Zehirlenmesine Maruz Kalmış Ağ Trafiği[90]

1.3.2.2. Oltalama (Phishing)

Literatürde sazan avlama, yemleme ve kimlik avı gibi adlandırmalar ile de karşılaşılan oltalama yöntemi adını İngilizcedeki "*phishing"* kelimesinden alır. Bu adın verilmesi balık avlama yöntemiyle benzerliğinden almaktadır. Bu yöntem için, saldırgan güven duyulacak bir kişi veya duruma bürünerek kurbandan hassas bilgilerini paylaşması ister. Bu yöntem kullanılırken saldırgan kendini prestijli veya uzman kişi olarak göstererek güven duygusu aşılmaktadır[91].

[89] Fatih Ertam, Tuncer, Türker ve Engin, Avcı, "Adli Bilişimde Ağ Cihazlarının Önemi ve Güvenilir Yapılandırmaları", *Engineering Sciences*, S: 8, No: 3, 2013, s. 175.
[90] http://berkay22demirel.blogspot.com/2017/10/bilgisayar-aglar-ders-7-arp-zehirlenmesi.html?m=0 (09.09.2020)
[91] Tom Jagatic, Johnson, Nathaniel, Jakobsson, Markus ve Menczer, Filippo, "Social Phishing" *Communications of the Acm*, S: 50, No: 10, 2007, s. 94.

1.3.2.3. Sosyal Mühendislik

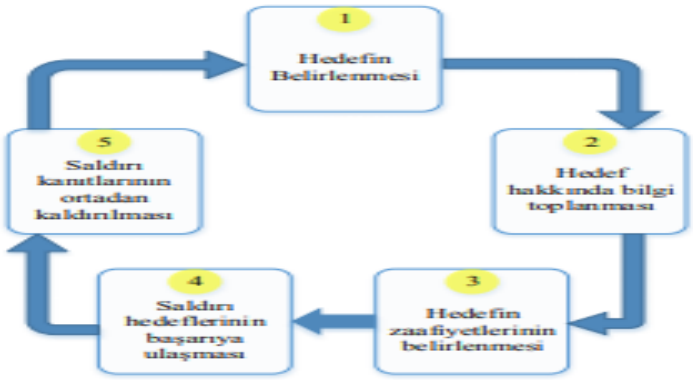
Son dönemlerde sıkça karşılaşılan yöntemlerin başında gelen sosyal mühendislik, insanların küresel dünyada sosyal ağlar vasıtasıyla yoğun bir etkileşime girmesi ile büyük bir hız kazanmıştır. Sosyal mühendislik, teknolojinin ilerlemesine göre kendini değiştiren ve geliştiren bir türdür. Sosyal mühendislik, güvenliğin en zayıf halkası olan insanı çeşitli yollarla kandırıp devre dışı bırakarak istediklerini elde etme yöntemidir. Yani sosyal mühendislik kurbanı etkileme bazen zorlama ve hatta sahte ilişkilerle bağlılık ve dürüstlük gibi ilkeleri aşılayarak kişinin normalde paylaşamayacağı gizli ve önemli bilgilerini paylaşmasını sağlayan yöntemlerdir[92]. Bu konuda kullanılan yöntemler, temel olarak ikiye ayrılır. Bunlar:

- Teknoloji temelli Sosyal Mühendislik Yöntemleri
    - Oltalama saldırıları
    - Ortadaki adam
    - İstenmeyen e-postalar
    - Truva atları, solucanlar vb.
- İnsan temelli Sosyal Mühendislik Yöntemleri
    - Sahte senaryo kurgulama
    - Omuz sörfü: Klavyede tuşlama yaparken kurbanın bilgilerini çalma yöntemi.
    - Güven kazanarak bilgi edinme
    - Kendini zavallı gösterme
    - Telefon oltalaması (Voice Phishing) saldırıları: Kısaltması vishing olan ve kendini telefonda emniyet memuru, hâkim veya savcı gibi tanıtarak kurbanı kandırma yöntemi.

[92] Hasan Bağcı, "Sosyal Mühendislik ve Denetim", *Denetişim*, S: 1, 2009, s. 43.

- Çöp kurcalama (Dumpster Mixing): Çöp karıştırmada denen bu yöntemde bilgi elde etmek için kurbanın çöpünü habersizce karıştırma yöntemidir[93].

Görüldüğü gibi sosyal mühendislik birçok saldırı tür ve yöntemi kullanılmaktadır. Şekil 1.14'te sosyal mühendislik yaşam döngüsü görülmektedir.



Şekil 1.14 Sosyal Mühendislik Yaşam Döngüsü[94]

1.3.2.4. Hizmet Dışı Bırakma (DoS)

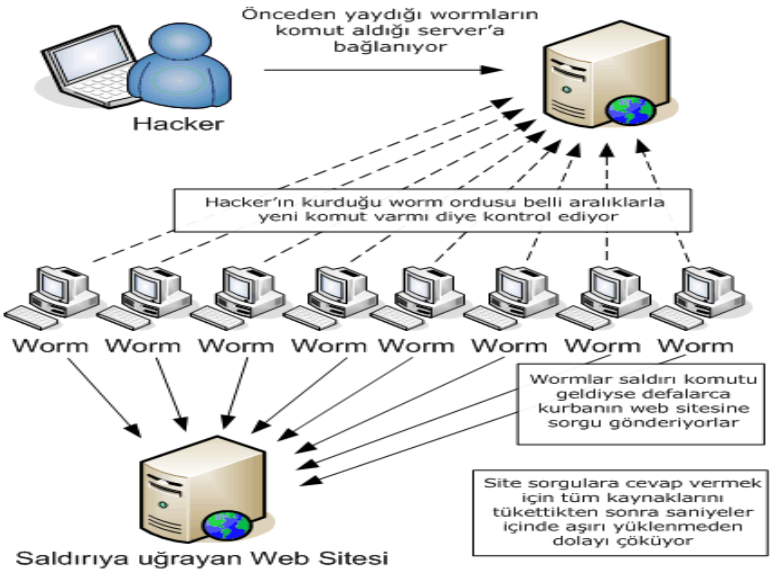
Denial of Service olarak bilinen ve dilimize servis reddi veya servis dışı bırakma olarak geçen DoS saldırıları ağ saldırıları içinde sıklıkla karşılaşılan saldırılardır. Bu saldırılar, yasal olarak erişilmek istenen bilgiye erişim yetkisi olan istemcilerin, sistem erişimlerini engellemeyi amaçlar. Bu yüzden hizmet aksamasına veya hizmetin tamamen devre dışı kalmasına yol açar. Saldırgan, talep edilen sunucuya sürekli istek göndererek cevap verme kapasitesini zorlar ve sistem sunucusunun cevap verme potansiyelini aşmasını sağlayarak hizmeti servis dışı bırakır. Bu saldırı, büyük kurum ve kuruluşlar için önemlidir. Örneğin alışveriş sitesi

[93] Anıl Keskin, Duygu ve Gözenman, Samet, "Hile Riski Açısından Sosyal Mühendislik", *Tıde Academıa Research*, S: 1, No: 2, 2019, s. 288-291.
[94] M. Zekeriya Gündüz ve Daş, Resul, "Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri" *Pd Ş. Sağıroğlu, Pdm Alkan, Pde Akyıldız Ve Dds Akleylek, Ed*, 9, 2016, s. 2.

için bir dakikalık erişim kesintisi bile ciddi mali kayıplara yol açabilir. Bu yüzden DoS atak belirtilerini önceden anlamak gerekir. DoS atak belirtilerine örnek olarak:

- Alışılmışın dışındaki düşük ağ performansı,
- Web sitesindeki belirli kısımlarına erişememe,
- Web sitesine erişimde güçlük yaşanması,
- Email kutusundaki spamların artışı[95] gösterilebilir.

DDoS (Distributed Denial of Service) ise DoS ile aynı saldırı türü olarak görülse de aslında DoS'a göre daha gelişmiştir. DoS saldırısında tek bir hedefe yönelik servis dışı bırakmak sağlanırken DDoS saldırılarında saldırı birden fazla kaynaktan dağınık şekilde yapılır ve zombi cihazlarla botnetler oluşturulur. Şekil 1.15'te DDoS saldırı mimarisi görülmektedir. DoS ve DDoS saldırılarının ortak özelliği sisteme girmek değil, sisteme ulaşılmasını ve sistemin hizmet vermesini engellemektir.

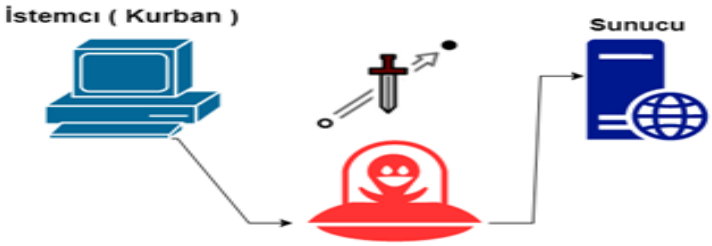


Şekil 1.15: DDoS Saldırı Mimarisi[96]

[95] Deniz Mertkan Gezgin ve Buluş, Ercan. (2008), "Kablosuz Erişim Noktalarına Yapılan DoS Saldırıları" *Akademik Bilişim*, 2008, s. 87.
[96] https://yazilimportal.com/dos-sald%c4%b1r%c4%b1s%c4%b1-nedir-ve-nas%c4%b1l-korunulur-e1c6f4895cfd (16.09.2020)

1.3.2.5. Ortadaki Adam (Man in The Middle) Saldırıları

Kısacası MITM (Man in The Middle) saldırıları olarak bilinen ortadaki adam saldırıları, saldırganın kurbanın iletişime geçtiği ortam ile kurban arasındaki verilere ulaşabildiği, bu verileri değiştirebildiği ve aralarındaki trafiği dinlediği saldırı biçimidir. Saldırgan gönderici, alıcı ve ikisi arasında gönderilen her bilgiyi koklar[97]. Bu saldırı türünün nasıl gerçekleştiği Şekil 1.16'da görülmektedir.



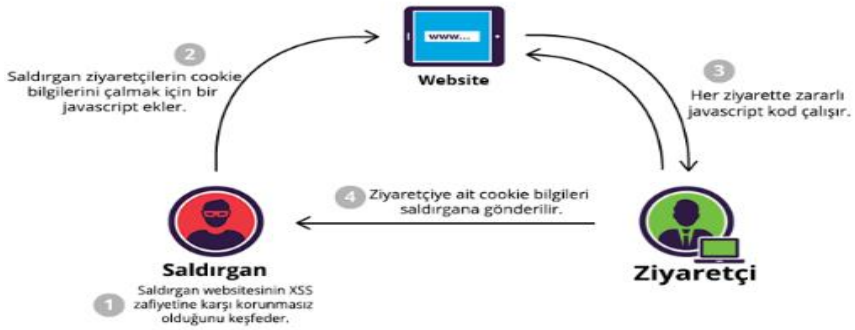
Şekil 16: MITM Saldırısı[98]

1.3.2.6. Siteler Arası Betik Çalıştırma (XSS)

Siteler arası betik çalıştırma, Cross Site Scripting (XSS) olarak da bilinen script kodları ile web sayfasına yapılan saldırı biçimidir. Literatürde XSS için HTML (Hyber Text Markup Language) enjeksiyon veya betik enjeksiyonu da denilir. Güvenilir olmayan web sitesine giren kullanıcı girdisini, tarama işlemine tabi tutmadan gösteren web sayfasındaki kaynak kod içerisinde yer alıp istemci tarafında betik çalıştırılmasıdır[99]. Bu, saldırganın kurbanın tarayıcısıyla birlikte oturumlarını ele geçirmesine, web sitesini değiştirmesine veya kullanıcıyı kötü niyetli sitelere

[97] Bing, Chen Wu, Jianmin, Wu, Jie ve Cardei, Mihaela, " A Survey Of Attacks and Countermeasures in Mobile Ad Hoc Networks ", *Wireless Mobile Network Security* Springer, Boston, MA, 2007, s. 116.
[98] https://medium.com/@oguzalbastr02/ortadaki-adam-sald%c4%b1r%c4%b1s%c4%b1-mitm-detayl%c4%b1-anlat%c4%b1m-5e5f86af1d6a (16.09.2020)
[99] Özel, Abdurrahin, Kaya, Çetin ve Eken, Süleyman, "Javascript Güvenlik Açıkları ve Güncel Çözüm Önerileri", 7. *Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı*, 2014, s. 254.

yönlendiren komut dizilerini yürütmesini sağlar[100]. Çalışma prensibi Şekil 1.17'de görülmektedir.



Şekil 1.17: XSS Çalışma Prensibi[101]

1.3.3. Bilişim Sistemi Uygulamalarına Yapılan Siber Saldırı Türleri

1.3.3.1. Parola Saldırısı (Password Attack)

Kullanıcı sistem girişi ve şifre isteyen tüm uygulama ve web siteleri için oluşturulan şifrelerin etkisiz hâle getirildiği veya bu şifrelerin kırılarak ele geçirildiği saldırılardır. Amaç, sistemdeki yetkili kişinin şifresi öğrenilerek yasal yollarla sisteme giriş sağlanmasıdır. Online (aktif) ve offline (pasif) olarak parola kırılabilir. Bu konuda kullanılan etkili yöntemlerden bazıları:

- Medusa, Hydra, John The Ripper[102]
- Kötücül Yazılımlar
- Oltalama
- Omuz Sörfü
- Sosyal Mühendislik örnek olarak verilebilir.

[100] Daşdemir, Atakan, *Türkiye'de En Çok Ziyaret Edilen Bazı Web Sitelerin Güvenlik Değerlendirmesi*, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya, 2018, s.23.
[101] https://medium.com/@kerem_tamci/stored-xss-ve-microsoft-e7a17b9040c (18.09.2020)
[102] Kaya, Ömer Faruk ve Öztürk, Erdinç, "Veri ve Ağ Güvenliği için Uygulama ve Analiz Çalışmaları", *Istanbul Ticaret Universitesi Fen Bilimleri Dergisi*, S: 16, No: 31, 2017, s. 94-95.

1.3.3.2. Kripto Krikosu (Crypto Jacking)

Bitcoin gibi sanal paralar üzerinde yapılan saldırılar, kripto krikosu olarak tanımlanır. İngilizce *crypto jacking* olan bu saldırı temelde kripto yani şifrelenmiş sanal paralara yönelik yapılmış veya yapılmakta olan saldırı modelidir. Burada paraları yetkisiz erişim yoluyla elde etmek amaçlanmaktadır. Bu konuda masum kurbanlar para korsanlarına karşı kriptolu sanal paralara sahip olsalar dahi kripto krikosu şifrelenmiş bu sanal paralar üzerinde kötü amaçlı yazılım ile birlikte kod çözme teknikleri kullanarak erişim sağlayabilir.

1.3.3.3. Sıfır Gün İstismarı (Zero Day Exploit)

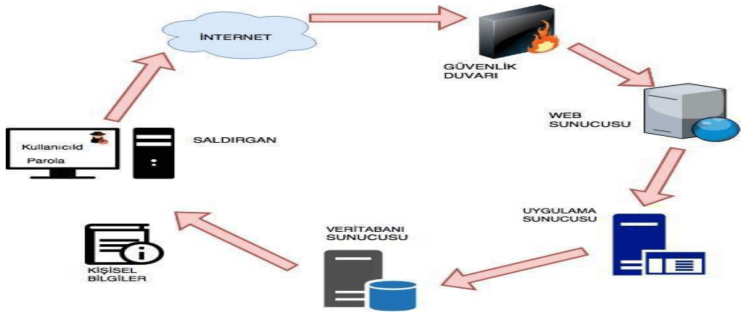
Sıfır gün istismarı, daha önceden bilinmeyen veya fark edilmemiş ancak kötü sonuçlara neden olabilecek her türlü donanımsal veya yazılımsal açıklara verilen durumu ifade eder. Bu nedenle sıfır gün saldırıları gerçekleşmeden saldırının tespiti neredeyse imkânsızdır. Burada sistem, donanım veya yazılım açıkları bulunduğu anda saldırgan bu açığın kapatılmasına fırsat vermeden saldırır. Sıfır gün istismarı, kendini belli etmediği için tespiti de çok zordur. Saldırı önceden öngörülemez. Klasik bir sıfır gün istismarı sistemde habersiz biçimde yaklaşık 300 gün aktif kalabilir. Bu süre bazen 2,5 yıla kadar uzayabilir. Bu açık, bilindikten sonra saldırı şekli daha çok artmaktadır[103]. Yani sıfır gün açıkları bulunup ortaya çıkarıldığında bunlar yeni sıfır gün açıklarına yol gösterir.

1.3.3.4. SQL (Structured Query Language) Enjeksiyon

Burada oluşturulan web uygulamaları için kullanıcıların girdikleri veriler ile yapılmış SQL sorgularında manipülasyon yapma işlemidir[104]. Bu, fazla veri yığını

[103] Oğuz Bozoklu ve Çil, Celal Zaim, "Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, S: 3, No: 1, 2017, s. 17.
[104] Chris Anley, "Advanced SQL injection in SQL server applications", *An NGSSoftware Insight Security Research (NISR) Publication*, 2002, s. 3.

taşıyan veri tabanları için ciddi bir saldırı yöntemidir. SQL enjeksiyonu, veri tabanında SQL ile işlemler yapıldığı sırada devreye girer ve SQL enjeksiyonu için saldırgan verinin ait olduğu kullanıcı girişi veya web sitesine kötücül yazılım göndererek veri tabanına ulaşma ve SQL enjeksiyon yapma fırsatı bulur. Amaç, veri tabanındaki hassas içerikli verilere ulaşmaktır. Bunun da en kesin yolu veri tabanına sızmaktır. SQL enjeksiyonda, saldırgan kurbanı kullanarak veri tabanına kötücül kod parçalarını enjekte ettirebilir[105]. Bunun sonucunda verilere ulaşım sağladıktan sonra saldırgan veri tabanını amaçları doğrultusunda yönetmeye başlar. Şekil 1.18'de SQL enjeksiyonun nasıl gerçekleştiği görülmektedir.



Şekil 1.18: SQL Enjeksiyon Yaşam Döngüsü[106]

1.4. SİBER SALDIRININ TARİHSEL GELİŞİMİ

Siber saldırının geçmişine bakıldığında her ne kadar tarihi eski olmasa da insanlığa verdiği zararlar oldukça büyüktür. Bu zararlar, kimi zaman bir bireye kimi zaman prestijli bir kuruma kime zamanda ülkelere karşı yapılmıştır. Hedef kitlesine göre saldırganın kurbandan elde etmek istediği bilgiler farklılık gösterebilir. Saldırılar şöhret, para, güç ve millî duygular ile yapılabilir. Bu çalışmada siber saldırının tarihsel süreci incelenirken görsel-işitsel medya, çıkan haberler, blog sayfaları ve literatür çalışmalarına göre kronolojik bir sıralama yer alır.

[105] Kara İlker ve Aydos, Murat, "Detection and Analysis of Attacks Against Web Services By the SQL Injection Method", In *2019 3rd International Symposium On Multidisciplinary Studies And Innovative Technologies (ISMSIT)*, 2019, s. 1.
[106] https://womaneng.com/sql-injection-nedir/ (20.09.2020)

1971 yılında Bold, Beranek ve Newman tarafından ekrana "*I'm the creeper, catch me if you can*" yazdıran ve kendi kendine çoğalma özelliği olan zararsız Creeper Virüsü oluşturulmuştur[107]. Bu virüs, özellik olarak zararlı bir virüs değildi. 1981 yılında bilgisayar virüsü kavramı Prof. Leonard M. Adelman tarafından ortaya atılmıştır. 1982 yılında Rich Skrenta, arkadaşlarıyla eğlenmek için virüs yazmıştır. Yine 1982 yılında Sibirya doğalgaz boru hattında patlamaya neden olan mantık bombaları kullanılmıştır[108]. Virüsü literatüre kazandıran 1984 yılında doktora çalışması ile Fred Cohen olmuştur. Bilgisayarları koruma amaçlı ilk virüs 1986 yılında Basit ve Amjad Farooq Alvi kardeşlerce yazılmıştır. Brain adlı bu virüs saldırganın zarar vermesini engellemek maksadıyla yazılsa da ilerleyen zamanlarda kullanım amacının dışında çıkmıştır. Yine aynı yılda mantık bombası kullanılarak maddi zararların yanı sıra insan sağlığını da ciddi yönde etkileyen Çernobil Nükleer santralinin patlatılmasına neden olmuştur. Bu mantık bombası, CIH virüsü olarak bilinen mantık bombası yazılımcısı tarafından yararlı bir yazılım olduğu söylenerek[109] piyasaya sürülmüştür. İnternet üzerinde çevrim içi bulunma durumunun artmasıyla e-posta trafiği de yaygınlaşmıştır. Bu durum saldırganlara yeni fırsatlar vermiş ve kötücül yazılım bulaştırma oranı artmıştır. 1987 yılında Clausthal Teknoloji Üniversitesinde okuyan öğrencilerden biri tarafından yazılan "Christmas Tree" adındaki solucan sistemlere enfekte olmuştur ve bu sistemler içinde Avrupa Akademik Araştırma Ağı (EARN), BITNET ve Uluslararası İş Makineleri (IBM)[110] gibi birçok önemli kuruluş vardı. Bu yüzden dünya çapında birçok zarara yol açmıştır. Teknolojideki ilerlemeler ile virüsün rolü zamanla değişime uğramış ve ilk şifrelenmiş virüs Cascade oluşturulmuştur, bu virüs bulaştığı cihazların şifresini değiştirmiştir. Virüsle yapılan ve tarihe geçen ilk siber saldırı 1988 Kasım ayında Robert Tappan Morris tarafından yapılmıştır. Aslında Morris'in amacı, internetin kapasitesini ölçmektir ve bu amaç için yazdığı programı internete yüklemesi ile internetin çökmesine neden olmuştur ancak bunu zarar vermek amacıyla yapmamış sadece

[107] https://siberci.com/siber-guvenlik-tarihi/ (24.09.2020)
[108] Yılmaz, Onur, "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", *Cyberpolitik Journal*, S: 2, No: 3, 2017, s. 29.
[109] Berrin Akbulut, *Türk Ceza Hukuku'nda Bilişim Suçları,* Yayınlanmamış Doktora Tezi, Konya, 1999, s. 59-60.
[110] https://en.wikipedia.org/wiki/Christmas_Tree_EXEC (27.09.2020)

kapasite ölçümü yapmak istemiştir. Morris'in yazdığı bu program, "Morris Solucanı" olarak adlandırılır[111]. Ağ tabanlı küresel saldırı örneği olarak bilinir.

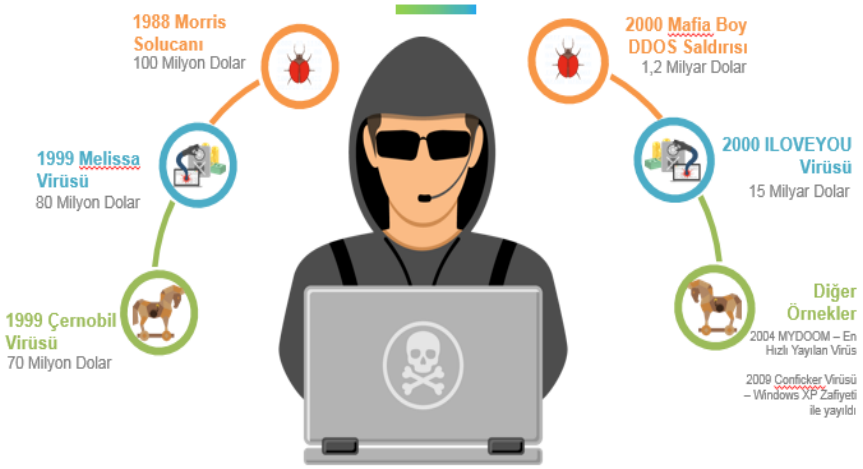
1989 yılında yaygın olarak bilinen ilk Truva atı fidye yazılım şeklinde oluşturulmuştur. "AIDS Truva Atı" olarak isimlendirilmiştir. Bu Truva atı, AIDS hastalığıyla ilişkili olan disketler aracılığıyla posta yoluyla dağıtılarak bulaşmıştır[112]. 1995 yılında bilgisayarları bozan yazılım ve virüsler yerini, kullanıcı etkinliğini izinsiz gözetlemeye yönelik yazılımlara bırakmıştır. 1998 yılında ilk DDoS saldırısı Pentagon ve Meksika hükümetine karşı yapılmıştır. En eski ve etkili olan Truva atı Melissa 1999 yılında yazılmış ve birçok kişiye Word belgesi göndererek yayılması hızlı olmuştur.

2000'li yıllarda da çeşitli siber saldırılar devam etmiştir. 2000 yılında I LOVE YOU virüsü e-posta aracılığı ile tüm dünyaya yayılmış ve verdiği zarar sonucu diğer virüs türlerine örnek olmuştur[113]. 2004 yılında spam yoluyla Mydoom virüsü yayılmış ve bu ulaştığı cihazları birer botnet hâline getirip kendi amacı doğrultusunda köleleştirmiştir. İlerleyen yıllarda cihazların işletim sistemlerine arka kapılar eklenmiştir. Rusya'nın yaptığı düşünülerek sorumlu tutulduğu 2007 yılı Estonya siber saldırısı ve Rusya'nın 2008 yılında Gürcistan'a gerçekleştirdiği siber saldırı, siber saldırıları siber savaş boyutuna taşımıştır[114] ve devamında 2008 yılında doğrudan Microsoft'u hedef alan saldırı düzenlenerek Windows işletim sistemlerine Conficker adı verilen solucan botnet oluşturma amacıyla bulaştırılmış[115] ve bu dünya çapında ciddi mali zarara neden olmuştur. Elbette siber saldırı dünyasına bomba etkisi yapan ve iki ülke gerginliğinin en net hissedildiği saldırı, 2009 yılında gerçekleşen Stuxnet İran Nükleer yakıt zenginleştirme tesisine yapılan saldırıdır. Bu, dünyanın en büyük siber savaşı olarak kabul edilebilir. Virüsün etkileri ancak 2010 yılında fark edilmiştir.

---

[111] https://www.webtekno.com/30-yil-once-tarihin-ilk-siber-saldirisini-duzenleyerek-interneti-cokerten-adam-h56353.html (28.09.2020)
[112] https://www.eset.com/tr/trojan-horse/ (28.09.2020)
[113] https://e-bergi.com/y/pc-virus-tarihi/ (28.09.2020)
[114] Ercan Karakoç ve Yılmaz, Bahadır, "Askeri Güç ve Teknolojik Dönüşüm", *Uluslararası Sosyal Araştırmalar Dergisi,* C: 13, S: 72, 2020, s. 232.
[115] https://www.siberportal.org/red-team/cyber-attacks/siber-saldirilarin-evrimi-1986-2017/ (29.09.2020)

Basit bir virüs olarak görünse de çok karmaşık ve anlaşılması güç bir virüstür. Burada enerji sistemlerinin SCADA (Supervisory Control and Data Acquisition) adı verilen merkez kontrol ve veri toplama merkezi ile PLC (Programmable Logic Controller)'ler yani programlanabilir mantıksal denetleyiciler kontrol altına alınarak buradaki gizli veriler de ele geçirilmiştir[116]. Şekil 1.19'da dünyadaki siber saldırıların mali zararları görülmektedir. Saldırılarda sisteme bulaşan kötücül yazılımların sistemden temizlenmeleri ciddi maliyete neden olmuştur.



Şekil 1.19: Siber Saldırıların Getirdiği Mali Zararlar[117]

2010 sonrasında, Amerika'nın 2004 ve 2009 yılları arasında Afganistan Savaşında tuttuğu 92.000 belgeyi içeren Wikileaks belgelerinin basına sızdırılmıştır. Bu durum, istihbarat konusunda kendini öncü kabul eden Amerika için bir vurgun niteliğindedir[118]. 2014 yılında Yahoo, 3 milyon kullanıcı hesap bilgilerinin sızdırıldığını ifade edilmiştir. 2017 yılında fidye yazılım türündeki Wannarcry, Windows işletim sistemlerine ait bilgisayarları hedef alıp şifrelenen dosyalara karşılık Bitcoin fidyesi istemiştir[119]. Bu saldırıların tamamı ciddi mali zararlara yol açmıştır.

---

[116] Şener Çelik, "Stuxnet Saldırısı vee ABDnin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, C: 15, S: 1, 2013, s. 138.

[117] Sena Nezgitli, "Avrupa Birliği Siber Güvenlik Kanunu Sunumu", 6th International Management Information Systems Conference, 2019, s. 6.

[118] https://www.haberturk.com/gundem/haber/1268485-wikileaks-nedir (30.09.2020)

[119] https://www.siberportal.org/red-team/cyber-attacks/siber-saldirilarin-evrimi-1986-2017/ (30.09.2020)

İKİNCİ BÖLÜM

SİBER GÜVENLİK TÜRLERİ, AMACI VE SİBER GÜVENLİĞİN TARİHSEL GELİŞİMİ

2.1 SİBER GÜVENLİK

Siber güvenlik kavramı siber saldırı sonucunda ortaya çıkmıştır. Bu durum savaş stratejisi olarak düşünülebilir. Çünkü saldırı olmadan savunma ve güvenlikten söz edilemez. Bu nedenle güvenlik kavramı savaş ve saldırıların sanal âleme geçmesi ile yeni bir boyut kazanarak siber güvenlik kavramını ortaya çıkarmıştır. Siber güvenlik bu kapsamda kendi bünyesinde birçok güvenlik kriterini barındırır ve bu bölümde tanımlamalar ile kavramların anlaşılması sağlanacaktır.

2.1.1. Siber Güvenlik Nedir?

Siber güvenlik kavramının gerek literatürde gerekse birçok kurum ve uluslararası kuruluşta tanımı mevcuttur. Siber güvenlik, siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünüdür[120].

[120] BGYS Standardı ISO/IEC 27001 - 27002

Kurumsal olarak, USOM 2014 yılında yayınladığı "Siber Güvenliğe İlişkin Temel Bilgiler" kitapçığında, siber ortamdaki bilişim sistemlerinin saldırılardan korunması, bu ortamda bilginin güvenlik ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) korunması, saldırı ve buna karşı yapılan güvenlik mekanizmasının ortaya konarak önceki güvenlik durumuna geri dönülmesi[121] olarak ifade edilmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde ise, siber uzaydaki bilişim sisteminin saldırılardan korunması, işlenen verinin her yönden (gizlilik, erişilebilirlik ve bütünlük bakımından) güvende olması, saldırılar ve yapılan güvenlik durumlarının tespiti ile tespitler sonucu savunma mekanizmasının işletilerek olay sonrası sistemlerin güvenli hâle geri döndürülmesi[122] olarak tanımlamıştır. Uluslararası Standartlar Teşkilatı (ISO), siber güvenlik için siber uzaydaki bilgi varlığının gizliliği, bütünlüğü ve erişilebilirliğinin korunması durumu[123] olarak ifade ederek ISO/IEC 27001 Bilgi Güvenliği Standartlarını ortaya koymuştur. Tüm tanımlardan yola çıkarak siber güvenlik için uluslararası alanda bilgi varlığını kapsayan siber uzaydaki veriye; gizlilik, bütünlük ve erişilebilirlik koşullarıyla ulaşılmasını esas alan güvenlik çeşididir.

2.1.2. Siber Güvenlik ile İlgili Kavramlar

2.1.2.1.Bilgi Güvenliği

Bilgi güvenliği, siber güvenlik yerine kullanılan kavramların başında gelmektedir. Ancak bilgi güvenliği ve siber güvenlik birbirleri ile eş anlamlı değildir. Siber uzay, sanal bir ortam olarak veri alışverişinin yoğun olduğu bir ortamdır. Bu ortamın güvenliği sadece bilgi ve verilerin güvenliğinden ibaret değildir. Bunun oluşmasını sağlayan her türlü yazılım, donanım ve sistemleri de kapsadığı için siber güvenliğin kapsam alanı bilgi güvenliğine göre daha geniştir.

[121] Ulusal Siber Olaylara Müdahâle Merkezi, 2014, s. 5.
[122] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 8.
[123] https://www.iso.org/isoiec-27001-information-security.html (04.10.2020).

TDK'de bilgi kavramı, insanın idrak edebildiği olgu, gerçek ve ilkelerin tümü[124] şeklinde ifade edilir. Bilgi güvenliği, bilginin var olduğu ortamda içerisinde gönderilen hedeften ulaşacağı kaynağa gidene kadar gizlilik, bütünlük ve erişilebilirliğinin kaybolmaması durumudur[125]. Bilgi güvenliği, bilgilerin izinsiz erişimi, kullanımı, üçüncü kişilere aktarımı, ortadan kaldırılması, değiştirilmesi veya bozulmasının önüne geçilme sürecidir[126]. ISO'ya göre, kritik öneme sahip bilginin korunması, bütünlüğünün muhafazası ve ulaşılabilir olması için alınacak tedbir ve önlemlerdir[127].

2.1.2.2. Ulusal Siber Güvenlik

Bir ülke için mevcut olarak var olan veya ileriye yönelik siber uzayda oluşabilecek her türlü siber saldırı konusunda verinin gizlilik, bütünlük ve erişilebilirliğinin korunmasını amaçlayan siber güvenlik stratejisi ve belirlenen eylem planlarının tümüdür. Ulusal siber güvenlik ülkelerin oluşturduğu stratejik eylem planında gerçekleştirmek istedikleri güvenlik amaçlarını belirler.

2.1.2.3. Siber Caydırıcılık

Siber caydırıcılık, gerek bireylerin gerek kurumların ve hatta ulusların maruz kalabileceği siber zorbalık, siber saldırı, siber tehdit ve siber savaş konusunda gösterdikleri güçlü direnme politikalarının tümüdür. Yani siber caydırıcılık, ülkeler için beşinci savaş alanıdır[128]. Siber caydırıcılık, siber savunma için olmazsa olmazdır.

---

[124] https://sozluk.gov.tr/ (05.10.2020)
[125] Yılmaz Vural ve Sağıroğlu, Şeref, "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme" *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, S: 23, No: 2, 2008, s. 508.
[126] Muhammet Baykara, Daş, Resul ve Karadoğan, İsmail, "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi" *1st International Symposium on Digital Forensics And Security (Isdfs'13)*, 2013, s. 231.
[127] https://www.isokalitebelgesi.com/bilgi-nedir-bilgi-guvenligi-nedir-bilgi-guvenligi-yonetim-sistemi-nedir (06.10.2020)
[128] Minhaç Çelik, "Siber Ordu Kurmak için Devletler Özel Sektör ile Çalışıyor", *TMMOB Bilgisayar Mühendisleri Odası Dergisi*. S: 5, 2015, s. 32 , s. 32-33.

Çünkü kötü bir durumu engellemek ancak iyi bir savunma politikası ile mümkündür. Siber uzaydaki bilginin varlığını tehdit eden her unsur göz önüne alınarak etkili bir caydırıcılık politikası izlenmelidir. Siber caydırıcılık kavramını ilk olarak 1994 yılında James Der Derian kullanmıştır. Siber caydırıcılık aslında sanal ortamdaki tehlikeleri bertaraf etmek için yapılan her türlü önleme ve engelleme girişimleridir[129]. Kısaca siber caydırıcılık, sanal ortamda gerçekleşebilecek her türlü saldırı ve yürütülen kötü amaçlı faaliyetleri korkutup cesaret kırarak vazgeçirme yöntemidir.

2.1.2.4. Parola Güvenliği

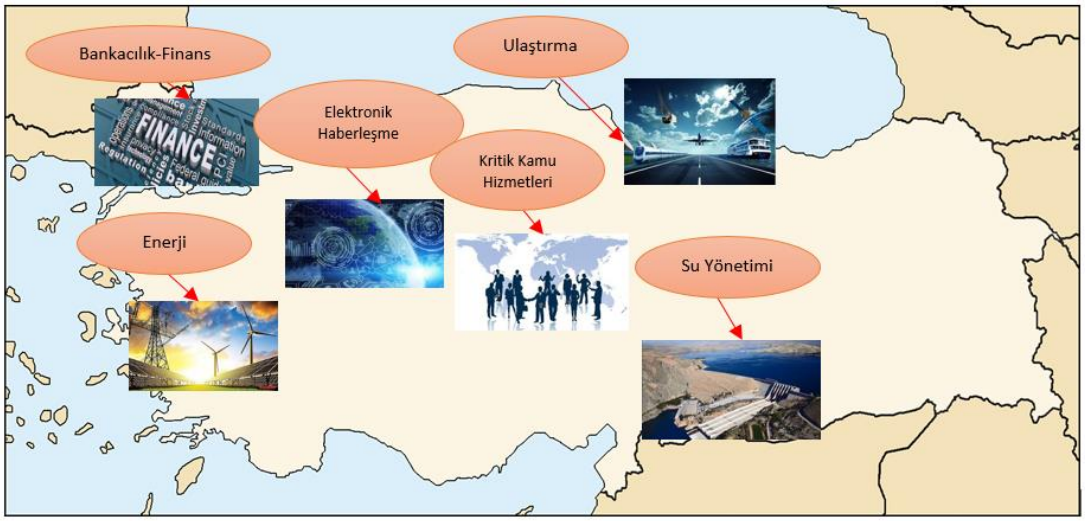
Siber güvenlik kapsamında kullanıcı adı ve şifrenin talep edildiği her web sayfası, uygulama ve sistem yönetimi için önemli güvenlik türlerinden biridir. Parola güvenliği, hassas veri içeriği barındıran sistemler için önemlidir. Kısacası girişi sadece kullanıcı adından ibaret olmayan ve kişinin gerçek kişi olup olmadığının anlaşılmasını sağlayan çeşitli rakam, numara, harf ve karakter gibi simgelerden oluşan farklı veri uzunluğuna sahip şifrenin korunmasını sağlayan güvenlik modelidir.

2.1.2.5. Kritik Altyapıların Güvenliği

İnsanların en temel ihtiyaçlarını bünyesinde barındıran enerji, su, ulaştırma, finans, haberleşme ve iletişim gibi sistemlerin ve bunların sahip olduğu altyapıların sağlandığı güvenlik modeline kritik altyapı güvenliği denir. Bu, ulus güvenliği ile ortak amaçlar gütmektedir. Çünkü bu sistemleri elinde tutan ve yöneten devletlerin bizzat kendisidir. Tarihe bakıldığında *kritik altyapı* kelimesine 1997 yılında ABD'nin Kritik Altyapıların Korunması Hakkındaki Raporunda yer verilmiştir[130]. Kritik altyapılar ABD mevzuatında, ABD için fiziksel ve sanal sistemler ve bunların yetkisiz bırakılması ya da yok edilmesiyle ulusal güvenlik, kamu sağlığı, emniyet veya hepsinde olumsuz etkiye neden olması durumu olarak tanımlanmaktadır. Kritik

[129] Ş.Sağıroğlu, M. Alkan, R. Samet, G. Ulutaş ve diğ., 2018, s. 26.
[130] Critical Foundations Protecting America's Infrastructures, "*The Report of the President's Commission on Critical Infrastructure Protection*", 1997, s. 5.

altyapı; AB komisyonu 2014 yılı 702 sayılı tebliğinde ise, insanların hayati fonksiyonları, sağlık, emniyet, güvenlik, maddi ve manevi refahının sürdürülmesinde duraksaması ya da tamamen ortadan kalkmasıyla bir ulustaki sistem ve varlıkla alakalı durumlar[131] olarak tanımlamıştır. Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanında kritik altyapılar, işlenen bilgide gizlilik, erişilebilirlik ve bütünlüğüne zarar vermesi hâlinde can kaybı, ciddi ekonomik zarar, ulusal güvenlik zaafiyeti ya da kamusal düzenin zarar görmesine neden olabilecek bilişim ile beraber endüstriyel kontrol sistemlerini de kapsayan sistem bütünüdür[132] şeklinde ifade edilmiştir. Şekil 2.1'de Türkiye için belirlenen altı kritik altyapı görülmektedir.



Şekil 2.1 Türkiye için Belirlenen Kritik Altyapılar

2.2. Siber Güvenliğin Amacı: CIA Modeli

İngilizce "*confidentiality, integrity ve availability*" kelimelerinin baş harflerinin oluşturduğu CIA modeli siber güvenliğin amacını özetleyen üç özelliktir. Ancak bunlar var olursa siber güvenlikten söz edilebilir. Confidentiality gizliliği, integrity bütünlüğü ve availability ise erişilebilirliği temsil etmektedir. Bunlar

[131] Mustafa Ünver, Canbay, Cafer ve Özkan, Hüseyin Burhan, "Kritik Altyapıların Korunması", *Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,* 2010, s. 3.
[132] UDHB, *Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı*, s. 6.

ITU'nun siber güvenlik tanımında konumlandırdığı ve siber güvenliğe ait olan ana ilkelerdir. Bu ilkeleri tanımlamak gerekirse:

- **Gizlilik**: İzinsiz ve yetkisiz kişinin veriye ulaşımı engellenerek sistemi yalnızca yetkili kullanıcının çalıştırabileceği ve sistemde gelen ya da giden mesajları bu kişinin görebileceği[133] anlamına gelmektedir.

- **Bütünlük**: Kaynaktan çıkan verinin kaynaktan çıktığı hâliyle herhangi bir değişim ve dönüşüm içerisine girmeden hedefe varma durumudur[134].

- **Erişilebilirlik**: Yetki ve izin sahibi olan kişinin bilgi varlığına gereken durum ve şartlarda tam ve eksiksiz ulaşabilmesidir[135].

Şekil 2.2'de siber güvenliğin sağlanması için gereken CIA modeli görülmektedir. Bu üç kritik özellik aslında siber güvenlik amacıyla beraber siber güvenliğin nasıl sağlanması konusunda da yol gösterici niteliktedir.



Şekil 2.2 Siber Güvenliğin Amacı: CIA Modeli[136]

[133] Christopher A. Bartos, "Cyber Weapons are not Created Equal", *Faculty and Researcher Publications*, C: 142, S: 6, No: 1, 2016, s. 32.
[134] Mehmet Ada, *NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi*, Gazi Üniversitesi Bilişim Enstitüsü, Yüksek Lisans Tezi, Ankara, 2018, s. 11.
[135] Şerife Karadağ, *Siber Uzayın NATO'nun Güvenlik Anlayışına Etkisi*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 2019, s. 34.
[136] https://www.defenceturk.net/bilgi-guvenligi-ve-siber-guvenlik-turkiye-siber-guvenlik-kumelenmesi (12.10.2020)

2.3. SİBER GÜVENLİĞİ SAĞLAMA YÖNTEMLERİ

2.3.1. Anti virüs

Anti virüs, başta kötücül yazılımlar olmak üzere birçok virüsü sistemde algılayarak sistem yöneticisine veya sistem kullanıcısına bu virüsleri haberdar eden yazılımlardır. Bu hususta anti virüs sadece virüsleri algılamayla kalmaz, virüslerden temizleme ve sistemi virüslerden kurtarma görevlerini de üstlenen koruyucu yazılım programlarıdır. Bu programları oluşturan kişilerin yapması gereken belirli sorumlulukları mevcuttur. Bunlar:

- Üretici firma, oluşturduğu bu programları daima güncelleyerek mevcut olan tüm virüs tanımlamalarını yapmalı,
- Güven vermeli ve kalite esasını bünyesinde barındırmalı,
- Virüsleri algılayabilmesi için virüs veri tabanı kapasitesini genişletmeli,
- Sistem performansını yavaşlatan etkilerden kurtarmalıdır[137].

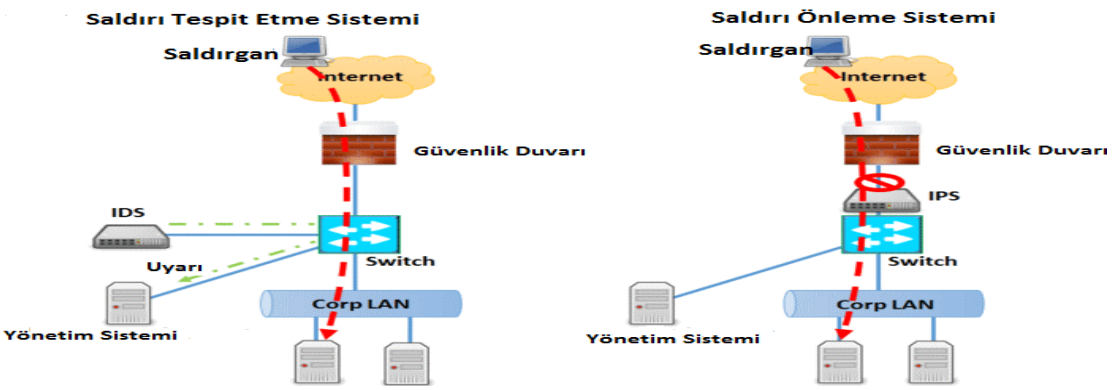
2.3.2. IDS/IPS (Saldırı Tespit Etme ve Önleme Sistemleri)

Intrusion Detection System ve Intrusion Prevention System kelimelerinin baş harfleri ile oluşan bu sistemler saldırıları tespit etme ve önleme amacıyla kullanılırlar. IDS, dışarıdan gelebilecek saldırılara karşı sistem ağında gerçekleşen durumları inceleyen yazılım ve donanımlardan oluşan sistemlerdir[138]. IDS saldırıları algılarken yapay zekâ yöntemlerinden, yapay sinir ağları ve makine öğrenmesi tekniklerini kullanır. Bunun yanı sıra genetik algoritma ile de saldırı tespitleri yapmak ve saldırının gen haritasını çıkarmak için modellemeler de yapılabilir[139]. Burada amaç, güvenlik

[137] https://it.bilgi.edu.tr/tr/guvenlik/antivirus/ (15.10.2020)
[138] Xin Zhang, Jia, Li, Shi, Hongyan, Tang, Zhongbin ve Wang Xiaoling, "The application of machine learning methods to intrusion detection", *2012 Spring Congress on Engineering and Technology*, *IEEE*, 2012, s. 1.
[139] Gözde Karataş, "Genetic Algorithm for Intrusion Detection System", *2016 24th Signal Processing And Communication Application Conference (Siu), IEEE,* 2016, s. 1341.

duvarında oluşan sistem açıklarının kapatılmasıdır. IDS için kullanılan araçlardan bazıları; Haystack, W&S, Midas, Ides, Nadir, Nsm, Hyperview, Ustat, Idiot, Dids[140]dir. IPS, saldırıyı önlemek için kullanılan sistemlerdir. Bunlar, Snort açık kaynak kodlu bir yazılım olarak ağda meydana gelen olağan dışı durumları tespit ederek önlemeyi sağlayan IDS/IPS amaçlı kullanılan sistemlerdir[141].

Şekil 2.3'te IDS ve IPS çalışma mimarileri görülmektedir. IPS güvenlik duvarından sonra IDS ise ağ yönlendirme işlemi yapan switch yani anahtardan sonra konumlandırılır. IDS, IPS için bilgi toplar ve veri tabanına kaydeder. Bu yüzden IDS pasif, IPS aktif rol üstlenir.



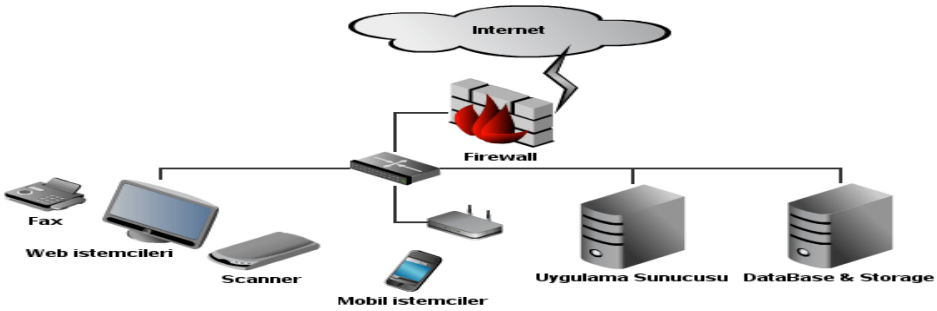
Şekil 2.3 IDS/IPS Mimarisi[142]

2.3.3. Güvenlik Duvarı (Firewall)

Güvenlik duvarı çalışma düzeni, sistemin genel erişim yerleri dışında özel bölümlere erişim sağlayan kapalı alanlardır. Sistem içinde var olan ve yetki erişimi bulunan kullanıcıların yetkisi dâhilinde erişim sağlamasına izin veren güvenlik

[140] Muhammet Baykara ve Daş, Resul, "Saldırı Tespit ve Engelleme Araçlarının İncelenmesi", *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, S: 10, No:1, 2019, s. 61-64.
[141] Kevser Ovaz Akpınar, *Ethercat Tabanlı Bir Scada Sisteminde Kural ve Makine Öğrenmesine Dayalı Saldırı ve Anomali Tespiti*, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi, Sakarya, 2019, s. 11.
[142] https://sibertehdit.com/ips-ve-ids-nedir-bu-sistemler-nasil-atlatilir/ (16.10.2020)

aracıdır[143]. Örnek olarak bir kurumda tüm kişilerin erişebileceği web sayfasının var olmasına ek olarak kurumun iç işlerinin yürütülmesi için kendi kurum personelinin erişebildiği yerler için kullanılan güvenlik sistemidir. Kısaca ağ trafiğinde gelen paketlerin duruma göre yoluna devam etmesi veya bu paketler için işlemin sonlanmasına karar verilen yerdir[144]. Şekil 2.4'te firewall çalışma prensibi görülmektedir. İnternetten gelen veri, güvenlik duvarından geçip doğru yere yönlendirilir.



Şekil 2.4 Güvenlik Duvarı Çalışma Şeması[145]

2.3.4. NAC (Sistem Ağ Erişimi)

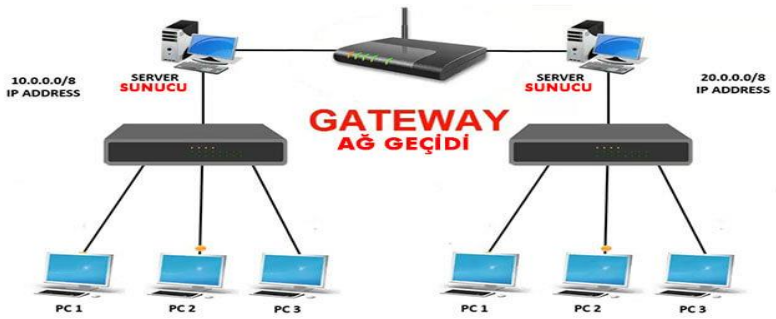
Network Access Control kelimelerinin baş harflerinden oluşan NAC, sistem ağına erişim kontrolünü sağlar. NAC, sistemde temel olarak veri paketlerini almak ve bunları iletmek için birden fazla ağ arayüzüne sahip ağ cihazının oluşturduğu sistemdir[146]. Sanal ortamda ağ erişim kontrolü için iki yöntem mevcuttur. İlk olarak ana makine üzerinde çalışan sanal makinayı geçici güvenlik aracına entegre edilerek yapılabilir. İkinci olarak, geçici güvenlik aracının birden fazla ağ erişim protokolüne

[143] Enis Karaarslan, "Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar", *Akademik Bilişim*, 2003, s.1.
[144] Ayhan Erdem ve Kocaoğlu, Ramazan, "Yeni Bir Ağ Güvenliği Yaklaşımı: Dinamik Zeki Güvenlik Duvarı Mimarisi" *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, S: 29, No: 4, 2014, s. 707.
[145] https://alycck.wordpress.com/2016/03/03/kullanim-senaryosu/ (16.10.2020)
[146] Puqi Tang ve Liu, Hsin-Yuo, "Security enabled network access control." *U.S. Patent No. 7,185,365*. Washington, Dc: U.S. Patent And Trademark Office, 2007, s.1.

uyumlu olup olmadığını göstererek ağ erişiminin kontrol edilmesi[147] ile de sağlanabilir. NAC sistemdeki kullanıcının güvenliğini sağlar. Ağ güvenliğini denetleyerek sistem içi yetkilendirmeyi yapar. NAC, sistemi sıfır gün saldırıları, solucanlar gibi siber saldırılara karşı korur. İki aşamalı yetkilendirme yapar. Bunlar kullanıcı ve cihaz temelli olarak ikiye ayrılır[148]. Böylece denetim mekanizması kesintisiz gerçekleştirilir.

2.3.5. Web ve E-mail Gateway

Gateway sistemler için geçiş kapısıdır. Gateway, ağ üzerindeki farklı protokollerin iletişim kurmasını sağlayan donanım ve yazılımların tamamıdır. Bu geçiş kapısı, web trafiği ve mail trafiğini düzenlemek konusunda oldukça önemlidir ve farklı protokollerin anlaşmasını sağlayarak güvenlik sorununu da çözmüş olur. Bu durum doğrudan siber güvenlik sağlama yöntemlerinden biri değildir. Aslında temel olarak protokol uyumunu sağlayarak farklı iletişim durumlarının birbirlerini herhangi bir kötücül yazılım olarak görmesinin önüne geçmiş olur. Şekil 2.5'te iki sunucu gateway sayesinde iletişime geçerek birbirlerini tehdit olarak algılamazlar.

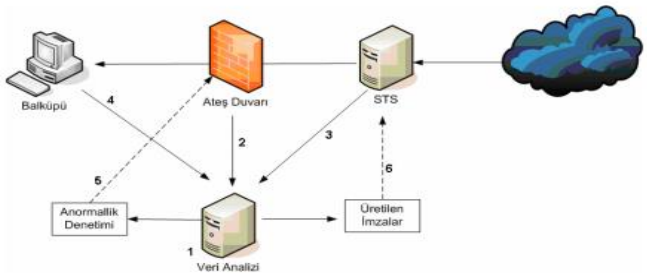


Şekil 2.5 Gateway Çalışma Prensibi[149]

[147] Sanjay Sawhney, Conover, Matthew ve Montague, Bruce, "Systems and methods for providing network access control in virtual environments, "*U.S. Patent No. 8,938,782*, Washington, Dc: U.S. Patent And Trademark Office, 2015, s. 18.
[148] Hüsnü Demir, Yüce, Hüseyin, Akın Gökhan, "Network Access Control Ağ Erişim Kontrolü (NAC) Sunumu", Ulak-CSIRT, 2008, s. 2.
[149] https://www.somut.net/126/pcdonanim/gateway-nedir.1.html (16.10.2020)

2.3.6. Honeypot (Bal küpü)

Honeypot, bal küpü anlamında kullanılan siber güvenlik mekanizmasıdır ve aslında saldırganı tuzağa çekme yöntemidir. Yani bu bal küpü farklı amaçlar için sisteme sızmak isteyen saldırganın takip edildiği tuzak bir ağdır[150]. Aslında bal küpü, saldırganı saldırma faaliyeti için kendisine doğru cezbeden güvenlik elemanıdır[151]. Bu, saldırganı yakalamak ve onun saldırı stratejisini öğrenmek adına iyi bir yöntemdir. Honeypot'un IDS'den farkı, her ne kadar iki sistemin de amacı saldırıyı tespit etmek olsa da IDS'de saldırının olması beklenir ve saldırı gerçekleşince tespit edilir, ancak honeypot saldırganın başarılı saldırı gerçekleştirebilmesi için tüm koşulları yerine getirir[152] ve saldırı yapması için ona imkân sağlar. Bir nevi saldırganın siber saldırı için kullandığı oltalama yöntemini saldırgana uygulayarak saldırganın oltalanmasıdır. Şekil 2.6'da honeypot çalışma prensibi görülmektedir.



Şekil 2.6 Honeypot Çalışma Prensibi[153]

[150] Niels Provos, "A Virtual Honeypot Framework", *Usenıx Security Symposium*, C: 173, No: 2004, 2004, s. 1.
[151] Christian, Seifert Welch, Ian ve Komisarczuk, Peter, "HoneyC -the Low- Interaction Client Honeypot", *Proceedings of the 2007 NZCSSRCS, Waikato University, Hamilton, New Zealand*, S: 6, 2007, s. 1.
[152] Iyad Kuwatly, Sraj, Melek, Al Masri, Zaid, "A Dynamic Honeypot Design for Intrusion Detection", *The IEEE/ACS International Conference Onpervasive Services, ICPS 2004, Proceedings*, 2004, s. 95.
[153] Yavuz Gökırmak, Yüce, Emre, Bektaş, Onur, Soysal, Murat, Orcan, Serkan, "Ipv6 Balküpü Tasarımı", *Tübitak ULAKBİM,* 2011, s. 3.

2.3.7. SIEM (Güvenlik Bilgi ve Olay Yönetimi)

SIEM açılımı, Security Information and Event Management olarak ifade edilir. SIEM kısaca güvenlik bilgileri ve olay yönetimidir. SIEM, sistem kayıtlarını tutar ve bunlarla ilişki kurar[154]. Log kaydı olarak da bilinen sistem kayıtlarının tutulması, sistem faaliyetlerinin anlaşılması için çok önemlidir. Bu kayıtlarla beraber olabilecek siber olaylar da yönetilmiş olur. Aslında SIEM çalışan hareketlerini izleyen kayıt korelasyon[155] yönetiminin tamamıdır.

2.3.8. URL Filtreleme

URL, Uniform Resource Locator'un kısaltmasıdır. Türkçeye standart kaynak bulucu olarak geçmiştir ve özetle internet adreslerinin sahip olduğu adların[156] tümüdür. URL filtreleme, URL'in belirli sınırlamalara tabi tutularak alınan güvenlik önlemidir. Bu yasaklı siteler ya da zararlı içerik barındıran sitelere girişi engeller. Girilmesi veya erişilmesi istenmeyen siteler için uygulanır. Bu uygulamaya örnek olarak güvenli internet ile beraber gençlerin fiziksel ve ruhsal gelişimlerinin korunması için internet servis sağlayıcılarının illegal sitelere uyguladıkları içerik filtreleme uygulaması verilebilir. Kurum ve kuruluşlar çalışanlarının erişmesini istemedikleri siteler için URL filtreleme uygulayabilir. Böylece hem sistemler hem de çalışanlar güvende kalır. Bu hususta URL filtrelemenin kalıcı olması adına bu filtreleme işlemi log olarak tutulabilir. Yani sisteme tanıtılan URL filtreleme kimliğiyle eşleşen trafik girişlerinin görüntülenmesi[157] bu kayıtlarla tutulmuş olur.

---

[154] Mustafa Kaytan, *Web Tabanlı Oltalama Saldırılarının Makine Öğrenmesi Yöntemleri ile Tespiti*, İnönü Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Malatya, 2016, s. 32.

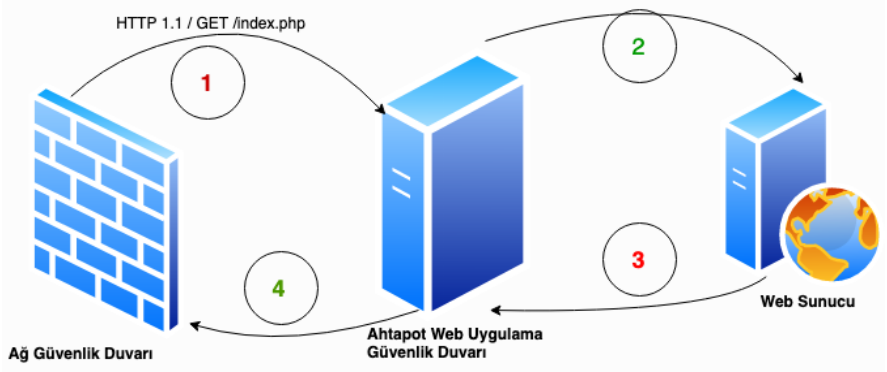
[155] Halil İbrahim Ulus ve Demirci, Mehmet, "Kurum İçi Saldırıların Tespiti ve Önlenmesi için Sunucu İzleme Uygulaması", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, S: 6, No: 3, 2018, s. 514.

[156] Özlem Özgen ve Elmasoğlu, Kamile, "Sosyal Medya ve Marka İletişimi: Havayolu Şirketlerinin Twitter Kullanımına Yönelik Bir Araştırma", *İletişim Kuram ve Araştırma Dergisi*, S:43, 2016, s. 198.

[157] Bahattin Yalçınkaya, Gedikli, Muhammet Emin ve Cibaroğlu, Mehmet Oytun, "Elektronik Belge Yönetim Sisteminde Log Analizi: İstatistiksel Bir Değerlendirme", *Bilgi Yönetimi ve Bilgi Güvenliği,* 2019, s. 64, s. 61-77.

2.3.9. WAF (Web Uygulama Güvenlik Duvarı)

Web Application Firewall, bilinen firewalldan farklı olarak web güvenliğini sağlamak amacıyla geliştirilmiştir. Bu yöntem web güvenliği sağlanamadığı durumlarda devreye girer. Web güvenliği, sunucu sistem yöneticisine ulaşamamasında, sisteme ait yazılımın yetersiz belgelenmesinde, bunun sonucunda yazılımı yapan kişiye ulaşılamamasında veya donanımsal nedenlerden[158] sağlanamayabilir. Touseef ve arkadaşları 2019 yılında yapılan ve altı web sitesine uygulanan[159] WAF ile web uygulama güvenlik açıklarının büyük bir kısmı kapatmayı başarmışlardır[160]. Şekil 2.7'de WAF çalışma prensibi görülmektedir.



Şekil 2.7 WAF Akış Şeması[161]

2.3.10. Anti DDOS

DDoS saldırılarının önüne geçmek için kullanılır. Anti DDoS sistem sunucusunu korur. Burada sistem geniş kullanıcı kitlesine sahip olsun veya olmasın

---

[158] Enis Karaarslan, Tuğlular, Tuğkan ve Şengonca, Halil, "Kurumsal Web Güvenliği Yapısı", *Akademik Bilişim*, 2008, s. 244.

[159] Pariwish Touseef , Amjad Alam, Khubaib , Jamil, Abid, Tauseef, Hamza, Ajmal, Sahar ve diğ., "Analysis of Automated Web Application Security Vulnerabilities Testing*", ICFNDS '19 Proceedings of the 3rd International Conference On Future Networks And Distributed Systems,* No: 36, 2019, s. 1.

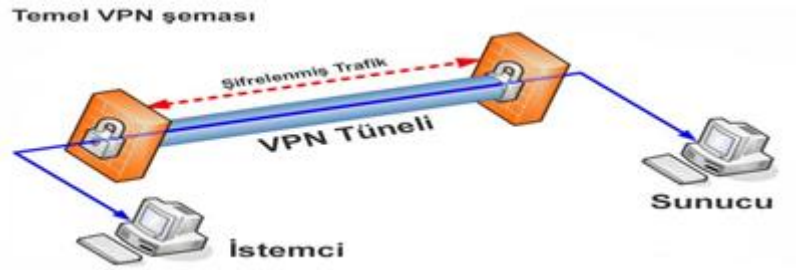
[160] Erhan Saygılı ve Kılıç, Fatih, "Web Uygulama Güvenliği: Bir Örnek Çalışma Web Application Security: A Case Study", *Proceedings of the International Conference on All Aspects of Cyber Security,* C: 2, 2019, s. 46.

[161] https://docs.ahtapot.org.tr/kullanim-klavuzlari/web-uygulama-guvenlik-duvari-kullanimi/ (18.10.2020)

sunucuya fazla yük bindirmemek adına çoklu sunucu ve botnetleri kendinden uzak tutan Anti DDoS'lar sayesinde DDoS ve DoS saldırılarının önüne geçilir. Bu da sistemin aksamadan çalışmasını ve veriye erişim imkânı olan kişinin erişmesini sağlar.

2.3.11. VPN (Sanal Özel Ağ)

Virtual Private Network kelimelerden oluşan ve sanal özel ağ olarak adlandırılan VPN, verinin herkese açık olan hat üzerinden gönderilmeden önce şifrelenerek koruma altına alınması[162] işlemidir. Temel amaç, büyük kurum ve kuruluşlara ait olan şubeler arasında yapılan iletişim ve veri alışverişini güvenli hâle getirmektir. Burada merkez ve uç noktalardaki çalışma sahâlârı ve birbirleri arasına VPN kurularak sistem güvenliği üst düzeye çıkarılmış olur[163]. Konunun en iyi örnekleri; banka ve finans sektörü, kurum ve kuruluşların intranet portalıdır. İntranet, internetin dış dünyaya kapalı olarak kullanılabildiği bir network sistemidir. Şekil 2.8'de VPN müşterisinin, internete VPN tünelinden geçerek VPN sunucusundan talep ettiği veriyi aldığı görülmektedir. Burada Perimeter Network, VPN müşterisinin çevrelenmiş ağını ifade etmektedir.



Şekil 2.8 VPN Çalışma Prensibi [164]

[162] Erhan Kahya, "Bilgisayar Ağ Sistemleri Güvenliği", *Akademik Bilişim, 07-IX. Akademik Bilişim Konferansı Bildirileri*, 2007, s. 286.
[163] Ömer Aydın ve Temurtaş, Hasan, "Perakende Satış Alanında SAP ERP ile Entegre Bir Yazılım", *Dumlupınar Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, S: 035, 2015, s. 47.
[164] http://onuraltinkaynak.com/windows-10da-vpn-baglantisi/ (20.10.2020)

2.4. SİBER GÜVENLİĞİN TARİHSEL GELİŞİMİ

Siber güvenlik, siber saldırılar sonucu ortaya çıkan sanal âlemde meydana gelen olay ve durumların güvenli bir şekilde yürütülmesi prensibine dayanmaktadır. Siber güvenlik tarihi de siber saldırıların sonrasında şekillenmiştir.

Siber güvenlik ilk olarak siber âlemin nasıl denetlenip kontrol edilebileceği üzerine 1970 ve 80'lerden beri süregelen bir konu olarak başlamış[165] ve günümüzde siber uzaydaki güvenliğin nasıl sağlanacağı konusunda birçok devlet ve uluslararası örgüt çalışmaları ile devam etmiştir. Aslında siber âlem için düşünülen denetim kavramının yerini, siber saldırıların olumsuz etkileriyle beraber siber güvenlik ve siber savunma prensipleri almıştır. Çünkü siber âlemi kontrol etmenin mümkün olamayacağı internetin yaygınlaşması ve sanal âlemde bulunan cihaz kapasitesindeki artışla beraber anlaşılmıştır. Siber güvenliğe yönelik durumlar 1980'lerde başlayarak günümüze kadar ulaşmıştır. Siber güvenlik için ilk patent, ortak anahtarlama sistemi RSA (Rivest-Shamir-Adleman) ile ABD girişimde olmuştur[166]. Ayrıca ABD yasal düzenlemeler konusunda da bu alan için öncülük yapmıştır. 1984 yılında "Kapsamlı Suç Kontrol Yasası'nın" kabul edilmesiyle bilgisayar ve bilişim ağlarına yetkisiz erişim konusu üzerinde durulmuştur. Bu yasanın devamında, yasa eksiklerini doldurmak adına 1986 yılında verilerin değiştirilmesi ve yok edilmesi gibi zarar verme durumları eklenerek "Bilgisayar Dolandırıcılığı ve Kötüye Kullanma Yasası (CFAA)" kabul edilmiştir[167]. 1986 yılında oluşturulan Brain virüsünü temizlemek için 1988 yılında ilk antivirüs programı yazılmıştır. 1987 yılında oluşturulan Christmas Tree'ye karşı zarar gören IBM ilk antivirüs programını piyasaya sunmuştur[168]. Bu süreç, 1980'li yıllarda daha çok bilgisayarlara yönelik saldırıların olduğunu göstermektedir ve devamında bu saldırılar kapsamında gerek yasal düzenleme gerek siber güvenlik adımlarının atıldığı görülmektedir. 1988'de Robert Morris tarafından üretilen Morris

[165] Sevda Ünal, *Siber Uzamın Güvenlikleştirilmesi Söylemi: Türkiye, ABD ve Avrupa Birliği Örnekleri*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Anabilim Dalı, Doktora Tezi, Ankara, 2015, s. 243.
[166] https://siberci.com/siber-guvenlik-tarihi/ (20.10.2020)
[167] A.g.e., s. 171.
[168] https://e-bergi.com/y/pc-virus-tarihi/ (20.10.2020)

solucanı internetin çökmesine neden olmasıyla CERT (Computer Emergency Response Team) yani Bilgisayar Acil Müdahâle Ekibi oluşturulmuştur[169]. Bunlar siber güvenlik konusunda donanımlı ve birçok teknik bilgiye sahip kişilerden oluşan bir siber güvenlik ordusudur. 1989 yılında Zaman Bombası adı verilen virüsün İsrail'de ortaya çıkmasıyla kullanıcı sayısı fazla ve güvenilirliği yüksek Norton adı verilen anti virüs programı 1990 yılında oluşturulmuştur[170].

İnternet kullanımının yaygınlaşması ağ güvenliği problemini meydana getirmiş ve 1995 yılında Kaliforniya üssüne yapılan virüs saldırısından sonra NASA ilk güvenlik duvarı programını tasarlanmıştır[171]. Devamında Netspace web sayfalarının güvenli kullanımı için SSL (Secure Socket Layer) denilen güvenli yuva katmanı protokolü ile beraber HTTP (Hyper Text Transfer Protocol) denilen hiper metin transfer protokolünü piyasaya sürmüştür[172]. Sistemlerin önemini göstermek amacıyla ilk kez *kritik altyapı* terimi, 1997 yılında ABD Başkanlık Komisyonu'nun Kritik Altyapıların Korunması Hakkındaki Raporu'nda kullanılmıştır[173].

2000 yılından sonra uluslararası işbirliği ön plana çıkarak 2004 yılında Avrupa Siber Suçlar Sözleşmesi yayınlanmıştır[174]. Ancak asıl bilinçlenmeyi tetikleyen 2007'de Estonya'ya yönelik gerçekleştirilen siber saldırı olmuştur. Bu saldırı, ülkeler ile beraber büyük kurum ve kuruluşların organize olma durumunu meydana getirmiştir[175]. 2008 yılında Avrupa Güvenlik Stratejisinin Uygulanmasına İlişkin Rapor 'da siber güvenliğe ait bir bölüm oluşturulmuştur[176]. Siber savaş ve saldırı konusunda ülkelerin bilinçlenmesini, 2009 yılında İran'a yapılan Stuxnet saldırısı tetiklemiş ve aslında bu post-modern dönem için uygulanan *sessiz sızma* faaliyetinin

[169] https://cahitcengizhan.com/bilisim-guvenligi-turlerinin-tarihsel-gelisimi/ (21.10.2020)
[170] https://e-bergi.com/y/pc-virus-tarihi/ (20.10.2020)
[171] https://cahitcengizhan.com/bilisim-guvenligi-turlerinin-tarihsel-gelisimi/ (21.10.2020)
[172] https://siberci.com/siber-guvenlik-tarihi/ (20.10.2020)
[173] Critical Foundations Protecting America's Infrastructures, 1997, s.1.
[174] Council of Europe, Convention on Cybercrime, 2004, s. 2.
[175] Seda Yılmaz ve Sağıroğlu, Şeref, "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, 2013, s. 159.
[176] Council of the Europe Union , *European Security Strategy*, 2008, s. 13.

siber güvenlik önlemleri ile yürütülmesini[177] sağlamıştır. Sessiz sızma doğrudan savaş uygulamak yerine devletlerarasında önemli sayılabilecek her türlü bilgi edinme yoluna başvurma yöntemidir. Bu yüzden ulusal ve uluslararası örgütlerin kurulması ve yaptırım gücü olan mevzuat, sözleşme ve yasalar oluşturmak istenmiştir. Stuxnet'in baş aktörlerinden biri olan ABD 2009 yılında Cyber Security Policy Review adında ülkenin siber güvenlik politika değerlendirmesini yapmıştır. Bu, İran'dan gelebilecek bir hamle için tedbir amaçlı düşünülmüştür. Güvenlik, oluşan teknoloji ile şekillenmektedir. Türkiye siber olaylar karşısında ülke politikasını belirlemek için Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planını yürürlüğe koymuştur ve siber güvenlik kavramının stratejik önemini açıklamıştır[178]. Tarihi 1999 yılına dayanan IoT (Internet of Things) yani Nesnelerin İnterneti 2008 yılında internete bağlanan cihaz sayısının artması[179] ve akıllı cihaz kullanım oranlarının yükselmesi ile kullanım alanları genişlemiştir. Bu cihazların güvenlik özellikleri olmadığından DDoS, Botnet gibi kritik saldırılarda kullanılmıştır. Bu kapsamda Avrupa Siber Suçlar Sözleşmesi'nin de devamı niteliğinde Avrupa Siber Güvenlik Yasası 12 Mart 2019 tarihinde çıkarılmıştır. Yasa'nın 3. başlığında IoT'lerin güvenlik durumuna göre sınıflandırılmaları konusunda Siber Güvenlik Alanında Belgelendirme Çerçevesi oluşturulmuştur[180].

[177] Fikret Birdişli, "Uluslararası Güvenliğin Tarihsel Gelişimi ve Post-Modern Güvenlik Dönemi", *Güvenlik Bilimleri Dergisi*, 2020, s. 250.
[178] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı,* 2013, s. 17.
[179] https://radore.com/blog/nesnelerin-internetinin-gecmisi-ve-gelecegi.html (24.10.2020)
[180] Sena Nezgitli ve Benzer, Recep, "Avrupa Birliği Siber Güvenlik Kanunu", *Journal of Information Systems and Management Research*, S: 2, No:1, 2020, s. 14.

ÜÇÜNCÜ BÖLÜM

İNGİLTERE VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASININ KARŞILAŞTIRILMASI

Bu bölüm, çalışmanın temelini oluşturmaktadır. Siber güvenlik konusunda Türkiye ve İngiltere'nin dünya sıralamasındaki yerlerini ve güvenlik politikaları yönünden birbirleri ile kıyasları ITU'nun belirlediği beş ana kritere göre yapılacaktır. Bu analizlerin sonucunda Dijital Dönüşüm Ofisi başta olmak üzere Bilgi Güvenliği Derneği'nin Türkiye için yaptığı siber güvenliği çalışmaları ele alınacaktır. Analiz aşamasına geçmeden önce ITU Siber Güvenlik Endeksi'nin nasıl ortaya çıktığı ve tarihsel süreci incelenecektir.

3.1. ITU SİBER GÜVENLİK ENDEKSİNİN TARİHİ

ITU, iletişim teknoloji adına uyumu sağlamak için teknik standartları belirlemek ve dünya çapında hizmet yetersizliği olan topluluklara erişim hizmeti vermek için faaliyet gösteren uluslararası bir organizasyondur[181]. Bu kapsamda ITU birçok görev ve sorumluluk yürütmektedir. Bünyesinde barındırdığı Dünya Bilgi Toplumu Zirvesi (WSIS) ve Tam Yetkili Temsilciler Konferansı ile ortak yürütülen bilgi ve iletişim teknolojilerinin güvenli kullanımını sağlamaktır. ITU bu kapsamda 17 Mayıs 2007 tarihinde Global Cybersecurity Agenda (GCA) olarak bilinen Küresel Siber Güvenlik Gündemi için ilk çalışmasını başlatmıştır[182]. Bu bilişim teknolojileri ve ağları için önemli bir adımdır. Çünkü iletişimde istenen temel iki kriterden biri güvenli iletişim, diğeri ise bu iletişimin küresel düzeyde olmasıdır. Bu kapsamda, belirlenen gündemi eyleme dökme faaliyetleri adına C5 eylemi yani Action Line 5

[181] Ş. Sağıroğlu, M. Alkan, R. Samet, G. Ulutaş ve diğ. , 2018, s. 76.
[182] https://www.itu.int/en/action/cybersecurity/Pages/default.aspx (25.10.2020)

ortaya konmuştur. Bu eylem planında, GCA için vurgulanan yedi temel hedef bulunmaktadır. Bunlar:

- Uluslararası alanda hâlihazırda uygulanabilecek ulusal ve bölgesel mevzuatlarla uyum gösterebilecek siber güvenlik politikasının geliştirilmesi,
- Ulusal ve bölgesel olarak siber güvenlik alanında çalışacak kuruluşların kurularak bu kuruluşlar tarafından güvenlik politikaları oluşturulması,
- Uluslararası standartlarda onaylanmış azami güvenlik ölçütleri ile beraber yazılım ve donanım sistemleri için akreditasyon programlarının meydana getirilmesi,
- Var olan ve yeni teşebbüsler arasında uluslararası işbirliği sağlayacak, siber olayları izleyip uyaracak ve olaylara müdahâle edebilecek uluslararası bir modelleme oluşturulması,
- Kişiler için sayısal kimlik sisteminin oluşturulup bu verilerin dünya çapında bilinirliği için bir modelin meydana getirilmesi,
- Sektörel bazda siber güvenlik alanında gerçekleşen bilgi alışverişini sağlamak için kurumsal kapasitenin geliştirilmesi,
- Bahsi geçen tüm bu hususlar hakkında uluslararası işbirliği, karşılıklı iletişim ve koordinasyonun sağlanmasıdır[183].

Bu yedi kriterin uygulanabileceği ve aynı zamanda siber güvenlik ile ilgili incelemelerin de yer alacağı Küresel Siber Güvenlik Endeksi(GCI)[184] oluşturulmuştur. GCI'nın faaliyetlerini yürütebilmesi için uzman bir ekibe ihtiyaç duyulmuştur. Bunun için ITU, kamu kurumları ve özel sektörde uluslararası boyutta yetişmiş uzmanlardan oluşan Üst Düzey Uzmanlar Grubu (HLEG)'nu 2007 yılında kurmuştur[185]. HLEG, siber suçlara müdahâle edilebilmesi adına öneriler geliştirerek üye devletler için siber güvenliği teşvik eden teklifler sunmaktadır.

[183] https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (25.10.2020)
[184] Serkan Yenal ve Akdemir, Naci, "Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi", *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C:11, S: 1, 2020, s. 426.
[185] ITU, *GCA Chairman's Report*, 2007, s. 3-4.

Şekil 3.1'de HLEG tarafından 2008 Küresel Strateji Raporu'nda siber güvenlik için olması gereken beş ana kriter görülmektedir. Ayrıca ITU tarafından oluşturulan Siber Güvenlik Kapısı (Cybersecurity Gateway) yine uluslararası siber dünyayı bir araya getiren bir platformdur. Bu platform içerisinde kamu ve özel sektör teşebbüsleri, Sivil Toplum Kuruluşları (STK), akademik kuruluşlar, bölgesel organizasyonlar yer alır. Bu alanda gerek ulusal gerek bölgesel ve hatta uluslararası siber güvenlik alanında yapılan ve yayınlanan çalışmalar paylaşılarak bilgi alışverişinde bulunulur[186].



Şekil 3.1 HLEG Küresel Strateji Raporundaki Siber Güvenliğin Beş Ana Unsuru[187]

Bu beş ana kriter ile beraber ilki 2014 yılında oluşturulan Küresel Siber Güvenlik Endeksi versiyon 1 şeklinde yayınlanmıştır. Daha sonra 2017 yılında 2. versiyon GCI ve son olarak 2018 yılına ait 3. versiyon GCI, ITU tarafından yayınlanmıştır[188]. 4. versiyon çalışmalarına 2019 yılında başlanmıştır. Ancak dünyayı etkisi altına alan Kovid-19 virüsü nedeniyle çalışmalar hâlen devam etmektedir.

[186] http://groups.itu.int/cybersecurity-gateway/HOME.aspx (25.10.2020)
[187] ITU, 2017, s.3.
[188] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (25.10.2020)

3.2. İNGİLTERE VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRILMASI

Türkiye ve İngiltere için siber güvenlik politikalarına yön verme konusunda GCI oldukça önemlidir. GCI; yasal düzenlemeler, kurumsal yapılanma, teknik çerçeve, kapasite geliştirme ve uluslararası iş birliğinden oluşan beş temel güvenlik kriterine dayanmaktadır. 2014, 2017 ve 2018 GCI kapsamında bu iki ülkenin yıllar içinde siber güvenlik adına yaptıkları ve yaptıklarının sonucunda uluslararası düzeyde sıralamaları incelenmiştir. Bu endeksler aynı zamanda küresel dünyadaki siber durumların yanı sıra ülkelerin kendi bölgeleri içindeki sıralamalarını göstermektedir. ITU'nun GCI için kullandığı metodoloji, beş ana başlık kapsamında uzman grup tarafından hazırlanan sorulardan oluşan anket ile beraber ölçek etkinliğidir. Veri toplama aracı anket sonucunda katılımcı ülkeler tarafından elde edilmiş ve ülkelere gönderilen bu anketlerin geri dönüşlerine göre belirlenen kriterler doğrultusunda bir puanlama sistemi ortaya konulmuştur. Bu puanlama da ülkelerin hem dünya hem de bölgesel sıralamalarını belirlemiştir. Anket soruları yıllara göre farklılık gösterebilir ancak temel amaç ülkelerin kendi sıralamalarını görerek küresel anlamda siber güvenlik farkındalığı oluşturmaktır. Türkiye ve İngiltere GCI'ya göre Avrupa bölgesinde yer almışlardır. İki ülkenin aynı bölgede yer alması sadece küresel sıralama kıyası için değil aynı zamanda bölgesel sıralamaları konusunda da kıyaslama imkânı sunmaktadır.

3.2.1. Yasal Düzenlemeler (Legal Measures)

2014 yılı GCI yasal düzenlemeler *ceza hukuku* ile *düzenleme ve uyum*[189] adlı iki alt kategori tarafından desteklenmektedir. Ceza hukukunda, siber suç mevzuatının bilişim ve bilişim altyapısına yetkisiz erişimle mücadelesi konusu ele alınmıştır. Düzenleme ve uyum başlığında ise siber güvenlik yönetmeliği, verilerin nasıl

[189] ITU, *Global Cybersecurity Index-Cyberwellness Profile (v1) Report,* 2015, s.31.

korunmaya alınacağı ve siber güvenlik için yapılması gereken standardizasyon işlemlerinin kapsamı ele alınmıştır.

Türkiye, yasal düzenlemeler için *ceza hukuku* kapsamında 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi" Hakkındaki Kanun çalışmasını yaptığını belirtmiştir. Bu konuda, TCK işlenmiş suç ve suçun kapsamıyla beraber yaptırımları içerir[190] ve "Bilişim Alanında Suçlar" alt başlığındaki madde 243-246 ile beraber "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" alt başlığındaki 135,136 ve 138. maddelerle ele alınmıştır[191]. Bu konuda TCK 243-245. maddeler özellikle bilişim alanında işlenen suçlara yönelik yaptırım ve cezai uygulamalarını kapsamaktadır. Türk Ceza Kanunu'nun 243 maddesine göre "*(1)Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî 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. (4)Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır*." Burada *hukuka aykırı olarak giren* ifadesi ile sisteme yasadışı yollardan kişi veya kişilerin izni olmaksızın giren kişi anlamında kullanılmıştır ve içerik daha çok sistemine girmeyi engellemek içindir[192]. TCK 244. maddesine göre *"(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*

[190] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, RG: 23.05.2007, 26530, s.10103.
[191] Uğur Boğa, *Bilişim Suçlarıyla Mücadele Yöntemleri*, Radyo ve Televizyon Üst Kurulu, Uzmanlık Tezi, 2011, Ankara, s. 73.
[192] Uğur İhtiyaroğlu, "Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi", *Hacettepe Hukuk Fakültesi Dergisi*, S: 10, No: 2, 2020, s. 408.

veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hâlinde, 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 beş bin güne kadar adlî para cezasına hükmolunur." Bu maddenin 1. ve 2. Fıkralarında verilere sadece bilişim sistemi kullanarak yapılan faaliyetleri kapsamış olup ileride kullanılacak yeni yöntemler konusunda cezaî bir yaptırım belirtmemiştir[193]. Madde 245'te ise "*(1)Başkasına ait bir banka veya kredi kartının izinsiz kullanılması suretiyle yarar sağlama suçunun cezası 3 yıldan 6 yıla kadar hapis ve beş bin güne kadar adli para cezasıdır. (2)Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçunun cezası 3 yıldan 7 yıla kadar hapis cezası ve 10 bin güne kadar adli para cezasıdır. (3) Sahte bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlama suçun cezası 4 yıldan 8 yıla kadar hapis cezası ve 5000 güne kadar adli para cezasıdır."* 243 ve 244. maddelere göre 245. madde için cezaî yaptırım konusundaki artışın nedeni Türkiye'de işlenen siber suç sayısındaki en yüksek oranın kredi kartı ve banka kartı dolandırıcılığı alanında olmasıdır[194]. 5651 sayılı Kanun içinde internet için içerik, yer, erişim ve toplu kullanım sağlayıcılarının yükümlülüklerinden bahsedilmiştir[195]. Siber güvenlik adına *düzenleme ve uyum* kapsamında ayrıca 5809 sayılı "Elektronik Haberleşme Kanunu[196]" 10.11.2008 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Devamında Elektronik Haberleşme Güvenliği (2008)[197] ve Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması (2013)[198] hakkındaki yönetmelikler yayımlanmıştır. Kanunun ve bu iki yönetmeliğin de temel amacı, kişilerin güvenli iletişim kurma haklarını yasal güvence altına almaktır.

---

[193] Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", *Article Letter Summer,* 2015, s. 80.
[194] Metin Turan, Külcü, Özgür, "Türkiye'de bilişim suçlarının tanımlanması ve yaşanan ihlallere yönelik içerik analizi" *Türk Kütüphaneciliği,* S:*28, No:* 1, 2014, s. 44"
[195] A.g.k., s. 10104-10104(1).
[196] Elektronik Haberleşme Kanunu, RG: 10.11.2008, 27050 (mükerrer), s. 10377.
[197] Elektronik Haberleşme Güvenliği Yönetmeliği, RG: 20.07.2008, 26942, s.1.
[198] Ayça Çiğdem Ayözger, *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul, 2016, s. 12.

İngiltere (Birleşik Krallık), yasal düzenleme konusunda, *ceza hukuku* adına 1990 yılında "Bilgisayarı Kötüye Kullanma Yasası[199]", 1998 yılında "Veri Koruma Yasası[200]", 2006 yılında "Dolandırıcılık Yasası[201]"nı çıkartmıştır. Bu kapsamda yasal düzenleme adına İngiltere'nin bu sürece erken dâhil olduğu görülmektedir. Bilgisayarı Kötüye Kullanma Yasası suçlunun işlediği bilgisayar suçunun fiili zarar derecesine göre kademelendirilmiş ceza yaklaşımını benimser. Bu yasa, bilgisayara doğrudan yetkisiz erişim ve başka suçların işlenmesi için bilgisayarın aracı olarak kullanıldığı yetkisiz erişim[202] olmak üzere iki gruba ayırır. Veri Koruma Yasası ise kişisel verilerin işlenmesi durumunda veri sahibi olan gerçek kişinin korunmasını hedefler ve bu sağlık sektörü için önemlilik arz eder[203]. Dolandırıcılık Yasası, bilişim sistemi kullanılarak yapılan dolandırıcılıkları ele almaktadır. Yasayla beraber internet üzerinden işlenen sahtecilik ve yanıltıcı hizmet alımı suç olmuştur[204]. *Düzenleme ve uyum* için Ofcom (Office of Communications), Telekom Yönetmeliği ve Bilgi Komisyon Yönetmeliği[205]ni oluşturmuştur. Bu yönetmelikler, bilgiyi koruyarak bireylerin güvenli iletişimini sağlamıştır. Ofcom İngiltere'nin telefon ve yayın şirketlerinin yasalara uyup uymadıklarını denetleyen resmî bir kurum[206]dur.

2017 yılı GCI yasal düzenlemeler kapsamında siber suç mevzuatı (Cybercriminal legislation), siber güvenlik düzenlemesi (Cybersecurity regulation) ve siber güvenlik eğitimine yönelirken 2018 yılı GCI siber suç mevzuatı, siber güvenlik düzenlemesi ve istenmeyen posta sınırlanması/engellenmesi alt başlıkları ön plana çıkmıştır.

[199] Computer Misue Act, RA: 29.06.1990, 18.
[200] Data Protection Act, RA: 16.07.1998, 29.
[201] Fraud Act, RA: 08.11.2006, 35.
[202] Oliver Morton, "Tool, A. Windows Domain Enumeration", *Project Report Nettynum*, 2014, s. 56.
[203] Amy Iversen, Liddell, Kathleen, Fear, Nicola, Hotopf, Matthew ve Wessely, Simon, "Consent, confidentiality, and the data protection act", *Bmj*, S: 332, No: 7534, 2006, s. 165.
[204] Ian Walden, *Computer Crimes and Digital Investigations*, Oxford University Press, Oxford, 2016, Chapter 3, s. 55.
[205] ITU, 2015, s. 500.
[206] https://www.gov.uk/government/organisations/ofcom (26.10.2020)

Türkiye, 2014 yılı sonrası yasal düzenleme kapsamında 6 Şubat 2014 tarihinde yayımlanan 6518 sayılı kanun ile 5809 sayılı Elektronik Haberleşme Kanununa eklenen Ek madde 1 ile Bilgi ve Teknolojileri ve İletişim Kurumuna siber güvenlikle ilgili yeni görevler tahsis etmiştir. Bu ek madde 1 ile Siber Güvenlik Kurulunun, görev ve yetkileri düzenlenmiştir[207]. 2017 yılı GCI Avrupa bölgesi için Türkiye yasal düzenlemeler için siber suç mevzuatı ve siber güvenlik düzenlemesi hakkında başarılı olurken siber güvenlik eğitimi konusunda beklenen başarıyı sergileyememiştir.

İngiltere, NATO ile 2017 yılında Mutabakat Zaptı imzalayarak kendi yasalarını Genel Veri Koruma Yönetmeliği (GDPR) ve AB Ağ ve Bilgi Güvenliği (NIS) Direktifi[208] ile uyumlu hâle getirmiştir. Bunun sonucunda 2017 GCI raporuna göre İngiltere, Avrupa bölgesinde yasal düzenleme kategorisinde başarılı olmuştur. ITU'ya göre Tablo 3.1'de 2017 yılında İngiltere ve Türkiye için yasal düzenleme kategorisindeki durumları görülmektedir.

Tablo 3.1 2017 GCI Türkiye-İngiltere Yasal Düzenlemedeki Durumları[209]

	2017 GCI	
	Türkiye	Birleşik Krallık
Siber Suç Mevzuatı		
Siber Güvenlik Düzenlemesi		
Siber Güvenlik Eğitimi		
Yasal Düzenlemeler		

İyi
Kötü
Orta

2018 yılı, 2014 yılına nazaran yasal düzenlemeler konusunda daha kapsamlıdır. Ancak 2017 ve 2018 yılları arasındaki zaman aralığı oldukça az olması nedeniyle yasal düzenlemeler için benzer alt başlıklar görülmektedir.

[207] Elektronik Haberleşme Kanunu, 2008, s. 10410.
[208] Muharrem Bayrak, "ABD ile Birleşik Krallık'ın AB ve NATO Çerçevesinde Siber Alanlarının Tarihsel Analizi", *Cyberpolitik Journal*, S: 5, No: 9, 2020, s. 42.
[209] ITU, *Global Cybersecurity Index (v2) Report*, 2017, s. 37.

Türkiye, 07.04.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu[210]nu yürürlüğe sokmuştur. Bu 2018 yılı GCI için yasal düzenleme konusunda büyük önem arz etmektedir. KVKK; kişisel verilerin işlenmesi, özel hayatın gizliliği kapsamında veri işleyen kişi veya kişilere getirilecek yükümlülüklerin usul ve esaslarını belirlemektedir.

İngiltere, yasal düzenlemeler hususunda 2018 Veri Koruma Yasası (DPA)[211], Genel Veri Koruma Yönetmeliği (GDPR)'nin uygulayıcısı niteliğindedir. 2018 Ağ ve Bilgi Sistemleri Yönetmeliği (NISR)[212] ise AB'nin Ağ ve Bilgi Sistemleri Direktifi'ni uygulamak için oluşturulmuştur. Bu, 2018 GCI için İngiltere'nin siber güvenlik adına yasal düzenlemeler konusunda yaptığı faaliyetlerin göstergesidir. İlk olarak 1998 yılındaki DPA'nın on yıllık süre içinde yetersiz kalması sonucu yenilenerek 2018 yılı DPA yayımlanmıştır. 2018 yılında DPA, kişisel veriler ve bu verilerin korunması hususuna dikkat çekmektedir. Bu başlık içinde İngiltere 2018 GCI raporunda Belçika, Danimarka, İspanya, Litvanya, Sırbistan ve Slovakya ile beraber kendi bölgesinin en iyi örnekleri arasında yer almıştır[213].

3.2.2. Kurumsal Yapılanma (Organizational Measures)

Kurumsal yapılanma başlığı için 2014 GCI'da yer alan alt başlıklar; politika, yönetişim için yol haritası, sorumlu kurum ve ulusal kıyaslama[214]dır. Siber güvenlik endeksinin belirlenmesinde ülke içi kurumsal yapılanma ve bu yapılanma oluşturulurken belirlenecek politika ışığında yönetişim modelinin belirlenmesi oldukça önemlidir. Bu, ülkenin kendi durumunu analizi ederek siber güvenlik alanında nasıl yol alacağını belirler.

[210] Kişisel Verilerin Korunması Kanunu, RG: 24.03.2016, 29677, s. 12301.
[211] Data Protection Act, RA: 23.05.2018, 12.
[212] The Network and Information Systems Regulations, RG: 10.05.2018, Part 1.
[213] ITU, *Global Cybersecurity Index (v3) Report, 2018*, s. 35.
[214] ITU, 2015, s. 32-33.

Türkiye, politika olarak Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı[215]'nı belirlemiştir. Bu eylem planı AB ve NATO'nun siber güvenlik stratejileri ile uyumlu olarak hazırlanmıştır. Temel amacı, kamu kurum ve kuruluşları için BİT hizmetlerinin sunumu konusunda güvenliğin sağlanmasıyla beraber hizmet, işlem ve verilerin oluşturulmasına imkân sağlamasıdır. Bu eylem planı doğrultusunda 29 ana eylem ve 95 alt eylem belirlenerek *yönetişimsel yol haritası* oluşturulmuştur. Bakanlar Kurulunca 11 Haziran 2012 tarihli Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyon Hakkındaki Kararla Siber Güvenlik Kurumu[216], Türkiye için siber güvenlik faaliyetlerini yürüten *sorumlu kurum* olmuştur. *Ulusal kıyaslama* içinde üç siber güvenlik tatbikatı düzenlenmiştir. İlk tatbikatın 25-28 Ocak 2011 tarihinde gerçekleştirilmesiyle kurumlar arası bilgi paylaşımı ile beraber tecrübelerin aktarılarak tüm seviyelerde bilgi farkındalığı oluşturmak[217] amaçlanmıştır. 2012 yılında "Redhack" hacker grubunun Türkiye'deki kamu kurumlarını hedef aldığı saldırıların ortaya çıkması ile 25 Aralık 2012 tarihli ikinci Ulusal Siber Güvenlik Tatbikatı[218] yapılmıştır ve bunu üçüncü Ulusal Siber Güvenlik Tatbikatı izlemiştir. Elektronik haberleşme iletişim araçları ISO/IEC 27001 ile uyumlu hâle getirilerek siber güvenlik gelişimine katkı sağlamıştır.

İngiltere, politika olarak 2011 yılında Ulusal Güvenlik Stratejisini[219] yayınlamıştır. Temel amaç, ülke vatandaşlarının güvenlik düzeyini ve güvenli ağ kullanımını sağlayarak refah düzeyini arttırmaktır. *Yol haritasını* yayınlanan Ulusal Güvenlik Stratejisine göre belirlemiştir. *Kurumsal yapılanma* konusundaki yetkili kurumu, Kabine Ofisine bağlı Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA)[220]dir. OCSIA, ulusal siber güvenliğin ilerlemesinden sorumlu olduğu için ulusal siber

[215] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013, s. 13.
[216] Elektronik Haberleşme Kanunu, 2008, s. 10410.
[217] Tübitak Bilgem, *Siber Güvenlik Tatbikat Raporu*, 2012, s. 13.
[218] Gül Nazik Ünver, "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Dergisi*, S: 2, No: 3, 2017, s. 110.
[219] Government UK, *A Strong Britain in an Age of Uncertainty: The National Security Strategy Report*, 2011, s. 29,42.
[220]https://www.gov.im/about-the-government/departments/home-affairs/office-of-cyber-security-and-information-assurance/ (28.10.2020)

güvenliği *kıyaslama* yine bu kurumun yetkileri arasındadır ve bu konu hakkındaki faaliyetleri yürütür.

2017 ve 2018 GCI için kurumsal yapılanmanın alt başlıkları strateji, sorumlu kurum ve siber güvenlik ölçümleri olmak üzere ortak başlıklardır. Siber güvenlik ölçümü, 2014 yılı yönetişim için yol haritasının belirlenmesi hususunda siber yönetişimin alt başlıklarından biridir. Yani 2014 yılındaki yönetişim kavramı daha özele indirgenerek siber güvenlik ölçümü alt başlığı ile ele alınmıştır. Siber güvenlik ölçümü, eylem planlarının içinde yer alan eylemlerin gerçekleştirilme durumuna istinaden başarıyı kapsayan tamamlayıcı belge[221] olarak tanımlanmıştır. Türkiye'nin siber güvenlik yönetişim modeli Şekil 3.2'de görülmektedir.

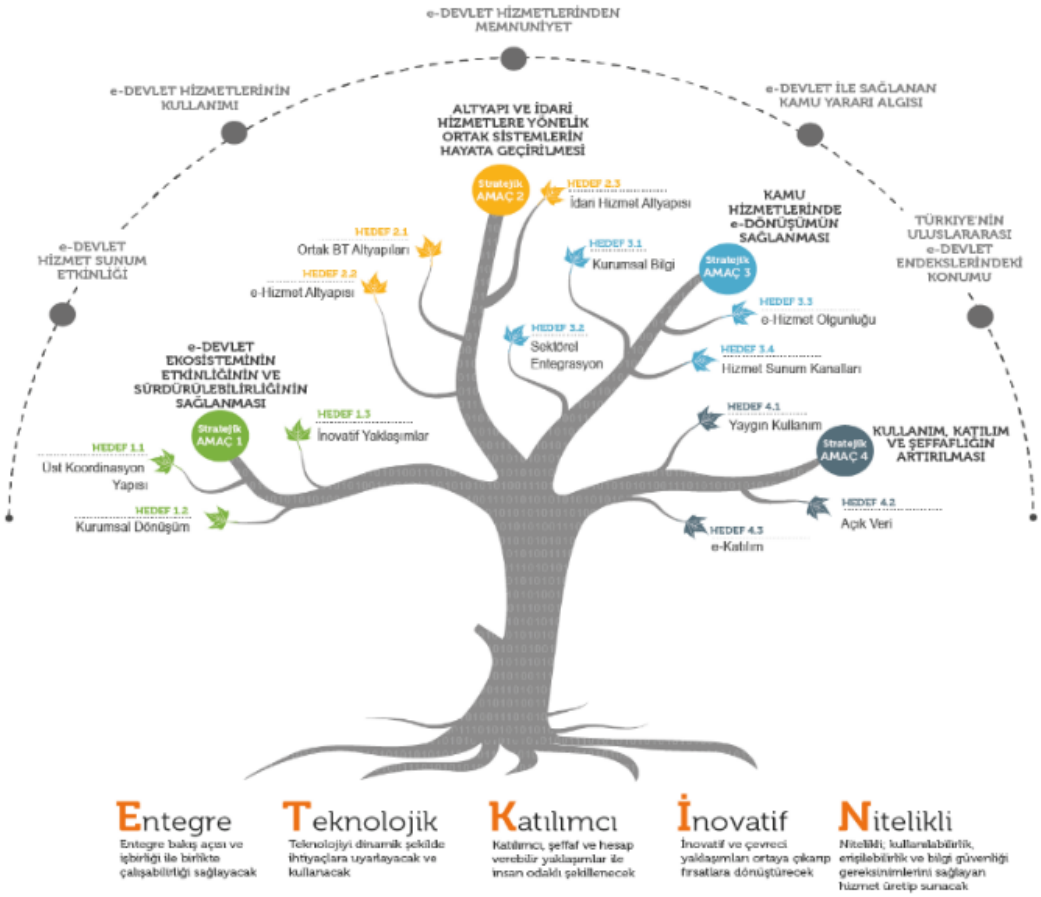


Şekil 3.2 Türkiye Siber Güvenlik Yönetişim Modeli[222]

Türkiye, belirlediği strateji doğrultusunda 2017 ve 2018 GCI kapsayacak biçimde 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı[223]'nı ve 2016-2019 Ulusal Siber Güvenlik Stratejisi[224]'ni, 2013-2014 Eylem Planı'nın devamı niteliğinde UDHB tarafından Mart 2016'da ortaya konmuştur. 2014 yılı GCI'da belirtildiği gibi sorumlu kurum Siber Güvenlik Kurumudur. Şekil 3.3'te 2016-2019 Ulusal e-Devlet

[221] T.C. Ulaştırma ve Altyapı Bakanlığı, Ulusal Siber Güvenlik Stratejisi 2020-2023, 2020, s. 33-34.
[222] Dijital Türkiye Platformu, *Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler Raporu*, 2017, s. 8.
[223] T.C. UDHB, *2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı, 2016.*
[224] UDHB, 2016, s. 8-9.

Stratejisi ve Eylem Planı'nın vizyon ve strateji odağı açıkça görülmektedir. Bu eylem planında açık veri kullanımı ve kullanım amaçlarındaki katma değer için ölçümleme çalışmalarının yapılacağı[225] belirtilmiş ve Ulusal Siber Güvenlik Strateji 2020-2023 için örnek oluşturmuştur.



Şekil 3.3 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı Haritası[226]

İngiltere, 2017 ve 2018 GCI için belirlenen stratejiler, 2015 yılı Ulusal Güvenlik Stratejisi (NSS)[227] ile beraber onun tamamlayıcısı olarak düzenlemiş ve 2018 yılında Kabine Ofisi tarafından Ulusal Güvenlik Yeteneği İncelenmesi (NSCR) [228] ortaya koymuştur. Sorumlu kurum 2014 yılında belirtildiği gibi Kabine Ofisine

[225] UDHB, 2016, s. 53.
[226] UDHB, 2016, s. 3.
[227] Goverment UK, *National Security Strategy and Strategic Defence and Security Review 2015*, 2015, s. 82.
[228] Goverment UK, *National Security Capability Review (NSCR)*, 2018, s. 3.

bağlı Siber Güvenlik ve Bilgi Güvencesi Ofisidir. Siber güvenlik ölçümleri ile ilgili ülke olarak yapılan herhangi bir çalışma belirtilmemiştir. İngiltere 2017 GCI raporunda kurumsal yapılanma alt başlıklarından olan strateji kategorisinde yaptığı çalışmalar sonucunda indeksin anlaşılmasına yardımcı olmak için örnek gösterilmiştir[229]. Tablo 3.2'de 2017 GCI için iki ülkenin kurumsal yapılanma konusunda üç alt kategorideki durumları görülmektedir. Tabloya göre Türkiye ve İngiltere'nin siber güvenlik ölçüm konusuna odaklanmaları gerekir.

Tablo 3.2 2017 GCI Türkiye-İngiltere Kurumsal Yapılanma Durumları[230]

	2017 GCI	
	Türkiye	Birleşik Krallık
Strateji		
Sorumlu Kurum		
Siber Güvenlik Ölçümleri		
Kurumsal Yapılanma		

İyi
Kötü
Orta

3.2.3. Teknik Çerçeve (Technical Measures)

GCI belgeleri içinde en detaylı bölüme sahip başlıklardan biridir. 2014 yılı GCI için Bilgisayar Olay Müdahâle Ekibi (CIRT), Bilgisayar Acil Durum Müdahâle Ekibi (CERT) ve Bilgisayar Güvenliği Olay Müdahâle Ekibi (CSIRT) ile standartlar ve sertifikasyon[231] olmak üzere üç alt kategori bulunur. Bu ekipler, siber güvenlik alanında uzman bilgisine ihtiyaç duyar. Çocukların çevrimiçi korunmasına ilişkin başlık 2014 GCI'da teknik çerçevenin alt başlığında yer almayarak farklı bir başlık olarak incelenmiştir. 2017 ve 2018 GCI'da ise çocukların çevrimiçi korunması başlığı teknik çerçevenin altında yer almıştır.

Türkiye, resmî olarak CIRT için SOME adıyla ulusal CERT'e sahiptir. SOME'ye BTK ev sahipliği yapmaktadır ve 20 Aralık 2013 tarihinden beri Türkiye

[229] ITU, 2017, s. 41.
[230] ITU, 2017, s. 37.
[231] ITU, 2014, s. 32.

CERT üyesidir[232]. *Standartlar ve sertifikasyon* başlıkları kapsamında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile beraber 5809 sayılı Elektronik Haberleşme Kanunu yer almaktadır. Standartlar için ülkedeki standartları düzenleyen Türk Standartları Enstitüsü, ISO/IEC 27001, ISO/IEC 15408 ve ISO/IEC 12207 uluslararası standartları ile uyumlu olarak siber güvenliği standartlaştırmak için hizmet vermektedir. ISO/IEC 27001, uluslararası kabul gören bilgi güvenliği konusunda şirket veya kurumların risk yönetim, görev sorumluluklar, acil durumlar karşısında olayın nasıl yönetileceği hususundaki süreci gösteren standarttır. Bu standart, şirketin bilgi güvenliğinin doğru uygulandığını sertifikalandırarak belgelendirme[233] yapılmasını sağlar. ISO/IEC 15408 değerlendirilmesi yapılmış ve sertifika almış güvenlik hedeflerini kapsayan bilgi sistemi konusunda güvenlik değerlendirme standardıdır[234]. ISO/IEC 12207 ise Bilgi Teknolojisi Yazılım Yaşam Döngüsü Süreçlerini içeren standarttır[235].

Türkiye *çocukların çevrimiçi korunması* üzerine Ceza Kanunu (Madde 226)[236], 5651 sayılı Kanun (Madde 8)[237] ile beraber BM Çocuk Hakları Sözleşmesi'nin ilgili hükümlerini (Madde 16, 17(e), 34(c))[238] kabul ederek uygulamaktadır. Kurumsal olarak desteği 5651 sayılı Kanun kapsamında BTK vermektedir.

İngiltere, 2014 yılının sonunda CIRT kuracağını belirtmiştir ve mevcut olarak Kritik Altyapılar, Hükümet Ağı ve Askeri Ağlarda CIRT'lar mevcuttur. Bilgi teknolojileri çözümleri konusunda standardizasyon çalışmaları yapılmıştır. Bilgi Güvenliği Uzmanları Enstitüsü (IISP) tıpkı Türkiye'deki TSE gibi sertifikasyon çalışmaları yürütülmektedir. IISP'nin amacı bilgi güvenliği konusunda sertifikasyon

---

[232] https://www.first.org/members/teams/tr-cert (05.11.2020)
[233] Georg Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management", *Journal of Information Security,* S: 4, 2003, s. 92.
[234] Daisuke Horie, Yajima, Kenichi, Azimah, Noor, Goto, Yuichi ve Cheng, Jingde, "GEST: A Generator of ISO/IEC 15408 Security Target Templates", *Computer and Information Science 2009,* Springer, Berlin, Heidelberg, 2009, s. 149.
[235]https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073099056067082074047082081113088112 (05.11.2020)
[236] TCK, RG: 12.10.2004, 25611, s. 9019.
[237] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 2007, s.10104-3.
[238] United Nations, *Birleşmiş Milletler Çocuk Hakları Sözleşmesi,* 1989, s. 6,11.

çalışmaları ile bilgi güvenliği standartlarını yükseltmektir. Bu kapsamda IISP tarafından dört üyelik modeli belirlenmiştir. Bu üyelik modelleri:

- Bağlı: Enstitü ile ilişki kurmak isteyen herkese açık olan üyelik şeklidir.
- İlişkili: Bazı tanımlanmış üniversitelere veya bazı uluslararası eğitim organizasyonlarının bilgi güvenliğine sahip üyelik modelidir.
- Tam üyelik: Daha tanımlanmamıştır ve davetiye esaslı üyelik esas alınacaktır.
- Arkadaşlık: Henüz başlatılmayan ancak üst düzey aydınların sahip olacağı üyelik biçimidir[239].

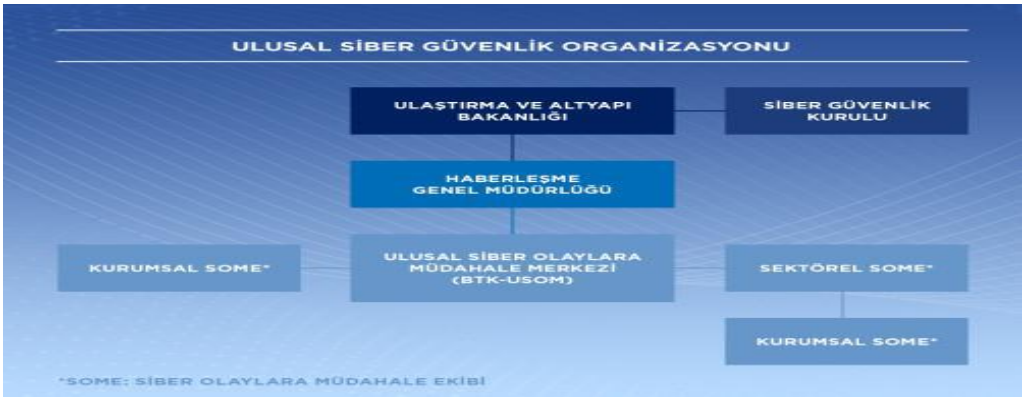
İngiltere *çocukların çevrimiçi korunması* konusunda Cinsel Suçlar Yasası[240] (Madde 48-50), Çocukları Koruma Yasası (Madde 1)[241], Ceza Adaleti ve Göçmenlik Kanunu (Madde 63)[242], Kötü Amaçlı İletişim Yasası (Madde 1)[243] gibi düzenlemeler yapmıştır ve Türkiye gibi BM Çocuk Hakları Sözleşmesi[244] ve ilgili maddelerini kabul etmiştir. Uygulama mekanizması Çocuk İstismarı ve Çevrimiçi Koruma Komutanlığı (CEOP)[245] ve İnternet İzleme Kurumu (IWF)[246]'dur.

2017 GCI teknik düzenlemeler için ulusal CIRT, hükümet CIRT, sektörel CIRT, kuruluşlar için standartlar, profesyoneller için standartlar ve çevrimiçi çocuk koruması[247] olmak üzere altı alt kategoriyi kapsarken 2018 GCI'da 2017 ile benzer olarak CERT/CIRT/CSIRT, standart uygulama çerçevesi, standardizasyon gövdesi, istenmeyen postaları ele almak için kullanılan teknik mekanizmalar ve yetenekler,

[239] https://whatis.techtarget.com/definition/IISP-Institute-of-Information-Security-Professionals (06.11.2020)
[240] Sexual Offences Act, RA: 20.11.2003, 42, s. 29-30.
[241] Protection of Children Act, RA: 20.07.1978, 37, s. 1.
[242] Criminal Justice and Immigration Act, RA: 08.05.2008, 4, s. 50.
[243] Malicious Communications Act, RA: 29.07.1988, 27, s. 1.
[244] United Nations, 1989, s. 6,11.
[245] https://www.ceop.police.uk/safety-centre/ (06.11.2020)
[246] https://www.iwf.org.uk/ (06.11.2020)
[247] ITU, 2017, s. 5.

siber güvenlik amaçlı bulut kullanımı, çevrimiçi çocuk koruma mekanizması[248] olarak altı alt kategoriyi kapsamaktadır.

Türkiye, teknik düzenleme kapsamında 2017 ve 2018 GCI için USOM ile beraber kurumsal SOME'nin etkinlik alanı genişletmiştir. Bu hususta siber güvenlikle alakalı tedbir almayan firmalara USOM tarafından idari para kesme ceza yetkisi[249] verilmiştir. USOM'un ulusal siber güvenlik organizasyonu Şekil 3.4'te görülmektedir. SOME'ler USOM'a bağlı olarak sektörel SOME ve kurumsal SOME olmak üzere ikiye ayrılmıştır. Bunun sonucunda sektörel SOME hizmet alanı kritik altyapı olarak belirlenirken kurumsal SOME'ler için kamu kurumları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları[250] için hizmet alanı belirlenmiştir. Ayrıca Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan "Güvenli Yazılım Geliştirme Temel Kuralları[251]", "Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri[252]" gibi birçok teknik doküman da Türkiye'nin teknik düzenlemeler konusunda önemli belgelere sahip olduğunu gösterir.



Şekil 3.4 Ulusal Siber Güvenlik Organizasyon Şeması[253]

[248] ITU, 2018, s.8.
[249] https://www.aa.com.tr/tr/turkiye/usoma-idari-para-cezasi-kesme-yetkisi-verildi-/1268694 (07.11.2020)
[250] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *Kurumsal SOME Kurulum ve Yönetim Rehberi*, 2014, s. 10.
[251] Tübitak Bilgem, *Güvenli Yazılım Geliştirme Temel Kuralları Dokümanı (Sürüm 1.12)*, 2014, s. 4.
[252] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri*, 2013, s. 6.
[253] https://www.uab.gov.tr/siber-guvenlik (07.11.2020)

İstenmeyen e-postalara yönelik 6698 sayılı KVKK'nın 16 Ekim 2018 tarihli Resmî Gazete'de yayımlanan kararına göre "*İlgili kişilerin rızalarını almadan ve Kanunun 5 inci maddesinde hüküm altına alınan işleme şartlarını sağlamadan, telefon numaralarına SMS göndermek, arama yapmak veya e-posta adreslerine posta göndermek suretiyle reklam içerikli ileti yönlendiren veri sorumluları ile veri sorumluları adına reklam içerikli mesaj/e-posta göndermek veya arama yapmak amacıyla ilgili kişilerin açık rızaları bulunmaksızın bu verileri kullanan veri işleyenlerin söz konusu veri işleme faaliyetlerini Kanunun 15 inci maddesinin (7) numaralı fıkrası uyarınca derhal durdurması gerektiği*[254]" hususlarında kamuoyunun bilgilendirilmesi ve bu kararın kurumun internet sitesi ile Resmî Gazete'de yayımlanması oy birliği ile kabul edilmiştir. *Çevrimiçi çocuk korunma mekanizması* için KVKK "Çocukların Kişisel Verilerinin Korunması" hakkında pratik broşürlerin[255] olduğu önerilere yer vermiştir. Ayrıca Türkiye Halkla İlişkiler Derneği tarafından oluşturulan TÜHİD Meslek İlkeleri'nin 3. maddesinde "*Çocuklarla ilgili ürünlerin tanıtılması için hazırlanan halkla ilişkiler mesajlarında onların güven duygularını zedeleyecek, ruhsal ve fiziksel zayıflıklarını etkileyecek içerik bulunmamasına özen gösterirler*"[256] ifadesi yer almaktadır.

İngiltere, 2017 ve 2018 GCI için teknik düzenlemeler konusunda 2014 yılı GCI raporunda *CIRT* kurulacağını taahhüt etmiştir. Bu kapsamda ulusal CIRT, CERT-UK adı altında faaliyete geçirilmiştir. CERT için dört ilkeden oluşan görevler belirlenmiştir. Bunlar:

- Ulusal siber güvenlik olay yönetimi,
- Kritik altyapı hizmeti veren şirket ve kurumlara destek verilmesi,
- Akademisyenlerin siber güvenlik konusunda farkındalık ve sektörel seviyelerini teşvik etmek ve yetiştirmek için faaliyet yürütmesi,

[254] Kişisel Verileri Koruma Kurumu Kurul Kararı, RG: 16.10.2018, 119, s. 1.
[255] https://www.kvkk.gov.tr/Icerik/6737/Cocuklarin-Kisisel-Verilerinin-Korunmasi-Bakimindan-Dikkat-Edilmesi-Gerekenler (08.11.2020)
[256] http://www.tuhid.org/tuhid-meslek-ilkeleri.html (08.11.2020)

- Diğer SOME'ler ile iletişim kurularak koordinasyon ve işbirliği yapılması[257] istenmiştir.

CERT bünyesi altında Siber Güvenlik Bilgi Paylaşım Ortaklığı (CISP) kurularak siber güvenlik bilgi paylaşımı ile katılımcılar, güvenlik açıkları konusunda bilgi sahibi yapılarak katılımcı bilgi düzeyi arttırılmıştır[258]. *İstenmeyen e-postalar* içinde GDPR'nin 21. Maddesi uyarınca veri sahibine ait verilerin pazarlama amacıyla işlenmesinin yanı sıra bilimsel ve tarihsel araştırmalar için istatistiksel amaçlarla işlenmesinde kişinin *itiraz hakkı* mevcuttur[259]. *Çocukların çevrimiçi korunması* hakkında ICO'nun DPA ile beraber GDPR açık ve net hükümler içererek şeffaflık esasıyla bu görevi üstlenir[260]. Belçika, Danimarka, Estonya, Litvanya, Lüksemburg ve Sırbistan ile beraber İngiltere 2018 yılı GCI raporunda teknik çerçeve konusunda en iyi örnekler arasında yer almıştır[261].

2014 yılına kıyasla 2017 ve 2018 GCI teknik düzenleme başlığı altındaki alt kategori sayısının artması ile beraber ülke sorumluluklarının da bu alanda arttığı görülmektedir. Tablo 3.3'te Türkiye ve İngiltere için 2017 GCI teknik düzenleme konusundaki mevcut durumları görülmektedir. İki ülke de teknik düzenlemeler konusunda başarılı olarak iyi kategorisinde yer almışlardır.

[257] Yunus Emre Karabulut, Boylu, Gülistan, Küçüksille, Ecir U. ve Yalçınkaya, Mehmet A., "Characteristics of Cyber Incident Response Teams in the World and Recommendations for Turkey", *Balkan Journal of Electrical and Computer Engineering*, S: 3, 2015, s. 175.
[258] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp (09.11.2020)
[259] https://gdpr-info.eu/art-21-gdpr/ (09.11.2020)
[260] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/ (10.11.2020)
[261] ITU, 2018, S. 40.

Tablo 3.3 2017 GCI Türkiye-İngiltere Teknik Düzenleme Durumları[262]

	2017 GCI	
	Türkiye	Birleşik Krallık
Ulusal CERT/CIRT/CSIRT		
Hükümet CERT/CIRT/CSIRT		
Sektörel CERT/CIRT/CSIRT		
Kuruluşlar için Standartlar		
Profesyoneller için Standartlar		
Çevrimiçi Çocuk Koruma		
Teknik Düzenleme		

İyi
Kötü
Orta

3.2.4. Kapasite Geliştirme (Capacity Building)

2014 GCI için standardizasyon geliştirme, insan gücü geliştirme, profesyonel sertifikasyon ve acente sertifikası[263] olmak üzere dört ana başlıkta değerlendirilir. Kapasite geliştirmenin temel amacı, ülkenin mevcut kapasitesini görmekle beraber standartlaşma ve yetiştirilebilecek uzman insan kapasitesini arttırmaktır.

Türkiye; TSE, standardizasyon işlemlerini üstlenen kurumdur. Bu konu hakkında uluslararası siber güvenlik standartları (örneğin ISO/IEC 27000 ailesi) ile uyum sağlama sürecini yönetir. Aynı zamanda ülkenin sektörel ihtiyaçları doğrultusunda standardizasyon faaliyetleri yürütür. İnsan gücü, kapasite geliştirme için çok önemlidir. Kapasite geliştirmenin belki en önemli kısmı insana yapılan yatırımdır. Çünkü siber güvenlik ancak insan ile var olabilir. Bu nedenle Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) bilgi güvenliği, güvenlik testi ve denetimi[264] vb. birçok eğitim vermektedir. TÜBİTAK'ın yanı sıra TSE de özellikle temel seviye güvenlik belgelendirme[265] ve dünya standartları ISO/IEC gibi eğitimler düzenlemektedir. Akademik düzeyde siber güvenlik alanında insan gücü geliştirmek adına Bahçeşehir Üniversitesi BİT hukuku ve siber güvenlik[266] lisansüstü programları

[262] ITU, 2017, S. 37
[263] ITU, 2015, s. 34.
[264] https://egitim.sge.gov.tr/ (11.11.2020)
[265] https://www.tse.org.tr/IcerikKategori?ID=869&ParentID=2289 (11.11.2020)
[266] https://bau.edu.tr/icerik/8856-fen-bilimleri-enstitusu-siber-guvenlik (12.11.2020)

örnek verilebilir. Bilinçlendirme çalışmalarında www.bilgiguvenligi.gov.tr, www.bilgimikoruyorum.org.tr web siteleri vatandaşlara yardım etmektedir. Türkiye'nin 2014 GCI beyanına göre uluslararası düzeyde dört yüz kamu uzmanına sahiptir. Acenta sertifikasyonu konusunda ISO/IEC 27001 sertifikasyonu bulunan 106 elektronik iletişim hizmet sağlayıcısı bulunmaktadır[267].

İngiltere, 2014 GCI için ulusal ve sektörel olarak resmî olarak araştırma ve geliştirme olmadığını belirtmiştir. İnsan kapasitesini artırma konusunda Getsafeonline kamuoyu ile beraber işletmelere yönelik bilinçlendirme programı[268] yürütmektedir. IISP'nin sertifikasyon programları[269] da bu amaç için mevcuttur. İngiltere sahip olduğu sertifikalı uzman sayısını belirtmeyi tercih etmemiştir. Ulusal Bilgi Güvence Teknik Kurumu (CESG) acente sertifikasyonu için görevli tek kurumdur[270]. İngiltere bu konuda Avrupa bölgesinin en iyi örneği olarak raporda yer almıştır[271].

2017 ve 2018 GCI, kapasite geliştirmek için ülkelere daha çok sorumluluk yüklemiştir. Bu kapsamda alt kategoriler çoğalmış ve mevcut kapasite geliştirme yollarına ek yollar ilave edilmiştir. 2017 ve 2018 GCI alt kategorilere bakılırsa: halkı bilinçlendirme kampanyaları, siber güvenlik profesyonel eğitim kursları, ulusal eğitim programları ve akademik müfredatlar, teşvik mekanizmaları, evde yerleşen siber güvenlik endüstrisi başlıklarının ortak olduğu görülmektedir. 2017 GCI için bu bölümde standardizasyon kuruluşları, iyi uygulamalar, profesyonel eğitim kursları ve R&D (araştırma ve geliştirme) programları[272] yer alırken, 2018 GCI için de profesyoneller için siber güvenlik standartları ile sertifikasyon ve siber güvenlik R&D programları[273] yer almaktadır.

[267] ITU, 2014, s. 276.
[268] https://www.getsafeonline.org/ (12.11.2020)
[269]Institute of Information Security Professionals, *Information Security Skills Framework Document,* 2010, s. 5.
[270] ITU, 2015, s. 491.
[271] ITU, 2015, s. 6.
[272] ITU, 2017, S. 6.
[273] ITU, 2018, S. 8.

Türkiye, kapasite geliştirme için özellikle vatandaşı *bilinçlendirme* konusunda birçok çalışma yapmıştır. Siber güvenlik[274], siber zorbalık[275], kredi kartı ve banka kartı şifre güvenliği[276] vb. birçok kritik konuda görsel-işitsel medya kullanılarak kamu spotları yayınlanmaktadır. Bunlar, siber uzayda yaşanan olumsuz durumlara karşı halkı bilinçlendirme faaliyetleridir. *Siber güvenlik profesyonel ve ulusal eğitim programları* çerçevesinde BTK Akademi siber güvenlik analisti eğitimi[277], TÜBİTAK güvenlik analizi, sistem ve ağ güvenliği, uygulama güvenliği eğitimlerini vermektedir[278]. Bahçeşehir Üniversitesine ek olarak, Gazi Üniversitesi Adli Bilişim, Bilgisayar Bilimleri gibi lisansüstü ve doktora programları[279] ile Sabancı Üniversitesi Siber Güvenlik lisansüstü programları[280] gibi birçok üniversitede *akademik müfredatlar* oluşturulmuştur. Türkiye, siber güvenlik kümelenmesini amaçlayarak yol haritasını belirleyecektir[281]. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından düzenlenmiş Siber Zekâ Bilgi Yarışması[282] ile gelecek nesilleri siber uzay ve yapay zekâ konusunda eğitmek amaçlanmıştır. *Siber güvenlik sertifikasyon* eğitimleri için BTK siber güvenliğe giriş eğitimi[283], Bilge Adam siber güvenlik[284], İstanbul Aydın Üniversitesi siber güvenlik ve siber olaylara müdahâle eğitimi[285] verilmektedir. Bu konuda Türkiye Avrupa bölgesi için en iyi örneklerden biri olmuştur[286].

İngiltere, halkın bilinçlendirilmesi için yürütülen faaliyetlerde Birleşik Krallık Siber Güvenlik Stratejisi için kamu bilinci esas almıştır[287]. Siber Güvenlik Bilim Araştırma Enstitüsü (RISCS), Ulusal Siber Güvenlik Merkezi (NCSC) ve Hewlett Packard Enterprise (HPE)'ın teknik raporuna göre kuruluşlar, siber güvenlik sürecine

[274] https://www.youtube.com/watch?v=x0jVmMmtyG4&ab_channel=elifkayademir (14.11.2020)
[275] https://www.youtube.com/watch?v=6uwEJ2XTS1g&ab_channel=TRTHaber (14.11.2020)
[276] https://www.youtube.com/watch?v=caGk0_j20Lg&ab_channel=KlanIstanbul (14.11.2020)
[277] https://www.btkakademi.gov.tr/portal/course/siber-guvenlik-analisti-egitimi-5020#!/about (15.11.2020)
[278] https://egitim.sge.gov.tr/ (15.11.2020)
[279] http://be.gazi.edu.tr/posts/view/title/doktora-programlari-16558 (15.11.2020)
[280] https://sec.sabanciuniv.edu/ (15.11.2020)
[281] https://siberkume.org.tr/Activities (16.11.2020)
[282] https://cbddo.gov.tr/haberler/4906/siber-zeka-bilgi-yarismasi (16.11.2020)
[283] https://etkinlik.btk.gov.tr/etkinlik/detay/siber_guvenlige_giris_egitimi (16.11.2020)
[284] https://www.bilgeadam.com/akademi/bilisim-uzmanligi/siber-guvenlik (16.11.2020)
[285] https://www.aydin.edu.tr/tr-tr/arastirma/arastirmamerkezleri/sem/digital-bilisim-egitimleri/Pages/Siber-G%C3%BCvenlik-ve-SOME-E%C4%9Fitimi.aspx (17.11.2020)
[286] ITU, 2018, S. 47.
[287] Goverment UK, 2011, s. 23.

çalışanlarını dâhil ederek ilerlemeleri[288] gerektiğini belirtmiştir. İlk kez Ulusal Siber Güvenlik Becerileri Stratejisi İngiltere tarafından 21 Aralık 2018[289] tarihinde yayımlanmıştır. Bu strateji, kamuyu siber güvenlik konusunda bilinçlendirmeye yönelik olarak yapılmıştır. *Eğitim faaliyetleri ve sertifikasyon* konusunda BSI tarafından Bilgi Güvenliği Yönetim Sistemi (BGYS) Çevrimiçi Eğitim Kursları ISO/IEC 27001: 2013[290], EC-Council tarafından çeşitli siber güvenlik program[291] eğitimleri verilmektedir. Tablo 3.4'te Türkiye ve İngiltere'nin 2017 GCI kapasite geliştirme durumları görülmektedir.

Tablo 3.4 2017 GCI Türkiye-İngiltere Kapasite Geliştirme Durumları[292]

	2017 GCI	
	Türkiye	Birleşik Krallık
Standardizasyon Kuruluşları		
İyi Uygulamalar		
R&D Programları		
Halkı Bilinçlendirme Kampanyaları		
Profesyonel Eğitim Kurumları		
Akademik Müfredatlar		
Teşvik Mekanizmaları		
Evde Yetiştirilen Siber Güvenlik Endüstrisi		
Kapasite Geliştirme		

İyi
Kötü
Orta

3.2.5. Uluslararası İşbirliği (Cooperation)

2014 yılı GCI devlet içi işbirliği, ajans içi iş birliği, kamu sektörü ortaklığı ve uluslararası iş birliği[293] olmak üzere dört alt başlıktan meydana gelmiştir.

[288] https://www.ncsc.gov.uk/news/awareness-only-first-step (17.11.2020)
[289] Goverment UK, *Inıtıal National Cyber Security Skills Strategy*, 2018, s. 16-19.
[290] https://www.bsigroup.com/en-GB/iso-27001-information-security/iso-27001-training-courses/ (17.11.2020)
[291] https://www.eccouncil.org/programs/ (17.11.2020)
[292] ITU, 2017, s. 37.
[293] ITU, 2015, 34-35.

Türkiye, siber güvenliğin sağlanması yönünde organizasyonlara ve *devletlerarası* ilişkilere önem vermiştir. Bu kapsamda siber güvenliğin sınır ötesi varlığını koruyabilmesi adına Arnavutluk, Bosna Hersek, Kosova, Makedonya, Karadağ, Sırbistan, Bulgaristan, Ukrayna gibi sınıra yakın ülkelerle iş birliğine gitmiştir. Aynı zamanda Türk dünyasından Azerbaycan, Kırgızistan gibi ülkelerle iş birlikleri mevcuttur. Fas, Nijerya, Sudan Cumhuriyeti, Senegal, Sırbistan, Tunus, İran, Tayland, Mısır gibi çeşitli ülkeler ile de işbirliği faaliyetleri yürütülmektedir. Bunları 2014 GCI'da bildirmiştir. Bu konuda, Türkiye ikili ilişkileri sadece devletler ile sınırlandırmayarak üyesi olduğu NATO ile siber güvenlik alanında yakın çalışmalar yürütmüştür. Bu kapsamda Siber Güvenlik Enstitüsü, NATO tarafından kurulan Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE)[294] ile yakın temas hâlindedir ve Ulusal Gönüllü Katılımcı (NVC) bulundurma faaliyetini yürütmek üzere daimi temsilci görevlendirmiştir[295]. *Ajans içi iş birlik ve kamu sektör ortaklığı* için ulusal düzeyde 2013-2014 Strateji Eylem Planı'nında, ulusal siber güvenlik alanının etkin kullanımı ile kurumlar ve özel sektör arasında işbirliğinin yapılması gerektiği ifade edilmiştir[296]. Türkiye *uluslararası anlaşmalara* dâhil olmak için 2010 yılında Avrupa Siber Suçlar Sözleşmesini imzalayarak 2014 yılında ülkesinde yürürlüğe sokmuştur[297]. *Uluslararası işbirliği* konusunda TR-CERT ile USOM faaliyetlerine başlamış, ITU tarafından 2012 yılında Bulgaristan'da gerçekleştirilen Acil Müdahâle Ekibi için Uygulamalı Öğrenme (ALERT)[298] programına katılım sağlamıştır. 2014 yılında ITU tarafından düzenlenen Uluslararası Siber Kalkan Tatbikatı (ICSE)'na[299] ev sahipliği yapmıştır. Yaptığı çalışmalar neticesinde Türkiye, Avrupa Bölgesi için en iyi örnek olmuştur[300].

[294] https://ccdcoe.org/cycon/ (18.11.2020)
[295] https://sge.bilgem.tubitak.gov.tr/tr/nato-ccdcoe-daimi-temsilciligi (18.11.2020)
[296] UDHB, 2013, s. 6.
[297] Önder Kutlu, Kahraman, Selçuk ve Dinçer, Selçuk, "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi", *ASSAM Uluslararası Hakemli Dergi,* 2019, s. 4.
[298] https://www.itu.int/net/pressoffice/press_releases/2012/83.aspx (18.11.2020)
[299] https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/International-Cyber-Shield-Exercise.aspx (19.10.2020)
[300] ITU, 2015, s. 26.

İngiltere, ikili anlaşmalarda devletlerden ziyade uluslararası organizasyonlara önem vermiştir ve ITU, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)[301], NATO ve Avrupa CERT Grup ile yapılan iş birliklerini 2014 GCI'ya belirtmiştir[302]. *Ajans içi iş birlik ve kamu sektörü ortaklığı* için Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA)[303], özel sektör ve CISP arasındaki işbirliğini yönetmekten sorumlu olan resmî kuruluştur. *Uluslararası işbirliği* konusunda BM, ITU, ENISA, NATO ve Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) ile faaliyetler yürüttüğünü belirtmiştir.

2017 ve 2018 GCI için ortak alt kategoriler çift taraflı anlaşmalar, çok taraflı anlaşmalar, uluslararası katılım, kamu özel sektör ortaklıkları, kurumlar arası ortaklıklardan oluşmaktadır. 2018 yılında bazı eklemeler yapılarak kategori başlıklarında değişiklikler olmuştur. Uluslararası katılım yerine uluslararası forumlara/derneklere katılım, kurumlar arası ortaklıklar yerine ise kurumlar arası/kurum içi ortaklıklar olarak adlandırılmıştır. Ayrıca 2017 GCI kapasite geliştirmenin alt kategorisi olan iyi uygulamalar 2018 GCI'da en iyi siber güvenlik uygulamaları başlığı ile adlandırılmıştır.

Türkiye, 2015 yılı ENISA Siber Güvenlik Ayı[304]'na katılımı *uluslararası katılıma* kategorisine örnektir. *Çift taraflı anlaşmalar* için TÜBİTAK ve Katar Ulusal Araştırma Fonu ile imzalanan Bilim ve Teknoloji Alanında İşbirliği Protokolü kapsamında 2018 yılı mart ayı sonunda iki ortak araştırma projesi duyurulmuştur[305]. 2017 yılında Kamu Bilişimcileri Derneği'nin düzenlediği Kamu Siber Güvenlik Zirvesi[306] gerçekleştirilmiştir. Bu zirvede kamu bilişim çalışanlarının bilgi paylaşımları ile beraber kamu kaynaklarının verimli kullanımı hedeflenmiştir. 2017 yılında T.C. Cumhurbaşkanlığı Savunma Sanayii Müsteşarlığı'na bağlı Türkiye Siber Güvenlik Kümelenmesinin düzenlediği 3. Uluslararası Siber Savaş ve Güvenlik

[301] ENISA, *Good Practice Guide Network Security Information Exchanges*, 2004, s. 48.
[302] ITU, 2015, s. 491.
[303] https://www.gov.im/about-the-government/departments/home-affairs/office-of-cyber-security-and-information-assurance/ (20.11.2020)
[304] ENISA, *The European Cyber Security Month 2015 Deployment Report*, 2015, s. 9.
[305] https://h2020.org.tr/tr/ikili-isbirlikleri/qa (22.11.2020)
[306] https://www.biltam.com.tr/haberler/kamu-siber-guvenlik-zirvesi2017.html (22.11.2020)

Konferansı[307] yapılmıştır. 2018 GCI'da yer alan *en iyi siber güvenlik uygulaması* konusunda 2017 SSTEK A.Ş. olarak bilinen Savunma Sanayi Teknolojilerinin yürüttüğü Savunma Sanayi Bakanlığının desteklediği Türkiye Siber Güvenlik Kümelenmesi[308] örnek olarak verilebilir.

İngiltere, 12-14 Kasım 2018 tarihleri arasında gerçekleşen elliden fazla ülkenin bulunduğu İnternet Yönetişim Forumu (IGF)[309]'na katılım sağlamıştır. Bu *çok taraflı anlaşmalar* için iyi bir örnektir. *İkili anlaşmalar* için diyalog hâlinde bulunan İngiltere ve Hindistan'ın 20 Haziran 2018 tarihinde 4. İngiltere-Hindistan Siber Diyaloğu[310] gerçekleştirilmiştir. *Kamu ve özel sektör işbirliği* kapsamında 2016 Siber Güvenlik Stratejisi[311] hükümetin yol haritasını belirlemektedir ve bu dijitalleşme yolunda atılan kritik bir adımdır. Ülke içindeki işbirliği ve bilgi paylaşımı esas alınmıştır. *En iyi uygulama* için NCSC tarafından 2016 yılında siber güvenliğe yönelik 10 adım[312] siber dünyadaki değişimlere uyum sağlamak adına güncelleştirilmesi, 2016 yılında ICO tarafından BT Güvenliği için Pratik Bir Kılavuz[313]'un yayımlanması ve siber saldırılara karşı Cyber Essentials Scheme programı tarafından güvenlik duvarının en son sürümünün geliştirilmesi örnek olarak verilebilir. 2017 GCI için İngiltere uluslararası işbirliği başlığı altındaki kamu-özel işbirliği kategorisinde yürüttüğü faaliyetler ile örnek olarak gösterilmiştir[314]. Tablo 3.5'te iki ülkenin işbirliği durumları görülmektedir.

[307] https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1068&LangID=1 (23.11.2020)
[308] Tamyapar, Berkay, "Siber güvenlik ve Türkiye'de Yürütülen Siber Güvenlik Çalışmaları", 2019, s. 12, s. 1-16.
[309] https://en.unesco.org/news/internet-governance-forum-be-held-unesco (23.11.2020)
[310] https://www.gov.uk/government/news/the-4th-uk-india-cyber-dialogue (23.11.2020)
[311] Carr, Madeline, "Public–private partnerships in national cyber-security strategies", *International Affairs*, S: 92, No: 1, 2016, s. 45.
[312] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security (24.11.2020)
[313] ICO, *A practical guide to IT security*, 2016, s. 1,9.
[314] ITU, 201, s. 45.

Tablo 3.5 2017 GCI Türkiye-İngiltere İşbirliği Durumları[315]

	2017 GCI	
	Türkiye	Birleşik Krallık
Çift Taraflı Anlaşmalar		
Çok Taraflı Anlaşmalar		
Uluslararası Katılım		
Kamu Özel Sektör Ortaklıkları		
Kurumlar Arası Ortaklıklar		
İş Birliği		

İyi
Kötü
Orta

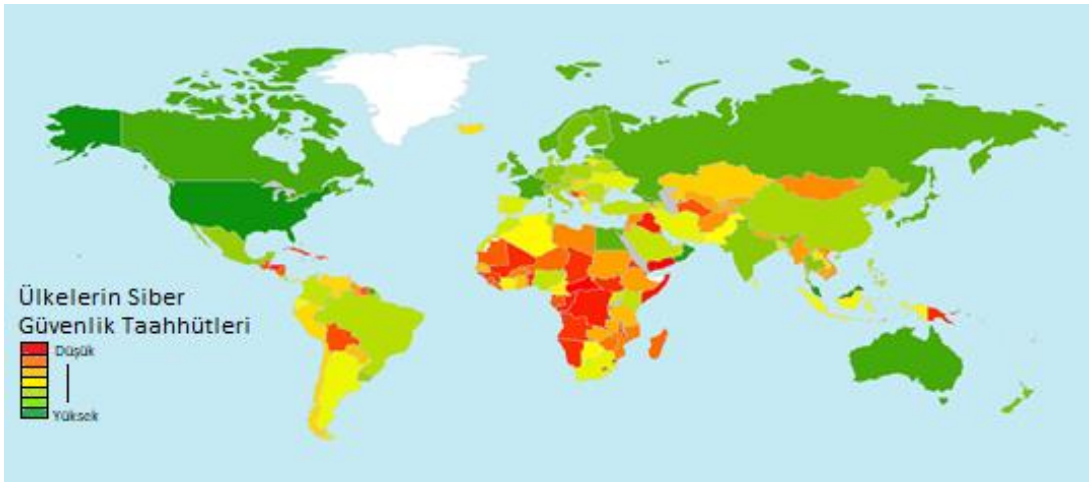
Tüm bu belirtilen başlıklar ve alt kategorileri doğrultusunda 2014, 2017 ve 2018 yıllarına ait GCI için dünya sıralamasında Türkiye ve İngiltere'nin durumu Tablo 3.6'da görülmektedir. 2014 yılı için yakın sıralamalarda yer alan iki ülke 2017 yılında sıralamaları değişmiştir ve siber güvenlik konusundaki dünya sıralamalarında iki ülke için düşüş yaşanmıştır. 2018 yılı GCI için her iki ülkenin de bulundukları konumu topladıkları ve kendilerini geliştirdikleri görülmektedir. Hatta İngiltere siber güvenlik alanında bu endeks bazında dünya lideri olmuştur.

Tablo 3.6 GCI Dünya Sıralamasına göre Türkiye ve İngiltere

Global Cyber Security Index	**2014**	**2017**	**2018**
Türkiye	7	43	20
Birleşik Krallık	5	12	1

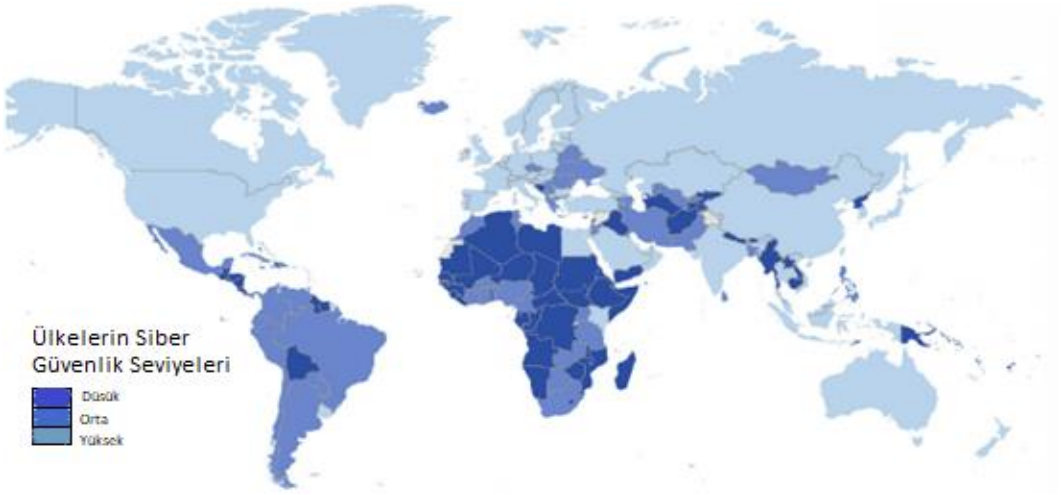
2017 ve 2018 yılları için ülke taahhütleri mevcuttur ve Şekil 3.5'te 2017 GCI için 193 üye ülkenin siber güvenlik taahhütleri görülmektedir. Yeşil en yüksek kırmızı ise en düşük taahhüt anlamına gelmektedir. İngiltere'nin taahhüdü Türkiye'ye göre daha yüksektir.

[315] A.g.r., s. 37.



Şekil 3.5 Küresel Ölçekte Ülkelerin Siber Güvenlik Taahhütleri[316]

2018 GCI için yüksek, orta ve düşük etkili taahhüt seviyeleri Şekil 3.6'da görülmektedir. Türkiye ve İngiltere siber güvenlik konusunda ülkelerine kazandırdıkları faaliyetler doğrultusunda yüksek seviye kategorisinde yer almışlardır[317].



Şekil 3.6 Küresel Ölçekte Ülkelerin Siber Güvenlik Taahhütleri Isı Haritası[318]

[316] ITU, 2017, s 13.
[317] ITU, 2018, s. 14.
[318] A.g.r., s. 13.

3.3. DİJİTAL DÖNÜŞÜM OFİSİ VE BİLGİ GÜVENLİĞİ DERNEĞİ'NİN YÜRÜTTÜĞÜ SİBER GÜVENLİK FAALİYETLERİ

ITU'nun siber güvenlik endeksleri incelendiğinde Türkiye'nin siber güvenlik politika ve yönetişim modellemesi hususunda Dijital Dönüşüm Ofisi ve Bilgi Güvenliği Derneği'nin yaptığı çalışmalar bu süreçlere de katkı sağlamıştır. Çalışmanın bu kısmında Dijital Dönüşüm Ofisi başta olmak üzere BGD'nin siber güvenlik alanında yaptığı çalışmalar incelenecektir.

Dijital Dönüşüm Ofisi; *Siber Kümelenme, HackZeugma, KamuNET, 81 İlde 81 Siber Kahraman ve HackIstanbul* gibi Türkiye siber güvenlik alanında kurumsal yapılanma, teknik çerçeve ve özellikle kapasite geliştirme konularına katkı sağlayan projeleri hayata geçirmiştir. Ulusal ve uluslararası yürütülen çalışmalar uluslararası iş birliği konusuna uzun soluklu yenilikler getirmektedir. Bu projeler;

- *Siber Kümelenme:* Bu proje, 2017 yılında başlamış olup teknoloji üreterek siber güvenlik alanında dünya rekabetinde lider olma yolunda emin adımlarla ilerlemeyi hedeflemektedir. Bu projenin temel hedefi, siber güvenlik için bir ekosistem oluşturmak ve yerli/millî siber güvenlik yazılım ve donanım ekipmanları geliştirmektir. Bu amaç özellikle kurumsal yapılanma ve teknik çerçeveye katkı sağlamaktadır.
- *HackZeugma:* 2020 Teknofest yarışmasında Operasyonel Teknolojiler kapsamında düzenlenmiştir. Temel amacı; Operasyonel Teknolojiler başta olmak üzere özellikle siber güvenlik alanına yeni yetenekler kazandırarak kapasite geliştirme konusuna yardımcı olmaktır.
- *KamuNET:* RTÜK'ün de faydalandığı hizmetlerden biri olan bu proje temelde kamu kurumları arasındaki veri iletişiminin kapalı ve güvenli bir ağ üzerinden yapılmasını sağlar. Burada temel amaç; siber uzayda var olan tehlike ve risk yaklaşımlarından uzak kalarak kamu hizmetlerinin güvenli bir biçimde sürekliliğini sağlamaktır. KamuNET kurumsal yapılanma adına önemli adımlardan biridir.

- *81 İlde 81 Siber Kahraman:* Siber güvenliğin olmazsa olmazı olan siber uzman yetiştirilmesi için gençlere eğitim imkânı sunulmaktadır. BU eğitim kapsamında ağ güvenliği, sistem güvenliği ve web güvenliği gibi temel siber güvenlik eğitiminin yanı sıra siber saldırılara yönelik saldırı teknikleri ve uygulamalı hacking simülasyon eğitimleri de verilmektedir.
- *HackIstanbul:* Uluslararası hackerları bir araya getirmek suretiyle bu hackerlara yeteneklerini gösterme imkânı sunan bir yarışmadır. Bu yarışmanın temel amacı; dünya çapında gerçekleşen siber saldırıların yöntemini anlamak ve saldırıların nasıl gerçekleştiği konusunda farkındalık sağlamaktır[319]. Bahsedilen bu son iki proje ise özellikle kapasite geliştirme konusuna katkı sağlamaktadır.

Bilgi Güvenliği Derneği; 22.07.2007 tarihinde, bilgi güvenliği alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, millî teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak amacı ile kurulmuştur. BGD'nin vizyonu da "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmak" şeklinde belirlenmiştir[320]. BGD'nin projeleri:

- *ISCTurkey;* ilk olarak 2006 yılında Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı olarak yürütülen bir faaliyet olmuştur. Bu konferans için siber güvenlik alanında belirlenen çeşitli konu başlıkları yer almaktadır. 13. ve en sonuncusu olan *ISCTurkey 2020* Konferansı'nın konu başlığı "*Siber Güvenlik ve Güvenli Veri Paylaşımı*" olmuştur. Bu konu, siber güvenlik alanında yaşanan güncel gelişmeler hususunda şekillendirilmiştir. Siber saldırıların değişimi ve karmaşası karşısında verinin güvenli bir şekilde nasıl

[319] https://cbddo.gov.tr/projeler/hack-istanbul/ (07.07.2021)
[320] https://www.cybermagonline.com/ (09.07.2021)

paylaşılacağı konusunda çalışmalar paylaşılmıştır. Çalışma sonunda yapılması gerekenler için sonuç bildirisi yayınlanmıştır[321].

- *Siber Güvenlik Çalıştayı:* 2011 yılında gerçekleşen bu çalıştay Aselsan, BTK ve BGD'nin ortak çalışması hâlinde gerçekleştirilmiştir. Çalıştay sonunda 25 maddeden oluşan bir bildiri yayınlanmıştır. Çalıştay kapsamında siber güvenlik felsefesi, güncel siber güvenlik istihbaratı başta olmak üzere ülke güvenliği için olmazsa olmaz olan *kritik altyapılara yönelik siber tehditler ve Türkiye için öneriler* gibi özgün konu başlıkları yer almıştır[322]. Bu çalıştayın amacı; Türkiye'nin siber güvenliğine yönelik özellikle ulusal ve uluslararası olarak ne yapması gerektiği ve karşılaşılan sorunlar için ne tür çözüm yolları bulması gerektiğini açıkça ifade etmektir.
- *Siber Güvenlik Hukuk Çalıştayı:* Bu çalıştay, T.C UAB, Türkiye Barolar Birliği ve BGD'nin iş birliği ile gerçekleştirilmiştir. Geniş katılımcı kitlesine sahip çalıştayda özellikle siber güvenlik kavramının hukuksal boyutları ele alınmıştır. Siber saldırıların zaman ve mekândan bağımsız olarak anonim gerçekleşmesi sonucunda yaptırımlar konusunda hazırlanan 5237 sayılı TCK, 5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*" ve 5070 sayılı "*Elektronik İmza Kanunu*"[323] hakkındaki düzenlemelerin günümüz ihtiyaçlarına göre tekrar gözden geçirilmesi gerektiği ifade edilmiştir. Bu çalıştayın temel amacı, siber saldırılara karşı oluşturulacak siber caydırıcılık hakkında ITU'nun ana kriterinden biri olan yasal düzenlemeler hakkında çözüm önerileri sunmaktır.
- *Veri Merkezi Çalıştayı:* Bu çalıştay 2013 yılında gerçekleştirilmiştir. Çalıştay, artan siber uzay kapasitesi ile beraber oluşan veri kümeleri ve bunların nasıl yönetileceği konusunda veri merkezlerine çözüm önerileri sunmaktadır. Bu konuda BGD ve Türk Telekom'un iş birliği ile gerçekleşmiştir[324].

---

[321] https://www.iscturkey.org/bildiriler/2020/iscturkey_2020_sonuc_bildirgesi.pdf (07.07.2021)

[322] https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/siber2011-SonucBildirgesi.pdf (08.07.2021)

[323] https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/hukuk-2012-SonucBildirgesi.pdf (08.07.2021)

[324] https://www.bilgiguvenligi.org.tr/faaliyetler/etkinlikler/2013-2/veri-merkezi-calistayi-2013/ (08.07.2021)

- *Siber Güvenlik Uzmanı Yetiştirme Eğitim Kampı ve Mobil Dünya'da Çocuk ve Gençlerin Güvenliği:* 2015 yılında gerçekleşen bu iki etkinlik siber uzay konusunda gençleri bilinçlendirme için yapılmıştır. Bu etkinlikler hem geleceğin siber güvenlik uzmanlarını yetiştirmeyi hem de gençleri siber dünya ile yakınlaştırarak teknolojiyi güvenli bir biçimde kullanmaları adına yardımcı olmuştur[325]. Çocukların ve gençlerin çevrimiçi maruz kaldıkları siber zorbalık konusunda bilinçlendirme ve "*çocukların çevrimiçi korunması*" konusunda Türkiye için yapılan önemli etkinliklerdendir.
- *CyberMag:* Siber güvenlik alanında Türkiye'deki ilk dergidir. Ulusal ve uluslararası olaylara yön veren dergi konu ve içerik konusundan siber güvenlik alanında birçok öncü ismi bir araya getirmektedir. Siber güvenlik hakkında tüm gelişme ve önerilerin bulunacağı makale, haber ve gündem başlıkları yer almaktadır. Değişen siber güvenlik ihtiyaçlarına yön vererek farkındalığı arttırmak ve siber güvenlik gündemini güncel tutmak derginin temel amaçları arasında yer almaktadır[326]. Derginin yanı sıra birçok yayın faaliyeti ile de BGD siber güvenlik alanına katkı sağlamaktadır. Bu yayınlar; *Siber Güvenlik ve Savunma* başlığı adı altında dörtlü kitap serisi yayınlanmıştır. Bu kitaplar birbirinin devamı niteliğindedir[327].

DDO ve BGD de Türkiye'nin gerek ulusal gerek uluslararası yönetişim modeline yön vermek adına ciddi çalışmalar yürütmüştür ve yürütmeye devam etmektedir. ITU'nun temel güvenlik kriterlerinin esas alarak yürütülen tüm bu faaliyetler; gerekli uzman insanı yetiştirerek kapasite geliştirmeyi ve topyekûn bilinçlendirme oluşturmayı amaçlamaktadır. Ayrıca yerli ve millî teknoloji hamleleri ile teknik çerçevedeki mevcut durumda ilerlemeyi hedeflemektedir. Siber güvenliğin etkisini arttırmak için yasallardaki mevcut durum analiz edilerek ilerleyen dönemlerde ortaya çıkabilecek muhtemel yasal boşluklar için önerilerde de bulunulmaktadır.

[325] https://www.bilgiguvenligi.org.tr/faaliyetler/etkinlikler/2015-2/ 08.07.2021)
[326] https://www.cybermagonline.com/ (09.07.2021)
[327] https://www.bilgiguvenligi.org.tr/kitaplar/ (09.07.2021)

SONUÇ VE ÖNERİLER

Teknolojinin ortaya çıkışı ve ilerlemesi hızlı bir biçimde gerçekleşmiştir. Bu konuda devrim niteliğinde olan internetin bulunması ve internet kullanımının yaygınlaşması dört boyut ile sınırlı olan insanlık tarihini beşinci boyuta taşımıştır. Bu boyut sanal ile gerçeklik arasında köprü kurarak insanlığın somut ve soyut kavramlar arasında bir geçit olarak kullanmıştır. Bu geçitte var olan insan sayısı gün geçtikçe artmaktadır.

İnternetin ilk ortaya çıkışı, askeri hizmetlerin yürütülmesi için düşünülse bile daha sonrasında tüm hizmet sektörleri için internet kullanımı yaygınlaşmıştır. İnternet ve beraberinde getirdiği teknoloji, insanlara mobilite ve çevrimiçi alışkanlıkları için yeni bir soluk getirmiştir. İnternet ve internete bağlı cihazların artışı ile birlikte eğitim, sağlık, hizmet, finans ve bankacılık gibi birçok alanda insan davranışları değişim göstermiştir. Bu yaygınlık, internete bağlanabilen cihazların sadece bilgisayarlarla sınırlandırılamayacağını ve bu konuda teknolojinin nasıl geliştirilebileceği konusunda düşünülmesini sağlamıştır. Bu düşünceler, mühendisler tarafından üretime dönüştürülmüş ve telefon, tablet gibi birçok cihazın da internet dünyasında yer alması gerektiği anlaşılmıştır. İnternete bağlı cihaz sayısındaki artış, internet kullanımını yaygın hâle getirerek interneti erişebilir kılmıştır. İlerleyen süreçte internete bağlanan yeni cihazlar teknoloji ile şekillenerek *Nesnelerin İnterneti* kavramını ortaya çıkartmış ve bu internet için devrim niteliğinde olmuştur. Televizyondan bulaşık makinesine hatta buzdolabına kadar birçok teknolojik ürün internetle tanışmış ve internete bağlı cihaz sayısında ciddi bir artış yaşanmıştır. 2018-2023 yıllarını kapsayan Cisco'nun *Yıllık İnternet* raporunda 2023 yılına kadar dünya nüfusunun yaklaşık 2/3'nün internet erişimine sahip olacağı ve internete bağlanacak cihaz sayısının 2023 yılı dünya nüfusunun üç katı [328] olacağı öngörülmektedir. Bu da beş yıl içinde internete bağlı olan cihaz sayısının iki katına çıkacağının göstergesidir. Elbette bu cihaz artışı internet

[328] Cisco, *Cisco Annual Internet Report (2018-2023)*, 2020, s. 1.

kontrolü ve güvenlik problemlerini de beraberinde getirmiştir. Bu artış, aynı zamanda bilişim sistemlerinin yönetimini zorlaştırmıştır.

İnsan, internete bağlı cihazları ve bu cihazların oluşturduğu sistemleri internet kullanımında yaşanan artış sonucunda yönetmekte zorlanmıştır. Bu durum genişleyerek küresel dünyanın sorunu hâline gelmiştir. Bu uluslararası mesele için BM, AB, NATO, ITU gibi birçok uluslararası kurum ve kuruluş çeşitli çözümler üretmek ve uluslararası işbirliği konusunda çalışmalar yürütmektedir. İnternet ve bağlı cihazların oluşturduğu bu ortam *siber uzay* olarak adlandırılarak sınırları belirlenmek istenmiştir. Sınırın belirlenmek istenmesindeki temel amaç, siber uzayın kavram ve kapsamının karmaşık bir içeriğe sahip olmasıdır.

Siber uzay ve kapsam alanının belirlenmesi ile beraber siber uzay ve siber uzayda oluşturulan faaliyetlerin neler olduğu anlaşılmak istenmiştir. Bireylerin, kurumların ve ülkelerin siber uzayda başına gelen kötü olaylar ile beraber siber uzay ortamında neler yaşandığı konusu merak uyandırmıştır. Çünkü siber olayda gerçekleşen saldırıların kim tarafından, nereden, nasıl ve ne şekilde geleceği belirsizdir. Siber uzayın küreselliği, siber saldırıların anonimliği ve siber uzaydaki hayatın zamandan bağımsız olarak hareket etmesi ciddi riskler meydana getirmiştir. Saldırıyı yapan taraf bazen belirsiz bazen de suç, olaylardan habersiz masum kurbanın üzerine atılarak gerçekleştirilmektedir. Yani saldırganın belirlenmesi, manipülasyona açık bir durumdur. Siber saldırıların diğer bir sorunu da zamandan bağımsız olarak her an gerçekleşebilmesidir. Kısacası, bu saldırılarla ancak uluslararası işbirliği yapılarak mücadele edilebileceği anlaşılmıştır.

İyi bir iş birliği ve uluslararası farkındalık temel esas alınarak siber güvenliğin sağlanması için ITU tarafından beş temel kriter belirlenmiştir. Yasal düzenleme, kurumsal yapılanma, teknik çerçeve, kapasite geliştirme ve uluslararası iş birliğinden oluşan bu kriterler alt başlıkları ile zenginleştirilmiş ve etkili bir siber güvenliğin nasıl yapılacağı konusunda ülkelere rehberlik etmiştir. ITU'nun 2014, 2017 ve 2018 yılı

siber güvenlik endeksi raporuna göre Türkiye ve İngiltere için ortaya çıkan sonuçlar aşağıda maddelenmiştir.

- 2014 yılı GCI için dünya genelinde Türkiye 475 puan, İngiltere 490[329] puan almıştır. Türkiye'nin indeksi 0,647 iken İngiltere'nin 0,706[330] olmuştur. Dünya sıralamasında Türkiye 7. olurken İngiltere 5. sırada yer almıştır. Kendi bölgeleri olan Avrupa Bölgesinde ise Türkiye 4. sırada yer almış ve bölgesel indeksi 0,6471 iken İngiltere 2. sırada yer almış ve bölgesel endeksi 0,7059 [331] olmuştur.
- 2014 yılı GCI için Avrupa bölgesi sıralamasında beş kategori içerisinde yaptığı çalışmalarla uluslararası işbirliği başlığında en iyi uygulamayı Türkiye sergilemiştir. İngiltere yaptığı çalışmalarla kapasite geliştirme konusunda bölgesinin bu alanında en iyi örneği[332] olmuştur.
- 2017 GCI için Türkiye 0.581 puan almış ve küresel ölçekte 43. sıraya yerleşmiştir. İngiltere ise yaptığı çalışmalar sonucu 0,783 puan alarak 12. sıraya yerleşmiştir.
- 2017 GCI'a bölgesel olarak bakıldığında Türkiye Avrupa bölgesinde 22. sırada yer bulurken İngiltere 4. sırada yer almıştır[333].
- 2017 GCI raporunda yer alan dünya ülkeleri başlangıç, gelişen ve lider konumuna sahip olarak üç kategoriye ayrılmıştır. Yaptıkları siber güvenlik çalışmalarına göre üç durumdan birine ait olma ilkesi benimsenen raporda bu doğrultuda Türkiye gelişen kategorisinde yer alırken İngiltere lider kategorisinde kendine yer bulmuştur[334].
- 2018 yılı GCI raporuna göre 0,931 puanla İngiltere 1. olurken Türkiye 0.853 puanla küresel ölçekte 20. sırada yer almıştır. Bölgesel olarak İngiltere yine 1. sırada yer alırken Türkiye 11. sırada yer almıştır[335]. 2017 GCI raporundaki

[329] ITU, 2014, s. 43.
[330] A.g.r., s. 2.
[331] A.g.r., s. 14.
[332] A.g.r., s. 26.
[333] ITU, 2017, s. 56-57.
[334] ITU, 2017, s. 15.
[335] ITU, 2018, s. 60.

düşüşten sonra 2018 sıralaması iki ülke için de siber güvenlik alanına tekrar yoğunlaştıklarının göstergesidir.

2014, 2017 ve 2018 yılları için oluşturulan raporlarda Türkiye özellikle *uluslararası işbirliği* konusunda gerek ikili ilişkiler gerekse uluslararası kuruluşlara üye olmak, yapılan organizasyonlara katılmak ve bu organizasyonlara ev sahipliği yapmak gibi önemli görevleri üstlenmiştir. *Kurumsal yapılanma* için 2013-2014 eylem planındaki eksiklerin giderilmesi için 2016-2019 Eylem Planı hazırlanıp yürürlüğe konmuştur. 2016-2019 Eylem Planı'ndaki boşluklar için de 2020-2023 Eylem Planı hayata geçirilmiştir. *Kapasite geliştirme* konusunda, siber güvenlik eğitimleri konusunda yetersiz kalan Türkiye bu açığı BTK başta olmak üzere birçok kurum ve kuruluşun desteği alınarak düzenlenen eğitim, seminer ve konferanslarla kapatmak için adımlar atmıştır. *Yasal düzenlemeler* konusunda Ceza Kanununa yapılan eklemeler ve yeni çıkan yasalar umut verici olmakla beraber daha çok yasal düzenleme yapılması gereklidir. *Teknik çerçeve* hususunda uluslararası belirlenen CERT modellemesi ışığında USOM ve SOME'ler görev yapmaktadır.

Bu üç rapor için İngiltere'nin de Türkiye gibi avantaj ve dezavantajları mevcuttur. Türkiye *uluslararası iş birliği* ve ortaklığa eğilim gösterirken İngiltere siber saldırı geçmişinin başlarında *yasal düzenlemeleri* ve siber uzayda gerçekleşen yasadışı faaliyetleri suç olarak kabul edip yaptırım ön görmesi konusunda çalışmalar yürütmüştür. Tıpkı Türkiye gibi İngiltere de *kurumsal yapılanma* konusunda eylem planları ortaya koymuş ve bu konuda sorumlu resmî bir kurum belirlemiştir. *Kapasite geliştirme* konusunda iyi örnekler sergileyerek en iyi uygulamaları sergileme konusunda birinci olmuştur. İngiltere, *teknik çerçeve* için CERT modeline Türkiye'ye göre daha geç dâhil olsa da yaptığı çalışmalarla ilerlemeler kaydetmiştir.

2014 yılında kendi bölgeleri ve uluslararası sıralamada iyi olan bu iki ülkenin 2017 yılında yapılan çalışmalardaki yetersizlikleri siber güvenlik stratejilerine yansımış ve düşüş yaşanmıştır. Bu düşüşten ders çıkartarak 2018 yılında iki ülke de

iyi bir siber yönetişim haritası belirleyerek uluslararası siber güvenlik endekslerini üst sıralara taşımayı başarmışlardır. Bu raporlarda İngiltere *yasal düzenlemeler* konusunda önde olurken Türkiye *uluslararası işbirliği* konusunda önde olmayı benimsemiştir. *Teknik çerçeve* konusunda iki ülkenin de benzer eğilimler gösterdikleri ve belirlenen uluslararası CERT modelini kabul ederek ülkelerine uyarladıkları görülmektedir. Gerek siber saldırılar gerek siber saldırı türlerine maruz kalmak konusunda iki ülkenin de küresel düzeyde dünya sıralamasında üst sırada yer aldıkları istatistiksel verilerle ortaya konmuştur. Bu nedenle bu iki ülke, doğru bir güvenlik ve savunma mekanizmasına yönelmesi gerektiği bilincinde davranışlar sergilemiştir.

İyi bir siber güvenlik için CIA modeline uymak çok önemlidir. İngiltere ve Türkiye'nin mobilite, internet ve sosyal medya kullanımı oldukça yüksektir. Güvenlik halkasının en zayıf faktörünün insan olduğu düşünülürse iki ülkede güvenlik zafiyetlerine karşı vatandaşlarını bilinçlendirme konusunda iyi bir güvenlik stratejisini hayata geçirmeleri gerekir. Türkiye'nin İngiltere'ye göre üç güvenlik endeksi içinde sıralama olarak daha aşağıda yer alma nedenlerinden biri eğitim ve farkındalık konusunda yaptığı çalışmaların daha az olmasıdır.

Öneriler

ITU tarafından belirlenen başlıklar ve alt başlıklarından oluşturulmuş anket sorularının ülkeler tarafından cevaplanması ile ülkelerin puanlandırılıp sıralamada yer alması doğru ama tek başına yeterli bir süreç değildir. Anketin gönderilerek doldurulması bazen ülkelerin itibar kazanma kaygısıyla yapmadıkları uygulamaları yapmış gibi göstererek fazla puan alarak üst sıralara yerleşmelerini sağlarken bazen de güçlü siber güvenlik politikasına sahip ülkelerin rakip ülkelere bu politikalarını belirtmek istememesinden dolayı yaptıkları uygulamaları kasıtlı olarak gizli tutup düşük puan almaları ile sonuçlanabilir. Bu indeks tek başına yeterli ve sağlıklı bir ölçüt değildir ve ülkeler için bu konuda tek rehberlik kaynağı olmayabilir. Siber güvenlik ve ülkelerin doğru sıralamada yer alabilmesi için yeni kriterler ve uygulama yöntemleri geliştirilmelidir.

Yasal düzenlemeler

Türkiye yasal düzenlemeler konusunda özellikle bilişim sistemi içerisinde yürütülen yasa dışı faaliyetler için TCK'da yaptırımlar ön görse bile bunlar siber saldırganlar için caydırıcı değildir. Yasal düzenlemelerde boşluklar mevcuttur, bunlar gelişen ve değişen siber suçlara göre düzenlenmelidir. Bu düzenlemeler yapılırken siber güvenlik endeksi yüksek olan ülkeler örnek alınarak yasalar iyileştirilebilir.

Kurumsal Yapılanma

Türkiye gerek eylem planları gerek siber güvenlik için sorumlu bir kuruma sahip olsa bile stratejik eylem planlarının sürekliliği esas alınmıştır. Bu konuda yapılan eylem planlarının gelişimi ve değişimi takdir edicidir. Bu eylem planları temellerini 2013-2014 Eylem Planı'ndan alarak kendisini tekrara düşmeden eksiklerini görerek kendisinden önce gelen eylem planları için tamamlayıcı, kendisinden sonra gelenler için ise yol gösterici nitelik taşımalıdır. Bu hususta Türkiye için KamuNET Projesinin uygulanması hızlandırılmalıdır. KamuNET ile kamu kurumlarının aralarındaki haberleşme gizliliği sağlanmıştır. Ayrıca devam eden ve kamuda ortak veri kavramını ortaya koyan Kamu Entegre Veri Merkezi Projesi[336]'nin tamamlanması hâlinde Türkiye'deki kamu kurumlarının siber güvenlik yapıları kökten değişecektir. Bu proje sayesinde kamu kurumlarının ayrı ayrı yaptığı siber güvenlik yatırımları tek çatı altında toplanarak güçlü bir siber güvenlik merkezi oluşturulması hedeflenmiştir. Bu projenin, ITU'nun kurumsal yapılanma modeline uyum göstereceği düşünülmektedir. Bu nedenlerden ötürü bahsedilen proje biran önce hayata geçirilip RTÜK'ün de bu projeden faydalanması kurum veri güvenliği adına olumlu bir adım olacaktır. Kurumsal yapılanmanın güvenliğini tehdit eden siber saldırı ve siber tehditlere karşı hazır durumda olmak için yapılan siber tatbikatlara ek olarak siber tehdit analizleri yapılmalı ve olabilecek siber saldırıların önceden öngörülerek önünün kesilmesi amaçlanmalıdır. Tatbikatlar sadece ulusal saldırı faaliyetleri ile değil uluslararası

[336] https://hgm.uab.gov.tr/kamu-entegre-veri-merkezi-projesi (06.07.2021)

faaliyetlerle de yürütülmelidir. Türkiye'nin böyle girişimleri mevcuttur ancak sayısı arttırılmalıdır.

Teknik Çerçeve

İyi bir siber güvenlik için iyi bir siber savunma ve oluşan teknik olayları analiz etmek için uzman bilgisi ile doğru yorumlamak önemlidir. Bu gelişim ancak nitelikli insan gücü ile beraber yerli ve millî güvenlik ürünleri ile mümkündür. Türkiye bu konuda kendisini geliştirmeli ve özellikle yerli ve millî yazılım ve donanımlara sahip siber güvenlik ürünleri konusunda dünyaca üretim yapan lider ülkelerin üretim stratejilerini incelemeli ve kendine önemli bir yol haritası belirleyerek üretim yapacak uzman kişiler yetiştirmelidir. Ayrıca teknik çerçevede yer alan CERT modellemesini Türkiye oldukça başarılı bir şekilde uygulamaktadır. Bu nedenle RTÜK'ün, Türkiye'nin ulusal siber güvenlik yapılanması olan USOM ile uyumlu çalışması gerekmektedir. Çünkü USOM gerçekleşebilecek siber saldırıları önceden kurumlardaki SOME'lere haber vererek bu saldırılardan kurumları korumaktadır.

Kapasite Geliştirme

Ülkenin siber güvenlik kapasitesinin gelişmesi ve küresel siber güvenlik endeksinin artması ancak sahip olduğu insan topluluğundaki farkındalık düzeyinin artması ile mümkündür. Tüm siber saldırılar güvenlik çemberinin en zayıf halkası olan insan üzerine kurgulanır. Ancak bilinçli bireyler ile beraber güçlü bir ülke savunmasından söz edilebilir. Bu nedenle özellikle Türkiye için farkındalık, eğitim ve siber güvenlik konusunda müfredat çalışmalarına ağırlık verilmelidir. Türkiye siber güvenlik eğitimi konusunda lisans, yüksek lisans ve doktora seviyesinde öğrenci yetiştirilmesine ağırlık vermelidir. Kodlama, ulusal etik hacker yetiştirilmesi, siber güvenlik için yazılım geliştirme gibi birçok siber güvenlik eğitimi çocuklara erken yaşta verilmeli ve bu konuda uzman kişiler yetiştirilmelidir. Gençlerin ve çocukların

fiziksel ve ruhsal sağlıklarının korunması için yaşayacakları istem dışı siber zorbalık, çocuk pornografisi gibi olumsuz durumlardan uzak tutulması adına Türkiye için RTÜK gibi düzenleyici ve denetleyici kurumlar, Bilgi Güvenliği Derneği gibi STK'lar ile iş birliği yaparak topyekûn bilinçlendirme kampanyası yürütebilir aynı zamanda çeşitli eğitim, seminer ve konferanslar verebilir. Yapılan bu çalışmalar gençler ve çocukların bilinç düzeyini arttırarak siber uzayda karşılaşacakları olumsuz durumlara karşı onları korur.

Uluslararası İşbirliği

Siber güvenliğin zaman ve mekândan bağımsızlığı ile beraber suçu işleyenin anonimliği uluslararası işbirliğinin önemini artırmaktadır. Siber güvenlik konusunda işbirliği hem ülke diyalogları hem de uluslararası kuruluşlara katılım ile beraber bir anlam kazanmaktadır. Bu konuda Türkiye ikili ilişkiler ile beraber uluslararası alanda bu konuya önem vermektedir. Bu verilen önem sonucunda uluslararası oluşturulan organizasyonlara temsilci göndererek aktif görev almalıdır. Özellikle ITU'nun HLEG oluşumunda Türkiye adına görevlendirilmiş bir uzman mevcut değildir. Bu da siber güvenlik konusunda belirlenen güvenlik stratejileri ve planları için söz sahibi olma yetkinliğini kısıtlar. NATO tarafından kurulan Müşterek Siber Savunma Mükemmeliyet Merkezine ulusal daimi temsilci görevlendirmesi gibi HLEG için de ulusal siber güvenlik uzmanı görevlendirilmelidir. İkili ve uluslararası ilişkilerde iyi olan Türkiye bu ilişkilere ek olarak yeni siber güvenlik ilişkileri kurmalı ve bunları yapılan ortak çalışmalarla geliştirerek siber güvenlik konusunda iş birliğini arttırmalıdır.

KAYNAKÇA

Ada, Mehmet (2018), *NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi*, Gazi Üniversitesi Bilişim Enstitüsü, Yüksek Lisans Tezi, Ankara.

Adır, Arif Emre (2019), "Kurumlar İçin Siber Güvenlik Laboratuvarı Altyapısının Oluşturulması", Yüksek Lisans Tezi, Konya.

Akbulut, Berrin (1999), *Türk Ceza Hukuku'nda Bilişim Suçları,* Yayınlanmamış Doktora Tezi, Konya.

Akkuş, Bülent (2016), "Yeni Dünyanın Babil Kulesi (?): Özne-Bilgi-İktidar İlişkisi Bağlamında Siber Uzay ve Özgür Bilgi Sorunsalı Üzerine", *Ankara Üniversitesi SBF Dergisi,* Cilt: 71, No: 4, s. 1147-1170.

Alıcı, Münevver (2019), "Siber Uzayda Sosyal Medya ve Gözetim: Facebook Örneği", *Cyberpolitik Journal*, Sayı: 4, No: 8, s. 183-202.

Aliusta, Cahit ve Benzer, Recep (2018), "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dâhil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* S: 4, No:2, s. 35-42.

Alkan, Mustafa (2012), "Siber Güvenlik ve Siber Savaşlar Sunumu" , Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu.

Altay, C. Müjdat (2015), "Netaş Siber Güvenlik Sunumu", Netaş Siber Güvenlik Basın Buluşması.

Anley, Chris (2002), "Advanced SQL injection in SQL server applications", *An NGSSoftware Insight Security Research (NISR) Publication*, s. 1-25.

Arslan, Mehmet Emin (2016), "Siber Güvenlik ve Siber Saldırı Türleri".

Artuk, Mehmet Emin, Gökcen, Ahmet ve Yenidünya, Caner (2011), *Ceza Hukuku Özel Hükümler*, Turhan Kitapevi, 11. Baskı, Ankara.

Aslay, Fulya (2017), “Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi”, *Internetional Journal of Multidisciplinary Studies and Innovative Technologies*, S: 1, No: 1, s. 24-28.

Atasever, Süreyya, Özçelik, İlker ve Sağıroğlu, Şeref (2019), “Siber Terör ve DDoS”, *Journal of Natural and Applied Sciences*, S: 23, No: 1, s. 227-233.

Atıcı, Bünyamin, Gümüş, Çetin (2003), “Sanal Ortamda Gerçek Tehditler: Siber Terör”, *Polis Dergisi*, S: 37, s. 57-66.

Aydın, Ömer ve Temurtaş, Hasan (2015), “Perakende Satış Alanında SAP ERP ile Entegre Bir Yazılım”, *Dumlupınar Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, S: 035, s. 47-64.

Ayözger, Ayça Çiğdem (2016), *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul.

Bağcı, Hasan (2009), “Sosyal Mühendislik ve Denetim”, *Denetişim,* S: 1, s. 42-51.

Baktır, Halil Özgür, Çelik, Baran, Işık, Sait (2015), “Remnux Linux Dağıtımının İncelenmesi ve Örnek Bir Kötücül Yazılım Analiz Uygulaması Sunumu”, Akademik Bilişim.

Baliga, Arati, Kamat, Pandurang ve Iftode, Liviu (2007), "Lurking in the shadows: Identifying systemic threats to kernel data", *2007 IEEE Symposium on Security and Privacy (SP'07)* IEEE, s.246-251.

Bartos, Christopher A. (2016), “Cyber Weapons are not Created Equal”, *Faculty and Researcher Publications,* C: 142, S: 6, No: 1, s. 30-33.

Baykara, Muhammet ve Daş, Resul (2019), “Saldırı Tespit ve Engelleme Araçlarının İncelenmesi”, *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, S: 10, No:1, s. 57-75.

Baykara, Muhammet, Daş, Resul ve Karadoğan, İsmail (2013), "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi" *1st International Symposium on Digital Forensics And Security (Isdfs'13),* s. 231-239.

Bayrak, Muharrem (2020), "ABD İle Birleşik Krallık'ın AB ve NATO Çerçevesinde Siber Alanlarının Tarihsel Analizi", *Cyberpolitik Journal*, S: 5, No: 9, s. 22-51.

Bayraktar, Gökhan (2015)," Siber Savaş ve Ulusal Güvenlik Stratejisi", *Yeniyüzyıl Yayınları*, İstanbul.

Ben-Asher, Noam ve Gonzalez, Cleotilde (2015), "Effects of Cyber Security Knowledge on Attack Detection" *Computers in Human Behavior*, C: 48, s. 51-61.

Bickford, Jeffrey, O'Hare, Ryan, Baliga, Arati, Gnapathy, Vinod, Iftode, Liviu (2010) "Rootkits on smartphones: attacks, implications and opportunities", *Proceedings of the eleventh workshop on mobile computing systems and applications*, s. 49-54.

Birdişli, Fikret (2020), "Uluslararası Güvenliğin Tarihsel Gelişimi ve Postmodern Güvenlik Dönemi", *Güvenlik Bilimleri Dergisi*, s. 235-260.

BGYS Standardı ISO/IEC 27001 – 27002.

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

Bozoklu, Oğuz ve Çil, Celal Zaim (2017), "Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi" *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, S: 3, No: 1, s. 6-26.

Brenner, Susan W. (2001), "State Cybercrime Legislation in the United States of America: A Survey", *Richmond Journal of Law and Technology*, Cilt: 7, S: 3, No: 4, s. 1-16.

Canbek, Gürol (2005), *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme,* Gazi Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara.

Canbek, Gürol ve Sağıroğlu, Şeref (2016), "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, Cilt: 9, Sayı: 3, s.165-174.

Canbek, Gürol ve Sağıroğlu, Şeref (2008), "Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler", *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, S: 23, No: 1, s. 165-180.

Carr, Madeline (2016), "Public–private partnerships in national cyber-security strategies", *International Affairs*, S: 92, No: 1, s. 43-62.

Cisco (2020), *Cisco Annual Internet Report (2018-2023).*

Civelek, Dilek Yüksel (2011), *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, Devlet Planlama Teşkilatı, Uzmanlık Tezi, Ankara.

Coleman, Kevin (2008), "The Cyber Arms Race Has Begun", *CSO online,* s. 1-4.

Computer Misue Act, RA: 29.06.1990, 18.

Council of Europe (2004), *Convention on Cybercrime*.

Council of the Europe Union (2008), *European Security Strategy*.

Criminal Justice and Immigration Act, RA: 08.05.2008, 4.

Critical Foundations Protecting America's Infrastructures (1997), *The Report of the President's Commission on Critical Infrastructure Protection.*

Çahmutoğlu, Ersin (2020), "Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi", *Analytical Politics*, S:1, No:1, s. 63-79.

Çalışma Grubu 4 (2006), "E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları", *Türkiye Bilişim Derneği*.

Çelik, Minhaç (2015), "Siber Ordu Kurmak için Devletler Özel Sektör ile Çalışıyor", *TMMOB Bilgisayar Mühendisleri Odası Dergisi*. S: 5, s. 32-33.

Çelik, Şener (2013), "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* C: 15, S: 1, s. 137-175.

Daban, Ceylan (2016), "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", *Cyberpolitik Journal,* S: 1, No: 1, s. 78-94.

Daşdemir, Atakan (2018), *Türkiye'de En Çok Ziyaret Edilen Bazı Web Sitelerin Güvenlik Değerlendirmesi*, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya.

Data Protection Act, RA: 16.07.1998, 29.

Data Protection Act, RA: 23.05.2018, 12.

Değirmenci, Olgun (2002), *Bilişim Suçları,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Demir, Hüsnü, Yüce, Hüseyin, Akın Gökhan (2008), "Network Access Control Ağ Erişim Kontrolü (NAC) Sunumu", Ulak-CSIRT.

Dijital Türkiye Platformu (2017), *Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler Raporu.*

Disterer, Georg (2013), "ISO/IEC 27000, 27001 and 27002 for Information Security Management", *Journal of Information Security,* S: 4, s. 92-100.

Elektronik Haberleşme Güvenliği Yönetmeliği, RG: 20.07.2008, 26942.

Elektronik Haberleşme Kanunu, RG: 10.11.2008, 27050 (mükerrer).

ENISA (2004), *Good Practice Guide Network Security Information Exchanges*.

ENISA (2015), *The European Cyber Security Month 2015 Deployment Report*.

Erdem, Ayhan ve Kocaoğlu, Ramazan (2014), "Yeni Bir Ağ Güvenliği Yaklaşımı: Dinamik Zeki Güvenlik Duvarı Mimarisi" *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,* S: 29, No: 4, s. 707-715.

Ertam, Fatih, Tuncer, Türker ve Engin, Avcı (2013), "Adli Bilişimde Ağ Cihazlarının Önemi ve Güvenilir Yapılandırmaları", *Engineering Sciences*, S: 8, No: 3, s. 171-181.

Fraud Act, RA: 08.11.2006, 35.

Gehem, Maarten, Usanov, Artur, Frinking, Erik ve Rademaker, Michel (2015), *Assessing Cyber Security: A Meta Analysis of Threats, Trends, and Responses to Cyber Attacks*, The Hague Centre For Strategic Studies.

Gezgin, Deniz Mertkan ve Buluş, Ercan. (2008), "Kablosuz Erişim Noktalarına Yapılan DoS Saldırıları" *Akademik Bilişim*, s. 83-89.

Girgin, Osman. (2020), "Siber Uzay'da Üstünlük Mücadelesi; Amerika Birleşik Devletleri ve Rusya Federasyonu", *Academic Review of Humanities and Social Sciences*, S: 3, No: 1, s. 36-58.

Government UK (2011), *A Strong Britain in an Age of Uncertainty: The National Security Strategy Report.*

Government UK (2015), *National Security Strategy and Strategic Defence and Security Review 2015.*

Government UK (2018), *Inıtıal National Cyber Security Skills Strategy.*

Government UK (2018), *National Security Capability Review (NSCR).*

Gökırmak, Yavuz, Yüce, Emre, Bektaş, Onur, Soysal, Murat, Orcan, Serkan (2011), "Ipv6 Balküpü Tasarımı", *Tübitak ULAKBİM*, s. 1-4.

Gündüz, M. Zekeriya ve Daş, Resul (2016), "Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri" *Pd Ş. Sağıroğlu, Pdm Alkan, Pde Akyıldız Ve Dds Akleylek, Ed*, *9*.

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

Güntay, Vahit (2017), "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi*, S: 6, No: 2, s. 81-108.

Güntay, Vahit, (2018), "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", *Güvenlik Stratejileri Dergisi*, S: 14, No: 27, s. 79-111.

Hekim, Hakan ve Başıbüyük, Oğuzhan (2013), "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, Sayı: 4, No: 2, s. 135-158.

Hildreth, Steven A. (2001), "Cyberfare Warfare 11", *Congressional Research Service Report for Congress No. Rl30735*.

Horie, Daisuke, Yajima, Kenichi, Azimah, Noor, Goto, Yuichi ve Cheng, Jingde (2009), "GEST: A Generator of ISO/IEC 15408 Security Target Templates", *Computer and Information Science 2009*, Springer, Berlin, Heidelberg, s. 149-158.

ICO (2016), *A practical guide to IT security*.

Institute of Information Security Professionals (2010), *Information Security Skills Framework Document.*

Ipsos (2018), *Cyberbulling A Global Advisor Survey Report*.

ITU (2007), *GCA Chairman's Report*.

ITU (2015), *Global Cybersecurity Index-Cyberwellness Profile (v1) Report*.

ITU (2017), *Global Cybersecurity Index (v2) Report*.

ITU (2018), *Global Cybersecurity Index (v3) Report*.

Iversen, Amy, Liddell, Kathleen, Fear, Nicola, Hotopf, Matthew ve Wessely, Simon (2006), "Consent, confidentiality, and the data protection act", *Bmj*, S: 332, No: 7534, s 165-169.

İhtiyaroğlu, Uğur (2020), "Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi", *Hacettepe Hukuk Fakültesi Dergisi,* S: 10, No: 2, s. 406-440.

İlbaş, Çığır ve Av. Köksal, Mehmet Ali (2011), "Türkiye'nin Siber Suç Haritası 1990-2011 Sunumu".

İlker, Kara ve Aydos, Murat (2019), "Detection and Analysis of Attacks Against Web Services By the SQL Injection Method", In *2019 3rd International Symposium On Multidisciplinary Studies And Innovative Technologies (ISMSIT),* s. 1-4.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, RG: 23.05.2007, 26530.

Jagatic, Tom, Johnson, Nathaniel, Jakobsson, Markus ve Menczer, Filippo (2007) "Social Phishing" *Communications of the Acm,* S: 50, No: 10, s. 94-100.

Kâhya, Erhan (2007), "Bilgisayar Ağ Sistemleri Güvenliği", *Akademik Bilişim, 07-IX. Akademik Bilişim Konferansı Bildirileri,* s. 279-288.

Kara, İlker (2018), "Fidye Yazılım Virüsünün Tespiti, Teknik Analizi ve Çözümü", *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi,* S: 2, No: 2, s. 87-94.

Kara, Oğuz, Aydın, Üzeyir ve Oğuz, Ahmet (2006) "Ağ Ekonomisinin Karanlık Yüzü: Siber Terör", *V. Uluslararası Bilgi, Ekonomi ve Yönetim Kongresi,* C: 2, s. 156-170.

Karaarslan, Enis (2003), "Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar", *Akademik Bilişim,* s. 1-8.

Karaarslan, Enis, Tuğlular, Tuğkan ve Şengonca, Halil (2008), "Kurumsal Web Güvenliği Yapısı", *Akademik Bilişim,* s. 237-246.

Karabulut, Yunus Emre, Boylu, Gülistan, Küçüksille, Ecir U. Ve Yalçınkaya, Mehmet A. (2015), "Characteristics of Cyber Incident Response Teams in the World and

Recommendations for Turkey", *Balkan Journal of Electrical and Computer Engineering*, S: 3, s. 175-178.

Karadağ, Şerife (2019), *Siber Uzayın NATO'nun Güvenlik Anlayışına Etkisi*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Karakoç, Ercan ve Yılmaz, Bahadır (2020), "Askeri Güç ve Teknolojik Dönüşüm", *Uluslararası Sosyal Araştırmalar Dergisi*, C: 13, S: 72, s. 230-241.

Karataş, Gözde (2016), "Genetic Algorithm for Intrusion Detection System", *2016 24th Signal Processing And Communication Application Conference (Siu), IEEE,* s. 1341-1344.

Karataş, Gözde, Akbulut, Akhan ve Zaim, Abdül Halim (2016), "Mobil Cihazlarda Güvenlik–Tehditler ve Temel Stratejiler", *Istanbul Commerce University Journal of Scienc,* S: 15, No: 30, s. 55-75.

Kaya, Ömer Faruk ve Öztürk, Erdinç (2017), "Veri ve Ağ Güvenliği için Uygulama ve Analiz Çalışmaları", *Istanbul Ticaret Universitesi Fen Bilimleri Dergisi,* S: 16, No: 31, s. 85-102.

Kaytan, Mustafa (2016), *Web Tabanlı Oltalama Saldırılarının Makine Öğrenmesi Yöntemleri ile Tespiti*, İnönü Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Malatya.

Keskin Anıl, Duygu ve Gözenman, Samet (2019), "Hile Riski Açısından Sosyal Mühendislik", *Tıde Academia Research,* S: 1, No: 2, s. 281-306.

Kızılay, Şeyma. (2020), "Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası", *International Journal of Economics Administrative and Social Sciences,* Sayı: 3, No: 1, s 33-44.

Kişisel Verileri Koruma Kurumu Kurul Kararı, RG: 16.10.2018, 119.

Kişisel Verilerin Korunması Kanunu, RG: 24.03.2016, 29677.

Kurnaz, İbrahim (2016), "Siber Güvenlik ve İlintili Kavramsal Çerçeve", *Cyberpolitik Journal*, S: 1, No: 1, s. 56-77.

Kutlu, Önder, Kahraman, Selçuk ve Dinçer, Selçuk (2019), "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi", *ASSAM Uluslararası Hakemli Dergi*, s. 1-14.

Kuwatly, Iyad, Sraj, Melek, Al Masri, Zaid (2004), "A Dynamic Honeypot Design for Intrusion Detection", *The IEEE/ACS International Conference Onpervasive Services, ICPS 2004, Proceedings,* s. 95-104.

Lalonde Levesque, Fanny, Nsiempba, Jude, Fernandez, Jose M., Chiasson, Sonia ve Somayaji, Anil (2013), "A Clinical Study of Risk Factors Related to Malware Infections" *In Proceedings of The 2013 Acm Sıgsac Conference On Computer and Communications Security*, s. 97-108.

Li, Jinku, Wang, Zhi, Jiang, Xuxian, Grace, Mike ve Bahram, Sina (2010), "Defeating Return-Oriented Rootkits With" Return-Less" Kernels", *Proceedings of The 5th European Conference on Computer Systems*, s. 195-208.

Malicious Communications Act, RA: 29.07.1988, 27.

Mcafee Labs (2015), *Threats Report May 2015.*

Microsoft (2013), *Microsoft Security Intelligence Report*, C: 15.

Microsoft (2015), *Microsoft Security Intelligence Report*, C: 17.

Milhorn, H.Thomas (2007), "Cybercrime: How to Avoid Becoming A Victim", *Universal Publishers*, Florida.

Moore, Robert (2010), *Cybercrime: Investigating High-Technology Computer Crime*, Anderson Publishing.

Morton, Oliver (2014), "Tool, A. Windows Domain Enumeration", *Project Report Nettynum*, s. 1-90.

Nezgitli, Sena (2019) "Avrupa Birliği Siber Güvenlik Kanunu Sunumu", 6th International Management Information Systems Conference.

Nezgitli, Sena ve Benzer, Recep (2020), "Avrupa Birliği Siber Güvenlik Kanunu", *Journal of Information Systems and Management Research*, S: 2, No:1, s. 10-17.

Oğuz, Samet, Ceyhan, E. Burak ve Sağıroğlu, Şeref (2015), "Teknolojinin Casuslukta Kullanılması ve Karşı Önlemler", *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTurkey).*

Ovaz Akpınar, Kevser (2019), *Ethercat Tabanlı Bir Scada Sisteminde Kural ve Makine Öğrenmesine Dayalı Saldırı ve Anomali Tespiti*, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi, Sakarya.

Önaçan, Mehmet Bilge Kağan ve Atan, Hasan (2016), "Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği, *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, S: 17, No: 1, s. 13-21.

Özbek, Mücahid (2015), "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", *Article Letter Summer,* s. 73-88.

Özel, Abdurrahim, Kaya, Çetin ve Eken, Süleyman (2014), "Javascript Güvenlik Açıkları ve Güncel Çözüm Önerileri", 7. *Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı*, s. 252-257.

Özgen, Özlem ve Elmasoğlu, Kamile (2016), "Sosyal Medya ve Marka İletişimi: Havayolu Şirketlerinin Twitter Kullanımına Yönelik Bir Araştırma", *İletişim Kuram ve Araştırma Dergisi*, S:43, s. 181-202.

Protection of Children Act, RA: 20.07.1978, 37.

Provos, Niels (2004), "A Virtual Honeypot Framework", *Usenıx Security Symposium*, C: 173, No: 2004, s. 1-14.

Rid, Thomas ve Mcburney, Peter (2012), "Cyber-Weapons", *Rusi Journal*, S: 157, No: 1, s. 6-13.

Riley, Ryan, Jiang, Xuxiian ve Xu, Dongyan (2008), "Guest-Transparent Prevention of Kernel Rootkits with Vmm-Based Memory Shadowing" *International Workshop On Recent Advances İn Intrusion Detection,* Springer, Berlin, Heidelberg, s. 1-20.

Sağıroğlu, Şeref Alkan, Mustafa Samet, Refik Ulutaş, Güzin ve diğ. (2018), *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Grafiker Yayınları, Ankara.

Sawhney, Sanjay, Conover, Matthew ve Montague, Bruce (2015), "Systems and methods for providing network access control in virtual environments." *U.S. Patent No. 8,938,782,* Washington, Dc: U.S. Patent And Trademark Office, s. 1-21.

Say, Meriç ve Sağıroğlu, Şeref, "Bilgisayar Veri Güvenliği Üzerine Bir İnceleme: Klavye Dinleme Sistemleri", s. 1-5.

Saygılı, Erhan ve Kılıç, Fatih (2019), "Web Uygulama Güvenliği: Bir Örnek Çalışma Web Application Security: A Case Study", *Proceedings of the International Conference on All Aspects of Cyber Security,* C: 2, s. 45-48.

Seifert, Christian, Welch, Ian ve Komisarczuk, Peter (2007), "HoneyC -the Low-Interaction Client Honeypot", *Proceedings of the 2007 NZCSRSC, Waikato University, Hamilton, New Zealand,* S: 6, s. 1-9.

Sexual Offences Act, RA: 20.11.2003, 42.

Singer, Peter W. ve Friedman, Alman (2015), *Siber Güvenlik ve Siber Savaş*, (Çev. Ali Atav), Buzdağı Yayınları, Ankara.

Sökmen, Aşkın İnci (2020), "Yeni Savaş Alanı: Uzay", *Security of the Future,* s. 87-117.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2013a*), 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.*

_____ (2013b), *Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri.*

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2014*), Kurumsal SOME Kurulum ve Yönetim Rehberi.*

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016a), *2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı.*

_____ (2016b), *2016-2019 Ulusal Siber Güvenlik Stratejisi.*

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, *Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı.*

T.C. Ulaştırma ve Altyapı Bakanlığı (2020), *Ulusal Siber Güvenlik Stratejisi 2020-2023*.

Tamyapar, Berkay (2019), "Siber güvenlik ve Türkiye'de Yürütülen Siber Güvenlik Çalışmaları", 2019, s. 1-16.

Tang, Puqi ve Liu, Hsin-Yuo (2007), "Security enabled network access control." *U.S. Patent No. 7,185,365*. Washington, Dc: U.S. Patent And Trademark Office, 1-15.

The Network and Information Systems Regulations, RG: 10.05.2018, Part 1.

Touseef, Pariwish, Amjad Alam, Khubaib, Jamil, Abid, Tauseef, Hamza, Ajmal, Sahar ve diğ. (2019), "Analysis of Automated Web Application Security Vulnerabilities Testing*", ICFNDS '19 Proceedings of the 3rd International Conference On Future Networks And Distributed Systems,* No: 36, s. 1-8.

Turan, M. ve Külcü, Ö. (2014), "Türkiye'de bilişim suçlarının tanımlanması ve yaşanan ihlallere yönelik içerik analizi" *Türk Kütüphaneciliği*, S:*28,* No: 1, s. 18-46.

Tübitak Bilgem (2012), *Siber Güvenlik Tatbikat Raporu.*

Tübitak Bilgem (2014), *Güvenli Yazılım Geliştirme Temel Kuralları Doküman (Sürüm 1.12).*

Türk Ceza Kanunu, RG: 12.10.2004, 25611.

Türkay, Şeyda (2013), "Siber Savaş Hukuku ve Uygulanma Sorunsalı", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, S: 71, No: 1, s. 1177-1227.

Ulus, Halil İbrahim ve Demirci, Mehmet (2018), "Kurum İçi Saldırıların Tespiti ve Önlenmesi için Sunucu İzleme Uygulaması", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, S: 6, No: 3, s. 507-523.

Ulusal Siber Olaylara Müdahâle Merkezi (2014), *Siber Güvenliğe İlişkin Temel Bilgiler*, USOM, Ankara.

United Nations (1989), *Birleşmiş Milletler Çocuk Hakları Sözleşmesi.*

Utku, Anıl ve Doğru, İbrahim Alper (2017), "Android Kötücül Yazılımlar için İzin Tabanlı Tespit Sistemi" *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, S: 32, No: 4, s. 1015-1024.

Ünal, Ali Nadi ve Yarman, Bekir Sıddık Binboğa (2014), "Millî Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü", *7th International Conference On Information Security and Cryptology*, İstanbul, s. 278-284.

Ünal, Sevda (2015), *Siber Uzamın Güvenlikleştirilmesi Söylemi: Türkiye, ABD ve Avrupa Birliği Örnekleri*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Anabilim Dalı, Doktora Tezi, Ankara.

Ünver, Gül Nazik (2017), "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Dergisi*, S: 2, No: 3, s. 101-126.

Ünver, Mustafa, Canbay, Cafer ve Özkan, Hüseyin Burhan (2010), "Kritik Altyapıların Korunması", *Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,* s. 1-50.

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

Walden, Ian (2016), *Computer Crimes and Digital Investigations*, Oxford University Press, Oxford.

Wu, Bing, Chen, Jianmin, Wu, Jie ve Cardei, Mihaela (2007), "A Survey Of Attacks and Countermeasures in Mobile Ad Hoc Networks", *Wireless Mobile Network Security* Springer, Boston, MA, s. 103-135.

Yalçınkaya, Bahattin, Gedikli, Muhammet Emin ve Cibaroğlu, Mehmet Oytun (2019), "Elektronik Belge Yönetim Sisteminde Log Analizi: İstatistiksel Bir Değerlendirme", *Bilgi Yönetimi ve Bilgi Güvenliği,* 2019, s. 61-77.

Yenal, Serkan ve Akdemir, Naci (2020), "Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi", *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C:11, S: 1, s. 414-450.

Yılmaz, Onur (2017), "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", *Cyberpolitik Journal*, S: 2, No: 3, s. 17-38.

Yılmaz, Sacit (2011), "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *Barolar Birliği Dergisi*, S: 92, s. 62-100.

Yılmaz, Seda ve Sağıroğlu, Şeref (2013), "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, 2013, s. 159, s. 158-166.

Zhang, Xin, Jia, Li, Shi, Hongyan, Tang, Zhongbin ve Wang Xiaoling (2012) "The application of machine learning methods to intrusion detection", *2012 Spring Congress on Engineering and Technology*, *IEEE*, s. 1-4.

ELEKTRONİK KAYNAKLAR

http://be.gazi.edu.tr/posts/view/title/doktora-programlari-16558 (15.11.2020)

http://berkay22demirel.blogspot.com/2017/10/bilgisayar-aglar-ders-7-arp-zehirlenmesi.html?m=0 (09.09.2020)

https://cbddo.gov.tr/projeler/hack-istanbul/ (07.07.2021)

http://etkinlik.btk.gov.tr/etkinlik/detay/btk_hacker_kamp/ (05.07.2020)

http://groups.itu.int/cybersecurity-gateway/HOME.aspx (25.10.2020)

http://nitelikliveri.com/diger-konular/log-kayitlariyla-siem-nasil-yapilir/ (17.10.2020)

http://www.cyberbullying.ca. (15.08.2020)

http://www.tuhid.org/tuhid-meslek-ilkeleri.html (08.11.2020)

https://alycck.wordpress.com/2016/03/03/kullanim-senaryosu/ (16.10.2020)

https://bau.edu.tr/icerik/8856-fen-bilimleri-enstitusu-siber-guvenlik (12.11.2020)

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/arp-(adres-%C3%A7%C3%B6z%C3%BCmleme-protokol%C3%BC) (02.09.2020)

https://blog.emsisoft.com/en/27233/what-is-a-botnet/ (22.08.2020)

https://cahitcengizhan.com/bilisim-guvenligi-turlerinin-tarihsel-gelisimi/ (21.10.2020)

https://cbddo.gov.tr/haberler/4906/siber-zeka-bilgi-yarismasi (16.11.2020)

https://ccdcoe.org/cycon/ (18.11.2020)

https://docs.ahtapot.org.tr/kullanim-klavuzlari/web-uygulama-guvenlik-duvari-kullanimi/ (18.10.2020)

https://e-bergi.com/y/pc-virus-tarihi/ (28.09.2020, 20.10.2020)

https://egitim.sge.gov.tr/ (11.11.2020, 15.11.2020)

https://en.unesco.org/news/internet-governance-forum-be-held-unesco (23.11.2020)

https://en.wikipedia.org/wiki/Christmas_Tree_EXEC (27.09.2020)

https://esube.albaraka.com.tr/ (25.08.2020)

https://etkinlik.btk.gov.tr/etkinlik/detay/siber_guvenlige_giris_egitimi (16.11.2020)

https://gdpr-info.eu/art-21-gdpr/ (09.11.2020)

https://h2020.org.tr/tr/ikili-isbirlikleri/qa (22.11.2020)

https://hgm.uab.gov.tr/kamu-entegre-veri-merkezi-projesi (06.07.2021)

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/ (10.11.2020)

https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073099056067082074047082081113088112 (05.11.2020)

https://it.bilgi.edu.tr/tr/guvenlik/antivirus/ (15.10.2020)

https://medium.com/@kerem_tamci/stored-xss-ve-microsoft-e7a17b9040c (18.09.2020)

https://medium.com/@oguzalbastr02/ortadaki-adam-sald%c4%b1r%c4%b1s%c4%b1-mitm-detayl%c4%b1-anlat%c4%b1m-5e5f86af1d6a (16.09.2020)

https://mqplanet.com/hosting/anti-ddos (18.10.2020)

http://onuraltinkaynak.com/windows-10da-vpn-baglantisi/ (19.10.2020)

https://radore.com/blog/nesnelerin-internetinin-gecmisi-ve-gelecegi.html (24.10.2020)

https://sec.sabanciuniv.edu/ (15.11.2020)

https://sge.bilgem.tubitak.gov.tr/tr/nato-ccdcoe-daimi-temsilciligi (18.11.2020)

https://siberci.com/siber-guvenlik-tarihi/ (24.09.2020, 20.10.2020)

https://siberkume.org.tr/Activities (16.11.2020)

https://sibertehdit.com/ips-ve-ids-nedir-bu-sistemler-nasil-atlatilir/ (16.10.2020)

https://sozluk.gov.tr. (17.07.2020, 04.08.2020, 05.10.2020)

https://threatmap.checkpoint.com/. (13.08.2020)

https://whatis.techtarget.com/definition/IISP-Institute-of-Information-Security-Professionals (06.11.2020)

https://womaneng.com/sql-injection-nedir/ (20.09.2020)

https://www.aa.com.tr/tr/turkiye/usoma-idari-para-cezasi-kesme-yetkisi-verildi-/1268694 (07.11.2020)

https://www.akademikkaynak.com/literatur-taramasi-nedir-ve-nasil-yapilir.html (06.07.2021)

https://www.aydin.edu.tr/tr-tr/arastirma/arastirmamerkezleri/sem/digital-bilisim-egitimleri/Pages/Siber-G%C3%BCvenlik-ve-SOME-E%C4%9Fitimi.aspx (17.11.2020)

https://www.bilgiguvenligi.org.tr/faaliyetler/etkinlikler/2013-2/veri-merkezi-calistayi-2013/ (08.07.2021)

https://www.bilgiguvenligi.org.tr/faaliyetler/etkinlikler/2015-2/ 08.07.2021)

https://www.bilgiguvenligi.org.tr/kitaplar/ (09.07.2021)

https://www.bilgeadam.com/akademi/bilisim-uzmanligi/siber-guvenlik (16.11.2020)

https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/siber2011-SonucBildirgesi.pdf (08.07.2021)

https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/siber2012-SonucBildirgesi.pdf (08.07.2021)

https://www.biltam.com.tr/haberler/kamu-siber-guvenlik-zirvesi2017.html (22.11.2020)

https://www.bsigroup.com/en-GB/iso-27001-information-security/iso-27001-training-courses/ (17.11.2020)

https://www.btkakademi.gov.tr/portal/course/siber-guvenlik-analisti-egitimi-5020#!/about (15.11.2020)

https://www.ceop.police.uk/safety-centre/ (06.11.2020)

https://www.cyberdefensemagazine.com/nato-and-definition-rules-for-cyber-warfare/ (12.08.2020)

https://www.cybermagonline.com/ (09.07.2021)

https://www.defenceturk.net/bilgi-guvenligi-ve-siber-guvenlik-turkiye-siber-guvenlik-kumelenmesi (12.10.2020)

https://www.dia.com.tr/siber-saldiri-nedir-siber-saldirilardan-nasil-korunulur/. (01.08.2020)

https://www.eccouncil.org/programs/ (17.11.2020)

https://www.egm.gov.tr/siber/sibersucnedir#/. (08.08.2020)

https://www.ekizer.net/bilisimsuclari-sibersuclar/ (10.08.2020)

https://www.eset.com/tr/trojan-horse/ (28.09.2020)

https://www.first.org/members/teams/tr-cert (05.11.2020)

https://www.getsafeonline.org/ (12.11.2020)

https://www.gov.im/about-the-government/departments/home-affairs/office-of-cyber-security-and-information-assurance/ (20.11.2020, 28.10.2020)

https://www.gov.im/about-the-government/departments/home-affairs/office-of-cyber-security-and-information-assurance/

https://www.gov.uk/government/news/the-4th-uk-india-cyber-dialogue (23.11.2020)

https://www.gov.uk/government/organisations/ofcom (26.10.2020)

https://www.guvenliweb.org.tr/galeri-detay/internette-1-dakikada-neler-oluyor (15.07.2020)

https://www.haberturk.com/gundem/haber/1268485-wikileaks-nedir (30.09.2020)

https://www.haberturk.com/turkiye-internet-kullanim-istatistiklerinde-son-durum-ne-2171017-ekonomi. (15.07.2020)

https://www.hurriyet.com.tr/teknoloji/siber-saldiri-ne-demek-internet-siber-saldiridan-mi-coktu-41424233/ (28.07.2020)

https://www.icisleri.gov.tr/5-uluslararasi-siber-suclar-calistayi. (05.07.2020)

https://www.iscturkey.org/bildiriler/2020/iscturkey_2020_sonuc_bildirgesi.pdf (07.07.2021)

https://www.iso.org/isoiec-27001-information-security.html (04.10.2020).

https://www.isokalitebelgesi.com/bilgi-nedir-bilgi-guvenligi-nedir-bilgi-guvenligi-yonetim-sistemi-nedir (06.10.2020)

https://www.itu.int/en/action/cybersecurity/Pages/default.aspx (25.10.2020)

https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (25.10.2020)

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (25.10.2020)

https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/International-Cyber-Shield-Exercise.aspx (19.10.2020)

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets (03.10.2020)

https://www.itu.int/net/pressoffice/press_releases/2012/83.aspx (18.11.2020)

https://www.iwf.org.uk/ (06.11.2020)

https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks (20.08.2020)

https://www.kaspersky.com.tr/resource-center/threats/top-7-cyberthreats (13.08.2020)

https://www.kbd.org.tr/kategori/yazilar/66721/siber-guvenlik-pazari-bas-donduruyor (01.07.2021)

https://www.kvkk.gov.tr/Icerik/6737/Cocuklarin-Kisisel-Verilerinin-Korunmasi-Bakimindan-Dikkat-Edilmesi-Gerekenler (08.11.2020)

https://www.microsoft.com/security/blog/2017/09/06/ransomware-1h-2017-review-global-outbreaks-reinforce-the-value-of-security-hygiene/ (01.09.2020)

https://www.millîyet.com.tr/gundem/siber-saldiri-nedir-nasil-olur-siber-saldiri-mi-var-korunma-yollari-nelerdir-6126736/. (26.07.2020)

https://www.millîyet.com.tr/siber-suc-nedir--molatik-12976/ (10.08.2020)

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security (24.11.2020)

https://www.ncsc.gov.uk/news/awareness-only-first-step (17.11.2020)

https://www.ncsc.gov.uk/section/keep-up-to-date/cisp (09.11.2020)

https://www.ntt.co.jp/index_e.html. (25.07.2020)

https://www.parsecuremap.com/#2/42.3/-17.7/. (03.08.2020)

https://www.siberportal.org/red-team/cyber-attacks/siber-saldirilarin-evrimi-1986-2017/ (29.09.2020, 30.09.2020)

https://www.somut.net/126/pcdonanim/gateway-nedir.1.html (16.10.2020)

https://www.sonsuzteknoloji.com/virus-ve-solucan-arasindaki-fark-nedir/ (19.08.2020)

https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1068&LangID=1 (23.11.2020)

https://www.ticaret.gov.tr/video-galeri/kamu-spotu (05.07.2020)

https://www.tse.org.tr/IcerikKategori?ID=869&ParentID=2289 (11.11.2020)

https://www.uab.gov.tr/siber-guvenlik (07.11.2020)

https://www.webtekno.com/30-yil-once-tarihin-ilk-siber-saldirisini-duzenleyerek-interneti-cokerten-adam-h56353.html (28.09.2020)

https://www.youtube.com/watch?v=6uwEJ2XTS1g&ab_channel=TRTHaber (14.11.2020)

https://www.youtube.com/watch?v=caGk0_j20Lg&ab_channel=KlanIstanbul (14.11.2020)

https://www.youtube.com/watch?v=x0jVmMmtyG4&ab_channel=elifkayademir (14.11.2020)

https://yazilimportal.com/dos-sald%c4%b1r%c4%b1s%c4%b1-nedir-ve-nas%c4%b1l-korunulur-e1c6f4895cfd (16.09.2020)

ÖZET

İnsanlık tarihinin, teknoloji ile şekillenmesi ile beraber insanlık hızlı bir değişim süreci içine girmiştir. Teknoloji, birçok alanda yer almaya başlamış ve bunun sonucunda bu alanda yer alan cihaz sayısı artmış ve bu artış siber uzayı oluşturarak geliştirmiştir. Siber uzaydaki bu büyüme bazı sorunları da beraberinde getirmiştir. Siber uzaydaki kapasite artışı ile beraber teknolojinin var olması ve ilerlemesinin önüne geçerek siber tehdit ve siber saldırılar meydana gelmiştir. Bu tehdit ve saldırıların tarihsel geçmişi köklü olmasa bile var oluşları ve ilerlemeleri hızlı ve karmaşık olmuştur.

Siber uzayın başkarakteri, insan ve insanlığın geliştirdiği teknolojiler olduğu düşünülürse siber tehdit ve saldırılardan yine en çok insan etkilenmiştir. Bu etkilenme, bazen bireysel bazen de toplumsal olmuştur. Bu da siber saldırıların yıkıcı etkilerine karşı siber güvenlik ve savunma ihtiyacını ortaya koyarak bu saldırılara karşı topyekûn mücadele etme durumunu ortaya koymuştur.

Bu çalışmada, Türkiye ve İngiltere için siber güvenlik politikaları incelenmiş, bu politikaları belirlerken nasıl yollar izledikleri ve siber güvenliği sağlamak için ne tür yöntemler kullandıkları araştırılmış ve yaptıkları çalışmalar neticesinde uluslararası alandaki siber güvenlik sıralamalarından bahsedilmiştir. Sıralama da aldıkları yerleri belirleyen kriterler ele alınmış ve incelenmiştir. Tüm bu araştırma ve incelemelerin sonucunda iki ülkenin siber güvenliği sağlama konusunda iyi oldukları yönleri vurgulanarak eksik kaldıkları taraflar kıyaslama yöntemiyle gösterilmiştir ve gelecekteki siber güvenlik politikaları için belirlenecek yol haritasına katkıda bulunulmuştur.

Anahtar Kelimeler: Siber Kavram, Siber Uzay, Siber Güvenlik, Siber Saldırı, Siber Güvenlik Endeksi, Siber Yönetim Modeli.

ARŞİV Kayıt Bilgileri

Tezin Adı İngiltere ve Türkiye'nin Siber Güvenlik Politika Yaklaşımlarının Karşılaştırılması

Tezin Yazarı Sena NEZGİTLİ

Tezin Danışmanı Uğur BOĞA

Tezin Konumu Uzmanlık Tezi

Tezin Tarihi Haziran 2021

Tezin Alanı Siber Güvenlik

Tezin Yeri RTÜK – ANKARA

Anahtar Kelimeler Siber Kavram, Siber Uzay, Siber Güvenlik, Siber Saldırı, Siber Güvenlik Endeksi**,** Siber Yönetişim Modeli

ABSTRACT

With the shaping of human history by technology, humanity has entered into a rapid change process. Technology has started to take place in many areas and as a result, the number of devices in this area has increased and this increase has created and developed cyberspace. This growth in cyberspace has brought some problems with it. With the increase in capacity in cyber space, cyber threats and cyber attacks have occurred by preventing the existence and progress of technology. Although the historical background of these threats and attacks is not deep-rooted, their existence and progress has been rapid and complex.

Considering that cyberspace is the protagonist, human and the technologies developed by humanity, the most people have been affected by cyber threats and attacks. This influence was sometimes individual and sometimes social. This has revealed the need for cyber security and defense against the destructive effects of cyber attacks, and has revealed the situation of fighting against these attacks as a whole.

In this study, cyber security policies for Turkey and England were examined, how they followed while determining these policies and what methods they used to provide cyber security were researched and as a result of their studies, cyber security rankings in the international field were mentioned. In the ranking, the criteria that determine the places they take were discussed and examined. As a result of all these researches and examinations, the sides that the two countries are good at in terms of providing cyber security are emphasized and the shortcomings are shown by comparison method and contributed to the roadmap to be determined for future cyber security policies.

Key words: Cyber Concept, Cyber Space, Cyber Security, Cyber Attack, Cyber Security Index, Cyber Management Model.

ÖZGEÇMİŞ

Sena NEZGİTLİ 1992 yılında Ankara'da doğdu. Ahmet Cevdet Paşa İlkokulu, Alparslan Anadolu Lisesi'nden mezun oldu. 2010 yılında Gazi Üniversitesi Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği bölümünde lisans eğitimini tamamladı. 2015-2017 yılları arasında özel sektörde çalıştı. 2018 yılı şubat ayında Radyo ve Televizyon Üst Kurulunda uzman yardımcısı olarak göreve başladı. İyi derecede İngilizce bilen Sena NEZGİTLİ Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Bölümünde yüksek lisans eğitimine devam etmektedir.