İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

SİBER GÜVENLİK YÖNETİM MODELLERİ VE ETKİLERİNİN ARAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Aycan Ramazan GÜNDÜZHEV

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

HAZİRAN 2019

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

SİBER GÜVENLİK YÖNETİM MODELLERİ VE ETKİLERİNİN ARAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Aycan Ramazan GÜNDÜZHEV
(708151023)

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA
Eş Danışman: Dr. Ahmet Güven PADO

HAZİRAN 2019

İTÜ, Bilişim Enstitüsü'nün 708151023 numaralı Yüksek Lisans Öğrencisi Aycan Ramazan GÜNDÜZHEV, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "SİBER GÜVENLİK YÖNETİM MODELLERİ VE ETKİLERİNİN ARAŞTIRILMASI" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Ertuğrul KARAÇUHA** İstanbul Teknik Üniversitesi	.....
Eş Danışman :	**Dr. Ahmet Güven PADO** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Serhat ŞEKER** İstanbul Teknik Üniversitesi	.....
	Prof. Dr. Muhammed Oğuzhan KÜLEKCİ İstanbul Teknik Üniversitesi	.....
	Prof. Dr. Hülya ŞAHİNTÜRK Yıldız Teknik Üniversitesi	.....

Teslim Tarihi : 02 Mayıs 2019
Savunma Tarihi : 14 Haziran 2019

Aileme,

ÖNSÖZ

Bu çalışmada teknolojinin en sıcak gündem maddelerinden birisi olan siber güvenlik ile ilgili olarak yönetim modeli araştırılmıştır. Başta siber, siber güvenlik, bilgisayar korsanlığı olmak üzere kavram açıklamaları yapılmıştır. Daha sonra siber güvenlik tarihine yön veren siber saldırılar ve virüs yayılımları incelenmiştir. Buralardan yapılan çıkarımlar ve literatür taramaları sayesinde etkili bir siber güvenlik yönetim modelinde olması gereken beş alt başlık tespit edilmiştir.

Gerek kamu gerekse özel sektör özelinde siber güvenlik, sağlanması gereken en önemli değerlerden bir tanesidir. Hayatımıza giren teknoloji sayesinde yaşamlarımızın bir kopyasının da aslında siber dünyada olduğunu söylesek yanlış olmaz. Bu nedenle gerek kişisel verilerin gizliliği gerek organizasyonların maddi, manevi ve itibar değerleri veyahut gerekse devletlerin varlıklarını, stratejileri korumaları için teknolojinin hayatımıza bu denli girdiği bir dönemde siber güvenlik konusuna çok dikkat etmeleri gerekmektedir. Siber saldırılarda korunmanın en iyi yolu en başta iyi bir siber güvenlik yönetim modeline sahip olmaktır.

Tez çalışmamın planlanmasında, araştırılmasında, oluşturulmasında, düzenlenmesinde bana yol gösteren, benden desteklerini ve güvenini esirgemeyen çalışmalarım boyunca değerli katkılarını, tecrübesini ve ilmini cömertçe aktarmaya çalışan değerli tez danışmanlarım sayın hocam Prof. Dr. Ertuğrul KARAÇUHA'ya ve Dr. Ahmet Güven PADO'ya ve teşekkürlerimi sunarım.

Haziran 2019

Aycan Ramazan GÜNDÜZHEV
(Elektronik ve Haberleşme Mühendisi)

İÇİNDEKİLER

Sayfa

ÖNSÖZ ..... **vii**
İÇİNDEKİLER ..... **ix**
KISALTMALAR ..... **xiii**
ÇİZELGE LİSTESİ ..... **xv**
ŞEKİL LİSTESİ ..... **xvii**
ÖZET ..... **xix**
SUMMARY ..... **xxi**
1. GİRİŞ **1**
1.1 Tezin Konusu ve Önemi 1
1.2 Tezin Amacı ve İçeriği 8
2. SİBER GÜVENLİK KAVRAMININ TEMELLERİ VE TERMİNOLOJİ **11**
2.1 Siber 11
2.2 Siber Uzay/Alan/Ortam 11
2.3 Siber Terörizm 12
2.4 Siber Suç 16
2.5 Siber Casusluk / İstihbarat 20
2.6 Siber Savaş 22
2.7 Siber Güvenlik Kavramı 25
2.8 Siber Güvenlik'in Önemi 28
3. BİLGİSAYAR KORSANLIĞI, MOTİVASYONLARI VE SALDIRI YÖNTEMLERİ **33**
3.1 Bilgisayar Korsanı 33
3.2 Bilgisayar Korsanı Çeşitleri 34
3.2.1 Beyaz şapkalı / etik bilgisayar korsanları 34
3.2.2 Siyah şapkalı bilgisayar korsanları 35
3.2.3 Gri şapkalı bilgisayar korsanları 35
3.2.4 Siber muhalif bilgisayar korsanları 36
3.2.5 Suicide bilgisayar korsanları 36
3.2.6 State sponsored bilgisayar korsanları 36
3.2.7 Script kidding 36
3.3 Bilgisayar Korsanlığı Motivasyonları 37
3.4 Bilgisayar Korsanlığı / Siber Saldırı Yöntemleri 40
3.4.1 Servis dışı bırakma saldırıları (DoS & DDoS) 41
3.4.2 Yemleme - oltalama saldırıları (Phishing) 43
3.4.3 Araya giren adam saldırısı (Man in the Middle Attack (MitM)) 44
3.4.4 Sosyal mühendislik (Social Engineering) 46
3.4.5 Kabloya saplama yapma (Wiretapping) 47
3.4.6 Açık mikrofon dinleme 48
3.4.7 İstem dışı yığın ileti (E-posta) gönderme (Spam - Junk Mail) 48
3.4.8 Şifre atağı (Brute Force, Dictionary Attack) 48
3.4.9 Zararlı yazılım kullanımı (Virüs-Solucan-Truva Atı vb.) 49

3.4.10 Arka kapı kullanımı (Backdoor - Trapdoor)… 50
3.4.11 SQL veri tabanı saldırısı (SQL injection attack) 51
4. DÜNYA SİBER TARİHİNE YÖN VEREN ÖNEMLİ SİBER SAVAŞLAR VE ZARARLI YAZILIMLAR 53
4.1 Kosova Krizi - 1999 53
4.2 ABD ve Çin Arasında Yaşanan Siber Saldırılar - 2001 54
4.3 Estonya Siber Saldirisi -2007 55
4.4 İsrail Orchard Operasyonu – 2007 56
4.5 Gürcistan Siber Saldırısı - 2008 57
4.6 Stuxnet - 2010 58
4.7 Duqu- 2011 61
4.8 Shady Rat (2006- 2011) 62
4.9 Sony Firmasına Karşı Yapılan Siber Saldırılar – 2014 64
4.10 Türkiye ve Rusya Arasında Yaşanan Siber Saldırılar – 2015 65
4.11 Wanna Cry – 2017 66
4.12 Dünya Genelince Yaşanan Büyük Siber Saldırılar ve Virüs Yayılmaları Sonucu 69
5. SİBER GÜVENLİK YÖNETİM MODELİ İNCELEMESİ 73
5.1 Risk Yönetimi 74
5.1.1 Risk tanımı 74
5.1.2 Belirsizlik 76
5.1.3 Tehdit 77
5.1.4 Bilgi sistemleri riski / siber risk nedir? 80
5.1.5 Bilgi teknolojileri risk yönetimi tanımı 81
5.1.6 Risk yönetim şeması 85
5.1.6.1 Durumun belirlemesi 86
5.1.6.2 Tehlike ve risklerin belirlenmesi 88
5.1.6.3 Risk analizinin yapılması: 91
5.1.6.4 Risklerin değerlendirilmesi, derecelendirilmesi ve önceliklendirilmesi 96
5.1.6.5 Riskleri azaltmak ve iyileştirmek 97
5.1.6.6 İzleme ve inceleme 99
5.1.7 Risk yönetim sürecinde başarı 100
5.2 Siber Güvenlikte İnsan Etkisi 100
5.3 Siber Kriz Yönetimi 105
5.3.1 Kriz öncesi 107
5.3.2 Kriz anı 109
5.3.3 Kriz sonrası 111
5.4 Siber Güvenlik Yönetim Modelinde Organizasyon Yapısı Ve Teknolojik Yatırımların Etkisi 111
5.4.1 Siber güvenlik organizasyon yapısı 111
5.4.1.1 Program yönetimi 113
5.4.1.2 Güvenlik operasyon merkezi 114
5.4.1.3 Acil durum operasyonları ve vaka yönetimi 114
5.4.1.4 Güvenlik mühendisliği ve varlık güvenliği 114
5.4.2 Siber güvenlik yatırımları 117
5.5 Türkiye'nin Siber Güvenlik Stratejisinin İncelenmesi ve Yasal Mevzuat 122
5.5.1 Genel bakış 122
5.5.1.1 Sorumlu kurumlar ve düzenleyici ve denetleyici kurumlar 126
5.5.1.2 Farkındalık çalışmaları 128
5.5.1.3 Ar-Ge faaliyetleri 129

5.5.1.4 Uluslararası iş birliği sağlama 130
5.5.1.5 Ulusal siber olaylara müdahale merkezi (usom), kurumsal ve sektörel siber olaylara müdahale ekibi 130
5.5.2 Yasal mevzuat 135
5.5.2.1 5237 Sayılı yeni türk ceza kanunu'nda bilişim suçları 137
5.5.2.2 5237 Sayılı yeni türk ceza kanunu'nda bulunan diğer bilişim suçları 139
5.5.3 Bilişim suçlarında uluslararası hukuk uygulaması – avrupa konseyi siber suçlar sözleşmesi 147
5.5.3.1 Genel değerlendirme 147
5.5.3.2 Sözleşmede tanımlanan suçlar 148
5.5.3.3 Avrupa konseyi siber suçlar sözleşmesini imzalayan ülkeler 149
5.5.3.4 Siber suç sözleşmesi'ne göre uluslararası adli yardımlaşma konusundaki temel ilkeler 149
6. SONUÇLAR ve ÖNERİLER 151
KAYNAKÇA 161
EKLER 171
ÖZGEÇMİŞ 175

KISALTMALAR

BM : Birleşmiş Milletler
IPv6 : Internet Protokolü sürüm 6
IPv4 : Internet Protokolü sürüm 4
BDDK : Bankacılık Düzenleme ve Denetleme Kurumunu,
BTK : Bilgi Teknolojileri ve İletişim Kurumunu,
EPDK : Enerji Piyasası Düzenleme Kurumunu
SPK : Sermaye Piyasa Kurulu
CISO : Chief Information Security Officer
BGBY : Bilgi Güvenliği Baş Yöneticisi
CIO : Chief Information Officer
BBY : Baş Bilgi Yöneticisi
IAF : Israel Air Force (İsrail Hava Kuvvetleri)
ICT : Information and Communications Technology (Bilgi ve Haberleşme Teknolojisi)
ICS : Industrial control systems (Endüstriyel kontrol sistemi)
PLC : Programmable logic controllers (Programlanabilir Mantıksal Denetleyici)
CCDCOE : Cooperative Cyber Defense Center of Excellence (Siber Savunma Mükemmeliyet Merkezi)
NATO : North Atlantic Treaty Organization (Uluslararası Askeri İttifak)
ISP : Internet Service Provider (İnternet Servis Sağlayıcı)
GPS : Global Positioning System (Küresel Konumlama Sistemi)
ITU : International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
CEO : Chief Executive Officer (Yönetim Kurulu Başkanı)
DDOS : Distributed denial-of-service (Dağıtılmış Servis Dışı Bırakma)
CPS : Cyber Phsical Systems
SF : Siber fiziksel sistemler
ICS : Industrial control systems (Endüstriyel kontrol sistemleri)
IOT : İnternet of Things (Nesnelerin internet)
DoS : Denial of service (Servis Dışı Bırakma)
TCP : Transmission Control Protocol (İletim Kontrol Protokolü)
UDP : User Datagram Protocol (Kullanıcı Veribloğu İletişim Kuralları)
ICMP : Internet Control Message Protocol (İnternet kontrol mesaj protokolü)
ARP : Address Resolution Protocol (Adres çözümleme protokolü)
DNS : Domain Name System (Alan isimlendirme Sistemi)
MitM : Man in the Middle Attack (Araya giren kişi)
TDK : Türk Dil Kurumu
ABD : Amerika Birleşik Devletleri
SOC : Security Operation Center (Siber Operasyon Merkezi)

ÇİZELGE LİSTESİ

Sayfa

Çizelge 2.1 : 2018 küresel risk raporuna göre teknoloji başlığı altındaki ulusal riskler ve tanımları **15**
Çizelge 2.2 : Siber suç sınıflandırmaları **18**
Çizelge 2.3 : Konvansiyonel savaş ile siber savaş arasındaki farklar **24**
Çizelge 2.4 : Farklı siber eylemlerin ana karakteristikleri **24**
Çizelge 3.1 : Bilgisayar korsanlığı adımları ve açıklamaları **34**
Çizelge 4.1 : Stuxnet ile yaygın kötü amaçlı yazılım karşılaştırılması **59**
Çizelge 5.1 : 2016-2019 Ulusal siber güvenlik stratejisine göre siber güvenlik kuruluna üye kurum ve düzenleyici ve denetleyici kurum listesi (yazar tarafından düzenlenmiştir). **127**
Çizelge 5.2 : USOM, kurumsal SOME, sektöre SOME hizmet alanları **132**
Çizelge 5.3 : Kritik altyapıların ait oldukları kurumlar ve parametreler **134**
Çizelge A.1 : Avrupa konseyi siber suçlar sözleşmesini imzalayan onaylayan ve yürürlüğe koyan ülke listesi. **172**

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1 : Siber terörizm kavramsal çerçeve **14**
Şekil 2.2 : Ulusal risklerin birbirleri ile bağlılık raporu **17**
Şekil 2.3 : 2001-2017 yılları arasında siber suçların uğrattığı maddi hasar (milyon dolar) **19**
Şekil 2.4 : 2013-2018 Dünya üzerinde gerçekleşen siber saldırıların dağılımı (verileri temel alınarak yazar tarafından tasarlanmıştır)..... **20**
Şekil 2.5 : Gerçek zamanlı yapılan DDOS ataklarının haritası **23**
Şekil 2.6 : Siber eylemler arasındaki ilişki **25**
Şekil 2.7 : Gizlilik, bütünlük ve erişilebilirlik üçgeni (Yazar tarafından tasarlanmıştır). **26**
Şekil 2.8 : 2017-2018 yılında siber ataklara hedef olan ilk 10 sektör **27**
Şekil 2.9 : Sektör bazında 2018 küresel atak oranları **28**
Şekil 2.10 : 2018 Küresel risk raporuna göre olabilirlik açısından ilk 5 küresel risk **30**
Şekil 2.11 : Symantec güvenlik tehdit raporu istatistikleri (Yazar tarafından tasarlanmıştır). **31**
Şekil 2.12 : Toplam kötü amaçlı yazılım (2016 - 2018) **32**
Şekil 2.13 : Toplam mobil kötü amaçlı yazılım (2016 - 2018) **32**
Şekil 3.1 : Bilgisayar korsanlarının bilgisayar korsanlığı motivasyonları 2018 ..... **38**
Şekil 3.2 : Bilgisayar korsanlarının yaklaşık bilgisayar korsanlığı yapma süreleri .. **38**
Şekil 3.3 : Bilgisayar korsanlarının bilgisayar korsanlığı motivasyonları 2018 ..... **39**
Şekil 3.4 : 2015- 2017 yıllarına göre en çok kullanılan 10 atak karşılaştırması **41**
Şekil 3.5 : DoS atağının ana mantığının topolojisi (Yazar tarafından tasarlanmıştır). **42**
Şekil 3.6 : DDoS atağının ana mantığının topolojisi (Yazar tarafından tasarlanmıştır). **43**
Şekil 3.7 : Oltalama-Yemleme (Phising) Saldırıları (Yazar tarafından tasarlanmıştır). **44**
Şekil 3.8 : Man in the middle / IP aldatmacası (Yazar tarafından tasarlanmıştır). **45**
Şekil 3.9 : Man in the middle / Şebeke trafiği dinlemesi (Yazar tarafından tasarlanmıştır). **45**
Şekil 3.10 : Sosyal mühendislik hayat döngüsü **47**
Şekil 3.11 : Kaba kuvvet (Brute Force) ana mantığı topolojisi (Yazar tarafından tasarlanmıştır). **49**
Şekil 3.12 : Sözlük atağı (Dictionary Attack) ana mantığı topolojisi (Yazar tarafından tasarlanmıştır). **49**
Şekil 3.13 : Zararlı yazılım internet sitesi uygulaması (Truva atı ve Virüs) (Yazar tarafından tasarlanmıştır). **50**
Şekil 3.14 : Zararlı yazılım e-posta uygulaması (Truva atı ve Virüs) (Yazar tarafından tasarlanmıştır). **50**
Şekil 4.1 : Ülkelere göre stuxnet saldırısından etkilenen abone sayılar **60**

Şekil 4.2 : Ülkelere göre siemens yazılımı yüklenmiş ve stuxnet saldırısından etkilenmiş abone değeri (%) **61**
Şekil 4.3 : Shary RAT saldırısından etkilendiği tespit edilen organizasyonlar şeması **63**
Şekil 4.4 : Shary RAT saldırısının ülkelere göre dağılımı **63**
Şekil 4.5 : AIDS ınfo disk trojan tarafından gönderilen mesaj..... **66**
Şekil 4.6 : Genel fidye yazılım atak şeması (Yazar tarafından tasarlanmıştır)..... **67**
Şekil 4.7 : Windows versiyonlarına göre virüsten etkilenme yüzdeleri **68**
Şekil 5.1 : Siber Güvenlik ile İlgili Yönetim Modeli Şeması (Yazar tarafından tasarlanmıştır). **74**
Şekil 5.2 : Örnek bir risk matrisi (Yazar tarafından tasarlanmıştır). **75**
Şekil 5.3 : Belirsizlik ile risk arasındaki ilişki. **76**
Şekil 5.4 : Tehdit etkeni kategorileri **78**
Şekil 5.5 : Risk yönetim ve risk değerlendirme süreci **83**
Şekil 5.6 : Risk yönetim şeması **86**
Şekil 5.7 : Siber fiziksel sistemlerin siber güvenliği için risk analiz çerçevesi **93**
Şekil 5.8 : Güvenlik risk analiz modeli **94**
Şekil 5.9 : Güvenlik açığı yaşam döngüsü **95**
Şekil 5.10 : Data ihlal oranları. **102**
Şekil 5.11 : Data kaybına neden olan sebepler ve aktörler **103**
Şekil 5.12 : Bilgi güvenliği anket verilerine göre 3 ana başlık (Yazar tarafından tasarlanmıştır). **104**
Şekil 5.13 : Siber kriz yönetim şeması genel görümümü (Yazar tarafından tasarlanmıştır). **107**
Şekil 5.14 : Bilgi güvenliği baş yöneticisi organizasyon şeması **113**
Şekil 5.15 : Mckinsey & Company Şirketine Göre Siber Güvenlik Organizasyon Yapısı **117**
Şekil 5.16 : Siber güvenlik yatırımları için karar verme süreci **120**
Şekil 5.17 : Örnek bir örtük sınıf analizi **121**
Şekil 5.18 : Türkiye'nin kritik altyapı sektörleri **133**
Şekil 5.19 : USOM organizasyon şeması **135**

SİBER GÜVENLİK YÖNETİM MODELLERİ VE ETKİLERİNİN ARAŞTIRILMASI

ÖZET

Teknolojinin yüksek bir hızla gelişmesine paralel olarak bu gelişmelerin ürüne dönüşmesi de bir o kadar hızlı olmaktadır. Bu nedenle de dijital sistemler kavramı hayatımızın en güncel başlıklarından biri haline gelmiştir. Teknolojinin iyi yanlarını kullanmak her ne kadar keyif verici, işimizi kolaylaştırıcı ve düzenleyici olsa da gerek devlet gerek organizasyon gerekse de bireysel boyutta kullandığımız sistemlerin siber uzay içerinde bulunduğunu unutmamalıyız. Bunun nedeni aslında siber uzayın bizim düşündüğümüz kadar güvenli bir yer olmayışı ve kendimizi siber uzayın kötü yanlarından ve risklerinden korumamız gerektiğidir.

Teknolojideki gelişmelerin ve internete bağlanan cihaz sayısındaki yüksek artışın bir yansıması olarak hayatımıza giren dijitalleşme kavramı çok kısa bir sürede kabul görmüş durumdadır. Yalnızca bireysel olarak değil aynı zamanda da gerek devlet bazında gerekse büyük/küçük çaplı küresel firmalar olsun, tümü bir dijital dönüşüm içerisindedir. Dünya üzerindeki dijitalleşme konusunu rakamlar üzerinden incelemek, genel resmi görmemiz kolaylaştıracaktır. Wearesocial'ın 2019 ocak ayı verilerine göre dünya üzerindeki internet kullanıcı sayısı 4.3 milyardır. Bu sayı 2018 yılının ocak ayı ile karşılaştırıldığında %9,1 artış görülmektedir. Bunun yanı sıra aktif sosyal medya kullanımlarında %9 ve yalnızca mobilde sosyal medya kullanımında da %10 artış görülmektedir.

İnternet dünyasına yön veren en büyük kurumlarından biri olan Cisco firmasının 2019 verilerine göre de internet ağına bağlı olan cihazların sayısı 2022 yılına kadar küresel nüfusun üç katından fazla olacaktır. Raporda 2017 yılında kişi başına düşen internet bağlantılı cihaz sayısı 2,4 olarak belirtilirken, bu sayının 2022 yılında kadar kişi 3,6 cihaz olacağını savunulmaktadır. Yine 2017 yılında yaklaşık olarak 18 milyar olan internete bağlı cihaz sayısının 2022'ye kadar 28,5 milyar olacağını ön görmektedir.

İnternetin hayatımıza ne kadar hızlı giriş yaptığı rakamlarla da görülebildiği üzere, farkındalığında bununla birlikte artması gerekmektedir. Dijital sistemlere yönelik siber saldırıların sayısı ve etkisi gün ve gün artmaktadır. Dijitalleşme kavramı organizasyonları ve devletleri yeni platformlara sürüklemekte ve yeni dijital teknolojiler ile birlikte altyapı yenileştirmeye sürüklemektedir. Dijital sistemlere olan bağımlılığımız her geçen gün artması ile birlikte kuruluşlar, bireyler ve sistemler de siber riske karşı bir o kadar hassaslaşmaktadır. Güvenlik cihazları ve kapasiteleri her ne kadar artsa da siber korsanlarda bir o kadar organize ve karmaşık bir hale gelmektedir. Kötü amaçlı araçlara kolay erişim, artan tehdidin nedenlerinden biridir. Organizasyonların bu yeni kavram yani siber tehdit ile nasıl başa çıkacaklarını bilmeli ve siber saldırıların, tehditlerin sistemlerini ve operasyonlarını nasıl etkileyebileceğini anlamalıdırlar.

Bireysel olarak veya kamu/özel sektör firmalarında kullanılan sistemler fark etmeksizin, internete erişimi olan hatta olmayan tüm cihazlar siber saldırıların ve kötü

amaçlı yazılımların hedefi halindedir. Özellikle bu siber atakların hayatımızı idame ettirebilmemiz için hayati öneme sahip olan elektrik, su, haberleşme, finans, sağlık gibi sektörlere yapıldığı düşünülürse, sonuçları itibariyle halk için çok büyük bir kaosa, can ve mal kaybına ve maddi zarara neden olabilecektir.

Organizasyon perspektifinden bakacak olursak, bir organizasyon için en kritik öneme sahip olan iş sürekliliğidir. Bir siber saldırı veya kötü amaçlı yazılımın şirket içerisine bulaşması ile itibar, paydaş kaybetme, maddi ve manevi zarar hatta üretim yapamama durumları ortaya çıkabilmekte ve bu durum organizasyonun büyük bir kriz içine girmesine neden olabilmektedir.

Son olarak bireysel perspektifi inceleyecek olursak en basit olarak her türlü kişisel verimizin, banka hesap bilgilerimizin olduğu cep telefonları ve bilgisayarlar bireyler için çok değerli konumdadır. Bunun yanı sıra bilgisayarların kameralarına gizli erişim ile insanların izlenmesi, gizli ses kayıtlarının alınması gibi durumlarda göz önüne alındığında bireysel olarak da siber güvenlik karşısında bir farkındalığımızın olması gerektiği aşikardır.

Sonuç olarak, siber ve siber güvenlik kavramını çok iyi anlamak, yaşanmış siber olaylardan çıkarımlar yapmak, farkındalığı arttırmak, siber güvenlik konularındaki araştırmaların incelemek, politikaları belirlemek ve aksiyonlar almak gerekmektedir. Bu bahsedilen konuların hepsi etkili bir siber güvenlik yönetim modelini oluşturan temel faktörlerdir ve siber güvenlik konusunda iyi bir savunma sistemi iyi bir yönetim modelinden geçmektedir.

RESEARCH OF CYBER SECURITY MANAGEMENT MODELS AND EFFECTS

SUMMARY

In parallel with the rapid development of technology, the transformation of these developments into the products is as fast as it is. For this reason, the concept of digital systems has become one of the most up-to-date titles of our lives. Although to use the good aspects of technology is enjoyable, facilitating and organizing our business, we should not forget that the systems we use both in government, organization and individual dimensions are in cyber space. The reason for this is that cyber space is not as safe as we think. So that we should always protect ourselves from bad sides of it.

Although we have adopted technology very quickly in our lives, as technology users, we are just becoming aware of the bad aspects and risks of cyber space such as cyber attacks, hackers, and internet fraud. Especially individuals often have multiple mobile phones, smart watches, computers. Considering that these products are also connected to the internet, they should be more conscious and at times skeptical.

Today, not only individuals and institutions benefit from the internet but also objects. Internet access and digitization has made it possible for people to access the refrigerator, car, television, air conditioning, etc. Furthermore, objects can communicate among themselves.

M2M technology should also be mentioned under the Internet of Things. Because it is almost impossible to do the work of M2M systems with manpower in developed societies today. For example; There are M2M lines that provide remote monitoring and management of devices in many fields such as traffic lights, logistics, electricity, remote surgery, water, natural gas meters, smart grids, air conditioning systems, transportation, medical automation, intelligent agriculture, monitoring and control systems. The magnitude of the chaos caused by a problem in such M2M systems is unpredictable. Here, it shows how digitalization makes our lives easier and how we can face big problems in case of any problems.

As a reflection of the developments in technology and the high increase in the number of devices connected to the internet, the concept of digitalization has been accepted in a very short time. Not only individually, at the same time both in governments and small/large global companies are all in a digital transformation. If we examine the digitalization issue on the world in terms of numbers, it will be easier to see the general picture. According to the January 2019 data from wearesocial, the number of internet users in the world is 4.3 billion. Compared to January 2018, this figure increased by 9.1%. In addition, 9% increase in active social media usage and 10% increase in social media use in mobile.

According to Cisco, which is one of the biggest guiding institutions in the internet world, thanks to the 2019 data, the number of devices connected to the internet network will be more than three times the global population by 2022. In 2017, while the number of Internet-connected devices per capita is 2.4, this number is expected to be 3.6 devices by 2022. Again, it predicts that the number of devices connected to the Internet

will be 28.5 billion by 2022, which was approximately 18 billion in 2017.

It is necessary to increase the awareness of the Internet in the way that we are aware of how fast the internet is entered into our life. The number and effect of cyber attacks on digital systems are increasing day by day. The concept of digitalization drives organizations and states to new platforms so that together with new digital technologies, the infrastructure of organizations and governments have been forced to renew their infrastructure to ensure compliance. As our dependence on digital systems increases day by day, organizations, individuals and systems are becoming more vulnerable to cyber risk. Although security devices and their capacities increase, cyber hackers are becoming more organized and complex as well. Easy access to malicious tools is one of the reasons for increased threat. Organizations should know how to deal with this new cyber threat and understand how cyber attacks can affect their systems and operations.

Regardless of the systems used individually or in public / private sector companies, all devices that access to the Internet or even do not have access to the Internet are the targets of cyber attacks and malware. Especially considering that these cyber attacks are made to the sectors such as electricity, water, communication, finance and health which are of vital importance in order to maintain our lives, they can cause great chaos, loss of life and property and cause material damage for the people.

Estonian cyberattacks and Georgia cyberattacks are the most important examples of attacks on such critical infrastructure. It has shown that cyberattacks, which are the dark side of cyber space, can harm critical infrastructures. And also these attacks shows us very clear how it can cause chaos across the country.

From an organization perspective, business continuity is the most critical for an organization. With a cyber-attack or infiltration of malware into the company, reputation, stakeholder loss, material and non-pecuniary damage, and even the inability to produce can occur and this situation may cause a big crisis in the organization.

Finally, if we examine the individual perspective, mobile phones which has most of all our personal data, bank account information and computers are very valuable for people. In addition to this, as an individually, it is obvious that we should have an awareness of cyber security. For instance, why we need to have an awareness of cyber security is, secretly audio and video recording with unauthorized access to personal computer’s cameras. If people are aware of what could happen, they will be more careful.

Consequently, it is necessary to understand the concept of cyber and cyber security very well, to make inferences from experienced cyber incidents, to raise awareness, to examine researches on cyber security issues, to determine policies and to take actions. All of these issues are key factors in establishing an effective cyber security management model. A good defense system for cyber security goes through a good cyber security management model.

One of the most important points to keep in mind is that cyber security should not be considered only technologically. An effective cyber security model ranges from risk management to human impact on cyber security, from crisis management to regulatory arrangements and organizational structures, and even cyber security investments.

Within the framework of the cyber security management model of the organizations or governments, it is necessary to follow the cyber security problems very closely and

take actions to eliminate the problems as soon as possible. Otherwise it is obvious that both governments and organizations might face with really major cyber problems.

1. GİRİŞ

Siber güvenlik söz konusu olduğunda birçok ülke ve organizasyonun kendi özelinde düzenlemeler mevcuttur. Türkiye de siber güvenlik stratejisinden sorumlu olan ulaştırma, denizcilik ve haberleşme bakanlığı 2013-2014 ve 2016-2019 olmak üzere iki adet ulusal siber güvenlik stratejisi yayınlamıştır. Bunun yanı sıra Türkiye, Avrupa Konseyi Siber Suç Sözleşmesine 10.09.2010 tarihinde katılmıştır. Organizasyon bazında ise her firma kendi özelinde oluşturduğu bir siber güvenlik yönetim modeli çerçevesinde siber saldırılardan korunmaya çalışmaktadır.

1.1 Tezin Konusu ve Önemi

İçinde bulunduğumuz bilgi çağında, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde gelişmesi ve bireylerin bu değişimleri çok da fazla yadırgamadan benimsemeleri, teknolojik gelişmelerin umulmadık bir hızda yayılmasına, teknolojik ürünlere yüksek bir talep olmasına, insanların ve organizasyonların işlerinin kolaylaştığını, yer yer insan iş gücünün azaldığı ve maliyet anlamında tasarruflar yapıldığını ve işlerin otomatikleştirilerek daha hızlı bir iletişim ve tedarik ağına sahip olmanın verdiği avantajları görmeleri ve bunun gibi sayılabilecek binlerce olumlu katkı, siber uzayın/dünyanın da kapılarını açmıştır.

Bu sayede artık bireyler, organizasyonlar hatta devletler zamana ve mekana bağlı kalmaksızın sorumluluklarını büyük bir kısmını yerine getirebilecek esnekliğe sahip olmuşlardır. Günümüzde bireyler akıllı telefon, tablet ve akıllı saat gibi teknoloji ürünleri sayesinde bankacılık işlemlerini, fatura işlemlerini, günlük ev alışverişlerini halledebilir, yemek için sipariş verebilir veya işletmelerindeki gelişmeleri telefonundan takip edebilir duruma gelmiştir. Organizasyonlar ise teknolojik gelişmeler sayesinde insan gücünün yerini alan robotlar sayesinde büyük tasarruflar sağlamış ve her zaman aynı kalitede, beklenilen miktarda ürün elde etmeyi garantilemiştir. Bunun yanı sıra firmalar arasındaki iletişimin kolaylaşması, istenilen veriye istenilen yerden ulaşılması ve büyük veri analizi ile kişiye özel reklamlar düzenlenmesi de organizasyonlar için büyük avantajlar arasındadır.

İletişim araçlarının teknolojinin yardımı ile gelişmesi ile birlikte, insanlar arasındaki iletişimi sağlayan platformların sayısı da bir hayli artmıştır. Aslında yalnızca iletişim sağlayan platform değil, insanların istedikleri anda çok kısa süreler içerisinde şahsi internet sayfaları kurabildiği düşünülürse paylaşım yapılabilecek binlerce hatta yüz binlerce internet sitesi bulunmaktadır. En büyük sorunlardan bir tanesi de bu kadar çok paylaşım yapılan ortamın olduğu bir dünya da "doğru bilgiye" ulaşmanın zorluğudur. Sosyal medya kullanımını rakamlar ile inceleyecek olursak 2016 yılında dünya üzerinde yaklaşık 2,3 milyar kullanıcı varken 2019 yılı itibariyle 3,5 milyar aktif sosyal medya kullanıcı bulunmaktadır. Burada atlanılmaması gereken nokta sosyal medyalara üye olabilmek için kişisel verilerin rıza dahilinde sitelerin kullanımına veya sayfaların veri tabanına kayıt edilmesine izin verilmesinin zorunlu kılınmasıdır. Ayrıca sitelerdeki kişisel paylaşımlar da ilk bakışta her ne kadar masum gözükse de kişisel bilgi güvenliği riske atılmaktadır.

Sosyal ağlar ile bireyleri internet dünyasına hızlı girişine paralel olarak devletler de sistemlerini internet ortamına taşımışlardır. E-devlet tarzında yapılan uygulamalar sayesinde devlet daireleri üzerindeki yükler hafifletilmiş olup, vatandaşların tüm verileri tek bir sistem üzerinde birbiri ile entegre bir hale gelmiştir. Bu sayede de bilgiye erişim kolaylaşmış ve devlet nezdinde işlemler hızlanmıştır. E-devlet sistemi olarak devlet yönetimini internet ortamına taşıma konusunda en başarılı ülkelerden bir tanesi Estonya'dır. Estonya ülke genelinde toplumu %98'i bir şekilde internet kullanımı yapan bir ülke olarak internetin tüm nimetlerinden yaralanmaktadır. Fakat 2007 yılında karşı karşıya kaldığı siber saldırılar nedeni ile ülkenin kritik altyapılarını kullanamaz hale gelmiş ve son çare olarak da tüm ülkenin internetini dış dünyaya kapatma kararı almıştır. Bu ve bunun gibi birçok örnek bize gösteriyor ki siber dünyanın olumlu yanları olduğu kadar dikkat edilmesi gereken aksi taktirde yıkımı çok büyük olan olumsuz yanları da bünyesinde barındırmaktadır.

Günümüzde internetten sadece bireyler ve kurumlar değil nesneler de faydalanmaktadır. İnternet erişimleri sayesinde insanların, buzdolabından arabaya televizyondan klimaya kadar erişimleri olanaklı hale gelmiştir. Bunun da ötesinde nesneler de kendi aralarında iletişim kurabilir hale gelmiştir. Hayatımızı kolaylaştıracak robotların Ekonomik Kalkınma ve İş birliği Örgütünün hazırladığı raporu belli bir periyot içerisinde inceleyecek olursak internete bağlı cihaz sayısı 2010 yılında 80 milyon iken, 2015 yılında bu sayının 290 milyona yakın bir sayı olacağı ve

2020 yılında da 1 milyarı aşkın cihazın internete bağlanabileceği öngörülmüştür [146].Türkçe karşılığı nesnelerin interneti olan Internet of Things (IOT) kavramı ile internete bağlanan cihazların sayısının her geçen gün artması beklemek çok da yanlış olmayacaktır. İşte bu noktada bizler birçok firmadan birçok farklı üreticiden farklı yazılımlar kullanarak ürettiklen ürünlerle karşı karşıya kalacağız. Ürünler, kimi zaman farklı üreticilerin ürünleri ile iletişim sağlarken sırasında bazı güvenlik açıkları çıkacaktır. Bu durumda da ne kadar çok internete bağlanan cihaz ortaya çıkarsa siber açıklar ile ilgili sorunlarla karşılaşma riskin de bir o kadar artmasını beklemek yanlış olmayacaktır.

Nesnelerin internetinden bahsetmişken M2M teknolojisinden de bahsetmek gerekmektedir. Çünkü M2M sistemlerin yaptığı işleri günümüzde gelişmiş toplumlarda insan gücü ile yapmak neredeyse imkansızdır. Örnek vermek gerekirse; trafik ışıkları, lojistik, elektrik, uzaktan ameliyat, su, doğalgaz sayaçları, akıllı şebekeler, iklimlendirme sistemleri, ulaşım, tıbbi otomasyon, akıllı tarım, görüntüleme ve kontrol sistemleri gibi pek çok alanda cihazların uzaktan izlenmesini ve yönetilmesini sağlayan M2M hatlarında yaşanacak bir sorunun neden olacağı kaosun büyüklüğü tahmin dahi edilemez.

İnternetin hayatımızın hangi aşamalarında ne seviyede olduğunun örnekleri, yararları ve zararlarına verilebilecek daha yüzlerce örnek mevcuttur. Anlaşılması gereken ise bilişim dünyası hızla ilerlemekte ve siber dünya her gün biraz daha değişmektedir. Öyle ki internet, günümüzde kritik altyapı sektörleri için yaşamsal bir öneme sahip hale gelmiştir. İlk bakışta insan hayatına çok büyük yararlar sağlayacağı düşünülse de zaman içerisinde bu bağımlılığın siber teröristler, bilgisayar korsanları gibi kötü niyetli kişi ve grupların eğlence, menfaat hatta iddia uğruna masum kişi, kurum veya devletler için çok büyük zararlara neden olabileceği görülmüştür.

Çok net bir şekilde görülmektedir ki dijitalleşme, sosyal değişime yol açmıştır. Bu değişim, kuruluşların süreçleri, karmaşık işlemleri ve altyapıyı kontrol etme şeklini değiştirmektedir. Daha önce de belirtildiği gibi dijital dönüşümünde ardında kolaylıklar kadar tehditler de büyümektedir. Gerek bireysel gerek ise ülkeler gibi büyük aktörler, kritik altyapılara saldırarak çok kötü sonuçlara neden olabilmektedir. Bu da yeni bir savaş türünün doğduğunun bir numaralı kanıtıdır. Dijitalleşme ile suçluların ve bilgisayar korsanlarının suç eylemlerini işleyebilecekleri yeni bir platform ortaya çıkmıştır.

Gerek ülke gerekse özel sektör organizasyonu olsun şirketin veya ülkenin gizli bilgileri, kişisel verileri, şirket sırlarını, devlet sırlarını, yüksek riskli operasyonlarını, askeri stratejik dokümanlarını, kritik altyapı ve devlet fonksiyonlarını korunması gereken önemli olan değerlerdir. Bu durum, kuruluşların ve hükümetlerin kendi faaliyetlerinin zayıflıklarının farkında olmaları, değerlerini ve varlıklarını korumanın bir yolunu bulmaları gerektiği anlamına gelir. Bu konuda risk ve güvenlik açığı analizleri, insan kaynakları yönetimi, teknolojik gelişme ve kurulum, işletme ve bakım, operasyonel yönetim, teknolojik yatırımlar gibi konular ele alınmalı ve ilgili siber güvenlik hususları göz önünde bulundurulmalıdır.

Artık günümüzde internetin bu denli hayatımıza girmesi ile birlikte her devletin, organizasyonun ve bireyin kabul edilen bir nokta var ki o da gerek kritik altyapıların (örneğin internet oylama sistemleri, sağlık, iletişim, bankacılık sistemleri,…) gerek özel sektör organizasyonlarının işini sürdürebilirliğin gerekse kişisel verilerin güvenceye alınması için siber güvenlik yönetimi modelinin gerekli olduğudur. İyi hazırlanmış ve uygulama adımları kontrol alanları belli olan bir siber güvenlik yönetim modeli ile siber saldırılar karşısında başarı da kolay bir şekilde yakalanacaktır. Bununla birlikte farkında olunmalıdır ki, bir tane doğru siber güvenlik yönetim modeli yoktur. Dünyanın dört bir yanında bulunan her bir ülke, her bir organizasyon kendi içerisinde farklı bir siber güvenlik yönetimine sahip olabilir. Hatta günümüzde çok sayıda firma tarafından siber güvenliğin öneminin daha yeni yeni anlaşıldığını düşünmekteyim. Bu durumun gerçekleşmesindeki en önemli nedenlerden bir tanesi de şirketin üst düzey yöneticilerinin teknolojinin nerelere gittiğini iyi görememeleri ve siber saldırıların başlarına ne gibi işler açacaklarının farkında olmamalarıdır.

Siber güvenlik yönetim modeli çerçevesinde alınan stratejik kararlar her organizasyonun ve/veya ülkenin siber saldırılara karşı duruşunu belirtmektedir. Tabi bu durumda da bir firma için göz ardı edilebilen bir risk seviyesi başka bir firma için önlem alınması gereken önemli bir risk olarak görülebilir. Burada en önemli nokta sistemlerin çalışabilirliği için gerekli asgari koşulların sağlanması ve risklerinde bu çerçevede değerlendirilmesidir. Kısacası tek bir siber güvenlik yönetimi modeli olmamasına rağmen, her organizasyon ve/veya devlet kritik kaynaklarını dikkatli bir şekilde yönetme ve koruma gerekliliğinin farkındadır. Dünyadaki hükümetlerin ve organizasyonların, kritik altyapılarına güvenlik sağlamak için temel motivasyonları bu kritik altyapıların devlet gözünden bakılacak olursa ülkenin ve halkın refahını

etkileyebilecek, eksikliğinde de bir kaos ortamı doğurabilmesidir. Motivasyonlara organizasyon gözünden bakacak olursak, hizmetin sağlanamaması, maddi kayıpların oluşması, itibar kaybı ve şirketin borsa da toplam değerinin düşmesi gibi durumların ortaya çıkmasını engellemektir.

Siber uzayın genişlemesi ve siber saldırıların sonuçlarının ağırlığının artmasına paralel olarak etkili bir siber güvenlik yönetim modeli araştırma çalışmaları da hızlanmıştır. Her ne kadar her ülke ve organizasyon kendi içerisinde bir yönetim modeli araştırması yapsa da ortak kanı, ülkelerin kritik altyapıların siber güvenliğinin sağlanması konusunda uluslararası platformda iş birliği yapmaları gerektiğidir. Bunun en büyük nedenlerinden bir tanesi siber uzayın bir coğrafi sınıfının olmayışıdır. Amerika'da yaşayan bir bilgisayar korsanı sağlıklı bir internet bağlantısı olduğu sürece dünyanın her bir yanına siber saldırı geçekleştirebilmektedir. Bu konuya ülkeler arasındaki siyasi gerginliklerin bir yansıması olarak yaşanan ülkeler arası DDoS saldırıları gösterilebilmektedir. Bu nedenle de tespit edilen bir bilgisayar korsanı dünyanın diğer ucunda olabileceğinden hangi ülke sınırları içerisinde ise bazı durumlarda yerel yönetimden de destek istenebilir.

Yalnızca kendi başlarına gelen saldırılar için değil, aynı zamanda da kötü amaçlı bir yazılımın dünya genelinde çok kısa sürede yayılabileceği daha önce yaşanan örneklerden de görüldüğünden uluslararası iş birliği çok büyük önem taşımaktadır. Bunun yanı sıra kamu-özel sektör birlikteliğini arttırmak gerekmektedir. Bahsedilen kritik altyapıların birçoğu özle sektörde bulunan organizasyonlar tarafından yönetilmektedir. Bu nedenle de özel sektörlerin de kendi içerilerinde etkili bir siber güvenlik yönetimine sahip olmaları gerekmekte ve kamu tarafındaki ilgili kuruluş tarafından da denetlenmelidir. Siber güvenlik konusunda gerek kamu-özel sektör gerekse özel sektör-özel sektör arasındaki bilgi paylaşımından her zaman olumlu sonuçlar çıkacaktır.

Fakat özel sektörün belirli saldırılar hakkında bilgi paylaşmaya daha az eğilimli olduğu, ancak bu bilgilerin siber güvenliğin güçlendirilmesine önemli ölçüde katkıda bulunabileceği belirtilmektedir. Özel sektörün, altyapılarında tespit ettikleri siber güvenlik saldırıları ve güvenlik açıkları ile ilgili bilgileri paylaşmasının mümkün olmadığı, bunun nedeninin bu bilgilerin organizasyonun itibarını, güvenini sarsacağı ve toplumun veya iş ortaklarının iş birliğinin önceliğini yeniden düşünebileceği varsayılmaktadır [147].

Siber güvenlik konusunun yalnızca teknoloji ile kontrol altına alınabilecek bir durum olduğu konusunda çok geniş bir yanlış anlayış bulunmaktadır. Siber güvenlik konusu 360 derece uçtan uca ele alınması gereken bir konudur. Yalnızca teknolojik açıdan olaya yaklaşmak, yalnızca tek yöne bakan bir pencereden her yeri görmeye çalışmak gibidir. Bir yer çok net bir şekilde görebilir fakat bu durumda diğer taraflarda ne olduğundan bir haber olunur.

Bu nedenle tezin de konusu olan etkili bir siber güvenlik yönetim modeli oluşturmanın anahtarı ancak sürecin tamamına hakim olmak ve uçtan uca bir şekilde siber güvenlik olgusunu ele almaktır.

Bilgiler ışığında siber güvenlik yönetim modeli oluşturulması en temelden başlamalıdır. Siber kelimesinin kavramsal anlamını tam olarak anlamak ve siber uzaya tam olarak hakim olmak gerekmektedir. Daha önce yaşanan dünya siber tarihine yön vermiş siber saldırıların ve virüs yayılımlarının analizi, siber saldırıları anlamak için ilk aşamada çok değerli bir veridir. Fakat tabi ki her şey bununla sınırlı değildir. Siber güvenlik yönetim modelini insan, teknoloji, yönetim, yatırım, yasal mevzuat, kriz süreci, risk yönetimi gibi başlıkların bir bütünü olarak ele almak gerekmektedir.

En yüksek seviyedeki teknolojik cihazların olduğu bir organizasyonda dahi çok çok basit bir insan hatası ile çok büyük bir siber sorunlar oluşabilmektedir. Yüksek güvenlikli bir kurumda, siber güvenlik farkındalığı ve bilinci olmayan bir çalışanın şirket bilgisayarına takmış olduğu bir harici bellek veya oltalama maili olarak gelen bir mailin farkına varmayarak maile tıklayarak, eklentiyi bilgisayarına indirmek ve çalıştırmak gibi çok basit hatalar ile tüm organizasyonun içerisine kötü amaçlı bir yazılımın sızması hiç de sürpriz olmayacaktır. Bu örnek dahi aslında siber güvenlik konusunun yalnızca teknolojik açıdan ele alınamayacağının en güzel örneklerindendir.

Peki etkili bir siber güvenlik yönetim modelinde neler olması gerekmektedir? Bu sorunun cevabına gelecek olursak en temelde siber güvenlik yönetim modelinin çok iyi bir risk yönetimine ihtiyacı vardır. Risk yönetimi sayesinde en genel olarak risklerin tespit edilmesi ve sorunun daha yaşanmadan önlenmesi sağlanabilmektedir. Bunun yanı sıra risk yönetimi sayesinde belirlenecek kriterler ile teknolojik yatırımlarında yönü belli olacaktır. Risk matrisi değerine göre düşük seviyedeki bir riskin önlenmesi için boşu boşuna çok büyük yatırımların yapılmasına gerek yoktur. En makbul olan risk ile bu riskten korunma yolunca harcanan çaba ve maddi

imkanların birbiri ile örtüşmesidir. Ayrıca basit sorunlar için kişi ve kaynak ayrılmasına da gerek kalmayacaktır. Her firma için tolere edebilecekleri risk seviyesi değişmek ile birlikte bu tamamen organizasyonun kararıdır.

Öte yandan insan faktörüne gelecek olursak, dünyanın son dönemdeki en büyük virüs yayılımı olan Wannacry virüsünü örnek vermek tam olarak konu ile örtüşmektedir. Wannacry virüsünün dünya üzerinden çok büyük bir hızla yayılması ve başarılı olmasında tabii ki sistem açıkları olduğu gibi asıl büyük pay insanların virüslere ve siber uzaya karşı olan bilgisizliği ve farkında olmama durumudur. Wannacry virüsü internet üzerinden gönderilen bir elektronik posta içerisinde bulunan bir dosyanın bilgisayara indirilerek tüm dosyaları şifrelemesi ile bilgisayar kullanılamaz hale gelmesine neden olmaktadır. Hatta bazı virüsler çok masun görülerek sanki hiçbir zarar vermiyormuş gibi boş bir dosya ile organizasyona sızar ve çok uzun süreler sistem açıklarını, bireylerin yetkilerini keşfetmek için kullanılabilir. Eğer insanlar bu tarz elektronik postalar hakkında biraz daha fazla farkındalığa sahip olmuş olsaydı belki de Wannacry virüsü bu kadar çok yayılmayacaktı. Ya da başka bir örnek olarak, Stuxnet virüsünün İran'ın internete dahi kapalı olan üretim tesisine bir taşınabilir harici bir bellek içerisinde, bilinçsiz bir çalışan tarafından taşındığı ve bu virüsü bulaştırıldığı çok da uzak bir ihtimal değil gibi durmaktadır. Bu iki örnek dahi internete dahi bağlantısı olmayan ortamların aslında tehdit altında olduğunun, bu nedenle insan hatalarının önüne geçmenin tek yolun çalışanların yetkilerini kontrol etmede, eğitim vermede ve farkındalıklarını arttırmada olduğunu işaret etmektedir.

Şirket çalışanları üzerinde siber bir farkındalık beklemek için öncelikle yönetim seviyesinde bir siber güvenlik bilinci başlamalıdır. Organizasyon içerisinde alınan kararların hiyerarşik bir yapı izlediği düşünülürse, siber güvenlik ile ilgili bir yöneticinin şirkette olması ve sadece bunun üzerinde çalışması, çalışan bilincini de olumlu yönde etkileyecektir. Bu nedenle son dönemin yeni pozisyonu olan bilgi güvenliği baş yöneticisinin organizasyonlar için çok yararlı olacağı düşünülmektedir. Yalnızca farkındalık ile ilgili değil aynı zamanda da siber savunmanın temeli olan teknolojinin yatırım tarafında da bilgi güvenliği baş yöneticisi ve ilgili ekipler söz sahibi olacaktır. Doğru yatırımlar ileri de karşılaşılması olası siber saldırılara karşı hem teknolojik avantaj hem de eğitim, konferans vs ile de farkındalık sağlayacaktır.

Güvenlik ile ilgili teknolojilerin sürekli gelişmesi ile birlikte organizasyonlar kendilerine avantaj sağlasalar da siber saldırı ve insan üretimi ile yapılan yazılımlarda

açıkların sıfır seviyesine düşürülmesi neredeyse imkansızdır. Bu nedenle de her ihtimale karşı organizasyonlar her zaman her an bir siber saldırı ile karşı karşıya kalacakmışçasına tetikte olmalı ve bir kriz yönetimi belirlemelidir. Kriz anında panik yapmak yerine önceden belirlenen adımlar uygulanmalı ve en az hasar ile saldırıların ve kayıpların atlatılması sağlanmalıdır.

Daha önce siber saldırı ile ülkelerin de organizasyonların da karşı karşıya kalabileceğini belirtmişti. Siber uzayda sınır yoktur. Bu nedenle dünyanın iki ucundaki bir grup bilgisayar korsanı birleşerek çok farklı bir hedefe toplu saldırı yapabilmektedir. Ayrıca herhangi bir ülkede başlayan virüs yayılımı çok kısa bir sürede tüm dünya da yayılabilmektedir. Bu nedenle siber uzay konusunda tüm dünya ülkeleri iletişim halinde olmalıdır. Tabi ki her ülke önce siber güvenliğe yönelik kanunları ile halkını, kamu kurumlarını ve özel sektör organizasyonlarını güvence altına almalıdır. Bu konuyu sadece siber olarak değil bilişim olarak da değerlendirmek gerekmektedir. Bir bankaya veya kuruma siber saldırı yapmak bir bilişim suçu olduğu gibi kişisel verilerin izinsiz kullanılması da bir bilişim suçudur.

Özetle toplayacak olursak, siber uzay günümüzde en çok üzerinde durulması gereken konulardan bir tanesidir. Siber uzayın karanlık tarafı olarak görülen siber saldırılar, en çok dikkat edilmesi ve dikkat edilmemesi halinde çok büyük sorunlara yol açacak bir kavram olarak görülmektedir. Siber sorunlar ile baş etmenin en etkili yolu da olaya uçtan uca hakim, 360 derecelik bir bakış açısı ile kurulmuş bir siber güvenlik yönetim modeli olarak görülmektedir.

1.2 Tezin Amacı ve İçeriği

Tezin amacı, öncelikle siber güvenlik konusuna ve eğer siber güvenlik konusuna yeterince dikkat edilmez ise gerek kamu organizasyonları gerek özel sektör organizasyonları gerek bireysel gerekse de devletler seviyesinde ne denli büyük zararlara yok açabileceğine ve siber güvenlik konusunun sadece teknolojik cihazlar ile olamayacağına, siber güvenlik yönetim modeli içerisinde çok fazla etken olduğuna dikkat çekmektir.

Özellikle Avrupa Birliği, yaptığı güncellemeler ile siber güvenlik konusunda detaylı bir düzenlemeye sahiptir. Avrupa Birliği, siber güvenlik konusunda devletleri bir araya getirerek oluşturduğu, Budapeşte'de imzalanan Avrupa Birliği Siber Suçlar sözleşmesi

ile siber güvenliğin ne denli önemli olduğuna dikkat çekmekte ve bu konu ile de kanuni düzenlemeler sağlamaktadır. Bunun yanı sıra Avrupa Konseyi üyesi olsun veya olmasın bu sözleşmeyi ülkelerin imzalayabilir olması siber güvenlik konusunun coğrafi sınırlarının olmadığının da bir kanıtıdır. Avrupa Komisyonu bu sözleşme ile birlikte bireysel ve organizasyonel boyutta siber güvenlik konusunda yüksek seviyede bir korumanın bir ayağını oluşturmaktadır.

Toplumların, devletlerin ve organizasyonların birer bilişim toplumuna dönüşmesi ile birlikte sayısız veri dijital ortama taşınmıştır. Bunun yanı sıra sistemlerin etkili bir şekilde çalışabilmeleri, hizmet verebilmeleri dijital dünyada yalnızca teknolojik sistemler ile mevcut duruma gelmiş durumdadır. Devlet sırlarının saklandığı veri tabanlarından bankaların para transferlerine, haberleşme sektöründen sağlık sektörüne, ulaşım sektöründen kritik altyapılara kadar her şeyin yönetimi dijital bir şekilde yapılmaktadır. Bu nedenle bu sistemlerde ortaya çıkabilecek bir sorun büyük kaoslara ve maddi, manevi ve itibar kayıplarına neden olacaktır. İşte bu sebeple bu sistemlerin ve verilerin siber saldırılardan korunması için gerek teknik/fiziksel ve gerekse yasal önlemlerin alınması gerekmektedir.

Tez çalışması kapsamında bilişim dünyasının en sıcak gündemi olan siber güvenlik ile ilgili yapılan araştırmalar, dünya siber tarihine yön veren önemli siber savaşlar ve zararlı yazılımlar yayılımları, bilgisayar korsanlarının bilgisayar korsanlığı yapma motivasyonları, siber güvenlik konusunun ortaya çıkması ile birlikte gerek özel gerekse kamu sektöründeki organizasyon şemalarına yeni eklenen kutucuklar ve bunların görev tanımları, siber saldırı ile karşı karşıya kalınan bir kriz anında yönetimin nasıl olması gerektiği, Türkiye'deki yasal mevzuat ve son olarak da siber güvenlik ile ilgili olarak Türkiye'deki çalışmaların neler olduğu bulunmaya çalışılacaktır. Buralardan çıkarılan sonuçlar ile birlikte etkili bir siber güvenlik yönetim modelinde olması gereken alt başlıklar tespit edilmeye çalışılacaktır.

2. SİBER GÜVENLİK KAVRAMININ TEMELLERİ VE TERMİNOLOJİ

2.1 Siber

Siber kelimesinin Türk Dil Kurumuna (TDK) göre tam olarak bir karşılığı bulunmamak ile birlikte, siber kelimesinin nereden geldiğini anlamak için siber ile ilgili diğer terimler daha ortaya çıkmamışken var olan sibernetik kavramını anlamak gerekmektedir. İngilizce' de cybernetics olarak geçen kavram dilimizde sibernetik olarak geçmektedir [1]. Wiener kitabında [2] hayvanlardaki kontrol ve iletişim süreçleriyle makinelerdekinin benzer şeyler olduğuna dikkati çekti. Bu nedenle Wiener sibernetik'i ilk olarak makineler ve hayvanlarda kontrol ve iletişim çalışması olarak tanımlamıştır. Daha sonra bu kavram farklı alanlarda da kullanılmıştır.

Bu bilgilerin de ışığından siber terimi insan yaşamı ile makinelerin yönetişimi şeklinde birbirleri ile bilgi alışverişi olarak tanımlanmaktadır [1]. Günümüzde ise daha çok sanal erişim, sanal yaşam, bilgisayar ağlarına ait olan, sanal gerçeklik vb olarak kullanılmaktadır.

2.2 Siber Uzay/Alan/Ortam

Bilgisayar bilimleri, bilişim, haberleşme kısacası teknoloji alanındaki gelişmelerin artması ile birlikte hayatımıza halihazırda yeni terimlerde girmiş bulunmaktadır ve ilgili alanlardaki gelişmelerin artması ile daha da yeni kelimelere tanık olmak bizi şaşırtmayacaktır. Bunlardan biri olan siber uzay kavramı İngilizce' de cyberspace olarak tanımlanmakta ve dilimizde siber ortam, siber alan olarak da karşılık bulmaktadır.

Siber uzay kavramı ile kez 1982 yılında bilim kurgu romanlarıyla bilinen William Gibson tarafından "Burning Chrome" adlı romanda kullanılmıştır. Bu terim popüler kültür tarafından sıkça kullanılmaya başlanmış olup, bilgisayarlar ve bilgi teknolojilerinden internete kadar teknolojileri betimlemek için popüler televizyon şovları ve filmlerde kullanılmıştır [3].

Siber uzay kavramı farklı şekillerde tanımlara sahiptir. Bu tanımları inceleyecek olursak:

- Amerika Birleşik Devleti hava kuvvetleri için hazırlanan kitaba göre 5.boyut olarak tanımlanan siber uzay, yeryüzü, hava, deniz hatta uzaydan bağımsız ve iletişim altyapılarını kullanan sanal bir ortamdır [4].
- Bilgisayar ağlarının oluşturduğu, üzerinde iletişimin gerçekleştiği kavramsal ortamdır [5].
- İnternet, iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağımlı ağların oluşturduğu bilgi ortamındaki küresel bir alandır [6].

Yapılan tanımlar incelendiğinde siber uzayın aslında halen büyümekte olan, insanlara her türlü elektronik bilgiye erişime olanak sağlayan yeni bir dünya olarak tanımlanabilmektedir. Siber uzay sayesinde coğrafi sınırlar ortadan kalmış olup, insanlar arasında bilgisayar ve haberleşme sistemleri sayesinde tam bir bağlantı kurulmuştur.

Biraz önce de bahsedildiği gibi siber uzay ilgili birden fazla tanım bulunmaktadır. Bu tanımlar da göz önünde bulundurulduğunda siber uzay ile ilgili aşağıdaki çıkarımları yapılabilmektedir.

- Siber uzay adından da anlaşılacağı üzere, zihnimizde olan gerçekliğin ve sanalın birleşenlerinden oluşan bir sanal boşluktur. Gerçek bir fiziksel lokasyonu olmamak ile birlikte, siber uzay dünya için dijital bütünleyici olarak değerlendirilebilmektedir.
- İnsanlar, siber uzaya fiziksel cihazlar ile yapay işlemci fonksiyonları sayesinde ulaşabilirler. Bu nedenle bu cihazlar siber uzayın sınırı veya siber uzaya açılan pencere olarak değerlendirilebilmektedir.
- Etkileşim ve iletişim zamandan ve boşluktan bağımsızdır.

2.3 Siber Terörizm

Siber terörizm kavramını anlamaya çalışmadan önce terör kavramını anlamak, terör kelimesinin kökeninin ne olduğunu, terör kavramının hayatımızda ne kadar zamandır olduğunu incelemek faydalı olacaktır. Bu incelemenin nedeni günün sonunda çok eski

zamanlarda dahi hayatımızda olan terör kavramının motivasyonu ile son dönemde teknolojideki gelişmelerin olumsuz bir yanı olarak ortaya çıkan siber terörizm kavramının motivasyonlarının benzer olduğunu açıkça gözler önüne sermektedir.

Genel olarak kabul edilen tam bir tanımı olmak ile birlikte terör kavramı, içerisinde şiddet barındıran, zaman ve mekandan bağımsız olarak psikolojik ağırlıklı olarak toplum ve bireyler üzerinde korku ve kaos yaratmayı hedefleyen, hedefi genellikle politik olan, insanlık için maalesef hayatının bir parçası olmuş bir şiddet hareketidir. Terör kelimesi Latince' de korkutmak, ürkütmek veya sindirmek anlamlarına gelen "terrere" kelimesinden dünya dillerine girmiştir [7].

Terörizm kelimesi genellikle birbiri ile bağlantılı ve direkt olarak bir politik hedefe karşı sürekli olarak yapılan saldırı ve/veya olay durumundan anlam kazanmaktadır. Bozdemir'e göre terör, politik olaylara karşı ortaya çıkan bir stratejik yaklaşım olarak tanımlanmıştır. Bu yaklaşım kendi içerisinde sürekli olarak bir örgütlenmiş, sistematik bir duruş ve sürekli olarak sürdürülen bir terör methodu ile hareket etmektedir [8].

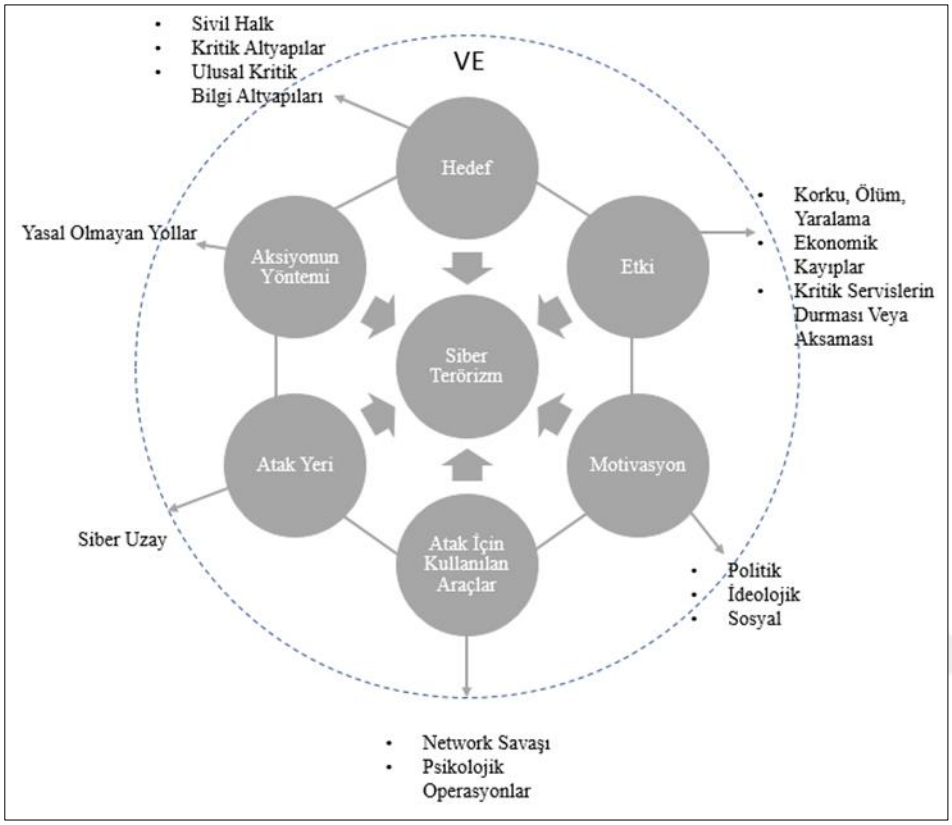
Terör ve terörizm kavramlarının açıklamaları ışığından siber terörizm kavramı, ağ yapılarına, bilgisayarlara kısacası bilginin saklandığı herhangi bir yere yapılan kanunsuz atakların ve tehditlerin özellikle hükümetleri ve/veya politik ve sosyal açıdan insanları hedef alması olarak tanımlanmaktadır. Bir saldırıyı siber terörizm olarak sınıflandırmak için yapılan saldırının insan, mal, mülk karşısında bir zarar verme durumu veya en azından toplumda bir korku yaratması gerekmektedir [9].

Siber terörizm, bilgi savaşları ve siber suçun karışımı olarak düşünülebilmektedir. Fakat bilgi savaşları ile siber terörizm arasında çok büyük ve keskin bir fark bulunmaktadır. Siber terörizm planlı bir şekilde yapılan politik bir ataktır ve bu atak, gizli gruplar veya bireyler tarafından bilgi, bilgisayar sistemleri, verilere karşı olarak savaş dışı hedeflere zarar verecek şekilde yapılmaktadır. Fakat siber terörizmden daha eski bir kavram olan bilgi savaşları ise düşmanın kaybetmesi için uluslar tarafından yine bilgi, bilgisayar sistemleri, verilere karşı yapılan saldırıdır [10].

Kısacası siber terörizm ortaya çıktığında hedef ne olursa olsun en azından yan etki olarak toplumda korku, endişe ve kendini güvende hissetmeme durumu da ortaya çıkmaktadır.

[11] 'a göre siber terörizm ile ilgili Şekil 2.1'de gösterilmiş olan kavramsal çerçeve oluşturulmuştur ve bu çerçeve içerisinde 'AND (VE)' kavramının neden kullanıldığı,

kavramsal çerçeve içerisindeki bileşenlerin tamamı bir araya gelerek siber terörizm kavramını oluşturması olarak açıklanmaktadır. Buradan da anlaşılacağı üzere siber terörizm kavramının oluşması için çerçeve içerisindeki her bir bileşen hayati değer taşımaktadır. Bir veya birden fazla bileşenin eksik olması durumundan siber terörizm kavramı oluşmayacaktır.



Şekil 2.1 : Siber terörizm kavramsal çerçeve [11].

Terör ve siber terörizm tanımları incelendiğinde aslında en temelinde ikisinin de toplumda kargaşa çıkarmayı ve toplumda korkunun egemen olmasını istediklerini hedefledikleri açıkça gözükmektedir. Fakat çoğu olayda olduğu gibi toplumun içinde yer aldığı bir olayda etki küçük olmayacaktır.

Toplumdaki olayların nasıl zincir etkisi yarattığına örnek verecek olursak, metro çalışanlarının grev yaptıkları bir ortamda, insanlar sabah işlerine ulaşmaları, sınavları varsa sınav yerlerine ulaşmaları kısacası günlük hayatlarını devam ettirebilmeleri için toplu taşıma olarak metro dışında yalnızca otobüs kullanabileceklerdir. Bunun yanı sıra bisiklet ve şahsi araçlar da tercih edilecek ulaşım araçlarından olacaktır. Fakat böyle bir durumda otobüs duraklarında insan izdihamları, arttırılan otobüs seferleri nedeniyle trafik sıkışıklıkları, kargaşa nedeni ile insanların sinir ve stres seviyelerinin

artmaları bir hayli olası bir durum olarak ortaya çıkmaktadır. Peki metro çalışanlarının yapmış olduğu bir grev nelere neden olabilir? Bir ambulans hastaneye yetişemeyebilir, itfaiye acil ihtiyaç duyulan bir lokasyona zamanında erişemeyebilir, sınavını kaçıran bir öğrencinin tüm emekleri boşa gidebilir veya iş görüşmesini kaçıran bir kişi hayatındaki büyük bir şansı da kaçırmış olabilir.

Yani kısacası eğer toplumun merkezde olduğu olumlu veya olumsuz bir durum var ise o durumun sonuçlarını tahmin edebilmek ne yazık ki çok da kolay olmayabilir ve belki de beklenilenden çok daha fazla bir etki yaratabilmektedir.

Biraz önce verilen metro çalışanlarının grev örneğinin nedeni 2018 Ulusal Risk Raporunun siber atakların nelere sebep olabileceklerini gösterdiği birbiri ile bağlantılılık raporudur.

2018 ulusal risk raporuna göre teknoloji başlığı altındaki ulusal riskler ve tanımları Çizelge 2.1'de gösterilmektedir.

Çizelge 2.1 : 2018 küresel risk raporuna göre teknoloji başlığı altındaki ulusal riskler ve tanımları [12].

ULUSAL RİSK	TANIMLARI
1. Teknolojik gelişmelerin olumsuz yanları	İstemli veya istemsiz olarak ortaya çıkan teknolojik gelişmelerin (yapay zeka, yerbilimi mühendisliği, sentetik biyoloji) olumsuz yanları, insan, çevre ve ekonomik zarara neden olabilecektir.
2. Kritik bilgi altyapılarının ve ağ yapılarının çökertilmesi (Kritik bilgi altyapılarının çökmesi)	Siber bağımlılığın artması ile birlikte kritik bilgi altyapılarının ve ağ yapılarının kesintiye neden olabilecek zayıflıkları ve açıkları da artmaktadır. Bu altyapılara uydu, internet, vb. örnekler verilebilir. Böyle bir durum, geniş çağlı bir kesintiye neden olabilecektir.
3. Büyük kapsamlı siber ataklar	Büyük boyutlu siber ataklar ve kötü amaçlı yazılımlar yüksek ekonomik kayıplara, jeopolitik gerginliklere ve çok geniş bir şekilde internete olan güvenin kaybolmasına neden olabilecektir.
4. Çok büyük boyutta veri dolandırıcılığı ve veri hırsızlığı	Özel veya resmi verilerin istismar edilmesi, kanuna aykırı bir şekilde suistimal edilmesi, tahmin edilmez boyutlarda zararlara neden olabilecektir.

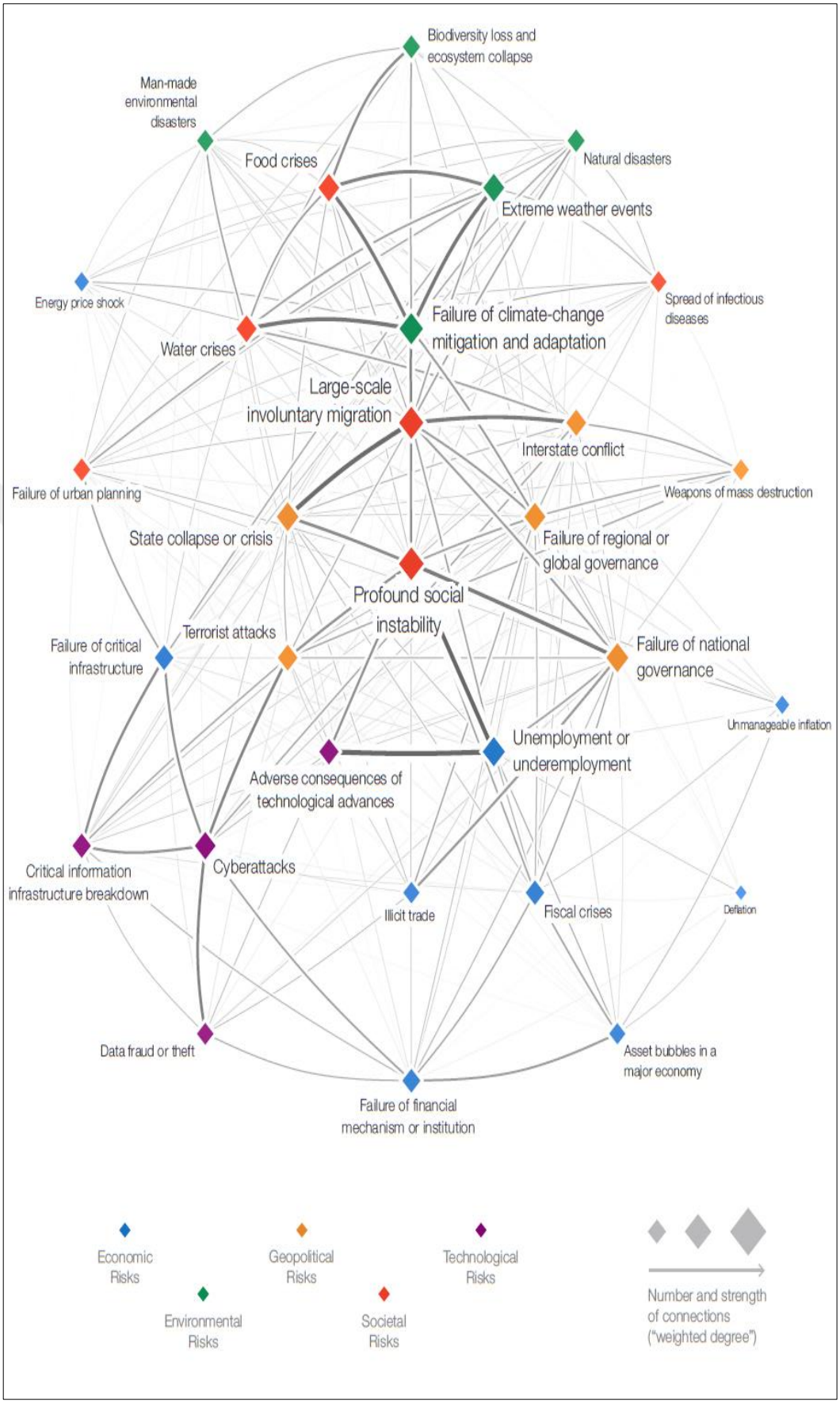
Şekil 2.2'den de açıkça görüleceği üzere siber terörizmin en çok hedef aldığı ulusların kritik bilgi altyapılarının çökmesi (Critical information infrastructure breakdown) durumu birçok başlık ile bağlantılı durumdadır. Şekil 2.2'yi biraz daha dikkatli inceleyecek olursak, kritik bilgi altyapılarının çökme durumunun, siber atak ile direkt olarak bağlantılı olduğu çok net bir şekilde görülmektedir. Diğer bir yandan da siber atakların terörist ataklar ile direkt bağlantılı olduğu görülmektedir.

Yukarıdaki bilgiler göz önünde bulundurulduğunda olası bir siber terörist atak durumunda kritik bilgi altyapılarının çökmesi çok olası gözükmektedir. Bu durumun gerçekleşmesi de kritik altyapıların sekteye uğramasını doğurarak şehir planlamalarının çökmesi ve kriz durumunun ortaya çıkmasına neden olabilecektir. Şehir planlamalarının çökmesi su, yemek gibi en temel ihtiyaçlar ile bağlantılı olup, kriz durumu büyük ölçekli zorunlu göçlere dahi neden olabilecektir.

En temelinde Şekil 2.2'nin de merkezinde görüleceği gibi içten içe sosyal bir kararsızlık bulunmaktadır.

2.4 Siber Suç

İçerisinde bulunduğumuz bilişim çağında teknolojinin ne kadar hızlı ilerlediğini ne kadar dinamik bir şekilde değişmelerin ve gelişmelerin yaşandığının en yakın şahitleriyiz. Teknolojinin bu denli hızlı bir şekilde gelişmesinin hayatımıza çok büyük kolaylıklar ve faydalar sağladığı çok aşikardır. Teknolojik gelişmelerin hayatımızda sağladığı kolaylık ve faydalara, coğrafik sınırlar olmaksızın insanlar arası iletişimden, kaybolan bir evcil hayvanın tasmasında bulunan GPS sayesinde bulunmasına, bilgiye istenilen zaman ve yerde kolayca ulaşılmasından, internet üzerinden alışverişe veya yatalak hastaların durumlarının uzaktan izlenmesi gibi daha sayamayacağımız kadar çok örnek verilebilmektedir. Fakat bu kadar olumlu gelişmenin yanı sıra tahmin edilebileceği ve günümüzde ne bir şekilde görebildiğimiz üzere bazı olumsuzluklarda teknolojinin gelişmesine paralel olarak arttığı görülmektedir. Teknolojinin hızla gelişmesi ile birlikte geleneksel suç işleme şeklinde dahi değişiklikler olmuş ve siber suç kavramı ortaya çıkmıştır.



Şekil 2.2 : Ulusal risklerin birbirleri ile bağlılık raporu [12].

Bölüm 2.2'de anlatılan siber alan/uzay, siber suçlular tarafından coğrafik sınırlar olmadığından çevirim içi olunduğu sürece kurbanlara atak yapmak için kullanılabilmektedir. Bu nedenle bilgi ve haberleşme teknolojileri (Information and Communications Technology (ICT)) siber uzayda, siber suç olarak adlandırılan ve temel olarak bilgisayar ve internet ile bağlantılı olarak yapılan suçlar olarak tanımlanan bir suç alanı ortaya koymak zorunda kalmıştır. Siber suç kavramının siber suçlular için çekici olmasının nedenleri arasında uzak coğrafyalardan saldırıların yapılabilmesi, takibinin zor olması, yakalanma durumuna karşı uluslararası birçok işlemin gerekmesi gösterilebilmektedir [148].

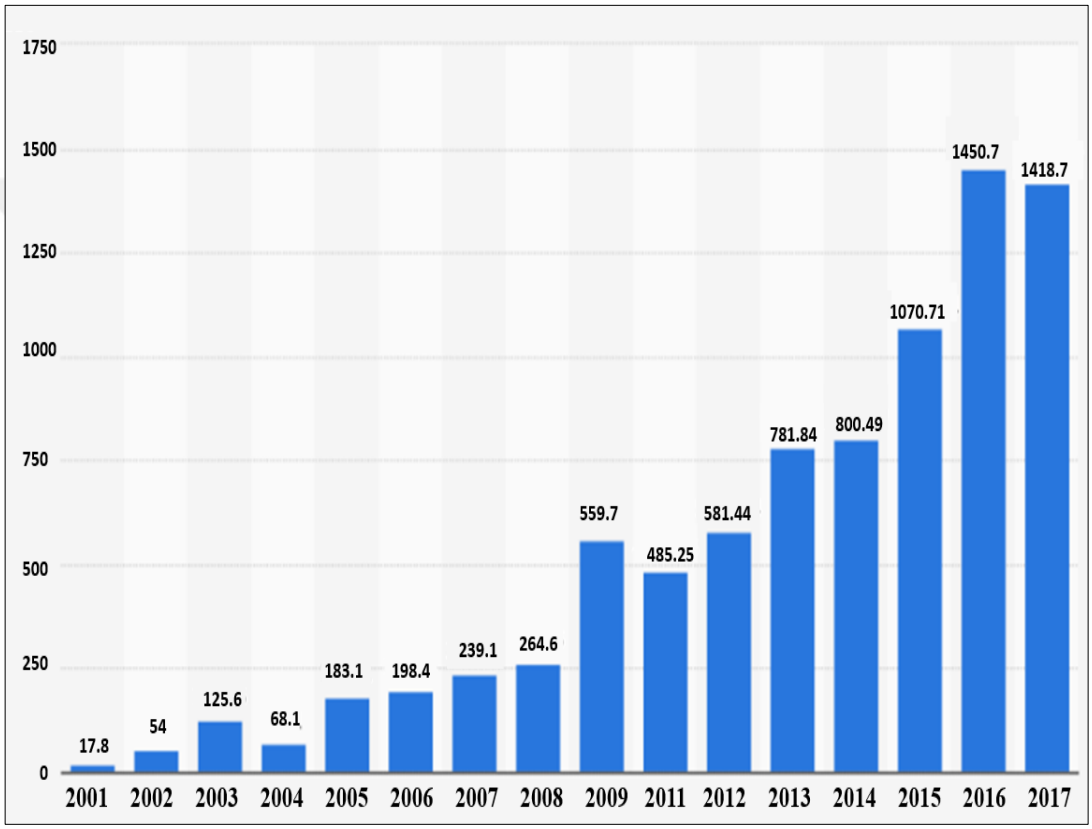
Siber suç kavramının kapsadığı bazı suç çeşitleri Çizelge 2.2'de gösterilmektedir.

Çizelge 2.2 : Siber suç sınıflandırmaları [13].

SİBER SUÇ ÇEŞİTLERİ	TANIMLARI
1. Bilgisayar Korsanlığı (Hacking)	Bilgisayar ve ağ sistemlerine zorla ve yasal olmayarak girmek bilgisayar korsanlığı olarak bilinmektedir.
2. Çocuk Pornografisi (Child Pornography)	Internet ortamı çocuk tacizcileri tarafından dünyanın her yerinde çocuk pornografilerine erişim için kullanılmaktadır.
3. Siber Tacizci (Cyberstalking)	Internet servislerini kullanarak kişi karşısında sürekli tekrar eden ve rahatsızlık verecek derecede davranışlardır.
4. Hizmet Engelleme Saldırısı (Denial of Service Attack)	Kurbanın ağının bant genişliğini gereksiz e-posta veya farklı yöntemler ile doldurarak servislere cevap veremez hale getirmektir.
5. Virüs Yayılımı (Virus Dissemination)	Kötü amaçlı yazılımların kendilerini başka yazılımlara ekleyerek/gizleyerek yayılmasıdır.
6. Yazılım Korsanlığı (Software Piracy)	Hırsızlar tarafından ürünün orjinali ile benzer/birebir olacak şekilde yasal olmayan kopyalarının üretilmesi, dağıtılmasıdır.
7. İnternet Aktarmalı Sohbet (Internet Internet Relay Chat (IRC))	Sunucu içerisindeki odalar içerisinde kişiler birer oda içerisinde birbirleri ile rastgele şekilde bir denk gelerek konuşmasıdır.
8. Kredi Kartı Dolandırıcılığı (Credit Card Frud)	Mal, mülk kısacası ürün almak için kredi kartlarının yetkili kişiler dışındaki kişiler tarafından kullanılmasıdır.
9. Para Sızdırmak (Net Extortion)	Şirketin gizli verilerinin para sızdırmak için ortaya çıkarılmasıdır.
10. Oltalama (Phishing)	Kişinin/kurbanın kullanıcı adı ve şifre gibi gizli verilerinin sahte bir internet sayfası aracılığıyla orjinal siteyi taklit ederek alınmaya çalışılmasıdır.

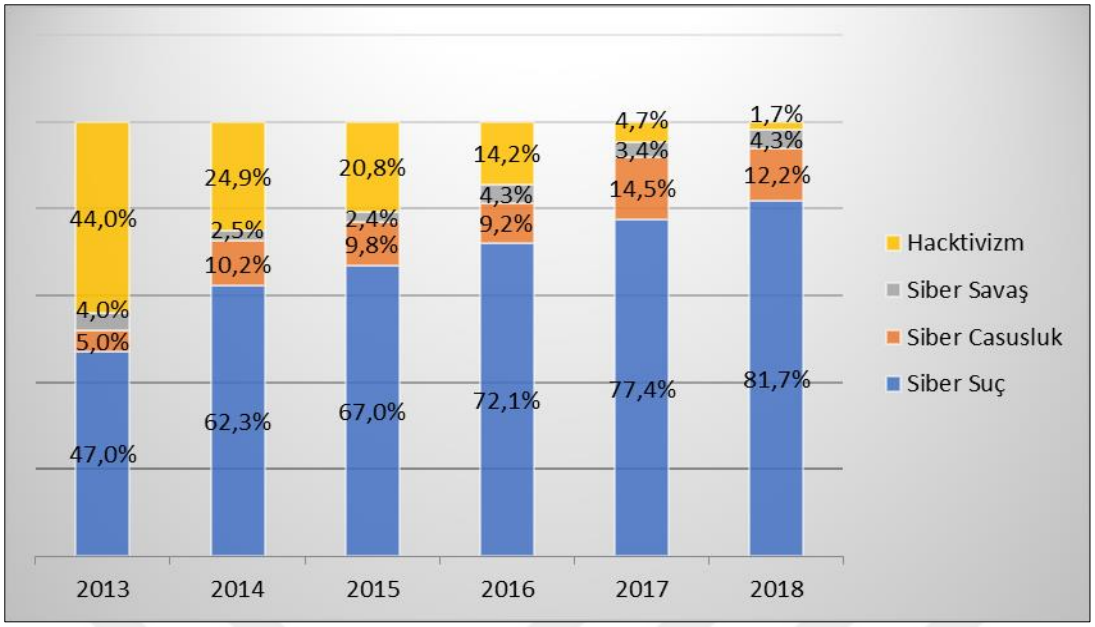
Bilgiler göz önüne alındığında, suç işleme şeklinin değişmesi ve günlük hayatımızı önemli ölçüde kolaylaştıran teknoloji ve internet, bir yandan da yeni hukuki düzenlemeleri zorunlu kılan bir sorun hâline gelmiştir [14].

Amerika Birleşik Devletleri'nde FBI bünyesinde kurulan ve 2001 yılında itibaren faaliyet gösteren "İnternet Suç Şikayet Merkezine (Internet Crime Complaint Center)" göre 2001- 2017 yılları arasında ilgili merkeze rapor edilen siber suçların maruz bıraktığı maddi hasarın değişimini gösteren grafik Şekil 2.3'de gösterilmiştir.



Şekil 2.3 : 2001-2017 yılları arasında siber suçların uğrattığı maddi hasar (milyon dolar) [15].

Şekil 2.3'de açıkça görüleceği üzere daha önce de bahsedildiği gibi son yıllarda (2014 sonrası) siber suçların neden olduğu maddi hasarda giderek büyümekte olup, siber suç sorunu artık sadece bir ülkenin değil tüm dünyanın sorunu haline gelmektedir. Bu yorumu destekleyecek bir şekil de Şekil 2.4' tür. Şekil 2.4, siber saldırılarla ilgili istatistikler tutan "hackmageddon" internet sitesinin 2013 yılından bu yana dünya üzerinde gerçekleşen siber saldırıların dağılımlarını ortaya koymaktadır. Grafikten de net bir şekilde görüldüğü üzere 2013 yılında %47 olan siber suç oranının sürekli artış ile 2018 yılında %81,7' ye çıktığı görülmektedir.



Şekil 2.4 : 2013-2018 Dünya üzerinde gerçekleşen siber saldırıların dağılımı ([16-19] verileri temel alınarak yazar tarafından tasarlanmıştır).

İstatistiksel veriler ve siber uzay dünyasında sınır olmadığı göz önüne alınırsa, yani dünyanın bir ucundaki bir bilgisayardan dünyanın diğer ucundaki bilgisayara hiçbir gerçek coğrafi zorunluluk olmadığı ve birden fazla internet servis sağlayıcı (Internet Service Provider (ISP)) üzerinden hedefe ulaştığı düşünülürse, ulusların siber suça karşı kendi önlemleri ve yasal yaptırımları dışında uluslararası bir anlaşma ve topluluğa da gereksinim olduğu aşikardır.

Bunun bilincinde olan devletler, uluslararası örgütler ve sivil toplum kuruluşları bu konu ile ilgili çok sayıda girişimde bulunmuş olup, bu girişimlerin en önemlisi, Avrupa Konseyi bünyesinde kabul edilen 2001 tarihli Siber Suç Budapeşte Sözleşmesi veya diğer adı ile Avrupa konseyi siber suç sözleşmesidir [20].

Uluslararası alanda yukarıda örnekleri verilen siber suçlarla mücadele kapsamında ülkemizde de çeşitli çalışmalar yapılmaktadır. Örneğin; Türkiye, 10 Kasım 2010 tarihinde Uluslararası Siber Suç Sözleşmesi'ni imzalayarak anlaşmaya taraf olmuş ancak yürürlüğe girmesi 2 Mayıs 2014'te Resmi Gazetede yayınlanmasıyla gerçekleşmiştir [21].

2.5 Siber Casusluk / İstihbarat

İstihbarat ve casusluk, insanın tarih boyunca karşıt kurumlar, ülkeler, devlet veya topluluklar kendi lehlerine avantaj ve üstünlük sağlamak amacıyla birbirlerine karşı

yürütmüş oldukları faaliyetlerden biri olmuştur. Teknolojinin son yıllardaki hızlı ve keskin gelişmesi ile birlikte her ne kadar bu kavramlar değerini kaybetmese de istihbarat ve casusluk kavramların uygulanma yöntemlerinde değişiklikler meydana gelmiştir [22].

Daha önceleri casusluk ve istihbarat aracılığı ile bir bilgiye erişmek daha uzun, daha maliyetli, daha tehlikeli olmak ile birlikte, elde edilen bilgiler fiziksel olarak var olmakta ve bu bilgileri elde etme dahi fiziksel olarak gerçekleşmekteydi [23]. Fakat daha önce de bahsedildiği üzere teknolojinin gelişmesi ile birlikte casusluk ve istihbarat olguları, siber casusluk ve siber istihbarat olarak evrilmiştir.

Siber savaş kapsamı içerisinde yapılması en zor tanımlardan birisi olarak siber casusluk gösterilmektedir. Her ülkenin bu konu ile ilgili kendi bakış açısı olması ve bu konunun diğer konulara istinaden biraz daha üstü kapalı ve ülke itibarları da göz önünde olduğundan dolayı gizli tutulmasından kaynaklı olarak tek bir genel tanıma indirmek pek mümkün olmamaktadır. Bunun yanı sıra birçok ülkenin siber casusluk ve siber istihbarat ile kendi tanımları mevcuttur. Siber casusluk kavramını bilginin nasıl elde edildiği, çalınan bilginin nasıl kullanıldığı, bilgiyi elde etmek için ne tür bir saldırı tekniği kullanıldığı da etkileyebilmektedir.

Uluslararası olarak siber operasyonları ile ilgili olarak tanımları, kuralları ve yönetmeliklerin kabul edildiği bir kılavuz olarak görülen Talin kılavuzu, 2013 yılında Estonya'nın Talin şehrinde NATO (Uluslararası Askeri İttifak) siber savunma merkez birliği önderliğinde oluşturulan konferans sonrasında oluşturulmuştur. Uluslararası kabul gören Talin kılavuzuna göre siber casusluk ve istihbarat "*Gizlice yapılan bir hareket veya sahte iddialar ile siber beceriler kullanılarak karşı devlet/kurum ile ilgili bilgi toplamak veya bilgi toplamaya yeltenmek*" olarak tanımlanmıştır [24].

Birçok insan ve birçok sözlük tarafından siber casusluk gizli bilgileri kötü amaçlar için hedef alarak gizlice elde etmek olarak tanımlansa da Talin kılavuzuna göre yukarıda ki tanımdan da görüleceği üzere, atak niyeti, çalınan bilgi ile ilgili hiçbir ifade bulunmamaktadır. Bu tanımı her ne kadar eksik olarak değerlendirsek de uluslararası kanunda uygun olarak görülmektedir.

Yabancı siber ataklar karşısında devletlerin kendilerini savunmaları artık teknik bir problem olmaktan çıkmıştır. Yabancı ataklar karşısında korunma da asıl problem politik ve kanuni durumlardır. Bu nedenle Talin kılavuzunda yazan tüm ulusları

kapsayan siber casusluk ve istihbarat tanımı atak kurbanı ülkelerin en küçük bir ihlale dahi tam olarak önlemleri alması konusunda imkan sağlamaktadır.

2.6 Siber Savaş

Daha önceki tanımların bazılarında da olduğu gibi siber savaş kavramı içinde uluslararası kabul göre ve uluslararası standartlarda belirli bir tanımı olmamak ile birlikte, literatür taramalarında en çok karşılaşılan ve kabul gören tanım Richard A. Clarke ve Robert K. Knake'e aittir. Richard A. Clarke ve Robert K. Knake'e göre siber savaş bir devletin, başka bir devletin bilgisayar veya iletişim ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirdiği sızma faaliyetleridir [23].

Farklı bir kaynakta da siber savaş, devletler veya devlet benzeri aktörler tarafından gerçekleştirilen, kritik ulusal altyapıları, askeri sistemleri veya ülke için önemli endüstriyel yapıyı tehdit eden, simetrik veya asimetrik, saldırı veya savunma maksatlı dijital ağ faaliyetler olarak tanımlanmıştır [25].

Teknolojinin hızla artması ile birlikte birçok profesör ve bilim yazarı siber savaşların ilerleyen dönemlerde daha da etkili olacağını hatta belki de siber savaşların beşeri olarak gerçekleştirilen savaşlardan daha etkili olacağını düşünmektedir.

Siber uzay içerisinde en önemli olgu bilgidir. Büyük savaş ustası Çinli komutan Sun Tzu'ya göre üstün başarı düşmanın direncini savaşmadan kırmaktır [26]. Bu tanımdan yola çıkacak olursak aslında siber savaşın ne kadar önemli olduğu bir kez daha anlaşılmış olacaktır. Çünkü düşmanın direncini savaşmadan kırmak demek, düşmanın bilgilerinin herhangi bir fiziksel/beşeri tahribat yaratman ele geçirmek demektir. Bu da tam olarak siber savaş başlığı altında olan bir konudur. Siber savaş tek bir yöntem ile değil, birden fazla unsur kullanılarak gerçekleştirilebilir. Siber savaşın nelere yol açabileceğine örnek vermek gerekirse,

- Ülke vatandaşlarına ait bilgiler ele geçirilebilir, değiştirilebilir ve/veya silinebilir.
- Trafik sistemine sızılabilir ve trafik ışık sistemi üzerinde yapılan birçok değişiklik ile can ve mal kaybına neden olacak kazalara neden olunabilir.
- Banka sistemlerine sızılarak ülke ekonomisine büyük zararlar verilebilir.

- Devlete ait önemli bilgilerin tutulduğu sunuculara sızılabilir ve bu sayede çok önemli stratejik bilgiler ele geçirilebilir.
- Hastane sistemlerine sızılarak hasta bilgileri ele geçirilebilir ve sağlık hizmetleri durabilir.
- Uydu sistemleri ele geçirilerek ülke çapında büyük bir kaosa neden olunabilir.
- Ülkenin internet sistemi tamamen kapatılabilir ki bu da çok büyük bir kaosa neden olacaktır.
- Nükleer tesislerin kontrolü ele geçirilerek burada büyük sorunlar ortaya çıkartılabilir. Hatta bu tesisler imha dahi edilebilir.

Teknolojinin çok yüksek bir hızla gelişmesi, biraz önce yukarı da verilen örnekler, siber savaşın daha zor bir kimlik tespiti olması, coğrafi sınırları olmaması gibi durumlar göz önüne alındığında siber savaşın her geçen gün adından biraz daha fazla söz ettireceği aşikardır.

Şekil 2.5'te ülkeler arasında yapılan DDOS atalarının gerçek zamanlı izlenebildiği internet sayfasının görseli bulunmaktadır. Buna benzer bu tarz saldırıların izlenebildiği başka sitelerde bulunmaktadır.

Şekil 2.5 : Gerçek zamanlı yapılan DDOS ataklarının haritası [27].

Çizelge 2.3'ten de açıkça görülebileceği üzere siber savaşın maliyeti çok düşüktür. Ayrıca coğrafi sınırlardan bağımsız olması, saldırı kaynağının tespitinin zor, hatta bazı

durumlarda imkansız olması ve son olarak da saldırının belirtilerinin tespit edilemezliği siber savaşı güçlü bir silah haline getirmektedir.

Çizelge 2.3 : Konvansiyonel savaş ile siber savaş arasındaki farklar [28].

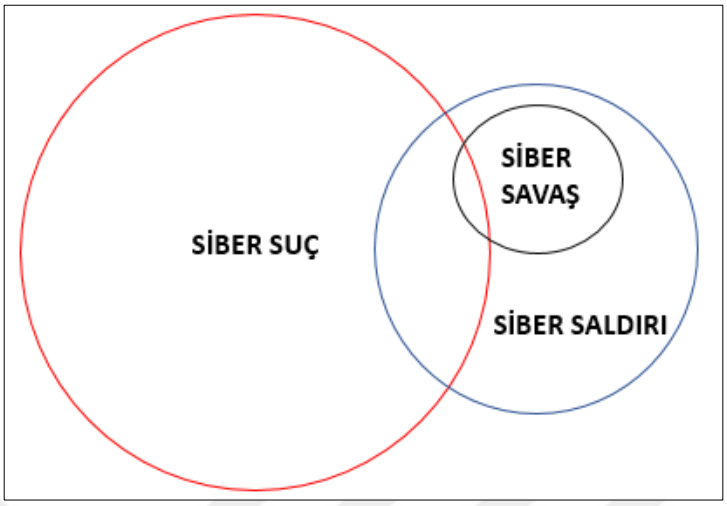
DEĞİŞKENLER	KONVANSİYONEL SAVAŞ	SİBER SAVAŞ
SALDIRININ KAYNAĞININ TESPİTİ	Kolaydır.	Zordur. Bazen de imkânsızdır.
SALDIRININ HIZI	En hızlı muharebe silahı hızındadır.	İnternet hızındadır.
SALDIRININ ETKİSİ	Coğrafi sınırlar içerisindedir.	Siber uzay içerisindedir.
SAVAŞÇILARI	İki veya daha fazla ülke orduları savaşmaktadır.	Tek bir kişi, bir grup, bir örgüt veya devletler savaşmaktadır.
MALİYETİ	Genellikle oldukça pahalıdır.	Ucuzdur.
KULLANILAN SİLAHLAR	Tank, top, tüfek, füze, bomba vb. kullanılır.	Bilgisayarlar, bilgi sistemleri vb. kullanılır.
İLERİ TEKNOLOJİ İHTİYACI	Vardır.	Yoktur. Mevcut teknoloji genellikle yeterlidir.
SALDIRININ BELİRTİLERİ	Tespit edilebilir.	Tespit edilemeyebilir.
HASAR TESPİTİ	Kolaydır.	Zordur.

Siber güvenlik ile ilgili terimlerden bahsederken daha önce siber saldırı, siber suç gibi kavramlardan da söz edilmişti. Siber savaş kavramının da hayatımıza girmesi ile birlikte her ne kadar bu üç kavram birbirine benzeseler de aralarında bazı farklılıklar bulunmaktadır. Oona A. Hathaway ve Rebecca Crootof'a göre siber aksiyonlar (Siber Savaş, Siber Suç ve Siber Atak) arasındaki ilişki Çizelge 2.4'te belirtilmiştir.

Çizelge 2.4 : Farklı siber eylemlerin ana karakteristikleri [29].

	Siber Eylemin Türü		
	Siber Saldırı	Siber Suç	Siber Savaş
Sadece devlet dışı aktörlerin dahil olduğu eylem		X	
Bilişim sistemleri aracılığıyla işlenen ve ceza hukukunun uyulması gereken kurallarının ihlalinin varlığı		X	
Amacı bilişim sistemlerinin işlevini engelleme olan siber eylem	X		X
Amacı politik ve ulusal güvenliğin sağlanması olan siber eylem	X		X
Yapılan atağın etkilerin silahlı saldırıya eşdeğer olması veya siber eylemin silahlı çatışma bağlamında icra edilmesi			X

Siber suç, siber saldırı ve siber savaş arasındaki ilişki Oona A. Hathaway ve Rebecca Crootof'a göre Şekil 2.6'daki gibi gösterilmiştir.



Şekil 2.6 : Siber eylemler arasındaki ilişki [29].

Şekillerden de açıkça yorumlanabileceği üzere, siber suç, devletler ile herhangi bir ilgisi olmaksızın devlet dışı faktörler tarafından işlenmekte ve ceza hukuku normlarını ihlal etmektedir. Siber saldırılar ise, devlet veya devletin ilgisi olmaksızın gerçekleşebildiği gibi, bilişim sistemlerinin işlevini, politik ve ulusal güvenliği sağlamak amacıyla, engellemektir. Siber savaş ise siber saldırı niteliklerine ek olarak siber savaş etkisinin, silahlı atak etkisine eşit olması gerekmesi veya herhangi bir silahlı çatışma kapsamında gerçekleştirilen eylemdir.

2.7 Siber Güvenlik Kavramı

Siber güvenlik kavramı temel olarak internet bağlantılı veya bazı durumlarda bağlantısız sistemlerin, donanım, yazılım ayırmaksızın siber ataklardan korunması için kullanılan ve sürekli geliştirilen bir sistem olarak tanımlanabilmektedir.

Birleşmiş Milletlerin (BM) haberleşme, bilgi ve iletişim teknolojileri alanındaki yetkili organı olan Uluslararası Telekomünikasyon Birliği (ITU) tarafından siber güvenlik, "siber uzayda organizasyon, çevre ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünü" olarak tanımlanmıştır. Siber uzayda organizasyon ve kullanıcıların varlıklarını, bireyler, bilgi işlem donanımları, altyapılar, uygulamalar, hizmetler, haberleşme sistemleri ve siber uzayda iletilen ve/veya saklanan bilgiler oluşturmaktadır [30].

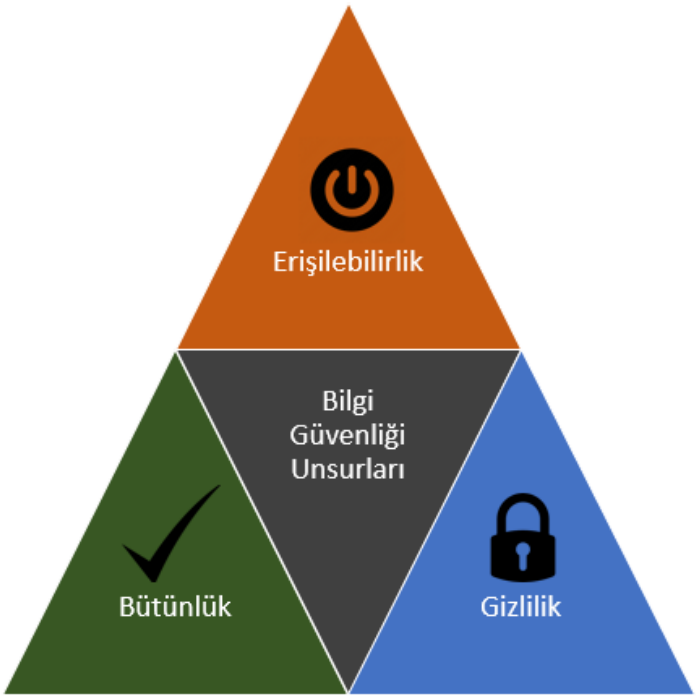
Diğer bir tanımlamada ise siber güvenlik kavramı, TAG-Cyber firmasının kurucusu ve CEO'su olan Edward Amoroso tarafından siber güvenlik adlı kitabında "siber güvenlik, zararlı ataklarının sistemlerde, bilgisayarlarda ve networklerde oluşturabileceği risklerin azaltılmasını kapsamaktadır. Bu kavram virüslerin tespiti ve durdurulması, kötü amaçlı erişimlerin engellenmesi, sistemlere sızmaların tespit edilmesi, şifrelenmiş iletişimin aktif edilmesi ve kimlik doğrulamanın zorunlu hale getirilmesine olanak sağlayacak araçları kapsamaktadır." şeklinde tanımlamıştır [31].

Uluslararası Telekomünikasyon Birliği (ITU) tarafından da kabul edildiği gibi güvenliğin temel amacı, elektronik ve/veya diğer ortamlarda bulunan her türlü bilginin;

- Gizliliğini (Confidentiality),
- Bütünlüğünü (Integrity),
- Kullanılabilirliğini (Availability),

sürekli olarak sağlamaktır.

Şekil 2.7'den de görüleceği üzere güvenlik alanında gizlilik, bütünlük ve kullanılabilirlik en temel üç bileşenidir ve bu üç bileşen birbiri ile iç içe olacak şekilde ele alınmalıdır.

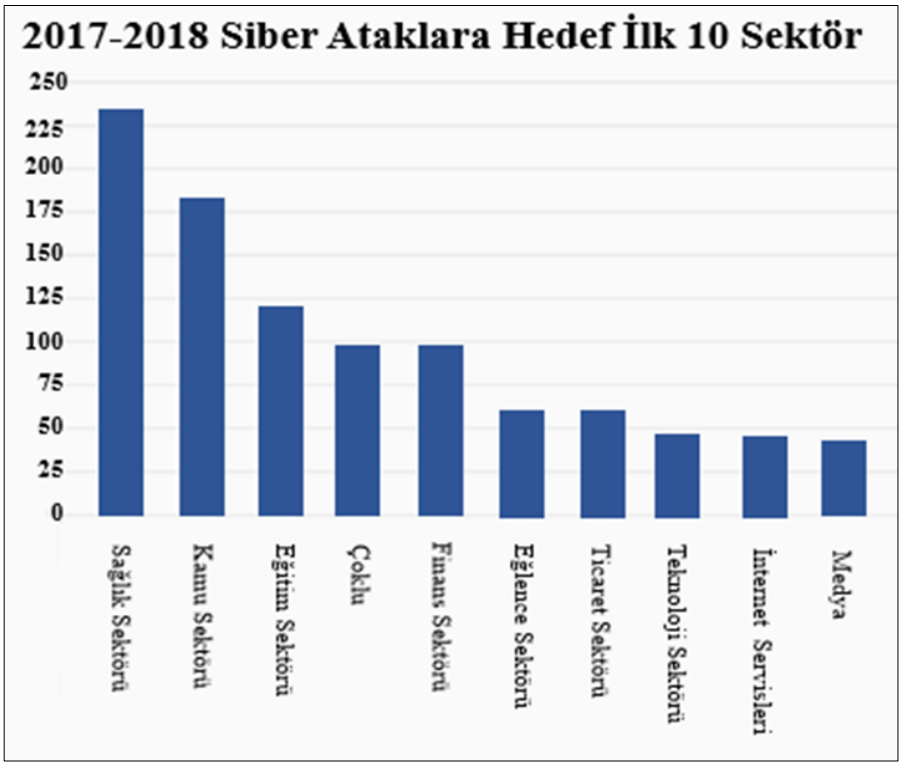


Şekil 2.7 : Gizlilik, bütünlük ve erişilebilirlik üçgeni (Yazar tarafından tasarlanmıştır).

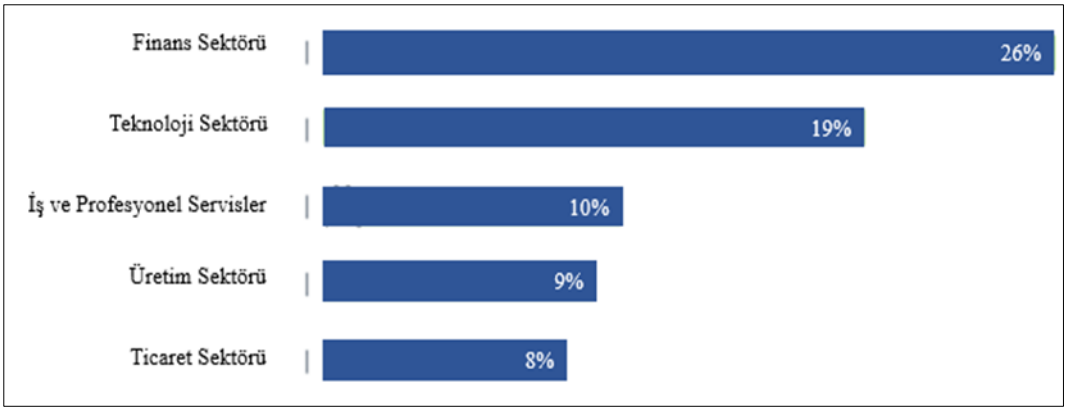
Kısaca bu üç bileşeni inceleyecek olursak;

Gizlilik (Confidentiality)

Gizlilik kavramı en yakın tabir ile mahremiyet olarak tasvir edilebilmektedir. Datanın ve bilginin, erişmemesi gereken kişi ve/veya kişiler tarafından erişimini engellerken bunun yanı sıra yetkili kişiler tarafından erişimin sağlanması konusunda alınan tedbirleri içermektedir. Bilginin veya dosyaların güvenlik seviyeleri konusunda kategorize edilmeleri bu konuya örnek olarak verilebilmektedir. NTT Güvenlik 2018 Küresel Tehdit İstihbarat Raporuna [32] göre Şekil 2.9 da gösterildiği üzere siber atakların en sıklıkla hedefi olan finans sektörü olarak gösterilirken, McAfee firmasının 2017-2018'de yapılan atakların sektör bazı değerlendirildiği raporuna göre [33] Şekil 2.8 da gösterildiği üzere siber ataklara en çok hedef olan sektör sağlık sektörü olmuştur. Gerek sağlık gerekse finans sektöründe sistemlere giriş, sanal para ticareti sırasındaki sistemlere giriş ve/veya data transferi sırasında kullandıkları kullanıcı adı, şifre sorgulaması gizlilik konusu için standart birer örnek iken bunun yanı sıra uygulanan 2-way authentication veya 3D-güvenlik olarak adlandırılan önlemler son yıllarda bu konunun öneminin fark edildiğinin ve geliştiğinin işareti olarak gösterilmektedir.



Şekil 2.8 : 2017-2018 yılında siber ataklara hedef olan ilk 10 sektör [33].



Şekil 2.9 : Sektör bazında 2018 küresel atak oranları [32].

Bütünlük (Integrity)

Bütünlük kavramı, bir önceki başlıkta anlatılan gizlilik ihlali durumunda verinin uçtan uca tüm döngüsü boyunca bozulmamasını, yetkisiz kişiler tarafından değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesine karşı içeriğin korunması olarak tanımlanabilmektedir. Fakat bu tehditlere karşı koruma sağlarken aynı zamanda da bilginin kaynağına yetkili kişiler tarafından uygun zamanlarda yetkili kişiler tarafından erişimi sağlamakta ve böylece bilginin biraz önce de bahsedildiği gibi istenilerek veya yanlışlıkla değiştirilmesini önlenmektedir.

Kullanılabilirlik (Availability)

Kullanılabilirlik, veri ya da bilgiye yetkili kişilerce istenildiği zaman her yerden erişim sağlayabilmesidir. Bu kavramın sağlanabilmesi için sistemlerde ortaya çıkabilecek en küçük bir arıza dahi göz önüne alınmalı ve sistemin tüm donanım ve yazılımı kontrol ve bakım altında güncel olarak tutulması gerekmektedir. Sistem güncellemesi var ise yapılarak sistemin en güncel şekilde tutulması, bant genişliği konusunda bir sorun varsa analizinin yapılması ve aksiyonunun alınması, siber atak yaşanması ve/veya riskinin bulunması durumlarında proxy server, firewall (güvenlik duvarı) gibi ek güvenlik cihazları ile önlemler alınması, mümkün ise distributed denial-of-service (DDoS) hizmeti alınması verilebilecek örnekler arasındadır.

2.8 Siber Güvenlik'in Önemi

Siber güvenlik kavramının önemini yapılan bazı araştırmalar ve raporlar sonrasında elde edilen rakamlar ile açıklamak daha verimli ve somut olacak olsa da daha önce

endüstri 4.0 ile birlikte hayatımıza giren siber fiziksel sistemler (SFS), nesnelerin interneti, akıllı fabrikalar üzerinden giriş yapmak daha doğru olacaktır.

Endüstri 4.0 ile birçok sistem gerçek zamanlı bağlantı, iletişim ve anında tanımlama gerçekleştirebilmektedir. Bu sistemleri ise insan, makina ve robot unsurlar oluşturmaktadır. Endüstri 4.0 ile son derece yüksek bir esneklik içinde müşteri taleplerine göre özelleşmiş ve dijitalleşmiş akıllı imalat modeli geliştirilmektedir. Ayrıca bu akıllı imalat modeli ile birlikte endüstri 4.0 adı altında imalat endüstrisi, bilgi teknolojileri ile harmanlanarak ortaya akıllı fabrika modeli ve ham maddeden ürünün son haline kadar robotlar ve makinalar sayesinde kullanıcının takip edebileceği akıllı bir üretim platformu ortaya çıkmıştır [34].

Fakat bu akıllı fabrika sistemleri içerisinde bulunan birbirinden farklı üretici firma tarafından ve üretimin farklı esnalarında kullanılan cihazları ele aldığımızda her birisinin kendine has gerek yazılımsal gerekse donanımsal özellikleri bulunmaktadır. İşte birbirinden farklı sistemlerin birlikte kullanmak, iş birliğini, sürdürülebilirliği ve etkinliği mümkün kılmanın yanı sıra, farklı yazılım ve donanımsal özellikleri ile de birçok riski beraberinde getirmektedir.

Siber saldırı olabilecek sistemler sadece akıllı fabrikalar şeklinde düşünülmemelidir. Raylı sistem yönetiminin sağlandığı kontrol sistemlerine (ICS), üretim tesislerine, uçaklara, telefonlara, şahsi bilgisayarlara, araçlara ve bunun gibi internete bağlantısı olan veya küçük bir harici bellek ile kullanıcı hatası nedeni ile internete bağlantısı olmaksızın yüzlerce alanda yüzlerce ürüne siber saldırı yapılabilmektedir. Kısacası ne kadar çok cihaz internete bağlanırsa, risk de bir o kadar artacaktır. Bunun en büyük nedenlerinden bir tanesi kullanıcı farkındalığı olmaması ve sistemlerin siber açıklarının artmasıdır.

Dünya Ekonomik Formunun 2018 yılında yayınlanan Küresel Risk Raporunun, tezin ana unsurları olan siber güvenlik, siber saldırılar, data hırsızlıkları kısacası tezin ana fikri ile tamamen örtüştüğü görülmektedir. 2018 yılında yayınlanan rapora göre, olabilirlik açısından ilk 5 küresel risk kategorisine siber güvenlik ilk olarak 2012 yılında girmiştir. Küresel risk raporunun Dünya üzerindeki iklim değişikliğinden mali dengesizliklere, doğal afetlerden ekonomik krizlere kadar çok geniş bir yelpazede incelendiği göz önüne alındığında siber atakların ilk kez 2012 yılında olabilirlik açısından ilk 5 küresel risk kategorisine girmesi ve bundan sonraki 7 yılda siber olaylar

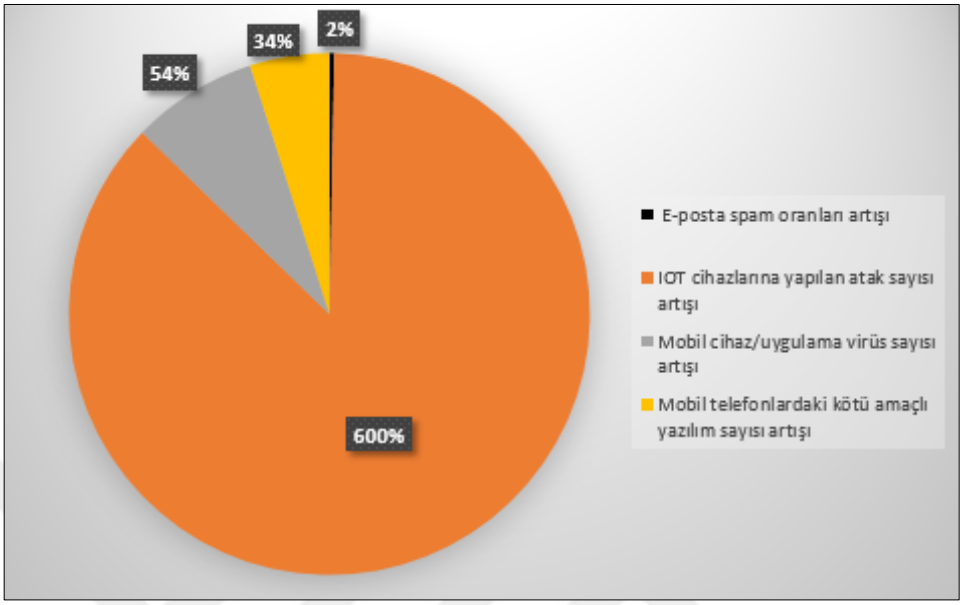
ile ilgili 5 başlığın raporda yer alması, daha önce de belirtildiği gibi siber güvenlik konusunun ne denli önemli olduğunun ve riskin her geçen gün teknolojinin gelişmesi ile arttığı veriler ile gözler önüne sermiştir.

Dünya Ekonomik Forumun Şekil 2.10'de gösterilen 2018 Küresel Risk Raporundan Türkçeye uyarlanan kesiti incelendiğinde, Dünya için çok önemli olan işsizlik, ülkeler arası anlaşmazlık, su krizi, istemsiz göç, nüfusların yaşlanması gibi başlıkları geride bırakarak 2018 yılının olabilirlik açısından ilk 5 küresel risk olarak değerlendirilen siber ataklar ve veri sahtekarlığı ve hırsızlığı konularının Dünya genelinde önlem alınması gereken, kritik altyapıları hedef alarak gündelik hayatımızı dahi durduracak kadar tehlikeli olan siber olaylara dikkat çekilmiştir.

2018 Küresek Risk Raporundan çıkartılacak en önemli sonuçlardan bir tanesi şudur ki, siber dünyayı dikkate almayan devletlerin, kamu kuruluşlarının, özel sektörde hizmet eden organizasyonların karşılaşabilecekleri sorunlar çoğu zaman telafisi olmayan hasarlara neden olacaktır. Bu nedenle de iyi bir savunma yapabilmek için yani sağlam bir siber güvenlik yönetimi oluşturabilmek, kurumların, devletlerin kendilerini siber olaylardan koruyabilmeleri için ilk yapılması gereken düşmanı yani siber atakları, bilgisayar korsanlarını, gerek organizasyonel eksikleri gerek eksik yatırımları gerekse de farkındalık seviyelerini iyi bilmektir.

Şekil 2.10 : 2018 Küresel risk raporuna göre olabilirlik açısından ilk 5 küresel risk [12].

Symantec firmasının 2018 internet güvenlik tehdit raporuna [33] göre Şekil 2.11'de gösterildiği üzere nesnelerin interneti (IOT) cihazlarına yapılan atak sayısının 2016 yılına göre %600 arttığı görülmektedir.



Şekil 2.11 : Symantec güvenlik tehdit raporu istatistikleri (Yazar tarafından tasarlanmıştır).

Aynı raporda geçen diğer rakamlara göz atacak olursak;

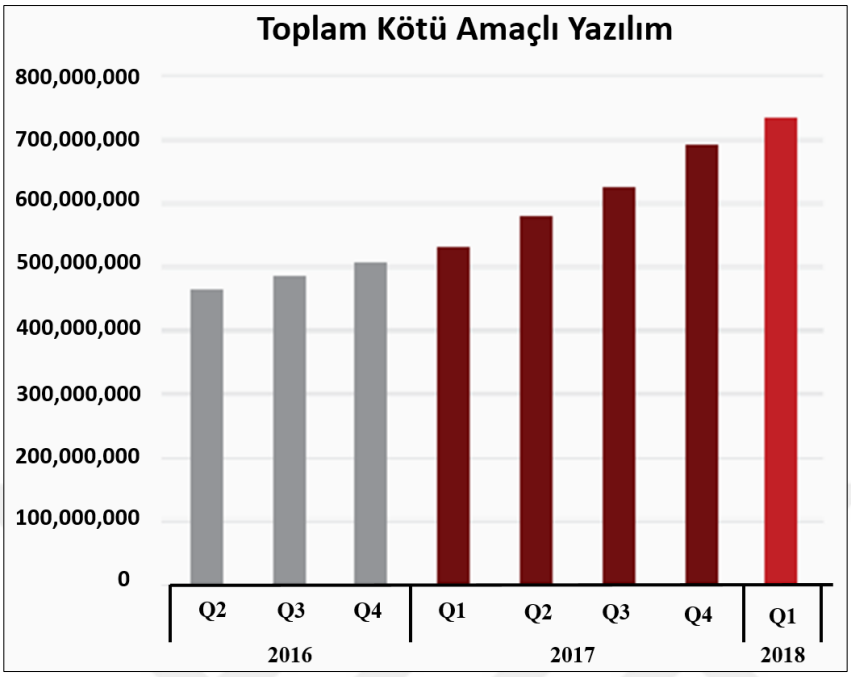
- E-posta spam oranları 2016 yılına göre %2,
- Mobil telefonlarda/uygulamalarda 2016 yılına göre virüs sayısı %34,
- Mobil telefonlardaki kötü amaçlı yazılım 2016 yılına göre %54

artmıştır.

Yine bir başka raporda [33] 2016 yılının ikinci çeyreğinden 2018 yılının ilk çeyreğine kadar kötü amaçlı yazılımların mobil ve total değerlerinin karşılaştırıldığı Şekil 2.12 ve Şekil 2.13'deki grafikler incelendiğinde artışın ne kadar yüksek olduğunu ve siber atakların her geçen gün artan internet bağlantılı cihaz sayısı ile aslında ne kadar artabileceği ve bununlar birlikte de son kullanıcı ve şirketler açısından ne kadar tehlikeli gerek kişisel veri güvenliği, gerekse şirket bazında maddi ve itibar konularında ne kadar tehlikeli olabileceği açıkça görülmektedir. Çünkü internete bağlanan her yeni sistem veya yapılan her güncelleme ile sistemler her ne kadar korunsa da bir yandan da yapılan hatalar ile sistemler açıklar verebilmektedir.

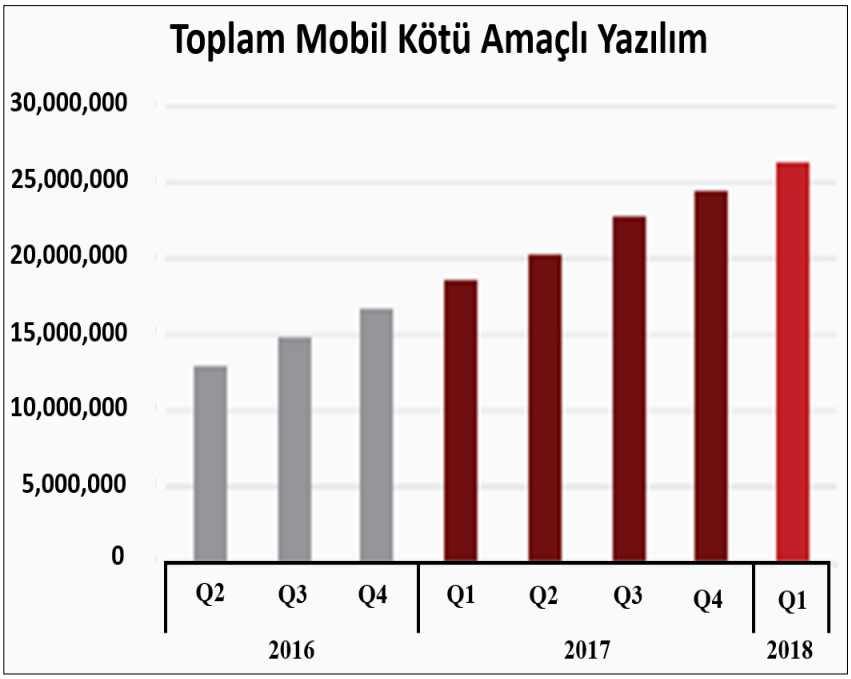
Grafik değerleri tam olarak belirtememesine rağmen grafikler incelendiğinde;

- Toplam kötü amaçlı yazılım sayılarının 2018 yılının birinci çeyreğinin 2016 yılının ikinci çeyreğine kıyasla yaklaşık %60 oranında bir artışı,



Şekil 2.12 : Toplam kötü amaçlı yazılım (2016 - 2018) [33].

- Toplam mobil kötü amaçlı yazılım sayılarının 2018 yılının birinci çeyreğinin 2016 yılının ikinci çeyreğine kıyasla yaklaşık %100 oranında artışı gözlenmektedir.



Şekil 2.13 : Toplam mobil kötü amaçlı yazılım (2016 - 2018) [33].

3. BİLGİSAYAR KORSANLIĞI, MOTİVASYONLARI VE SALDIRI YÖNTEMLERİ

3.1 Bilgisayar Korsanı

Birleşmiş Milletlerin (BM) haberleşme, bilgi ve iletişim teknolojileri alanındaki yetkili organı olan Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılan tanımlamada bilgisayar korsanı kavramı iki kavramın karşılaştırılması ile açıklanmıştır. ITU'ya göre "computer hacker" ve "computer craker" olmak üzere iki kavram bulunmakta ve bu kavramlar arasında yasal olarak herhangi bir ayırım yapılmasına gerek olmamasına rağmen tanımsal olarak küçük bir farklılık bulunmaktadır. ITU tarafından yasal olarak herhangi bir ayırım yapılmamasının nedeni bu iki kavramın da yasal olmayan erişimi temsil etmesidir. Fakat iki kavram arasında yukarıda bahsedilen küçük farklılık bu iki kişi arasında ki motivasyon olarak gösterilmektedir.

ITU, bilgisayar korsanı kavramını yasa dışı olmayacak şekilde programlanabilir sistemlerin detaylarını keşfetmekten zevk alan kişi olarak tanımlamaktadır. Bunun yanı sıra cracker kavramını ise yasaları ihlal ederek genel olarak bilgisayar sistemlerine zarar veren, bu sistemlere izinsiz bir şekilde sızan kişi olarak tanımlamaktadır [36].

Fakat günümüzde "craker" tanımı neredeyse kullanılmamaktadır. Bunun yanı sıra iyi ve kötü bilgisayar korsanı kavramının ortaya çıktığı görülmektedir. Literatür de bu kişiler beyaz şapkalı, gri şapkalı ve siyah şapkalı bilgisayar korsanı olmak üzere üç ana başlık altında toplanmakta ve üç ana başlığı yanı sıra literatürde ön plana çıkan bilgisayar korsanı çeşitleri de bölüm 3.2 'de anlatılmaktadır. Birden fazla bilgisayar korsanı çeşidi olmasına rağmen, hangi bilgisayar korsanı olduğu fark etmeksizin bilgisayar korsanlığı işlemi Çizelge 3.1'de gösterildiği üzere genel olarak 5 adımdan oluşmaktadır.

Çizelge 3.1 : Bilgisayar korsanlığı adımları ve açıklamaları [37].

BİLGİSAYAR KORSANLIĞI ADIMLARI	SÜREÇ AÇIKLAMASI
1. Keşif	Atak yapılacak sistem ile ilgili bilgi toplama evresidir.
2. Tarama ve Numaralandırma	Açıklıkların taranması ve atak yapılacak yerin numaralandırılarak belirlenme evresidir.
3. Erişim Kazanma	Sisteme erişim için kullanıcı adı ve/veya şifre bilgisi ele etme evresidir.
4. Erişimi Sürdürme	İşlemlerini yapabilmesi için elde ettiği erişimi sürdürme evresidir.
5. İzleri Kaybetme	Bütün işlemler tamamlandıktan sonra herhang bir şekilde tespit edilmemesi için kullanılan kullanıcı bilgilerinin silinmesi log dosyalarının temizlenmesi vb işlemlerin yapıldığı evresidir.

3.2 Bilgisayar Korsanı Çeşitleri

Bölüm 3.1'de de açıklandığı üzere bilgisayar korsanları, arzuları, hizmet ettikleri amaçları veya motivasyonları doğrultusunda içlerinde birkaç çeşide ayrılmış durumdadır. Fakat genel olarak bilgisayar korsanı kavramı bu çeşitlerin hepsinin karşılanması açısından biraz fazla genel kalmak ile birlikte, literatürde en çok karşılaşılan bilgisayar korsanı çeşitleri aşağıdaki gibidir.

- Beyaz Şapkalı / Etik Bilgisayar Korsanları
- Siyah Şapkalı Bilgisayar Korsanları
- Gri Şapkalı Bilgisayar Korsanlar
- Hactivist Bilgisayar Korsanlar
- Suicide Bilgisayar Korsanları
- State sponsored Bilgisayar Korsanları
- Script kidding

3.2.1 Beyaz şapkalı / etik bilgisayar korsanları

Beyaz şapkalı bilgisayar korsanları aynı zamanda etik bilgisayar korsanları olarak da bilinmektedir. Adından da anlaşılabileceği üzere siber ortamda yani siber uzay

içerinde siyah şapkalı bilgisayar korsanlarının tam tersi motivasyon ile hareket eden bilgisayar korsanı çeşidi olarak tanımlanmaktadır. Etik bilgisayar korsanları bir şirkete bağlı çalışabilecekleri gibi şirketten bağımsız bireysel olarak da çalışabilmektedirler. Ana motivasyonları sistemler üzerindeki açıkları birer siyah şapkalı bilgisayar korsanı gözünden bakarak tespit ederek daha sonra bunların kapatılması ve/veya gerekli mercilere haber verilmesi, sistemin daha güvenli hale getirilmesidir. Bilgi, birikim ve kullandıkları bilgisayar korsanlığı araçları açısından siyah şapkalı bilgisayar korsanlarından bir farkları bulunmamaktadır.

Etik bilgisayar korsanlığı, yine aynı şekilde sızma testi olarak da bilinmektedir. Fakat siyah şapkalı bilgisayar korsanlarının yaptığı yasal olmayan sızmalardan farklı olarak etik bilgisayar korsanları sisteme giriş, sızma testi yapılması, zayıflık tespiti gibi konularda çalışken yasal olarak izni bulunmaktadır. Bu yasal yetkiye tüm risk yönetim süreci içerisinde, güvenliğin arttırılması gözü ile bakılmaktadır. Beyaz şapkalı bilgisayar korsanları siber güvenlik açısından en gerekli ve önemli kavramların biri olarak gösterilmektedir [38].

3.2.2 Siyah şapkalı bilgisayar korsanları

Siyah şapkalı bilgisayar korsanları, ya da uluslararası literatürde geçtiği gibi "Black Hat Hacker" olarak adlandırılan bilgisayar korsanları isminden de tahmin edilebileceği üzere kötü amaçlı bilgisayar korsanları olarak belirtilmektedir. Sistemlerdeki açıkları kendi şahsi çıkarları amaçları için kullanabilecekleri gibi tespit ettikleri açıkları dark web adı verilen internetin yasal olmayan yüzünde de para karşılığı satabilmektedirler.

Bu etiketi benimsemiş olan bilgisayar korsanları en az üç veya dört işletim sisteminde, ağ yapılarında ve ağ protokollerinde, bilgisayar korsanlığı araçlarında, bilgisayar yazılımı konusunda uzman kişilerdir. Siyah şapkalı bilgisayar korsanlarının adeta imzası, ağa sızma, bilgi çalma gibi konularda kötü niyetli yazılım ve etik olmayan yasadışı yöntemlere başvurmaları ve bu eylemleri sürekli olarak denmeleridir. Siyah şapkalı bilgisayar korsanları bölüm 3.1'de daha önce bahsedilen "craker" kavramı ile tam olarak örtüşmektedir [39].

3.2.3 Gri şapkalı bilgisayar korsanları

Gri şapkalı bilgisayar korsanları, beyaz şapkalı bilgisayar korsanları ile siyah şapkalı bilgisayar korsanları arasında bir yere yerleştirilebilmektedirler. Bu tarz bilgisayar

korsanları şahsi kazançları için sistemleri ele geçirmezler fakat yine de sisteme izinsiz, yasa dışı bir şekilde girerek sistemin açıklıklarını ve zayıflıklarını tespit ederek buldukları açıkları ilgili organizasyon veya şirket ile paylaşırlar ve bu sayede güvenliğin arttırılmasına yardımcı olmaktadırlar. Gri şapkalı bilgisayar korsanlarının çalışma şekillerine bakıldığında sistemlere izinsiz girişleri nedeniyle siyah şapkalı bilgisayar korsanlarına benzerken, organizasyonların sistemlerinde ki zayıflık ve açıklıkları tespit ettiklerinden bunların düzeltilmesi için uyarması bakımından da etik bilgisayar korsanları gibi hareket etmektedir [39].

3.2.4 Siber muhalif bilgisayar korsanları

Siber muhalif bilgisayar korsanları daha çok politik konularda ön plana çıkan ve toplumun dikkatini çekme motivasyonu ile diğer bilgisayar korsanları ile aynı seviyede bilgi düzeyine ve bilgisayar korsanlığı araçlarını kullanım becerisine sahip olmasına rağmen bunu sadece toplumda bazı değişikliklere önderlik edebilmek ve toplumu biraz daha politik, siyasi ve gizli konularda aydınlatmak amacıyla sistemlere sızan, gerekli ise bilgi çalan kişiler olarak tanımlanmaktadırlar.

3.2.5 Suicide bilgisayar korsanları

İsimlerinden de tahmin edilebileceği üzere suicide bilgisayar korsanları, bir amaç uğruna uzun dönem hapse girmeyi dahi göze alabilecek şekilde bir sistemi hackleme ve sisteme sızma yapan bilgisayar korsanlarına denmektedir. Burada önemli nokta suicide bilgisayar korsanları kötü oldukları kadar iyi de olabilmektedirler [41].

3.2.6 State sponsored bilgisayar korsanları

Hükümetler tarafından özel olarak kiralanan ve diğer hükümetlerin sistemlerini hackleme ve yüksek gizlilikteki bilgileri çalmak motivasyonu ve görevi için bilgisayar korsanlığı yapan kişiler olarak tanımlanmaktadırlar [40].

3.2.7 Script kidding

Script Kidding'i aslında bilgisayar korsanı bilgi seviyesi olarak değerlendirirsek yanlış yapmış olmayız. Bu bilgisayar korsanları, normal bir bilgisayar korsanı veya craker kadar bilgi düzeyine sahip olmayan, bir bilgisayar korsanlığı aracını kendi yazmak veya sisteme sızmak için kendi yazdığı araçları kullanmak yerine internet üzerinden başka üst seviye bilgisayar korsanlarının yazdığı araçlar ile atak yapmayı

denemektedirler. Bu seviyedeki bilgisayar korsanları için yapılan atağın kalitesinden çok yapılan atak sayısı önemlidir [42].

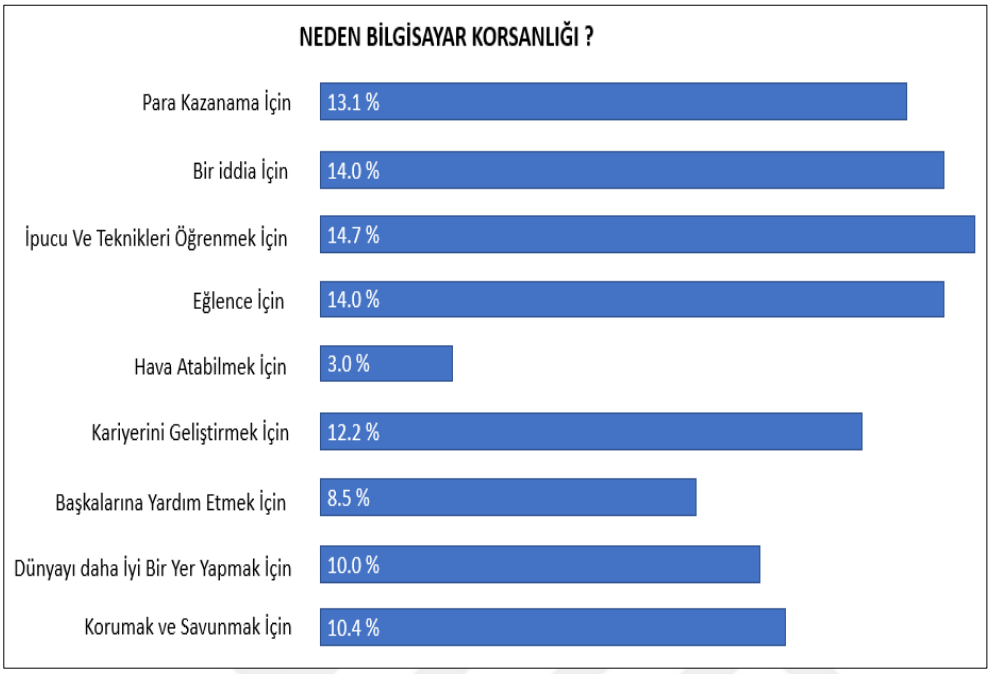
3.3 Bilgisayar Korsanlığı Motivasyonları

Bölüm 3.2'de açıklandığı üzere birçok bilgisayar korsanı çeşidi bulunmakla birlikte bu bilgisayar korsanlarının her birisinin motivasyonu, bir sisteme sızma isteği ve nedeni, sonunda elde etmeyi beklediği farklılık göstermektedir. Bu başlık altında bir bilgisayar korsanlarının motivasyonu bilmek tehdide karşı daha etkili bir cevap vermede kolaylık sağlayacaktır. Burada bir örnek vermek gerekirse, her çalışanın önceliği farklıdır. Örneğin, bir çalışanın iş hayatında ki ilk önceliği para iken, bir başkasının çalışma ortamı, müdürü, iş arkadaşları, şirketin çalışanına verdiği değer veya evi ile işi arasında ki mesafe dahi olabilir. Böyle bir durumda önceliği evi ile işyeri arasında ki mesafe olan birisine, evinden 2-3 saat uzaklıktaki bir yerden iş teklifi gelse dahi bu kişinin teklifi kabul etme olasılığı çok düşüktür. Daha önce de belirtildiği gibi, bilgisayar korsanlarının motivasyonunu bilmek tehdide karşı daha etkili bir cevap vermede kolaylık sağlayacaktır. Bu bölümde bazı bilgisayar korsanı forum raporları ile aynı zamanda literatürdeki araştırmalar, bilgisayar korsanlarının motivasyonlarını anlamak için incelenmiş olup, aşağıdaki bulgular tespit edilmiştir.

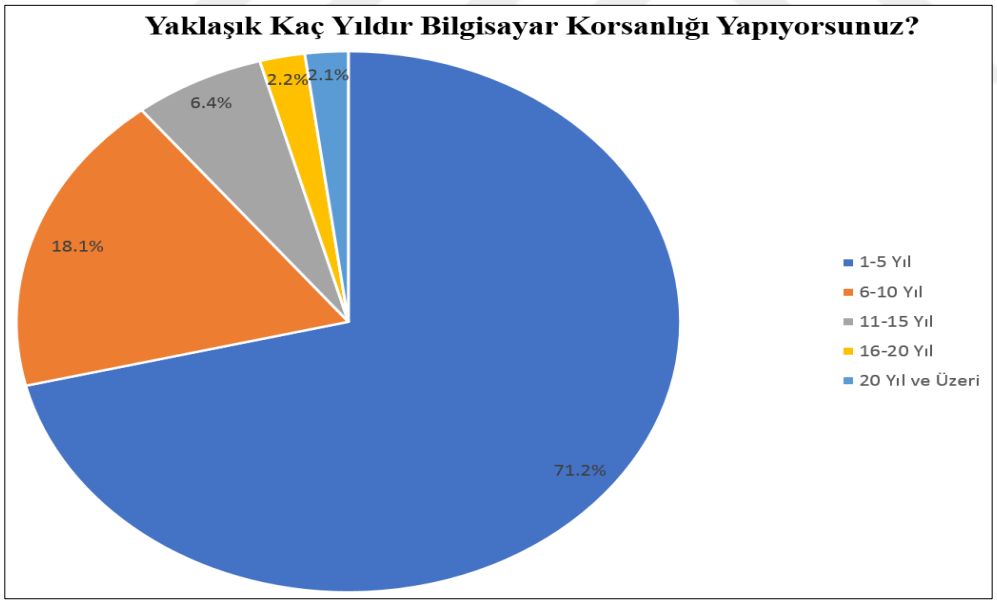
Hackerone, interneti daha güvenli olması ve şirketlerin zayıflıklarını tespit ederek bunların giderilmesi için çalışan bir bilgisayar korsanı topluluğudur. Şekil 3.1'den görüleceği üzere firmanın 195 ülkeden 1700 bilgisayar korsanı ile yaptığı 2018 yılı raporuna göre [43], 2016 yılına göre karşılaştırıldığında bilgisayar korsanlarının bir numaralı motivasyonu olan parasal çıkarların 2018 raporunda 4. Sıraya gerilediği görülmektedir.

Raporda ilk sırayı, bilgisayar korsanlığı yöntemleri ve tekniklerinde yeni bilgiler öğrenmek, ikici ve üçüncü sırayı ise aynı orana sahip olan eğlence ve iddia için bilgisayar korsanlığı yapmak almaktadır. Bu da aslında bilgisayar korsanı çeşitliliğinin de yıllar içerisinde arttığının ve motivasyonlarının da çeşitlendiğini göstergesidir. Bunun yanı sıra son yıllarda siber güvenlik, siber atak, nesnelerin interneti (IoT) gibi konularındaki artış göz önüne alındığında bilgisayar korsanlarının kaç yıldır bilgisayar korsanlığı yaptıkları konusunda da büyük bir kısmın yakın geçmişte olması beklenmekte ve raporda da bu beklenti 1-10 yıldan bu yana bilgisayar korsanlığı

yapanların oranının Şekil 3.2'de görüldüğü üzere yaklaşık %83 çıkması ile desteklenmektedir.



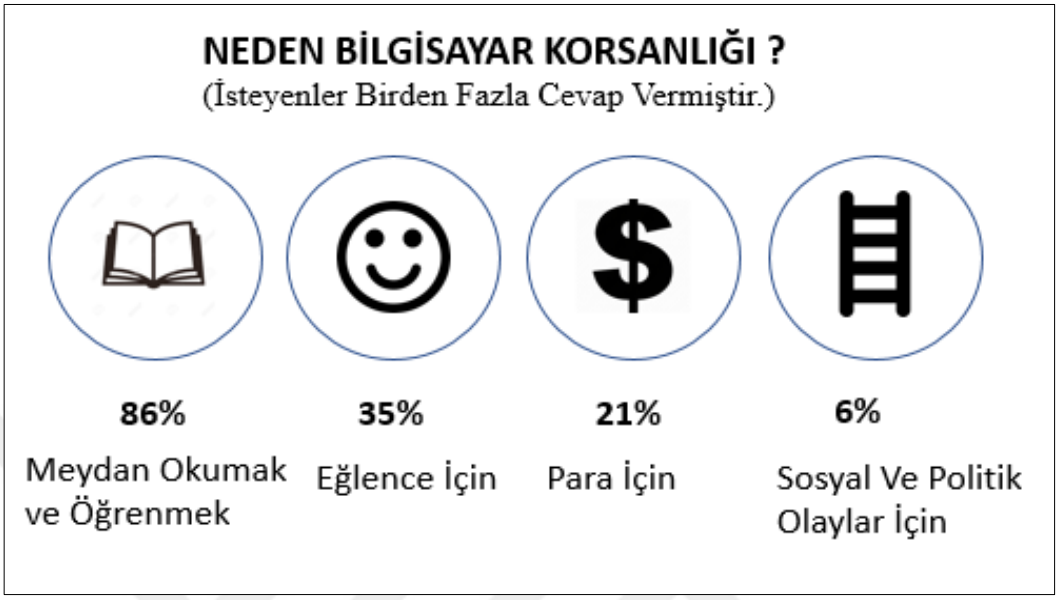
Şekil 3.1 : Bilgisayar korsanlarının bilgisayar korsanlığı motivasyonları 2018 [43].



Şekil 3.2 : Bilgisayar korsanlarının yaklaşık bilgisayar korsanlığı yapma süreleri [43].

Şekil 3.3'de gösterilen başka bir raporda, [44] yapılan araştırma sonrasında bilgisayar korsanlarının bilgisayar korsanlığı işi yapmasının nedeni ankete göre 4 ana başlık altında toplanmıştır. Bir önceki raporlarda örtüşecek şekilde ankete katılan bilgisayar korsanlarının %86'sı bilgisayar korsanlığı yöntemlerini, tekniklerini ve iddia için

bilgisayar korsanlığı yaptığını belirtirken, %35'lik bir oran bilgisayar korsanlığı işlemini eğlence olarak görmektedir. Finansal kazanç tabanlı yaklaşım %21 ile 3. sırada yer almaktadır.



Şekil 3.3 : Bilgisayar korsanlarının bilgisayar korsanlığı motivasyonları 2018 [44].

Raporda, anketin yanı sıra insanların neden suç işlediklerine dair yıllardır oraya atılan teorilerde incelenmiş olup, klasik teori suçluların çıkar ve finansal durumları tarttıktan sonra işlediğini, biyolojik teori, bu kişiler için suç işleme arzusunun önüne geçemediklerini, psikologların teorisinde ise bilinçsizlik ve gelişim aşamasındaki bazı bozuklukların buna neden olduğunu öne sürmüştür.

Bu teorilerin ışığında ortaya çıkan kriminolojik teori, bilgisayar korsanlarının davranışlarını açıklamada birçok teoriye sahiptir ve bu teori, suçun biyolojik, sosyal ve psikolojik etkenlerini belirlemede ve bu sayede de bilgisayar korsanlarının neden suç işlediklerini, motivasyonlarını anlamamıza yardımcı olmaktadır.

İncelenen iki raporun yanı sıra akademik olarak bir literatür taraması yapıldığında yine bilgisayar korsanlarının motivasyonlarının yukarıdakiler ile örtüştüğü görülmüştür. Bazı bilgisayar korsanı gruplarının motivasyonlarına örnek verecek olursak;

- Script kidding bilgisayar korsanları

  Literatürde script kidding bilgisayar korsanlarının motivasyonlarının eğlence ve atak yapmanın vermiş olduğu heyecan olarak tanımlanmaktadır [45].

- Kötü amaçlı yazılım geliştiricileri

  Kshetri, kötü amaçlı yazılım geliştirici olan bilgisayar korsanlarının motivasyonlarını kendi sanal alemlerinde görülür ve popüler olma, saygı duyulması şekilde açıklamaktadır [46].

- Hacktivist bilgisayar korsanları

  Diğer bilgisayar korsanı çeşitlerine nazaran daha az sayıda olan hactivistlerin motivasyonu para değil, tam olarak politik meseleler, yargı kararları ve toplumu politik durumlar ile ilgili aydınlatmaktır [47].

- Hırsız

  Siyah şapkalı bilgisayar korsanlarının bir yan dalı olan hırsız bilgisayar korsanlarının tek amacı parasal kazanç elde etmektir. Kshetri çoğunluğun para ile motive olduğunu fakat bazılarının farklı motivasyonları olduğunu belirtmektedir [46].

- Terörist

  Siber terörizm günümüzün en önemli konuları arasında olmak ile birlikte bu teröristlerin motivasyonları politika olarak gösterilmektedir. Bazı terörist bilgisayar korsanları state sponsored çatısı altında hükümetler tarafından kiralanan bilgisayar korsanları olarak getirtilmektedir [45].

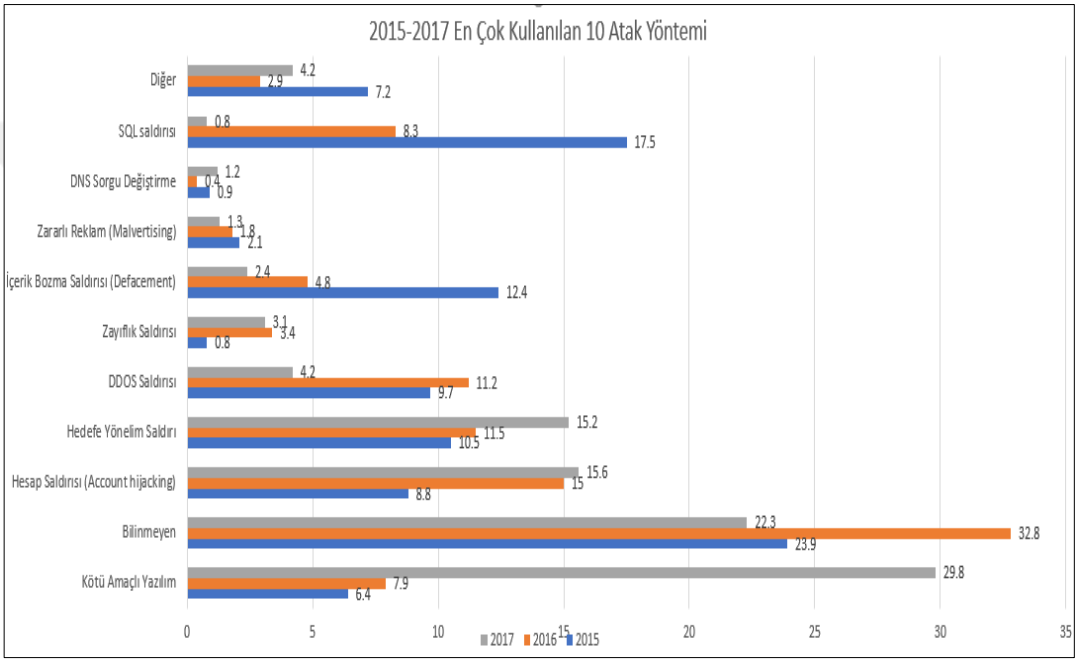
3.4 Bilgisayar Korsanlığı / Siber Saldırı Yöntemleri

Bölüm 2.8'de de belirtildiği gibi nesnelerin interneti kapsamında internete bağlanan cihaz sayısındaki artış ile doğru orantılı olarak, bu cihazların ve dolayısı ile kullanıcıların güvenlik ihlallerine, siber saldırılara, kişisel bilgi çalınması gibi siber olaylara maruz kalma riskinin de aynı doğrultuda artacağı düşünülmektedir.

Artık siber saldırıların sadece bilgisayar sistemleri ile sınırlı kalmayıp, bir ülkenin haberleşme sistemlerine enerji ve ulaşım ağlarına, ulaşım sistemlerine dahi zarar verebileceği, ülkenin gizli evraklarının dahi etkilenebileceği bir saldırı çeşidi haline gelmiştir.

Bu nedenle siber güvenlik ile ilgili bir yönetim modeli incelemesi aşamasında en önemli konulardan bir tanesi de siber saldırıları bilmek ve değişimlerini görmektedir.

2017 yılı siber saldırı istatistiklerinde en sık kullanılan 10 siber atak, 2015,2016 ve 2017 yıllarına göre karşılaştırıldığında, yıllar içerinden siber atak tekniklerindeki değişim Şekil 3.4 da görülmektedir. Bu değişimin başlıca nedenleri arasında gelişen teknoloji, alınan güvenlik önlemleri ve bilinçlenme gösterilebilir. SQLi adı verilen saldırının 2015 yılında istatistikteki saldırıların %17,5 ini oluştururken, 2017 yılında sadece %0,8 ini oluşturması buna örnek verilebilir.

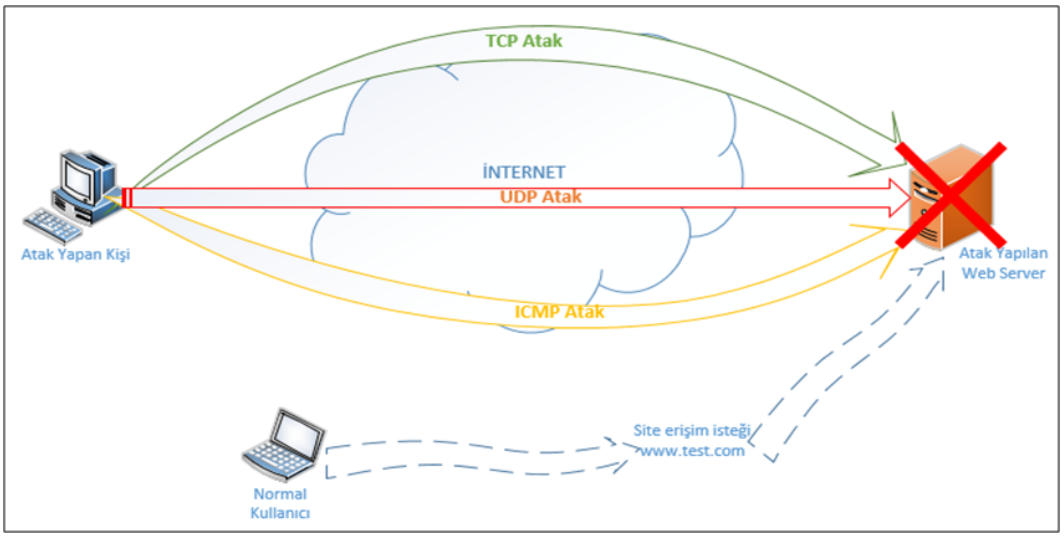


Şekil 3.4 : 2015- 2017 yıllarına göre en çok kullanılan 10 atak karşılaştırması [48].

3.4.1 Servis dışı bırakma saldırıları (DoS & DDoS)

DoS (Denial of Service), en sık kullanılan atak çeşitleri arasından olmak ile birlikte, Türkçe karşılığını "Sistem Çökertme" olarak belirtsek yanlış olmayacaktır. DoS atakları en yıkıcı siber atakların başında gelmek ile birlikte, bugüne kadar iş ve dünya ekonomine en çok zarar veren siber atak çeşidi olarak belirtilmektedir [49].

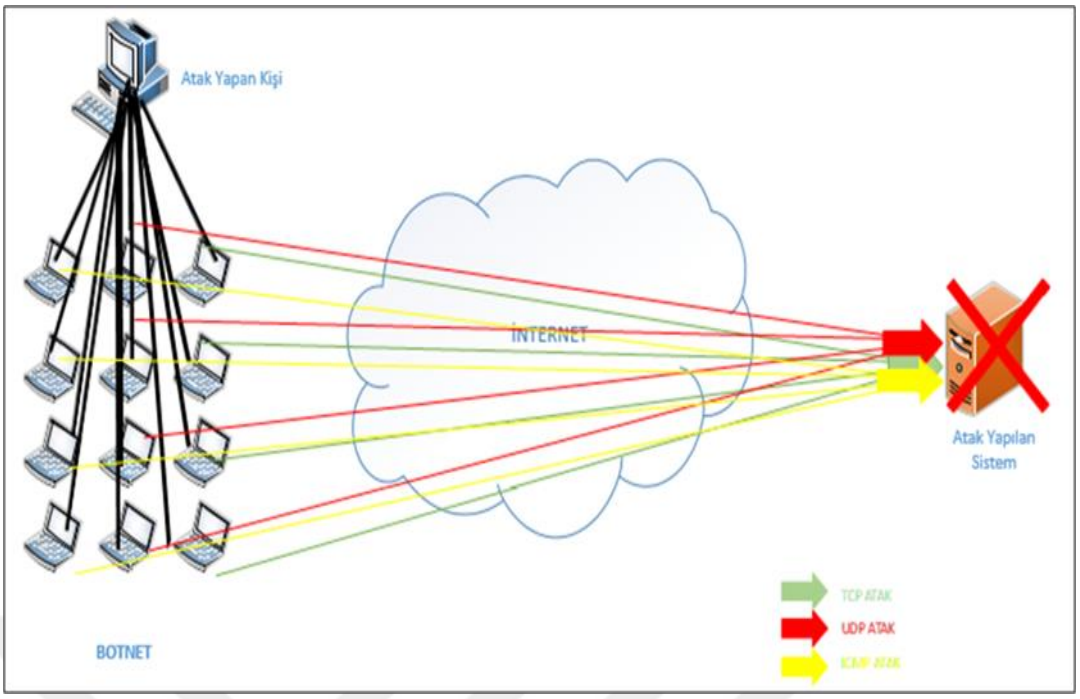
DoS (Denial of Service) ya da biraz önce belirttiğimiz gibi sistem çökertme atağı, atak yapan bir birey tarafından internet bağlantısı ile tek makina hedef alınarak yapılan ve genel mantık olarak da bu hedefe doğru çok sayıda istek, TCP, UDP, ICMP paketleri göndererek en nihayetinde bu sistemin artık cevap veremez ve erişilemez bir hale gelmesine sebep olan bir atak çeşididir. Şekil 3.5'de ana mantığı ile DoS atak topolojisi görülmektedir.



Şekil 3.5 : DoS atağının ana mantığının topolojisi (Yazar tarafından tasarlanmıştır).

DDoS(Distributed Denial of Service) ise DoS'un bir gelişmiş versiyonu [49] olmak ile birlikte, yine hedef üzerine yapılan yüksek sayıda istek ve paketler ile sistemi devre dışı bırakma mantığı ile çalışmaktadır. Dos ile aralarındaki fark ise yapılan atağın yalnızca bir bilgisayardan değil, herhangi bir siteye girildiğinde veya bağlantıya tıklandığında normal bir kullanıcının bilgisayarına inen bir kötü amaçlı yazılım ile birlikte normal kullanıcı bilgisayarlarının, bilgisayar korsanlığı dünyasında köle ağ (botnet) adı verilen bir köle bilgisayarlar grubuna dahil olması ile, dünyanın çeşitli yerlerindeki normal kullanıcıların bilgisayarlarının bu atağı planlayan kişi tarafından DDoS atağı için kullanılması ile olmaktadır. Şekil 3.6'da ana mantığı ile DDoS atak topolojisi görülmektedir.

DDoS atağı DoS atağına göre çok daha etkili olmak ile birlikte dünya üzerinden yapılan DDoS ataklarını izlemek için online internet siteleri dahi bulunmaktadır.



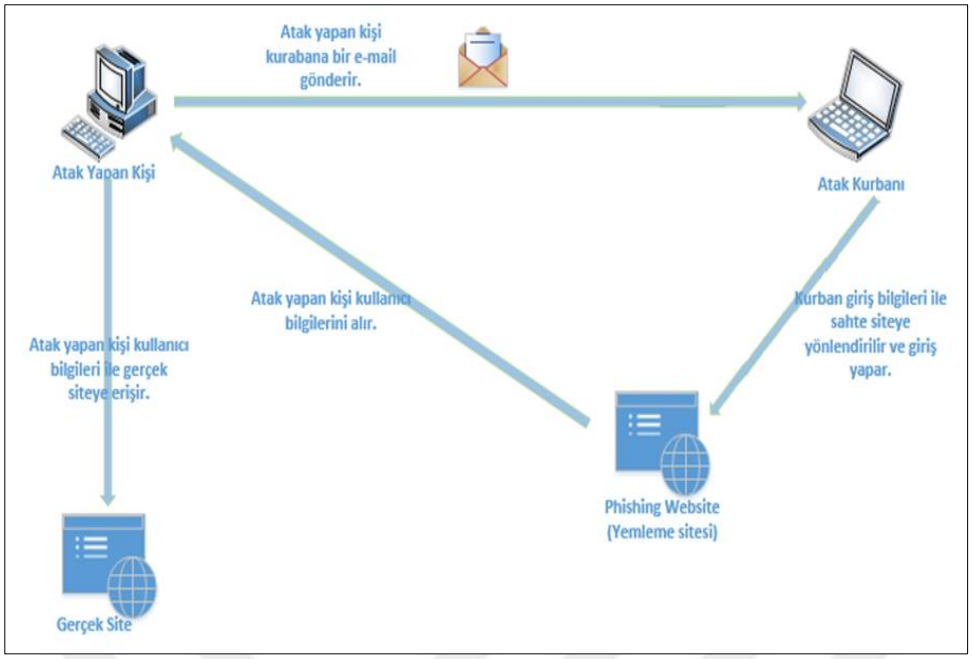
Şekil 3.6 : DDoS atağının ana mantığının topolojisi (Yazar tarafından tasarlanmıştır).

3.4.2 Yemleme - oltalama saldırıları (Phishing)

Oltalama ya da diğer adı ile yemleme saldırısı, sosyal mühendislik saldırı tekniğinin aslında bir parçası olarak görülmektedir. İnternetin hayatımıza hızlı girişi sonrasında alışverişten banka hesaplarımızın yönetmeye, borsada döviz alım satım işlemlerinden hastane raporlarımıza kadar neredeyse her şeye internet üzerinden erişimimiz bulunmakta ve bunlara kişisel kullanıcı bilgilerimiz ile erişim sağlamaktayız.

Özellikle bankacılık ve alışveriş denildiğinde dikkat edilmesi gereken en önemli atakların başında yemleme tekniği gelmektedir. E-Bay, Paypal başta olmak bankaların online siteleri bu saldırı ile en çok karşı karşıya gelen firmalardır [50].

Bu saldırıda temel mantık, yemleme atağı yapan kişi tarafından gerek banka gibi gerekse bir alışveriş sitesinden gelmiş gibi gönderilen bir mail üzerinden kullanıcının sahte fakat gerçeğine neredeyse birebir kadar benzeyen bir siteye yönlendirme ile başlamaktadır. Daha sonra sitenin sahte olduğunu anlamayan kullanıcı bilgilerini buraya girmekte ve atak yapan kişi arka tarafta bu kullanıcı bilgilerini çalmaktadır. Şekil 3.7'de yemleme saldırısının nasıl gerçekleştirildiği görselleştirilmiştir.



Şekil 3.7 : Oltalama-Yemleme (Phising) Saldırıları (Yazar tarafından tasarlanmıştır).

3.4.3 Araya giren adam saldırısı (Man in the Middle Attack (MitM))

- Şebeke trafiğinin dinlenmesi (Sniffing - Monitoring)
- IP/ DNS aldatmacası - gizlenmesi (IP/DNS Spoofing)…

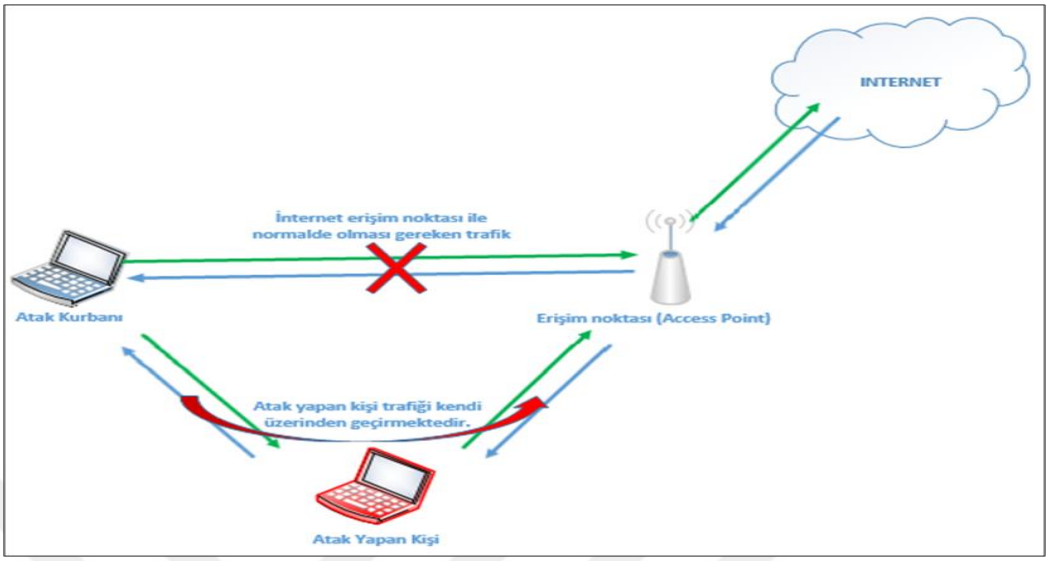
Ayrı ayrı olarak da incelenebilecek olan şebeke trafiği dinlemesi ve IP/DNS aldatmacası saldırıları aslında ana mantık olarak atak yapan bir kişi tarafından kullanıcı ile sunucu arasına sızmaya dayandığından orjinal adı man in the middle attack olan siber saldırı başlığında incelenebilmektedir. Türkçe çevirisi araya giren kişi saldırısı olarak tanımlansa yanlış olmayacaktır.

Araya giren kişi atağı adresi çözümleme protokolü (ARP) ve alan isimlendirme sistemi (DNS) protokollerinin kötü niyetli olarak manipülasyonu ile gerçekleştirilmektedir [51].

Özellikle ortak alanlarda herkese açık kablosuz internet bağlantılarında bu atak tipine rastlamak çok olasıdır. Atak yapmayı planlayan kişi bu atağı birçok şekilde yapabilmektedir. En yaygın olarak gerçekleştirilen ataklar şebeke trafiği dinlemesi ve IP aldatmacasıdır. Yöntem ise kurulan bağlantının arasına sızmaktır.

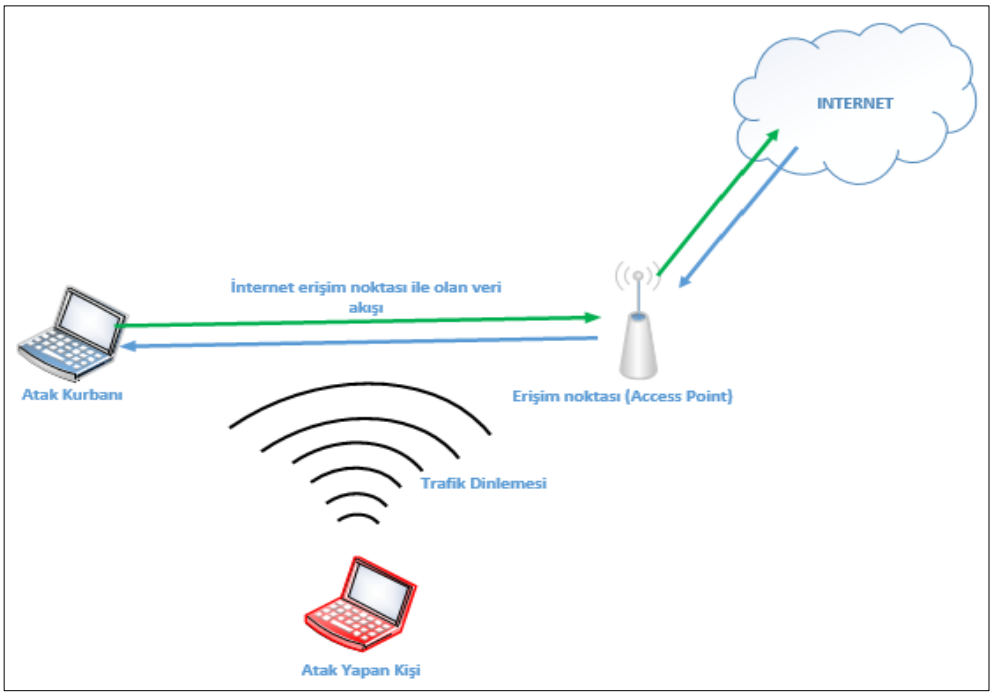
IP aldatmacası ile atak yapan kişi internet kullanıcısı kişi ile internet erişimi sağlayan erişim noktası arasına kendisini yerleştirerek kullanıcının erişim noktasına gönderdiğini zannettiği verileri kendi üzerinden geçirir ve erişim noktasından gelen

cevapları da kullanıcıya yine kendisi üzerinden geçirerek trafiği izleyebilmektedir. IP/DNS aldatmacası Şekil 3.8'de gösterilmiştir.



Şekil 3.8 : Man in the middle / IP aldatmacası (Yazar tarafından tasarlanmıştır).

Diğer bir yöntem olan şebeke trafiğinin dinlenmesin de ise Şekil 3.9'den de görüleceği üzere yine atak yapan kişi, direkt kullanıcı ile erişim noktası arasında kurulan bağlantı üzerindeki trafiği çeşitli paket yakalama araçları sayesinde dinlemektedir ve bu sayede kullanıcı adı, şifre, kişisel veriler ve bunun gibi birçok veriye ulaşabilmektedir.



Şekil 3.9 : Man in the middle / Şebeke trafiği dinlemesi (Yazar tarafından tasarlanmıştır).

3.4.4 Sosyal mühendislik (Social Engineering)

Sosyal mühendislik en kısa ve öz tanımı ile herhangi bir kod yazmaksızın bilgisayar korsanlığı işleminin gerçeklemesi olarak tanımlanmaktadır. Teknolojiyi üst düzeyde kullanılarak, kod yazarak, bilgisayarları ele geçirerek yapılan saldırıların yanı sıra sosyal mühendislik saldırısında, kişinin insani zafiyetlerinden (güven duyma ihtiyacı, aceleci davranma, korku, merak vb.) yararlanmak temel alınmaktadır. Bu nedenle atak yapan kişi, atak yapacağı hedef ile ilgili ilk olarak, özellikle sosyal ağ siteleri üzerinden bir araştırma yapmakta ve ardından ikna, etkileme ve/veya tehdit yolları ile kişiden bilgiler almakta veya atak yapan kişi, kandırılan kurbana kendisi adına zararlı ve tehlikeli işleri yaptırmaktadır [52].

Sosyal mühendislik siber atak türü Şekil 3.10'da da gösterildiği gibi 4 evreden oluşmaktadır [53].

- Araştırma evresi (Investigatin)

  Hedef Belirleme

  Kurbana ait bilgileri toplama

- Kanca atma evresi (Hook)

  Etkileşimde kontrolü sağlama

  Hikayeler uydurma

  Hedefi meşgul et

- Oynama/ harekete geçme evresi (Play)

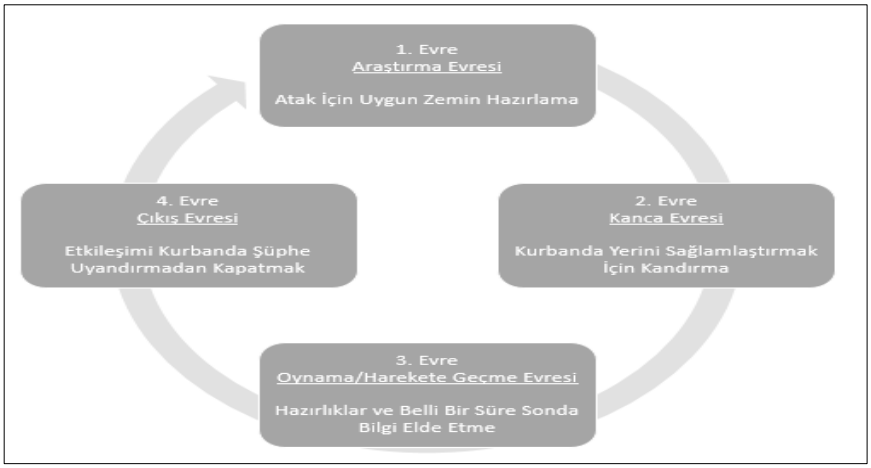
  Kurbanda ki yerini sağlamlaştırma

  Atak yapma

  Data hortumlama

- Çıkış evresi (Exit)

  Tüm izleri kapatarak ve yok ederek olağan gir şekilde etkileşimi bitirmek



Şekil 3.10 : Sosyal mühendislik hayat döngüsü [53].

En çok kullanılan sosyal mühendislik yöntemleri ise şunlardır [54]:

- Kurbanın dikkatini çekme ve aç gözlülüğünü uyandırmak için sahte sözler vermek,
- Herhangi bir faydaları olmayan ancak kullanıcıya virüslere karşı en iyi korumayı vadeden yazılımların uygulamaya konulması
- Yemleme, oltalama
- Güvenilir bir kaynak olduğuna karşı tarafı ikna etmek,
- Genel olarak sahte senaryolar uydurmak,
- Sosyal paylaşım sitelerinde, ortak tanıdıklar üzerinden yakınlık kurarak, bilgi, para vb. elde etmek,
- Başka bir kişiyi taklit ederek, telefon veya e-posta yolu ile sanki bu kişiymiş gibi iletişim kurmak,
- Karşı tarafın zor durumda olduğunu ve bu sebeple yardım ediyormuş izlenimi vermektir.

3.4.5 Kabloya saplama yapma (Wiretapping)

Cai and Yeung [55]' ın daha güvenli ağ kodlamasının teorisinin ele alındığı akademik makalede bahsedildiği üzere, güvenliği tam olarak sağlanmamış ağ kablolarına özel teçhizatlar ile fiziksel olarak kurulan bir bağlantı üzerinden gönderici ile alıcı arasındaki tüm trafiğin, konuşmaların, vb. yetkisi olmayan üçüncü kişiler tarafından dinlenmesi/ele geçirilmesine yönelik siber saldırı türüdür.

3.4.6 Açık mikrofon dinleme

Son zamanlarda akıllı telefon sayısındaki artış nedeniyle bir hayli popüler olan açık mikrofon dinleme saldırısı, bilgisayarların ve cep telefonlarının mikrofon ve kameralarının casus yazılım sayesinde istenildiği zaman erişime açılarak ortamın sesinin dinlenmesi ve görüntüsünün anlık olarak alınmasına neden olmaktadır.

Son yıllarda çıkan wikileaks belgelerinde dahi bu iddia yer bulmuş ve haberlerde de bazı istihbarat örgütlerinin bu yöntem ile ortam dinleme ve anlık görüntü erişimi elde ettikleri iddia edilmiştir [56].

3.4.7 İstem dışı yığın ileti (E-posta) gönderme (Spam - Junk Mail)

Saldırının da adından tahmin edileceği üzere istem dışı yığın ileti gönderme yöntemi ile yapılan siber saldırı tipinde, kullanıcıya, bilgisi dışında ve istemsizce yüzlerce elektronik postanın gönderilmesine dayanmaktadır. Bu saldırı tipi genellikle pazarlama, alışveriş ve kampanya kodları dağıtan web sitelerinde olmakta ve daha çok bilgisayara zarar vermek veya yemleme yolu ile kullanıcıları dolandırmak için kullanılmaktadır.

Bu saldırı türünden korunmak için alınan en yaygın önlemler, birincil e-posta adresinin pazarlama firmalarına ve/veya kampanya kodu dağıtan firmalara verilmemi, bilinmeyen kullanıcılardan gelen e-postaların önemsiz kategorisine konulması, e-posta filtreleme kullanılmasıdır [57].

3.4.8 Şifre atağı (Brute Force, Dictionary Attack)

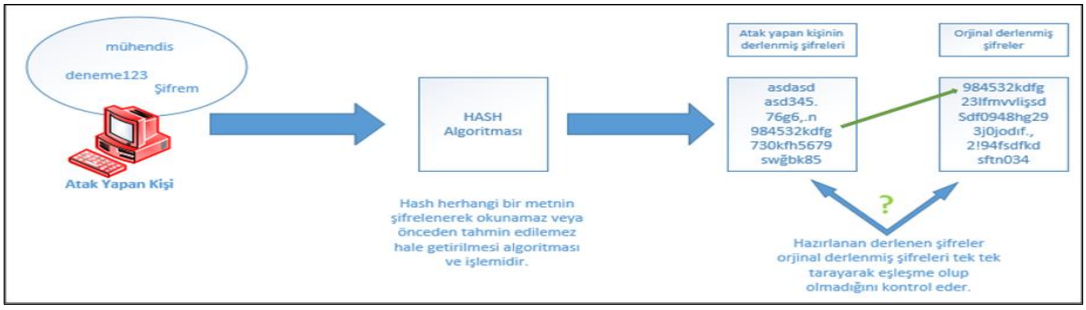
- Kaba kuvvet (Brute Force)
- Sözlük atağı (Dictionary Attack)

Kaba kuvvet (Brute Force) ve sözlük atağı (Dictionary Attack), atak teknikleri bakımından küçük farklılıklar gösterse de temelde ikisi de şifreleri deneme yöntemi kırmayı deneyen birer saldırı türüdür. Bu nedenle bu iki saldırı türünü tek başlık altında toplamak yanlış olmayacaktır. Aralarındaki saldırı tekniğindeki farklılığa gelecek olursak şu şekilde açıklanabilmektedir.

Kaba kuvvet (Brute Force) saldırısında atak yapan kişi sisteme verdiği düz metinleri hash algoritması kullanarak yeni bir derlenmiş şifre listesi elde eder ve bu listeyi saldırı yaptığı veri tabanındaki şifreler ile karşılaştırarak bir eşleşme elde etmeyi bekler. Bu

saldırıda sisteme verilen düz metinler için bir sosyal mühendislik yapılabilir ve kişinin işi, yaşı, iş yer, unvanı gibi kelimeler sisteme verilebilir.

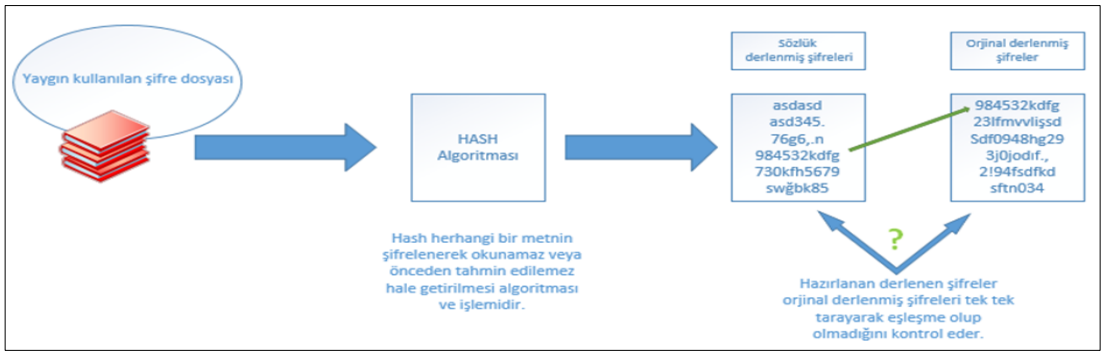
Kaba kuvvet (Brute Force) saldırısının ana mantık şeması Şekil 3.11'de gösterilmiştir.



Şekil 3.11 : Kaba kuvvet (Brute Force) ana mantığı topolojisi (Yazar tarafından tasarlanmıştır).

Sözlük atağında (Dictionary Attack) ise kaba kuvvet (Brute force) atağından farklı olarak, kaba kuvvet atağından derlenmiş şifre oluşturmak için verilen düze metinler sosyal mühendislik kullanılarak atak yapan kişi tarafından verilirken, sözlük atağın da ise en yaygın kullanılan şifrelerin olduğu dosyadan derlenmiş şifrelerin oluşturulmasıdır [58].

Sözlük atağı saldırısının ana mantık şeması Şekil 3.11'de gösterilmiştir.



Şekil 3.12 : Sözlük atağı (Dictionary Attack) ana mantığı topolojisi (Yazar tarafından tasarlanmıştır).

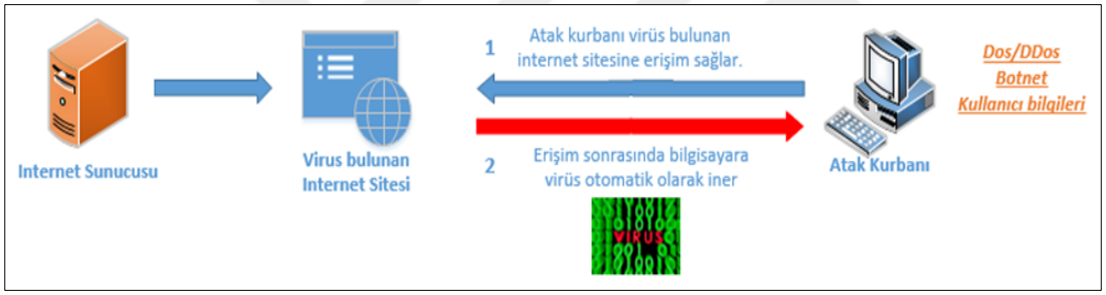
3.4.9 Zararlı yazılım kullanımı (Virüs-Solucan-Truva Atı vb.)

Zararlı yazılım kullanma saldırıları son yılların en çok kullanılan saldırı türlerindendir. Bu artış 2015-2106 ve 2017 yıllarının karşılaştırılmasını yapıldığı Şekil 3.4 de açıkça görülmektedir. Yine başka bir raporda [35] 2016 yılına kıyasla zararlı yazılım saldırılarında ki artış mac cihazlarda %80 olarak belirtilmiş olup, bilgisayarlara internet ortamından indirilen zararlı yazılım sayılarında ise mevcut zararlı yazılımların

geliştirilmiş sürümleri ve yeni ortaya çıkan zararlı yazılımlar olarak toplam değerlendirildiğinde %92 artış görülmektedir.

Zararlı yazılımların bilgisayarlara en sık bulaşma yöntemi internet veya e-posta olarak bilinmektedir. Bu iki yöntemde de bilgisayara virüs indikten sonra bilgisayar DDOS bölümünde anlatıldığı üzere botnet'e dahil olabilir veya kullanıcı bilgileri ve belgeleri çalınabilir. Şekil 3.13 ve Şekil 3.14'te truva atı ve virüs birleşimi ile bu virüslerin bilgisayarlara en sık bulaşma yöntemi gösterilmiştir.

Şekil 3.13 da gösterildiği üzere truva atı bilgisayara hiçbir uyarı olmaksızın otomatik iner. Kullanıcının bu işlemden bazı durumlarda haber dahi olmamaktadır. Şekil 3.14'de ise e-postayı sorgulamadan açan ve sıkıştırılmış dosyaları direkt olarak bilgisayarına indiren kullanıcılar büyük risk altındadır. Bilgisayara indirme işlemi sonrasında atak yapan kişi, bilgisayara için asıl kullanıcı için aynı önceliğe sahip olmaktadır [59].



Şekil 3.13 : Zararlı yazılım internet sitesi uygulaması (Truva atı ve Virüs) (Yazar tarafından tasarlanmıştır).

Şekil 3.14 : Zararlı yazılım e-posta uygulaması (Truva atı ve Virüs) (Yazar tarafından tasarlanmıştır).

3.4.10 Arka kapı kullanımı (Backdoor - Trapdoor)

Arka kapı kullanımı, genellikle gizli yollarla yapılan ve kimlik doğrulama mekanizmasından sıyrılarak uzak bilgisayarlara, sistemlere kısacası bilgi ve iletişim teknolojilerine izinsiz bir şekilde erişim sağlamayı amaçlayan bir siber atak türüdür.

Arka kapılar genellikle test edilen bir sisteme erişim için sistemin geliştiricisi tarafından açık bırakılmakta fakat unutulması durumunda ise kötü niyetli kişiler tarafından port tarama ile tespit edilerek arka kapı saldırısı amacı ile kullanılabilmektedir. Bunun yanı sıra bazen sistemi geliştiren kişi bu arka kapıları kasten bırakabilmektedir [60].

3.4.11 SQL veri tabanı saldırısı (SQL injection attack)

SQL enjeksiyon saldırısı veri tabanı kullanan internet siteleri için büyük bir sorun teşkil etmektedir. Şekil 3.4'den görüleceği üzere son yıllarda popülerliği düşmekte olmasına rağmen sürekli olarak göz önünde bulundurulması gereken bir tehdittir. SQL komutları, giriş ve şifre gibi bilgilerin içerisine gömülerek gönderilmektedir. Başarılı bir SQL atağı, veri tabanına erişim sonrasında verilerin okunmasına, değiştirebilmesine hatta veri tabanında yetkili komutları dahi çalıştırabilmesine olanak sağlamaktadır [61].

4. DÜNYA SİBER TARİHİNE YÖN VEREN ÖNEMLİ SİBER SAVAŞLAR VE ZARARLI YAZILIMLAR

4.1 Kosova Krizi - 1999

Bağımsızlık isteyen Kosova'ya karşı dağılma sürecinde olan Yugoslavya Federal Cumhuriyeti ordusunun tepkilerin dur demek için Uluslararası Askeri İttifak olarak bilinen NATO tarafından Birleşmiş Milletler Güvenlik Konseyi'nden müdahale kararı çıkmamasına rağmen, mart -haziran tarihleri arasında çeşitli Sırbistan hedeflerine hava saldırıları düzenlemiştir [62].

NATO hava saldırıları ile Sırbistan hedeflerinin vurulmaya başlanması ile birlikte "Black Hand" isimli bilgisayar korsanlarının oluşturduğu topluluk, Amerika Birleşik Devletleri ve NATO'yu hedef alacak şekilde siber saldırılara başlamıştır. Asıl amaçları NATO askeri operasyonlarını durdurmak olan siber korsanlar, ilk büyük siber savaşın mimarları olmuşlardır. Savaş sırasında "Black Hand" bilgisayar korsanları grubunun NATO'ya ait en önemli bilgisayarları ele geçirdiği ve bilgisayarlar üzerindeki tüm verileri sildiği iddia edilmektedir [63]. Bunu yanı sıra hava operasyonları sırasında Belgrad'da bulunan Çin Büyükelçiliğinin de yanlışlıkla bombalanması sonucu Çinli siber korsanlar da siber saldırılarla ABD ve NATO devlet web sitelerine saldırmışlardır.

NATO ve ABD'ye karşı Sırp bilgisayar korsanları grubunun yapmış olduğu siber saldırıda daha ilerleyen zamanlarda Estonya ve Gürcistan örneklerinde de göreceğimiz gibi "DDOS" yani servis durdurma saldırısı ve binlerce zararlı virüsün olduğu bağlantı içeren elektronik posta gönderilmiştir. Bu nedenle NATO'nun resmi internet sayfası virüslerden temizlenmek için günlere kapalı kalmıştır. Fakat yapılan siber saldırılar incelendiğinden saldırılarda Sırp bilgisayar korsanlarına ek olarak Çinli ve Rus bilgisayar korsanı topluluklarından olduğu fark edilmiştir [64].

Uluslararası Askeri İttifak'ın (NATO) ilk defa bir siber saldırı ile karşı karşıya kaldığı siber savaş olarak tarihe geçen Kosova Krizi, bize ülkelerin, siber uzayda da tıpkı reel politikada olduğu gibi ittifak yaptıklarını ortaya koymuştur. Bu nedenle günün

sonunda Kosova Krizi, siber uzayın uluslararası aktörler tarafından hukuki olarak düzenlenmesi gerektiği ihtiyacını gündeme getirmiştir [62].

4.2 ABD ve Çin Arasında Yaşanan Siber Saldırılar - 2001

Çin Halk Cumhuriyet'i ile artan gerilim ve yaşanan siber olaylar sonrasında, 26 Nisan 2001 tarihinde Amerika Birleşik Devletleri İç İstihbarat ve Güvenlik Gücüne bağlı olan Ulusal altyapıyı koruma merkezi tarafından 01-009 numaralı yayını yapılmış ve bu bildirisinde Amerika Birleşik Devletleri ile Çin Halk Cumhuriyeti arasında yaşanan siber olaylar nedeniyle internet sitelerinin bilgisayar korsanları tarafından ele geçirildiğine ve kullanılamaz hale geldiğine dikkat çekmiştir. Ayrıca internet sitelerine yapılan saldırıların Çin Halk Cumhuriyeti için yüksek önem arz eden günlerde veya Amerika ile Çin arasındaki gerginliklerin yıldönümüne geldiğine dikkat çekmektedir.

İki ülke arasında tansiyonları yükselten olaylara baktığımızda aşağıdaki iki olay ön plana çıkmaktadır.

- Kosova Savaşı'nda Çin'in Belgrad Büyükelçiliği'nin Bombalanması 1999 yılında bir NATO jeti Kosova Savaşı sırasında Çin büyükelçiliğini bombaladı. En az 12 saat sonra Çin'in Kızıl Bilgisayar Korsanları Birliği ABD web sitelerine karşı binlerce siber saldırı başlattı [65].
- 2001 yılında bir Amerikan casus uçağı ile Çin jeti pasifikte çarpışmıştır. Çin jeti düşünce Çinli bilgisayar korsanları Beyaz Saray'ın sitesine saldırmıştır [66].

Yaşanan bu olaylar sonrasında iki ülke arasındaki tansiyonlar son derece yükselmiş ve yukarıda bilgiler ışığında da beklenildiği üzere iki ülke arasında siber saldırılar başlamıştır. Bu siber saldırılar sırasında Amerika Birleşik Devletine ait internet çok sayıda internet sitesi Çinli bilgisayar korsanı tarafından ele geçirilmiş ve hatta Çinli bilgisayar korsanları "USA Kill" ve "China killer" başlıkları ile forumlar açmışlardır [67].

Yaşanan siber saldırılara ek olarak bir diğer konu da Amerika Birleşik Devletleri İç İstihbarat ve Güvenlik Gücü tarafından araştırılan, arkasında yine Çinli bilgisayar korsanları olduğu düşünülen Kaliforniya eyaletinin elektrik şebeke sisteminin 17 gün boyunda ele geçirilmesidir [67].

Amerika Birleşik Devleti, Çin'i ilk kez resmi olarak 2013 yılında yayınladığı yıllık raporunda uyarmıştır. Bu raporda Çin Halk Cumhuriyeti'nin başta Amerika olmak üzere birçok ülkenin savunma, strateji, diploması bilgilerini çaldığını açıkladı. Bunun yanı sıra Madiant şirketi de Şubat 2013 tarihli raporunda Çin'in gizili bir askeri birliğinin ABD şirketlerine casusluk amaçlı saldırılarda bulunduğunu ve 140 şirkete yönelik saldırının Çin Halk Kurtuluş Ordusu ile bağlantısının olduğunu belirtmiştir [65].

Hatta bazı uzmanlar, Çinlilerin dünya üzerindeki en saldırgan siber saldırıları yapan bilgisayar korsanlarının ülkesi olarak tanımlamakta ve bundan dolayı, NATO ile Çin sisteminin entegre edilmesi halinde, Çinli program yazılımcılarının NATO bilgi sistemine sızma ihtimali tehlikesine dikkat çekmişlerdir.

İki ülke arasında yaşanan bazen diplomatik bazen bir kaza eseri gerçekleşen olaylarda dahi, siber dünyanın ne kadar hızlı bir şekilde oyunda rollerin değişmesine en güzel örneklerden birisidir Amerika ile Çin arasındaki ilişki, aynı zamanda bu saldırılar ile birlikte aslında sadece bilgisayar ve internet altyapısının değil, şehirler için kritik altyapılarında siber saldırılardan etkileneceğinin en güzel örneklerindendir.

4.3 Estonya Siber Saldırısı -2007

Estonya ile Rusya Federasyonu arasındaki ilişkiyi tarihsel süreçte kısa bir şekilde ele alacak olursak, iki ülke arasından demografik ve sosyokültürel yapıları kapsamında bazı gerginlikler olduğu görülecektir. Sovyet Sosyalist Cumhuriyetler Birliği tarafından Estonya'ya önemli oranda Rus nüfus yerleştirilmesi, Doğu Blok'unun yıkılması sonrasında Estonya'nın Rus azınlığa vatandaşlık verme konusunda isteksiz tavrı Estonya ile Rusya Federasyonu arasında uzun zamandır devam eden bir gerginliğe neden olmuştur.

İkinci Dünya Savaşı'nda Alman askerlerine karşı savaşırken ölen Sovyet askerlerini simgeleyen heykelin 26 Nisan 2007 tarihinde Talin Meydanından kaldırılması kararı ile birlikte Estonya'ya karşı siber güvenlik tarihine geçen çok büyük bir servis durdurma saldırısı gerçekleştirilmiştir. Estonya'nın geçmişte Rusya Federasyonu ile yaşanan ve halen günümüze kadar gelen sorunlar göz önüne alındığında bu siber saldırının Rusya Federasyonu kaynaklı olduğu düşünülmektedir [68].

2007 yılında Avrupa ülkeleri arasında dijitalleşme ve interneti kabullenme, kullanma verileri göz önüne alındığından Estonya en önde gelen ülke konumundadır. Ülke genelinde toplumu %98'i bir şekilde internet kullanımı yapmaktadır. Bu kadar geniş bir internet ortamı tabii ki de ülke ekonomisinin en önemli dayanağı haline gelmiştir. Dünya üzerindeki en gelişmiş e-devlet yapısının yanı sıra internet bankacılığı, elektronik medya gibi birçok internet ve haberleşme teknolojileri bulunmakta ve bunlarda ülke ekonomisine büyük katkı sağlamaktadır. Estonya internet üzerinden oylama yapmayı, ülke seçimlerine entegre ederek seçimleri oy kullanma işlemini bu şekilde yapan ilk devlet olarak Dünya tarihine geçmiştir [69].

Bazı verilere göre Estonya, halkının %60'a yakının günlük ihtiyaçlarının önemli bir kısmını internet üzerinden karşıladığı, ülkedeki bankacılık işlemlerinin yaklaşık %96'sinin internet bankacılığı aracılığı ile internet üzerinden gerçekleştirildiği belirtilmiştir. [70] Bu seviyede bir internet kullanımının olduğu, devletin altyapılarının bu denli internet üzerinden sağlandığı bir ülkede bu sistemlere yapılan saldırının da etkisi bir o kadar katlanarak artmıştır. Estonya'ya karşı yapılan servis dışı bırakma saldırısı (DDOS) bölüm 3.4.1'de ayrıntı olarak anlatılmıştır. Bu bilgilerin de ışığında Estonya'ya yapılan servis dışı bırakma saldırısı ile bankacılık, finans, medya kuruluşları, devlet kurumları, ülke resmi internet sitesi gibi birçok sisteme saldırılar yapılmış ve ülkenin internet altyapısı çökertilmek istenmiştir.

Estonya, ulusal internet ağını yurtdışından erişime kapatma kararı alması ile saldırılardan kurulsa da saldırılardan çok fazla zarar görmüştür. Estonya olayı, siber uzayın, politik amaçlar uğruna kullanılmaya başlandığının ve bu ortamı artık devletlerin rekabet alanı olarak gördüklerinin bir miladı olmuştur.

4.4 İsrail Orchard Operasyonu – 2007

2007 yılında IAF (Israel Air Force, İsrail Hava Kuvvetleri) pilotları Suriye sınırlarına radarlar tarafından tespit edilmeksizin girmiş ve 17 ton mühimmatı Suriye'nin nükleer materyaller ile dolu olduğu düşünülen askeri tesisinin üzerine bırakmıştır. Bu saldırı sonrasında da İsrail hava kuvvetleri pilotları burunları dahi kanamadan kaçabilmişlerdir. Bu saldırı yapılır yapılmaz İsrail hava kuvvetlerinin Suriye'nin güçlü savunma altyapısını siber kapasitelerini kullanarak alt ettiği konusunda söylendiler başlamıştır. Konu ile ilgili olarak Israil savunma kuvvetlerinin en büyük birimi olarak

bilinen “Birim 8200”, Suriye’nin Kuzey Kore ile birlikte nükleer başlıklar ile ilgili çalıştığını konusunda Amerika ulusal güvenli birimine ihbar etmiştir [71].

Peki 6 Eylül 2007 tarihinde gerçekleşen bu saldırıda nasıl oldu da İsrail’e ait saldırı yapan uçaklar radarlar tarafından tespit edilemedi?

Saldırı 5 Eylül saat 23:00 gibi İsrail’in kuzeyinden ayrılan 10 adet İsrail savaş uçağının 7 tanesi Suriye tarafına ayrılması planlanarak yapılmıştır [71].

Saldırı gecesi İsrail, Suriye’nin hava savunma sistemlerini ele geçirmiş ve sistemler ile istedikleri düzenlemeleri yapmaları sayesinde Rus yapımı hava savunma sistemleri ve radarlar İsrail uçaklarını tespit edememiştir.

Der Spilger’e göre Suriye’nin Kuzey Kore ile birlikte nükleer savaş materyalleri projesi ile ilgili bilgilerin alınmasında da ayrı bir siber olay yatmaktadır. İsrail gizli haber alma örgütünün Suriyeli bir hükümet çalışanının bilgisayarını Orchard saldırısından yaklaşık 1 yıl önce ele geçirdiği belirtilmiştir. Ayrıca yine aynı şekilde 2006 yılının sonlarından hükümet çalışanı kişi Londra’da Kensington bölgesinde otelde konaklar iken bilgisayarı odasında bıraktığında bir Israil gizli servis ajanı tarafından içerisine Truva atı adı verilen virüs yüklendiği de belirtilmiştir [72].

Bu olay son teknoloji ile üretilmiş ve çok yüksek güvenlilik sağladığı düşünülen savunma sistemlerinin bile siber saldırılar sonucunda nasıl çalışamaz duruma getirilebildiğinin kanıtı olmakla birlikte, siber savaşın net bir örneği olma özelliği taşımaktadır.

4.5 Gürcistan Siber Saldırısı - 2008

Estonya’ya karşı gerçekleştirilen siber saldırıların üzerinden bir yılı çok kısa bir süre geçmişti ki Estonya da kullanılan teknik ile çok benzer fakat bazı farklılıklardan dolayı farklı kategoride değerlendirilebilecek olan Gürcistan siber saldırıları yaşanmıştır. Gürcistan’a yönelik gerçekleştirilen siber saldırıların neden farklı bir kategoride değerlendirilebileceğini, Estonya siber saldırısından ne gibi bir farklı yanı olduğunun analizini yapabilmek için Rusya ile Gürcistan arasındaki politik anlaşmazlıkları da incelemek gerekmektedir.

Sovyet Sosyalist Cumhuriyetler Birliğinin dağılması sonrasında Abhazya ve tam olarak Rusya ile Gürcistan arasında kalan Güney Osetya bölgeleri bağımsız bölgeler

olarak varlıklarını sürdürmektedirler. 7 Ağustos 2008 yılında Gürcistan'ın Güney Osetya bölgesine asker çıkarmasına cevap olarak, Rusya devleti de 8 Ağustos 2008 yılında Güney Osetya'ya girmiştir. Rusya'nın Gürcistan karşısında aldığı bu kararın başlıca nedenleri arasında Gürcistan'ın NATO ya tam üyelik isteği ve batı devletlerin yaklaşım çabası geldiği birçok kaynakta ileri sürülmektedir [68].

Gürcistan'a yönelik siber saldırılar ise 7 Ağustos 2008 gecesinden itibaren Estonya saldırısına benzer şekilde ülkenin kritik altyapılarını hedef alan "DDoS" saldırıları şeklinde başlamıştır [64].

Gürcistan'a karşı yapılan siber saldırı her ne kadar Estonya'ya saldırısına benzer bir şekilde medya, banka, hükümet, finans, sağlık, internet sayfaları ve buna benzer birçok sistemlerine çok yoğun istek yaparak sistemlerin çökmesini hedef almış olsa da Estonya saldırılarında olduğu kadar etkili olmamıştır. Bu nedeni saldırının gerçekleştiği dönemde Gürcistan nüfusunun sadece %10'unun o dönemde internet erişiminin olmuş olmasıdır. Bu nedenle bu saldırı Estonya saldırıları ile karşılaştırıldığında kısmen etkili olmuştur [73].

Daha önce Gürcistan'a karşı gerçekleştirilen siber saldırıların Estonya'ya karşı gerçekleştirilen siber saldırılar ile her ne kadar benzerlik gösterse de ayrı bir kategoride incelendiğini belirtilmişti. Yaşanan siber saldırı ve durum tarihçesi göz önüne alındığından Gürcistan siber saldırıları literatürde genel kabul gördüğü üzere gerçek bir hibrit savaş niteliği taşıyan ilk sıcak çatışma olduğudur. Yani geleneksel savaş yöntemleri ile birlikte siber saldırının da bir silah olarak kullanıldığı ilk örnektir [68].

Gürcistan siber saldırılarının en çarpıcı sonuçları arasında NATO Siber Savunma Mükemmeliyet Merkezi tarafından Kasım 2008 yılında yayınlanan "Gürcistan'a Karşı Gerçekleştirilen Siber

Saldırılar: Belirlenen Yasal Dersler" isimli bildiridir. Bu bildiriye göre Rusya ile Gürcistan arasından meydana gelen siber saldırılara karşı Silahlı Çatışma Hukuku'nun (Law of Armed Conflict - LOAC) uygulanabilirliği üzerinde görüşmeler yer almaktadır.

4.6 Stuxnet - 2010

Stuxnet olayı, siber uzayda gerçekleştirilmiş en büyük gelişme ve siber güvenlik tarihinde dönüm noktası olarak kabul görmektedir. Stuxnet olayının neden siber

güvenlik tarihine yeni bir bakış açısı kazandırdığını anlayabilmek için öncelikle Stuxnet saldırısının nasıl gerçekleştiğini, etkilerinin neler olduğunu ve yaygın kötü amaçlı yazılımlardan farkının ne olduğunu anlamamız gerekmektedir.

Stuxnet solucanı, endüstriyel kontrol sistemlerinin (ICS) normal fonksiyonlarını, programlanabilir mantıksal denetleyicisinin (PLC) kök kullanıcı takımı (PLC rootkit) sayesinden etkileyen ilk solucan tipi olarak görülmektedir. Stuxnet solucanının ana hedefi programlanabilir mantıksal denetleyicilerin kodları üzerinden değişiklikler yaparak, endüstriyel kontrol sistemlerinin davranışlarını atak yapan kişinin isteği doğrultusunda değiştirmektedir.

Stuxnet'in siber güvenlik tarihine yeni bir bakış açısı kattığı daha önce dile getirilmiştir. VirusBlokAda tarafından Belarus'ta 2010 yılının temmuz ayında keşfedilen Windows solucanı üzerinde araştırmacıların yoğun çalışmaları olmuştur ve bu çalışmalar sonrasında araştırmacılar aslında Stuxnet'in bulunan Windows solucanından aylar önce yayıldığı yönündedir [74].

Fakat geçmişteki kötü amaçlı yazılımlar ile Stuxnet karşılaştırıldığında, aslında araların çok keskin farklılıklar olduğu görülmektedir.

Çizelge 4.1 : Stuxnet ile yaygın kötü amaçlı yazılım karşılaştırılması [74].

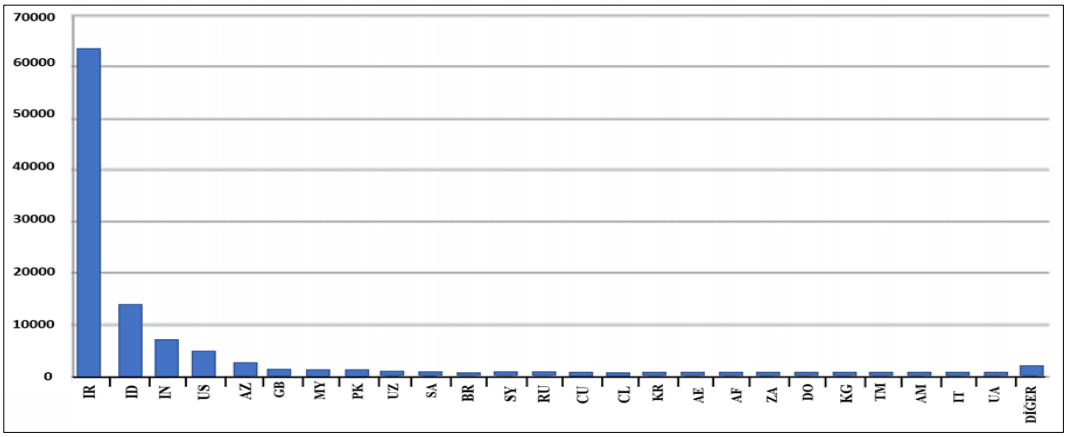
DEĞİŞKENLER	STUXNET	YAYGIN KÖTÜ AMAÇLI YAZILIM
HEDEF	Çok Seçici.	Rastgele
HEDEF ÇEŞİDİ	Endüstriyel Kontrol Sistemleri	Bilgisayarlar
BOYUTU	500Kbyte	1Mbyte'dan Daha Düşük
MUHTEMEL İLK BULAŞMA YÖNTEMİ	USB Bellek	İnternet veya Başka Ağlar
FAYDANILAN YÖNTEM	4 - Sıfırıncı Gün Açığı (4, alışılmadık daha fazla yatırımı temsil temektedir.)	Sıfırıncı Gün Açığı

Çizelge 4.1 de Stuxnet ile yaygın görülen kötü amaçlı yazılımlar arasındaki farklar belirtilmiştir. Çizelgeden de açıkça görüleceği üzere, kötü amaçlı yazılımların çoğu mümkün olduğunca çok bilgisayarı etkilemeye çalışırken, Stuxnet endüstriyel kontrol sistemlerini ve buna bağlı olarak spesifik koşullar altında bu kontrol sistemlerinin koşullarını değiştirmeyi hedeflemektedir.

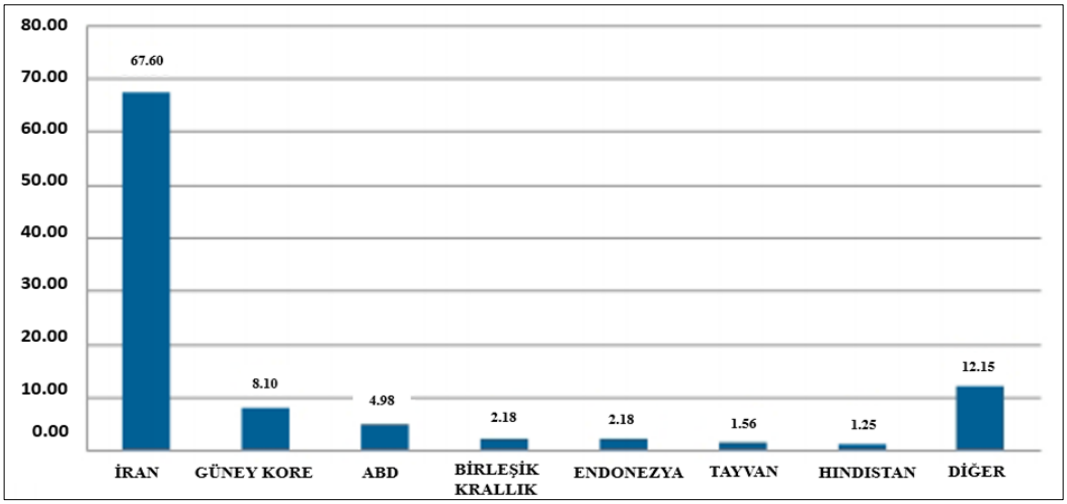
İkinci olarak kötü amaçlı yazılımların boyutları karşılaştırıldığında aslında Stuxnet'in ne kadar büyük, karışık ve üzerine çok düşünülmüş bir solucan olduğu da açıkça görülmektedir. Stuxnet' in kodu birden fazla dilde yazılmış ve yaklaşık 500Kbyte'dır Boyutun büyüklüğünün anlaşılması açısından bazı kötü amaçlı yazılım solucanların boyutları şu şekildedir. SQL Slammer 376 byte, Code Red 4 Kbyte, Nimda 60Kbyte.

Stuxnet'in kodunu inceleyen uzmanlar, kodun çok karmaşık ve çok başarılı olduğu konusunda hemfikirler fakat bu durum başka soruları da beraberinde getirmektedir. Uzmanlar bu kadar büyük ve başarılı bir kod yazmak için çok yüksek bir kaynağa ve desteğe ihtiyaç duyulacağını ayrıca hedef ile ilgili de detayların bilinmesi gerektiğini düşünmekte ve bu da Stuxnet'in arkadaşında bir hükümet veya hükümetler olabileceği, bu saldırının aslında İran'a karşı yapılan bir siber saldırı olarak değerlendirmektedir. Hatta birçok güçlü kaynak İsrail ve ABD'nin ortaklaşa bu solucanı ürettiğini düşünmektedir bunun nedeni tüm dünyada yayılmasına rağmen en çok İran'ı etkileyen Stuxnet solucanı, İran nükleer tesislerine sızarak, yaklaşık olarak 1000 santrifüjü çalışamaz duruma getirmiş, uranyum zenginleştirme programını yaklaşık 2 yıl sekteye uğratmıştır [75].

Şekil 4.1 ve Şekil 4.2'de sırası ile ülkelere göre stuxnet saldırısından etkilenen abone sayıları ve ülkelere göre siemens yazılımı yüklenmiş ve stuxnet saldırısından etkilenmiş abone değerleri gösterilmiştir. Şekillerden de İran'ın bu saldırıdan en çok etkilenen devlet olduğu açıkça görülmektedir.



Şekil 4.1 : Ülkelere göre stuxnet saldırısından etkilenen abone sayılar [76].



Şekil 4.2 : Ülkelere göre siemens yazılımı yüklenmiş ve stuxnet saldırısından etkilenmiş abone değeri (%) [76].

Siber saldırı korkusu, 2007 yılında Estonya'ya yapılan saldırı ile artmıştır. Estonya'nın maruz kaldığı siber saldırı türüne bakıldığında daha önce bölüm 3.4.1'de açıklanan DDoS atak türünün ve Stuxnet solucanı ile karşılaştırıldığında ise bir hayli basit bir teknik olarak kalmaktadır.

Stuxnet saldırısının siber güvenlik dünyasına yeni bir bakış açısı katmasının en önemli nedeni, internetten izole edilmiş bir ortamın tam olarak siber saldırılara güvenli bir ortam olmadığını kanıtlamasıdır. Yüksek motivasyona sahip atak yapan kişiler, saldırı yapacakları hedef ile ilgili araştırma, yüksek bilgi ve engin kaynaklar sayesinde beklenmedik kombinasyonlar ortaya koyabilmektedir.

4.7 Duqu- 2011

Duqu virüsü tam anlamı ile baştan son bir casusluk virüsü olarak tanımlanabilmektedir. Duqu virüsü bulaştığı endüstriyel kontrol sistemlerinin ne gibi açıklıkları olduğu, nerelerden bu sisteme saldırı yapılabileceği, önemli verilerin neler olduğu, sistem ve ağ bilgileri gibi birçok bilgiyi arar ve bulduktan sonrada bu bilgilerin ana merkeze raporlamasını yapmaktadır. Aynı zamanda da bu endüstriyel kontrol sistemlerinin benzerlerinin oluşturulması için de keşif amaçlı kullanılabilmektedir.

Bilgisayar ve endüstriyel kontrol sistemlerinde ki bahsedilen virüs ilk olarak 1 Eylül 2011 yılında keşfedilmiştir. Macaristan Budapeşte Üniversitesi Teknoloji ve Ekonomi Üniversitesinde bulunan sistem güvenliği ve kriptografi laboratuvarında yapılan incelemede bu kötü amaçlı yazılım için 60 sayfalık bir rapor hazırlanmış ve virüs,

Duqu olarak adlandırılmıştır. Bunun nedeni virüsün oluşturduğu klasörlerin başına "DQ" koymasıdır. Aynı raporda Duqu virüsünün İsrail ile bağlantısı olduğu da keşfedilmiştir. Yine aynı raporda Duqu virüsünün farklı farklı modülleri olduğu, her modülünde kendi özelinde işleri gerçekleştirdiği belirtilmiştir. Ayrıca Duqu virüsünün dünya genelince 400 milyon bilgisayara bulaştığı da belirtilmiştir [71].

4.8 Shady Rat (2006- 2011)

Dünya'nın ilk defa McAfee'nin 2011 yılında "Operation Shady RAT" adı ile yayınladığı rapor ile haberdar olduğu Shady RAT (Uzaktan Yönetim Aracı, Remote Administration Tool) saldırıları 2006 ile 2011 yılları arasında kesin olarak kaç firmayı etkilediği bilinmeyen bir casusluk eylemidir.

Shady RAT saldırısı ile ilgili olarak temel olarak 3 bölümden oluştuğunu söylenmektedir [77].

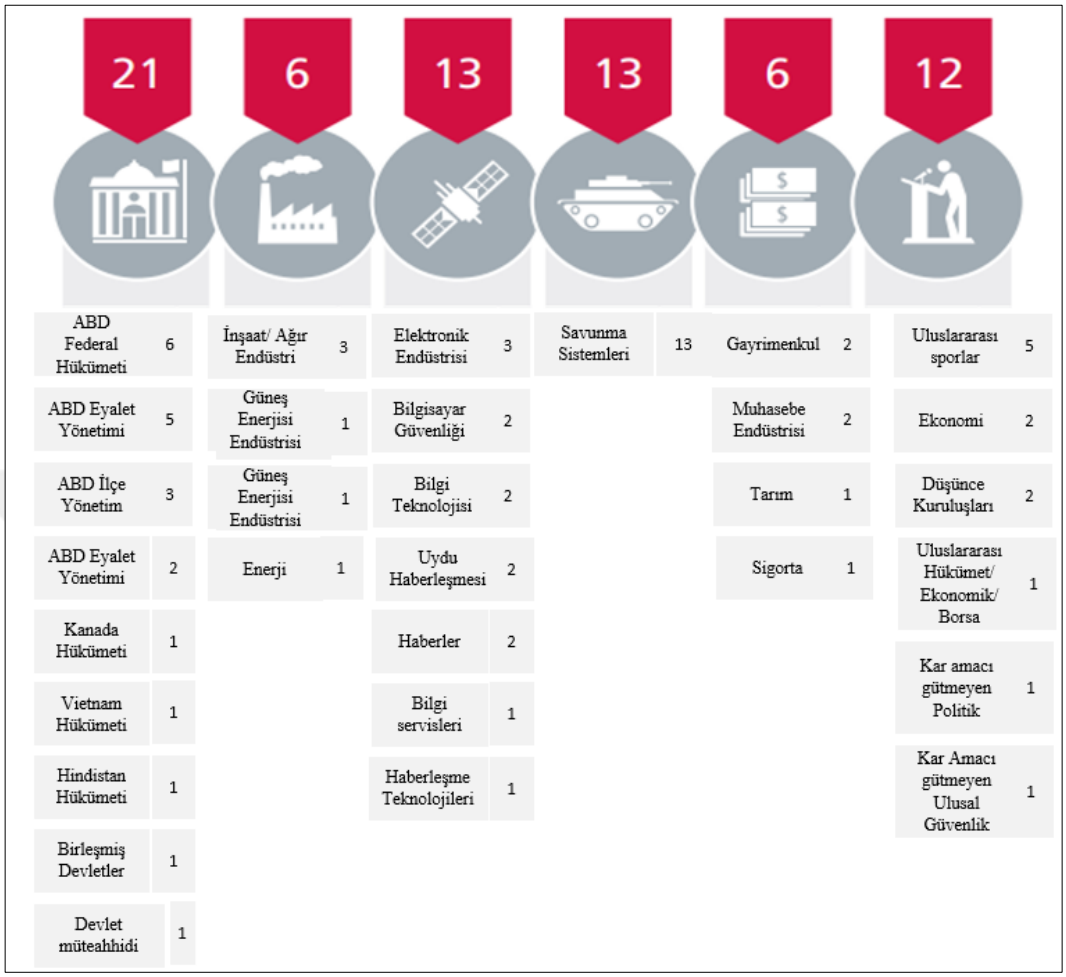
1.Bölüm: Hedef alınan kuruluş, hükümet, firma, vs. tespit edildikten sonra bu organizasyona yönelik olarak e-postalar hazırlanır ve gönderilir. Bu e-postalar Microsoft Word dosyası, Microsoft Excel dokümanı, sunumlar, pdf dosyaları olacak şekilde ekler ile beslenmiş olmak ile birlikte, e- postalar hedef alınan firma ile ilgili olacak şekilde isimlendirilmiştir. Örneğin, 2011 proje bütçesi, güncellenmiş iletişim listesi, katılımcı listesi gibi.

2.Bölüm: Bölüm 1'de gönderilen e-posta ve içerisindeki ek kısmında bulunan Excel dosyası açıldığından ve bilgisayara indirilmeye başlandığında içerinde bulunan Trojan adı verilen virüs de indirilmiş ve çalıştırılmış olmaktadır. Trojan bilgisayara indirildiği an itibariyle uzak yönetim ile iletişime geçmeye çalışmaktadır.

3.Bölüm: Trojen virüsü uzak bilgisayar ile ip adresi ve port bilgisi sayesinden iletişim kurar kurmaz, atak yapan kişi istediği komutları son kullanıcının bilgisi olmaksızın gizli bir şekilde çalıştırmasına olanak kılmaktadır.

McAfee'nin 2011 yılında yayınladığı rapora göre 2006-2011 yılları arasında 70'den fazla organizasyonun bu saldırıdan etkilendiği ve gizliliklerinin ihlal edildiği yönündedir. Şekil 4.3' de 35 özgün sektör için yapılan 71 atağın dağımı gösterilmektedir. İlk bakışta atakların ABD özelinde gerçekleştiği düşünülse de Şekil 4.4'de de görüleceği üzere, ataklar 14 coğrafik bölgeye dağılmıştır. Bu

organizasyonlar içerinde açıkça görülmektedir ki hükümetler, özel firmalar ve kar amacı gütmeyen kuruluşlar da Shady Rat atağının kurbanı olmuştur [78].



Şekil 4.3 : Shary RAT saldırısından etkilendiği tespit edilen organizasyonlar şeması [78].

Shady Rat Kurbanı Firmanın Ülkesi	Shady Rat Kurban Sayısı	Shady Rat Kurbanı Firmanın Ülkesi	Shady Rat Kurban Sayısı
ABD	49	Endonezya	1
Kanada	4	Vietnam	1
Güney Kore	2	Danimarka	1
Tayvan	3	Singapur	1
Japonya	2	Hong Kong	1
İsviçre	2	Almanya	1
Birleşik Krallık	2	Hindistan	1

Şekil 4.4 : Shary RAT saldırısının ülkelere göre dağılımı [78].

Sonuç olarak, özellikle uluslararası piyasalarda rol alan büyük firmalar göz önüne alındığında bu firmaların ekonomik başarıları ve varlıklarını sürdürebilmeleri açısından şirket sırlarının, rekabet planı ve stratejilerinin çok önemli olduğu düşünülürse, Shady RAT saldırısı için dünya piyasası üzerinde son derece etkili olduğu aşikardır. Bu nedenle etki çapı ve süresi bakımından değerlendirildiğinde Shady RAT, siber uzay içerisinde şu ana kadar yapılmış en geniş çaplı siber saldırı türüdür denilebilmektedir [79].

4.9 Sony Firmasına Karşı Yapılan Siber Saldırılar – 2014

Sony Pictures Entertainment firmasına karşı yapılan siber saldırı, bizlere siber saldırıların aslında ne kadar güçlü birer silah olduğunu, en azından devletler arasında hoşlanılmayan bir durum olduğunda, ardında neredeyse hiçbir iz bırakmadan çok hızlı, etkili ve dünya tarafında duyurulacak şekilde etki yaratacağının en güzel örneklerindendir.

Amerika merkezli dünyaca ünlü Sony Pictures Entertainment yapım stüdyosu tarafından yayınlanması planlanan ve Kuzey Kore lideri Kim Jong-un ile özel bir röportaj için Kuzey Kore'ye giden Amerikalı iki gazetecinin CIA tarafından Kim'e suikast düzenlemeye ikna edilmesini konu alan "The Interview" (Röportaj) filmi nedeni ile karşı karşıya kaldığı siber saldırı bunun en güzel örneklerindendir.

"The Interview" filmi nedeni ile GOP bilgisayar korsanları grubunun hedefi haline gelmiş olan Sony, ilk başta her ne kadar şirkete ve çalışanlarına gönderilen tehdit içerikli e-postaları dikkate almaz iken ardından işin ciddiyetini kavrayarak "The Interview" filminin galasını iptal etmiştir. Filmin iptal edilmesi sonrasında açılama yapan zamanın Amerika Birleşik Devletleri başkanı Barack Obama "Sony büyük bir hata yaptı", "Orantılı, yerinde, zamanında ve uygun bir yolla cevap vereceğiz" ve "Bir yerlerdeki diktatörün Amerika Birleşik Devletleri'ne sansür uygulamaya başladığı bir topluma değiliz. Birilerinin hicivli bir filmin yayınlanması noktasında insanları korkutmasına izin verilirse, hoşlanmadıkları bir belgesel veya haber gördüklerinde ne yapmaya başlayacaklarını hayal edin" şeklinde açıklamalarda bulunmuştur [80].

"The Interview" filmi nedeni ile Sony firmasına yapılan siber saldırı sonrasında Sony'nin aldığı karar büyük tartışmalara neden olmuştur. İfade özgürlüğü ile tam anlamıyla ters düşen bu siber saldırı sonrasında siber saldırıların artık sadece para

ve/veya bilgi hırsızlığı için değil, insan etiği ve düşünce özgürlüklerine dahi müdahil olabildiği görülmüştür.

Kuzey Kore tarafından yapıldığı öne sürülen siber saldırı Sony firmasının ilk kez karşı karşıya kaldığı bir durum değildir. 2011 yılında Sony'nin bir PS3'ün sistemini kıran bilgisayar korsanına dava açması sonucu ardı ardına Anonymous dâhil olmak üzere birçok hactivist grubun hedefi haline gelmiştir. Bu eylemler sonucunda Play Station ağındaki 11 milyon kayıtlı kullanıcının kişisel bilgileri ele geçirilmiş ve Sony'nin yaptığı açıklamaya göre saldırılar yıl sonundaki maliyeti 171 milyon doları bulmuştur [81].

4.10 Türkiye ve Rusya Arasında Yaşanan Siber Saldırılar – 2015

Özellikle arkasında devlet desteği olan siber saldırılar her ne kadar saldırıya kaynak olan devlet tarafından hiçbir zaman kabul edilmese de zamanlamaların manidar oluşu, iki devlet arasında yaşanan bir diplomatik olay sonrasına denk gelmesi ve yapılan saldırının destek almadan yalnızca küçük bir bilgisayar korsanı tarafından yapılamayacak kadar etkili ve büyük olması aslında ilk başta söylediğimiz gibi kaynak olan devlet tarafından kabul etmese de tahmin edilmesi çok da zor olmamaktadır. Bu olayın ilk örneklerinden bölüm 4.2'de anlatılan Amerika ile Çin arasında ki siber savaşlar verilebilmektedir.

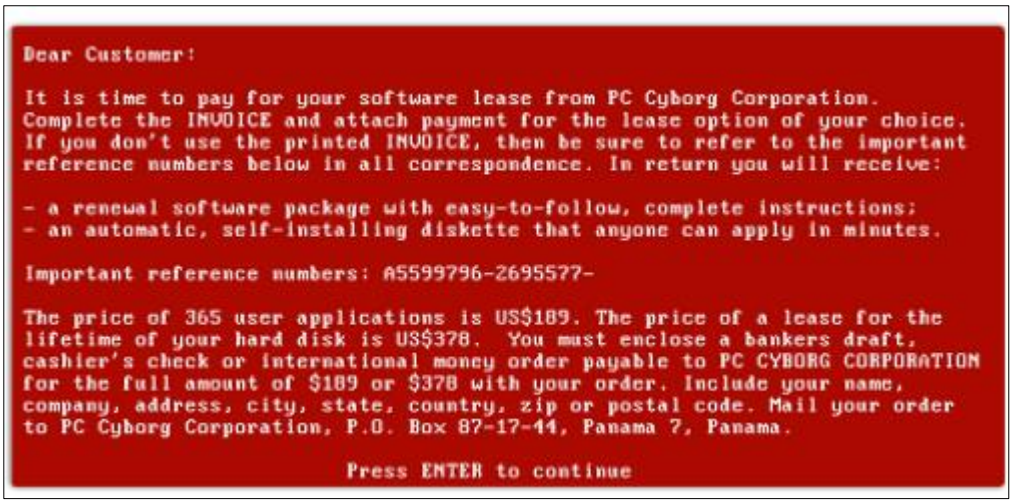
Amerika ile Çin arasında yaşanan olayın bir benzeri de Türkiye ile Rusya arasında yaşanmıştır. Türkiye, tarihinin en büyük siber saldırılarına 14 ve 24 Aralık 2015 tarihlerinde 6 ayrı "DNS Sunucusu" hedef alınarak maruz kalmıştır. DNS sunucularına yapılan DDoS saldırıları sonrasında sunucular isteklere cevap veremez hale gelmiş, "edu.tr", "gov.tr" ve "com.tr" gibi "tr" uzantılı 400 bin siteye 1 hafta boyunca ya hiç girilememiş ya da sitelere girişlerde sorunlar yaşanmıştır. Biraz önce belirttiğimiz gibi bu tarz saldırıların genellikle bir devlet tarafından üstlenilmek yerine kimlikler gizli tutularak, paravan korsan grupları tarafından üstlenilmektedir. Türkiye'ye karşı yapılan siber saldır da Anonymous korsan grubu tarafından üstlenilmiş fakat saldırının büyüklüğü ve etkisi göz önüne alındığında uzmanlar bu saldırının arkasında bir devlet desteği olduğu konusunda hemfikir olmuşlardır. Siber saldırıların 24 Kasım 2015 tarihinde Rusya ile yaşanan uçak krizi sonrası gerçekleşmiş olması sebebiyle saldırıların arkasında Rusya'nın olması ihtimalini doğurmaktadır [28].

4.11 Wanna Cry – 2017

Hayatımızın son döneminde yoğun bir şekilde ön plana çıkan dijitalleşme sayesinde dataları dijital ortamlarda depolama, depolanan verilere 7x24 erişebilme gibi, herhangi bir sorun anında verileri geri kurtarma ve internet üzerinden lokasyondan bağımsız olarak erişme gibi birçok özellik de hayatımıza girmiş durumdadır. Kısacası dijitalleşme, bilgisayar kullanıcıları için yaşam kalitesini bir şekilde arttırmıştır. Fakat her zaman söylenildiği gibi madalyonun iki yüzü vardır. Dijitalleşme her ne kadar hayatımıza kolaylıklar getirmiş olsa da bir yandan da yeni sorunlara da ortam sağlamıştır.

Bu bölümde anlatılacak olan 2017 yılından gerçekleşmiş olan WannaCry fidye virüsü son dönemde ortaya çıkan en büyük fidye yazılım olarak değerlendirilebilmektedir.

İlk fidye yazılım 1989 yılında geliştirilmiş ve PC Cyborg Trojan adı ile bilinmektedir. Fakat siber dünyasında bu yazılım AIDS Info Disk Trojan adı ile de anılmaktadır. AIDS Info Disk Trojan fidye yazılımı sisteme bir kez girdikten sonra tüm dosyaları ve dizinleri şifrelemeye ve kullanıcının C sürücüsünü kullanılamaz hale getirmekteydi. Dosyalardaki ve dizinlerdeki şifrelerin kaldırılarak bilgisayarın tekrardan kullanılabilir hale getirilmesi için fidyeci Şekil 4.5 de gösterildiği üzere 189 dolar fidyeyi Panama da bir adrese postalanmasını talep ediyordu [82].



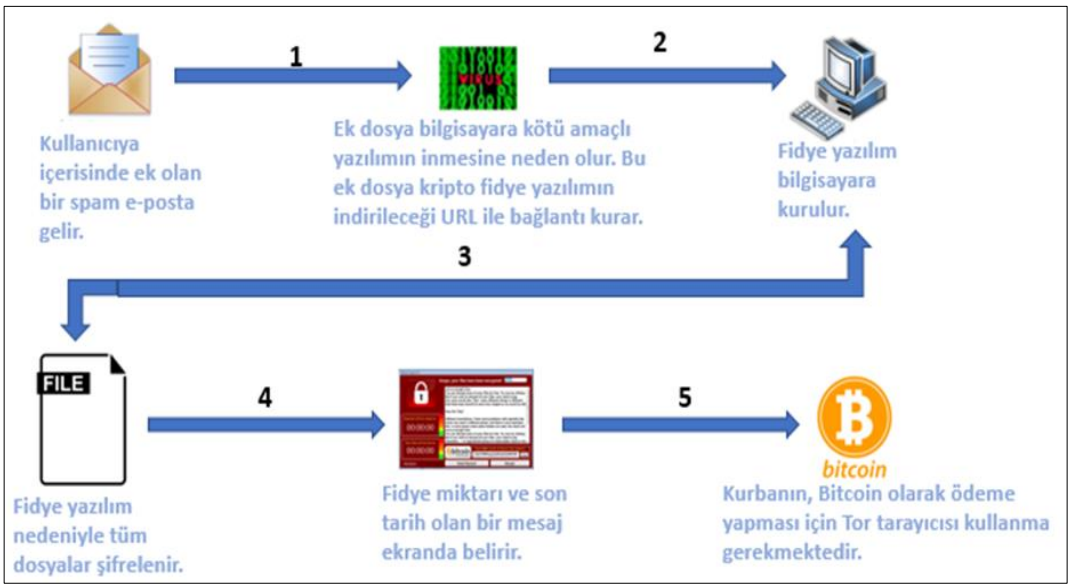
Şekil 4.5 : AIDS ınfo disk trojan tarafından gönderilen mesaj [82].

Fidye yazılımlar sadece ev kullanıcılarını değil, aynı zaman iş dünyasını da etkileyebilmektedir. Hatta bir şirket içerisine bulaşmış bir fidye yazılımın ne kadar

tehlikeli olabileceği, günümüzde şirketlerin veri, plan ve stratejiye verdikleri değerden tahmin edilebilmektedir.

Fidye yazılımlar hassas dataların kaybolmasına, şirketlerin adlarının kirlenmesine ve güvenin azalmasına, finansal olarak para kayıplarına ve düzenli yapılan basit işlerin dahi aksamasına neden olabilmektedir. Fakat bunun yanında şu da bilinmelidir ki şifrelenen bir bilgisayar veya dosyayı Kurtarmak için ödenen fidye, bu şifrelerin kaldırılacağının garantisi olmadığı gibi dosyaların şifrelerinin çözülmesi de fidye yazılımının sistemden kaldırıldığı anlamına gelmemektedir [83].

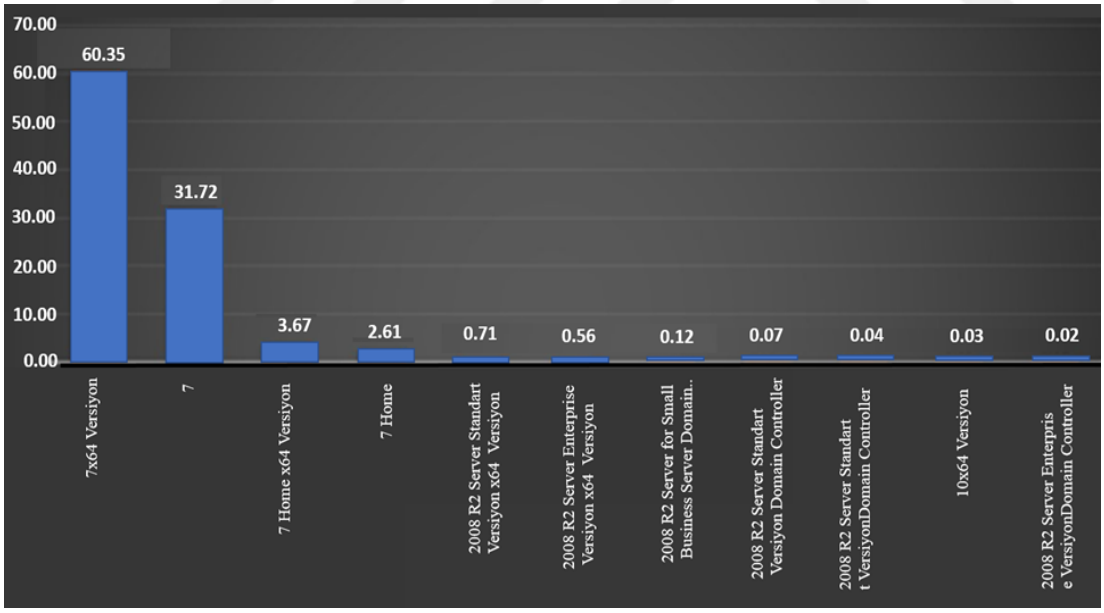
Fidye yazılımlar kilitleyen fidye yazılım ve şifreleyen fidye yazılım olmak üzere 2 kategori de değerlendirilmektedirler. Kilitleyen fidye yazılımında adından da anlaşılacağı üzere fidye yazılımı kullanıcının bilgisayarını tamamen kilitlemekte ve kullanıcı kaynaklarına sadece ve sadece ödemeyi yaptıktan sonra erişebilmektedir. Şifreleyen fidye yazılımda ise virüs kullanıcının sistemine herhangi bir kilitleme yapmamaktadır. Kullanıcının internet erişimi yapmasına ve kendi istekleri doğrultusunda araştırmalar yapmasına olanak sağlamaktadır ve bu virüs sadece kullanıcı bilgisayarındaki dosyaları şifrelemektedir. Şifreleyen fidye yazılımların kullanıcıların internet erişimi olması isteme sebeplerinin başından genellikle kripto para birimlerini desteklemeleri ve internet üzerinden kripto para transferi ile fidyeleri toplamalarıdır [84].



Şekil 4.6 : Genel fidye yazılım atak şeması (Yazar tarafından tasarlanmıştır).

Genel olarak fidye yazılımların çalışma mantıkları Şekil 4.6 de gösterilmiştir. Şekil 4.6, aslında tam olarak WannaCry fidye yazılımının da çalışma mantığı ile birebir örtüşmektedir. WannaCry virüsü Windows işletim sistemi kullanan bilgisayarlara bulaştığı gibi, Windows'un içerisinde bulunan açıklardan faydalanarak bilgisayarınızı kullanamaz hale getirmekte ve tamamen kontrolü kendi eline geçirmektedir. Dosyalara tekrar erişim sağlanabilmesi için mağdurdan Bitcoin olarak ödenmek üzere 300 dolarlık bir ücret talep etmekte ve ayrıca bu ücret hemen ödemez ise talep edilen fidye miktarı ikiye katlamakta ve mağdur kişiden 600 dolar istenmektedir.

Daha önce WannaCry virüsünün Windows işletim sistemi kullanan bilgisayara bulaştığını, bu işletim sistemindeki açıklar sayesinde bilgisayarları kullanılamaz hale getirdiği belirtmişti. Şekil 4.7, Windows versiyonlarına göre kullanıcıların yüzde kaçının bu virüsten etkilendiğini göstermektedir. Bu grafiğe göre özellikle Windows 7x64 Edition kullanıcıları olmak üzere, Windows 7 temelli işletim sistemleri WannaCry virüsünden en fazla etkilenen işletim sistemi olmuşlardır. Virüsten etkilenen total sayıya oranlandığından %98 oranında Windows 7 kullanıcılarının etkilendiği görülmektedir.



Şekil 4.7 : Windows versiyonlarına göre virüsten etkilenme yüzdeleri [85].

Yine aynı istatistik raporunda bu saldırıdan 400.000'den fazla makinenin etkilendiği, virüsün yayılması ile birlikte ilk gün etkilenen firma ve kuruluşlar arasında İngiltere'nin sağlık örgütü olan National Health Service (NHS), İspanya'nın en büyük telekomünikasyon firması olan Telefonica, FedEx bulunmaktadır [85].

Kullanılan Windows sürümünün güncel olmaması, spam e-postaların siber güvenlik bilincinden yoksun bir şekilde direkt olarak tıklanması, işletim sistemi sahibi olan Windows' un bu denli büyük bir açığının olması WannaCry virüsünün yayılmasında ve birdenbire dünyanın son dönemde ortaya çıkan en büyük fidye yazılımı olmasına olanak sağlamıştır.

4.12 Dünya Genelince Yaşanan Büyük Siber Saldırılar ve Virüs Yayılmaları Sonucu

İnternet hayatımıza girdiği ile andan itibaren kişisel olarak hayatımızı çok değiştirmenin yanı sıra, özellikle son dönemde savaş kavramını ve doğasını da değiştirmektedir. Genel olarak bakıldığında siber araçlar, stratejiler ve taktikler ülkelerin bilgi teknolojileri alanında kendilerini geliştirmeleri için çok yararlı olmaktadır. Fakat internet denildiği zaman ise, zayıf tarafın savaşta güçlü olan düşman tarafına atak yapabilme imkanı veren için müthiş bir araç olarak gözükmektedir.

Artık dünya genelinde de terörizmin, rakip firma analizlerinin, ülke stratejilerinin çalınması gibi birçok olayın siber saldırılar üzerinden yapıldığı ve/veya yapılabileceği göz önüne alındığında gerek ülkeler gerekse firmalar ve kuruluşlar olmak üzere siber saldırının tespiti, analizi, araştırması, prosedürü, siber olaylar aralarındaki ilişkinin ortaya çıkarılması gibi birçok konuda planlamalar yapması gerekmektedir.

Dünya genelinde yaşanan siber saldırıların anlatılması sonrasında aslında her birinin ayrı bir nedenden ortaya çıktığı, yer yer benzerlikler gösterdiği, yer yer bir sonraki saldırıya altyapı sağladığı görülmüştür. Bu nedenle yaşanan bu siber saldırılardan genel olarak şu çıkarımlar yapılabilmektedir.

- Kosova Siber Saldırısı ile birlikte olayın içinde dahi olmayan aktörlerin her an siber uzayda olaya müdahil olabildiği görülmüş ve Uluslararası Askeri İttifak (NATO)'nun dahi siber saldırılara maruz kalabildiği görülmüştür.
- Amerika ve Çin arasında yaşanan siber saldırılar incelendiğinde iki ülke arasında artan gerilimin nasıl bir siber savaşa dönüştüğü gözler önüne serilmiştir.
- Türkiye- Rusya arasında yaşanan siber saldırılar, Estonya'ya karşı yapılan siber saldırılar ve Gürcistan'a karşı yapılan siber saldırılar ülkeler arasındaki

politik durumların artık siber uzay boyutunda yansımaları olduğunu ve sonucunun siber savaş olduğunu çok net bir şekilde göstermiştir.

- Duqu virüsü bize bir endüstriyel kontrol sisteminin ağ ve sistem açıklarını, bu kontrol sistemine gerekirse yapılacak bir siber atak için açıklarını ve zayıflıklarını göstermenin yanı sıra benzerlerinin oluşturulması için de keşfin yapılabileceğini göstermiştir. Ayrıca bir kullanıcı hatası ve/veya ajanların çalışması sonrasında nasıl Stuxnet gibi Dünya'nın belki de en büyük virüslerinden birisine dönüşebildiğini de göstermiştir.
- İsrail Orchrad Operasyonu, askeri bir güç ile yapılan bir saldırıya, siber uzaydaki operasyonların nasıl entegre edilebileceğini çok açık bir şekilde göstermiştir. Bu alana Gürcistan'a karşı yapılan siber saldırılar da eklenebilmektedir.
- WannaCry virüsü bilinçsiz kullanıcıların gerek kendi ve firmaları gerekse ülkelerine ve hükümetlerine dahi zarar verdiğini göstermiştir.
- Sony firmasına karşı yapılan siber saldırı yine politik bir nedenden dolayı nasıl düşünce özgürlüğünün dahi kısıtlanabildiğini göstermiştir.
- Shady Rat virüsü yıllarca ülke ve firma stratejilerinin nasıl çalındığının en güzel örneklerindendir. Bu virüsün yayılmasında da temel sorun bilinçsiz kullanıcı olarak görülmektedir.
- Bu çıkarımların yanı sıra;
    - Siber savaşın, geleneksel savaşa göre daha ucuz olduğu,
    - Yaşanan olaylar karşısında askeri tepkilere göre daha hızlı tepki verildiği,
    - Saldırı yapan ülke ve/veya kişileri tespitinin zor olduğu için sorumluluk kabul edilmediği,
    - Her geçen yıl siber saldırı ve virüs tarzlarının değiştiği için tespitinin zorlaştığı,
    - Ülkelerin barış zamanında siber saldırı stratejilerini ve taktiklerini her an geliştirdikleri,

- Bilinçsiz kullanıcılar nedeni ile Stuxnet, Duqu, Shady Rat gibi virüslerin firma ve ülkelere ne kadar çabuk yayıldığı, bu nedenle siber bilincinin çok önemli olduğu,
- Bilgi ve veri hırsızlığına karşı siber uzayın da artık göz önünde bulundurulması gerektiği,

gibi çıkarımlar da yapılabilmektedir.

Kısaca toparlayacak olursak, internetin hayatımıza girmesi ile birlikte ülkeler arasında yaşanan tüm askeri ve politik çatışmaların siber uzayda da bir boyutu oluşmaktadır. Yaşanan krizin siber uzay ortamına taşındıktan sonra boyutu kestirilmesi pek mümkün olmayan sonuçlar doğurmaktadır. Ayrıca siber bilincinin olmaması nedeniyle de kötü amaçlı yazılımların ne denli kolay yayıldığı görülmektedir. Bu nedenle gerek hükümet gerek bireysel gerekse de firma özelinde siber bilinci arttırıcı yönde çalışmalar yapılmalıdır.

5. SİBER GÜVENLİK YÖNETİM MODELİ İNCELEMESİ

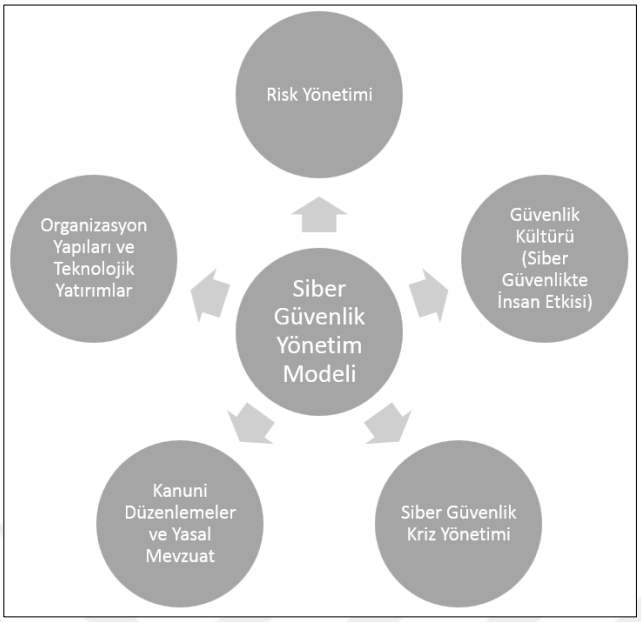
Günümüzde yaşamakta olduğumuz teknoloji temelli yaşamın en kritik yönü açıkça siber güvenliktir. Günlük hayatımızı ve hayatımızı idame ettirebilmek için var olan kurum ve kuruluşlar göz önüne alındığında devlet kurumları, e-devlet sistemi, bankalar, elektrik dağıtım kurumları, su tedarik sistemleri, nükleer santrallar, haberleşme sektörü, hastaneler ve bunlar gibi verilebilecek yüzlerce örnek hayatımızı daha da yaşanır kılmak ile beraber her geçen gün biraz daha teknolojik hale gelmektedir.

Yüksek seviyede teknolojinin hayatımıza ve şirketlerin hayatına girmesinin olumlu yanları olduğu kadar, siber risk dediğimiz riskinde bir o kadar artmasına neden olmaktadır. Her yıl gerek kamu gerekse özel sektörde hizmet veren organizasyonlar siber güvenliklerini arttıracak donanım ve yazılım cihazlarına binlerce hatta milyonlarca dolar para ödemektedirler. Fakat en iyi ürünü almak, en son çıkan yazılıma sahip olmak yine de siber güvenlik konusunda tam anlamı ile güvenli olmayı temin etmemektedir. Bunun nedeni bazı organizasyonlarda halen siber güvenlik konusunu yalnızca teknolojik yönden ele almasıdır. Şekil 5.1'den de görüleceği üzere, siber güvenlik yalnızca teknolojik olarak ele alınması gereken bir konu değildir.

Tezimde, herhangi bir organizasyonun siber güvenlik konusu ile başa çıkabilmek ve iyi bir politika ile organizasyonların en az hasar ile siber saldırıları atlatabilmesi için kritik altyapılarının güvenliğini sağlamak için kullanılabilecek siber güvenlik yönetimi modelinin teorik yönlerini sağlamaktır.

Tezimde sunulan siber güvenlik yönetim modeli, yönetim perspektifinden, geçmişte yaşanan siber saldırılardan, bilgisayar korsanlarının motivasyonlarından, bilgi güvenliği baş yöneticilerinin yorumlarından, organizasyon yapılarından ve değişikliklerinden, insan doğasından ve teknolojik yatırımlar gibi başlıklar çerçevesinde analiz edilmiştir. Buna göre de iyi bir siber güvenlik yönetim modelinde dikkat edilmesi ve dikkatle incelenmesi gereken 5 madde, risk yönetimi, siber güvenlikte insan etkisi, siber güvenlik ile ilgili teknolojik yatırımlar ve organizasyon yapıları, kriz yönetimi, kanuni düzenlemeler ve yasal mevzuat olarak belirlenmiştir.

Bu bölümde bu 5 maddenin her birisi siber güvenlik perspektifinden incelenmektedir.



Şekil 5.1 : Siber Güvenlik ile İlgili Yönetim Modeli Şeması (Yazar tarafından tasarlanmıştır).

5.1 Risk Yönetimi

5.1.1 Risk tanımı

Risk, herhangi bir olayın olma sıklığı ve olma ihtimalinin ölçülmesinin yanı sıra olayın sonuçlarının da öngörülmesi olarak tanımlanabilmektedir. Literatür de risk kavramının birden farklı tanımı bulunmaktadır. Bazı tanım örnekleri:

- "Zarara uğrama tehlikesi" [86].
- "Tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar yaratma potansiyeli" [87].
- "Nesne/amaç üzerindeki belirsizlik etkisi" [88].

Yukarıdaki tanımlardan da görüleceği üzere risk özelinde iki kavram ön plana çıkmaktadır. Bunlardan birisi tehdit, ikincisi de belirsizlik kavramıdır. Riskin tehlike anlamına geldiği durumlarda yalnızca olumsuz sonuçlar beklenirken, risk kavramının belirsizlik olarak kullanıldığı durumlarda hem olumlu hem de olumsuz sonuç beklemek doğru olacaktır. Bunun nedeni riskin çoğunlukla tam ve net olarak tahmin edilemez olmasından kaynaklanmaktadır.

Risk ile ilgili olarak belirsizlik ve tehdit anlamına gelebileceği belirtilmiş olsa da risk kavramı algıya bağlı bir kavram olarak görülmektedir. Yani bir şirket veya bir birey gözünden risk olarak değerlendirilebilecek bir durum başka bir şirket veya birey gözünden risk olarak değerlendirilemeyebilir. Bu da şirketin risk yönetim politikası kapsamında değerlendirilmelidir.

Riskin, oluşma olasılığı ve etkinin kapsamı ile orantılı olması gerektiğini belirten ünlü Fransız matematikçi Blaise Pascal'ın tanımı da göz önüne alındığında

$$R = P*C$$

Formülü elde edilmektedir. Matematiksel olarak formülde R ile ifade edilen risk değeri, olayın olma sıklığı (P) ile olayın sonuçlarını yani etkisi (C) ile çarpımı ile hesaplanmaktadır [89].

Formülde P ile gösterilen olayın olma sıklığı aynı zamanda olayın olma olasılığı olarak da değerlendirilebilmektedir. Blaise Pascal'ın formülüne ek olarak risk yönetim süreçlerinin olmazsa olmazı olan risk matrisi de bize bir olayın olma olasılığının arttığında ve eğer bu olayın etkisi büyük ise çok büyük risk içerdiğini fakat düşük olasılık ve düşük etkinin düşük risk ortaya çıkardığını göstermektedir. Şekil 5.2'de örnek bir risk matrisi görülmektedir.

Siber Olayın Yaşanma İhtimali	Yaşanan Siber Olayın Şiddeti/Etkisi				
	1 Çok Hafif	2 Hafif	3 Orta Derece	4 Yüksek	5 Çok Yüksek
1 Çok Düşük	1 Anlamsız	2 Düşük	3 Düşük	4 Düşük	5 Düşük
2 Düşük	2 Düşük	4 Düşük	6 Düşük	8 Orta	10 Orta
3 Orta Derece	3 Düşük	6 Düşük	9 Orta	12 Orta	15 Yüksek
4 Yüksek	4 Düşük	8 Orta	12 Orta	16 Yüksek	20 Yüksek
5 Çok Yüksek	5 Düşük	10 Orta	15 Yüksek	20 Yüksek	25 Tolere Edilemez

Şekil 5.2 : Örnek bir risk matrisi (Yazar tarafından tasarlanmıştır).

Riskin var olması demek aynı zamanda bunun sonucu olacağı anlamına da gelmemektedir. Her riskin bir nedeni olduğu gibi sonucu olması içinde riskin gerçekleşmesi gerekmektedir. Yani var olan bir riske karşı alınacak tedbirler sayesinde riskin gerçekleşmesi engellenebilmekte ve olumsuz sonuçların ortaya çıkmasının da

önüne geçilebilmektedir. Buradan da riskin yönetilebilen bir oldu olduğu risk yönetim kavramının ne kadar önemli olduğu sonucu çıkarılabilmektedir.

5.1.2 Belirsizlik

Belirsizlik ile risk kavramlarının birbiri ile iç içe oldukları çok aşikardır. Risk daha önce yapılan tanımı da göz önüne alarak kısaca sistemleri ve projeleri etkileyecek planlanmayan olaylar olarak belirtilebilmektedir. Belirsizlik kavramı ise kesinliğin eksikliği ile ortaya çıkmış olan bir olgudur.

Belirsizlik durumunda olay ile ilgili olarak başından sona bir bilinmezlik durumu hakimdir. Bu nedenle belirsizlik kavramı ölçülebilir veya tahmin edilebilir bir kavram değildir. Bunun nedeni olay ile ilgili hiçbir bilgiye sahip olunmamasıdır. Belirsizlik ve risk kavramlarını iyi bir şekilde anlamak risk yönetimi konundan çok önemli bir kavramdır. Bunun nedeni şirketler veya kurumlar için sistem operasyonları özelinde alınan kararlarda belirsizlik ve risk farklı sonuçlara neden olabilmektedir [90].

Kısacası risk, bilinen bilinmeyen ve belirsizlik ise bilinmeyen bilinmeyen olarak kısa ve öz bir şekilde özetlenebilmektedir.

Nistor Costel riskin belirsizlikten türediğini belirtmiş ve şu benzetmeyi yapmıştır. Eğer risk, tehdit ile ilişkili ise, belirsizlik bu durumda öngörülemez olumlu durumlardan üreyen negatif veya pozitif bir bileşen olabilir. Bu durumda da negatif bileşenler risk ile ilişkili durumdadır [90].

Şekil 5.3'te risk ile belirsizlik arasındaki ilişki tasvir edilmiştir.

Şekil 5.3 : Belirsizlik ile risk arasındaki ilişki [91].

Risk ve belirsizlik farklılıkları;

- Risk olgusunda gelecekteki olayın sonuçlarını tahmin etmek olanaklı iken, belirsizlik durumunda gelecekte ortaya çıkacak olayların sonuçlarını tahmin etmek imkansızdır. Mutlak bilinmezlik hakimdir.
- Risk ölçülebilir, sınıflandırılabilir ve değerlendirilebilir bir olgudur. Fakat belirsizlik ölçülemez ve değerlendirilemez
- Risk kontrol edilebilir fakat belirsizlik kontrol edilemez bir olgudur.
- Risk yönetimi sürecinde her bir risk değeri için bir olasılık çalışması yapılabilir ve sonunda bir olasılık değeri çıkarılabilir. Fakat belirsizlik durumunda herhangi bir olasılıktan söz bahsetmek söz konusu değildir.

5.1.3 Tehdit

Risk kavramının var olmasındaki en önemli 3 etkenden biri olan tehdit kavramının literatür de birden farklı tanımı bulunmaktadır. Bazı tanım örnekleri:

- "Bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedeni" [87].
- "Güvenliği ihlal edebilme veya zarara neden olabilme potansiyeline sahip bir durum veya olay" [92].

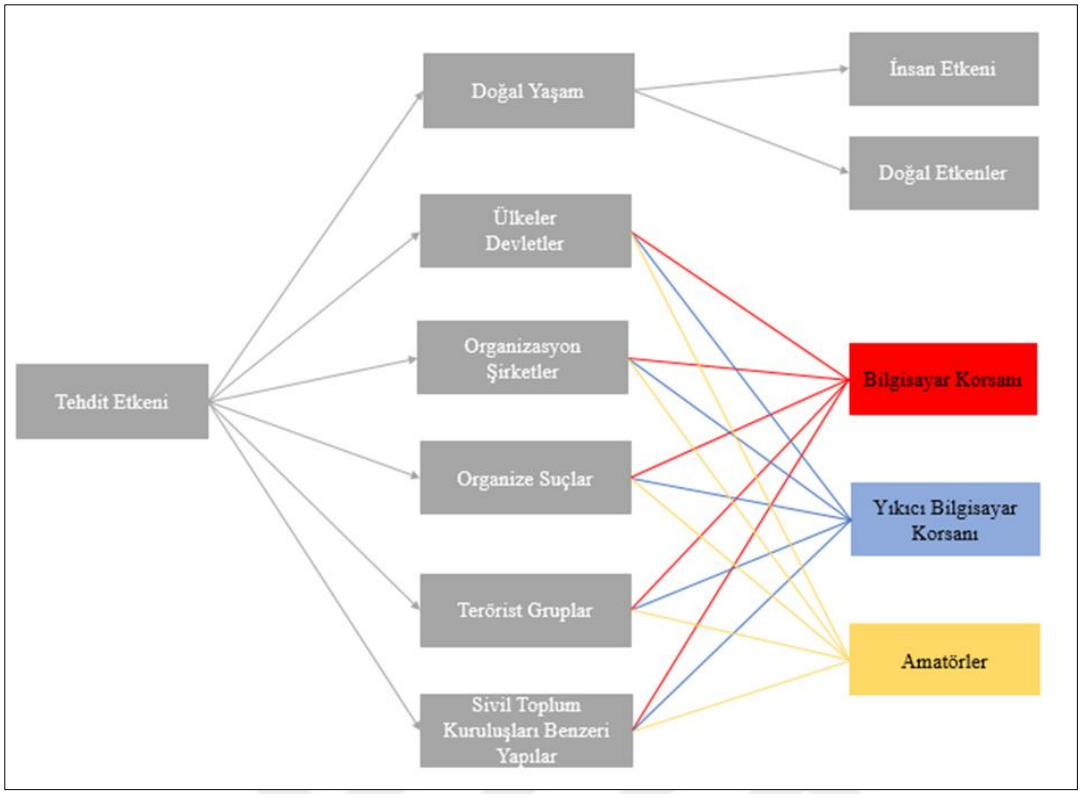
Riskin ortaya çıkmasındaki en önemli 3 faktörden biri olmasının nedeni, tehdit kavramının olmadığı bir yerde açıklık olsa dahi hiçbir sorun ortaya çıkmamasıdır. Bunun nedeni değer üzerindeki bir açıklık ancak tehdit ile buluşunca ortaya risk çıkmaktadır. Kısaca

$$\text{Risk} = \text{Değer} \times \text{Zayıflık} \times \text{Tehdit}$$

olarak değerlendirilebilmektedir.

Peki tehdit nasıl ortaya çıkmaktadır? Özellikle endüstri 4.0 ile birlikte gelişen ve ortaya çıkan siber uzay kavramında, tehditlerinde ortaya çıkması yalnızca bir bilgisayar korsanı tarafından olabilecek olsa da bir grup bilgisayar korsanı topluluğu ile de olabilmektedir.

Şekil 5.4'de gösterilen tehdit etkeni kategorilerine biraz daha detaylı bakacak olursak;



Şekil 5.4 : Tehdit etkeni kategorileri [93].

- Ülkeler / Devletler

Birçok hükümet artık günümüzde bilginin ne kadar değerli olduğunu ve bilgiyi korumanın günümüzde neredeyse birinci öncelik olduğunu düşünmektedir. Daha önce bölüm 4'de anlatılan dünya siber tarihine yön veren önemli siber savaşlar ve zararlı yazılımlar göz önüne alındığında ülkeler arasında artık politik ve reel savaşların birer kopyalarının siber uzayda gerçekleştiği de açıkça görülmektedir.

Bahsedilen değerler, içerisinde ekonomik verilerden ülke stratejilerine, ülke bireylerinin sağlık ve kimlik verilerinden askeri sırlara kadar bilgileri içermektedir. Yapılan bir saldırı karşısında da karşıt devlet, saldırı yaptığı devlete ait özellikle diplomatik, askeri ve ekonomik sırlar aramaktadır.

İşte bu bahsedilen saldırıların hepsi uzaktan, devletin kendisini ifşa etmesine gerek kalmaksızın daha az bir risk ile bilgi sistemlerindeki açıkların zayıflıklarından yararlanılarak yapılmaktadır.

- Terörizm ve terörist gruplar

Terörist gruplar daha çok bilgi sistemleri altyapılarına yönelik, ülke içerinde huzursuzluk ve karmaşa çıkarmak ile ilgilenmektedir. Bu kritik altyapıların başında

acil servisler, su ve elektrik altyapıları, finans servisleri gelmektedir. Şekil 2.2' de terörizmin ulusal siber suçlardaki yeri açıkça görülmektedir.

Terörist eylemcilerin motivasyonlarının daha çok politik olduğu görülmektedir. Yapılan siber saldırılar sonrasında terörist eylemciler çok kısa bir sürede etkinin, Dünya üzerinde yarattığı yankının büyüklüğünü ve siber saldırıların gücünü keşfetmişlerdir.

- Şirketler ve kurumlar

Özel firmalar rakipleri ile ilgili aktif olarak bilgi ve istihbarat araştırması yaparken, rakipleri ile ilgili önemli bilgilere erişme konunda İngilizcesi "offensive IW" olarak belirtilen bilgi savaşları kurallarına bağlı kalmak üzerinde anlaşmışlardır [93].

Şirketin cirosu, pazardaki yeri ve rekabet ortamındaki duruşu bilgi savaşları taktiklerinin kullanılması için birer kurumsal motivasyon olarak gösterilebilmektedir.

- Organize suçlar ve suçlular

Organize suçlar ve suçlulardan bahsedildiğinde neden tehdit etkeni oldukları ile ilgili ilk akla gelen konu kendi çıkarları doğrultusunda bilgi elde etmeye çalışmalarıdır. Bu suçlular bireysel ve organize bir şekilde banka hesapları, kredi kartı bilgileri ve para getirebilecek diğer sanal durumlar ile ilgilenmektedirler. Pennsylvania bölgesindeki çekilişin kazananlarının açıklanması sonrasında 15,2 milyon dolar değerindeki tahsil edilmeyen biletin bir kopyasının online ortamda bastırılarak kazanan kişi olduğunu iddia eden bir dolandırıcı bu konuya verilecek güzel örneklerdendir [93].

Bunun yanı sıra internet üzerinden alışveriş yapılabilen sitelerin veri tabanı erişimleri konusunda gözden kaçırdıkları açıklar nedeniyle bilgisayar korsanları tarafından yıllar içerinden binlerce hatta dünya genelinde milyonlarca kredi kartı bilgisinin çalınmasına neden olmaktadır. Bu nedenle siber uzayda bulunan bu tarz suç örgütleri ve bireyler de çok büyük tehdit yaratmaktadır.

Şekil 5.4'ü biraz daha dikkatli inceleyecek olursak, doğal yaşam içerisinde insanlardan ve doğal yaşam nedeniyle de tehditler ortaya çıktığını görülmektedir. Yangın, sel, şimşek, deprem gibi doğal afetler de kurumların hayatta kalmaları konusunda rol oynamaktadır.

Fakat bizim için daha önemli olan kısma gelecek olursak, ülkeler, kurumlar, organize suç ekipleri, bireysel suçlular, terörist eylem grupları ve sivil toplum örgütü benzeri

yapılar bilgisayar korsanlarını, amatörler ve/veya yıkıcı bilgisayar korsanlarını hedeflerine ulaşma doğrultusunda bünyelerinde istihdam edebilmektedirler.

Bilgisayar korsanları, amatörler ve/veya yıkıcı bilgisayar korsanlarını bahsi geçen grupların birer parçası olabilmektedirler.

En önemlisi bu birlikteliğin iki yönlü olarak değerlendirilebilmesidir. Her kombinasyonun farklı bir özelliği ve farklı bir hedefi bulunmaktadır. Ayrıca herhangi bir grupta birden fazla kombinasyon da bulunabilir.

5.1.4 Bilgi sistemleri riski / siber risk nedir?

Risk, tehdit ve belirsizlik kavramlarının evrensel tanımlarının bölüm 5.1.1, bölüm 5.1.2, bölüm 5,1.3'de anlatılmasına istinaden tezin konusu olan siber güvenlik ile ilgili risk kavramına geçilebilir. Siber risk kavramı daha genel bir çerçevede bilgi sistemleri riski altında da değerlendirilebilmektedir.

Bilgi sistemleri riski, iş süreçlerini olumsuz yönde etkileyecek şekilde otomasyon sisteminin, ağ veya diğer kritik BT kaynaklarının kaybedilmesi potansiyelidir.

Bilgi teknolojileri risk tanımı ile aynı çizgide siber risk, bir kurumun bilgi teknolojisi altyapısında meydana gelebilecek beklenmedik bir teknik arıza ya da bu altyapı sistemlerine yönelik olarak gerçekleştirilen siber saldırılar sonucu kaynaklanabilecek muhtemel finansal kayıp ve marka değerine yönelik oluşabilecek zararları ifade eden risk durumudur [94].

Daha önce bölüm 4.6'da anlatılan İran'ın uranyum tesislerine yönelik yapılan Stuxnet saldırısı ele alındığında aslında tam olarak bu tanım ile oturmaktadır. Stuxnet virüsü daha önce de bahsedildiği gibi Siemens marka SCADA sistemlerine sızmış ve santrifüj dönüş hızlarını değiştirerek İran hükümetine büyük maddi zararlar verdiği görülmüştür. Tanımda bahsi geçen otonom sistem bir scada sistemi olabileceği gibi, bir uçak, bir veri tabanı veya basit bir bilgisayar dahi olabilir.

Organizasyonların riskleri başarılı bir şekilde belirlenmesi, belirlenen risklerin analiz edilmesi, risklere karşı hazırlıkların yapılması için dokümanlar oluşturmalıdır. Risk yönetim farkındalığı yaratmak ve tüm kurum geneline uygun bir risk protokolü oluşturabilmek ve paylaşabilmek için risk yönetim komitesi kurulması tercih edilen yöntemlerdendir.

Geçen her gün organizasyonlar biraz daha bilgi teknolojileri altyapılarına biraz daha bağımlı hale gelmektedirler. Şirketlerin, gelişmeleri ve varlıklarını sürdürebilmeleri için endüstri 4.0 ile birlikte bu durumun gerçekleşmesi artık bir zorunluluk haline gelmiştir. Bu nedenle firmalar bilgi teknolojileri risklerini özellikle de siber riskleri iş riskleri yönetim stratejileri içerisinde ele almalıdırlar.

Siber riskler genel olarak olası bir siber saldırı sonrasında şirketin ve/veya organizasyonun verilerinin zarar görmesi, çalınması, yok edilmesi, değiştirilmesi ve üzerinde oynanması sonrasında şirketin yaşayabileceği maddi kayıpları, şirketin itibar kaybını kısacası siber saldırı sonrasındaki olumsuz etkileri kapsamaktadır.

Bir siber saldırı sonrasında gizlice yerleştirilen bir virüsten, veri hırsızlığından veya veri ihlalinden kaynaklanan ve birinci parti risk kapsamında değerlendirilen risk başlıkları şunlardır;

- Veri kaybı
- Yazılımsal hatalar
- Verilerin şifrelenerek, şifrenin çözülmesi karşılığında fidye istenmesi
- Ağ kesintisi sonucu doğacak zararlar
- Kurum verilerinin silinmesi ve manipüle edilmesi
- İş Durması ve/veya yavaşlaması
- Çalınan verilerin ifşa edilmesi riski
- İtibar kaybı

5.1.5 Bilgi teknolojileri risk yönetimi tanımı

Günümüzde gerek bireysel ve kurumsal gerekse devlet katında her türlü gelişme bizi internet yani bilgi teknolojileri sistemlerine daha bağımlı hale getirmektedir. Örnek olarak devletlerin sistemlerini internete taşıdığı, internet üzerinden birçok işin çok kolay bir şekilde yapıldığı e-devlet modelleri, bireysel olarak internet üzerinden yapılan e-ticaret sistemleri, kurumsal firma gözünden bakacak olursak, kurumsal firmaların neredeyse tüm sistemlerinin internete erişimi olduğu ve verilerinin büyük veri tabanlarında tuttukları da göz önüne alındığında bu gelişmelerin daha da artacağı aşikardır.

Bu gelişmelerin sonucu olarak bilgi teknoloji sistemler üzerindeki riskler daha fazla fark edilmekte ve önemli olarak görülmektedir. Sistemler üzerindeki açıklar ve insan dikkatsizliği nedeniyle bugüne kadar Dünya üzerinde birçok virüs yayılmış, hatta ülkeler siber savaş nedeniyle tüm sistemlerini kaybetmiş ve ülkelerini internet dünyasından izole etmek zorunda kalmıştır.

Kısaca, bilgi sistemleri üzerindeki güvenlik açıkları ya da hatalar ciddi iş krizlerine ve itibar kayıplarına yol açabilmektedir. Bu sebeple pek çok düzenleyici kuruluş yeni uyum zorunlulukları getirmektedir.

Bilgi teknolojileri risk yönetimi, temel olarak faaliyetlerdeki risklerin belirlenmesi, çözümlenmesi ve tepki verilmesi süreçlerini kapsamaktadır. Asıl amacı sistemdeki olumlu sonuçların arttırılması ve sonucu olumsuz olabilecek olayların sonuçlarının en aza indirilmesini içermektedir. Bilgi teknolojilerinin değerlerinin belirlenmesi için iş süreçleri yöneticileri, denetçiler ve hukuk birimlerinin yakın bir çalışma yapması gerekmektedir.

Tüm Dünya üzerinden yönetim kurullarının bilgi teknolojileri ile ilgili olarak en çok merak ettiği konulardan bir tanesi de riskin nasıl azaltılacağıdır. Bu konuda öncelikle şu anlaşılmalıdır ki risk hiçbir zaman sıfırlanamaz. Önemli olan riski sıfıra indirmek değil, riskin farkında olup riski yönetmek ve olumsuz durumlardan kaçınabilmek için fırsatlar yaratmaktır. Burada da en önemli etkenlerden bir tanesi riskleri kurumdaki tüm risklerin bir parçası olarak belirlenmeli, ölçülmeli ve yönetilmelidir. Uygulanan bu yaklaşıma bilgi teknolojileri risk yönetimi adı verilmektedir.

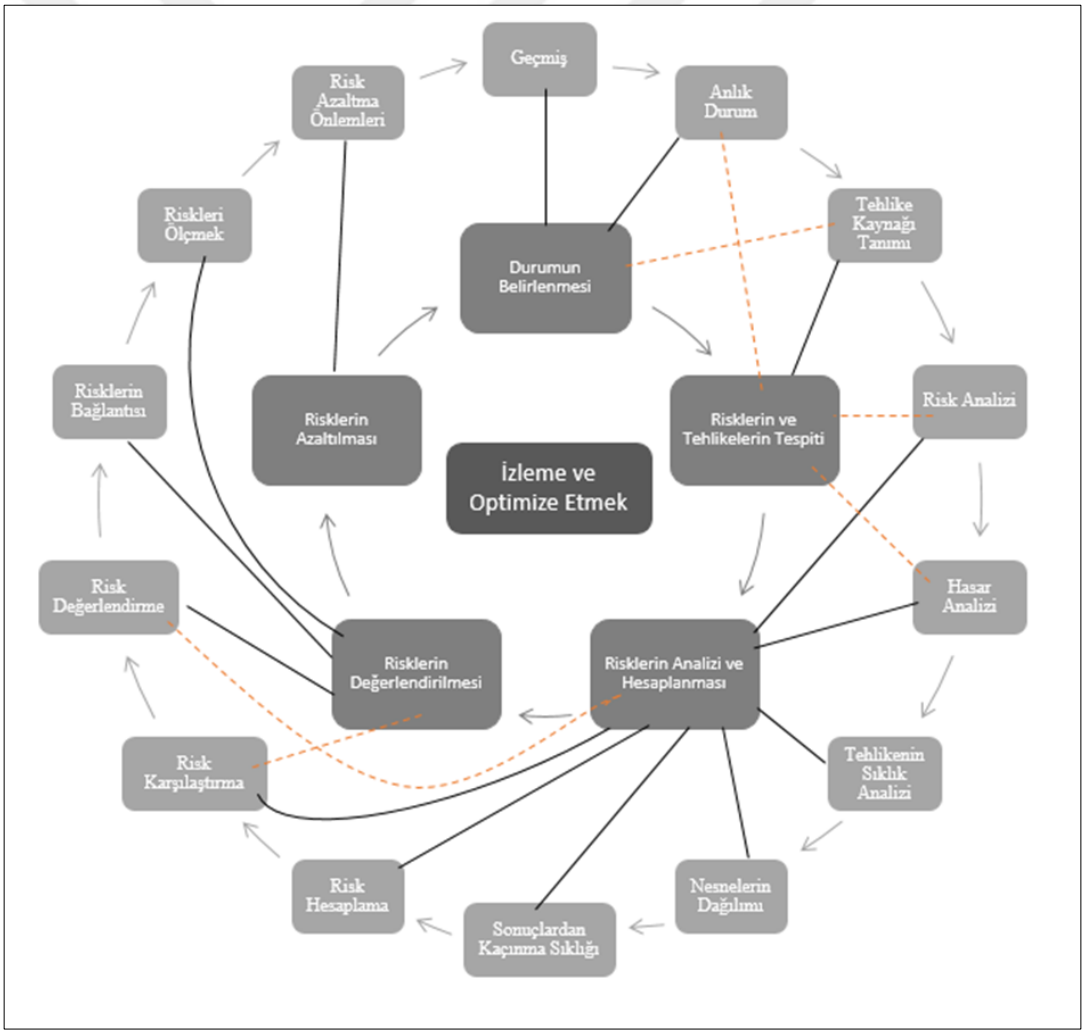
Peki bilgi teknolojileri konusunda riskin yönetilmesi neden önemlidir? Bunun nedeni aslında sorunun içinde mevcuttur. Bilgi her kuruluş için kritiktir ve bilgi teknolojileri sadece kendi kendisini ilgilendiren bir sistem değil, tüm bilginin işlenip, iletilip saklandığı bir sistemdir. Bu nedenle bilgi teknolojileri sadece bilgi teknolojileri birimi ve çalışanları ile ilgili değil, tüm kurum çapında ele alınması gereken bir sorumluluktur.

Örnek vermek gerekirse, bilgi teknoloji sistemlerinin güvenliklerinin üst seviyede olduğu bir kurumda çalışan bir bireyin, dışarıda bulduğu ve/veya hediye edilen bir harici belleği şirket ağındaki bir bilgisayarına takması veya şüpheli gelen bir e-postayı açması durumu kurumu büyük bir risk altında bırakabilmekte ve büyük maddi kayıplara neden olabilmektedir.

Son dönemde sayıları giderek artsa da çok az sayıda organizasyon bilgi sistemleri yönetim risk modeli oluşturmaktadır. Bunun nedeni daha önce de bahsettiğimiz gibi firmaların var olmak için teknoloji ye, internete kısacası bilgi sistemlerine bağımlılığının artması ve bununla birlikte de gelen güvenlik açıklarının farkına varmalarıdır.

Risk yönetiminin yapılabilmesi için bilgi teknolojileri adına risklerin değerlendirilmesi, yönetilmesi, analiz edilmesi gibi birçok adımı içinde barındıran bir risk yönetim çerçevesi oluşturulmalı ve bu çerçeveye bağlı kalınarak sürdürülmelidir. Risk yönetim çerçevesinde kurumun hedefleri üzerinde herhangi bir potansiyel etkinin oluşturacağı beklenmedik olaylar önceden belirlenir, analiz edilir ve değerlendirilir.

Şekil 5.5'te detaylı bir risk yönetim ve risk değerlendirme süreci gösterilmektedir.



Şekil 5.5 : Risk yönetim ve risk değerlendirme süreci [89]**.**

Genel olarak bir organizasyonun risk yönetim çerçevesine sahip olmasının faydalarına gelecek olursak, bu faydalar COSO (Committee of Sponsoring Organizations of the Treadway Commission) tarafından 2004 yılında yayınladığı kurumsal risk yönetimi-bütünleşik çerçeve raporunda çok net bir şekilde ifade edilmiştir.

Kısaca COSO'dan da bahsedecek olursak, Treadway Komisyonu olarak bilinen COSO, Amerika'da faaliyet gösteren 5 meslek kuruluşu (Amerika Muhasebe Derneği, Amerika Mali Müşavirler Enstitüsü, Uluslararası Finansal Yöneticiler Birliği, Yönetim Muhasebecileri Enstitüsü, İç Denetçiler Enstitüsü) tarafından işletme ve diğer kurumlar tarafından düzenlenen sahte mali raporların nedenini ortaya çıkarmak, bunları tespit etmek veyahut meydana gelme olasılığını azaltmak için 1985 yılında kurulmuştur [95].

COSO en son güncellemesini 2013 yılının Mayıs ayında yapmıştır. COSO iç kontrol yapısı birbirinden bağımsız olmayan zincir halkaları örneği gibi iç içe geçmiş beş bileşenden oluşmaktadır. Bunlar [95];

- Kontrol ortamı (Control Environment),
- Risk değerleme (Risk Assessment),
- Kontrol faaliyetleri (Control Activities),
- Bilgi ve iletişim (Information and Communication),
- İzleme/gözlem (Monitoring)

COSO [96]'ya göre etkin bir etkin bir kurumsal risk yönetimi,

- Risk yönetimi ve stratejisini hizalamasını,
- Riske karşı vereceği tepki kararlarını geliştirmesini,
- Operasyonel sürprizleri, maddi ve işgücü kayıplarının azaltmasını,
- Birden fazla ve çapraz kurumsal riskleri tanımlamasını ve yönetmesini,
- Fırsatları yakalamasını,
- Sermayenin, karın ve şirket bütçesinin dağıtımının iyileştirilmesini sağlamaktadır.

Bu adımlar birer birer kısaca incelenecek olursa;

i. **Risk yönetimi ve stratejisini hizalaması:** Yönetim ilk olarak farklı stratejik alternatifleri değerlendirir ve daha sonra seçilen stratejiyle uyumlu hedefleri belirler, operasyonlar ve amaçlar için bir temel oluşturur, ve ilgili riskleri yönetmek için mekanizmalar geliştirir.

ii. **Riske karşı vereceği tepki kararlarını geliştirmesi:** Risk yönetim çerçevesininin beşinci adımında da değerlendirileceği üzere, risk analizi ve değerlendirmeleri sonrasında elde edilen riskler karşısında organizasyonun nasıl bir duruş sergileyeceği, riskin göz ardı edip edilemeyeceği, riskin ortadan kaldırılması için maliyet ve risk analizlerinin göz önüne alınmasını sağlar.

iii. **Operasyonel sürprizleri, maddi ve işgücü kayıplarının azaltması:** Risk yönetimi birimleri sayesinde potansiyel olayları tanılanır, riskler değerlendirli ve tepkiler oluşturulur. Böylece istenmeyen sürprizler ve ilişkili maliyetler ve kayıpları azaltmak için organizasyon yeteneği kazanılır.

iv. **Birden fazla ve çapraz kurumsal riskleri tanımlamasını ve yönetmesi:** Organizasyon farklı bölümlerini etkileyen çok sayıda riskle karşı karşıya kalan kalabilir. Bu durumda risk yönetimi yalnızca tekil riskleri yönetmekle kalmaz, aynı zamanda birbiriyle ilişkili etkileri de anlamalıdır. Risk yönetimi birbiril ile ilişkili olan etkilere ve çoklu risklerin tümleşik tepkilerine en etkin tepkiyi vermeye olanak sağlar.

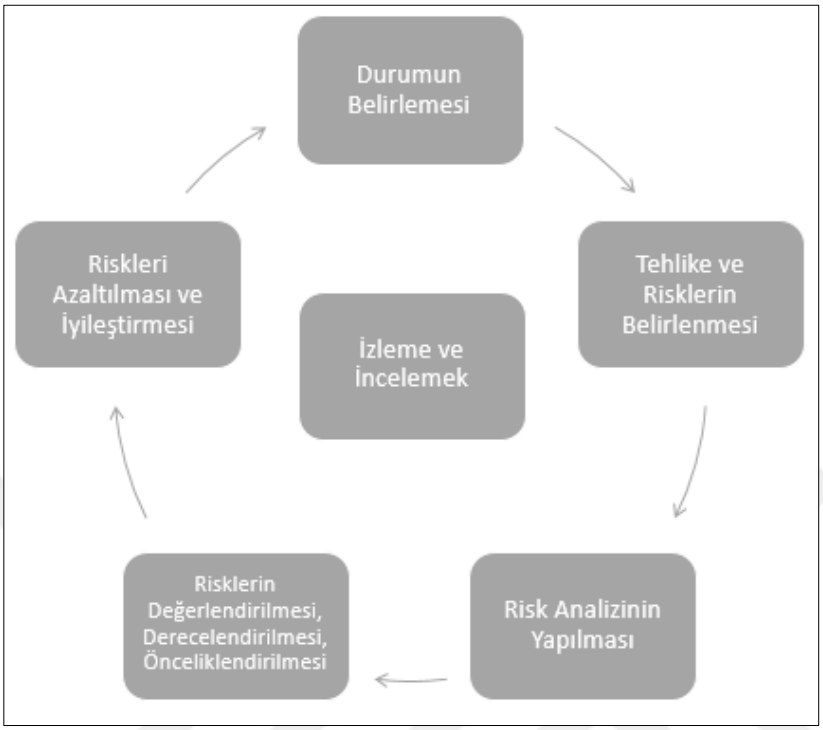
v. **Fırsatları yakalaması:** Potansiyel olayların sadece tehdit gözünden değil de, uçtan uca tam bir bütün olarak ele alınması sayesinde fırsatlar tespit edilebilir ve bu fırsatlardan proaktif bir şekilde yararlanılabilir.

vi. **Sermayenin, karın ve şirket bütçesinin dağıtımının iyileştirilmesini:** Risk yönetim süreci sayesinde kuvvetli bilgiler elde edilebilir. Bu sayede de genel sermaye ihtiyaçları etkin bir şekilde değerlendirilir ve sermaye tahsisini geliştirilir.

5.1.6 Risk yönetim şeması

Standart bir risk yönetim süreci 5 adımdan oluşmakta ve bu süreç birçok uygulamada bulunabilmektedir. Risk yönetim şeması ile ilgili birden çok şema olabilmesine rağmen, bu risk yönetim şemaları aslında birbirlerinden çok da farklı değildirler. Risk

yönetim şeması Şekil 5.6'da gösterildiği üzere temel olarak aşağıda belirtilen 5 adımdan oluşmaktadır [89].



Şekil 5.6 : Risk yönetim şeması [89].

Bu adımlar birer birer incelenecek olursa;

5.1.6.1 Durumun belirlemesi

Durumun belirlenmesi, organizasyonun risk ile karşı karşıya kaldığı bir durumda riski yönetebilmesi için dahili ve harici parametreleri belirlenmesidir. Durumun belirlenmesi risk yönetimi sürecinin kapsamını tanımlar ve risklerin değerlendirileceği kriterleri belirlemektedir.

Risk değerlendirme planlamasının başlangıcındaki hem dış hem de iç bağlamın gözden geçirilmesi, artan risklere tabi olabilecek süreçlerin belirlenmesine yardımcı olmaktadır ve bu nedenle risk değerlendirmesinden en yüksek değeri elde etmektedir. İç ve dış durumun belirlenmesindeki en önemli nedenlerden bir tanesi de risklerin iç ve dış etkenlerden dolayı çıkabiliyor olmasıdır. Örnek vermek gerekirse [97];

- Dış riskler, yasal düzenleme ortamı ve piyasa koşulları gibi, firmanın genel olarak etkileyemediği çevresel koşullardan kaynaklanan risklerdir.
- İç riskler, karar vermekten ve firmanın faaliyetleri ve amaçları dahil olmak üzere iç ve dış kaynakların kullanımından kaynaklanan risklerdir.

a) Harici durumun belirlenmesi

Harici durum ya da dış bağlam, organizasyonun amaçlarına ulaşmak istediği dış ortamdır. Harici durumu anlamak risk yönetimi için çok önemlidir. Özellikle risk kriterleri geliştirilirken dış paydaşların amaç ve endişeleri de göz önüne alınmalıdır. Kurum çapında bir içeriğe dayanmaktadır, ancak yasal ve düzenleyici gerekliliklerin spesifik detayları, paydaş algıları ve risk yönetimi sürecinin kapsamına özgü risklerin diğer yönleri ile ilgilidir [98].

Bir organizasyon için harici durum başlıca şunları kapsamaktadır:

- Sosyal ve kültürel, politik, yasal, düzenleyici, finansal, teknolojik, ekonomik, uluslararası, ulusal, bölgesel veya yerel doğal ve rekabetçi ortam
- Organizasyonun amaçları üzerinde etkili olan kilit faktör ve trendler
- Harici paydaşlar ile olan ilişki ve paydaşların değer ve algıları
- Güçlü yönler, zayıf yönler, fırsatlar ve tehditler

b) Dahili durumun belirlenmesi

Risk yönetimi süreci, kurumun kültürü, süreçleri, yapısı ve stratejisi ile hizalanmış olmalıdır. Dahili durum ya da iç bağlam ise, organizasyonun içerisindeki riski yönetme biçimini etkileyebilecek herhangi bir olgudur [98].

Dahili durumun belirlenmiş olması gerekmektedir. Bunun nedenleri ise,

- Risk yönetimi organizasyonun amaçları bağlamında gerçekleşir.
- Belirli bir projenin, sürecin veya faaliyetin amaçları ve kriterleri, kuruluşun bir bütün olarak hedefleri ışığında değerlendirilmelidir.
- Bazı kuruluşlar, stratejilerini, projelerini veya iş hedeflerini başarmak için karşılarına çıkan fırsatları yakalamakta başarısızdır. Bu durum devam eden örgütsel bağlılığı, güvenilirliği, güven ve değeri etkiler.

Bir organizasyon için dahili durum başlıca şunları kapsamaktadır:

- Yönetim, organizasyon şeması, roller ve sorumluluklar,
- Politikalar, hedefler ve bunlara ulaşmak için yürürlükte olan stratejiler
- Kaynak ve bilgi birikimi açısından yapabilme yeteneği,

- Dahili paydaşlar ile olan ilişki ve paydaşların değer ve algıları
- Organizasyon kültürü
- Bilgi sistemleri, bilgi akış durumu ve karar verme süreçleri
- Kuruluş tarafından kabul edilen standartlar, rehberler ve modeller
- Sözleşmeye dayalı ilişkilerin şekli ve kapsamı.
- Firmanın risk toleransı ve iştahı
- İnsanların, sistemlerin ve işlemlerin kabiliyeti
- Yönetişim, yapı, roller ve sorumluluklar

5.1.6.2 Tehlike ve risklerin belirlenmesi

Firmaya karşı olan risk ve tehditlerin belirlenmesi, etkin bir risk yönetiminde çok önemli bir adım olarak görülmektedir. Bu nedenle risk ve tehditlerin kapsamlı bir şekilde belirlenmesi gerekmektedir. Bu adımda gözden kaçan veya göz önüne alınmayan potansiyel bir risk, ilerleyen süreçlerde de analizden çıkarılacaktır. Bu durumda bahsi geçen riskin ilerleyen zamanlarda neden olacağı büyük maddi ve manevi sorunlara da davetiye çıkarmak demektir.

Bu evrede hasar, tehdit, tehlike senaryolarını tanımlanmalıdır. Bu senaryolar, tehlike kaynağını ve kişilerin maruz kalmasını tanımlamayı içerir. Bu senaryolarda oluşan risk olayına neden olabilecek potansiyel tetikleyicileri belirlenmesi gerekmektedir. Tek bir risk olayının belirli bir nedeni veya birden fazla olası nedeni olabilir. Ayrıca unutulmamalıdır ki tek bir neden birden fazla riske uygulanabilir.

Yine bu sırada yani risk olayı gerçekleşirken olası etkinin tanımlanması gerekmektedir. Yine göz önünde bulundurulması gereken durum, tek bir risk olayının belirli bir sonucu veya birden fazla olası sonucunun olabileceğidir.

Faka bu senaryolar oluşturulmadan önce tehlike ve risklerin belirlenmesinden önce risk kriterlerinin belirlenmesi birinci önceliktir. Bunun nedeni risk yönetim sürecinin neye karşı yapılacağının bilinmesidir. Tezin konusu dahilinde siber riskler ve tehditler üzerine yapılacak bir risk belirlemesi, risk yönetim şemasının devam eden 3.,4. ve 5. adımında da yarar sağlayacaktır. Fakat şu unutulmamalıdır ki risk evrensel bir kavramdır ve risk kriterinin belirlenmesinde de evrensel ve olmazsa olmaz bazı faktörler mevcuttur.

Bu nedenle risk kriterlerini belirlerken dikkate alınması gereken faktörler aşağıdaki gibidir [98].

- Firmanın ne kadar riski kabul edilebilir olduğu,
- Tolere edilebilecek risk miktarının ne kadar olduğu
- Risk seviyelerinin nasıl belirleneceği,
- Olasılığın nasıl tanımlanacağı, olasılığın ve sonucun zaman çizelgesinin belirlenmesi

İyi bir risk yönetim sürecinde firmanın sürecin bütününe bakarak, tüm riskleri göz önüne almalı ve daha sonra bu riskler karşısında bir analiz ve değerlendirme yapması gerekmektedir.

Risk ve tehditlerin belirlenmesine öncelikle bazı soruları sormak risklerin belirlenmesine yardımcı olacaktır.

- Hangi varlıkları korumamız gerekir?
- Hangi sistemlerde açıklarımı olabilir?
- Çalışanlarımız siber güvenlik dolaylı olarak bilgi teknolojileri hakkında yeteri kadar bilgi sahibi midir?
- Siber güvenlik dolaylı olarak bilgi teknolojileri hakkında yeterince eğitim verildi mi?
- Hangi aktiviteler en karmaşıktır?
- Firma içerisinden birisi firmaya nasıl zarar verebilir?
- Nerede savunmasızız?
- Hedeflerimize ulaşıp ulaşmadığımızı nasıl biliyoruz?
- Hangi varlıkları korumamız gerekir?
- En çok hangi bilgilere ihtiyaç duyuyoruz ve bunları sakladığımı veri tabanları gerçekten güvenilir mi?
- Ne yanlış gidebilir ki?
- Siber güvenlik dolaylı olarak bilgi teknolojilerine yeteri kadar yatırım yapıldı mı?

- Nasıl başarısız olabiliriz?
- Başarılı olmamız için doğru olan ne olmalı?

Risk belirleme işlemi organizasyonun iş liderleri ile birlikte bir iş kolunu veya tüm organizasyonu etkileyebilecek olan tehditlerin, siber saldırılara açık olma durumunun, yükümlülüklerin değerlendirilmesidir. Organizasyonun büyüklüğüne ve şirketin organizasyonun şeması bağlı olarak değişiklik gösterebilmesine rağmen temel olarak finanstan sorumlu başkan (CFO - Chief Financial Officer), bilgi sistemleri grubu başkanı (CIO - Chief Information Officer), , teknolojiden sorumlu başkan (CTO - Chief Technology Officer), departman/bölüm yöneticileri, Hukuk ve İç Denetim çalışanları, bilgi güvenliği yöneticisi, siber güvenlik yöneticisi ve risk yöneticisinden oluşmaktadır [99].

Risklerin belirlenmesi için en çok kullanılan yöntemler arasında delphi tekniği, balık kılçığı veya diğer adı ile ishikawa diyagramı ve risk kırılım tekniği bulunmaktadır.

Daha önce de bahsedildiği gibi organizasyon veya kuruluş, risk kaynaklarını, etki alanlarını, olayları ve nedenlerini ve bunların potansiyel sonuçlarını tanımlamalıdır. Bu adımdaki asıl amaç organizasyonun amaçlarına ulaşmasında gecikmelere neden olabilecek, amaçlarına ulaşmayı ve organizasyonun gelişmesini tamamen engelleyecek kapsamlı bir risk listesinin elde edilmesidir.

Fakat risk belirleme adımı içerisinde dikkat edilmesi gerek bir nokta vardır. Risk kaynağı veya nedeni açık olun veya olmasın, bu risk kaynağının veya nedenin oluşturduğu risk, organizasyon tarafından kontrol altında olsa dahi risk belirleme listesinde olması gerekmektedir [98]. Bunun yanı sıra sadece riskler değil riske neden olabilecek nedenler ve senaryolarda, neden olabilecekleri sonuçlar ile birlikte göz önünde bulundurulmalıdır.

Organizasyonlar risk belirleme işlemi yaparken daha önce bahsedildiği gibi uygun bilgiye sahip kişileri bir araya getirmeli ve kurumun amaçlarına uygun risk belirleme araçları kullanmalıdırlar.

Risk belirleme çalışması sonrasında elde edilecek olan risk listesi sayesinde, her riskin bir numarası, sahibi, açıklaması, sınıfı ve değeri olacaktır. Burada söz edilen değer risk matrisinde düşük orta ve yüksek olarak bahsedilen risk seviyelerine karşılık gelmektedir. Risk belirleme çalışmaları sırasında kullanılabilecek teknikler arasında

olay analizi, tehdit modelleme, saldırıya açık olma analizi, senaryolar ve beyin fırtınaları sayılabilmektedir.

5.1.6.3 Risk analizinin yapılması:

Risk analizi, riskin nedenleri ve kaynakları, olumlu ve olumsuz sonuçları ile bu sonuçların ortaya çıkma olasılığını dikkate almakta ve bu sayede de riskin anlaşılmasını sağlamaktadır. Risk analizinde sonuçları ve olasılıkları etkileyen durumlar belirlenmelidir. Çünkü risk analizi, risk değerlendirmesine, risklerin müdahale edilip edilmemesi gerektiğine ve en uygun risk müdahale stratejileri ve yöntemlerine ilişkin kararlara girdi sağlamaktadır [98].

Sonuçların ve olasılıklarının ifade ediliş şekilleri ve risk düzeyini belirlemek için birleştirildikleri yol riskin türünü belirlemektedir. Sonuçların ve olasılıklarının risk kriterleri ile tutarlı olması gerekmektedir. Farklı risklerin ve bu risklerin kaynaklarının arasındaki bağlılığı dikkate almak da önemlidir. Risk analizi yapılırken uzmanlar arasında görüş ayrılığı, belirsizlik, kullanılabilirlik, kalite veya sınırlamalar gibi faktörler belirtilmeli ve vurgulanmalıdır.

Risk analizi, riske, analizin amacına ve mevcut bilgi, veri ve kaynaklara bağlı olarak farklı derecelerde ayrıntılarla yapılabilir. Ayrıca sonuçlar ve oluşma olasılıkları bir olayın veya olay kümesinin sonuçlarını modelleyerek belirlenebilir. Ayrıca daha önce yaşanan tecrübelerden de çıkarımlar yapılabilir [98].

Siber güvenlik özelinde risk analizini konuşacak olursak, siber güvenlik konusunun tüm siber fiziksel sistemler için en büyük risk olduğu aşikardır. Bir siber fiziksel sistemin riskini analiz edebilmek için analiz modelinin, siber saldırının şiddeti, saldırının başarı olasılığı gerekmektedir.

Yüksek performanslara sahip gerçek zamanlı ve sağlam bir otonom sistem olan siber fiziksel sistemler (SFS), gelecekteki ağlar altında sıkı bir şekilde entegre edilmiş ve etkileşime giren farklı hesaplama ve fiziksel bileşen ölçeklerine sahip yeni akıllı karmaşık sistemlerdir [100]. İletişim, elektrik enerjisi, nükleer güç, ulaşım, petrol gibi kritik ulusal altyapılarda yaygın olarak kullanılmaktadır. Bunun dışında akıllı şehir ve ağ kontrol sistemleri de siber fiziksel sistemlere örnek olarak verilebilmektedir. İletişim, bilgi işlem ve kontrol teknolojisinin entegrasyonu ile siber saldırılar, siber fiziksel sistemlerin ana tehdidinden biri haline geldi. Stuxnet örneğine, siber

saldırıların kritik altyapılara çok büyük hasarlar verebileceğinin en güzel örneklerinden biri olarak gösterilebilmektedir.

Bu nedenle siber fiziksel sistemlerin istikrar ve güvenliğinden emin olmak için, risk analizini uygulamak çok önemlidir. Risk analizinin yapılabilmesi içinde değerinin tespiti ve hangi risklere maruz olduğunun tespiti önemlidir.

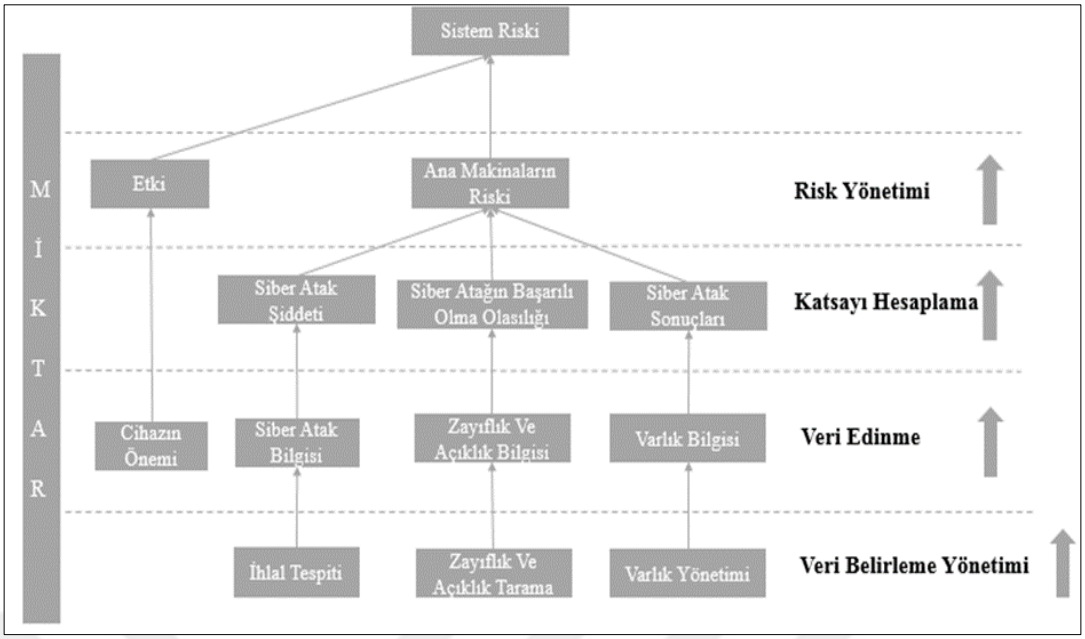
Güvenlik risk analizinin başlıca faydalarına bakacak olursak [101];

- Güvenli bilgi yönetimi geliştirmek
- Organizasyonun kritik olan varlıklarının tespiti, incelenmesi, yakından izlenmesi ve etkili bir şekilde korunmasını sağlamak
- İleride yapılacak olan analizler için geçmişten yararlı veriler bırakmak
- Organizasyonun zayıflık tespitini yapmak
- Organizasyonun güvenlik politikalarını güncel tutmak
- Organizasyonun güvenlik bilincini dolaylı yoldan da olsa arttırmak
- Karar vermede etkin güvenlik bilgi güvenliği politikalarının destelenmesini sağlamak

Güvenlik riskinin temel nedeni siber fiziksel sistemlerde bulunan güvenlik açıklarının varlığıdır. Potansiyel bilgisayar korsanları, güvenlik açıklarını kullanarak sistemde hasara, aksamaya, sistemden veri çalınmasına veya sistemin tamamen çalışmamasına neden olabilmektedir. Ayrıca hasarın derecesi saldırıya uğramış sunucuların veya sistemlerin değerine bağlıdır.

Siber atakların ve sistem zayıflıklarının giriş verisi olarak alındığı bir sistemde yapılan bir araştırmaya göre, siber fiziksel sistemlerin siber güvenliği için risk değerlendirme çerçevesi Şekil 5.7'de gösterilmiştir.

Risk analizi adımına gelmeden önce, belirleme adımları ve katsayı hesaplama adımları bulunmaktadır. Bu adımları daha yakından inceleyecek olursak belirleme adımlarında zayıflık taraması ile sistemin toplam zayıflık analizi, değer yönetimi ile sistemin toplam değeri ve saldırı tespit yöntemi, güvenlik duvarı sistem kayıtları ile de atak bilgileri elde edilmektedir.



Şekil 5.7 : Siber fiziksel sistemlerin siber güvenliği için risk analiz çerçevesi [100].

Daha sonra, siber saldırıların bilgilerine dayanarak şiddeti, güvenlik açıklarının bilgilerine dayalı saldırı başarı olasılığını ve saldırı sonucu da varlık değerlerinin bilgisine göre hesaplanmaktadır. Bu adım da katsayı hesaplama adımı olarak belirtilmektedir. Bu bilgiler elde edildikten sonra hedef sunucunun güvenlik riski hesaplanmaktadır. Total sistemin riskinin hesaplanması konusunda da cihaz öneminin direkt etkisi bulunmaktadır.

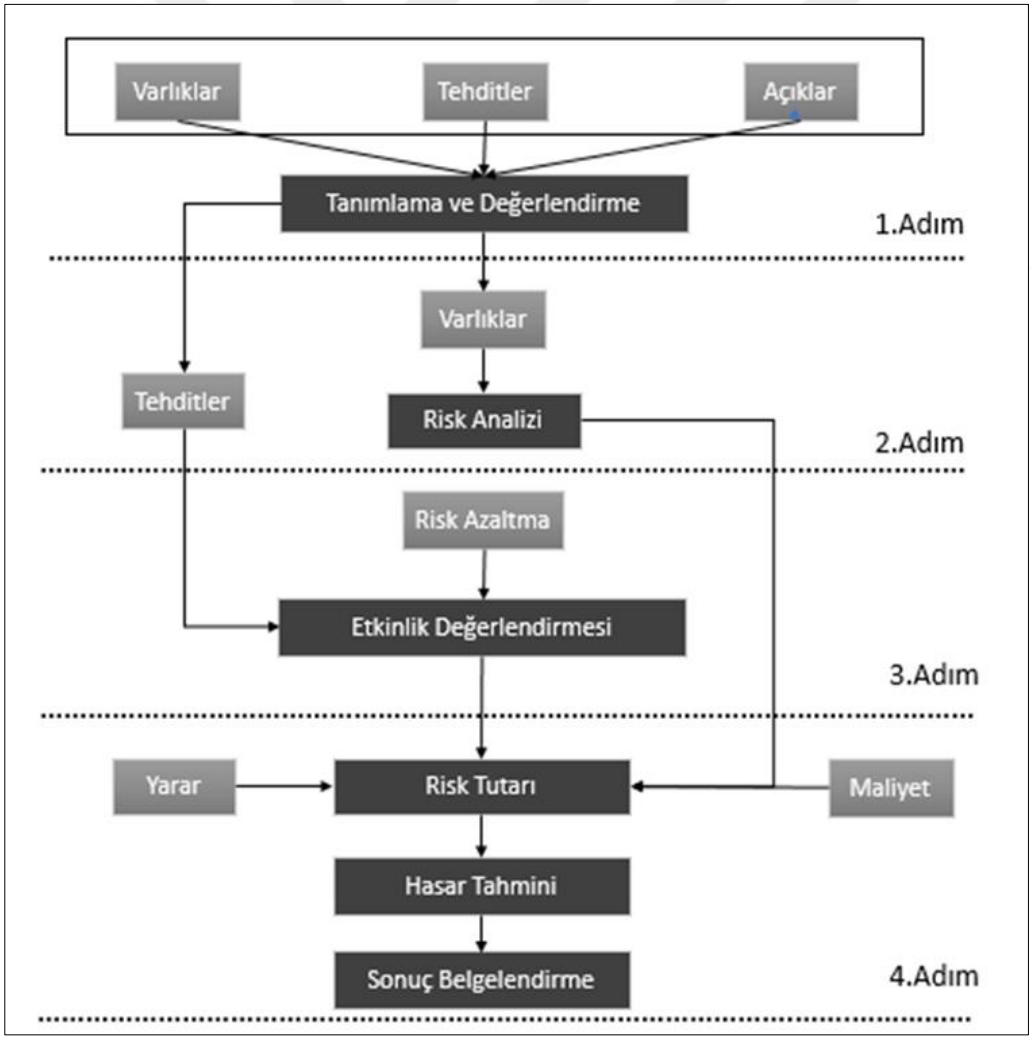
Şekil 5.8'de gösterilen başka bir araştırmada [101] risk analizinin 4 adımdan oluştuğu belirtilmiştir.

Risk analiz sürecini ikinci model üzerinden inceleyecek olursak aslında Şekil 5.7'deki sunucu ve sistem üzerindeki riskin tespiti konuda örtüştüğü görülecektir.

Risk analiz modelindeki birinci adımında gösterildiği üzere riski oluşturan 3 etken yani varlıklar, tehditler ve açıklıklar üzerinde bir tanımlama ve değerlendirme yapılmaktadır. İkinci adımda ise Sistemin tüm varlıkları, tehditleri ve açıklıkları yani birinci adımdaki verileri göz önüne alınarak toplam bir risk analizi yapılmaktadır. Üçüncü adımda ise, mevcut tehditlerin neden olduğu riskleri azaltmaya yönelik gerekli yönetim belirlenmesi ve etkinlik değerlendirmesi yapılmaktadır.

Risklerin azaltılması konusunda kısa bir giriş yapacak olursak, en yaygın risk azaltma yöntemlerinde hangi uygulamalar kullanılabileceği aşağıda belirtilmiştir [101].

- **Erişim kontrolü**: Parola tabanlı kimlik doğrulama sistemi, akıllı kart tarzında fiziksel erişim ekipmanları, şifre tanımlamaya dayalı sistemler kullanılabilir.
- **Şifre kontrolü**: Şifreleme algoritmaları, açık anahtar yapısı (AAA) kullanılabilir.
- **İnternet güvenlik kontrolü**: Saldırı tespit sistemleri, güvenlik duvarları, DDoS saldırılarından korunmak için bulut teknolojisinden yararlanma gibi önlenmeler alınabilmektedir.
- **Uygulama güvenlik kontrolü:** Veri tabanı güvenliği, sistem dosyası güvenliği gibi uygulamaları kapsamaktadır.
- **Fiziksel/çevresel güvenlik kontrolü:** Tesisleri güvenliği, kurum güvenliği, giriş/çıkış kontrolü gibi uygulamaları kapsamaktadır.



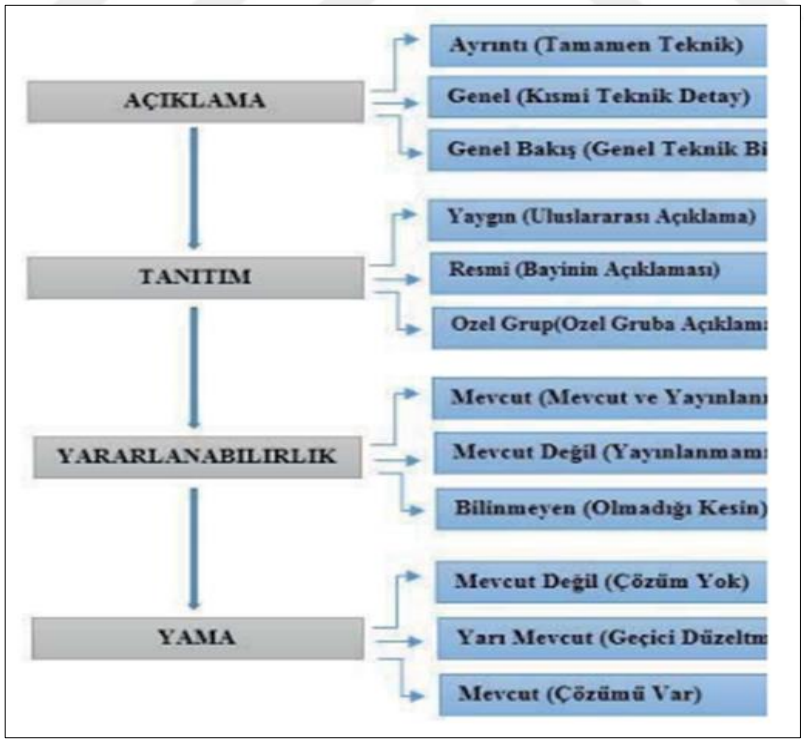
Şekil 5.8 : Güvenlik risk analiz modeli [101].

Son adım olan dördüncü adımda ise ikinci ve üçüncü adımda hesaplanan risk tutarına fayda ve maliyetler de eklenerek son risk tutarı elde edilmektedir.

Bilgi güvenliği, siber güvenlik gibi konulardaki güvenlik açıklarının risk analizine de bir göz gezdirecek olursak, güvenlik açıklarının risk faktörünün yani dolaylı olarak risk analizinin en önemli faktörlerinden olduğu görülmektedir.

Daha önce de belirttiğim gibi kusursuz, hiçbir açığı olmayan, mükemmel bir sistem bulunmamaktadır. Bilgisayar korsanlarının çeşitlerinin anlatıldığı bölüm 3.2'de siyah ve beyaz şapkalı bilgisayar korsanları arasındaki farklar açıkça belirtilmişti. Sisteminde bir açık olan ve bu açığın farkında olmayan bir organizasyon eğer şanslı ise, bu açık bir beyaz şapkalı korsan tarafından fark edilir ve kapatılması için bir şans elde edilmiş olur. Fakat siyah şapkalı bir korsan tarafından ilk olarak fark edildiğinde gerek maddi gerek ise sistemsel olarak büyük kayıplar vermek çok olası bir durumdur.

[101] 'a göre güvenlik açıklarının bir yaşam döngüsü bulunmaktadır ve güvenlik açıklarının kapatılması için yayınlanan ve/veya uygulanan her yama yeni bir açık keşfinin yani yeni bir döngünün başlangıcı olabilir. Bu döngü Şekil 5.9'da gösterilmektedir.



Şekil 5.9 : Güvenlik açığı yaşam döngüsü [103].

5.1.6.4 Risklerin değerlendirilmesi, derecelendirilmesi ve önceliklendirilmesi

Risk değerlendirmesi, derecelendirilmesi ve risklerin önceliklendirilmesi konusu başlığından da tahmin edilebileceği üzere risk analizinin sonuçlarına dayanarak, hangi risklerin önlem alınmaya ihtiyacı olduğu ve önlem uygulamasının önceliğine dayanarak karar vermede yardımcı olmaktır.

Risk değerlendirmesi, analiz sürecinde bulunan risk düzeyini, şartlar göz önüne alınarak belirlenen risk kriterleriyle karşılaştırarak içerir ve ancak bu karşılaştırmanın sonrasında ortaya çıkan riske önlem alınıp alınmayacağına karar verilebilmektedir.

Siber güvenlik ya da genel adı ile bilgi teknolojileri özelinde daha önce belirtilen risk analiz modelleri, risk analiz çerçeveleri dikkate alındığında en önemli bileşenlerin tehdit, açıklık ve varlık olduğu açıkça görülmektedir. Risk değerlendirmesi konusunu da güvenlik özelinde konuşacak olursak, güvenlik risk değerlendirmeleri yapılırken bazı yöntemlerden faydalanıldığını söyleyebiliriz. Bu yöntemler başlıca; Bilgi Güvenliği Değerlendirme Metodolojisi (IAM), Güvenlik Açığı Değerlendirme Çerçevesi (VAF) ve Operasyonlu Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (OCTAVE) ‘dir [101].

- **Bilgi güvenliği değerlendirme metodolojisi (IAM):** Bilgi Güvenliği Değerlendirme Metodolojisi, bir kuruluşun potansiyel güvenlik açıklarını analiz etmek ve Ulusal Güvenlik Ajansı (NSA) deneyimleri ile ABD Savunma Bakanlığı'nın bir eğitim programında kullanmak için oluşturulan bir güvenlik değerlendirme yöntemidir. Kısacası bu bilgi güvenliği değerlendirme metodolojisi yapısal güvenlik açıklarını analiz ederek güvenlik risklerini değerlendiren bir yöntemdir [101].
- **Güvenlik açığı değerlendirme çerçevesi (VAF):** Güvenlik açığı değerlendirme çerçevesi 1988 yılında KPMG Peat Marwick LLP ile Amerika Birleşik Devleti Kritik Altyapı Güvencesi Ofisi Komisyonu tarafından geliştirilen bir yöntemdir. Bu yöntem ilgili organizasyonun asgari temel altyapısıyla, seçilen varlıklardan toplanan güvenlik açığı verilerini analiz eder ve daha sonra nitel değerlendirmenin bir sonucu olarak güvenlik açığı derecesini hesaplar [101].

- **Operasyonel kritik tehdit, varlık ve güvenlik açığı değerlendirmesi (OCTAVE):** OCTAVE Amerika Birleşik Devletlerin de Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü tarafından geliştirilen bir güvenlik değerlendirme yöntemidir. Octave yönetimine göre güvenlik değerlendirmesi üç adımdan oluşur. Bunlardan birincisi, varlıklara dayalı tehdit senaryolarının dosyası oluşturma, ikincisi önemli özellikler ile ilgili güvenlik açıklarını tanıma ve son olarak da riski değerlendirme, ölçmek ve güvenlik stratejileri geliştirmedir [101].

Risk değerlendirmesi sırasında göz önünde bulundurulması gereken bazı kriterler bulunmaktadır. Bu kriterlerde başlıca, riskin organizasyona karşı yaratabileceği etkinin büyüklüğü, önem derecesi, maliyet ve faydalar, yasal koşullar ve en son olarak da paydaşların endişeleri bulunmaktadır.

Daha önce de belirtildiği gibi organizasyon tarafından risk değerlendirmesi, derecelendirilmesi ve önceliklendirilmesi kriterleri sonrasında mevcut kontrollerin sürdürülmesi dışında, risk hakkında hiçbir şekilde önlem almama kararı çıkabilir. Bu karar, kuruluşun risk tutumundan ve kurulan risk kriterlerinden kaynaklanmaktadır.

5.1.6.5 Riskleri azaltmak ve iyileştirmek

Risklerin iyileştirilmesi, riski hafifletmek, bu seçenekleri değerlendirmek ve daha sonra eylem planlarını hazırlamak ve uygulamak için çeşitli seçenekler geliştirmeyi içerir. Tahmin edilebileceği gibi en yüksek puan alan riskler acil olarak ele alınmalı ve buna göre de bir aksiyon planı çıkartılmalıdır. Burada dikkat edilmesi gereken bir nokta da en uygun risk iyileştirme yönetimini seçmek, elde edilen faydalara karşı her bir etkinliğin uygulanma maliyetlerini dengelemek anlamına gelir. Yani çok küçük bir risk için, çok büyük maliyetlere neden olabilecek bir iyileştirme yöntemi seçmek, her ne kadar riskin ortadan kalmasına neden olacak olsa da verimli değildir. Kısaca çok iyi bir maliyet, fayda analizi yapılmalıdır.

Bu nedenle riskle mücadele ve iyileştirme kararları organizasyonların iş liderleri ve orta ve üst seviye yönetici ve çalışanlarla birlikte yapılan bir çalışmadır. Riskle mücadele ve iyileştirme seçenekleri tek tek veya kombinasyon halinde düşünülebilir ve uygulanabilir. Bu sayede de organizasyon iyileştirme seçeneklerinin kombinasyonunun yararlanabilir.

İyileştirme planı öncelik sırasını çok net bir şekilde ortaya koymalıdır. Bunun nedeni küçük risklerin, acil kapsamındaki risklerden daha önce planlanmaması ve böylece büyük risklerin bir an önce giderilerek, olası bir arıza, çökme, hizmet verememe, veri çalınması gibi durumların önüne geçmektir.

Risk iyileştirmesi, sistem için yeni riskler doğurabilmektedir. Literatür de riske müdahale edildikten sonra kalan bu risk, artık risk olarak geçmektedir. Bu nedenle izleme, önlemlerin etkili kaldığına dair güvence vermek için risk tedavi planının ayrılmaz bir parçasıdır [104].

Risk iyileştirme adımı kendi içerisinde bir yaşam döngüsüne sahiptir ve bu yaşam döngüsünü öncelikle risk iyileştirmenin değerlendirilmesi, ardından artık risk düzeylerini tolere edilebilir olup olmadığına kararı, karar sonrasında eğer bu artık riskler tolere edilemez ise, yeni bir risk iyileştirme yönetimi üretilmesi ve son olarak da bu yönetim etkinliğinin değerlendirilmesi oluşturmaktadır.

Riskle mücadele etme, iyileştirme kapsamında riskin çeşidine ve riskin doğasına göre temel olarak 4 seçenek mevcuttur [104].

- **Risk değiştirme:** Risk değiştirme, riski olumlu veya olumsuz etkileyebilecek denkleme yeni bir girdi tanıttığınızda ortaya çıkar. Teknoloji yönetimi ve bilgi güvencesi alanında geleneksel olarak risk azaltılmasına odaklanılmaktadır. Risk değişikliği için, bir risk belirlendiğinde ve doğrulandığında, bir kontrol (genellikle bir teknolojinin, sürecin, prosedürün veya çalışan eğitiminin tanıtılması) belirlenir ve orijinal risk seviyesini dengelemek için uygulanır. Bu kontrol belirlenirken genellikle çalışan bilgilendirme ve eğitimi, teknoloji, süreçler ve prosedürler ile ilgili durumlarda göz önüne alınmaktadır.
- **Risk transfer:** Risk transferi, bir kuruluşun bir riski kendi bünyesinden bir diğerine taşımanın yollarını ve araçlarını tanımladığı seçenektir. Bu seçenek temek olarak iki şekilde sağlanmaktadır. Birincisi riske karşı sigortalama, ikincisi ise dış kaynak kullanımıdır. İki durumda da riski kabul eden üçüncü taraf, bu yükümlülüğün farkında olmalı ve kabul etmeyi kabul etmelidir.
- **Riskten kaçınma:** Riskten kaçınma seçeneği oldukça basit ve uygulaması kolay bir seçenek olarak görülmektedir. Temel olarak kabul edilemez riskin görüldüğü anda, bu riski getiren etkinliğe devam etmemeye karar vermektir. Fakat aynı zamanda riskten kaçınma iş hedeflerini karşılayan alternatif daha

kabul edilebilir bir etkinlik seçmek veya alternatif daha az riskli bir yaklaşım veya süreç üzerinden ilerlemektir. Kısaca organizasyon bir riskin olduğunun farkında, bu riskin nelere sebep olabileceğinin de farkındadır. Bu nedenle de bu riskin ortaya çıkmasına izin verecek aktivitelerden kaçınmaktadır.

- **Riski kabul etme:** Risk kabulü, belirlenen risk seviyesinin, değişiklik veya aktarım yoluyla başka bir değişiklik yapılmaksızın bilinçli ve kasıtlı olarak kabul edilmesidir. Bu durum risk derecesinin kabul edilebilir bir seviyede olduğu veya riski iyileştirme veya yok etmek için gerçekleşecek olan maliyetin faydadan daha ağır olduğu durumlarda ortaya çıkmaktadır. Bu seçenek, diğer risk iyileştirme seçenekleri gerçekleştirildikten sonra artık bir riskin kaldığı durumlarla da alakalı olabilir. Bu seçenekte riski tedavi etmek için başka bir işlem yapılmamaktadır, ancak devam eden izleme önerilmektedir.

5.1.6.6 İzleme ve inceleme

Risk yönetimi şeması içerisinde bulunan izleme ve inceleme, risk yönetimi sürecinin planlı bir parçası olmalı ve düzenli kontrol veya gözetim içermelidir. Sonuçlar, uygun şekilde harici ve dahili olarak kaydedilmeli ve bildirilmelidir. Sonuçlar, firmanın risk yönetimi çerçevesinin gözden geçirilmesi ve sürekli iyileştirilmesi için de bir giriş olmalıdır.

İzleme ve inceleme adımı sayesinde firmanın risk kaydında belirlenen riskleri düzenli olarak gözden geçirme ve risk durumunu değiştiren herhangi bir eylem veya olayı belgeleme fırsatı çıkmaktadır.

İzleme ve inceleme adımı sürecin tamamında olduğunda ayrı bir adım olarak ele alınmamalıdır. İzleme ve inceleme yukarıda bahsedilen 5 adım ile de entegre bir şekilde varlığını belli etmelidir ve organizasyonun izleme ve inceleme süreçleri risk yönetimi sürecinin tüm yönlerini

- Kontrollerin hem tasarım hem de operasyonda etkili ve verimli olmasının sağlanması,
- Risk değerlendirmesini iyileştirmek için daha fazla bilgi edinmesi,
- Olaylardan, değişikliklerden, eğilimlerden, başarılardan ve başarısızlıklardan dersler çıkarabilme ve analiz edilmesi,
- Ortaya çıkan risklerin belirlenmesi,

- Risk kriterindeki değişiklikleri, riske göre risk iyileştirmelerinde gerekli olabilecek değişikliklerini de kapsayacak şekilde iç ve dış koşul değişikliklerini tespit edilmesi,

Amaçları ile kapsamalıdır [98].

5.1.7 Risk yönetim sürecinde başarı

Risk yönetim sürecinde başarı elde edilebilmesi için üst yönetim kadrosunun gerektiği gibi sorumluluk almasına, bilgi teknolojileri ekibinin güncel konuları çok yakından takip ederek, risk yönetim sürecine desteğinin ve katılımının tam olmasına, analiz, izleme, değerlendirme, önceliklendirme, durum belirleme ve iyileştirme ekiplerinin kısacası tüme risk yönetiminin yetkinliğine bağlı durumdadır. Bu yetkinlik çerçevesi içerisinde örnek olarak risk yönetim ekibinin uygun risk değerlendirme yöntemleri uygulamaları kullanması, maliyet-risk analizi sonuçlarını çok iyi yorumlanması, risk kriteri belirlerken önceliklere dikkat edilmesi, prosedürlerin yakından ve dikkatle takip edilmesi gibi birçok etken bulunmaktadır.

Bilgi teknolojileri, siber güvenlik gibi konuların henüz daha yeni yeni yaygınlaştığı düşünülecek olursa, önümüzdeki dönemde bilgi teknolojileri risk yönetimi kavramının daha da yaygınlaşacağı aşikardır. Bilgi bir organizasyon için en önemli olgudur. Bu nedenle bilgi korunmalı ve çok iyi bir şekilde saklanmalıdır. Bu nedenle bilgi teknolojileri riskleri konusunda firmaların yatırım yapmaları ve bu yatırım doğrultusunda farkındalık yaratma, risklerin değerlendirilmesi ve analizi çalışmalarında bulunmaları kaçınılmazdır.

5.2 Siber Güvenlikte İnsan Etkisi

Siber güvenlik yönetim modelinin içerisinde muhtemelen uygulanması ve kontrol etmesi en zor olan bölüm olan siber güvenlikte insan etkisi ya da literatürde geçtiği şekilde güvenlik kültürü, yönetim modeli içerisinde göz ardı edilmez bir yere sahiptir.

Organizasyonlar, her zaman yaptıkları gibi kendiler için bir risk ile karşı karşıya kaldıkları zaman yeni bir güvenlik sistemi satın almanın mı, riski göz ardı etmenin mi yoksa risk ile ilgili olarak ilgili firmalardan destek almanın mı organizasyon için daha karlı olduğunu anlayabilmek için bilişimden, risk yönetim modelinden, matematikten veya geçmiş verilerden yararlanabilir ve belki de en karlı yolu bulabilir. Fakat her ne

olursa olsun burada göz ardı edilmemesi gereken unsur insandır yani bu durumda şirketin çalışanlarıdır.

Organizasyonların en temelinde bünyesinde çalışan insanlar kadar savunmasız olduğunu anlamalıdır.

Güvenlik konusu organizasyonun departman ayırmaksızın tüm çalışanları tarafından anlaşılmalıdır. Bunun yanı sıra tüm organizasyon çalışanları kendilerini ve aynı zamanda da organizasyonu siber güvenlik konusunda nasıl savunmaları gerektiği konusunda ve yapacakları küçük gibi gözüken bir hatanın ne kadar büyük maddi ve manevi kayıplara neden olabileceğini veya organizasyonu daha büyük siber saldırılara maruz bırakacak zayıflıklar ortaya çıkarabileceğinin farkında olmalıdır.

Siber güvenlik yönetim modelinin bu bölümünde yapılan en büyük hata genellikle üst yönetim ve bilgi sistemleri çalışanlarının siber güvenlik ile ilgili güvenlik önlemlerinin daha öncelikli olduklarını ve sorumlulukları üzerlerinde hissetmesidir. Bu nedenle de siber güvenlik ile ilgili yapılan bir denetim sürecinde yalnızca üst yönetim veya bilgi sistemleri çalışanları denetlenmemelidir. Bunun yerine yapılması gereken siber güvenlik ile ilgili tüm dokümanların, tüm organizasyon çalışanları tarafından erişilebilir olması gerekmektedir. Bunun yanı sıra şirket içinde yapılacak olan küçük testler ile şirket çalışanlarının dikkat ve bilgi seviyeleri ölçülebilir ve ödüllendirme sistemi ile birlikte de siber güvenlik bilinci arttırılabilmektedir.

Sistemlerin başarısız olabilmesinin bir nedeni, sistemin çalışanlarının yanlış eylemidir.

Sistem güvenliği araştırmacıları, güvenlik başarısızlıklarını araştırmak ve başarısızlığa yol açan insan davranışını anlayabilmek için araştırmalar yapmaktadır. Bu insan davranışları ihlal, hata, yapılması gereken işin yanlış sırada yapılması olabilir.

Yaşanan her vaka her ne kadar nadir olsa da olay içerisinde ki insan davranışları belirli kalıplara uyma eğilimindedir. Bu kalıpları bir güvenlik hatası veya veri ihlali bağlamında anlamak, çalışanları desteklemek, güvenlik hatası ve ihlallerini veya veri ihlali olasılığını azaltmak için daha fazla koruyucu önlemlerin alınması ve uygulanması konusunda yeni fikirler ortaya çıkarmaktadır.

İnsan kararlarının, hareketlerinin nasıl veri ihlaline neden olabileceğini anlamak üzere İngiltere bilgi komisyonunun (ICO) yayını incelenmiş olup, diğer sorumlulukların yanı sıra komisyon, veri gizliliği yasalarını uygulamak için harekete geçebilmekte ve

konu ile ilgili yayınlar yapmaktadır. Bu yayınların analizleri, bilgi güvenliği ihlallerine yol açan en yaygın insan başarısızlıklarını belirlemek için toplanmıştır [105].

Elde edilen yayınlar, açıklanan ihlallerin, içerdekiler veya kuruluşa dışarıdan gelen kişilerin eylemlerinden kaynaklanıp kaynaklanmadığını belirlemek için analizinde kullanılmaktadır.

İçeriden ve dışarıdan olarak yapılan betimlemenin ayırımına gelecek olursak, içeriden olarak bahsedilen bireyler, verilerin sahibinin talimatı altında hareket eden bir birey olarak tanımlanmaktadır. Dışarıdan olarak belirtilen bireyler ise bu kapsam dışında kalanların tamamıdır. Temel olarak çalışanın eylemi, söz konusu kişi, veri denetleyicisinin çıkarları doğrultusunda hareket ettiğine veya yerel güvenlik politikasına göre hareket ettiğine inanıyorsa, iyi bir anlam ifade ediyordur. Bu tanıma uymayacak şekilde tam ters aksiyon ise kötü amaçlı bir aksiyon kategorisine girecektir.

İngiltere bilgi komisyonunun (ICO) raporlarını temel alarak bazı incelemeler yapılmıştır fakat bu incelemelerde sadece en büyük soruna yol açan ihlallerin araştırılması muhtemeldir, bunun nedeni birçok ihlal fark edilmeyebilir ve bu nedenle de bildirilmeyebilir. Bununla birlikte, bu raporlar, bağımsız bir üçüncü taraf tarafından soruşturmayı garanti edecek kadar önemli görülen veri ihlallerinin bir koleksiyonunu temsil etmektedir.

İncelenen 27 bildiri sonrasında içeriden olan kişilerin şirket dışından olan kişilere göre çok daha fazla data ihlallerinin sorumlusu olarak görülmektedir.

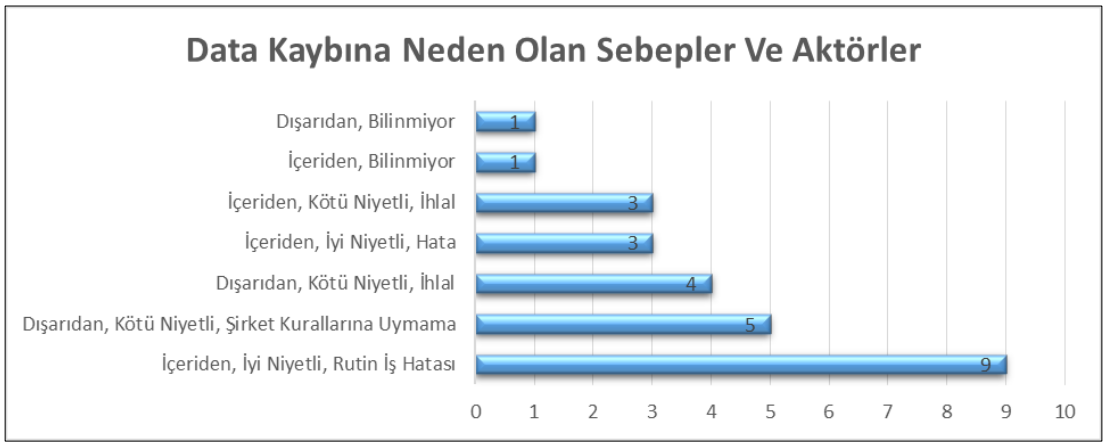
Şekil 5.10'da görülen değerler her ne kadar %63'e %37 gibi büyük bir fark olsa da burada dikkat edilmesi gereken nokta içeriden veya dışarıdan olan kişilerin iyi veya kötü niyetli olup olmadıklarıdır.

İhlale Neden Olan Kişi	Oran
İçeriden	17/27 (%63)
Dışarıdan	10/27 (%37)

Şekil 5.10 : Data ihlal oranları. [105].

Rapora göre data kaybına neden olan kişiler ve bunların sebepleri gösterilmiştir. Buradan da açıkca görüleceği üzere en çok daha kaybına neden olan aktörler şirket içerisinden ve iyi niyetli olan kişilerdir.

Şekil 5.11'de data kaybına neden olan sebepler ve aktörler gösterilmektedir.



Şekil 5.11 : Data kaybına neden olan sebepler ve aktörler [105].

Ayrıca İngiltere kökenli olarak her yıl yapılan bilgi güvenliği ihlalleri anketinde ki veriler siber güvenlik konusunda insan etkisinin ne kadar yeni ele alındığını ve öneminin giderek arttığını göstermektedir [106 - 108].

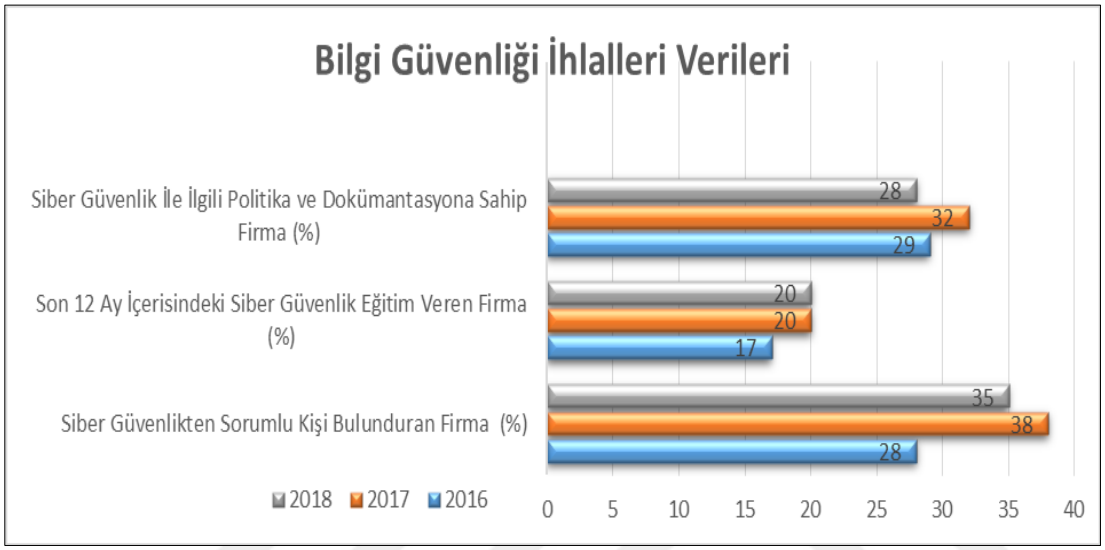
Araştırmanın yapıldığı firmalar içerisinde kaçının siber güvenlik konusunda sorumlu kişi veya kişilere sahip olduğu ile ilgili sorulan soruda çıkan veriler, 2016 yılında araştırmaya göre toplam 1008 firmanın yalnızca %28 inde siber güvenlikten sorumlu kişi bulunurken, 2017 yılına gelindiğinde bu ihtiyacın iki şekilde karşılandığını görüyoruz. Araştırma yapılan 1523 firmadan %49'u siber güvenlik ile ilgili konuları üçüncü parti, farklı bir firma üzerinden takip ederken, %38'lik kısmı şirket içerinde bulundurduğu bilgi güvenliği çalışanları ile siber güvenlik konusunu da ilerletmektedir. 2018 yılına gelindiğinde ise, 1519 firma arasında yapılan araştırmada çalışanların tamamen şirket bünyesinden oluşarak %35'lik bir kısmın bilgi güvenliği ve siber güvenlik üzerine çalıştığı görülmektedir. 2018 yılında dikkat çeken konu siber güvenlik çalışanlarının şirket bünyesinde olması ve belki de bu sayede üçüncü parti riskleri ortadan kaldırmak istemeleridir.

Araştırmanın bir diğer sorusunda son 12 ay içerinde organizasyon tarafından bir siber güvenlik eğitimi verilip verilmediği konusuna gelindiğinde ise, 2016 yılında organizasyonların %17'si, 2017 yılında %20'si ve 2018 yılında yine toplam organizasyonun %20'sinin son 12 ay içerinden siber güvenlik ile ilgili eğitim verdiği görülmüştür.

Siber güvenliğin yönetim pençesi kapsamlı yapılan araştırmada ise araştırma yapılan firmaların resmi siber güvenlik dokümantasyonları ve politikaları olup olmadığı

sorulmuştur. Buna göre şirketlerin 2016 yılında %29'unun, 2017 yılında %32'sinin ve 2018 yılında ise %28'nin siber güvenlik politikaları oldukları görülmüştür. Fakat politikalar kısmında dikkat edilmesi gereken bir nokta şirketlerin bu politikaları her yıl tekrar tekrar oluşturmadıklarıdır.

Yukarıda sözel olarak verileri bir de grafik üzerinde incelemek üzere Şekil 5.12 oluştrulmuştur.



Şekil 5.12 : Bilgi güvenliği anket verilerine göre 3 ana başlık (Yazar tarafından tasarlanmıştır).

Yapılan araştırmalar sonrasında iyi niyetli şirket çalışanlarının da siber güvenlik bilgilerindeki eksiklik nedeni ile hata yaparak şirkete gerek maddi gerek manevi ve itibar kaybı gibi büyük kayıplara neden olabileceği görülmüştür. Bu nedenle bu noktadan neler yapılabileceği ile ilgili düşünmek ve buna uygun aksiyon almak gerekmektedir.

- **Yönetim**: İnsani risklerden sorumlu bir yöneticinin olması gerekmektedir.
- **Roller ve sorumluluklar:** İnsani risklerden sorumlu yönetici belli olduktan sonra, tüm risklerin analizi, bu riskler ile ilgili roller ve sorumluluk haritası çıkartılmalıdır.
- **Risk**: Şirket yılda en az bir kere risk yönetimi ve içerinden yer alan risk analizini yapmalı, ayrıca güvenlik riski yaratabilecek çalışanlarını tespit etmek için de bir değerlendirme yapmalıdır. Yüksek risk taşıyan çalışanlar bu kapsamda bilgilendirilmelidir.

- **Kültür**: Şirket genelinde bir güvenlik kültürü ve planı çıkartıp, uzun yıllar bu plana sadık kalınmalıdır.
- **Etki**: Aslında risk analizi kısmını da biraz ilgilendiren bir konu olarak içeriden bir çalışanın siber güvenlik konusunda ki bilgisizliği nedeni ile yapacağı bir hatanın nelere neden olabileceğiniz anlaşılması ve analiz edilmesi gerekmektedir.
- **Tepki**: yönetim seviyesinde bir tepki planı olmalı ve bir hata nedeni ile oluşabilecek bir sorun karşısında en asgari zarar elde edilmesi planlanmalıdır.
- **Açıklık**: İlgili yöneticinin güvenlik konusunu tüm şeffaflığı ile çalışanlarına ve uçtan uca tüm paydaşlarına aktarması gerekmektedir.
- **Eğitim ve çalışanları sınama**: Siber güvenlik konusunda şirket çalışanlarına her dönem verilecek eğitimler ile bilgilerini taze tutmak gerekmektedir. Ayrıca bu eğitimler sonrasında yapılacak olan oltalama denemeleri ile bilgileri sınanmalıdır. Bunun yanı sıra bu sınamalara ödül koyarak konuya daha da ilgi çekilebilir.
- **Denetim**: Denetim komitesi, yıllık değerlendirme de güvenlik konusunda personelin hangi eğitimleri aldığı, risklere karşı hangi önlemler alındığı gibi konuları denetlemelidir.

Uygun politikalar ve çalışan farkındalığı ile birlikte şirket genelinde güvenlik kültürünün yayıldığı yönetimlerde içerideki siber güvenlik zaafiyetini azaltmak mümkündür. Her ne kadar siber saldırıların ve data ihlallerinin yarattığı tahribatı sıfıra indirmek mümkün olmasa da yine de en aza indirmenin yolları bulunabilmektedir.

5.3 Siber Kriz Yönetimi

CBS internet sitesinin 2015 yılı haberine göre her yıl yaklaşık 1,5 milyon siber atak meydana gelmektedir. Bu sayıyı biraz daha yakından inceleyecek olursak senelik 1,5 milyon siber atak aynı zamanda her gün 400 siber atağa, her saat 170 siber atağa hatta her bir dakika da 3 siber atağa karşılık gelmektedir. Her ne kadar az sayıda saldırı başarılı olsa da yaşanan siber atak sayısının yüksek olması, her kuruluşun etkili bir şekilde yanıt vermeye hazır olması gerektiğini göstermektedir.

Cybintsolutions [112] internet sitesinin 2018 verilerine göre ise,

- Her 39 saniye de bir siber atak meydana gelmektedir.
- Siber güvenlik ihlallerinin %95'i insan hatasından kaynaklanmaktadır.
- 2013 yılından bu yana ihlaller nedeniyle her gün 3,809,448 veri çalınmaktadır. Saniyede 44 veriye denk gelmektedir.
- 2020'de bir veri ihlalinin ortalama maliyeti 150 milyon doları aşacaktır
- Sağlık endüstrisinin %75'inden fazlası 2017-2018 yılı döneminde kötü amaçlı yazılımlarla
- 2018 yılının 2 çeyreğinde büyük ölçekli DDoS saldırıları boyut olarak %500 artış göstermiştir.

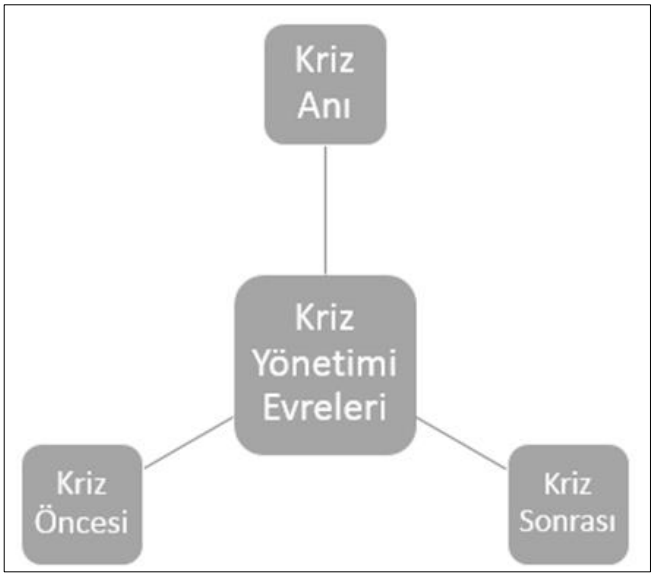
Bu ve daha bunun gibi verilebilecek birçok rapor özetinin bize gösterdiği ise siber atakların ve siber tehditlerin her geçen gün ve hatta dakika artış gösterdiği ve önlem alınmadığı takdirde sonuçlarının firma için telafi edilmez olduğundur.

Genel kriz yönetimi alanı, önleme, azaltma ve olaya tepki verme ve kurumsal öğrenme geniş spektrumunu kapsamaktadır. Ortak bir varsayım olsa da karar vermenin daha da merkezileştirilmesi, bir krizi ele almanın en etkili yolunun olmadığı, ağ modelleri veya merkezi olmayan yetkililerin genellikle hangi tepkinin en iyi şekilde çalışacağını değerlendirmede daha etkin olacağı Hart, Rosenthal ve Kouzmin tarafından belirtilmiştir [109].

Kriz yönetimi sadece bir siber olay karşısında müdahale olarak değil tamamen bir süreç olarak değerlendirilmelidir. Bu da demek oluyor ki, kriz yönetimi kriz öncesi, kriz anı ve kriz sonrası olarak 3 parçaya ayrılabilmektedir. Bunun yanı sıra etkili bir siber kriz yönetimi hazırlık, tepki ve kurtarma ve öğrenme adımlarını kapsamalıdır.

Bilgisayar acil müdahale ekipleri (CERTs) veya bilgisayar güvenliği olay müdahale ekipleri (CSIRTs) siber krizler durumunda önemli bir yere sahiptir. 1988 yılında ilk olarak Morris solucanının interneti vurması sonrasında Carnegie Mellon Üniversitesi tarafından ilk olarak geliştirilmiştir. CERTs veya CSIRTs bilgisayar güvenlik olaylarının üstesinden gelmede, zayıflıkların ve tehditlerin tespitinde ve özel güvenlik organizasyonları ile güvenlik konusunda uzman birliklerin ve kullanıcıların iş birliğini desteklemektedir [110].

Şekil 5.13'te Siber Kriz Yönetim Şemasının Genel Görümümü gösterilmektedir.



Şekil 5.13 : Siber kriz yönetim şeması genel görümümü (Yazar tarafından tasarlanmıştır).

Siber kriz yönetim evrelerini daha yakından inceleyecek olursak,

5.3.1 Kriz öncesi

Kriz öncesi evresi hazırlık evresi olarak da adlandırılabilmektedir. Hazırlık evresi sadece sistemlerin ve atakların 7/24 izlenmesi değil, bunun yanı sıra kaynaklarında bir kriz durumu için hazır olması evresidir. İyi donanıma sahip, çok fonksiyonlu bir ekibin krizin tüm yönleri ile başa çıkmak için hazır olması gerekmektedir. Buna ek olarak, kriz simülasyonu ve diğer simülasyonlar, yönetimin neler olabileceğini, hangi adımların atılacağını ve organizasyon gerçekten hazırlandığını anlamasını sağlamaktadır.

Hazırlık evresinin önemli bir kısmı, önleme ve erken uyarı sağlayabilecek sistemlere odaklanmaktadır. Bunlar, tehdit istihbaratı, güvenlik operasyonları merkezleri, olaya karşı tepki, dijital hukuksal yetenek, güvenlik bilgileri ve olay yönetimi, davranış analizi gibi geniş bir teknik yetenek portföyüyle sınırlı değildir. Yukarıda belirtilenlerin hepsi yardımcı güvenlik ve risk yönetimi kabiliyeti ile birlikte, hedef olması gereken "Durumsal Farkındalığı" ortaya çıkarması gerekmektedir.

Kısacası, durumsal farkındalık her zaman etrafınızda neler olup bittiğini bilir, böylece koşullar değiştiğinde en iyi nasıl tepkinin vereceğine karşı hazırlıklı olunmasını sağlayacaktır.

Kriz öncesi evrede 5 adım bulunmaktadır [111].

i. Siber krizleri tanımlamak ve tahmin etmek

Tehdit modelleme veya risk değerlendirmesi yoluyla organizasyon, potansiyel siber krizleri önceden belirlemelidir. Tehdit senaryoları, tahmin ettiğiniz tehditlere ek olarak, daha önce risk yönetimi bölümünde riskin ne olduğunu açıklamada kullandığımız "bilinen bilinmeyenleri" terimini tanımlamak ve en azından bunları tartışmak için de tavsiye edilir. Bu adım mutlak bir zorunluluktur, aksi takdirde tüm kriz yönetimi planlaması işareti tamamen kaçırabilir.

ii. Beyin fırtınası ve plan taslağı hazırlamak

Beyin Fırtınası ile elde edilen uygulama, çeşitli organizasyonel birimler üzerinde beklenen etkilerin ve yasal, finans, operasyonlar, satış, pazarlama, müşteri hizmetleri ve diğer iç ve dış hissedarlar arasında olası etkilerin bir analizini içermelidir. Beyin fırtınası sonucu tehdit modelleme veya risk değerlendirme aşamasında tanımlanan tehditlere neden potansiyel krizi ele entegre bir plan oluşturmak için temel olmalıdır. Ayrıca, her fonksiyonun belirlenen senaryolardan herhangi biri için hangi aşamada yapılması gerektiğini, koordinasyon ve uyum için özel vurgu yapılması gerektiğini de detaylandırmalıdır.

iii. Lideri tespit etmek ve eğitmek

Bir siber saldırı ile karşılaşılmadan önce şirket özelinde halka konuşucu bir kişi seçilmelidir. İlgili kişi olaya uçtan uca hâkim olmalı ve bir siber saldırı ile karşı karşıya kalınması durumunda halka açıklamayı bu kişi yapmalıdır. Farklı farklı bireylerden farklı yorumlar çıkmasının önüne geçilmeli ve organizasyon dışarısına verilen tek bilginin net bir şekilde bilinmesi gerekmektedir. Bir siber kriz durumunda paydaşlar ne olduğunu bilme hakkına sahiptir ve hatta bazı durumlarda tam bir açıklama yapmak için yasal zorunluluk bulunmaktadır.

iv. Sorumlu atama

Bir şirketin siber krizlere hazırlanmanın ve yanıt vermenin teknik ve teknik olmayan yönlerini denetleyen tek bir kişiye veya işleve ihtiyaç vardır. Bu kişi, bir ihlalin teknik yönlerinin, ortaya çıkabilecek 'riskler' dahil olmak üzere, tüm işletmeyi nasıl etkileyebileceğini anlamalıdır. Hazırlık ve müdahaleyi, kurumsal risk alma

bağlamında yönlendirmelidirler. Sorumlu kişi planın oluşturulmasından, değiştirilmesinden, kriz gününde uygulanmasından direkt olarak sorumlu olmalıdır.

v. Testler ve tatbikatlar

Siber yönetim takımları tarafından siber kriz durumuna karşı testler ve tatbikatlar yapılmalıdır. Eğer test ve pratik yok ise kağıt üzerindeki en iyi plan dahi pek bir işe yaramayacaktır. Güvenlik organizasyonları krize nasıl tepki vereceklerine odaklanmalı ve bu sırada da siber yönetim takımına sorunun ne olduğunu izah etmelidir. Bahsedilen test be tatbikatlar için en uygun ortam simülasyon ortamıdır. Simülasyon, kuruluşun siber yönetim planının ne kadar uygun olduğunu ve hangi koşullar altında başarısız olma ihtimalinin yüksek olduğunu değerlendirmesine yardımcı olurlar.

5.3.2 Kriz anı

Kriz anında yapılması gereken aksiyonlar aslında kriz öncesinde planlanan aksiyonların hayata geçirilmesidir. Büyük bir kriz ile karşı karşıya kalınması durumunda hazır ve koordineli tepkilerin gelmemesi durumunda para, zaman, müşteri, itibar, marka değeri gibi bir organizasyon için çok önemli olan değerler kaybedilebilir. Bu nedenle kriz anında alınacak olan aksiyonlar hayati önem taşımaktadır.

Detayları ile birlikte bu adımları inceleyecek olursak,

i. Kriz yönetim takımını toplamak

Resmi krize tepki olarak atılan ilk adım, siber yönetim takımının toplanmasıdır. Yöneticilerin bir krize tepki göstermesi gereken süre organizasyon ve paydaşları üzerindeki etkisiyle ilgilidir. Kesinleşmiş bir kriz yönetim planına veya protokolüne sahip olmak, krizin ilk birkaç saati boyunca düşünmeyi ve uygun davranmayı mümkün kılmaktadır.

ii. Kriz durumunu değerlendirmek

Kriz sürecinin tartışmasız en önemli adımı olarak bilinmektedir. Durumsal değerlendirme, kriz yönetiminin bilgi işlem ve bilgi yaratma yönlerini ifade eder. Bu adımda alınacak karar krize karşı verilecek tepkiyi, dolaylı olarak da organizasyonun maddi ve manevi kaybına doğrudan etki edecektir. Bu nedenle mümkün olduğunca çok veri ile birlikte karar verilmelidir.

iii. Durumu anlamaya çalışırken bir yandan karar vermek

Bu adımda görev atamaları yapılabilmektedir. Bir yandan da yeni bulgular elde etmeye yönelik araştırmalar devam etmelidir. Siber yönetim takımı, iç ve dış paydaşlarına verilen zararı, kuruluşun itibarını ve mal varlığını sağlayabilmek için mümkün olan her şeyi yapması önemlidir. Bu görev, tüm kriz yöneticileri için en önemli amaçtır. Ayrıca bu adımda zarar önlemek, bir krizin etkilerinin işin diğer bölümlerini yaymasını ve etkilemesini önleme çabasıdır.

iv. Çözüm alternatifleri oluşturmak

Bu aşamada uygulanabilecek olası çözümler belirlenir. Durumsal analizin tamamlanması ile birlikte krizi yönetmek için stratejiler tanımlanabilir ve uygulanabilir. Her durum için her aksiyon alınmamalıdır. Burada en önemli ve anahtar noktalardan bir tanesi esnekliktir. Bunun nedeni ise kriz durumunun çok hızlı bir şekilde değişebileceği gerçeğidir.

v. Çözümü seçmek ve uygulamak

Bu adım uygulama genellikle sürecin en zor kısmıdır. Yetkin insanlar, zaman ve para gerektirir ve yeterli kaynakların tahsis edilmesi önemlidir.

vi. Medya, müşteri ve kolluk kuvvetlerine bilgilendirme

Siber kriz durumunun ortaya çıkması ve durumun anlaşılması sonrasında gerek medya gerek iç ve dış paydaşlara bilgi verilmelidir. Ayrıca müşteri bilgiler gibi kişisel verilerinde olaya dahil olup olmadığı konusunda bilgiler verilmelidir. Gerekli ise kolluk kuvvetlerine ve ilgili yerlere de bilgi verilmelidir.

vii. İzleme ve takip etme

Siber yönetim takımı, bir kriz sorasında kilit paydaşlarının görüş ve davranışlarını izlemesinin ve onların tepkilerini anlamanın çok önemli olduğunu bilmelidir. Bunun nedeni daha önceki adımlara yapılan iletişimin başarılı olup olmadığını görmek ve ortaya çıkabilecek maddi ve manevi kayıpları takip etmektir.

viii. Son verme

Bir krizin ilk başladığı anda en büyük amaç, şirkete ve itibarına olası zararı en aza indirmektir. Fakat şu da iyi bilinmelidir ki bazı durumlarda amaç, krizle ilişkili olası olumsuzlukları organizasyon için pozitif hale getirmeye dönüşebilir. Son verme

adımında siber yönetim takımı artık siber krizin bittiğini ve kriz durumunun ortadan kalkabileceğini açıkladığı adımdır.

5.3.3 Kriz sonrası

Aslında kriz sonrası durum herhangi bir krizde olması gerektiği gibi neler yaşandığını, ne aksiyonlar alındığını, nerelerde aksaklıklar yaşandığını, neyin daha iyi yapılabileceği, hem iç hem de dış paydaşların davranış ve görüşlerini nasıl etkilediği, normal iş süreçlerinin ne oranda etkilendiği gibi soruların cevap bulduğu yerdir. Bir krize bir bütün olarak bakıldığında organizasyonun kendisini ve siber kriz yönetimini geliştirebilmek için en etkili, gerekli ve yararlı verilerin olduğu yer olarak dikkat çekmektedir.

Fakat burada unutulmaması ve atlanmaması gereken nokta değerlendirme sürecinin ancak kriz sona erdikten sonra gerçekleşen bir faaliyet olmadığıdır. Değerlendirme, kriz başladığında ve süresi boyunca devam ettiğinde başlayan bir süreçtir.

Hiçbir yönetim kurulu veya üst düzey yönetici ekibi, siber tehditlerin ciddiyetini veya olasılığını inkar edemez. Dolayısıyla, bir siber olay meydana gelmeden önce son derece etkili bir siber kriz yönetimi planı hazırlamak gerekmektedir.

5.4 Siber Güvenlik Yönetim Modelinde Organizasyon Yapısı Ve Teknolojik Yatırımların Etkisi

Siber güvenlik yönetim modeli içerisinde bulunan, organizasyon içerisindeki yapının ve teknolojik yatırımların incelendiği bu adımı iki adımda incelemek hem organizasyon şemaların siber güvenlik konusunun hayatımıza girmesi yeni eklenen güvenlik dalının ana amacının ne olduğu, bu güvenlik kırılımı altında ne konuların incelendiği, bu ekibe önderlik eden makamdaki üst düzey yöneticinin neler kazandırabileceği gibi konuları anlamamıza hem de bu yönetim ekibinin almış olduğu siber güvenlik yatırım kararlarını konusunu anlamamıza kolaylık sağlayacaktır.

5.4.1 Siber güvenlik organizasyon yapısı

Daha önce de birçok kez bahsedildiği üzere siber güvenlik konusu sadece teknolojik yaklaşım ile çözülebilecek bir konu değildir. Her ne kadar hayatımızda olan siber güvenlik konusu bir süredir konuşuluyor, araştırılıyor ve etkileri açık açık görülüyor olsa da organizasyonların adapte olabilmeleri için halen yeni sayılabilecek bir

başlıktır. En azından organizasyonel yapı itibariyle yeni bir oluşum gerektirmektedir denilebilir. Yaşanan siber olaylar ve sonrasındaki etkileri artık çok açık bir şekilde gözler önüne serilmiş olması sayesinde organizasyonlar siber güvenlik konusuna biraz daha eğilmiş ve siber güvenlik konusunda organizasyon şemalarını her geçen gün düzenlemektedirler.

Organizasyon şeması asla sabit kalacak bir şema değildir. Organizasyonların değişiklikleri ve yenilikleri takip edip bu yönde aksiyon alabilmeleri için, bu yenilikleri yönetecek ve operasyon ekiplerini takip edecek bir yönetim kadrosuna gerek vardır. Tıpkı siber güvenlik konusundaki konularda son dönemdeki gelişmelerde olduğu gibi de 2018-2019 yılı itibariyle de sanallaştırma konuları çok revaçta olup, firmalar organizasyon yapılarını buna göre değiştirmekte, ilgili operasyon takımları kurmakta, yöneticiler ve üst düzey yöneticiler belirlemektedir.

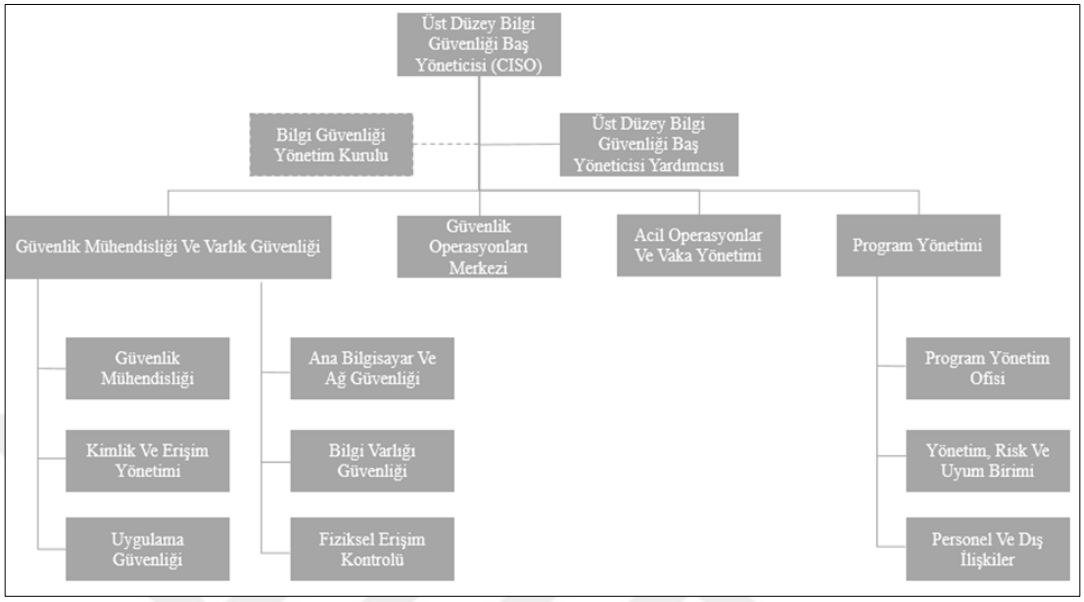
Araştırmamızın konusu olan siber güvenlik konusu özelinde organizasyon yapılarına yeni eklenen dalları inceleyecek olursak, halihazırda olan yönetim şemalarına kısaltması CISO, İngilizcesi Chief Information Security Officer ve Türkçe karşılığı da Bilgi Güvenliği Baş Yöneticisi olan kavramın girdiğini görmekteyiz. Burada dikkat edilmesi gereken nokta organizasyonun büyüklüğüne, organizasyon içerisindeki görev dağılımına ve isimlendirmesine göre bilgi güvenliği baş yöneticisi farklı bir isim ile de anılabilmektedir.

Siber tehditlerin dinamik ve gelişen doğası göz önüne alındığında, kıdemli bir siber lider olarak etkili olmanın anahtarı güvenilirliği oluşturmak ve sürdürmektir. Potansiyel siber liderin görevleri arasında, kilit paydaşların gözünde güvenilirliği oluşturma ve sürdürme rolleri vardır.

GlaxoSmithKline firmasının BGBY'si Robert Coles'a göre bilgi güvenliği baş yöneticisinin en temel görevi kilit paydaşları siber güvenliğe yönelik tehditlerin bir şekilde kabul edilebilir bir risk olarak görülmemesi gerektiği konusunda ikna etmektir [113].

Bilgi güvenliği dergisinin editörü Kathleen Richards bilgi güvenliği baş yöneticisi pozisyonunun an itibariyle 1000 veya daha fazla çalışanı olan firmalarda olduğunu söylemektedir. Aynı zamanda Richards, pazar araştırmacısı Gartner'in sonuçlarına dayanarak 150 veya üzeri çalışana sahip firmaların bünyelerinde bir bilgi güvenliği baş yöneticisinin çalışması önermektedir [114].

Bilgi güvenliği baş yöneticisi konusu Carnegie Mellon Üniversitesinin yazılım mühendisliği enstitüsü tarafından ele alınmış ve BGBY'nin organizasyon içerisinde Şekil 5.14'de gösterildiği gibi dallanması olması gerektiği belirtilmiştir.



Şekil 5.14 : Bilgi güvenliği baş yöneticisi organizasyon şeması [115].

Carnegie Mellon Üniversitesi tarafından Şekil 5.14'de belirtilen organizasyon şemasını daha iyi anlayabilmek için organizasyon şemasında bulunan alt başlıkları biraz daha yakından incelemek gerekmektedir.

5.4.1.1 Program yönetimi

Program yönetimi, program yönetim ofisi, yönetim risk ve uyum, personel ve dış ilişkiler üçlüsünden oluşmaktadır.

Program Yönetim Ofisi, bir bilgi güvenliği planını ve bu plana dayanan programı geliştirmek ve başarılı bir şekilde uygulamak için gerekli tüm faaliyetleri yerine getirir. Program yönetim ofisinin bazı görevlerine ve aktivitelerine örnek olarak [115],

- Bir bilgi güvenliği programı, planı ve süreçleri için bütçe ayarlama ve bu bütçeyi yönetmek aynı zamanda da geliştirmek, uygulamak ve sürdürmek
- Bilgi güvenliği rollerini ve sorumluluklarını tanımlayın
- Bilgi güvenliği programını ve planını uygulamak için yeterince eğitimli, yetenekli kaynakları tahsis etmek

- Tüm iç ve dış paydaşlarla iletişim kurun ve (gerektiği şekilde) rapor verilmesi verilebilmektedir.

Yönetim, Risk ve Uyum birimi, uygun gözetim, risk yönetimi ve kuruluşun uyması gereken yasal, düzenleyici, politika ve diğer bilgi güvenliği ile ilgili gerekliliklere uyumu sağlamak için gereken tüm faaliyetleri yerine getirir. Bu adımın bazı göre ve aktivitelerine örnek olarak [115],

- Bilgi güvenliği programı ve planı: bilgi güvenliği politikalarını tanımlanması, uygulanması
- Risk yönetimi sürecinin takip edilmesi

Personel ve Dış İlişkiler siber güvenlik sürecinde yer ala tüm iç ve dış paydaşların yönetimi ile ilgilenir. Bu adımın bazı göre ve aktivitelerine örnek olarak [115],

- Üçüncü parti ve dış paydaşlar ile ilişkiyi yönetme,
- Bilgi güvenliği ekibinin bilgi, beceri, yetenek ve kullanılabilirliğini yönetme,
- Kurum çapında, rol tabanlı bilgi güvenliği farkındalığı ve eğitim programı uygulamak verilebilmektedir.

5.4.1.2 Güvenlik operasyon merkezi

Güvenlik operasyon merkezi tüm sistemi uçtan uca izleyerek karşılaşılması olası siber atakları veya organizasyon içerisinden yapılması mümkün olan insan ihlallerine karşı izleme ve önlem alma merkezidir. Güvenlik operasyon merkezler, güvenlik açıklarını, virüsleri ve kötü amaçlı kodları yönetme, güvenlik olaylarını yönetmek, kurumun bilgi güvenliğine yönelik tehditleri analiz etmek ve yönetmek ve günlük kaydı yapmak gibi görevleri üstlenmektedir.

5.4.1.3 Acil durum operasyonları ve vaka yönetimi

Bu birimin temel sorumluluğu, personelin harekete geçirilmesi, müdahale planlarının etkinleştirilmesi ve çok etkili bir olay ilan edildiğinde zaman kritik olay yönetimi ve müdahale faaliyetlerinin yönetilmesidir.

5.4.1.4 Güvenlik mühendisliği ve varlık güvenliği

Birçok departmanı bünyesinde bulunduran güvenlik mühendisliği ve varlık güvenliği biriminin temelde güvenli mühendisliği ile varlık güvenliği başlıklarını aynı çatı

altında toplanmasındaki ana motivasyon, varlık güvenliğinin sağlanması için yapılan güvenlik mühendisliği sırasında meydana gelen gelişmeler ile bunun gerçekleşmesi için ortaya çıkan güvenlik faaliyetleri arasında daha fazla iş birliğini oraya çıkarmaktır.

Güvenlik mühendisliği ve varlık güvenliği birimi çatısında bulunan diğer birimleri kısaca açıklayacak olursak,

Güvenlik mühendisliği departmanı, kurumsal güvenlik mimarisinin geliştirilmesi ve sürdürülmesi, yeni sistemleri ve yazılımların canlıya alınmasından önce sertifikasyon ve akreditasyon süreçlerinin geliştirilmesi gibi konular ile,

Kimlik ve erişim yönetimi, nesneleri ve diğer varlıkları (bilgi, teknoloji ve tesisler) temsil eden kimlikleri tanımlamaktan ve yönetmekten sorumludur. Bu departman aynı zamanda kimlikleri ve erişim kontrollerini tanımlamaktan ve uygulamaktan sorumludur.

Ana Bilgisayar ve Ağ Güvenliği, internet alanındaki güvenlik gereksinimlerine göre güvenlik duvarları ve VPN gibi teknolojileri ile kullanarak güvenliği sağlamaktır. Bunun yanı sıra ağ içerisindeki gerekli kurulumlar ile de ilgili bir departmandır.

Bilgi varlığı güvenliği departmanı, bilgi ve hayati varlıkları belirlemek, önceliklendirme ve kategorilere ayırmak için var olan bir departmandır.

Fiziksel Erişim Kontrolü, tesisler, ağlar ve ana bilgisayarlar gibi diğer fiziksel varlıklara fiziksel erişim için dijital ve elektronik erişim kontrollerini sağlamaktadır.

Son olarak Bilgi Güvenliği Yürütme Kurulu (ISEC), Bilgi güvenliği baş yöneticisine tavsiyelerde bulunmaktan ve tüm bilgi güvenliği amaç ve gereksinimlerinin karşılandığından emin olmaktan sorumludur.

Son dönemde siber güvenlik konusu ile ilgili oluşturulan organizasyon şemaları incelendiğinde aslında tıpkı Carnegie Mellon Üniversitesi tarafından hazırlanmış olan Şekil 5.14'deki bilgi güvenliği baş yöneticisi şeması ile bu organizasyon yapılarının örtüştüğü görülmektedir. Carnegie Mellon Üniversitesi tarafından hazırlanan organizasyon şemasının bir yanda doğruluğunu ve gerçek organizasyonlarda kullanılabilirliğine bir örnek olarak Şekil 5.15'de görülen ve dünyanın en büyük yönetim danışmanlığı firmalarından biri olan McKinsey & Company tarafından hazırlanan yönetim şemasına göre de siber güvenlik söz konusu olduğundan

organizasyon şeması içerisinden bir CISO yani bilgi güvenliği baş yöneticisi bulunması çok kritik bir durumdur.

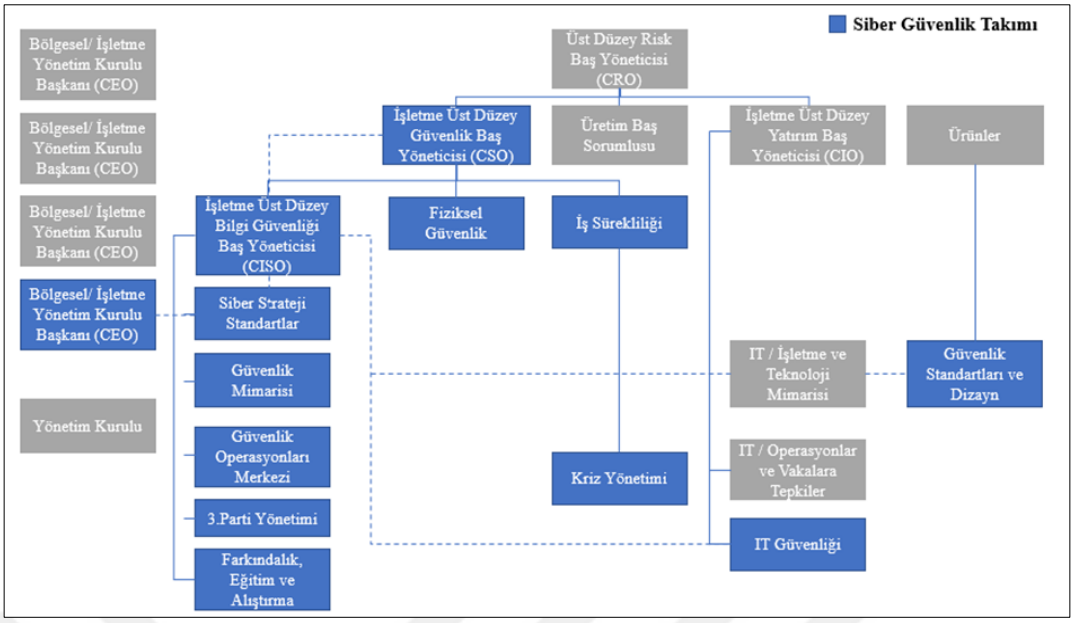
McKinsey & Company şirketi tarafından Mart 2018 yılında yayınlanan organizasyon yapısına göre siber güvenlik takımı olarak tanımlanan üst düzey yöneticiler, ekipler ve olgular mavi ile işaretlenmiştir. Buradan da açıkça görüleceği üzere CSO yani baş güvenlik yöneticisi altında bulunan bilgi güvenliği baş yöneticisi altına tüm siber operasyonlar yerleştirilmiştir.

Daha önce de dile getirildiği üzere şirketler özelinde hangi birimin hangi birim ile birebir bağlantısı olması gerektiği, hangi departman yöneticisinin kime raporlayacağı veya yönetim kurulunun kimler tarafından oluşturulacağı, şirketten şirkete değişmektedir. Burada etkili olan noktalar daha önce de belirtilmiştir.

Örnek olarak baktığımız McKinsey & Company şirketi tarafından hazırlanan organizasyon yapısında, genel bir baş yönetici (CEO), baş risk yöneticisi (COO) ve baş güvenlik yöneticisi (CSO) ile daha yakın çalışırken, bilgi güvenliği baş yöneticisi (CISO) daha çok baş güvenlik yöneticisi (CSO) ile iç içe çalışmaktadır. Bazı firmalarda bilgi güvenliği baş yöneticisi (CISO) direkt olarak baş yönetici (CEO) ile birebir de çalışabilmektedir. Bu tamamen organizasyonun değişkenlerine ve yapısına kalmış bir karardır.

Son olarak toparlayacak olursak, 113 bilgi güvenliği baş yöneticisi arasında yapılan araştırma ve ankete göre, siber tehditle ilgili konularla uğraşmaya gelince, işteki en iyi günleri sorulduğunda,

- Sistem güvenli açıklanın belirlenmesi (%19)
- Siber suçun durdurulması (%32)
- Bir siber olayın çözülmesi (%32)
- Çalışanların riskten uzak tutulması (%5)
- Güvenlik ile ilgili finansman elde edilmesi (%3)
- Siber güvenlik konusunda eğitimli yönetim ve kurulu (%3) gibi cevaplar vermişlerdir [114].



Şekil 5.15 : Mckinsey & Company Şirketine Göre Siber Güvenlik Organizasyon Yapısı [116].

CISO'nun rolü veya pozisyonu hala şekillenirken, etkili olması için kullanabileceği uygulamalar hakkında birkaç şey netleşirken, IBM Applied Insights Center tarafından yayınlanan yeni bir raporda, CISO'nun şirkete değer katması için birkaç yol olduğu belirtilmiştir [113].

- Siber tehditlere özel önem vererek kurumsal risk yönetimi etrafında güçlü bir stratejinin geliştirilmesine katkıda bulunmak
- Kapsamlı bir risk yönetimi platformu geliştirmek
- İhtiyaçlarını, sorunlarını ve kaygılarını anlayarak operasyon yöneticileri ile etkili ilişkiler kurmak
- Çevresindeki yaygın, sürekli ve etkili iletişim uygulamalarını sergilemek

5.4.2 Siber güvenlik yatırımları

Birçok konuda olduğu gibi başarının sırrı yatırım yapmaktadır. Nasıl ki bir üniversite öğrencisi ileride bir bilim insanı olabilmesi için daha ilkokul yıllarında kendisini geliştirmeye ve çok çalışmaya ihtiyacı var ise, yine aynı şekilde bir sporcunun da ileride iyi yerlere gelmesi ve başarılı olması için küçük yaşlardan başlayarak uyku düzenine, yeme içmesine dikkat etmesi ve yoğun bir antrenman programı ile kendisini diğerlerinden bir adım öne geçirecek aksiyonlar alması gerekmektedir. Bilim insanı olmak isteyin kişinin de sporcu olmak isteyen kişinin de yaptığı, kendisine yatırım

yapmaktır. Verilen örnekler çoğaltılabilir fakat varılmak istenen nokta her zaman şu olacaktır ki eğer başarı elde edilmek isteniyor ise yatırım yapmak çok önemli bir kavramdır.

Siber güvenlik çerçevesinden konuyu ele alacak olursak, bilindiği üzere siber saldırı sayısının artmasıyla birlikte, kuruluşlar ciddi kayıplarla karşılaşabilir bu kayıplar maddi kayıplar olabileceği gibi aynı zamanda da marka değerlerinde ki düşüş de olabilir. Bu nedenle organizasyonlar güvenliklerine, ne kadar yatırım yapmaları gerektiği ve hangi önlemlere yatırım yapmaları gerektiği konusunda düşünmeye ihtiyaç duyabilir. Organizasyonalar içeriden bulunan ve siber güvenlikten sorumlu olan üst düzey yöneticiler ve müdürler gerek kendi organizasyonlarının gerek ise başka organizasyonların başlarına gelen siber saldırılar ve bu siber saldırıların neden oldukları kayıplar nedeni ile daha büyük bir farkındalığa sahiptirler.

2018 yılında yapılan küresel bilgi güvenliği araştırmasında, yönetim kurulu üyelerinin ve C düzeyindeki yöneticilerin neredeyse yüzde 89'si şirketlerinin siber güvenlik fonksiyonlarının organizasyonun ihtiyaçlarını ile tam olarak karşıladığını inanmadıklarını belirtmiştir [117].

Literatürün önde gelen bakış açılarından biri, yatırımlarla ilgili kararların kapsamlı bir maliyet-fayda analizine dayanılarak yapılması ve kuruluşların parasal değerde en büyük zarara neden olan saldırılara ve olaylara dayanarak kararlar alınmasıdır. Ancak Rowe ve Gallaher'in belirttiği gibi birçok kuruluş, maliyetler, faydalar ve saldırı olasılığı hakkında mevcut verilerin olmaması nedeniyle bu sofistike finansal analizi yapamamaktadırlar [118].

Güvenlik yatırımlarının en uygun seviyesi yatırımın verimliliğine bağlıdır. Bu nedenle maliyetler yatırımlardan gelen güvenlik getirilerinden daha düşük olmalıdır. Bununla birlikte, birden fazla değişken, en uygun güvenlik seviyesini belirlemeyi de en uygun yatırım seviyesini belirlemeyi zorlaştırır. Bu durumda düşük veya çok yüksek yatırıma yapılmasına neden olur. Böyle bir durumda da en uygun seviye yatırımdan bahsetmek mümkün olmayacaktır.

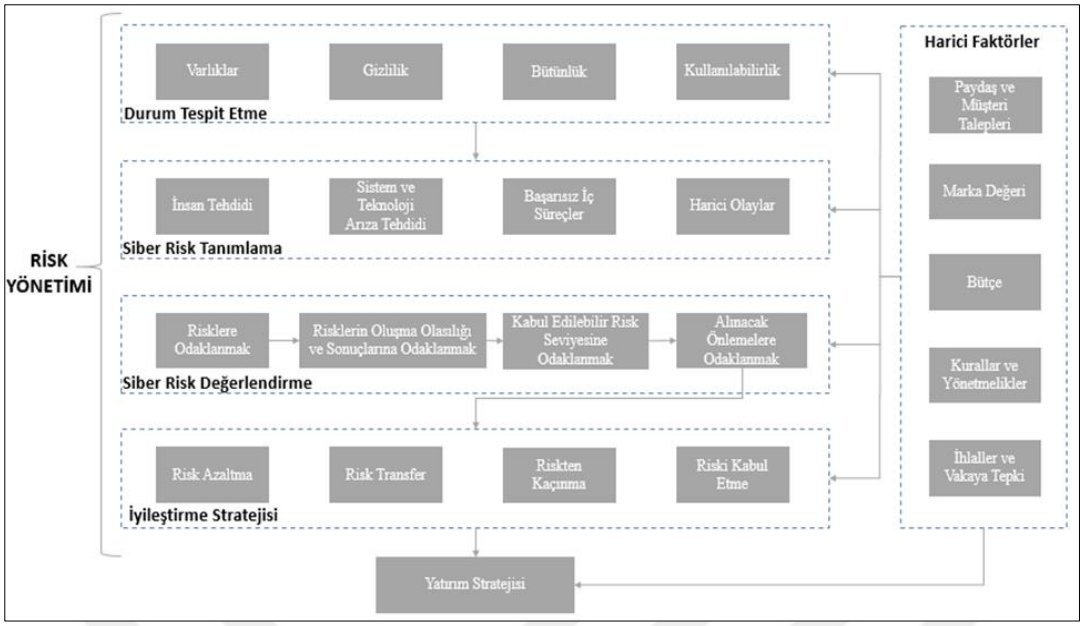
Siber güvenlik yatırımlarında karar vermenin belirsizliğini ve karmaşıklığını bir şekilde ele almak için birçok kuruluş, risklerin ve risk yönetiminin artan önemini kabul etmektedir. Bu nedenle de eğer etkili bir siber güvenlik yönetim modelinden bahsediyorsak, daha önce detaylı bir şekilde açıklandığı üzere risk yönetimi konusunu

dışarda tutmak mümkün değildir ki bu konu siber güvenlik yatırım konusu ile de ilişkilidir. Fakat burada bahsedilen risk yönetiminin daha önce açıklandığı üzere 5 adımdan oluşmalıdır. Bunun nedeni basit bir risk yönetimi modelinin sadece riskin oluşma olasılığını ve bu riskin oluşturabileceği zararı hesaplamasıdır. Fakat daha öncede belirtildiği gibi en önemli nokta etkili bir yatırım yapabilmektir. Bu da risklerin sınıflandırılması önceliklendirilmesi ve süreci baştan başa izleme ve gözlemlemenin de bir parçası olduğu risk yönetimi ile olabilir.

Risk yönetimini teoride planlamak kolaydır fakat nispeten pratikte daha zordur. Standart maliyet-fayda hesaplamaları yapmak neredeyse imkansızdır. Dolayısıyla, karar verme sürecini göz önünde bulundurarak organizasyonların diğer faktörlerden de etkilenmesi beklenmektedir. Kuruluşlar risk yönetimi sürecinin tamamını ele alarak bir yönetim şeması oluşturabileceği gibi sadece küçük bir kısmını gerçekleştirebilir veya sadece birkaç riske odaklanabilir.

Şekil 5.16, teorik olarak kolay olan siber güvenliğe ilişkin karar alma sürecinin pratikte nasıl görünebileceğini ve bu yatırım stratejisini etkileyebilecek tüm unsurların içeriklerini göstermektedir. Bu çerçeve küresel bilgi güvenliği anketi veri setinden analize dahil edilecek olan değişkenleri seçmek için kullanılmaktadır.

Daha önce de belirtildiği gibi kuruluşlar risk yönetimi sürecinin tamamını ele alarak bir yönetim şeması oluşturabileceği gibi sadece küçük bir kısmını gerçekleştirebilir veya sadece birkaç riske odaklanabilir. Bu duruma örnek vermek gerekirse, sabit bir bütçeyle ağır kısıtlanmış, tüm risk yönetim sürecini yerine getirmeyen organizasyonlar buna örnek verilebilir ve bu organizasyonlar sadece zayıflıkları, güvenlik açıklıklarını kapsayabilir. Bunun yanı sıra sadece kurallara ve yönetmeliklere uymak için siber güvenliklerine yatırım yapan kuruluşlar, müşterilerinin paydaşlarının isteklerini yerine getirmek için siber güvenlik konusunda yatırım yapanlar, itibar kaybı korkusu ile siber güvenlik yatırımı yapanlar veya sırf rakiplerinin yapmış olduğu siber güvenlik yatırımlarından geri kalmamak için aynı siber güvenlik yatırımını yapan firmalar buna örnek verilebilir. Bu örneklerden de açıkça görülebileceği üzere her firmanın aynı seviyede bir ve aynı sebepten ötürü siber güvenlik yatırımı yapmasını bekleyemez.

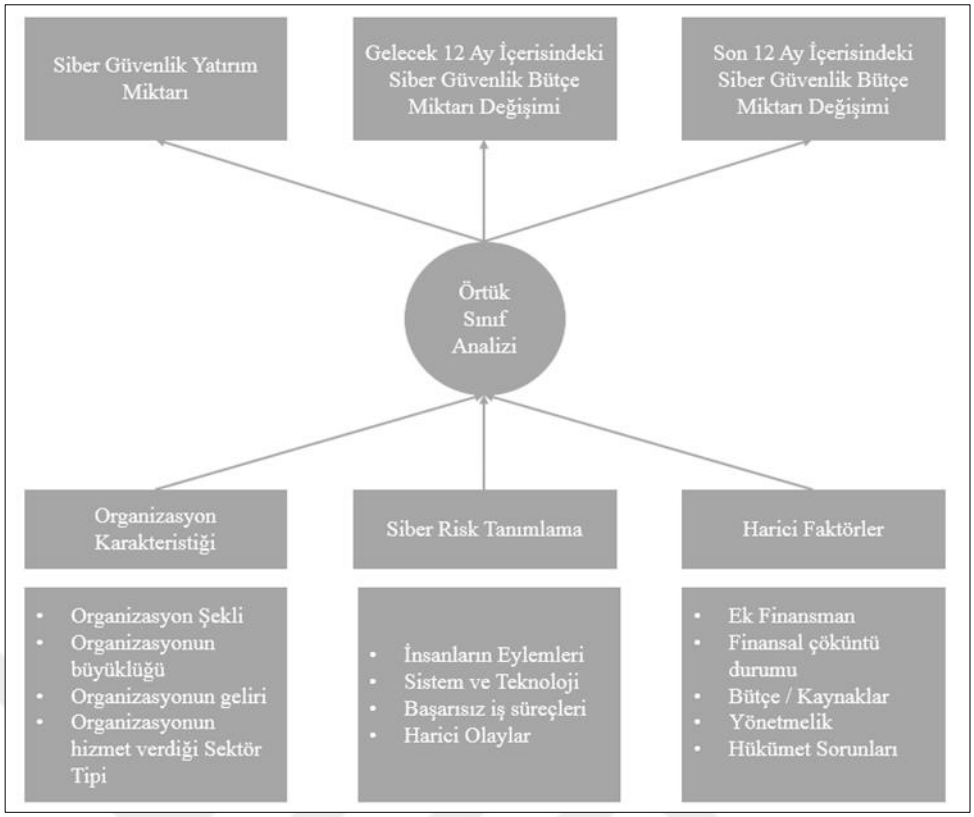


Şekil 5.16 : Siber güvenlik yatırımları için karar verme süreci [119].

Kuruluşların farklı yatırım davranışlarına sahip olup olmadığını değerlendirebilmek için örtük sınıf analizi en etkili yöntemlerden bir tanesidir. Örtük sınıf analizi göstergeler, gizli sınıflar ve değişkenlerden oluşur. Risk yönetimi sürecine dayanarak, yatırım davranışı üzerinde önemli etkiye sahip olabilecek beş farklı kategori modele dahil edilebilir. Bu kategoriler daha önce risk yönetim adımında da anlatıldığı gibi, durum oluşturulması, risklerin tanımlanması, risk değerlendirmesi, risklerin tedavi stratejisi ve dış faktörlerdir. Ayrıca, organizasyonun büyüklüğü, yıllık toplam geliri ve organizasyonun endüstri türü gibi örgütsel özelliklerin yatırım davranışı üzerinde önemli bir etkiye sahip olabileceği beklenmektedir [119].

Şekil 5.17'de örnek bir örtük sınıf analizi gösterilmektedir.

Şekil 5.17'de görülen olan örnek örtük sınıf analizi, siber güvenlik konusunda kullanılmak üzere küresel bilgi güvenliği araştırmasındaki veri setindeki değişkenlere dayanarak hazırlanmıştır. Bu değişkenler organizasyonun karakteristiği, siber risk tanımlama ve dış faktörlerdir. Diğer boyutlar küresel bilgi güvenliği araştırması veri setinde ele alınmamıştır. Göstergeler, veri kümesindeki farklı kümeleri ayırmak için kullanılır. Amaç, siber güvenlik alanındaki yatırım stratejisindeki farklı davranışları ayırt etmektir. Bu nedenle yatırım tutarı, önceki 12 aydaki yatırım değişimi ve gelecek 12 aydaki yatırım değişimi gösterge olarak kullanılmıştır.



Şekil 5.17 : Örnek bir örtük sınıf analizi [119].

Amaç aynı zamanda birden fazla ihtimal ortaya çıkararak organizasyon için en uygun siber güvenlik yatırım stratejisini belirlemektedir. Yukarıdaki değişken ve göstergelerden elde edilecek verilerin analizinde kullanılacak birçok method mevcuttur [119].

Organizasyonların ne kadar hızlı bir şekilde yapı değiştirdiği, teknolojideki gelişmelere göre kendi yapılarını bu değişime uydurarak gündemi takip etmeleri gerektiği çok aşikardır. Bu nedenle de organizasyonlar tarafından verilen yatırım kararları da bir o kadar önemli bir konumdadır. Organizasyon şemasına yeni katılan CISO yani bilgi güvenliği baş yöneticisi pozisyonunun yönetim kurulu içerinde yer alması veya CSO yani baş güvenlik yöneticisine organizasyonun siber güvenlik koruması konusunda ne durumda olduğunu ne yatırımlar yapılması gerektiği ile sunacağı etkili bir rapor bu konuda alınacak bir bütçeye ve bu da doğal olarak daha gelişmiş bir siber güvenlik koruma sistemine dönüşecektir.

5.5 Türkiye'nin Siber Güvenlik Stratejisinin İncelenmesi ve Yasal Mevzuat

5.5.1 Genel bakış

Dünya üzerindeki her ülkenin başına gelebileceği gibi Türkiye'nin de başına çok sayıda siber saldırı gelmiştir. Bu saldırıları kimi zamana devlet kurumları özelinde gerçekleşmiş, kimi zaman ise Türkiye'de hizmet veren özel kuruluşlara karşı yapılmıştır. Özel ve devlet fark etmeksizin tüm bu siber saldırılar günün sonunda Türkiye Cumhuriyetin de yaşayan vatandaşları etkilemiştir. Örneğin, Türkiye'nin 14 ve 24 Aralık 2015 tarihlerinde 6 ayrı "DNS Sunucusu" hedef alınarak yapılan DDoS saldırıları sonrasında sunucular isteklere cevap veremez hale gelmiş, "edu.tr", "gov.tr" ve "com.tr" gibi "tr" uzantılı 400 bin siteye 1 hafta boyunca ya hiç girilememiş ya da sitelere girişlerde sorunlar yaşanmıştır. Bunun yanı sıra HSBC Türkiye'ye yapılan siber saldırı sonrasında 2,7 milyon kullanıcının kart bilgileri çalışmış idi [120]. Ayrıca dünyaca ünlü bilgisayar korsanı topluluğu tarafından yapılan bir siber saldırıda birçok devlet kurumu internet sayfası erişilemez hale gelmiştir [121]. Her ne kadar herhangi bir bilgisayar korsanı tarafından üstlenilmese de Türkiye de 50 milyon vatandaşın kimlik bilgileri sızdırılmıştır [122].

20 Ekim 2012' de Resmi Gazete de yayınlanmasının ardından "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının" hazırlanarak yürürlüğe girmesiyle Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumluluğuna verilmiştir. 2013-2014 eylem planının ardından da UDHB 2016-2019 Ulusal Siber Güvenlik Stratejisi raporunu yayınlamıştır. İlgili sorumluluk UDHB'na verilmeden önce, siber suçlar ile mücadele konusunda Bilim, Sanayi ve Teknoloji bakanlığının önderliğinde ve koordinatörlüğünde Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK) tarafından yürütülmekte idi.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı [123];

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik

stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına,

Yönelik bir altyapı oluşturmaktır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacına ulaşmak için oluşturduğu 29 adımlı eylem planı incelendiğinde aşağıdaki 16 bulgunun ön plana çıktığı ve hedeflendiği görülmüştür.

1. Siber Güvenlik Konusunda bir kurul oluşturularak olayların tek bir merkezden yönetilmesini ve takip edilmesini kolaylaştırılması sağlanmaya çalışılmıştır.
2. Siber güvenlik konusunda yürürlükte bulunan yasal düzenlemelerin güncellenmesi eksik kısımlar var ise düzeltilmesi ile ilgili mevzuat çalışmalarının yapılması sağlanmaktadır.
3. Siber bir saldırı ile karşı kaşıya kalınması durumunda olay sonrasında incelenmek üzere delillerin toplanması, ileride yaşanacak olası saldırılar için birer ön analiz ve siber güvenlik politikasının eksiklerini görmesi ve geliştirilmesi için bir fırsattır.
4. Ulusal siber olaylarla mücadele merkezi oluşturarak (USOM), 7 gün 24 saat gerek özel gerek ise kamu özelinde oluşabilecek bir siber saldırı karşısında her an tetikte olmak ve bu sayede de kritik alt yapıların korunmasını sağlamaktadır.
5. Kritik alt yapıların belirlenerek ve risk analizleri yapılarak bir siber saldırı anından toplumum düzenini bozabilecek kritik alt yapı sorunlarının önceden önlemini almaktır.
6. Kamu ile ilgili oluşturulacak bir bilgi güvenliği programı ile, kamu özelinde yıllık güvenlik testlerinin yapılması sağlanmalı ve tespit edilen açıkların ivedilikle kapatılması fırsatı sağlanacaktır.
7. Siber güvenlik konusunda personele periyodik eğitimler vererek, farkındalık ve sorumluluk konularında gelişme sağlamaktır.
8. Yıllık veya dönemlik siber güvenlik testlerinin yanı sıra siber güvenlik tatbikatları sayesinde teorik olarak düzeltilen açıkların pratikte de işe yarayıp yaramadığı görülmesi sağlanacaktır.
9. Kritik altyapılar için güvenli yazılımlar üretilmesi sağlanmalıdır.

10. Yıllık siber istatistikler kullanarak tehditlerin tespit edilmesi izlenmesi ve gerekli ise önlenmesi sağlanmalıdır.
11. Kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren tam iş birliği yapılır.
12. Veri yedekliliği sağlanarak sayesinde veri kaybının önüne geçilmesi sağlanmalıdır.
13. Güvenli veri merkezleri kurulması gerekmekte ve kamu internet sayfaları bu veri merkezine taşınmalıdır.
14. Kamu da sorumlulukları belirleyerek erişim seviyelerinin paralelinde de belirlenmesi ile hiyerarşik bir düzen oluşturulması gerekmektedir.
15. Üniversitelerde siber güvenlik eğitimi ile ilgili eğitimlerin, yerli üretimin ve Ar-Ge faaliyetlerinin teşvik edilmesi ve siber konusunda uzman bireyler ve akademisyenler yetiştirilmesi gerekmektedir.
16. Ulusal ve uluslararası konferans, toplantı, seminer vb gerçekleştirerek veya katılım sağlayarak güncel konuların takip edilmesi gerekmektedir.

2016-2019 Ulusal Siber Güvenlik Stratejisi raporunda Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planından farklı olarak birkaç noktaya daha vurgu yapıldığı dikkat çekmektedir.

2016-2019 Ulusal Siber Güvenlik Stratejisi raporunda, her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması sağlanarak, merkezi bir kontrolün kontrolünün yanı sıra her kurumun önce kendisini kontrol etmesi sağlanarak en az iki aşamadan geçmesi amaçlanmaktadır. Bu durum bir yandan da merkezi otorite üzerindeki yükün azalmasını sağlayacaktır. Siber güvenlik ekosistemi içerinden iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması ile birlikte bir neyi birlikten kuvvet doğurarak, eksik olan kurumların eksiklerini diğer kurumlardan alacağı yardım ve tecrübe ile giderebilmesi amaçlanmaktadır. Son olarak internet protokolünün 4. Sürümünün (IPv4) internet dünyasına yeterli gelmemesi nedeniyle oluşturulan yeni 6. Sürüm ile ilgili olarak IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması vurgulanmıştır.

2016- 2019 Ulusal Siber Güvenlik Stratejisindeki 5 stratejik eylem altında 18 amaç ve ilke incelenecek olursa, stratejinin amacı ve daha önce siber güvenlik yönetim modeli

şemasında tek tek anlatılan alt başlıklar ile nasıl eşleştiğinin analizini aşağıdaki gibi yapabiliriz.

1. Kritik altyapılara ait envanter kayıtlarının oluşturulması ve güvenlik gereksinimlerinin karşılanması ile birlikte risk yönetim şemasının Şekil 5.6'da gösterilen 1. Adımının, durumun belirlenmesi adımının, yerine getirildiği görülmüştür.
2. Siber güvenlik alanında uluslararası standartlara uygun bir mevzuat oluşturmak ve bu mevzuatın denetim adımını da içermesi ile siber güvenlik üzerine insan etkisi başlığından bahsettiğimiz denetim mekanizmasının yerine getirmiş olduğu görülmüştür.
3. Kurumların sadece saldırı değil, kullanıcı hatalarına da dikkat etmesi gerektiğinin belirtilmesi ile güvenlik kültürü yani siber güvenlikte insan etkisi adımının yerine getirildiği ve daha önce dünya üzerinden siber güvenlik konusuna yön veren büyük siber saldırılar ve atakların analizinin dikkate alındığı görülmüştür. Bunun yanı sıra risk analizi adımında bahsedilen siber tehdit başlığının da dikkate alındığı görülmektedir.
4. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması ile birlikte siber güvenlik yönetim modeli üzerinde organizasyon yönetiminin dikkate alındığı ve bu adımın yerine getirildiği görülmüştür.
5. Siber güvenlik ile ilgili kurumların yöneticilerinin farkındalığının geliştirilmesi, yetkin personel yetiştirilmesi için gerek üniversite gerek devlet kurumu özelinde programlar oluşturulması gibi konular ile yine siber güvenlik yönetim modeli üzerindeki insan etkisi ve organizasyon yönetiminin dikkate alındığı görülmektedir.
6. Kamu kurumlarında siber güvenlik alanında uzman personel istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi ile birlikte siber güvenlik yönetim modeli üzerinde teknolojik yatırımların ne kadar önemli olduğu dikkate alınmıştır.
7. Yine aynı şekilde IPV6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması ile birlikte siber güvenlik yönetim modeli üzerinde teknolojik yatırımların ne kadar önemli olduğu dikkate alınmıştır. Aynı zamanda da IPv6 ile risklerin azalacağı da bir yandan düşünüldüğünden aynı

zamanda siber güvenlik konusunda risk analizinin de önemi bir yandan dikkate alınmıştır.

2016- 2019 Ulusal Siber Güvenlik Stratejisindeki amaçlar ve ilkelerin incelenmesi ile elde edilen 7 adımın içerisinde siber güvenlikte kanuni düzenlemeler ve yasal mevzuat ile siber güvenlik kriz yönetimi konularının diğer konular kadar vurgulanmadığı dikkat çekmektedir. Fakat burada belirtilmesi gerek nokta, oluşturulan siber güvenlik yönetim modelinin özel sektördeki bir firma gözünden bakıldığında kanuni düzenlemeler ve yasal mevzuat başlığına ihtiyaç duymasıdır. İncelenen ulusal siber güvenlik stratejileri halihazırda Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından oluşturulduğundan, kanuni düzenlemeler ve yasal mevzuat her daim göz önüne alınmaktadır. Bu nedenle bu bir eksik olarak görülmemelidir. Fakat ulusal siber güvenlik stratejisinde son dönemde gerek özel gerekse devlet nezdinde daha da ön plana çıkan siber güvenlik kriz yönetiminin yayınlanacak bir güncelleme veya bir sonraki ulusal siber güvenlik stratejisinde yer alması gerekmektedir.

5.5.1.1 Sorumlu kurumlar ve düzenleyici ve denetleyici kurumlar

Türkiye'deki kurumların hizmet sunumlarında bilgi ve iletişim hizmetlerini her geçen gün daha fazla kullanılması, bilgi ve iletişim sektöründeki bu gelişmelerin ilerleyen dönemlerde hayatımızın ne kadar çok içerisinde var olacağının fark edilmesi, söz konusu bilgi ve iletişim sistemlerinin güvenliklerinin sağlanması gerek siber güvenlik konusunda ülke güvenliği gerek ise yine diğer ülkeler ile rekabet edebilme konusunda yeni bir boyut haline gelmiştir.

Daha önce de belirtildiği üzere Türkiye'nin bilgi ve iletişim, siber uzay konusundaki farkındalığı ile birlikte 11 Haziran 2012 tarihli 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 20 Ekim 2012 tarihinde 28477 sayılı Resmi Gazetede yayınlanmıştır [123]. Bunun yanı sıra yine aynı Bakanlar Kurulu ile birlikte siber güvenlik ile ilgili olan tüm eylem planı hazırlanması, strateji geliştirmesi ve politikalar oluşturulması görevleri Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir. Bu nedenle Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2016-2019 Ulusal Siber Güvenlik Stratejisi gibi dokümanlar ilgili bakanlıkça yayınlanmakta ve yine bu

dokümanlar içerisinde de siber güvenlik kuruluna üye kurumlar ve düzenleyici ve denetleyici kurumlar açıkça belirtilmiştir.

Çizelge 5.1, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayınlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi dokümanına göre siber güvenlik kuruluna üye kurumları ve düzenleyici ve denetleyici kurumlarına üye kurumları göstermektedir.

Çizelge 5.1 : 2016-2019 Ulusal siber güvenlik stratejisine göre siber güvenlik kuruluna üye kurum ve düzenleyici ve denetleyici kurum listesi (yazar tarafından düzenlenmiştir).

SİBER GÜVENLİK KURULUNA ÜYE KURUM LİSTESİ	DÜZENLEYİCİ VE DENETLEYİCİ KURUM LİSTESİ
1. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)	1. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)
2. İçişleri ve Dışişleri Bakanlığı Müsteşarı	2. Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK)
3. Milli Savunma Bakanlığı Müsteşarı (MSB)	3. Enerji Piyasası Düzenleme Kurumu Başkanlığı (EPDK)
4. Kamu Düzeni ve Güvenliği Müsteşarlığı	4. Hâkimler ve Savcılar Yüksek Kurulu Başkanlığı (HSYK)
5. Milli İstihbarat Teşkilatı Müsteşarı (MİT)	5. İstanbul Tahkim Merkezi Başkanlığı
6. Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı	6. Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu Başkanlığı
7. Bilgi Teknolojileri ve İletişim Kurumu (BTK)	7. Radyo ve Televizyon Üst Kurulu Başkanlığı (RTÜK)
8. Mali Suçları Araştırma Kurulu Başkanı	8. Rekabet Kurumu Başkanlığı
9. Telekomünikasyon İletişim Başkanlığı (TİB)	9. Sermaye Piyasası Kurulu Başkanlığı (SPK)
10. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı (TÜBİTAK)	10. Türkiye Cumhuriyeti Merkez Bankası Başkanlığı (TCMB)
11. Ulaştırma, Denizcilik ve Haberleşme Bakanınca Belirlenecek Bakanlık ve Kamu Kurumlarının Üst Düzey Yöneticilerinden	11. Yüksek Seçim Kurulu Başkanlığı (YSK)

Çizelge 5.1'de belirtilen 11 adet Düzenleyici ve Denetleyici Kurum Listesine ek olarak Şeker Kurumu Başkanlığı, Tütün ve Alkol Piyasası Düzenleme Kurumu Başkanlığı (TAPDK), Kamu İhale Kurumu Başkanlığı (KİK), Yükseköğretim Kurulu Başkanlığı (YÖK) kurumları da Düzenleyici ve Denetleyici Kurum Listesinde anılmaktadır.

5.5.1.2 Farkındalık çalışmaları

Bilgi ve Teknoloji Kurumu (BTK), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı içerinden 23. Maddede siber güvenlik konusundaki farkındalığı ele almıştır ve bu konuda da farkındalığı artması amacı ile çeşitli sunumlar ve bilgilendirmeler yapmaktadır. Söz konusu sunumlarda;

- Siber güvenlik ile güncel bilgiler, kurumsal bilgi güvenliği politikaları, bilgi güvenliği ve siber güvenliğe yönelik tehditlerin neler olduğu, bireysel hataların ne sorunlara yol açabileceği, sosyal medya ve mobil cihazların siber güvenliği konusunda bilgilendirmeler yapılmakta,
- Elektronik ve Haberleşme sektöründe denetimi ve düzenleme yetkisini elinde bulunduran Bilgi ve Teknoloji Kurumunun siber güvenlik konusundaki çalışmaları hakkında bilgilendirmeler yapılmakta,
- Ülke genelindeki siber güvenlik politikaları, organizasyonları ve mevzuatı ile ilgili güncel bilgilendirmeler yapılmaktadır [125].

Siber güvenlik konusundaki farkındalık konusunu sadece bilgi ve teknoloji kurumu üzerine bırakmak tahmin edilebileceği üzere tam anlamı ile istenilen etkiyi sağlayamayacaktır. Siber güvenlik konusundaki farkındalık çok erken yaşlarda başlaması gereken bir konu haline gelmiştir. Örnek vermek gerekirse, Milli Eğitim Bakanlığının siber güvenlik konusunu müfredat içerisine alarak bu konuda da eğitim vermeye başlaması, çok büyük bir farkındalık başlatacaktır. Bunun yanı sora özel sektörde de aynı şekilde organizasyon içi siber güvenlik farkındalık seminerleri verilmesi, çalışanlar tarafından bu konunun benimsenmesi ve dikkate alınması sağlanacaktır.

Siber Güvenlik konusunda farkındalığın arttırılması için yapılması gereken çalışmaların bazıları bilgi ve teknoloji kurumu tarafından belirtilmiştir [126].

- Bilgi ve iletişim sistemleri ile bilgi ve iletişim şebekeleri kullanıcılarına yönelik ayrı ayrı siber güvenlik farkındalık programları oluşturmak,
- İnternet kullanıcıları için internet dünyası ile ilgili genel bilginin yanı sıra, kişisel mahremiyet, kişisel veri gizliliği ile birlikte siber ortamdaki kimliğin sınırları hakkında bir eğitim verilmesi,

- Siber güvenlik konusunda her ne kadar en iyi teknolojik altyapıya, en başarılı ve net kanuni düzenlemelere veya her ne kadar organizasyon şemasında siber güvenlik konusunda ayrı bütçe ayırarak yeni bir dal elde edilmiş olsun, günün sonunda siber güvenlik konusunda en zayıf halka insandır. Bunun farkında olan büyük ölçekli firmalar sürekli seminer, konferans veya çeşitli bilgilendirmeler ile personellerini bilgilendirmektedir. Fakat küçük ve orta ölçekli firmalarında bunu yapmaları bilgi ve teknoloji kurumu tarafından önerilmektedir.
- Devlet ve özel sektörde bir siber güvenlik kültürü oluşturulması sağlanmalıdır. Bu konuda devlet tarafından firmaların kendi oldukları durumu belirlemeleri için araçlar sunması, mail yolu ile ara ara bilgilendirme yapması, mali destek ve vergi indiriminde bulunması gibi imkanlar sağlanmalıdır.
- Kapsamlı bir ulusal farkındalık tesisi kurarak özle ve kamu personeli ayırmaksızın bir sertifika programı yürütülmelidir.
- Halka yönelik destek programları hazırlamak.

Farkındalık kampanyalarının yaygınlaşması ile birlikte gerek kamu gerekse özel sektörde siber güvenlik ile ilgili vakaların çok daha azalacağı aşikardır. Bu durum siber saldırı yapmayı amaçlayan bilgisayar korsanı için hem saldırının daha da zorlaşması hem de saldırıyı yapan bilgisayar korsanının tespiti konusunda büyük gelişmeler sağlayacaktır ve bu durumda bir caydırıcılık oluşturacaktır. Bununla birlikte farkındalığın artması sayesinde siber saldırı olaylarının başarı oranında bir düşüş beklemek doğal bir süreç olarak görülmektedir.

5.5.1.3 Ar-Ge faaliyetleri

Ulusal ve uluslararası alanda siber güvenliğin öneminin artması ile birlikte Ar-Ge çalışmalarına, yüksek lisans ve doktora çalışmalarına, ürün ve yazılım geliştirmelerine, güncel makale yayınlanmasına, uluslararası konu uzmanlarını bir araya getirebilmek için konferans ve seminerler düzenlemesine ve patent çalışmaları yapılabilmesi için birçok üniversite bünyesinde siber güvenlik konularında eğitim vermeye başlamıştır.

Bahsedilen konular ile ilgili olarak Ortadoğu Teknik Üniversitesi bünyesinde 15 Nisan 2014 tarihinde Siber Güvenlik ve Savunma Araştırma Laboratuvarı (CyDeS)

kurulmuştur. Bunun yanı sıra Boğaziçi Üniversitesi bünyesinde SOME (Siber olaylarla mücadele) eğitimi, İstanbul Aydın üniversitesi bünyesinde siber güvenlik ve siber olaylarla mücadele eğitimi, Atatürk Üniversitesi bünyesinde temel siber güvenlik eğitimi, Gebze Teknik Üniversitesi bünyesinde de siber güvenlik yüksek lisans ve doktora eğitimi verilmektedir.

Bahsi geçen üniversitelerin dışında daha farklı üniversitelerde de siber güvenlik eğitimi yaygınlaşmaktadır. Üniversitelerin dışında özel firmalar da siber güvenlik ile ilgili eğitimler vermekte, siber kamplar düzenlemektedir.

5.5.1.4 Uluslararası iş birliği sağlama

Bilgi ve Teknoloji Kurumu (BTK), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı içerinden 24 Maddede uluslararası iş birliğinin önemini ele almıştır. 24 maddeye bakıldığında ulusal ve uluslararası siber güvenlik etkinlikleri düzenlenmesinin gerekliliğinden bahsedilmiş ve siber güvenlik ile ilgili olarak, konunun ekonomik, sosyal ve hukuki boyutlarını da ele alacak şekilde konferans ve sempozyumlar düzenlenmesi ve yine siber güvenlik konulu uluslararası seminer, konferans, tatbikat ve çalışmalara katılım göstermek gerektiği ve önemi belirtilmiştir.

Nitekim Türkiye, Ulusal Siber Güvenlik Stratejisinde belirttiği üzere uluslararası koordinasyonu ve ilişkileri pekiştirmek ve siber güvenlik konusundaki farkındalık seviyesini arttırmak amacıyla Bilgi ve Teknoloji Kurumu önderliğinde 2012, 2013 ve 2014 yıllarında, sayıları 12 ile 20 ülke arasında değişen ülke katılımı ile gerçekleştirilen Siber Kalkan Tatbikatları düzenlenmiştir [127].

5.5.1.5 Ulusal siber olaylara müdahale merkezi (usom), kurumsal ve sektörel siber olaylara müdahale ekibi

Ulusal Siber Olaylara Müdahale Merkezi (USOM), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 4. eylem maddesi ile belirtilen "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı madde gereğince, 27 Mayıs 2013 Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde kurulmuştur. Yine söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür [128].

Ulusal Siber Olaylara Müdahale Merkezinin kuruluş amacı, temel olarak kamu ve özel sektör ayırmaksızın siber güvenlik konusunda ulusal ve uluslararası koordinasyonu sağlamaktır. Bu bağlamda, kolluk kuvvetleri, internetin büyük aktörleri, ulusal ve uluslararası kuruluşlar, özel sektör ve araştırma merkezleri arasındaki koordinasyon Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından sağlanmaktadır.

USOM, başkanlık seviyesinde kurulmuş bir merkez olup, sadece koordinasyon değil, aynı zamanda ulusal ve uluslararası seviyede ortaya dış kaynaklardan kendisine ulaştırılan tehditleri inceleyerek, bu tehditlerin bir krize neden olmadan önce tespit edilmesi ve giderilmesi için kamu kurumları ve özel kişiler/firmalar ile iş birliği içerisindedir. Bir krize neden olabileceği düşünülen önemli ihbarlar ilk aşamadan çözüm sürecine kadar USOM tarafından takip edilmektedir.

Ulusal Siber Olaylara Müdahale Merkezi, birçok konuda araştırma, güvenlik tehditleri ve önlemleri ile ilgili duyurular yayınlamıştır ve birçok firma açıklarını bu sayede kapatmıştır. Bunun yanı sıra USOM resmi internet sayfasında zararlı bağlantılar, ihbar seçenekleri olduğu gibi güvenlik bildirileri kısmında sektörde son yaşanan güvenlik olayları ile, firmalar tarafından açıkların kapatılması için çıkılan yeni sürümler vb bulunmaktadır. Bu bildirilere örnek vermek gerekirse, 21.03.2019 erişim tarihi ile yayınlanan güvenlik bildirilerinin bazıları şu şekildedir.

- TR-19-025 (İntel Bazı Donanımsal Yazılımları İçin Güvenlik Önerisi Yayınladı)
- TR-19-024 (VMware Güvenlik Güncellemesi Yayınladı)
- TR-19-023 (Microsoft Mart 2019 Güvenlik Güncellemelerini Yayınladı)
- TR-19-022 (Microsoft Güvenlik Güncellemesi Yayınladı)
- TR-19-021 (WordPress Güvenlik Güncellemesi Yayınladı)
- TR-19-020 (Cisco Güvenlik Güncellemesi Yayınladı)

Biraz önce de bahsedildiği üzere Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 4. eylem maddesine istinaden kurulan USOM'un yanı sıra kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması da yine 4. Eylem maddesinde belirtilmiştir.

Kurumsal ve Sektörel Siber Olaylara Müdahale ekiplerini incelemeye geçmeden önce, Kurumsal SOME, Sektörel SOME ve USOM'un hizmet alanlarını bilmek faydalı

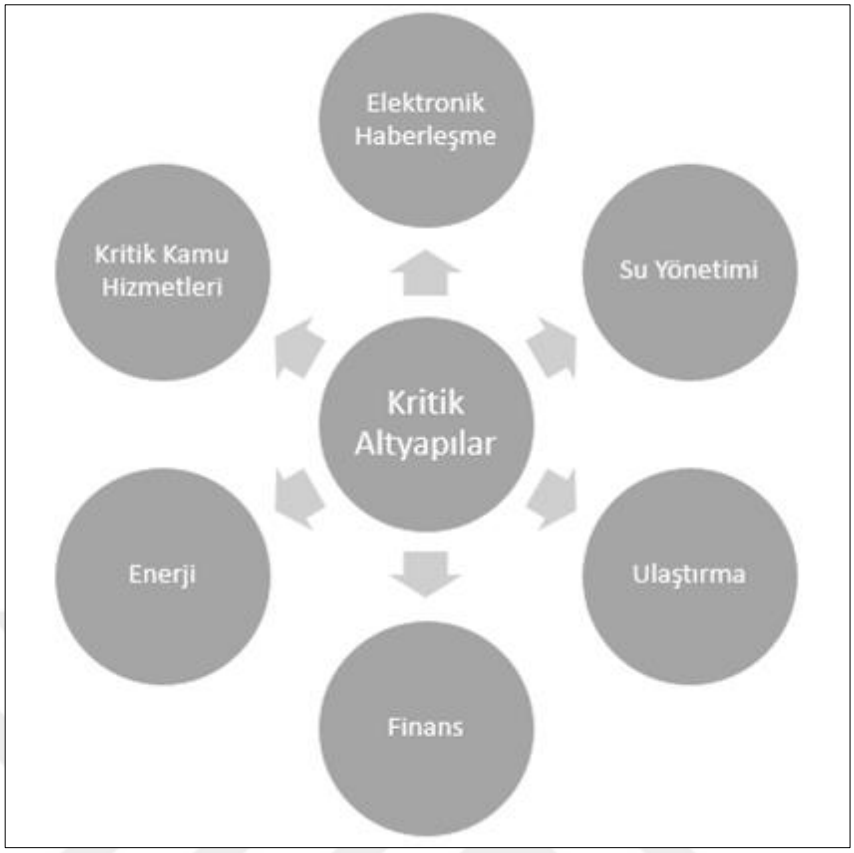
olacaktır. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı bünyesinde bulunan Haberleşme Genel Müdürlüğünün yayınladığı rapora göre organizasyonların hizmet alanları Çizelge 5.2'de gösterilmiştir.

Çizelge 5.2 : USOM, kurumsal SOME, sektöre SOME hizmet alanları [129].

ORGANİZASYON	KURULDUĞU KURUM / KURULUŞ	HİZMET ALANI
USOM	BTK/ Telekomünikasyon Başkanlığı (TİB)	Ulusal siber ortam
Sektörel SOME	Kritik sektörü düzenleyici ve denetleyici kurumlar Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili banaklık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

Çizelge 5.2'den de görüleceği üzere sektörel siber olaylara müdahale ekibinin hizmet alanı kritik altyapı sektörü iken adından da tahmin edilebileceği üzere kurumsal siber olaylara müdahale ekibinin hizmet alanı kamu kurum ve kuruluşları merkezlidir.

Sektörel siber operasyonlara müdahale ekibi, bilgi teknolojileri ve iletişim kurumu bünyesinde 10.09.2014 tarihinde kurulmuştur. Sektörel SOME'nin ana görevi kurumsal SOME'ler ile USOM arasındaki koordinasyonu sağlamak, iletişim faaliyetlerini düzenlemek ve sektör dahilinde kullanılacak iletişim yönetimi ile alakalı husus ve methodları belirlemektedir [130]. Sektörel SOME'lerin odak noktasında kritik altyapılar bulunmaktadır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 4. eylem maddesine istinaden USOM, Kurumsal SOME ve Sektörel SOME'ler oluşturulduktan sonra 5. Madde incelenebilir ve uygulanabilir olmaktadır. Kurumsal altyapı sektörlerine özel sektörel SOME'lerin kurulması, eğitimlerin ve bilgilendirmelerin yapılması, kritik altyapılara özel ekiplerin oluşturulmasını kapsayan 5.maddede bahsedilen kritik altyapılar Şekil 5.18'de gösterilmektedir.



Şekil 5.18 : Türkiye'nin kritik altyapı sektörleri [129].

Söz konusu olan kritik altyapılar siber güvenlik kurulu tarafından güncellenmektedir. Şekil 5.18'de belirtilen güncel kritik altyapıları inceleyecek olursak bu sektörlerin her birinde bir sektörel SOME'ler kurulması gerekmektedir.

Çizelge 5.3'de kritik altyapıların ait oldukları kurumlar ve kritik sistemlerin belirlenmesi için kullanılabilecek parametreler gösterilmektedir.

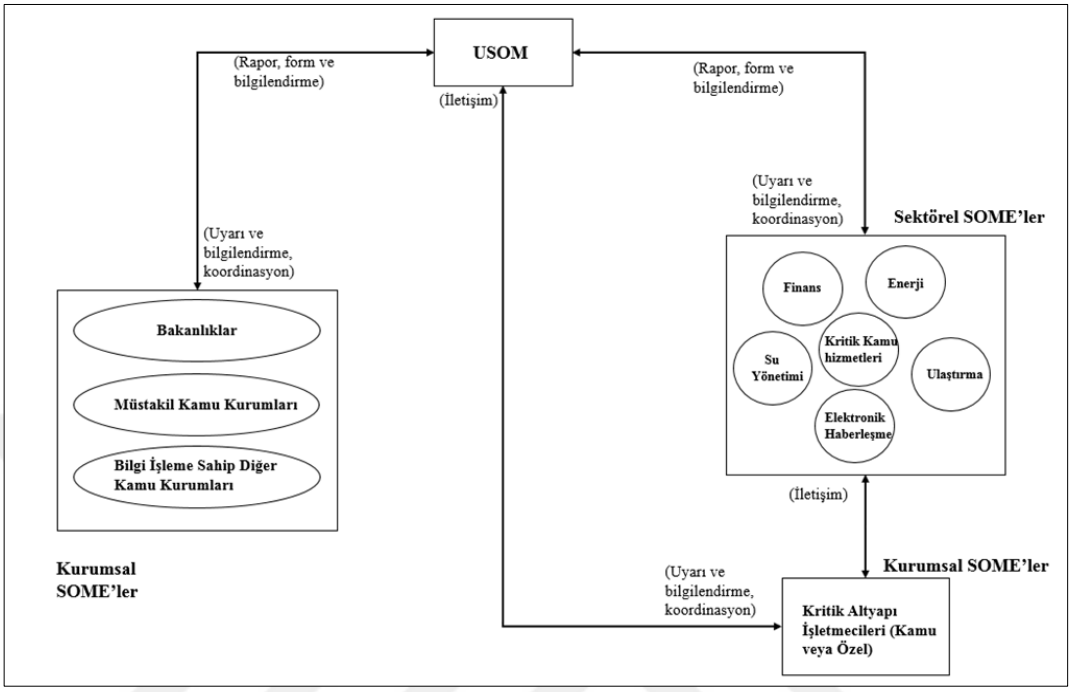
Herhangi bir güncelleme gereksinimi olduğu bir durumda sektörel SOME, USOM ile iş birliği içerisinde politikaları belirlemekte ve güncelleyebilmektedir. Kritik altyapılara karar veren siber güvenlik kurulunun kararlarının sektörel taraftaki karşılıkları sektörel SOME'ler tarafından yerine getirilmektedir. Sektörel SOME'ler kendi sektörlerinde hizmet veren kurum ve kuruluşlara siber güvenlik konusunda destek ve çözümler hakkında bilgi sağlamak ile yükümlüdür. İlgili sektörleri etkileyecek bir siber tehdit durumuna karşı önceden bilgilendirme yaparlar ve güvenlik açığı var ise duyuru ile paydaşları bilgilendirirler.

Çizelge 5.3 : Kritik altyapıların ait oldukları kurumlar ve parametreler [129].

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum	Kritik Sistemlerin Belirlenmesi İçin Kullanılabilecek Parametreler
Enerji	EPDK	Depolanan, satılan, iletilen ve dağıtılan enerji miktarı
Elektronik Haberleşme	BTK	Depolanan, saklanan veri, konuşma süreleri ve sayıları
Finans	SPK, BDDK	Mevduat hacmi
Su Yönetimi	Orman ve Su işleri Bakanlığı	Sistemin su kapasitesi, iletilen, üretilen su miktarı
Kritik Kamu Hizmetleri	1. İçişleri Bakanlığı 2. Adalet Bakanlığı 3. Maliye Bakanlığı 4. Çevre ve Şehircilik Bakanlığı 5. Çalışma ve Sosyal Güvenlik Bakanlığı 6. Gıda, Tarım ve Hayvancılık Bakanlığı 7. Sağlık Bakanlığı,	İşlem sayıları, iç ve dış kullanıcı sayıları
Ulaştırma	1.Karayolu Düzenleme Genel Müdürlüğü 2.Demiryolu Düzenleme Genel Müdürlüğü 3. Deniz ve İç sular Düzenleme Genel Müdürlüğü 4. Sivil Havacılık Genel Müdürlüğü 5. Tehlikeli Mal ve Kombine Taşımacılık Düzenleme Genel Müdürlüğü	Taşınılan yük ve/veya yolcu sayısı

Kurumsal SOME'ler ise Haberleşme Bakanlığının kurumsal SOME kurulum ve yönetimi rehberinde Tebliğ'de yer alan, kurumunda bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan ekip olarak tanımlanmıştır [128]. Bu nedenle kurumsal SOME'ler kamu veya özel fark etmeksizin kritik altyapı işletmecileri bünyesinde veya kamu kurumları bünyesinde bulunmaktadır. Siber olaylara müdahale eden bir ekip olmasından da tahmin edilebileceği üzere kurumsal SOME'ler genellikle bilgi işlem birimi bünyesinde kurulmaktadır. Fakat bilgi işlem birimi dışında kurulan kurumsal SOME'ler de bulunmaktadır. Bu tarz durumlarda ise kurum bünyesinde bilgi güvenliği veya siber güvenlikten sorumlu birim altında olması hayli yüksek bir ihtimaldir.

USOM, kurumsal SOME ve sektörel SOME arasındaki ilişki Şekil 5.19'da açıkça gösterilmektedir. Burada da çok net bir şekilde görüleceği üzere, sektörel SOME, kurumsal SOME ve USOM tam bir iletişim ve raporlama halindedirler.



Şekil 5.19 : USOM organizasyon şeması [129].

USOM organizasyon şemasında gösteriler ifadelerden uyarı ve bilgilendirme, herhangi bir siber olay öncesinde veya bir açıklık, zayıflık durumunda USOM tarafından hazırlanan bülten, duyuru gibi bilgileri ifade etmektedir. Koordinasyon, siber olay esnasında USOM ile kurumsal SOME ve onun bağlı olduğu sektörel SOME arasındaki uyumu ve iletişim ise siber olay öncesi, esnası ve sonrasında USOM ve/veya Kurumsal SOME'nin bağlı olduğu Sektörel SOME tarafından talep edilen rapor, form ve bilgilendirmeyi ifade etmektedir [129].

5.5.2 Yasal mevzuat

5237 Sayılı Yeni Türk Ceza Kanunu'na göre bilişim suçları aşağıda belirtilen başlıklar altında ilgili maddeler ve fıkralar ile yer almaktadır.

Yeni Türk Ceza Kanunu'nun;

"Topluma Karşı Suçlar" bölümü altında onuncu bölümünde bulunan ve "Bilişim Alanında Suçlar" başlığı altında ele alınan madde 243 "Bilişim sistemine girme", madde 244 "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" ve madde 245 "Banka veya kredi kartlarının kötüye kullanılması"

“Kişilere Karşı Suçlar” bölümü altında bulunan ve “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlığı altında ele alınan madde 135 “Kişisel verilerin kaydedilmesi suçu”, madde 136 ve madde 137 “Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu” ve son olarak madde 138 “Verileri yok etmeme suçu”

Bunların yanı sıra, 5237 Sayılı Yeni Türk Ceza Kanunu’na göre, bilişim sistemleri aracılığı ile işlenebilecek ancak salt bilişim suçu kapsamına girmeyecek yani tam olarak bilişim suçu olarak nitelendirilmeyecek suç tipleri de bulunmaktadır.

Bu kapsama girebilecek çok sayıda suç bulunmaktadır. Bilişim sistemlerinin hayatımıza çok hızlı girişi ve bilişim sistemlerinin çok yoğun bir şekilde kullanılması insanların suça bakış açılarını, suç işleme şekillerini değiştirmiştir. Bu nedenle de bilişim sistemleri aracılığıyla dolaylı olarak işlenebilecek suç miktarı her geçen gün artmaktadır. Bu kapsama giren suç tiplerine aşağıdaki örnekler verilebilir [131].

- Madde 124: “Haberleşmenin engellenmesi”
- Madde 125: “Hakaret suçu”
- Madde 132: “Haberleşmenin gizliliğini ihlal suçu”
- Madde 142: 2.fıkrası e bendi “Bilişim sistemlerinin kullanılması süretiyle nitelikli hırsızlık”
- Madde 157 ve 158: “Dolandırıcılık”
- Madde 214: “Suç işlemeye tahrik”
- Madde 215: “Suçu ve suçluyu övme”
- Madde 216: “Halkı kin ve düşmanlığa tahrik ve aşağılama”
- Madde 217: “Kanunlara uymamaya tahrik”
- Madde 226: “Müstehcenlik”
- Madde 239: “Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması “
- Madde 282: “Suçtan kaynaklanan malvarlığı değerlerini aklama”
- Madde 285: “Gizliliğin ihlali”
- Madde 299: “Cumhurbaşkanına hakaret”
- Madde 327: “Devletin güvenliğine ilişkin bilgileri temin etme”

- Madde 331: “Uluslararası casusluk”
- Madde 334: “Yasaklanan bilgileri temin”
- Madde 327: “Devletin güvenliğine ilişkin bilgileri temin etme”
- Madde 329: “Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama”
- Madde 216: “Halkı kin ve düşmanlığa tahrik ve aşağılama”
- Madde 217: “Kanunlara uymamaya tahrik”

5.5.2.1 5237 Sayılı yeni türk ceza kanunu’nda bilişim suçları

- Bilişim sistemine girme

Türk Ceza Kanunun bilişim alanındaki suçlar kapsamında ilk olarak 243. Madde düzenlenmiştir. Bu maddenin Türk Ceza Kanunu’nda yer bulması ile birlikte bilişim sistemine veya sistemlerine yapılan erişimlerde hukuka aykırı bir durum olması halinde yani izinsiz ve servis sahibi bilgisi olmaksızın sisteme bir giriş olması durumunda, bu eylemin bir suç tipi olduğu kanunlaştırılmıştır.

İlgili maddeye göre bireyin sisteme herhangi bir zarar versin veya vermesin gözetmeksizin, eğer birey hukuka aykırı bir şekilde erişim sağlıyor veya sistemde kalmayı devam ettiriyor ise bu durum suç için yeterlidir. Bunun yanı sıra 243. Maddenin 3. Fıkrasında belirtildiği üzere eğer sisteme hukuka aykırı bir şekilde giriş yapılmasının ardından sistemdeki veriler bir şekilde değiştirilirse veya veriler yok olur ise ceza ağırlaştırılmaktadır.

Bilişim sisteminin bir kısmına veya tamamına manuel olarak erişim sağlanabileceği gibi, özel programlanmış bilgisayar programları, korsan yazılımlar, virüs programları veya gizli yazılımlar ile de erişim sağlanabilir.

Bir sistem üzerinde suç işlemek için önce sisteme erişmek gerektiği göz önüne alınırsa bu maddenin ne denli yerinde bir kanun maddesi olduğu da açıkça görülecektir.

Bu maddede yer alan suç tipiyle, Avrupa Siber Suç Sözleşmesinin 2. Maddesinde öngörülen “hukuka aykırı erişim” düzenlemesine paralellik gösterdiği ve özellikle de veriler ele geçirilmeksizin verilere yetkisiz erişim eylemleri suç tipi haline getirdiği görülmektedir [132].

- Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Türk Ceza Kanunun bilişim alanındaki suçlar kapsamında bulunan 244. Maddede, bir bilişim sisteminin işlemesini sekteye uğratan veya sistemi komple bozan kişinin bir yıldan beş yıla kadar hapis cezası ile cezalandırılacağı, bunun yanı sıra sistemdeki verileri bozan, yok eden, değiştiren veya erişilmez kılan veya veri girişi sağlarken halihazırda var olan verileri başka yerlere izinsiz bir şekilde transfer eden kişinin altı aydan üç yıla kadar hapis cezası alacağını, birinci ve ikinci fıkrada bahsedilen eylemlerin banka, kredi kurumuna, bir kamu kurum veya kuruluşuna ait bir bilişim sistemine olma durumunda cezanın yarı oranında arttırılacağını belirtilmiştir [133].

244.Maddenin son fıkrasında ise, başka suç tipinde düzenlenmiş olması halinde ve daha ağır cezayı hak eden bir suç işlemesi durumunda bu maddeden cezaya hükmedilemeyeceği belirtilmiştir. Bireyin hırsızlık, kurum içi bilgi sızdırma, hırsızlık, güveni kötüye kullanma veya zimmet suçu olma durumunda 244/4'e istinaden madde 244'ten hükmedilmeyecektir [132].

Bilişim sistemlerinin hayatımıza girmesi ve çok hızlı bir şekilde gelişmesi de göz önüne alındığında bir sistemin çalışmasını engelleme, sistemi bozma, sistem içerisindeki verilerin silinmesi, değiştirilmesi gibi eylemeler daha da kolay hale gelmiştir. Özellikle DDoS, virüs, kötü amaçlı yazılım, trojan kullanarak hedeflenen saldırı kolaylıkla yapılabilmektedir. Bu nedenle de herhangi bir bilgisayar korsanının bu konuda yapacağı bir saldırı karşısında kurumlara yasal oturumda güvenlik sağlamak adına gerekli bir madde olduğu görülmektedir.

Madde 224'ün Türk Ceza Kanunu'nda yer alması ile birlikte, Avrupa Siber Suç Sözleşmesinin 4. maddesinde öngörülen "verileri etkileme" ve 5. maddesinde öngörülen "sisteme etki" düzenlemelerine paralellik sağlanmaya çalışılmıştır [132].

- Banka veya kredi kartlarının kötüye kullanılması

Türk Ceza Kanunun bilişim alanındaki suçlar kapsamında bulunan 245. Maddede kredi veya banka kartı temelli her türlü suçun bilişim suçları altında inceleneceği belirtilmiştir. Özellikle siber saldırı motivasyonu para olan bilgisayar korsanlarının çok sıklık ile kullandıkları kredi kartı veya banka kartı kopyalama, internet sitelerinin veri tabanlarına erişerek siteye üye olan ve kartını siteye tanıtan kullanıcıların kredi kartı bilgilerinin çalınması, çalınan bu bilgilerin internet ortamında satılması veya

kartların yasadışı alışveriş için , kart sahibinin rızası olmaksızın kullanılması ile kart sahibi kişiye ve bankaya zarar verme durumunda 245. Madde özelinde yargılanacaktır.

195 ülkeden 1700 bilgisayar korsanı ile yapılan ve Şekil 3.1'te belirtilen bilgisayar korsanlarının motivasyonları incelendiğinde paranın azımsanamayacak bir motivasyonu olduğu görülecektir. Bu nedenle de Türk Ceza Kanunun bireylerin kredi kartı ve banka kartı özelinde bir madde ile kanun çıkarmasının çok gerekli olduğu açıkça görülmektedir.

- Tüzel kişiler hakkında güvenlik tedbiri uygulanması

Türk Ceza Kanunun bilişim alanındaki suçlar kapsamında bulunan 246. Maddede yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunduğu madde metninde belirtilmektedir.

5.5.2.2 5237 Sayılı yeni türk ceza kanunu'nda bulunan diğer bilişim suçları

Daha önce 5237 Sayılı Yeni Türk Ceza Kanunu'na göre, bilişim sistemleri aracılığı ile işlenebilecek ancak salt bilişim suçu kapsamına girmeyecek yani tam olarak bilişim suçu olarak nitelendirilmeyecek suç tiplerinden bahsedilmişti. Bilişim dünyasındaki hızlı gelişmeler nedeniyle çok yakın bir zamanda neredeyse her suçun bilişim teknolojileri aracılığı ile işlenebilecek duruma geleceğiniz düşünmek yanlış olmayacaktır.

Yasal mevzuat konusuna genel giriş yaparken diğer bilişim suçlarına birçok örnek verilmiştir. Bu örneklerin bazı önemli olanlarını açıklayacak olursak;

- Haberleşmenin engellenmesi

İnsanın doğası gereğiyle haberleşme ihtiyacı bulunmaktadır. Bu ihtiyaç gerek Avrupa Birliği İnsan Hakları Sözleşmesi gerek BM Medeni ve Siyasi Haklar Sözleşmesi gerekse de ülkemizde Türk Ceza Kanunun 124. Maddesi ile güvence altına alınmıştır.

BM Medeni ve Siyasi Haklar Sözleşmesinin 17. Maddesi mahremiyet hakkı olarak geçmekte ve bu maddede kişinin haberleşmesine hiçbir şekilde hukuka aykırı veya keyfi bir şekilde bir müdahale edilmeyeceğini ve haberleşmesinin engellenemeyeceği yönündedir. Ayrıca yine aynı maddede kişinin böyle bir durum karşısında hukuk tarafından korunma hakkı olduğu belirtilmiştir [134].

Bunun yanı sıra Avrupa Birliği İnsan Hakları Sözleşmesinin 10. Maddesine göre ise ifade özgürlüğü olduğu vurgulanmaktadır. Bu hak düşünce hürriyetini ve resmi makamların müdahalesi ve memleket sınırları söz konusu olmaksızın, haber veya fikir almak veya vermek özgürlüğünü içerir. Bu ifade özgürlüğünün kullanılması, bazı durumlarda gizli haberlerin açıklanmasının engellenmesi ya da yargı erkinin üstünlüğünün ve tarafsızlığının sağlanması bakımından, kanunla belirli işlemlere, koşullara, sınırlamalara ya da yaptırımlara bağlı tutulabilir. Burada önemli olan nokta bu engelleme ve sınırlamaların yalnızca kamu güvenliği, düzenin korunması, suçu önlem ulusal güvenlik ve toprak bütünlüğü gibi önemli durumlarda ortaya çıkmasıdır [135].

Son olarak Türk Ceza Kanunun hürriyete karşı suçlar kapsamında bulunan 124. Madde incelendiğinde Avrupa İnsan Haklar Sözleşme ve BM Medeni ve Siyasi Haklar Sözleşmesi ile paralellik gösterdiği görülmektedir. 124. Maddeye göre basın ve yayın organının yayınını hukuka aykırı bir şekilde kesmek, engellemek bir yıldan beş yıla kadar ceza ile çarptırılacaktır [133].

Bilgisayar korsanlarının halka ulaşmak için kullandıkları en büyük silah olan televizyon kanalları düşünüldüğünde bir siber saldırı anında yayınlarının kesilerek, bilgisayar korsanları tarafından istem dışı yayınlar yapılabilmektedir. Bu nedenle de bu maddenin ne kadar da önemli olduğu açıkça ortaya çıkmaktadır.

- Haberleşmenin gizliliğini ihlal suçu

Türk Ceza Kanunun özel hayata ve hayatın gizli alanına karşı suçlar kapsamında bulunan 132. Maddede kişiler arasındaki haberleşmenin detaylarının dışarıya sızdırılıp sızdırılmadığı ile ilgilenilmektedir. Madde 132'ye göre kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası, kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis ve karşı tarafın rızası olmaksızın kendisi ile yapılan haberleşmenin detaylarını paylaşan, ifşa eden kişi altı aydan üç yıla kadar hapis cezası ile cezalandırılır [133].

Özellikle teknolojideki gelişme ile artık birçok kayıt şekli mevcuttur. Telefon ile bir kişi ile görüşüldüğü anda bir yandan da bir uygulama ile konuşmanın kaydedilebildiği, çok küçük gizli kayıt cihazlarının olduğu da düşünüldüğünde bu maddenin ne kadar da önemli olduğu açıkça ortaya çıkmaktadır.

Avrupa Siber Suç Sözleşmesi'nin 3. maddesinde düzenlenen bilgisayar sistemleri arasındaki iletişime müdahale suçunu yaptırım altına alacak bir düzenleme bulunmamaktadır [136]. Bilişim sistemleri arasındaki tüm haberleşme, kişiler arasındaki haberleşme niteliğinde değildir. Özellikle bilişim teknolojilerinin bu denli hızlı arttığı, yapay zeka sayesinde makinelerin birbirleri ile iletişim kurabildiği düşünüldüğünde bu durumda Türk Ceza Kanunu'nda 132.madde altında yer almadı gerektiğiniz düşünülmektedir.

- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması

Türk Ceza Kanunun özel hayata ve hayatın gizli alanına karşı suçlar kapsamında bulunan 133. Maddede kişiler arasındaki aleni olmayan konuşmaların dinlenmesi ve kayda alınması ele alınmıştır ve konuşmaları hukuka aykırı bir şekilde kişilerin rızası olmadan dinleyen veya kayda alan kişi iki aydan altı aya kadar hapis cezası ile cezalandırılabilmektedir. Türk Ceza Kanunu'nun 133. Madde si 3 fıkradan oluşmakta ve bu fıkraların birinci ve ikinci fıkrasında dinleme ve kayda alma suç olarak düzenlenmiştir. Fakat üçüncü fıkrada ise, elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi işaret edilecek elde edilen kayıtların kullanılması durumu kanunlaştırılmıştır [133].

Zaman zaman çağrı merkezleri ile olan konuşmaların internet dünyasında dolarak komik video kapsamında paylaşımlarının yapılması bu konuya verilebilecek en güzel örneklerdendir. Fakat olarak siber güvenlik bakış açısından bakacak olursak, bir bilgisayar sistemine giren bir bilgisayar korsanı zaten halihazırda 243.madde olan sisteme izinsiz girmeyi ihlal ettiği gibi daha sonra bilgisayarın kamera ve mikrofon özelliklerine erişime açarak ortamda ses dinlemesi yapabilmektedir. Bunun yanı sıra artık her kişinin cebinde en az bir tane olan akıllı telefonlarında bilgisayar korsanları tarafından ele geçirebileceği düşünüldüğünde ortam dinlemesi de çok hayal olamayacaktır. Bunun sonucu bir evdeki konuşmanın kayıt altına alınması olabileceği gibi, bir devlet sırının konuşulduğu ortamında dinlemesi mümkündür. Bu neden de kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması konusunun kanunen ele alınması çok önemlidir.

- Kişisel verilerin kaydedilmesi suçu

Türk Ceza Kanunun özel hayata ve hayatın gizli alanına karşı suçlar kapsamında bulunan 135.Madde 2 fıkradan oluşmaktadır. Birinci fıkrada kişisel verilerin hukuka aykırı bir şekilde kaydedilmesi, ikinci fıkrada ise siyasal, felsefi ve dinsel görüşlerinin, ırksal kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak kaydeden kimsenin birinci fıkrada da olduğu gibi altı aydan 3 yıla kadar hapis cezası ile cezalandırılır [133].

Kişisel verilerin kişilerin rızaları olmaksızın kayıt altına alınması aynı zamanda da kişilik haklarına karşı yapılmış bir saldırı niteliğindedir.

Özellikle bilişim teknolojilerinin gelişmesi ile birlikte günümüzde en önemli varlık veridir. Büyük veri işleme, analizi yapılması konusundaki hızlı ilerleme beraberinde veri ihtiyacı doğurmuştur. Bunun nedeni ne kadar çok veriye sahipseniz o kadar yakın bir gerçeklik ile tahmin edebilirsiniz anlamına gelmektedir. Özellikle banka gibi finans kurumlarının, müşterilerin kredi olanakları ve ödeme güçlerini tahmin etmek için, hastanelerin geçmiş hasta kayıtları ile gelecek hastalıkları tahmin etmeleri için, ticari şirketlerinde bir pazarlama stratejisi olarak kişiye özel reklam verebilmek adına kişisel verileri toplayım kullandığı bilinmektedir.

Tüm bilgileri göz önüne alındığında gerek sosyal medya gerekse internet üzerinde herhangi bir sitenin kişisel verileri kullanabilmesi için kişinin rızası olması gerekmektedir. Fakat burada dikkat edilmesi gereken nokta siber uzayda bilgisayar korsanlarının varlığıdır. Bunun nedeni verinin bu kadar değerli olduğu bir dönemde bilgisayar korsanlarının veri tabanında çok sayıda kişisel veri barındıran internet sitelerini, sosyal paylaşım platformlarını hedef almalarıdır. Bilgisayar korsanları veri tabanlarına sızarak buradaki kişisel verileri ele geçirerek bu verileri çok yüksek fiyatlara satabilmektedir.

Bu noktada kanun içerisine bir fıkra ekleyerek yasadışı şekilde kişisel verileri siber ortamda koruyamayan, siber ortamda satan veya satın alan firma ve bireylerinde cezalandırılma durumları 135., 136 veya 137. Madde altına alınabilir.

- Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu

Türk Ceza Kanunun özel hayata ve hayatın gizli alanına karşı suçlar kapsamında bulunan 136. ve 137. Maddeler, 135. Maddeyi pekiştirici bağlamda olup, halihazırda

kişisel verilerin izinsiz bir şekilde kaydedilmesi suç iken, eğer kişi rızası var ise ve kaydedilmiş ise de bu verilerin korunması da veriye sahip olan kurumdadır.

136.Maddeye göre kişisel verileri hukuka aykırı bir şekilde başka bir bireye veren veya başka bir firma ile paylaşan, yayan veya hukuka aykırı bir şekilde ele geçiren kişinin bir yıldan dört yıla kadar hapis cezası alacağı belirtilmiştir. 137. Madde de ise 136. Madde de bahsedilen suçlara ait cezaların görevi kötüye kullanan bir memur veya belirli bir meslek veya mevkiden yararlanılarak yapılması durumunda cezanın yarısı oranında arttırılacağı belirtilmiştir [133].

Madde 135 anlatılırken örnekte konuya siber güvenlik gözünden bakılmış olup, bir kez daha siber güvenlik özelinde bu maddelerin güncellenmesinin günümüzdeki teknolojik gelişmeler ile yararlı olacağını düşünmekteyim.

- Verileri yok etmeme suçu

Türk Ceza Kanunun özel hayata ve hayatın gizli alanına karşı suçlar kapsamında bulunan 138. Madde, başlığından da anlaşılacağı üzere uzun süreler boyunca şirket veri tabanlarında kişisel verilerin depolanmasını, istenilen her an erişebilir olma durumunun önüne geçebilmek için uygulamaya alınmış bir kanundur. Kişisel verilerin, eğer işlemleri bitmiş ise, yok edilmesini hem devlet hem de bireyin kendisi istemektedir. Bunun nedeni insanın her an fişlendiğini düşünmesinin önüne geçmek ve özgür bir ortam yaratmaktır.

Bir yandan da bilgisayar korsanları tarafından veri tabanlarına erişilmesi durumunda, kişisel veri kaybını minimum da tutmak ve kişilik haklarını korumak olarak düşünülebilir.

Kişisel verileri sistem içinden yok etmekle görevli olan kişilerin, yasal süresi dolmasına rağmen bu görevlerini yerine getirmeyerek kişisel verileri silmemeleri durumunda altı aydan bir yıla kadar hapis cezası verileceği belirtilmiştir [133].

- Özel hayatın gizliliğini ihlâl

Türk Ceza Kanunun özel hayata ve hayatın gizli alanına karşı suçlar kapsamında bulunan 134. Madde sayesinde inşaların özel hayatlarının gizliliği koruma altına alınmış durumdadır.

Özel hayat kavramı içerisinde temel olarak bağımsızlık ve gizlilik kavramlarını içeren bir olgudur. Birey nasıl bir hayat yaşayacağı konusunda, hayatında kimlerle iletişimde

olacağı konusunda, davranışları ve tercihleri ile ilgili özgür ve bağımsız olmalıdır. İnsan hayatı iki yönden oluşmaktadır. Bir tanesi hayatın herkes tarafından bilinmesinde sakında olmayan genel yöndür. Genel yön kısacası, insanın toplum içerisindeki hayatı, toplumsal ilişkiler ile gerçekleşmektedir ve bu nedenle de koruma kapasımda bulunmamaktadır. Fakat özel yön ise özel hayat ve bunun gizliliği ile ilgilidir. Özel yön topluma açık değildir bu nedenle de koruma altına alınması gerekmektedir.

Özel hayatın sınırları konusu tam olarak netlik kazanmamış olmak ile birlikte Alman Anayasa Mahkemesinin geliştirmiş bulunduğu kuşak teorisinden yararlanılabilir. Bu teoriye göre hayat kuşaklardan oluşmaktadır ve 3 kuşak iç içe durumdadır. Birinci kuşakta yani merkezde kişinin yalnızca kendisi tarafından bilinen düşünceleri, duyguları, korkuları ve ümitleri bulunmaktadır ve bu kuşak hayatın gizli alanıdır. Bunu çevreleyen kuşak ise özel hayat olup yalnızca en yakınları ile kişi paylaşım yaptığı alandır. Bu nedenle bu iki kuşak kanun nezdinde koruma altına alınmalıdır [137].

Özel hayatın gizliliği ihlali sorununa örnek olarak paparazzi olarak adlandırılan gazetecilerin teknolojik gelişmeler sayesinde ünlü kişilerin izinsiz fotoğraflarını ya da videolarını çekmek sureti ile kişilik haklarını ihlal etmesi verilebilir ve bu durum madde 134 ile koruma altına alınmış durumdadır.

Bunun yanı sıra özel hayatın gizliliği ihlali sorunu, bilişim teknolojilerinin hayatımıza girdiği her an biraz daha artmaktadır. 2014 yılında Apple firmasının firmaya ait bulut depolama sistemi olan "iCould" hesaplarının ele geçirilmesi ile birlikte birçok insanın, ünlü kişilerin telefonlarında depoladıkları şahsi fotoğrafları ele geçirilmiş ve hatta bazı ünlü kişilerin fotoğrafları internete sızdırılmıştır [138]. iCloud hesaplarının ele geçirilmesi konusu incelendiğinde her ne kadar madde 243 ile belirtilen sisteme izinsiz giriş maddesi çiğnenmiş olsa da sisteme gazeteci örneğinden de görüleceği üzere sisteme giriş yapılmadan sadece teknolojik gelişmeler kullanılarak da özel hayatın gizliliği ihlal edilebileceğinden, bu maddenin madde 243'ten bağımsız olarak ele alınması değerlidir.

Günümüzde her geçen gün değeri artan bulut teknolojileri ve kişisel verilerin daha çok yüksek boyutlarda ve her an her yerden erişimi istendiği için çok kullanılan bulut teknolojisi ve bilgisayar korsanlarının motivasyonları göz önüne alındığında, Türk

Ceza Kanunu tarafından madde 134 ile sağlanan özel hayatın gizliliği ihlali ile ilgili olan kanunu ne denli önemli olduğu bir kez daha anlaşılmaktadır.

134. Maddeye göre kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılmaktadır.

- Hakaret

Türk Dil Kurumu tarafından [139] onur kırma, onura dokunma, küçültücü söz veya davranış olarak tanımladığı "hakaret" ile ilgili kanun, Türk Ceza Kanunun şerefe karşı suçlar kapsamında bulunan 125. Maddesinde belirtilmiştir.

Türk Ceza Kanun'unu 125. Maddesinde her ne kadar bu konu ele alınmış olsa da hakaret suçuna neden olacak sözlerin tek tek bu madde içerisinde belirtilmesi imkansızdır. Bu nedenle hakaret suçunun ne olduğunu ve ne şekilde işlenebileceğini anlamak gerekmektedir.125. Maddeden anlaşılacağı üzere hakaret suçu iki şekilde işlenebilmektedir. Bunlardan birincisi belli somut bir durum ve olgunun isnat edilmesi suretiyle kişinin toplum içerisinden şeref ve saygınlığının zedelenmesi, ikicisi ise soyut ve genel nitelikteki söz ve davranışlarla kişinin bulunduğu toplum içerisinde değersizleştirilmesi, rencide edilmesi şeklindedir. Kısacası hakaret suçunda en temel nokta kişiyi toplum içerisinde rencide eden ve değersizleştiren davranışların cezalandırılmasıdır.

Bir kişiye alenen "homoseksüel", "şerefsiz", "hayvan herif", "hırsız", "aptal", "esrarkeş", "fahişe" gibi sözler söylemenin hakaret suçu oluşturacağı çok açıktır.

Konuyu siber uzay özelinde yorumlayacak olursak, artık insanların internet üzerinden iletişim kurduğu gerçeğinin farkına varmamız gerekmektedir. Özellikle sosyal paylaşım sitelerinin kullanım sıklığı düşünüldüğünde 125. Maddenin önemi bir kez daha ortaya çıkmaktadır. e-posta, facebook, skype, instagram, whatssapp, twitter vb. gibi sosyal medya araçlarıyla doğrudan mağdurun hedef alınarak hakaret edilmesi de hakaret suçunu oluşturur.

- Nitelikli hırsızlık

Türk Ceza Kanunun malvarlığına karşı suçlar kapsamında bulunan 142. Madde genel olarak nitelikli hırsızlık durumunu ele almaktadır. Türk Ceza Kanunu'nun 142. Maddesinin birinci fıkrasına göre hırsızlık suçunun işlenmesi durumunda iki yıldan beş yıla kadar hapis cezası uygulanacağı belirtilmiştir.

Fakat söz konusu olan maddenin ikinci fıkrası incelendiğinde "e" bendinde belirtildiği üzere eğer hırsızlık suçu bilişim sistemleri kullanılması ile gerçekleştirilişe, suçun cezasının üç yıldan yedi yıla kadar hapis cezasına çıkacağı belirtilmiştir.

Bilişim sistemi kullanmak suretiyle hırsızlık suçu işlemeye internet üzerinden banka hesaplarına sızarak, bilgisayar korsanının kendi hesabına veya başka bir hesaba parayı göndermesi veya internet sitelerinde kayıtlı bulunan hesap numaralarını ele geçirerek banka hesaplarından para havale edilmesi örnek verilebilir.

- Nitelikli dolandırıcılık

Türk Ceza Kanunun malvarlığına karşı suçlar kapsamında bulunan 158. Madde nitelikli dolandırıcılık konusunu ele almaktadır. Türk Ceza Kanunu'nun 158. Maddesinin birinci fıkrasının f bendine göre dolandırıcılık suçunun bilişim sistemlerinin, kişiler için güvenli liman olarak görülen banka veya kredi kurumlarının araç olarak kullanılması suretiyle iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmedileceği belirtilmiştir.

Bilişim sistemlerinin aktif kullanılması, internet siteleri üzerinden alışveriş yapmanın kolaylığı, cep telefonlarına indirilecek alışveriş uygulamaları ile ilan verme ve alışveriş yapmanın kolaylığı, internet üzerinden açık arttırma ve ihale sistemlerinin gelişmesi gibi durumlar göz önüne alındığından nitelikli dolandırıcılık yapan kişilerin bilişim sistemleri yardımı ile bunu yapmalarına karşı hazırlıklı olmak gerekmektedir. Örnek olarak internet sitesi üzerinden satın alınan bir ürün için kaparo gönderilmesinin ardından bir daha satıcıya ulaşılamama durumu bu konuya örnek verilebilmektedir.

Bilişim sistemi kullanılması suretiyle nitelikli dolandırıcılık suçu, sosyal medya üzerinden kişinin kendisini başka biri gibi göstererek para veya kontör istenilerek veya telefon ile aranarak banka hesabının terör örgütleri tarafından ele geçirildiği yönünde mağdura yalan bilgi vererek gerçekleştirilebilir. 2018 yılında yaşanan Çiftlik bank olayı [140] nitelikli dolandırıcılık olayına ülkemizde verilebilecek en güncel örnek olarak görülmektedir. İnsanları yalan bilgiler ile kandırarak internet sitesi üzerinde oluşturulan gerçek olmayan çiftliklerin içerisinde hayvanlara ve ürünlere sahibi olduğuna inandırmak sureti ile paralarını aldıktan sonra kaçan dolandırıcı, bilişim sistemlerini kullanarak nitelikli dolandırıcılık suçunu alenen işlemiş bulunmaktadır.

Bilişim sisteminin artık gerek hızı gerekse kolaylığı nedeniyle hayatımızda vazgeçilmez bir noktaya gelmiştir. Tek tık ile bankaya gitmeden para transferleri,

internet üzerinden çok kısa sürede alışveriş imkanı gibi kolaylıkların olması bilişim sistemlerini vazgeçilmez noktaya getirmiştir. Bu nedenle de nitelikli dolandırıcılara çok dikkat etmek gerekmektedir.

5.5.3 Bilişim suçlarında uluslararası hukuk uygulaması – avrupa konseyi siber suçlar sözleşmesi

Bilişim teknolojilerindeki ve siber dünyadaki gelişmelerin çok hızlı olması ve teknolojinin artık hayatımızın her yerinde var olarak bizim yaşam şeklimizi etkilediği açıkça görülmektedir. Yaşantımızı etkileyen bu teknolojik gelişmeler bizim yaşam şeklimizi değiştirdiği gibi, aynı zamanda da suç işleme ve bazı suç kavramını dahi değiştirmiştir. Artık bir birey evinde oturduğu yerden dünyanın diğer ucuna hiçbir coğrafi engel olmaksızın erişebilmekte ve siber suç işleyebilmektedir.

5.5.3.1 Genel değerlendirme

Avrupa Konseyi Siber Suçlar Sözleşmesi ya da diğer adı ile Sanal ortamda işlenen suçlar sözleşmesi 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılmıştır ve 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Siber Suçlar Sözleşmesinin en önemli özelliği Avrupa Konseyi dışındaki ülkeler tarafından da imzalanabilir olmasıdır.

Avrupa Komisyonu Siber Suçlar Sözleşmesinin başlıca üç amacı olduğu söylenebilir [20].

- Bazı siber suçların tanımlarını ortak hale getirerek, ulusal ve uluslararası düzeyde mevzuatın uyumlaştırılmasını ve benzerlik göstermesini sağlamak,
- Siber suçlar ile ilgili olarak yapılması olası bir soruşturma esnasında bilişim ortamına düşen ortak yetkileri tanımlamak ve devletler arasında karar verme kurallarını tekdüzeleştirmek,
- Avrupa Konseyi üyesi olsun veya olmasın devletlerin hükümleri bir an önce yürürlüklerine koymalarını mümkün kılmak için ulusal ve uluslararası hem geleneksel hem de yeni iş birliği yöntemlerini hemen belirlemektir. Bunun nedeni olarak da klasik adli yardımlaşma anlayışına tümüyle farklı yeni yetilerin verilmesinin, Avrupa Konseyi devletler arasında bile mutabık kalınan bir konu olmayışıdır.

Türkiye Büyük Millet Meclisinin Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporunda belirtildiği üzere, Türkiye, Avrupa Komisyonu Siber Suçlar Sözleşmesine iç hukuk düzenlemelerinin yapılması sonrasında dahil olmanın uygun olacağına karar vermiş ve bu karar ışığından da iç hukuk gereksinimlerini yerine getirmesinin ardından sözleşme 10.09.2010 tarihinde Türkiye adına Strazburg kentinde imzalanmıştır.

5.5.3.2 Sözleşmede tanımlanan suçlar

Sanal Ortamda İşlenen Suçlar Sözleşmesi ya da diğer adı ile Avrupa Komisyonu Siber Suçlar Sözleşmesi, internet ve bilgisayar, bilişim unsurları yardımı ile işlenen suçlara karşı yapılmış ilk uluslararası sözleşmedir [141].

Bu sözleşme ile amaç sanal ortamda işlenen suçlar karşısında etkin bir uluslararası iş birliği yaratmak, sanal ortamda işlenen suçların ortak tanımını yapmak ve bu sayede aynı dilden konuşabilmeyi sağlamaktır. Bunun yanı sıra tüm ülkelerin hukuki düzenlemelerinin sanal ortamda işlenen suçlar söz konusu olduğunda uyumlu hale getirmek ve suçların soruşturulması için ulusal ve uluslararası yetkilerin tanımlanmasıdır.

Siber uzaydaki hayatın her geçen gün arttığı, teknolojinin ve internetin hayatımıza her gün biraz daha girdiği göz önüne alınırsa, bunula beraber de siber risklerin artmasını beklemek çok doğru olacaktır. Bu risklere karşı bireysel olarak bazı konularda daha dikkatli olunabileceği gibi, hükümetlerin Avrupa Konseyi önderliğinde oluşturulan sanal ortamda işlenen suçlar sözleşmesini imzalaması ile de devletler tarafından vatandaşların korunmasına yönelik önemli bir adım atılmıştır. Tekrardan vurgulanacak olursa, bu sözleşme ile hükümetler vatandaşlarının özgürlüklerini güvence altına almaya, riskleri azaltmaya ve vatandaşlarının haklarını ve mahremiyetlerini korunma altına almaya çalışılmaktadır.

Bu kapsamda 49 maddeden oluşan Avrupa Komisyonu Siber Suçlar Sözleşmesinde suçlar 9 ana başlık altında toplanmaktadır [142]:

2. Madde: “Yasadışı Erişim”

3. Madde: “Yasadışı Araya Girme”

4. Madde: “Verilere Müdahale”

5. Madde: “Sisteme Müdahale”

6. Madde: “Cihazların Kötüye Kullanımı”

7. Madde: “Bilgisayarla Bağlantılı Sahtecilik”

8. Madde: “Bilgisayarla Bağlantılı Dolandırıcılık”

9. Madde: “Çocuk Pornografisiyle Bağlantılı Suçlar”

10. Madde: “Telif Hakkı ve Bununla Bağlantılı Hakların İhlaline İlişkin Suçlar”

Avrupa Konseyi Siber Suç Sözleşmesinden bağımsız olarak konu ile ilgili Türk kanunu incelendiğinden bu derece ayrıntılı bir şekilde birçoğunun karşılığı bulunmamaktadır. Bu nedenle iç tüzükte de bir değişikliğe giderek siber suçlar ile ilgili ayrıntılı bir bölüm oluşturulması gerektiğini düşünmekteyim.

5.5.3.3 Avrupa konseyi siber suçlar sözleşmesini imzalayan ülkeler

Avrupa Konseyi Siber Suç Sözleşmesi an itibariyle 63 ülke tarafından kabul görmüş ve onaylanmıştır. Bunun yanı sıra yalnızca 3 ülke tarafından onay imzalandığı halde onay verilmemiştir. İmzalandığı halde onay verilmeyen ülkeler İrlanda, İsveç ve Güney Afrika’dır. Daha önce de bahsedildiği üzere Avrupa Komisyonu önderliğinde bu sözleşme oluşturulmuş olsa da Avrupa Komisyonu dışında ülkeler de bu sözleşmeye dahil olabilmektedir. Kendilerince kabul görmüş ve onay veren ülkeler arasında 44 tanesi Avrupa Konseyine üye iken bu ülkelerin 19 tanesi Avrupa Komisyonu dışında kalan ülkelerdir. Bu ülkeler içerisinde Kanada, Amerika Birleşik Devletleri Japonya, İsrail gibi ülkeler bulunmaktadır [143].

Avrupa Konseyi Siber Suçlar Sözleşmesini imzalayan onaylayan ve yürürlüğe koyan ülkelerin güncel hali Ek-A1’de mevcuttur.

5.5.3.4 Siber suç sözleşmesi’ne göre uluslararası adli yardımlaşma konusundaki temel ilkeler

Avrupa Konseyi Siber Suçlar Sözleşmesini imzalayan, onaylayan, yürürlüğe sokan birçok devlet bulunmaktadır. Bu ülkelerin bazıları Avrupa Konseyi üyesi, bazıları ise Avrupa Konseyi üyesi değildir. Ayrıca her ülkenin kendi yasaları, kanunları ve tüzükleri olduğu gibi kendi kültürü de olduğu göz önüne alınırsa, uluslararası bir sözleşmede en önemli konulardan bir tanesi de uluslararası yardımlaşma konusundaki temel ilkelerdir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 23. Maddesine göre uluslararası iş birliği ile ilgili ön görülen temel ilkeler şu şekildedir [20]:

- Uluslararası veya ulusal bir siber suç işlenilmesi durumunda bu sözleşmeye taraf devletler arasındaki iş birliğinin en yüksek düzeyde olması umulmaktadır. Sözleşmeye dahil olan devletler arasında bilgi ve delillerin hızlı akışına engel olabilecek durumların asgari düzeye indirilmesi beklenmektedir.
- İlk maddede bahsedilen ilkeye ek olarak bu iş birliğinin sadece siber bir saldırı ile sınırlı kalmayıp, he bilgisayar sistemleri ve verilerine ilişkin tüm suçları hem de bir bilgisayar sistemi aracılığıyla işlenmeyen, sıradan bir suçun delillerinin elektronik şekilde toplanması bakımından mevcuttur. Yani eğer ki bir suça ait delillerin elektronik şekilde toplanması gerekiyor ise yine iş birliği yapılması umulmaktadır.
- Aksi öngörülmedikçe mevcut hükümlerin önceliği olacaktır.
- Her devlet kendi kurallarını, birkaç istisna dışında, uygulanmaya devam edecektir.

Bazı uzmanlar tarafından öncelikle mevcut hükümlerin önceliğinin olması Avrupa Komisyonu Siber Suç Sözleşmesinin faydalarını azalttığı düşünülse de, yenilenen dünyanın en önemli konusu olan siber uzay, siber saldırı, siber suç gibi konulara karşı yapılmış ilk uluslararası sözleşme sıfatı ile birlikte, ülkelerin bu konuya dikkatini çekmeleri, farkındalık yaratma konularında ve siber suçlar ile ilgili kanunlar konusunda çok faydalı bir sözleşmedir.

6. SONUÇLAR VE ÖNERİLER

Etkili bir siber güvenlik yönetim modeli ile ilgili yapılan araştırmalarda, siber güvenlik konusunun iki ana başlık altında incelenmiş olması gerektiği görülmüştür. Bunlardan bir tanesi en etkili teknik çözümlerin bulunmasını kapsayan teknik analiz, diğeri ise siber güvenlik ile ilgili yönetim ve yönetişimin gereken isteklerine cevap verebilecek stratejik analizdir. Bu iki kavramın birlikte olduğu bir siber güvenlik yöntemi, boyutu 360 derece, uçtan uca ele alarak sistemin tamamına hakim olmakta ve organizasyonlar için etkili bir siber güvenlik ortaya çıkarmaktadır.

Teknik çözümlerin, kurumlar, sistemler veya altyapılar için bir yere kadar siber güvenliği sağlayabilecek olması unutulmamalıdır. Bunun nedeni daha önce de belirtildiği üzere siber güvenlik konusunun yalnızca teknik bir konu olmadığı, teknolojik çözümlerin siber güvenlik için alt başlıklardan yalnızca biri olduğu unutulmamalıdır. Teknolojinin gelişmesi ve hayatımıza çok hızlı bir şekilde girmesi ile birlikte günümüzde tehditler hızla artıyorsa, daha karmaşık önlemleri olan çözümleri düşünmemiz gerekmektedir. Bu nedenle de tüm stratejik yönleri dikkate alan bir siber güvenlik yönetimi modelini ele almak gerekmektedir. Tezimde sunulan siber güvenlik yönetimi modelinin ana fikri, siber güvenliğin kuruluşun tüm bölümlerine yayılması ve kuruluşun her bir üyesinin siber güvenliğe dahil olması gerektiği yönündedir. Ayrıca, etkileşimlerinin karmaşıklığına rağmen, hükümetin, kamu otoritelerinin ve uluslararası en iyi uygulamaları iş birliği yapan ve paylaşan özel sektör kuruluşlarının katılımını içermelidir.

Bir kurumda tez içerinden bahsedilen siber güvenlik yönetimi modelinin uygulanması ayrı ayrı olabilmektedir. Bu durum her bir alt başlık için hedeflere ulaşıp, gelişim planlarının ayrı ayrı hazırlanabileceği ve bu planların birbirine bağlanması gerekmediği anlamına gelmektedir. Bunun nedeni her seviyenin kendi başarı kriterleri ve modele entegre olabilmesi için tamamlaması gereken görevleri olmasıdır.

Her ne kadar organizasyonun kendi yönetimsel kararları ve yatırımları doğrultusunda bahsedilen siber güvenlik yönetim modelinin belli sayıda alt başlığını uygulayabilecek olsa da bahsedilen siber güvenlik yönetiminin tüm alt başlıklarını uygulayan

organizasyon, karşılaşabileceği siber ataklar karşısında tam olarak güvenlikli durumda ve gelecekte karşısına çıkabilecek olan siber saldırılara karşı önceden hazırlıklı durumda olacaktır. Fakat burada dikkat edilmesi gereken noktalardan bir tanesi, bahsedilen siber güvenlik yönetiminin tüm alt başlıklarını uygulayan organizasyon için dahi her şey tamamen hallolmuş olmamasıdır.

Günümüzde siber dünyada coğrafi sınır kavramı bulunmamaktadır ve dünyanın her yerinde siber güvenlik ile ilgili bir durum ve gelişme yaşanmaktadır. Bu nedenle organizasyonların bugün itibariyle kullandıkları teknoloji ve strateji, kendilerini siber saldırılardan kısa bir süreliğine korumaktadır. Bu nedenle organizasyonlar, hızlı yönetim kararları ve doğru yatırımlar ile birlikte tetikte olarak, açıklarını kapatmalı ve kurumlarını sürekli siber güvenlik konusunda güncel tutmalıdır. Kısacası bu durum siber güvenlik yönetimi sürecinin çok dinamik olduğu ve kuruluşların planlarında olmayan ve gelecekte ele alınması gereken durumlar için hazırlanmaları gerektiği anlamına gelmektedir.

Tez çalışması sonrasında elde edilen en önemli bulgulardan bir tanesi, siber güvenlik konusunun Türkiye özelinde yeterli derecede önem görmemesi ve siber güvenlik kavramının tam olarak anlaşılamamasıdır. Öyle ki siber kelimesinin Türk Dil Kurumunun hazırlamış olduğu Türkçe sözlükte dahi karşılığı bulunmamaktadır. Yine diğer dikkat çekilmesi gereken nokta 2016-2019 Ulusal Siber Güvenlik Stratejisinin çok genel bir şekilde açıklamaları yaptığıdır. Bu nedenle de gerek bireyler, özel sektör gerekse kamu kuruluşlarının üzerine düşen görevler net bir şekilde belirtilmemiştir. Ayrıca 2016- 2019 Ulusal Siber Güvenlik Stratejisinde, siber güvenlik dünyasında Şekil 5.15'den de görüleceği üzere yeni bir başlık olan kriz yönetiminin yer almamasıdır. Tez çalışması sonrasında Türkiye için siber güvenlik özelinde görülen en büyük eksiklerden bir tanesi de 5237 Sayılı Yeni Türk Ceza Kanunu'nda siber güvenlik ile ilgili hiçbir başlığın olmamasıdır. Türk Ceza Kanunu'na göre bugün itibariyle bilişim suçları başlığı altında yalnıza 4 adet suç görülmektedir. Türkiye her ne kadar Avrupa Konseyi Siber Suç sözleşmesine üye olmuş olsa da kendi Ceza Kanunu'nda bu denli önemli bir konuya yer vermesi gerekmektedir. Her ne kadar USOM sorumluluğuna bırakılmış olan yazılım ve donanım ile ilgili ürün geliştirme, eğitim ve farkındalık ile ilgili geliştirmelerin, kamu ve özel sektör arasındaki koordinasyonun sağlanmasının yanı sıra kritik altyapı güvenliği, risk analizi, siber

güvenlikte insan etkisi, siber güvenlikte kriz yönetimi, yasal mevzuat gibi konularında Ulusal Siber Güvenlik Stratejisinde yer alması gerekmektedir.

Hayatımızı idame ettirebilmek için asgari koşulları temsil eden, temel ihtiyaçlarımızın direkt olarak fiziksel, ekonomik, sağlık, güvenlik vs olarak ilişkisi olan kritik alt yapıları önemleri vurgulanmalıdır. Sadece ulusal siber güvenlik stratejisi altında değil aynı zamanda Milli Güvenlik Kurulu altında da kritik altyapılara karşı ne şekilde siber güvenlikler alınması gerektiği belirtilmelidir.

Siber güvenlik kuruluna üye kurum listesi incelendiğinde hiçbir özel sektör temsilcisinin, akademisyenin ve sivil toplum kuruluşunun bulunmadığı görülmektedir. Halkın siber güvenliğini sağlamak her ne kadar devletlerin görevi olsa da insanların hayatları idame ettirebilmeleri için sosyal yaşamda etkileşimde oldukları birçok teknolojik firma bulunmaktadır. Bunların bile dışında insanlar sosyal medya, internet bankacığı gibi birçok uygulamayı bireysel amaçlar için kullanmaktadır. Bu nedenle de bir konumda özel sektör firmaları ile halk da iç içedir. Bu nedenle siber güvenlik ile ilgili alınacak kararlar özel sektör, akademik toplum ve sivil toplum kuruluşları tarafından da yakından takip edilmeli, fikirleri dikkate alınmalıdır.

Tez çalışması sırasında dikkat çeken noktalardan bir tanesi teknolojik gelişmelerin günden güne değiştiği bir durumda bilgi teknolojileri kurumunun internet sitesinin biraz daha geniş kapsamlı ve güncel olması gerektiği yönündedir. Bunun yanı sıra bir siber saldırı problemlerin çözülmesinde, siber saldırının ne kadar tekrarladığı durumunun fark edilmesinde ve siber atakların en çok hangi sektörlere ve neden yapıldığı ile ilgili soruların cevaplanmasında en yardımcı olacak veri istatiksel veri olarak görülmektedir. Bu konuda da Türkiye'nin zayıf kaldığı görülmektedir. Türkiye İstatistik Kurumu bünyesinde bilim, teknoloji, bilgi toplumu başlığı altında siber kavramı ile ilgili hiçbir istatistik bulunmamaktadır. En yakında zamanda Bilgi Teknoloji Kurumu ve Türkiye İstatistik Kurumu bir araya gelerek konu üzerinde çalışılmalıdır.

Avrupa nüfusuna oranla yüksek bir genç nüfus oranına sahip Türkiye'de herhangi bir konu ile ilgili yetişmiş personel bulmak sorun olmayacaktır. Fakat bu yalnızca Ulusal Siber Güvenlik Stratejisi ile akademik dünyanın bir araya gelmesi ile olabilecektir. Bu nedenle Türkiye'nin Ulusal Siber Güvenlik Stratejisi raporunda daha önce de belirtildiği üzere siber güvenlik kuruluna üye kurum listesine akademik bireyleri dahil

etmek gerekmekte ve daha sonra da akademisyenlerin ışığında lisans, yüksek lisans ve doktora programlarının tüm üniversitelerde açılmasının sağlanması gerekmektedir. Bunun yanı sıra gerek kamu gerekse özel sektörel yönelik yönetici bazında farkındalık eğitimleri, konferanslar, bakanlık düzeyinde siber düzenlemeleri başlatılmalıdır. Ayrıca ülke genelinde siber güvenlik farkındalık haftası tarzında bir hafta belirlemek de ilgi çekecektir.

Tez çalışması boyunca çıkarılan sonuç ve önerilmesi gereken noktalardan bir tanesi de Türkiye'nin dünya genelinde kullanılabilir bir güvenlik yazılımının olmamasıdır. McAfee, Symantec tarzı zararlı yazılım engelleme programları dünyanın neredeyse her köşesinde kullanılmakta, bu sayede de ellerinde çok büyük derece de veri bulundurmaktadırlar. Fakat tam anlamıyla yerli ve milli bir yapıya geçebilmek için yerli bir yazılıma ihtiyaç vardır. Bunun nedeni devlet sırları, askeri çizimler gibi gizli verilerin olduğu yerlerde yerli yazılımı kullanmak ve dünya çapında yayılması sağlanarak güvenlik konusunda söz sahibi olan bir devlet haline gelmektir. Ayrıca elde edilen veriler sayesinde daha da ileriye gitmek ve geliştirmeler yapmak kolaylaşacaktır.

Tez çalışmasında ile birlikte, bahsedildiği üzere günümüzde yapılan market araştırmaları ve sektörün önde gelen özel sektör firmalarının yeni yayınlanan organizasyon şemaları ile birlikte organizasyonların yapılarına yeni pozisyonlar, yeni sorumluluklar ve yeni mühendislik ve çalışma alanları girdiği görülmektedir. Yapılan araştırmaların sonrasında her ne kadar genel olarak günümüzde çalışan sayısı 1000'in üzerinden olan firmaların bünyelerinde siber güvenlik baş yöneticisi (BGBY,CISO) bulunuyor olsa da bu sayının 150'nin üzerinde olan her bir firma için olması gerektiği önerilmiştir. Bunun yanı sıra siber güvenlik baş yöneticisi sorumluluğu altında kurulması gereken bir program yönetimi, acil operasyonlar ve vaka yönetimi ekibi, genel olarak tüm güvenlik ten sorumlu bir güvenlik mühendisliği ve varlık güvenliği ekibi oluşturulmalıdır. Ayrıca en önemlilerinden bir tanesi olası siber saldırıların 7 gün 24 saat izlenmesini ve gerekli mercilere, USOM, CISO, BTK gibi, anında haber verilebilmesi için bir adet siber operasyon merkezleri (SOC) kurulmalıdır. Özel firmalar için Türkiye'de ki en önemli sorunlardan bir tanesi de firmaların birçoğunda kapsamlı bir siber operasyon merkezi olmamasıdır.

Tez çalışması ile tespit edilen özel sektör ile ulusal siber güvenliğin yani kamunun daha fazla koordinasyon içerisinde olması ve özel sektördeki firmaların siber güvenlik

konusundaki farkındalıklarının arttırılması ve gerekli önlemleri almalarını bir nebze zorunlu tutabilmek için bazı öneriler tespit edilmiştir. Bilgi ve teknoloji kurumu gibi devlet nezdinde siber güvenliğin yüzü olan kurumun, şirketlerin ve diğer kuruluşların siber güvenliklerini arttırmak için ne kadar harcadıklarını kontrol etmenin yanı sıra, harcamalarını etkili bir şekilde yapıp yapmadıklarını kontrol etmesi gerekmektedir. Bu nedenle özellikle büyük miktarda kişisel veri içeren kuruluşların, haberleşme sektörüne öncü olan firmaların, kritik altyapılarda hizmet veren firmaların ve devlet verilerini bünyesinde barındıran bazı özel firmalar ile finans sektörüne hizmet veren firmaların (Telekom firmaları, su ve elektrik dağıtım firmaları, borsaya veri aktaran firmalar, personel, müşteriler, hastalar, vergi mükellefleri vb.) sektörel değerlendirmeler sonrasında karar verilecek periyotlar ile yıllık veya dönemlik olarak BTK'ya aşağıdakileri bildirmelerini yapmaları veya BTK tarafından aşağıdaki bildirimlerin yapılmasının zorunlu kılınması gerektiğini düşünmekteyim:

- Personel siber bilinçlendirme eğitimlerinin ne sıklık ile verildiği,
- Güvenlik süreçleri en son ne zaman, kim tarafından ve hangi standartlarla denetlendiğinde,
- Bir olay yönetimi planının olup olmadığı ve en son ne zaman test edildiği,
- En son yapılan siber tatbikat raporu,
- Paydaşlar ile iletişimde olup olmama durumları,
- Kriz ve risk yönetimi planlarının var olup olmadığı ve var ise en son ne zaman güncellendiği,
- Bünyelerinde siber güvenlikten sorumlu olan personel varlığı ve sayısı ve bununla birlikte siber operasyon merkezlerinin olup olmadığı,
- Farkında oldukları saldırıların sayısı, raporu yani başarılı olup olmadıkları bilgisi.

Bu bildirim/raporlar sayesinde siber saldırılarında yalnızca meydana geldikten sonra ihlalleri bildirmekten ziyade, yönetim süreçlerinde (hem insanlar hem yatırımları hem de siber) güvenlik süreçlerinin daha proaktif bir şekilde izlenmesini sağlanacaktır. BTK tarafından eldeki verilerin karşılaştırılması ile birlikte bir organizasyonun zayıf olduğu bir alan ile ilgili tavsiyeler ve hatta eğitimler verilebilir bu sayede de firmaların siber güvenlik seviyeleri arttırılmış olacaktır. Diğer bir bakış açısından olayı

inceleyecek olursak, bu süreç, dahil olan organizasyonlar için müşterilere, hissedarlara, paydaşlara ve tedarikçilere siber güvenliği ciddiye aldıkları ve etkili süreçleri olduğu konusunda güven vermelerine yardımcı olacaktır. Bu da organizasyonların itibarını arttıracak ve bu sayede de doğal bir teşvik durumu ortaya çıkacaktır. Bunun yanı sıra bir sertifikasyon veya yılın en iyi siber güvenlik yönetim modeline uygun firmaların ödüllendirilmesi ve/veya uluslararası dergi ve organizasyonlarda isimlerinin geçmesi de iyi bir teşvik olacaktır.

Tez çalışması sırasında yapılan literatür taramalarında belirtilen dünya siber tarihine yön veren önemli siber savaşlar ve zararlı yazılımlardan da açıkça görüldüğü üzere gerek ülke gerekse organizasyon bazında olsun teknoloji günün sonunda insan kontrolündedir. Bu nedenle siber güvenlik konusunun sadece teknolojik cihazlar ile olamayacağı aşikardır. Siber güvenlik yönetim modeli içerisinde çok fazla etken bulunmaktadır. Bunlardan bir tanesi olan insan etkisi tarafımca en az teknolojik gelişmeler kadar önem arz etmektedir. Burada dikkat edilmesi gerek nokta insan etkisinden kastedilenin sadece organizasyonun kendi bünyesinde çalışanların özelindeki değil aynı zamanda üçüncü parti çalışanların özelinde de bir etkidir. Genel olarak organizasyonlar içerinden üçüncü parti olarak çalışan bireylerin de gerek ilgili organizasyon gerekse kullanılan ürünlerin ana sahibi olan firmadan destek için organizasyon bünyesinde bulunsun sistemlere erişim yetkileri bulunmaktadır. Bu nedenle tez çalışması sonrasında insan etkisi özelinde verilecek ilk öneri bünyesinde üçüncü parti çalışma bulunduran ve siber güvenlik konusunun önem arz ettiği firmaların, üçüncü taraf tedarikçileri seçerken veri koruma kurallarına dikkat etmesi gerektiği ve üçüncü parti çalışanların da kendi bünyesindeki çalışanlara uyguladığı siber güvenlik bilincine uygunluğun sağlanması için adımlar atması gerektiğidir. Şirket içi çalışanlara gelecek olursak, şirket içerisinde yapılacak interaktif eğitimler, siber güvenlikte önde gelen kişiler tarafından verilecek konferans ve eğitimler ile siber güvenlik ile ilgili farkındalık ve bilincin arttırılmasını sağlanmalıdır. Fakat her alanda olduğu gibi bu alanda da alınan eğitimi konferans ve bilgilerin pratikte uygulanmayışı nedeniyle zaman ile bu farkındalık kaybolmakta ve çalışanların ihlallere neden olması içten bile değildir. Bu nedenle şirket içerisinde bir ödül mekanizması kurulması çok yerinde bir adım olacaktır. Yılın belli dönemlerinden çalışanların haberi olmaksızın gizli bir şekilde yapılacak olan temiz masa kontrolü adı altında bilgisayarların kilitlenip kilitlenmediği, şifrelerin açıkta bırakıp bırakılmadığı kontrolleri sonrasında

yapılacak çekiliş ile ödüller verilebilir, siber güvenliğe uygun olmayan masalara ise herkese başlangıçta verilecek bir puan üzerinden düşüş yapılabilir. Bu da bireylerin dikkatini biraz daha arttıracaktır. Bunun yanı sıra yine ara ara şirket çalışanlarının bilgisi olmaksızın oltalama mailleri atarak bunları siber ekibine bildirenlerin ödüllendirilmesi, şirketin bazı yerlerine bırakılan taşınabilir harici belleklerin çalışanlar tarafından bilinçsizce şirket bilgisayarlarına takılıp takılmadığı ve bu sayede de farkındalığı kontrol edilebilir.

Yine tez çalışması sonrasında bilgisayar korsanlarının bilgisayar korsanlığı yapmalarındaki motivasyonun değişimi tespit edilmiştir. İlk bakışta toplumda da bir ön yargı olarak bulunan para için bilgisayar korsanlığı yapma algısı, teknolojinin gelişmesi ve siber dünyanın insanlara yeni iş alanları açması da göz önüne alındığında çok da sürpriz olmayan bir şekilde değişmiştir. Yapılan araştırma ve analizler sonrasında daha önceleri yalnızca para için bilgisayar korsanlığı yapılırken, yeni düzende bilgisayar korsanlığı yapılmasının en büyük motivasyonu, yeni bilgiler, ipuçları ve teknikler öğrenmek, iddia, kariyer fırsatı ve eğlence olarak görülmektedir. Para ise listede kendisine yer bulmakta fakat popülaritesini kaybetmektedir.

Tez çalışması sonrasına elde edilen en önemli sonuçlardan bir tanesi de risk, riskin giderilmesi için alınan önlemler, bütçe ve yatırım üçgeninin en temelde birbiri ile dirsek dirseğe ilişki de olmasıdır. Her riskin giderilmesine gerek yoktur. Risk analiz sürecinde göz ardı edilebilecek risklerinde tespit edilmesi ve bu risklerin yakından takip edilmesi gerekmektedir. Bu risk, risk matrisi içerisinde şirket politikasına göre düşük ve orta olarak yerlerde bulunmaktadır. Bu risk kontrol altında tutmak bir yandan da siber güvenlik için yatırımların başka yerlerde kullanılmasına olanak sağlayacaktır. Yine en başa dönecek olursak zaten bu nedenle siber güvenlik yönetim modeli bahsedilen 5 alt başlığın bir bütünü olarak ele alınmalıdır.

Tez çalışmasından açıkça anlaşılmaktadır ki bundan sonra devletler arasındaki ilişkilerinin bir kopyası da siber uzayda bulunmaktadır. Bu nedenle devletler arasındaki ilişkilerde kararlar alırken bu bilgiyi de göz önünde bulundurmak gerekmektedir. Hiçbir ülke Estonya, Gürcistan hatta Türkiye'nin de başına gelen internete erişememe sorunu ile karşı karşıya kalmak istemez. Ayrıca tez çalışmasından gelecekteki savaşların beşeri savaşların yanı sıra siber savaş olarak da gerçekleşeceği çıkarılmaktadır. Bu durumda da bilgiye daha önce hakim olan devletler çok kolay üstünlük sağlayabilecektir. Bu durumun bilincinde olarak başta savunma sanayii

özelinde olmak üzere siber savunma kapsamında yazılım ve siber saldırı kapasitemizi arttırabilmek için çalışmaların hızlandırılması gerekmektedir.

Tez çalışması süresinde;

- Bilgisayar korsanlarının kimliklerini ve yaptıkları atakları gizli tutmak istemeleri,
- Devletlerin karşılaştıkları siber atakları gizlemeye çalışmaları ve inkar etmeleri,
- Siber güvenlik yönetim modelinin genel olarak teknolojik yönden ele alınmış olması,
- Konu ile ilgili yapılan makale yayını sayısının az olması ve yapılan yayınların raporlara dayalı olması nedeniyle güncellik durumlarını her yıl kaybetmeleri,
- Kaynaklara ve karşılaştırma yapılan ülkeler ile ilgili dokümanlara çoğunlukla internet vasıtasıyla erişim sağlanma zorunluluğunun olması,
- Konu ile ilgili yazılmış Türkiye özelinde az makale, doküman ve veri olması,
- Yazılan makalelerin İngilizce olması ve bazı kavramların Türkçe karşılıklarının tam olarak karşılanamaması,
- Tez konusunun genişliği ve çoklu disiplinlerden alanlara sahip olduğu ve bu nedenle de birçok disiplini içerecek şekilde ele alınması gerekliliği,
- Çalışma kapsamında incelenen yönetim modeli içerisinde bulunan ele alınan 5 alt başlığın her birinin ayrı ayrı tez konusu olabilecek özellikte öneminin olması,
- Ülkemiz strateji belgeleri ve ilerleme durumlarını gösterir dokümanlara erişme konusunda sıkıntılar yaşanması gibi güçlüklerle karşılaşılmıştır.

Kısaca özetleyecek olursak gerek devlet gerekse özel sektör organizasyonu boyutunda siber güvenlik günümüzün en sıcak konu başlıklarından bir tanesidir. Eksikliği durumunda çok büyük zararlara neden olabilecek siber güvenlik konusu yalnızca teknolojik yönden ele alınmamalıdır. İnsan etkisi, risk yönetimi, kriz yönetimi, kanuni düzenlemeler ve son olarak da organizasyonel yapı ve teknolojik yatırımlar başlıkları ile bu konuyu incelemek etkili bir siber güvenlik yönetim modelini oluşturacaktır. Teknolojinin gelişmesi ile elde ettiğimiz birçok olumlu durumların yanı sıra

olumsuzluklarında farkında olan ve bunlara karşı önceden önlemler alan devlet ve organizasyonlar siber güvenlik konusundan hiçbir zarar görmeden çıkacaktır. Siber güvenlik konusu bireysel seviyeden devlet seviyesine kadar toplumun her köşesini etkileyebilecek bir durumdur. Bu nedenle de herkesin bu konuda bir bilince sahip olması gerekmektedir. Gelecekte daha büyük siber saldırılardan etkilenmemek, sektördeki itibari arttırmak ve paydaşlarının gözünde güvenli bir organizasyon algısı oluşturabilmek için çalışma özelinde siber güvenlik ile ilgili sorunları çok yakından takip edip en kısa zamanda sorunları ortadan kaldırmaya yönelik aksiyonlar alınması gerekmektedir.

KAYNAKÇA

[1] **Atıf Ünaldı,** (2003), "Netizen İnternet Vatandaşı", Alt kitap yayınları, Cilt No:1, s.10, (2003)

[2] **Wiener, N.,** (1948), "Cybernetics, or Control and Communication in the Animal and the Machine," Cambridge, MA: MIT Press, 1948

[3] **Wired, (2009),** Erişim Tarihi: 24/12/2018, http://archive.wired.com/ science/ discoveries/news/2009/03/dayintech_0317.

[4] **Libicki, M.C.**, (2009). Cyberdeterrence and Cyberwar. United States of America: RAND Corporation, 12-13.

[5] **Oxford Dictionaries (2018)**. British & World English, Cyberspace, http://www. oxforddictionaries.com/us/definition/american_english/cyberspace.

[6] **United States Department of Defence**., (2010). Department of Defence Dictionary of Military and Associated Terms; DoD, 13-71.

[7] **P. Wilkinson,** (1974) Political Terrorism, London, 1974, Palgrave; First Edition edition (December 1, 1974)

[8] **Bozdemir, M.** (1981), "Terör(mü) ve Terörizm(mi)?", S.B.F. Basım Yayım Yüksek Okulu Yıllığı, 6, 523-533.

[9] **D. Denning,** (2000), "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000.

[10] **L. J. Janczewski and A. M. Colarik,** (2008), Cyber Warfare And Cyber Terrorism, Information Science Reference

[11] **R. Ahmad, Z. Yunos and S. Sahib,** (2012), "Understanding cyber terrorism: The grounded theory method applied," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 323-328.

[12] **The Global Risks Report 2018,** (2018), Erişim: 20.11.2018, http://www3. weforum.org/docs/WEF_GRR18_Report.pdf

[13] **B. Sahu, N. Sahu, S. K. Sahu and P. Sahu**, (2013), "Identify Uncertainty of Cyber Crime and Cyber Laws," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 450-452.

[14] **BOZDOĞAN AKBULUT, B.** (2000). Bilişim Suçları. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 8 (1-2 (Milenyum Armağanı)), 545-555. Retrieved from http://dergipark.gov.tr/suhfd/issue/26619/280658

[15] **STATISTA,** (t.y.) Erişim Tarihi: 20.11.2018, https://www.statista. com/ statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

[16] **Motivations Behind Attacks, (2013),** Erişim Tarihi: 20.11.2018 https:// paulsparrows.files.wordpress.com/2014/01/2013-motivations. png? resize=595%2C346

[17] **Motivations Behind Attacks, (2016),** Erişim Tarihi: 20.11.2018 https:// www.hackmageddon.com/2016/01/11/2015-cyber-attacks statistics/

[18] **Motivations Behind Attacks, (2018),** Erişim Tarihi: 20.11.2018 https:// i2.wp.com/www.hackmageddon.com/wp-content/uploads/ 2018/01/2017-2016-motivations.png?ssl=1

[19] **Motivations Behind Attacks, (2018),** Erişim Tarihi: 20.11.2018 https:// i1.wp.com/www.hackmageddon.com/wp-content/uploads/ 2018/02/January-2018-Motivations.png?ssl=1Erişim 20.11.2018

[20] **Önok, Murat,** (2013), "Avrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C: 19, S: 2, ss. 1229-1270.

[21] **Özçoban, C.** (2014). 21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü. Yüksek Lisans Tezi, Harp Akademileri, Stratejik Araştırma Enstitüsü, İstanbul.

[22] **Çifçi, Hasan** (2013), Her Yönüyle Siber Savaş, İstanbul: TÜBİTAK Popüler Bilim Kitapları.

[23] **Clarke, Richard A. ve Knake, Robert K.**, (2010), Cyber War – The Next Threat to National Security and What to Do About It, İstanbul Kültür Üniversitesi, 148, Çeviri: Murat ERDURAN, İstanbul

[24] **Schmitt, M.** (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139169288

[25] **Coughlan, S. M.** (2016). *Is There a Common Understanding of What Constitutes Cyber Warfare?*. Lulu Press, Inc.

[26] **Savaş Sanatı, SUN TZU,** (2014), Erişim tarihi: 24/12/2018, http://savas-sanati.blogspot.com/2014/07/iii-savasta-strateji-19-madde.html

[27] **Cyberthreat Real-time MAP,** (t.y.), Erişim Tarihi: 24/12/2018, https:// cybermap.kaspersky.com

[28] **Celiktas, Baris.** (2016). KARADENİZ TEKNİK ÜNİVERSİTESİ * Sosyal Bilimler Enstitüsü Uluslararasi İlişkiler Anabilim Dali Uluslararasi İlişkiler Programi Siber Güvenlik Kavraminin Gelişimi Ve Türkiye Özelinde Bir Değerlendirme Yüksek Lisans Tezi Barış ÇELİKTAŞ MAYIS-2016 TRABZON. 10.13140/RG.2.2.21712.81923.

[29] **Hathaway, Oona A. and Crootof, Rebecca**, "The Law of Cyber-Attack" (2012). *Faculty Scholarship Series*. 3852.

[30] **Serıes X: Data networks, open system communıcations and security** - Overview of cybersecurity (ITU-T X.1205 (04/2008)), Erişim Tarihi: 12.12.2018 , https://www.itu.int/rec/T-REC-X.1205-200804-I

[31] **Amoroso, E.** (2006), Cyber Security. New Jersey: Silicon Press.

[32] **NTT Security 2018 Global Threat Intelligence Report,** (2018), Erişim: 12.12.2018,https://www.dimensiondata.com/insights/-/media/dd/ corporate/pdfs/gtir-executive-guide-2018.pdf

[33] **McAfee Labs Threats Report June 2018,** (2018), Erişim: 12.12.2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf

[34] **Fırat, S. Ü., & Fırat, O. Z.** (2017). Sanayi 4.0 Devrimi Üzerine Karşılaştırmalı Bir İnceleme: Kavramlar, Küresel Gelişmeler ve Türkiye. Toprak İşveren Dergisi, (114), 10-23.

[35] **Symantec Internet Security Threat Report,** (2018), Erişim: 12.12.2018, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[36] **Understandıng Cybercrıme: phenomena, challenges and legal response**, (2012), Erişim Tarihi: 08.11.2018, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[37] **The five phases of hacking,** (2016), https://null-byte.wonderhowto.com/how-to/five-phases-hacking-0167990/

[38] **S. Patil, A. Jangra, M. Bhale, A. Raina and P. Kulkarni**, (2017), "Ethical hacking: The need for cyber security," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1602-1606.

[39] **Kara, M. (**2013). Siber Saldırılar Siber Savaşlar ve Etkileri(Doctoral dissertation, İstanbul Bilgi Üniversitesi).

[40] **Security Breakers**, (2014), Erişim Tarihi: 05.11.2018 https://securitybreakers. wordpress.com

[41] **Type of Hackers,** (t.y.), Erişim Tarihi: 05.11.2018, http://www.omnisecu. com/ccna-security/types-of-hackers.php

[42] **Jordan, T.** (2009). Hacking and power: Social and technological determinism in the digital age. *First Monday*, *14*(7).

[43] **The 2018 Hacker Report,** (2018), Erişim: 13.11.2018, https://www.hackerone. com/sites/default/files/2018-01/2018_Hacker_ Report.pdf

[44] **Decoding The Minds Of Hackers,** (2018), Erişim: 20.11.2018 https://www. nuix.com/sites/default/files/report_nuix_black_report_2018_web_us.pdf

[45] **Rounds, M., & Pendgraft, N.** (2009, August). Diversity in network attacker motivation: A literature review. In *2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 319-323). IEEE.

[46] **Kshetri, N.** (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, *4*(1), 33-39.

[47] **Hacktivism: Means and Motivations … What Else?,** (2013), Erişim: 20.11.2018 https://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/#gref

[48] **Hackmageddon**, (2018), https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

[49] **F. Yihunie, E. Abdelfattah and A. Odeh,** (2018), "Analysis of ping of death DoS and DDoS attacks," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2018, pp. 1-4.doi: 10.1109/LISAT.2018.8378010

[50] **Karabatak, M., & Mustafa, T.** (2018, March). Performance comparison of classifiers on reduced phishing website dataset. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-5). IEEE.

[51] **Callegati, Franco & Cerroni, Walter & Ramilli, Marco.** (2009). Man-in-the-middle attack to the HTTPS protocol. Security & Privacy, IEEE. 7. 78 - 81. 10.1109/MSP.2009.12.

[52] **Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S.** (2009, August). Towards automating social engineering using social networking sites. In *2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 117-124). IEEE.

[53] **Incapsula**, (t.y.) ,https://www.incapsula.com/web-application-security/social-engineering-attack.html

[54] **Keleştemur, Atalay** (2015), Siber İstihbarat,1. Baskı, İstanbul: Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti.

[55] **Cai, N., & Chan, T.** (2011). Theory of secure network coding. *Proceedings of the IEEE*, *99*(3), 421-437.

[56] **BBC,** Erişim Tarihi: 24/12/2018, https://www.bbc.com/turkce/haberler-dunya-39197514

[57] **J. V. Chandra, N. Challa and S. K. Pasupuleti,** (2016) "A practical approach to E-mail spam filters to protect data from advanced persistent threat," 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, 2016, pp. 1-5.

[58] **Netwrix**, (2018), https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/]

[59] **Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R.**, (2017). Cyber-Attack Penetration Test and Vulnerability Analysis. *International Journal of Online Engineering*, *13*(1).

[60] **CANBEK, Gürol; SAĞIROĞLU, Şeref. (2007)** KÖTÜCÜL VE CASUS YAZILIMLAR: KAPSAMLI BİR ARAŞTIRMA. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 22.1.

[61] **Boyd, S. W., & Keromytis, A. D**. (2004, June). SQLrand: Preventing SQL injection attacks. In *International Conference on Applied Cryptography and Network Security* (pp. 292-302). Springer, Berlin, Heidelberg.

[62] **Yener, Yavuz** (2015), İlk Siber Savaş Örneği Olarak Kosova, Erişim Tarihi: 10.01.2019, https://siberbulten.com/makale-analiz/ilk-siber-savas-ornegi-olarak-kosova/

[63] **J.Arquilla, D.Ronfeldt,** (2001) Networks and Netwars The Future of Terror, Crime, and Militancy. USA, RAND Corporation, Sf.240-248.

[64] **BIÇAKCI, S .** (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. Uluslararası İlişkiler Dergisi, 9 (34), 204-226.

[65] **Altun, A.,** (2017), Abd-Çin Rekabeti Bağlamında Siber Savaş, International Journal of Akademik Value Studies, Vol: 3, Issue:9; pp:24-34 (ISSN:2149-8598)

[66] **NYTIMES**, The First World Hacker War, (2001), Erişim Tarihi: 17. 01. 2019 https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html,

[67] **Geers, Kenneth**, (t.y.), Erişim Tarihi: 10.01.2019, Cyberspace and the Changing Nature of Warfare, CCD COE, Tallinn, https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/Black Hat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf

[68] **DARICILI, A .** (2017). ANALYSIS OF ALLEGED CYBER ATTACKS FROM RUSSIAN FEDERATION. International Journal of Social Inquiry, 7 (2), 1-16.

[69] **Taskinen S., Nikkarinen M., Lal S.** (2017), The Estonian Cyberwar, Erişim tarihi: 17. 01. 2019 https://mycourses.aalto.fi/pluginfile.php/457047/mod_ folder/content/0/Kyber%20Crystal.pdf?forcedownload=1

[70] **OTTIS Rain** (2008), Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Erişim Tarihi : 07.01.2019 In Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, Reading: Academic Publishing Limited, 2008,

[71] **Mohan B. Gazula** (2017), Cyber Warfare Conflict Analysis and Case Studies , Erişim Tarihi: Erişim: 13.01.2019, http://web.mit.edu/smadnick/www/wp/2017-10.pdf]

[72] **Follath, E., & Stark, H.**, (2009). How Israel Destroyed Syria's Al Kibar Nuclear Reactor. *Spiegel Online*, *11*, 22-26.

[73] **TİKK Eneken**, (2010), Erişim Tarihi : 07.01.2019, International CyberIncidents: Legal Considerations, Tallinn, Cooperative Cyber Defense Centre of Excellence, 2010,

[74] **T. M. Chen and S. Abu-Nimeh**, (2011), "Lessons from Stuxnet," in Computer, vol. 44, no. 4, pp. 91-93, April2011. doi: 10.1109/MC.2011.115

[75] **Mueller, P., & Yadegari, B.,** (2012). The stuxnet worm. *Département des sciences de linformatique, Université de lArizona. Recuperado de: https://www2. cs. arizona. edu/~ collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report. pdf*.

[76] **W32.Stuxnet Dossier** (2011), Erişim: 07.01.2019, http://www.symantec. com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[77] **The Truth Behind the Shady RAT**,(2011), Erişim Tarihi: 13.01.2019 https://www.symantec.com/connect/blogs/truth-behind-shady-rat.

[78] **Revealed: Operation Shady RAT**, (2011), Erişim Tarihi: 13.01.2019, http://www.mcafee.com/us/resources/ white-papers/wp-operation-shady-rat.pdf

[79] **Yener, Yavuz (2015)**, Gelmiş geçmiş en geniş çaplı siber saldırı: Shady RAT, Erişim Tarihi:13.01.2019 https://siberbulten.com/makale-analiz/gelmis-gecmis-en-genis-capli-siber-saldiri-shady-rat/

[80] **Kuzey Kore-ABD arasında siber saldırı gerilimi** (2014), Erişim Tarihi: 19.01.2019 https://www.bbc.com/turkce/haberler/2014/12/141219_kuzey_kore_obama

[81] **Keleş, A.R. ve Sal, Y.** (2013). Hack Kültürü ve Hacktivism: Yeni Bir Siyaset Biçimi. Alternatif Bilişim Derneği Yayını, 33-34.

[82] **Ransomware Holding Your Data Hostage**, (2016), Erişim Tarihi 14.01.2019, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf

[83] **Scaife, N., Carter, H., Traynor, P., & Butler, K. R.** (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on (pp. 303-312). IEEE.

[84] **M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan,** (2018) "An Investigation on Wannacry Ransomware and its Detection," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 1-6.doi: 10.1109/ISCC.2018.8538354

[85] **Wannacry ransomware statistics, The Numbers Behind the Outbreak**, (2017), Erişim Tarihi:15.01.2019, https://blog.barkly.com/wannacry-ransomware-statistics-2017

[86] **TDK**, Erişim Tarihi: 02/06/2019 http://www.tdk.gov.tr/ index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf6b45afcd42.98554009

[87] **Ulusal Siber Güvenlik Raporuna**, (2016), Erişim tarihi: 02/06/2019, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf

[88] **International Organization for Standardization Guide 73: Risk management vocabulary**, (2009) , Erişim Tarihi: 14.02.2019, https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

[89] ***Häring, Ivo. (2015). Introduction to Risk Analysis and Risk Management Processes. 10.1007/978-981-10-0015-7_2.***

[90] **Toma, Simona-Valeria & Chirita, Mioara & Şarpe, Daniela,** (2012), Risk and Uncertainty, Procedia Economics and Finance. 3. 975-980. 10.1016/S2212-5671(12)00260-2.

[91] **Knight F H,** (2002/1921), Risk, Uncertainty and Profit, Washington, DC: BeardBooks

[92] **A.J.C.Blyth and L.Kovacich** (2001). Information Assurance: Computer Communications & Networks, Springer-Verley 3rd ed. 2015 edition

[93] **Vidalis, Stilianos.** (2019). A Critical Discussion of Risk and Threat Analysis Methods and Methodologies.

[94] **Eling, M., & Wirfs, J.** (2019). What are the actual costs of cyber risk events?. European Journal of Operational Research, 272(3), 1109-1119.

[95] **Bulut Ersin,** (2013), COSO 2013 Sunum, Erişim Tarihi: 29.03.2019, http:// www.tide.org.tr/uploads/TI%CC%87DE-COSO%20Sunumu%202013%20son.pdf

[96] **COSO, I. I.**, (2004). Enterprise risk management. *Integrated Framework*.

[97] ***Risk Management,*** *(t.y), Erişim Tarihi:17.02.2010,* https://survey. charteredaccountantsanz.com/

[98] ***International Organization for Standardization 31000 Risk management — Principles and guidelines,****(t.y), ErişimTarihi : 16.02.2019, https://www.iso.org/standard/65694.html*

[99] ***Barış Bağcı,*** *Bilgi Teknolojileri Risk Yönetimine Genel Bakış, (t.y), Erişim Tarihi: 16.02.2019, https://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx*

[100] ***W. Wu, R. Kang and Z. Li,*** *(2015), "Risk assessment method for cyber security of cyber physical systems," 2015 First International Conference on Reliability Systems Engineering(ICRSE),Beijing,2015,pp.1-5.doi: 10.1109/ICRSE.2015.7366430*

[101] ***In, H. P., Kim, Y. G., Lee, T., Moon, C. J., Jung, Y., & Kim, I.*** *(2004, October). A security risk analysis model for information systems. In Asian Simulation Conference (pp. 505-513). Springer, Berlin, Heidelberg.*

[102] ***A. Jumratjaroenvanit and Y. Teng-amnuay,*** *(2008)."Probability of Attack Based on System Vulnerability Life Cycle," 2008 International Symposium on Electronic Commerce and Security, Guangzhou City, pp. 531-535.*

[103] ***YILMAZ, S., & SAĞIROĞLU, Ş.*** *(2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 158-166.*

[104] ***International Organization for Standardization 27005- Information technolojy – securty techniques – Information security risk managemtn,*** *(t.y), ErişimTarihi : 23.02.2019, https://www.sis.se/api/document/preview/80005503/*

[105] ***M. G. Lee,*** *"Securing the human to protect the system: Human factors in cyber security," 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, Edinburgh, 2012, pp. 1-5.*

[106] ***Cyber Security Breaches Survey,*** *(2018), Erişim Tarihi : 27.01.2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf*

[107] ***Cyber Security Breaches Survey,*** *(2017),Erişim Tarihi : 27.01.2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf*

[108] ***Cyber Security Breaches Survey,*** *(2016),Erişim Tarihi : 27.01.2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf]*

[109] ***Hart, P., Rosenthal, U., & Kouzmin, A.*** *(1993). Crisis decision making: The centralization thesis revisited. Administration & Society, 25, 12–45.*

[110] ***Choucri, N., Madnick, S., & Ferwerda, J.*** *(2014). Institutions for cyber security: International Responses and global imperatives. Information Technology for Development, 20, 96–121.*

[111] ***Y. Golandsky,*** *"Cyber crisis management, survival or extinction?," 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), London, 2016, pp. 1-4.*

[112] **Cybintsolutions**, (2018), Erişim Tarihi: 20.02.2019, https://www.cybintsolutions.com/cyber-security-facts-stats/

[113] ***Klimoski, Richard.*** *(2018). Critical Success Factors for Cyber Security Leaders: Not Just Technical Competence. People + Strategy. 39.*

[114] ***Richards, K. (2014) Has the CISO role changed under the spotlight Information Security Magazine****,(t.y), Erişim Tarihi: 10.03.2019, www.infosccuritymag.com*

[115] ***Allen, Julia & Crabb, Gregory & Curtis, Pamela & Fitzpatrick, Brendan & Mehravari, Nader & Tobar, David.*** *(2015). Structuring the Chief Information Security Officer Organization. 10.13140/RG.2.1.1242.6967*

[116] ***A New Posture For Cybersecurity in A Networked World,*** *(2018), Erişim Tarihi: 03.16.2019,* https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

[117] ***EY's 19th Global Information Security Survey 2017-18.*** *(t.y), Erişim Tarihi: 10.02.2019,https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf*

[118] ***R., & Gallaher, M. P.*** *(2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. The Fifth Workshop on the Economics of Information Security (WEIS06), 1–23.*

[119] **de Vries, J.** (2017). What drives cybersecurity investment?: Organizational factors and perspectives from decision-makers.

[120] ***Haberler****, (2014), Erişim Tarihi: 03.16.2019, https://www.haberler.com/hsbc-turkiye-ye-siber-saldiri-soku-6681833-haberi*

[121] ***Sputniknews**, (2015), Erişim Tarihi: 16.03.2019,* https://tr.sputniknews.com/ *turkiye/201512241019853122-anonymous-turkiye-buyuk-saldiri*

[122] ***Webtekno**, (2017), Erişim Tarihi: 16.03.2019,* https://www.webtekno.com/ internet/turkiye-de-tam-50-milyon-kisinin-kimlik-bilgileri-calindi-h15929.html

[123] ***Eylem Planı,** (2013), Erişim Tarihi: 05.03.2019,* http://www.udhb.gov.tr/ *doc/siberg/SOME_2013-2014_.pdf*

[124] ***Ulusal siber Güvenli Stratejisi**, (2016), Erişim Tarihi: 19.03.2019,* http://www. udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf

[125] ***Farkındalık Çalışmaları,** (2017), Erişim tarihi: 17.03.2019,* https://www.btk. gov.tr/farkindalik-calismalari

[126] ***Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum Ve Alınması Gereken Tedbirler,** (2019), Erişim Tarihi : 03.17.2019, https://www.btk.gov.tr/uploads/undefined/sg.pdf*

[127] ***Uluslararası Siber Kalkan Tatbikatı,** (2014), Erişim Tarihi: 17.03.2019,* https:// www.trthaber.com/haber/ekonomi/uluslararasi-siber-kalkan-tatbikati-127469.html

[128] ***Kurumsal SOME Kurulum ve Yönetim Rehberi,** (2014), Erişim Tarihi: 20.03.2019*,http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh _V1.pdf

[129] ***Sektörel SOME Kurulum ve Yönetim**, (2014), Erişim Tarihi : 20.03.2019* ,https://www.usom.gov.tr/dosya/1470335484-Sektorel% 20SOME%20Rehberi.pdf

[130] **Korkmazer, S.** (2013). Siber güvenlikte USOM'un rolü. Siber Güvenlik ve Siber Terörizm Çalıştayı, 26-27 Şubat 2013, UTSAM, Polis Akademisi Başkanlığı.

[131] **Ergin,İ.** (2005). Polis Bilişim Sempozyumu Bildiriler "Yeni Türk Ceza Kanunu'nda Bilişim Suçları". S.23-29. Ankara: EGM Yay.

[132] **Dülger, M.V.**, (2004). Bilişim Suçları. Ankara: Seçkin Yayıncılık, 212-272.

[133] ***Türk Ceza Kanunu**, (2004), Erişim Tarihi:21.03.2019* https://www. tbmm. gov.tr/kanunlar/k5237.html

[134] ***Kişisel Ve Siyasal Haklar Uluslararası Sözleşmesi,** (1966),Erişim Tarihi: 21.03.2019,http://www.unicankara.org.tr/doc_pdf/metin133.pdf*

[135] ***Avrupa İnsan Hakları Sözleşmesi,** (2010), Erişim Tarihi: 21.03.2019, http://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf*

[136] **DEĞİRMENCİ Olgun**, 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi, TBB Dergisi, Sayı:58, Mayıs/Haziran 2005

[137] **Eker Kazancı, B.** (2007). Kişilerin İzinsiz Görüntüsünün Alınmasının TCK M.134 Çerçevesinde Korunması. Dokuz Eylül Hukuk Fakültesi Dergisi, Cilt:9, Sayı:1, s. 131-164.

[138] ***The Guardian,*** *(2014), Erişim Tarihi: 22.01.2019,* https://www.theguardian.com/technology/2014/sep/01/nude-celebrity-pictures-hack-jennifer-lawrence-rihanna

[139] ***TDK****, Erişim Tarihi: 22.03.2019,* http://www.tdk.gov.tr/index.php?option=*com_gts&kelime=HAKARET*

[140] ***BBC****, (2018) Erişim Tarihi: 22.03.2019,* https://www.bbc.com/turkce/ haberler-turkiye-43414402

[141] ***TBMM Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu,*** *(2012), Erişim Tarihi:23.03.2019,* https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf *]*

[142] ***Sanal Ortamda İşlenen Suçlar Sözleşmesi****, (t.y), Erişim Tarihi: 23.03.2019 http://moral.av.tr/SF/84/sanal_ortamda_islenen_suclar_s%C3%B6zlesmesinin_onaylanmas%C4%B1n%C4%B1n_uygun_bulunduguna_dair_kanun.pdf*

[143] ***Convention on Cybercrime***, (t.y.), *Erişim Tarihi: 21.03.2019,* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[144] **Wearesocail**, (2019), Digital Report 2019, Erişim: 04.04.2019,https://wearesocial.com/global-digital-report-2019

[145] **Cisco Visual Networking Index: Forecast and Trends, 2017–2022,** (2019), Erişim:04.04.2019,https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

[146] **OECD** (2012). *Machine-to-Machine Communications: Connecting Billions of Devices*;OECD Digital Economy Papers, No. 192, OECD Publishing, 1-45.

[147] **Rosner K**, 2013. Is Information Sharing a Help or Hindrance to Critical Energy Infrastructure Protection? Energy Security Forum. Available on the Internet:https://enseccoe.org/data/public/uploads/2017/02/ensecforum8-reduced.pdf

[148] ***A. Papanikolaou, V. Vlachos, A. Papathanasiou, K. Chaikalis, M. Dimou and M. Karadimou,*** *"Cyber crime in Greece: How bad is it?," 2013 21st Telecommunications Forum Telfor (TELFOR), Belgrade, 2013, pp. 1-4.*

EKLER

EK-A - Avrupa Konseyi Siber Suçlar Sözleşmesini imzalayan onaylayan ve yürürlüğe koyan ülke listesi

Çizelge A.1 : Avrupa konseyi siber suçlar sözleşmesini imzalayan onaylayan ve yürürlüğe koyan ülke listesi.

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ			
	İMZALANMA TARİHİ	ONAYLANMA TARİHİ	YÜRÜRLÜĞE GİRME TARİHİ
AVRUPA KONSEYİNE ÜYE ÜLKELER			
Arnavutluk	23/11/2001	20/06/2002	1/7/2004
Andora	23/04/2013	16/11/2016	1/3/2017
Ermenistan	23/11/2001	12/10/2006	1/2/2007
Avusturya	23/11/2001	13/06/2012	1/10/2012
Azerbaycan	30/06/2008	15/03/2010	1/7/2010
Belçika	23/11/2001	20/08/2012	1/12/2012
Bosna Hersek	9/2/2005	19/05/2006	1/9/2006
Bulgaristan	23/11/2001	07/04/2005	1/8/2005
Hırvatistan	23/11/2001	17/10/2002	1/7/2004
Kıbrıs	23/11/2001	19/01/2005	1/5/2005
Çek Cumhuriyeti	9/2/2005	22/08/2013	1/12/2013
Danimarka	22/04/2003	21/06/2005	1/10/2005
Estonya	23/11/2001	12/05/2003	1/7/2004
Finlandiya	23/11/2001	24/05/2007	1/9/2007
Fransa	23/11/2001	10/01/2006	1/5/2006
Gürcistan	1/4/2008	06/06/2012	1/10/2012
Almanya	23/11/2001	09/03/2009	1/7/2009
Yunanistan	23/11/2001	25/01/2017	1/5/2017
Macaristan	23/11/2001	04/12/2003	1/7/2004
İzlanda	30/11/2001	29/01/2007	1/5/2007
İrlanda	28/02/2002		
İtalya	23/11/2001	05/06/2008	1/10/2008
Letonya	5/5/2004	14/02/2007	1/6/2007
Lihtenştayn	17/11/2008	27/01/2016	1/5/2016
Litvanya	23/06/2003	18/03/2004	1/7/2004
Lüksemburg	28/01/2003	16/10/2014	1/2/2015
Malta	17/01/2002	12/04/2012	1/8/2012
Monako	2/5/2013	17/03/2017	1/7/2017
Karadağ	7/4/2005	03/03/2010	1/7/2010
Hollanda	23/11/2001	16/11/2006	1/3/2007
Makedonya	23/11/2001	15/09/2004	1/1/2005
Norveç	23/11/2001	30/06/2006	1/10/2006
Polonya	23/11/2001	20/02/2015	1/6/2015
Portekiz	23/11/2001	24/03/2010	1/7/2010
Moldova	23/11/2001	12/05/2009	1/9/2009
Romanya	23/11/2001	12/05/2004	1/9/2004
Rusya			
San Marino	17/03/2017	08/03/2019	1/7/2019
Sırbistan	7/4/2005	14/04/2009	1/8/2009
Slovakya	4/2/2005	08/01/2008	1/5/2008
Slovenya	24/07/2002	08/09/2004	1/1/2005
İspanya	23/11/2001	03/06/2010	1/10/2010
İsveç	23/11/2001		
İsviçre	23/11/2001	21/09/2011	1/1/2012
Türkiye	10/11/2010	29/09/2014	1/1/2015
Ukrayna	23/11/2001	10/03/2006	1/7/2006
İngiltere	23/11/2001	25/05/2011	1/9/2011

Çizelge A.2.(devam) : Avrupa konseyi siber suçlar sözleşmesini imzalayan onaylayan ve yürürlüğe koyan ülke listesi.

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ			
	İMZALANMA TARİHİ	ONAYLANMA TARİHİ	YÜRÜRLÜĞE GİRME TARİHİ
AVRUPA KONSEYİNE ÜYE OLMAYAN ÜLKELER			
Arjantin		05/06/2018	1/10/2018
Avustralya		30/11/2012	1/3/2013
Yeşil Burun Adaları		19/06/2018	1/10/2018
Kanada	23/11/2001	08/07/2015	1/11/2015
Çin		20/04/2017	1/8/2017
Kolombiya			
Kosta Rika		22/09/2017	1/1/2018
Dominik Cumhuriyeti		07/02/2013	1/6/2013
Gana		03/12/2018	1/4/2019
İsrail		09/05/2016	1/9/2016
Japonya	23/11/2001	03/07/2012	1/11/2012
Mauritius		15/11/2013	1/3/2014
Meksika			
Fas		29/06/2018	1/10/2018
Nijerya			
Panama		05/03/2014	1/7/2014
Paraguay		30/07/2018	1/11/2018
Peru			
Filipinler		28/03/2018	1/7/2018
Senegal		16/12/2016	1/4/2017
Güney Afrika	23/11/2001		
Sri Lanka		29/05/2015	1/9/2015
Tonga		09/05/2017	1/9/2017
Tunus			
Amerika Birleşik Devletleri	23/11/2001	29/09/2006	1/1/2007

ÖZGEÇMİŞ

Ad Soyad **:** Aycan Ramazan GÜNDÜZHEV

Doğum Yeri ve Tarihi **:** Konya, 15.03.1991

Adres **:** Güzelyalı/İSTANBUL

ÖĞRENİM DURUMU

- **Lisans** **:** 2013, Namık Kemal Üniversitesi, Mühendislik Fakültesi, Elektronik ve Haberleşme Mühendisliği

MESLEKİ DENEYİM

- 2015 yılında İngiltere'nin Londra kentinde 1 yıl süren dil eğitimini tamamladı.
- 2016-2018 yılları arasında Vodafone Telekomünikasyon A.Ş. bünyesinde network mühendisi olarak çalıştı.
- 2018 yılında Turkcell Telekomünikasyon A.Ş. bünyesinde çalışmaya başladı.