



ÇOK ULUSLU ŞİRKETLERİN VE ULUS DEVLETLERİN SİBER UZAYDA ETKİSİ



2023

**YÜKSEK LİSANS TEZİ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI**

Sevcan ÖZKAN

**Tez Danışmanı
Dr. Öğr. Üyesi Muhammed Ali YETGİN**

**ÇOK ULUSLU ŞİRKETLERİN VE ULUS DEVLETLERİN SİBER UZAYDA
ETKİSİ**

Sevcan ÖZKAN

Tez Danışmanı

Dr. Öğr. Üyesi Muhammed Ali YETGİN

T.C.

Karabük Üniversitesi

Lisansüstü Eğitim Enstitüsü

Uluslararası İlişkiler Anabilim Dalında

Yüksek Lisans Tezi

Olarak Hazırlanmıştır

KARABÜK

Haziran 2023

İÇİNDEKİLER

İÇİNDEKİLER	1
TEZ ONAY SAYFASI.....	11
DOĞRULUK BEYANI	12
ÖNSÖZ	13
ÖZ.....	14
ABSTRACT.....	16
ARŞİV KAYIT BİLGİLERİ.....	18
ARCHIVE RECORD INFORMATION	19
KISALTMALAR	20
ARAŞTIRMANIN KONUSU	23
ARAŞTIRMANIN AMACI VE ÖNEMİ.....	23
ARAŞTIRMANIN YÖNTEMİ.....	23
ARAŞTIRMANIN HİPOTEZLERİ / PROBLEM	24
KAPSAM VE SINIRLILIKLAR / KARŞILAŞILAN GÜÇLÜKLER	24
1. SİBER UZAYIN KAVRAMSAL ÇERÇEVESİ.....	26
1.1. Siber Uzay: Beşinci Etki Alanı.....	26
1.2. Siber Eylemler	30
1.2.1. Siber Suç & Siber Saldırı & Siber Savaş	30
1.2.2. Siber Terörizm.....	33
1.2.3. Siber İstihbarat ve Siber Casusluk	34
1.2.4. Siber Güvenlik	35
1.2.5. Siber Savunma.....	36
1.2.6. Siber Caydırıcılık	36
1.3. Siber Saldırı Araçları ve Yöntemleri	37
1.3.1. Dağıtılmış Hizmet Reddi Saldırıları	39

1.3.2. Virüsler.....	42
1.3.3. Solucanlar.....	42
1.3.4. Truva Atı.....	43
1.3.5. Casus Yazılımlar.....	43
1.3.6. Zombi Bilgisayar Orduları.....	44
1.3.7. Kök Kullanıcı Takımı	45
1.3.8. Mantık Bombaları	45
1.3.9. Fidyeye yazılımları.....	46
1.3.10. Klavye İşlemlerini Kaydeden Programlar	48
1.3.11. IP Aldatmacası veya Gizlenmesi	49
1.3.12. Arka Kapı Açıkları.....	49
1.3.13. Ortadaki Adam.....	51
1.3.14. Gelişmiş Kalıcı Tehditler	52
1.3.15. Kaba Kuvvet Saldırıları.....	53
1.3.16. Sosyal Mühendislik.....	53
1.3.17. Kimlik Avı - Yemleme - Oltalama	54
1.3.18. İstem Dışı Elektronik Postalar	55
1.3.19. Yapay Zeka (AI) Destekli Siber Saldırılar	57
1.3.20. Şebeke Trafikinin Dinlenmesi	57
1.3.21. SQL Enjeksiyonu.....	58
1.3.22. Kripto Hırsızlığı.....	58
1.4. Siber Uzayda Faaliyet Gösteren Aktörler ve Aktörler Arası İlişkiler	60
1.4.1 Ulus Devlet Aktörleri	61
1.4.1.1 Devlet Destekli Gelişmiş Kalıcı Tehdit Aktörleri	62
1.4.1.2 Siber Ordular	64
1.4.2. Devlet Dışı Aktörler.....	65
1.4.2.1. Hacktivistler	66
1.4.2.2. Siber Teröristler	67
1.4.2.3. Organize Siber Suçlular	68
1.4.2.4. Siber Paralı Askerler	69
1.4.2.5. Siber Milisler	70
1.4.2.6. Bilgisayar Korsanları	71
1.4.2.7. Senaryo Çocukları	72

1.4.2.8. İnternet Trolleri.....	72
1.4.2.9. İçerideki Siber Tehdit Aktörleri	73
1.5. Siber Unsurlar : Kritik Altyapılar.....	74
1.5.1. Kritik Altyapının Temel Bileşenleri (ICS, DCS, SCADA, OT).....	76
1.5.2. Enerji Sektörü.....	79
1.5.3. Barajlar Sektörü.....	80
1.5.4. Finansal Hizmetler Sektörü.....	82
1.5.5. Gıda ve Tarım Sektörü	84
1.5.6. Sağlık Sektörü.....	86
1.5.7. Acil Servisler Sektörü	88
1.5.8. Nükleer Reaktörler, Malzemeler ve Atık Sektörü	90
1.5.9. Ulaşım ve Lojistik Sektörü	91
1.5.10. Telekomünikasyon Sektörü	92
1.5.11. Kimya Sektörü	94
1.5.12. Kritik İmalat Sektörü	95
1.5.13. Ticari Tesisler Sektörü.....	97
1.5.14. Devlet Tesisleri Sektörü	98
1.5.15. Su ve Atık Su Sistemleri Sektörü	99
1.5.16. Savunma Sanayi Sektörü.....	101
1.5.17. Bilgi Teknolojileri Sektörü	103
2. SİBER UZAYDA ULUS DEVLETLERİN YENİ BİR ASKERİ YETENEK OLUŞTURMASI.....	105
2.1. Amerika Birleşik Devletleri'nin Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri	106
2.1.1. Temel Belgeler ve Stratejiler	107
2.1.2. Amerika Birleşik Devletleri'nin Siber Güvenlik Ulusal Organizasyon Yapısı	113
2.1.2.1. ABD Savunma Bakanlığı	113
2.1.2.1.a. ABD Siber Komutanlığı	114
2.1.2.1.b. Ulusal Güvenlik Ajansı	115
2.1.2.1.c. Savunma Bakanlığı Siber Suç Merkezi	117
2.1.2.1.d. Savunma Bilgi Sistemleri Ajansı.....	117
2.1.2.2. ABD İç Güvenlik Bakanlığı	118
2.1.2.2.a. Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA).....	118

2.1.2.2.b. Siber Güvenlik İnceleme Kurulu	119
2.1.2.2.c. Ulaştırma Güvenliği Ajansı.....	119
2.1.2.2.d. ABD Sahil Güvenlik	120
2.1.2.2.e. ABD Gizli Servisi	120
2.1.2.2.f. Göçmenlik Gümrük Muhafaza - İç Güvenlik Soruşturmaları	120
2.1.2.3. Federal Araştırma Bürosu (FBI).....	121
2.1.3. ABD Siber Diplomasisi	122
2.1.3.1. Japonya - ABD	122
2.1.3.2. Singapur - ABD	123
2.1.3.3. Hindistan - ABD.....	124
2.1.3.4. Polonya - ABD	124
2.1.3.5. Suudi Arabistan - ABD	125
2.1.3.6. AB - ABD	125
2.1.3.7. İsrail - ABD	127
2.2. Rusya Federasyonu'nun Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri.....	128
2.2.1. Temel Belgeler ve Stratejiler	129
2.2.2. Rusya Federasyonu'nun Siber Güvenlik Ulusal Organizasyon Yapısı	135
2.2.2.1. Federal Güvenlik Servisi.....	136
2.2.2.2. Rus İstihbarat Servisi.....	138
2.2.2.3. Rus Askeri İstihbarat Direktörlüğü.....	139
2.2.2.4. Federal Koruma Servisi (The Federal Protective Service - FSO)	141
2.2.2.5. Federal İletişim Servisi, Bilgi Teknolojileri ve Kitle İletişimi Denetleme Kurumu	142
2.2.3. Rusya Federasyonu'nun Siber Diplomasisi	142
2.2.3.1. Hindistan - Rusya	142
2.2.3.2. Endonezya - Rusya	143
2.2.3.3. Ermenistan - Rusya	143
2.2.3.4. ASEAN ve Rusya'nın Siber Güvenlik İşbirliği	144
2.3. Çin Halk Cumhuriyeti'nin Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri.....	144
2.3.1. Temel Belgeler ve Stratejiler	145

2.3.2. Çin Halk Cumhuriyeti'nin Siber Güvenlik Ulusal Organizasyon Yapısı	152
2.3.2.1. ÇHC Sanayi ve Bilgi Teknolojileri Bakanlığı	152
2.3.2.2. Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi/Koordinasyon Merkezi	153
2.3.2.3. Ulusal Savunma İçin Bilim, Teknoloji ve Sanayi Devlet İdaresi	153
2.3.2.4. Kamu Güvenliği Bakanlığı	154
2.3.2.5. ÇHC Devlet Güvenlik Bakanlığı	155
2.3.2.6. Halk Kurtuluş Ordusu Genelkurmay Başkanlığı.....	156
2.3.2.6.a. Genel Kurmay Başkanlığı Üçüncü Departmanı	156
2.3.2.6.b. Genel Kurmay Başkanlığı Dördüncü Departmanı.....	157
2.3.2.6.c. Stratejik Destek Gücü	157
2.3.2.7. Çin Siber Uzay İdaresi	158
2.3.3. Çin Halk Cumhuriyeti'nin Siber Diplomasisi.....	159
2.3.3.1. ABD - Çin	159
2.3.3.2. Rusya ve Çin.....	160
2.3.3.3. Avustralya - Çin.....	162
2.3.3.4. Endonezya - Çin.....	162
2.3.3.5. Şanghay İşbirliği Örgütü ve Siber Diplomasi	163
2.4. İran İslam Cumhuriyeti'nin Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri	164
2.4.1. Temel Belgeler ve Stratejiler	166
2.4.2. İran'ın Siber Güvenlik için Ulusal Organizasyon Yapılanması.....	169
2.4.2.1. İran Siber Polis	169
2.4.2.2. İran Siber Uzay Yüksek Konseyi (Supreme Council of Cyberspace-SCC).....	170
2.4.2.3. Ulusal Siber Uzay Merkezi	170
2.4.2.4. Ulusal Pasif Sivil Savunma Örgütü.....	171
2.4.2.5. Siber Savunma Komutanlığı.....	171
2.4.2.6. Basic Siber Uzay Konseyi.....	172
2.4.2.7. İran Siber Ordusu	172
2.4.2.8. DMO Elektronik Harp ve Siber Savunma Örgütü	173
2.4.2.9. İran Ulusal Bilgisayar Acil Durum Müdahale Ekibi	174
2.4.3. İran'ın Siber Diplomasisi	174

2.4.3.1. Rusya-İran.....	174
3.4.3.2. Çin - İran	175
2.5. Stratejik Siber Vakalar.....	176
2.5.1. Körfez Savaşı	176
2.5.2. Kosova Savaşı	177
2.5.3. İsrail - Filistin.....	178
2.5.4. Estonya Siber Saldırısı.....	179
2.5.4. Gürcistan Siber Saldırısı.....	180
3. SİBER UZAYDA ÇOK ULUSLU ŞİRKETLER.....	182
3.1. Endüstri 4.0.....	183
3.1.1. Ulus Devletlerin 4.0 Stratejileri.....	187
3.1.1.1. Almanya - Endüstri 4.0	188
3.1.1.2. ABD - Gelişmiş İmalat Ortaklığı.....	188
3.1.1.3. Japonya - Endüstri 4.1J ve Yeni Robot Strateji Planı	189
3.1.1.4. Güney Kore - İmalat Sanayi İnovasyonu 3.0	190
3.1.1.5. Çin Halk Cumhuriyeti - Çin Mahı 2025	191
3.1.2. Siber Uzayda Endüstri 4.0 ve Siber Casusluk	192
3.2. Otomotiv Sektörü	194
3.2.1. Endüstri 4.0'ın Otomotiv Sektörüyle Entegrasyonu	194
3.2.2. Otomotiv Endüstrisinde Uluslararası Rekabet Gücü ve Etkileri	195
3.2.2.1. Çip Endüstrisindeki Krizin Otomotiv Sektörüne ve Siber Uzaya Etkisi	197
3.2.2.2. Rusya-Ukrayna Savaşı ve Küresel Otomotiv Endüstrisine Etkileri	199
3.2.2.3. Çin - Tayvan Krizinin Otomotiv Endüstrisine Etkisi	200
3.2.2.4. Çip Stratejileri	201
3.2.3. Siber Uzay ve Otomotiv Endüstrisi	204
3.2.3.1. Otomotiv Endüstrisinde Siber Saldırıları	205
3.2.3.2. Otonom Araçlara Yönelik Siber Tehditler	205
3.2.3.3. Bağlantılı Araçlara Yönelik Siber Tehditler	206
3.2.3.4. Elektrikli Araçlara Yönelik Siber Tehditler	208
3.2.3.5. Otomobil Şirketlerine Yönelik Siber Tehditler	209
3.3. Finansal Hizmetler Sektörü	212

3.3.1. Endüstri 4.0'ın Finansal Hizmetler Sektörüne Entegrasyonu	212
3.3.2. 1929'dan Günümüze Dijitalleşen Finansal Hizmetler Sektörü	213
3.3.3. Finansal Teknolojinin Gelişimi	216
3.3.4. Finansal Teknoloji Şirketleri.....	222
3.3.5. Çin, ABD ve Avrupa'da Geleneksel Bankalar ve Finansal Teknoloji Şirketleriyle İşbirliği	223
3.3.6. Çin'de Dijitalleşen Bankacılık.....	225
3.3.7. Avrupa Birliği'nde Dijitalleşen Bankacılık.....	226
3.3.8. ABD'de Dijitalleşen Bankacılık.....	228
3.3.9. Finans Sektöründe Siber Saldırıları	229
3.3.9.1. Dijital Bankacılıkta Siber Güvenlik Tehditleri.....	230
3.3.9.2. Finansal Hizmetler Sektörüne Yönelik Devlet Destekli Siber Tehdit : Kuzey Kore ve İran Örneği.....	231
3.3.9.3. Siber Aklama ve Siber Terörizm	232
3.4. Telekomünikasyon, Bilgi ve İletişim Teknolojileri Sektörü	234
3.4.1. Endüstri 4.0'ın Telekomünikasyon ve BİT Sektörüyle Entegrasyonu	234
3.4.2. Telekomünikasyon ve BİT Sektöründe Uluslararası Rekabet Gücü ve Etkileri	235
3.4.2.1. 5G İletişim Ağı ve Uluslararası Rekabet	236
3.4.2.2. ABD ve Çin Arasındaki Jeopolitik Mücadelenin Odağı: Apple ve Huawei.....	238
3.4.2.2.a. Apple	239
3.4.2.2.b. Huawei.....	240
3.4.2.2.c. Dijital Ekonomik Rekabet: 5G Teknolojisi	242
3.4.2.2.d. Dijital İpek Yolu	243
3.4.2.2.e. Huawei ve ABD Hükümetinin Müdahaleleri	245
3.4.2.3. Telekomünikasyon Endüstrisindeki Küresel Tedarik Zincirinin Temeli : Hammadde	247
3.4.2.3.a. Çatışma Mineralleri : Demokratik Kongo Cumhuriyeti	248
3.4.2.3.b. Lityum Üçgeni : Bolivya, Şili, Arjantin.....	250
3.4.2.4. Metaverse	251
3.4.2.4.a. Çok Uluslu Şirketlerin Metaverse Stratejileri	252
3.4.2.4.b. Ulus Devletlerin Metaverse Stratejileri.....	254

3.4.2.5. Toplum 5.0.....	256
3.4.3. Siber Uzay ve BİT Sektörü	258
3.4.3.1 Çevrimiçi Sosyal Ağlar ve Siber Tehditler	259
3.4.3.2. İnternetteki Siber Tehditler : Deep Web ve Dark Web	261
3.4.3.3 Şirketlere Yönelik Siber Tehditler	266
3.4.3.3.a.Microsoft'a Yönelik Siber Saldırıları.....	266
3.4.3.3.b.Vodafone'a Yönelik Siber Saldırıları.....	266
3.4.3.3.c. T-Mobile'a Yönelik Siber Saldırıları	267
3.4.3.3.d.Sony Pictures Siber Saldırısı	268
3.5. Enerji Sektörü	269
3.5.1. Endüstri 4.0'ın Enerji Sektörüne Entegrasyonu	269
3.5.2 Enerji Sektöründe Uluslararası Rekabet Gücü ve Etkileri.....	271
3.5.2.1. Petrol ve Gaz Endüstrisinde Dijitalleşme.....	271
3.5.2.1.a. Petrol ve Gaz Şirketlerinin Teknoloji Endüstrisi ile İşbirliği ve Girişimleri	273
3.5.2.1.b. Covid-19'un Petrol ve Gaz Endüstrisine Etkisi	279
3.5.2.1.c. Rusya-Ukrayna Savaşının Petrol İhracatına Uluslararası Etkisi ve Norveç'in Artan Petrol İhracatı	281
3.5.2.2. Elektrik Enerjisi Endüstrisinde Dijitalleşme ve Rekabet	284
3.4.2.2.a. Avrupa Birliği	285
3.4.2.2.b. Çin Halk Cumhuriyeti	286
3.4.2.2.c. Güney Kore	286
3.4.2.2.d. ABD.....	287
3.4.2.2.e. Siber Uzayın İklim Değişikliğine Etkisi	287
3.5.3. Siber Uzay ve Enerji Sektörü	288
3.5.3.1. Petrol ve Gaz Endüstrisinde Siber Tehditler	288
3.5.3.1.a. Colonial Pipeline Siber Saldırısı.....	289
3.5.3.1.b. Avrupa Petrol Rafineri Limanlarına ve Depolama Tesislerine Yönelik Siber Saldırı (Amsterdam-Rotterdam-Antwerp).....	291
3.5.3.1.c. Saudi Aramco'da Triconex Denetleyici Saldırısı	292
3.5.3.1.d. Norveç'in Petrol ve Gaz Sektöründeki 50 Şirkete Yönelik Siber Saldırı.....	293
3.5.3.2. Nükleer Endüstrisinde Siber Tehditler	294
3.5.3.2.a. Stuxnet	296

3.5.3.2.b. Korea Hydro & Nuclear Power Co. Ltd'ye Yönelik Siber Saldırı.....	297
3.5.3.2.c. Çin Casus Balonu	298
3.5.3.3. Elektrik Enerjisine Yönelik Siber Tehditler	299
3.5.3.3.a. BlackEnergy Kötü Amaçlı Yazılımı.....	299
3.5.3.3.b. Industroyer Kötü Amaçlı Yazılımı	300
4. ULUSLARARASI HUKUKUN SİBER UZAYDAKİ ROLÜ	301
4.1. Siber Uzayda İnsan Hakları İhlalleri	302
4.1.1. İfade Özgürlüğü.....	303
4.1.2. Özel Yaşamın Gizliliği ve Kişisel Verilerin Korunması.....	305
4.2. Siber Uzayda Uluslararası Hukukun Uygulanmasındaki Zorluklar	306
4.2.1. Kuvvet Olarak Nitelendirilmesi	307
4.2.2. Meşru Müdafaa	308
4.2.3. Ayırt Etme İlkesi ve Siber Saldırıların Anonim Yapısı	309
4.2.4. Gereklilik ve Orantılılık İlkeleri	310
4.3. Uluslararası Hukukun Normlarının Siber Uzaya Uygulanması Yönündeki Girişimler	310
5. ARAŞTIRMANIN YÖNTEMİ VE SWOT ANALİZİ	316
5.1. Araştırmanın Yöntemi.....	316
5.2. Araştırmanın Modeli	319
5.3. Araştırmanın Genişletilmiş Modeli	321
5.4. Ulus Devletler için SWOT Analizi.....	325
5.4.1. Güçlü Yönler	325
5.4.2. Zayıf Yönler	328
5.4.3. Fırsatlar	333
5.4.4. Tehditler	334
5.5. Çok Uluslu Şirketler için SWOT Analizi.....	337
5.5.1. Güçlü Yönler	337
5.5.2. Zayıf Yönler	339
5.5.3. Fırsatlar	341
5.5.4. Tehditler	342
SONUÇ	344
KAYNAKÇA	347

TABLÖLÄR LİSTESİ	422
ŞEKİLLER LİSTESİ	423
ÖZGEÇMİŞ	425



TEZ ONAY SAYFASI

Sevcan ÖZKAN tarafından hazırlanan “ÇOK ULUSLU ŞİRKETLERİN VE ULUS DEVLETLERİN SİBER UZAYDA ETKİSİ” başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Dr. Öğr. Üyesi Muhammed Ali YETGİN

.....

Tez Danışmanı, Bankacılık ve Finans Anabilim Dalı

Bu çalışma, jürimiz tarafından Oy Birliği ile Uluslararası İlişkiler Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 20/06/2023

Ünvanı, Adı SOYADI (Kurumu)

İmzası

Başkan : Doç. Dr. Volkan TEMİZKAN (KBÜ)

.....

Üye : Dr. Öğr. Üyesi Muhammed Ali YETGİN (KBÜ)

Üye : Doç. Dr. Abdülkadir ÖZTÜRK (RTEÜ)

.....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile Yüksek Lisans derecesini onamıştır.

Prof. Dr. Müslüm KUZU

.....

Lisansüstü Eğitim Enstitüsü Müdürü

DOĞRULUK BEYANI

Yüksek lisans tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı herhangi bir yola tevessül etmeden yazdığımı, araştırmamı yaparken hangi tür alıntıların intihal kusuru sayılacağını bildiğimi, intihal kusuru sayılabilecek herhangi bir bölüme araştırmamda yer vermediğimi, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bu eserlere metin içerisinde uygun şekilde atıf yaptığımı beyan ederim.

Enstitü tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak ahlaki ve hukuki tüm sonuçlara katlanmayı kabul ederim.

Adı Soyadı : Sevcan ÖZKAN

İmza :

ÖNSÖZ

Bu çalışma Karabük Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi tarafından desteklenmiştir. Proje Numarası: KBÜBAP-22-YL-026.

Sosyal bilimler alanında siber uzay konusunda çalışma yürütme cesaretini bulmamı sağlayan, rehberliği ve uzmanlığıyla araştırmalarımın yönünü ve derinliğini belirlememde büyük etkisi olan değerli danışman hocam Dr. Öğr. Üyesi Muhammed Ali YETGİN'e en içten teşekkürlerimi sunarım. Aynı zamanda anlayışlı geri bildirimleri ve cesaretlendirmesi ile siber uzayın karmaşıklıklarını daha derinlemesine araştırmam için özgün bakış açısıyla bana ilham verdiği ve beni bugün olduğum araştırmacıya dönüştüren akıl hocalığı için de minnettarlığımı ifade etmek isterim.

Lisans eğitimim sürecinde yol gösterici tavsiyeleri ve akademik alanda sağladığı destekleri için Çankırı Karatekin Üniversitesi'nde Dr. Öğr. Üyesi Ali Samir MERDAN hocama teşekkürlerimi borç bilirim.

Eğitim hayatımda ve sosyal hayatımda yaşadığım tüm zorluklarda her daim desteğini hissettiren, bugünlere gelmem için türlü fedakarlıklarda bulunan ve emeklerini hayatım boyunca ödeyemeyeceğim sevgili babam Şerif ÖZKAN'a ve tertemiz enerjisiyle gücüme güç katan, çalışmamla ilgili her öğrendiği konuyu benimle paylaşan ve yorulduğumda beni cesaretlendirme gayretini her daim sürdüren sevgili eşim Akın ŞEN'e teşekkürlerimi sunarım. Son olarak çalışmamı, kalbimin en derin köşesinden gelen sonsuz sevgi ve teşekkürlerimi sunarak fiziksel olarak bizimle olamasa da ruhuyla her adımda bana rehberlik etmeye ve ilham vermeye devam eden rahmetli annem Mümine ÖZKAN'a ithaf ediyorum.

ÖZ

Gelişen bilimsel bilgi ve teknolojik gelişmeler, uluslararası ilişkileri derinden etkilemiş ve küresel ilişkilere daha birbirine bağlı ve veri odaklı bir yaklaşım sağlamıştır. Bu yaklaşım sonucunda küreselleşen günümüz dünyasında çok uluslu şirketlerin ve ulus devletlerin rekabeti, geleneksel maddi ürünlerin ve fiziksel alanların ötesine geçerek siber uzaya taşınmaktadır. Bu tezin amacı, çok uluslu şirketlerin ve ulus devletlerin siber uzaydaki etkisini, rekabetini ve stratejilerini araştırmaktır. Küresel etkileşimler için önemli bir alan haline gelen siber uzayda, şirketlerin ve devletlerin çok yönlü etkisini anlamak için araştırmada, çok uluslu şirketlerde finans, otomotiv, enerji ve telekomünikasyon sektörleri ve ulus devletlerde ABD, Çin, Rusya, İran'a odaklanılmıştır.

Tez çalışmasında siber eylemlerin, saldırı yöntemlerinin ve ilgili aktörlerin tanımlanmasının ardından, siber uzay yeteneklerini geliştirmeye aktif olarak dahil olan dört ulus devletinin strateji belgeleri ve kurumları detaylı bir şekilde incelenmiştir. Daha sonra telekomünikasyon, finans, enerji ve otomotiv gibi sektörlerde, ekonomik güçlerin diplomatik ilişkiler, egemenlik ve küresel güç dinamikleri üzerindeki etkisini vurgulayarak çok uluslu şirketlerin siber uzayı nasıl etkilediği analiz edilmiştir. Son olarak siber uzay çerçevesinde mahremiyet, gözetleme ve ifade özgürlüğü gibi insan hakları ihlallerinin yanı sıra, siber savaşı uluslararası hukuk içinde düzenlemenin zorlukları, sivil ve askeri alanlar arasındaki karmaşık sınırlar tartışılmıştır.

Araştırmada vaka çalışmaları, raporlar ve politika belgeleri dahil olmak üzere çeşitli kaynakları kapsamlı bir şekile inceleyen ve analiz eden içerik analiz yöntemi kullanılmıştır. Çalışma, çok uluslu şirketlerin ve ulus devletlerin siber uzayda oynadıkları önemli role ışık tutmaya çalışarak, küresel ilişkilerin birbirine bağlılığını ve dijital çağda rekabetin gelişen doğasını vurgulamaktadır. Sonuç olarak siber uzayın ortaya çıkışı, çok uluslu şirketler ve ulus devletler için yeni sınırlar açarak küresel etkileşimlerle devrim yaratmıştır. Çok uluslu şirketler, istihdam yaratma, vergi gelirleri ve yabancı yatırım yoluyla ülke ekonomilerine katkıda bulunarak küresel ekonomide önemli bir rol oynamakta ve teknolojik ilerlemelerin temelinde yer almaktadır. Siber uzayda çok uluslu şirketler, işlerini küresel olarak yürütmek için

dijital platformları ve teknolojileri kullanarak ulusal sınırları aşmaktadır. Bu ekonomik etki, çok uluslu şirketler ve ulus devletler arasındaki ilişkide temel bir faktördür. Ulus devletler de en son teknolojilere erişimin yanı sıra kendi ekonomilerinde yeniliği teşvik etmek için genellikle çok uluslu şirketlere bağımlıdır. Siber güvenlik, yapay zeka, veri analitiği gibi alanlarda çok uluslu şirketler ve ulus devletler arasındaki işbirlikçi girişimler, siber uzayda karşılıklı faydalarla ilerlemelere yol açmaktadır. Siber uzayın ortaya çıkışı, çok uluslu şirketler ve ulus devletler için yeni sınırlar açarak küresel etkileşimlerle devrim yaratmıştır.

Anahtar Kelimeler: Siber Uzay; Çok Uluslu Şirketler; Ulus Devletler; Uluslararası Hukuk



ABSTRACT

Developing scientific knowledge and technological developments have deeply affected international relations and provided a more interconnected and data-driven approach to global relations. As a result of this approach, the competition of multinational companies and nation-states in today's globalizing world is moving beyond traditional material products and physical spaces into cyberspace. This thesis aims to investigate the impact, competition and strategies of multinational companies and nation-states in cyberspace. To understand the multifaceted impact of companies and states in cyberspace, which has become an important area for global interactions, the research focuses on the finance, automotive, energy and telecommunications sectors in multinational companies and the USA, China, Russia, Iran in nation-states.

In the thesis study, after defining the cyber actions, attack methods and related actors, the strategy documents and institutions of the four nation-states that are actively involved in developing cyberspace capabilities are examined in detail. Then, it has been analyzed how multinational companies affect cyberspace, emphasizing the impact of economic powers on diplomatic relations, sovereignty and global power dynamics in sectors such as telecommunications, finance, energy and automotive. Finally, human rights violations such as privacy, surveillance, and freedom of expression within the framework of cyberspace, as well as the difficulties of regulating cyber warfare within international law, and the complex boundaries between civil and military spheres are discussed.

The content analysis method was used in the research, which extensively examines and analyzes various sources, including case studies, reports, and policy documents. The study highlights the interconnectedness of global relations and the evolving nature of competition in the digital age, attempting to shed light on the important role that multinational corporations and nation-states play in cyberspace. As a result, the emergence of cyberspace has revolutionized global interactions, opening new frontiers for multinational corporations and nation-states. Multinational companies play an important role in the global economy by contributing to national

economies through job creation, tax revenues and foreign investment, and are at the heart of technological advances. In cyberspace, multinational companies are transcending national borders, using digital platforms and technologies to run their businesses globally. This economic impact is a fundamental factor in the relationship between multinational companies and nation-states. Nation-states also often depend on multinational companies to foster innovation in their economies, as well as access to the latest technologies. Collaborative initiatives between multinational companies and nation-states in areas such as cybersecurity, artificial intelligence, and data analytics lead to mutually beneficial advances in cyberspace. The emergence of cyberspace has revolutionized global interactions, opening new frontiers for multinational corporations and nation-states.

Keywords: Cyberspace, Multinational Corporations, Nation painting, International Law

ARŞİV KAYIT BİLGİLERİ

Tezin Adı	Çok Uluslu Şirketlerin ve Ulus Devletlerin Siber Uzayda Etkisi
Tezin Yazarı	Sevcan ÖZKAN
Tezin Danışmanı	Dr. Öğr. Üyesi Muhammed Ali YETGİN
Tezin Derecesi	Yüksek Lisans
Tezin Tarihi	20.06.2023
Tezin Alanı	Uluslararası İlişkiler
Tezin Yeri	Karabük Üniversitesi / Lisansüstü Eğitim Enstitüsü
Tezin Sayfa Sayısı	423
Anahtar Kelimeler	Siber Uzay, Ulus Devletler, Çok Uluslu Şirketler, Uluslararası Hukuk

ARCHIVE RECORD INFORMATION

Name of the Thesis	The Impact of Multinational Corporations and Nation States in Cyberspace
Author of the Thesis	Sevcan ÖZKAN
Advisor of the Thesis	Assist. Prof. Dr. Muhammed Ali YETGİN
Status of the Thesis	Master's Degree
Date of the Thesis	20.06.2023
Field of the Thesis	International Relations
Place of the Thesis	UNIKA/IGP
Total Page Number	423
Keywords	Cyberspace, Nations States, Multinational Corporations, International Law

KISALTMALAR

AB	: Avrupa Birliđi
AGİT	: Avrupa Güvenlik ve İşbirliđi Teşkilatı
AI	: Artificial Intelligence
APT	: Advanced Persisent Threat
Ar-Ge	: Araştırma ve Geliştirme
BM	: Birleşmiş Milletler
BP	: British Petroleum
BT	: Bilgi Teknolojileri
BTC	: Bitcoin
CAC	: Cyberspace Administration of China
CIA	: Central Intelligence Agency
CISA	: Cybersecurity and Infastructure Security Agency
DCS	: Distributed Control System
DHS	: Department of Homeland Security
DOJ	: Department of Justice
DISA	: Defense Information Systems Agency
DMO	: Devrim Muhafızları Ordusu
DNS	: Domain Name System
DOD	: Department of Defence
DODIN	: Department of Defense Information Network
DoSS	: Distributed Denial of Service Ataack
FATA	: İran Siber Polisi
FBI	: Federal Bureau of Investigation

Fintech	: Finansal Teknoloji
FSB	: Federalnaya Slujba Bezopasnosti
FSO	: Federal Protective Service
FTP	: File Transfer Protocol
GRU	: Glavnoye Razvedyvatel'noye Upravleniye
HKO	: Halk Kurtuluş Ordusu
HTTP	: Hyper Text Transfer Protocol
IoT	: Internet of Things
IP	: Internet Protocol Address
ISHD	: İslam Devleti Hacking Birimi
İŞİD	: Irak-Şam İslam Devleti
ITU	: International Telecommunication Union
MIIT	: Ministry and Information Technology
MOIS	: Ministry of Intelligence and Security
MSS	: Ministry of State Security
MSTIC	: Microsoft Threat Intelligence Center
NAJA	: İran İslam Cumhuriyeti Kolluk Kuvvetleri
NATO	: North Atlantic Treaty Organization
NCSC	: National Counterintelligence and Security Center
NSA	: National Security Agency
SCADA	: Supervisory Control and Data Acquisition
SVR	: Sluzhba Vneshney Razvedki
SWIFT	: Society for Worldwide Interbank Financial Telecommunication
ŞİÖ	: Şangay İşbirliği Örgütü
TOR	: The Onion Router (Anonim Ağ)
UN	: United Nations

USSTRATCOM	: United States Strategic Command
USCYBERCOM	: United States Cyber Command
VPN	: Virtual Private Network (Sanal Özel Ağ)
WWW	: World Wide Web (Dünya Çapında İnternet)



ARAŞTIRMANIN KONUSU

Sürekli gelişen teknoloji ve küreselleşme ortamında, çok uluslu şirketlerin ve ulus devletlerin siber uzaydaki etkisi giderek daha önemli hale gelmiştir. Bu tez çalışmasında çok uluslu şirketlerin ve ulus devletlerin siber uzayda etkisi, rekabeti, stratejileri ve yeteneklerinin geliştirilmesi ele alınmıştır. Ayrıca inovasyon ve teknolojik ilerlemelerin küresel çatışmalar, rekabetler ve stratejik karar verme üzerindeki etkisi göz önünde bulundurularak, bu araştırma teknolojik gelişmeler bağlamında ulus devletler arasındaki çıkarları ve rekabetleri incelemektedir.

Siber saldırıların hukuksal boyutları ve önemi nedeniyle insan hakları ve savaş hukuku çerçevesinde incelenmiştir.

ARAŞTIRMANIN AMACI VE ÖNEMİ

Ulus devletler ve çok uluslu şirketler, siber uzayda hem savunma hem de saldırı yeteneklerini kullanarak uluslararası ilişkilerde belirleyici bir rol oynamaktadır. Araştırmanın birincil amacı, çok uluslu şirketlerin ve ulus devletlerin siber uzayda uyguladıkları kapsamlı ve çok yönlü etkiyi araştırmaktır. Bu çalışma çok uluslu şirketlerin ve ulus devletlerin, stratejik yatırımlarını, politikalarını, düzenleyici çerçevelerini, jeopolitik çıkarlarını ve güç dinamiklerini inceleyerek, bu aktörlerin dijitalleşmeyi şekillendirmede ve kontrol etmede sahip oldukları etki düzeyini belirlemeyi amaçlamaktadır. Araştırmanın, çok uluslu şirketlerin ve ulus devletlerin siber uzayda sahip olduğu etkinin kapsamını ve büyüklüğünü ortaya çıkarmada önemli bir rol oynayacağı düşünülmektedir.

ARAŞTIRMANIN YÖNTEMİ

Araştırmada İçerik Analiz yöntemi uygulanmıştır. Bu kapsamda çeşitli yazılı raporlar, uluslararası örgütlerin resmi raporları, ulus devletlerin hükümet raporları, güvenlik raporları, uluslararası mahkemelerde alınan kararlar, bilimsel çalışmalardan elde edilen her türlü görsel, işitsel, metinsel, algısal veri toplama araçları ile elde edilen veriler tematik analiz yöntemi ile metodolojik olarak araştırılmış ve ilgili çalışmalar hipotezler oluşturularak çözümlenmiştir. Bütüncül bir sonuç elde edebilmek için siber

güvenlik, uluslararası ilişkiler, hukuk ve teknoloji gibi alanlardan yararlanarak çok disiplinli bir yaklaşım kullanılmıştır. Araştırmadaki bulguların daha açıklayıcı bir şekilde ortaya konulması için Tematik Analiz yönteminden yararlanılarak SWOT Analizi ile incelenmiştir.

ARAŞTIRMANIN HİPOTEZLERİ / PROBLEM

Siber uzay, teknolojik gelişmeler, siber güvenlik önlemleri, bilgi yayma ve küresel yönetim yapıları gibi çeşitli boyutları kapsayan bir alan olarak giderek daha fazla önem kazanmaktadır. Bu alanda, çok uluslu şirketler ve ulus devletler tarafından kullanılan etkinin kapsamı hakkında belirsizlikler bulunmaktadır. Bu çalışmanın merkezinde yer alan kapsayıcı sorun, çok uluslu şirketlerin ve ulus devletlerin siber uzayda ne ölçüde etkisi olduğunu belirtmektedir. Problem ifadeleri P harfi ile kodlanmıştır. P₁ ve P₂ olmak üzere iki temel problem bulunmaktadır.

P₁; Çok uluslu şirketlerin siber uzayda etkisi hangi düzeydedir?

P_{1a}; Otomotiv şirketlerinin siber uzayda etkisi hangi düzeydedir?

P_{1b}; Finans şirketlerinin siber uzayda etkisi hangi düzeydedir?

P_{1c}; Telekomünikasyon, bilgi ve teknoloji şirketlerinin siber uzayda etkisi hangi düzeydedir?

P_{1d}; Enerji şirketlerinin siber uzayda etkisi hangi düzeydedir?

P₂; Ulus devletlerin siber uzayda etkisi hangi düzeydedir?

P₃; Siber uzayda uluslararası hukukun etkisi hangi düzeydedir?

KAPSAM VE SINIRLILIKLAR / KARŞILAŞILAN GÜÇLÜKLER

Bu araştırmada çok uluslu şirketlerin ve ulus devletlerin siber uzay üzerindeki etkisini incelemek için sektörler ve ülkeler arasında bir seçim yapılmıştır. Öncelikle, seçilen bilgi ve iletişim teknolojileri, telekomünikasyon, finans, enerji ve otomotiv sektörleri, küresel ekonominin önemli yönlerini temsil etmektedir. Ulus devletler arasından seçilen Amerika Birleşik Devletleri, Çin Halk Cumhuriyeti, Rusya

Federasyonu, İran İslam Cumhuriyeti, siber uzayda farklı jeopolitik, ekonomik ve teknolojik etkilere sahiptir.

Siber uzay üzerindeki etkileşimlerin incelenmesi ve tam bir anlayışın elde edilmesi için güvenilir ve güncel verilere ihtiyaç vardır. Ancak çok uluslu şirketler ve ulus devletler genellikle bu bilgileri gizli tutmakta veya kısıtlı bir şekilde paylaşmaktadır. Çok uluslu şirketlerin ve ulus devletlerin siber uzay üzerindeki etkilerini anlamak için aralarındaki ilişkileri de dikkate almak önemlidir. Bu ilişkiler genellikle politik, ekonomik ve teknolojik boyutları içerir ve bunların hepsini ayrıntılı olarak incelemek karmaşık bir süreçtir. Ayrıca siber uzay hızla değişen bir ortamdır ve yeni teknolojiler, saldırı yöntemleri, savunma stratejileri sürekli olarak yenilenmektedir. Siber uzayın hızla gelişen doğası ve sürekli değişen teknolojik ortam araştırmayı zorlaştıran faktörler arasındadır.

1. SİBER UZAYIN KAVRAMSAL ÇERÇEVESİ

1.1. Siber Uzay: Beşinci Etki Alanı

ABD Savunma Bakanlığı Askeri ve İlgili Terimler Sözlüğüne göre siber uzay *"internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler dahil olmak üzere birbirine bağlı bilgi teknolojisi (BT) altyapıları ağından ve yerleşik verilerden oluşan bilgi ortamında küresel bir etki alanı"* olarak tanımlanmıştır (U.S. Department of Defence [DOD], 2010, s. 58). Aynı zamanda siber uzay; siber strateji, siber güvenlik, siber savunma, siber suçlar, siber zorbalık, siber istihbarat, siber terörizm ve siber savaş gibi faaliyetleri barındıran dört geleneksel kara, deniz, hava ve uzay alanına eşit olarak beşinci savaş alanını temsil etmektedir (Quadri & Rasaq, 2020, s. 105). Nitekim 8-9 Temmuz 2016 tarihlerinde düzenlenen NATO Varşova Zirvesinde siber uzay, havada, karada ve denizde olduğu kadar etkili bir şekilde savunulması gereken "operasyon alanı" olarak kabul edilmiştir (NATO [North Atlantic Treaty Organization], 2016).

Günümüzde, siber uzay teknolojileri dünya çapındaki hükümetler, kuruluşlar, işletmeler ve paydaşları tarafından, iş süreçlerini daha verimli hale getirmek, üretkenliği artırmak ve karlılığı optimize ederek ekonomik büyümeyi desteklemek için daha fazla benimsenmektedir. Dolayısıyla ekonomik büyümeyi, toplumsal refahı, etkileşimi ve küresel işbirliğini mümkün kılması yönünde yeni araçlar sağlayarak günümüz dünyasını olağanüstü şekillerde dönüştürmektedir (Mbanaso & Dandaura, 2015, s. 17).

Gelişmiş ve gelişmekte olan ulus devletler, terör ağları, bireyler, yatırımcılar, üniversiteler, şirketler ve diğer paydaşlar siber uzayın kullanımına öncelik vermektedir (Quadri & Rasaq, 2020, s. 98). Siber uzay teknolojileri, yenilikler, girişimler, sosyal ağlar için yeni bir odak noktası haline gelirken aynı zamanda siber güvenlik konuları da önem kazanmaya başlamıştır. Bilgi teknolojisine toplumsal olarak artan bağımlılık, siber suçlar içinde yeni bir odak noktası haline gelmesine neden olmuş ve bu durum, yenilik fırsatları sunarken güvenlik stratejilerinin de değişmesine sebep olmuştur.

Fiziksel alan, güvenlikle en çok ilişkilendirilen boyuttur. Kara, deniz veya uzay gibi fiziksel alanlar, egemen devlet hukukunun yargı yetkisi altındaki bölgelere

ayrılmıştır. Ancak siber uzay, düzeni sağlayabilecek merkezi bir otoritenin bulunmamasından kaynaklanan zorluklarla karşı karşıyadır (Sims, 2011). Sınırları belirsiz ve teorik olarak kimse tarafından yönetilemeyen siber uzayın, asimetrik doğası, atıfta bulunulamaması, düşük maliyeti, yasal belirsizliği, casusluk ve askeri saldırganlık için etkili bir ortam olması, ulus devletler, devlet dışı aktörler, devlet destekli gruplar ve bireylerden oluşan gruplar için çekici bir alan haline getirmektedir. Dolayısıyla siber uzayda fiziksel ve sanal bileşenler (teknoloji), insanlar ve süreçler arasındaki artan karşılıklı bağımlılık seviyesi, durmaksızın öngörülemeyen güvenlik açıkları, tehditleri ve riskleri ortaya çıkartmaktadır (Mbanaso & Dandaura, 2015, s. 20).

Sonuç olarak siber uzay özellikle insan, süreç ve teknoloji unsurları tarafından karakterize edilen, sıfırlar(0000) ve birler(1111) ile dolu bir alan olarak özetlenebilir. Siber uzayın fırsatları ve yenilikleri, tehditleri ve riskleri, çatışmaları ve savaşı, güvenlik açıklarını, hızla gelişen siber komploları, gelişmiş ve gelişmekte olan ülkeler arasındaki dijital eşitsizlik faktörlerini barındırması ülkelerin, şirketlerin ve bireylerin siber güvenlik algısını yeniden şekillendirmektedir. Dolayısıyla siber uzay, insanlığa büyük faydalar vaat eden, aynı zamanda bilgi alanı içinde ulusların üstünlük ve hakimiyet arayışından kaynaklanan tehlikeleri de içeren yeni bir dünya sahnesi sunmaktadır (Mbanaso & Dandaura, 2015, s. 18).

Anonimlik / Atıf Sorunu; Anonimlik, isimsiz kalmak veya ismini açıklamadan hareket etmektir (Nissenbaum, 1999). Siber uzay, diğer fiziksel alanlarla karşılaştırıldığında yüksek düzeyde anonimlik sağlamasıyla farklılık göstermektedir. İnternetin doğasından kaynaklanan anonimlik durumu, kullanıcının gizlilik hakkının ayrılmaz bir parçası olduğu için siber tehdit aktörlerinin eylemlerini kolaylaştırmaktadır. Siber tehdit aktörleri, bu etki alanında fiziksel konumlarını gizleyebilir, saldırının sorumluluğunu reddedebilir ve iz bırakmadan eylemlerini gerçekleştirebilir (Applegate, 2011, s. 16). Siber saldırıların arkasındaki kişiler, kuruluşlar veya hükümetler, atıftaki belirsizlikler ve sınırlamalar nedeniyle, bu tür siber operasyonlara katılımları reddederken, çıkarlarını ilerletmek için bir araç olarak siber operasyonları benimserler. Özellikle rakip ulus devletler hem hükümetlerin iç politikalarını etkilemek hem de finansal piyasalarını manipüle etmek için gerçekleştirdikleri siber saldırılarda anonimlik pelerininin arkasına saklanmakta veya vekiller kullanarak eylemlerini yürütmekte, siber araçlara ve tekniklere yatırım

yapmaktadır. Çoğu zaman ulus devletlerin siber saldırıları düzenlemek için siber vekiller kullanması, siber saldırıların kaynağın gizlemek için sıklıkla kullanılan bir taktiktir. Bu strateji saldırıda bulunan ulus devlete veya ulus devlet destekli siber tehdit aktörlerine makul bir inkar edilebilirlik sağlamaktadır (Canfil, 2016, s. 218).

Ağ saldırılarının kaynağı belirli bir coğrafi konuma kadar takip edilebilir olsa da, saldırıyı gerçekleştiren ve saldırıyı gerçekten kimin emrettiği arasında oluşan boşluk, saldırıyı atfetmenin bir başka zorluk katmanını oluşturmaktadır (Canfil, 2016, s. 220). Belirli bir olayı atfetmenin kesin bir yolu yoktur, bunun yerine kaynak bulma, saldırı verileri ve diğer istihbarat mekanizmalarının bir kombinasyonu yoluyla sonuca ulaşılabilir (Goel & Nussbaum, 2021, s. 1083).

Asimetri; Siber saldırı faaliyetlerinde failin, rakibe göre haksız veya asimetrik bir üstünlüğü vardır (Das, 2021). Siber uzaydaki faaliyetler, farklı statülere sahip aktörler arasında (ulus devlet veya devlet dışı aktörler) gerçekleşebileceği gibi siber yetenekleri eşit olmayan taraflar arasında da görülebilmektedir. Fiziksel boyutta baskın güce sahip aktörler, siber uzayda da aynı siber yeteneklere sahip olamamaktadır. Kritik altyapının stratejik bir faktör olarak öne çıktığı günümüz dünyasında, ekonomik ve askeri olarak yeterince güçlü olamayan ulus devletler veya devlet dışı aktörler, siber uzayı asimetrik bir boyutla etkin bir şekilde kullanabilme yeteneğine sahip olabilmektedirler (Çelik, 2018, s. 116). Dolayısıyla asimetri özelliği siber tehdit aktörlerine veya kinetik savaşta üstün gelemeyen küçük ulus devletler için bir avantaj sağlamaktadır.

Maliyet Faktörü ve Kolay Elde Edilebilmesi; Kinetik silahlar genellikle devletlerin orduları veya savunma sanayi tarafından üretilirken, dijital silahların inşası ve işletilmesi için gerekli teknolojiler devlet dışı aktörler ve bireyler tarafından kolayca elde edilebilir. Karmaşık endüstriyel süreçler ve pahalı malzemeler gerektirmediği için siber saldırı araçları inşa edilmesi kolay ve nispeten ucuzdur (Bussolati, 2015, s. 4). Bir siber tehdit aktörü minimum teknik ve operasyonel kaynaklarla ağlara sızabilir ve siber saldırı gerçekleştirebilir. Minimum başarısızlık şansı ile siber saldırılar, düşük bir finansal yatırım karşılığında yüksek getiri sağlayabilir (Sims, 2011).

Hızı; Işık hızında gerçekleşen siber saldırılar karşısında tepki vermek için çok az uyarı alınmakta ve ilk siber saldırı karşısında etkili bir savunma veya karşı saldırı

için çok az zaman tanınmaktadır. Bu durumda sadece otomatik bir siber savunma sistemi herhangi bir etki yaratacak kadar hızlı çalışabilir (Phillips, 2012).

Fiziksel Varlıkların Yokluğu; Bombalama eylemi veya insansız hava araçlarıyla ve iyi finanse edilmiş organizasyon ile gerçekleşen kinetik savaşta etkiler gözlemlenebilmekte, bir süre sonra ortaya çıkartılarak karşılık verilebilmektedir. Ancak siber uzayda gerçekleşen saldırı eylemlerinde, fiziksel materyallere veya uzmanlığa ihtiyaç duyulmamaktadır. Dolayısıyla görünmeyen ve kötüye kullanılması amaçlanan güvenlik açığı konusunda uyarı alınmadığı sürece, siber tehdit aktörlerinin gerçekleştireceği saldırıların gelişimini görmek, savunma gerçekleştirmek ve kaynağını belirlemek zor bir durumdur (Phillips, 2012).

Sınır Aşan; Siber saldırıların etkisi yerel gibi görünse de, bu müdahaleler ulusal sınırları geçme yeteneğine sahiptir. Saldırganların fiziki ortama bağlı olmadan herhangi bir yerden saldırı özgürlüğüne sahip olması, ulus devletlerin tek başlarına siber güvenliklerini sağlamasını da zorlaştırmaktadır.

Uluslararası Hukuktaki Güçlükler; Mevcut uluslararası hukuk normları, devlet faaliyetlerini yönetir ancak var olan uluslararası hukuk normlarının mevcut teknolojiye uygulanması, siber saldırıları önlemek veya yönetmek için yasal boşlukları ve zorlukları beraberinde getirmektedir. Ayrıca internetteki iletişim ve ticareti desteklemek amacıyla çeşitli uluslararası hukuk normları mevcut olsa da, bu normlar silahlı çatışma hukuku içerisinde yer almamaktadır. Uluslararası hukukun siber uzayda nasıl uygulanabileceğine dair farklı bakış açıları da, bu alanda anlaşma olasılığını zorlaştırmakta ve kötü niyetli aktörler tarafından istismar edilmek üzere yasal bir boşluk riski doğurmaktadır (Moynihan, 2020). Siber uzayın anonim yapısı, siber saldırıları işleyen saldırganların inkar edilebilirliğini artırması ve net bir atıfta bulunmadan failleri belirlemek veya sorumlu tutmak için uluslararası hukukta zorluklar oluşturmaktadır. İnternet, doğası gereği suç işlemeye elverişli bir ortamdır. Küresel erişimi, sınırları aşma ve geniş bir izleyicisi kitlesine ulaşma yeteneği, kullanıcıların anonimliği, ana ağ sistemlerinin dağıtımı ve değiştirilebilirliği, siber suçlular için avantajlar yaratmakta ve kanun uygulayıcı kurumlardan etkili bir şekilde saklanmalarına olanak tanımaktadır (Dziundziuk, 2011).

Aktör Çeşitliliği; Harp alanlarının aksine, siber alanda çok sayıda ilgili tehdit aktörü bulunmaktadır. Siber uzayın doğuşundan bu yana bireyler, gruplar ve ulus

devletler, sistemlerin güvenlik açıklarından yararlanmaya, kötü amaçlı yazılımları yaymaya ve verileri çalmaya çalışarak çeşitli önem ve etkiye sahip suçlara girişmektedirler (Pawlicka, Choras, & Pawlicki, 2021). Ulus devletler, artan bir oranda casusluk ve asimetrik saldırı operasyonları gibi ulusal güvenlikleri için yeni bir araç olarak siber uzayı kullanmaktadır. Ulus devletler, siber saldırılardaki en olası ana oyuncular gibi görünse de, benzer şekilde devlet dışı aktörler de bireyleri ve şirketleri olduğu kadar ulusları da tehdit eden siber faaliyetler yürütmek için siber uzayı kullanmaktadır (Corn & Taylor, 2017).

1.2. Siber Eylemler

1.2.1. Siber Suç & Siber Saldırı & Siber Savaş

Siber suç, siber saldırı, siber savaş, siber terörizm terimleri, neleri içermeleri gerektiği dikkate alınmadan sıklıkla kullanılmaktadır. Bu kavramlardaki net olmama durumu, anlamlı bir yasal durumun oluşturulmasını da zorlaştırmaktadır (Hathaway vd., 2012).

Tablo 1: Farklı siber eylemlerin temel özellikleri

	Siber suç	Siber Saldırı	Siber Savaş
Yalnızca devlet dışı aktörleri içerir	✓		
Bir bilgisayar sistemi aracılığıyla işlenen ceza hukuku ihlali olmalı	✓		
Amaç, bir bilgisayar ağının işlevini baltalamak olmalıdır		✓	✓
Siyasi veya ulusal güvenlik amacı olmalı		✓	✓
Etkiler "silahlı saldırı" ile eşdeğer olmalı veya silahlı çatışma bağlamında faaliyet gerçekleşmelidir			✓

Kaynakça: (Hathaway vd., 2012, s. 833)

Çalışmanın bu bölümünde sıkça birbirleriyle ilişkilendirilen siber suç, siber saldırı ve siber savaş kavramlarına yönelik görüşlerin kapsamlı incelemesini içermektedir.

Siber suç terimi için evrensel olarak üzerinde anlaşmaya varılmış bir tanımı bulunmamakla birlikte, "siber suç", "bilgisayar suçu", "ileri teknoloji suçu" terimleri genellikle birbirinin yerine kullanılmaktadır. Siber suç, analitik olarak siber saldırılardan farklı ve geniş yasa dışı faaliyet alanlarını kapsayan bir kavramdır. Özellikle siber suç, genellikle yasadışı bir eylemde bulunmak için teknolojinin kullanılması olarak anlaşılmaktadır. Siber saldırıların aksine, siber suçlar hedef bilgisayar ağını zayıflatmakta ve çoğu siyasi veya ulusal güvenlik amacı taşımamaktadır ve genellikle devletler tarafından değil bireyler tarafından işlenmektedir (Hathaway vd., 2012, s. 834).

Siber suç konusunu ele alma çabaları, 1990 yılında BM Genel Kurulunun bilgisayar suçları mevzuatıyla ilgili bir kararı kabul etmesiyle başlamıştır. Mevcut karar daha sonra 2000 ve 2002 yıllarında BM Genel Kurulu tarafından, bilgi teknolojisinin suç teşkil eden kötüye kullanılmasıyla mücadeleyle ilişkin bir karar alınmasıyla genişletilmiştir (Marco, 2010, s. 27). Tüm bu girişimler, ulus devletleri ceza yasalarını siber suçları ele alacak şekilde güncellemeye teşvik etmiştir. Örneğin 1996 yılında Rusya hükümeti, *Rusya Federasyonu Ceza Kanunu (Bölüm 28. Bilgisayar Alanındaki Suçlar)* içerisinde siber suçlar ve cezaları düzenlemiştir (The Criminal Code Of The Russian Federation , 1996).

Avrupa Konseyi Temmuz 2004'te siber suç konusunu ele alan ilk uluslararası sözleşme olan Siber Suçlar Sözleşmesini kabul etmiştir. Sözleşme, telif hakları ihlalleri, çevrimiçi dolandırıcılık, çevrimiçi korsanlık, çocuk pornografisi, ağ güvenliği ihlalleri, siber suçluların soruşturulması için uluslararası işbirliği standartları, bilgisayar ağlarının aranması ve müdahale gibi bir dizi prosedürleri içermektedir (Council of Europe [COE], 2004).

Avrupa Komisyonu siber suç terimini uygulamada, üç suç faaliyeti kategorisine göre ayırmaktadır (Commission of the European, 2007);

1. Elektronik iletişim ağları ve bilgi sistemleri üzerinden işlenen dolandırıcılık veya sahtecilik gibi geleneksel suç biçimleri,

2. Elektronik ortamda çocuklara yönelik cinsel istismar veya ırksal nefrete teşvik gibi yasa dışı içeriklerin yayınlanması ile ilişkili suç biçimleri,
3. Elektronik ağlara ve kritik altyapılara özgü ağ saldırıları, DDoS saldırıları, bilgisayar korsanlığı gibi suç biçimleri.

Siber saldırı kavramı, çeşitli yaklaşımlarla farklı şekillerde tanımlanmıştır. Tanımlarda siber saldırıların; ne durumda saldırı sayılabileceği, saldırıların ardındaki motivasyonlar, hedef üzerindeki saldırının etkisi, hedeflenen varlıkların bilgisayar sistemlerinin ve ağlarının olduğu, siber saldırılarda en az iki aktörün yer aldığını göstermektedir.

Siber saldırılar, bir devlet aktörü veya devlet dışı aktör tarafından siyasi veya ulusal güvenlik amacı gereksinimini karşılamakta ve etkileri silahlı saldırı düzeyine yükselmek kaydıyla, silahlı çatışma bağlamı dışında gerçekleştirilen saldırıları içermektedir (Hathaway vd., 2012, s. 836). Tablo 1'de görüleceği üzere, siber saldırı durumu, bir siber tehdit aktörünün bilgisayar ağı aracılığıyla yasa dışı bir eylemde bulunması, bilgisayar ağını baltalaması ve siyasi veya ulusal güvenlik amacına sahip olması durumunda ortaya çıkar.

Hathaway vd. (2012) göre siber saldırı, siyasi veya ulusal güvenlik amacıyla bir bilgisayar ağının işlevlerini baltalamak için yapılan herhangi bir eylemden oluşmaktadır. Libicki'e göre siber saldırı, bir devlet tarafından başka bir devleti ilgilendiren elektronik sistemin kasıtlı olarak kesintiye uğratılması veya tahrip edilmesidir (Libicki, 2009, s. 23). Owens, Dam ve Lin tarafından yapılan tanıma göre siber saldırı, düşman bilgisayar sistemlerini, ağlarını veya bu ağlardan geçen bilgi programlarını değiştirmek, bozmak, aldatmak, kalitesini düşürmek veya yok etmek için kasıtlı eylemlerin kullanılması anlamına gelmektedir (Owens, Dam, & Lin, 2009). Uma ve Ganapathi ise siber saldırı eylemini, güvenli bilgilere erişmek, casusluk yapmak, ağları devre dışı bırakmak, hem veri hem de para çalmak amacıyla siber uzayın yetkisizce kullanılması olarak tanımlamıştır (Uma & Ganapathi, 2013, s. 390).

Tallin Kılavuzunda ise siber saldırı, *"insanların yaralanmasına veya ölmesine, nesnelerde hasara veya tahribata yol açması makul olarak beklenen, saldırgan veya savunma amaçlı bir siber operasyon"* olarak tanımlanmıştır (Droege, 2012, s. 558). Bu tanıma göre belirli bir eşiğe ulaşmış siber operasyonlar, siber saldırı olarak

nitelendirilmektedir, ancak her siber operasyon siber saldırı olarak tanımlanmamaktadır.

Siber savaş kavramı birçok akademik makalelerde ve kitaplarda bilgi savaşı olarak nitelendirilmektedir. Ancak siber savaş kavramı geniş çapta tartışılan bir kavram olmakla birlikte uluslararası arenada kabul görmüş bir tanımı bulunmamaktadır.

"Siber saldırı" veya "siber savaş" terimleri, siber silahların kullanılmasını ifade etmektedir. Ancak "siber savaş" terimindeki belirsizlik, siber silahların tanımlanmasındaki eşit belirsizliğe ve "siber silah" kullanımının ne zaman bir "siber savaş" durumu yaratan "siber saldırı" olduğu konusunda bir tanım karışıklılığı yaratmaktadır (Brown & Metcalf, 2014, s. 114). Herhangi bir saldırı eyleminin savaş eylemi olarak nitelendirilebilmesi için evrensel kriterleri karşılaması gerekmektedir. Dolayısıyla siber uzayda veya sınırları belirli bir alanda yürütülen saldırı eylemi savaş olarak nitelendirilecek ise araçsal, politik ve ölümcül olma potansiyeline sahip olması gerekmektedir (Rid, 2012, s. 7). Bugüne kadar gerçekleştirilen siber operasyonlar ve siber saldırılar, savaş olarak nitelendirilebilecek uluslararası normları karşılamadığı için "siber savaş" kavramı tartışma düzeyinde kalmaktadır.

Siber savaş, her zaman siber saldırıların koşullarını karşılar. Ancak tüm siber saldırılar siber savaş değildir. Yalnızca bir silahlı saldırıya eşdeğer etkileri olan veya silahlı çatışma bağlamında meydana gelen siber saldırılar, siber savaş düzeyine yükselmektedir. Dolayısıyla siber savaş, siyasi veya ulusal güvenlik amacıyla, bir bilgisayar ağının işlevini baltalayan, savaş suçları gibi ceza kanunlarını ihlal eden ve bir bilgisayar sistemi aracılığıyla işlenen mevcut bir silahlı çatışma bağlamındaki saldırıları içermektedir (Hathaway vd., 2012, s. 836).

1.2.2. Siber Terörizm

1998 yılında 12 yaşındaki bir bilgisayar korsanı Arizona'daki Theodore Roosevelt Barajı'nın kapaklarını kontrol eden bilgisayar sistemine girmiştir. Barajın su tahliye kapaklarının açılması durumu, nüfusu bir milyondan fazla olan Tempe ve Mesa şehirlerini sular altında bırakabilme riskini taşımaktadır (Lemos, 2002). Bu vaka, "internet terörü", "bilgisayar terörü" ve "siber terörizm" gibi terimlerin ortaya çıkmasına ve bilgisayar sistemlerinin temel bileşenlerine dünyanın her yerinden erişilebilir olduğunu göstermiştir (Dziundziuk, 2011, s. 18).

Mark M. Pollitt (1998), siber terörizm kavramını "*bilgiye, bilgisayar sistemlerine, programlarına ve verilere karşı, alt ulusal gruplar veya gizli ajanlar tarafından savaş dışı hedeflere karşı şiddetle sonuçlanan, önceden tasarlanmış ve politik olarak motive edilmiş bir saldırı*" olarak tanımlamaktadır (Pollitt, 1998). Siber terörizm, kamu güvenliğini bozmak, halkı korkutmak ve askeri bir çatışmayı kışkırtmak amacıyla gerçekleştirildiği takdirde ciddi sonuçlar doğuran kasıtlı, politik olarak motive edilmiş bir saldırı olarak anlaşılabilmektedir (Dziundziuk, 2011, s. 19).

1.2.3. Siber İstihbarat ve Siber Casusluk

İstihbarat servisleri, şirketler, organizasyonlar ülkeleri için ekonomik, askeri veya siyasi avantaj elde etme amacını taşımaktadırlar. Bu doğrultuda siber casusluk, bireylerden, gruplardan, rakiplerden, hükümetlerden siyasi veya ekonomik kazanç elde etmek amacıyla ağırları, programlar aracılığıyla yasadışı teknikler kullanarak gizli bilgileri elde etmeyi amaçlayan bir eylem olarak tanımlanabilir (Liaropoulos, 2011, s. 131).

Casusluk, çağlar boyunca ulus devlet yönetiminde önemli bir faaliyet olmuştur. Ulus devletler genellikle istihbarat toplama amacıyla, çeşitli şekillerde stratejik hedeflere ulaşmak için siber uzayda, siber yeteneklerini kullanarak askeri faaliyetlerini gerçekleştirirler. Özellikle ulusal endüstrilere ve askeri programlara fayda sağlayan teknolojik bilgileri çalmak, hedef bir ülkedeki siyasi karar alma mekanizmasına ilişkin görünürlük kazanmak veya bunları koz olarak kullanmak adına siber casusluk faaliyeti yürütmek, bir rejimi veya hareketi finanse etmek için para çalmak, karar verme mekanizmasını etkilemek için siber destekli bilgi operasyonları yürütmek, bir düşmanı zayıflatmak için siber tehdit faaliyetlerinde bulunmaktadırlar (Accenture, 2019, s. 32).

Siber uzay, yüksek düzeyde anonimlik sağlar. Bu sebeple ulus devletler, bir siber savaş tanımını benimsemeye veya siber saldırılar için resmi olarak tanım sunmaya yönelik çok az teşvikte bulunmaktadır. Bu tür saldırılar, düşük maliyetle gerçekleştirilebilir ve bilgisayar korsanları, siber milisler veya siber paralı askerler aracılığı gizlice başlatabilir, finanse edebilir veya yönlendirebilir olduğu için ulus devletler saldırıyı gerçekleştirdiğinde çok az veya hiç yasal sonuçla karşılaşmadan ve Silahlı Çalışma Hukukuna bağlı kalma ihtiyacı olmaksızın potansiyel olarak siyasi hedeflerine ulaşabilirler (Applegate, 2011, s. 16).

1.2.4. Siber Güvenlik

Siber güvenlik terimi genellikle bilgi güvenliği terimi ile birbirinin yerine kullanılsa da, bu iki kavram esasında benzer değildir. Siber güvenlik, geleneksel bilgi güvenliğinin sınırlarını aşarak yalnızca bilgi kaynaklarının korunmasını değil, kişinin kendisi de dahil olmak üzere diğer varlıkların korunmasını içermektedir (Solms & Niekerk, 2013, s. 97). Siber güvenlik, siber uzayda kuruluşları ve kullanıcı varlıklarını korumak adına kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar, güvenceler ve teknolojilerin bütünü olarak tanımlanmaktadır. Kuruluşların ve kullanıcıların varlıkları ise bilgi işlem cihazlarını, personelleri, altyapıları, uygulamaları, telekomünikasyon sistemlerini, siber uzayda iletilen veya depolanan bilgilerin tümünü içermektedir. Siber güvenlik, siber uzayda var olan güvenlik risklerine karşı kuruluşların ve kullanıcı varlıklarının güvenliklerinin sürdürülmesini sağlamayı amaçlamaktadır (ITU, 2008). ITU - T X.1205 sayılı tavsiye kararında tanımlanan siber güvenliğin temel hedefleri ise bilginin erişilebilirliği, özgünlük ve inkar edilemezliği içeren bütünlük ve gizliliğini sağlamaktır.

Siber güvenliğin sağlanması konusunda yürütülen çalışmalarda 8 önemli ilkenin varlığı söz konusudur (Ünver, Canbay, & Mirzaoglu, 2009, s. 23):

1. Uluslararası sözleşmeler ile teminat altına alınmış temel insan hak ve özgürlüklerin korunması
2. Demokratik toplum düzeninin gereklerine uyulması
3. Tedbirlerin ölçülülük ilkesine göre belirlenmesi
4. Karar alma süreçlerinde tüm paydaşların katılımını sağlayacak kapsayıcı bir yaklaşımın belirlenmesi
5. Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi
6. Geliştirilecek çözümlerde güvenlik ve kullanılabilirlik arasında denge kurulması
7. Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olduğunca uyumluluğun sağlanması
8. Uluslararası işbirliğinin sağlanması

1.2.5. Siber Savunma

Siber saldırıların artması ve karmaşık yapısının genişlemesiyle birlikte, siber savunma, ulus devletler ve çoğu kuruluş için siber uzayda stratejik istikrarı ve uluslararası güvenliği sağlamak amacıyla öncelik verilen politikalar arasındadır. Siber savunma, özel kuruluşların ve devlet kurumlarının ağlarına yönelik gerçekleştirilen siber saldırı eylemlerini önleme, tespit etme ve zamanında müdahale etme yeteneğini, kritik altyapının veya bilgi güvenliğinin korunmasını içeren savunma yeteneğini ifade eder (Galinec, Moznik, & Guberina, 2017).

USCYBERCOM, siber savunma terimini operasyonel şekilde tanımlayarak "savunma amaçlı siber operasyonları" şu şekilde tanımlamıştır;

siber tehditleri ve güvenlik açıklarını tespit etmek, analiz etmek, karşı koymak ve azaltmak için eylemleri doğrudan yönlendirmek; saldırgan eylemlerde bulunan veya bulunmak üzere olan rakipleri geride bırakmak; ve ABD'nin siber uzayda hareket özgürlüğü sağlayan kritik misyonları başka bir şekilde korumak. Bu siber operasyon hattı, saldırgan siber uzay operasyonlarına yanıt olarak gerekli müdahale eylemlerini tetikleyebilir (United States Government Accountability Office [GAO], 2011).

1.2.6. Siber Caydırıcılık

Caydırıcı seçenekler doğası gereği aktif veya pasif olabilir. Martin Libicki'ye göre bu seçenekler "(1) inkar yoluyla caydırma (saldırıları engelleme yeteneği) ve (2) ceza yoluyla caydırma (misilleme tehdidi)" olarak tanımlanmaktadır. İnkâr yoluyla caydırma durumu siber perspektiften bakıldığında zaman pasif caydırıcılık olarak tanımlanmaktadır. Ağları saldırılara karşı korumak veya bir saldırının etkilerini en aza indiren esnek ağlar oluşturmak için yapılan eylemleri içermektedir. Ancak bu içerik siber saldırılara karşı aktif olarak caydırmada önemli bir rol oynamamaktadır. Alternatif olarak ceza yoluyla caydırma aktif caydırıcılıktır. Bir siber saldırıya misilleme veya istenmeyen bir yanıt verilmesini içermektedir (McKenzie, 2017).

Siber uzayda, bir düşmanı caydırmanın mümkün olup olmadığı ve nasıl caydırılacağı konusunda akademik bir fikir birliği yoktur. Siber uzayın küresel doğası, karmaşık yapısı, sınırlarının belirsizliği ve henüz olgunlaşmamış uluslararası yasal politikalar siber tehdit aktörlerinin anonim kalmasını, konumlarını gizlemesini ve herhangi birini taklit etmek için kullanabileceği güvenlik açıklarını mümkün kılmaktadır. Bu durum ise siber saldırılara karşı misilleme yapmayı zorlaştırmaktadır.

Libicki'ye göre siber caydırıcılık uygulanabilir. Ancak uygulanabilir olması için siber caydırıcılığı, nükleer caydırıcılıktan veya genel askeri caydırıcılıktan ayırt edecek, siber caydırıcılığın neden ve nasıl sorunlu olabileceğini ortaya koyan üçü asıl, altısı yardımcı olmak üzere dokuz soru ortaya konulmuştur:

Asıl sorular

- Kimin yaptığı biliniyor mu?
- Varlıkları risk altında tutulabilir mi ?
- Durum art arda tekrarlanabilir mi?

Yardımcı sorular

- Misilleme, caydırıcılığı sağlamazsa, en azından silahsızlandırmayı sağlar mı?
- Üçüncü taraflar savaşa katılır mı?
- Misilleme, kendi tarafımıza doğru mesajı verir mi ?
- Saldırıya karşı yanıt vermek için bir eşik var mı?
- Artış önlenebilir mi?
- Saldırgana vurmaya değecek bir değer yoksa ne olur?

Soğuk Savaş dönemindeki nükleer caydırıcılık için cevaplanabilmesi kolay olan asıl ve yardımcı soruların, siber caydırıcılık söz konusu olduğunda cevaplanabilmesi zorlaşmaktadır. Siber uzayda siber caydırıcılığın ve güvenliğin sağlanması bu sorunların cevaplanarak stratejilerin ve planlamaların oluşturularak eyleme dönüştürülmesini gerektirmektedir (Şenol, 2018, s. 211).

1.3. Siber Saldırı Araçları ve Yöntemleri

Küreselleşen ve dijitalleşen günümüz dünyasında kritik altyapılarda oluşabilecek herhangi bir siber güvenlik açığı, siber yeteneklerle bir silaha dönüştürülebilme potansiyeline sahiptir. Bu durum, geleneksel saldırılar veya savunma için gerekli silah üstünlüğü ile birlikte yanında siber uzayda da saldırı ve savunma amaçlı yazılım üstünlüğün de önemli hale geldiği göstermektedir. Devlet dışı aktörler, devlet aktörleri, istihbarat servisleri, teröristler veya bireyler gibi birçok aktör, bilgisayar virüsleri, truva atları, solucanlar ve gizli dinleme gibi yetkisiz bir şekilde

bilgi istismar araçlarını kullanarak bilgilerin bütünlüğünü yok edebilme, engelleyebilme ve bozabilme yeteneklerini hızla artırmaktadır.

Siber uzayın yarattığı tehdit ortamını anlayabilmek ve ayrıntılı bir kamu politikası oluşturmak için geliştirilen tüm kötü amaçlı yazılımların yapısını anlamak önemlidir (United States General Accounting Office [GAO], 2004, s. 5). Çalışmada tehdit yazılımları anlamaya yönelik modüler bir yaklaşımla ele alınan bu bölümde; en düşük ve en yüksek seviyede bazı siber saldırı araçları açıklanmıştır. Dağıtılmış hizmet reddi saldırıları-Servis Dışı Bırakma (DoSS-DoS), Virüsler (Viruses), Solucanlar (Worm), Truva Atı (Trojan Horses), Casus Yazılımlar (Spyware), Zombi Bilgisayar Orduları (botnetler), Kök kullanıcı takımı (Rootkit), Mantık Bombaları (Logic Bombs - Time Bombs), Fidyeye yazılımları (Ransomware), Klavye İşlemlerini Kaydeden Programlar (Key loggers), IP Aldatmacası / Gizlenmesi (IP Spoofing), Arka Kapı Açıkları (Back Door), Ortadaki Adam (Man in the Middle Attack), Gelişmiş Kalıcı Tehditler (Advanced Persistent Threats - APT), Kaba Kuvvet Saldırıları (Brute Force), Sosyal Mühendislik (Social Engineering), Kimlik Avı/Yemleme/Oltalama (Phishing), İstem Dışı Elektronik Postalar (Spam E-mail), Yapay Zeka (AI) Destekli Siber Saldırıları, Şebeke Trafiğinin Dinlenmesi (Sniffing/Eavesdropping), SQL Injection (SQL Enjeksiyonu), Kripto Hırsızlığı (Cryptojacking), gibi bilgi güvenliğini tehdit eden siber saldırı araçları ve terimleri mevcuttur. Amaçları kullanıcıları uzaktan gözetleme, dosyaları silerek verileri yok etme, fiziksel ekipmanlara zarar verme ve ağ kaynaklarını tüketmek için geliştirilmiş bu yazılım ve programlar genel olarak Kötü Amaçlı Yazılımlar (Malware) olarak bilinmektedir.

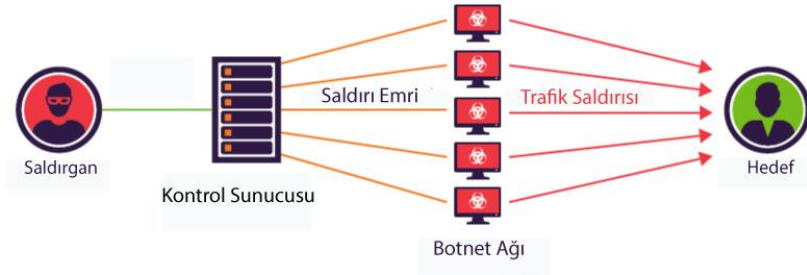
Siber saldırı araçları ve siber teknikler "silah" olarak kabul edilebilir mi? Sürekli gelişim gösteren bilgi ve teknoloji alanında yazılım ve donanım programlarının 'silah' olarak sınıflandırılabilmesi konusunda konvansiyonel silah sistemlerinde olduğu gibi resmi bir açıklık getirilememiştir (Çelik, 2013, s. 141). Dijital silahlar ve fiziksel silahlar arasındaki benzerlik belirsiz olduğu için bilgi sistemlerini yok etmeye veya bozmaya yönelik saldırılarda sonucun nasıl olacağı konusunda tartışmalar vardır. Aslında "siber silahlar" popüler kültürün bir parçası haline gelse de siber uzayda "silahı" neyin oluşturduğuna dair uluslararası arenada çok az fikir birliği vardır (Brown & Metcalf, 2014, s. 137). Savaş ve silah gibi kavramlar hukuk ve kamu politikası için büyük öneme sahiptir ve siber silahların tanımının yapılabilmesi için teknik bir temel bulunması gerekir. Bu nedenle mevcut uluslararası normların siber uzaya

uygulanamaması, kısmen bu yeni teknolojik alanda mevcut yasal kavramlar için uygulanabilir tanımların bulunamamasının bir sonucudur (Herr, 2014, s. 97).

Siber saldırı tekniklerinin, bilgisayar sistemlerine, ağlara veya dijital altyapıya zarar verme amacıyla tasarlandığı ve bireyler, kuruluşlar, devlet aktörleri tarafından hedeflerine karşı kullanıldığı vakalar mevcuttur. Siber saldırıların etkisi, finansal kayıplara, hassas verilerin ele geçirilmesine, kritik hizmetlerin aksamasına ve hatta bazı durumlarda fiziksel hasara kadar değişen önemli etkiler doğurmaktadır. Bu nedenle, siber saldırı araçları ve teknikleri zarar verme potansiyeli ve savunma önlemlerine duyulan ihtiyaç nedeniyle "silah" olarak sınıflandırılabilir.

1.3.1. Dağıtılmış Hizmet Reddi Saldırıları

DDoS saldırıları, bir web sitesini sağlayan altyapı gibi, herhangi bir ağ kaynağı için geçerli olan belirli bir kapasite sınırlarından faydalanır. Bir hedefe yönelik büyük miktarda istek göndererek web sitesinin sistemin kapasite sınırını aşmasını ve doğru şekilde çalışmasını engellemeyi amaçlar (Kaspersky, tarih yok(b)).



Şekil 1: DDoS Saldırısı

Kaynak: <https://www.mehmeteminsoylu.com/wordpress-te-ddos-saldirisi-nasil-engellenir/>

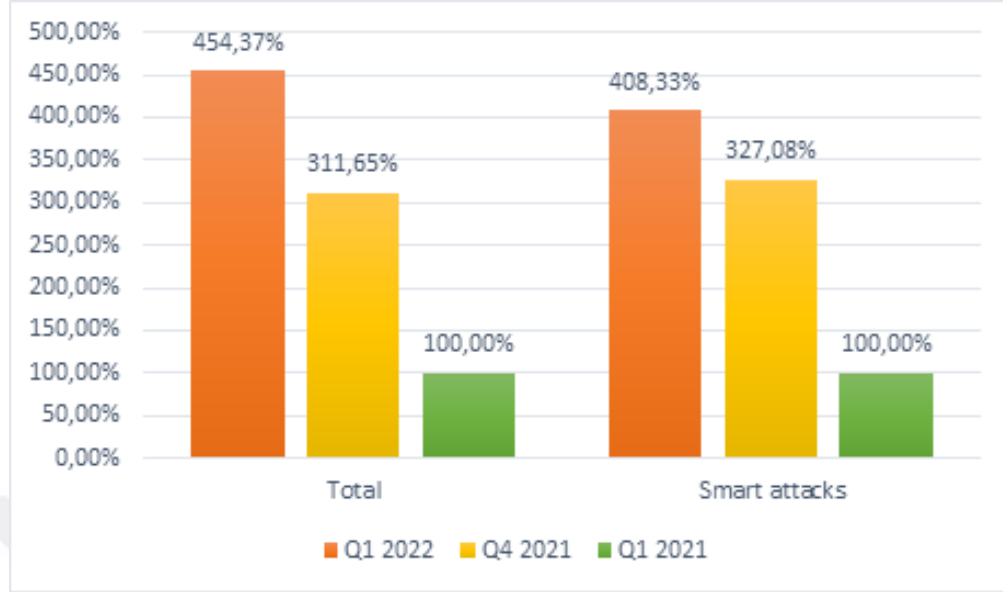
1980'li yıllarda amatör bilgisayar korsanları tarafından oyun amacı ile gerçekleştirilen DDoS saldırıları, 1990'lı yıllarda elektronik ticaret şirketlerine yönelik maddi kazanç elde etme amacıyla kullanılmış ve 2000'li yıllarda ulusal ve uluslararası güvenliğe tehdit olacak şekilde saldırı aracı olarak kullanılmaya başlanmıştır (Atasever, Özçelik, & Sağiroğlu, 2019). İstatistiklere göre saldırganlar tarafından her

geçen yıl giderek daha fazla kullanılan ve maliyet açısından düşük olan DDoS saldırıları, özellikle finansal ve devlet hizmetleri olmak üzere hastaneler, savunma sistemleri, ulaşım, hava trafik kontrolü, nükleer santraller, elektrik ve su gibi birçok internete bağlı sistemler için tehdit oluşturmakta ve ciddi finansal kayıplarla sonuçlanabilmektedir (Edwards, 2006, s. 35).

Rusya merkezli güvenlik şirketi olan Kaspersky'nin 2021'in dördüncü çeyreğinde sistemlerinde kaydedilen 86.710 DDoS saldırıları sonucunda sunduğu rapora göre ABD (%43,55), Çin (%9,96), Hong Kong (%8,80), Almanya (%4,85) ve Fransa (%3,75) oranlarında saldırılarda artış tespit edilmiştir (Kaspersky, 2022). (2022 güncel verilerine bakılacak) Gerçekleşen bu artış 2021'in üçüncü çeyreğine kıyasla toplam %52 orandadır. Her yılın son üç ayında DDoS saldırılarından bir artış gözlemlenmektedir.

2021'in ilk çeyreğine kıyasla, 2022'nin ilk dönemleri DDoS saldırılarının sayısı 4,5 kat artmıştır (Kaspersky, 2022a). Bu oranı ise Rusya ve Ukrayna arasında devam eden çatışma tarafından şekillenmiş ve jeopolitik durumun etkisiyle tüm zamanların en yüksek DDoS saldırısına tanık olmuştur. DDoS saldırıları, Ukrayna'nın veya Rusya'nın savaş kazanmasına yardımcı olmamıştır, ancak web sitelerini çevrim dışı hale getirmek siber uzayda saldırmanın en kolay yollarından biridir.

Şekil 2: DDoS saldırılarının karşılaştırmalı sayısı 2022'nin 1. çeyreği, 2021 4. çeyreği, 2022'nin 1. çeyreği



Kaynak: Kaspersky. (2022a). Cyberwar in Ukraine leads to all-time-high levels of DDoS attacks. https://www.kaspersky.com/about/press-releases/2022_cyberwar-in-ukraine-leads-to-all-time-high-levels-of-ddos-attacks

2022 Ocak ayında Kiev Belediye Başkanı Vitali Klitschko'nun resmi web sitesi (kyiv.klichko.org) Rusya topraklarından gelen bir DDoS saldırısına uğradığı açıklanmıştır (Interfax Ukraine, 2022). 2022 Şubat ayında ise Ukrayna Savunma Bakanlığı, Dışişleri Bakanlığı, Eğitim ve Bilim Bakanlıklarının da bulunduğu 70 hükümet web sitesine yönelik DDoS saldırıları gerçekleştirilmiştir. Ukrayna Dijital Dönüşüm Bakanlığı ise saldırıdan Rusya'yı sorumlu tutmuştur. Hükümet web sitelerine ek olarak birkaç devlet dairesinin, bankanın, radyo istasyonunun web siteleri DDoS saldırıları ile birkaç saatliğine devre dışı bırakılmıştır (Przetacznik & Tarpova, 2022, s.3). Mayıs 2022'de bilgisayar korsanları çevrimiçi trafiği filtrelemek ve işgal altındaki bölgelere yeniden yönlendirmek için Ukrayna'nın bazı telekom operatörlerine DDoS saldırısı başlatmıştır (Securelist, 2022).

Ukraynalı bir siber güvenlik danışmanlık şirketi olan Hacken'in CEO'su Dyma Budorin, Rus web sitelerinde DDoS saldırılarını otomatik olarak etkinleştiren ve herhangi bir teknik bilgiye ihtiyaç duyulmadan çalıştırılabilen Liberator adlı bir bilgisayar uygulaması başlatmıştır. Savaş başladığında birçok Ukraynalı vatandaş sığınaklarına saklanarak bu uygulama ile Rus web sitelerine yönelik DDoS saldırıları gerçekleştirebilmiştir (Antoniuk, 2022).

2022'nin üçüncü çeyreğinde ise Ukrayna ve Rusya odaklı bir siber savaştan Avrupa çağında yüksek yoğunluklu hibrit bir siber savaş gözlemlenmiştir. Çatışmanın başlangıcından bu yana geçen bir sene içerisinde dünya çapında bildirilen tüm siber saldırıların %61'i Rus yanlısı bilgisayar korsanları tarafından gerçekleştirilmiş ve bu saldırılar özellikle Polonya, Baltık ve İskandinav ülkelerini hedeflemiştir (Thales, 2023).

1.3.2. Virüsler

Virüsler kullanıcının farkına varmadan gerçekleştirdiği bir takım eylemler sonucunda sisteme zarar vermek amacıyla bulaşmaktadır. Örneğin virüs yerleştirilmiş bir e-postanın açılmasıyla, CD ya da DVD gibi donanım araçlarıyla, indirilen bir program veya açılan bir link aracılığıyla, aktif bir işletim sistemi üzerinden kendi kendine çoğalan ve yayılan programlardır (McAfee, tarih yok). Virüs bulaşmış sistemlerde; işlemleri devre dışı bırakabilir, dosyaları silebilir ve sistemi kapatmak için komutlar verebilir.

1.3.3. Solucanlar

1988'de Robert Morris tarafından internetin boyutunu ölçmek amacıyla tasarlanan ve piyasaya sürülen "Morris Solucanı" tarihte bilinen ilk örneklerden biridir (Spafford, 1989, s. 40). Ancak çoğaltma kodundaki bir hata nedeniyle solucan beklenenden çok daha hızlı yayılmış, ağda yaygın bir kesintiye ve tıkanıklığa neden olarak hizmet reddi (DoS) durumuna sebep olmuş ve internete bağlı çok sayıda bilgisayarı etkilemiştir. Sonuç olarak solucanlar, kendi kendini kopyalayarak çoğalma özelliğine sahiptir. Bu nedenle kendisini ağ bağlantısı üzerinden birçok kez kopyalayarak dağıtan solucanlar, ağ trafiğinde yoğunlaşarak yavaşlamasına sebep olabilir ve ağdaki korunmasız bilgisayarları etkiler (Yalman, 2018, s. 261).

Birçok solucan HTTP, Net BIOS, FTP ve e-posta yöntemleri gibi popüler ağ hizmetlerindeki güvenlik açıklarını hedefler veya sistemleri izinsiz girişlerden koruyan parolaları tahmin etmeye çalışarak diğer sistemlere bulaşabilirler. Örneğin e-posta solucanları, solucanın bir kopyasını içeren eki indirmeye ikna edilmiş şekilde tasarlanmış bir mesaj göndererek yayılır. Bu tür kötü amaçlı yazılımın ünlü bir örneği

2000'de binlerce bilgisayara yayılmaya başlayan "ILOVEYOU" solucanıdır. 2003'te adı duyulan Blaster solucanı ise, Microsoft Windows RPC arabirimindeki güvenlik açığı sebebiyle yayılan ve Microsoft'u büyük oranda etkileyen bir ağ solucanıdır (Graham, Howard, & Olson, 2011, s. 196). İki tür kötü amaçlı yazılım olan solucanlar ve virüsler yayılmak için oluşturulmuştur, ancak solucanlar virüslerden farklı olarak kullanıcıya gerek duymadan -kullanıcının dosyaya veya bağlantıyı açmasına gerek kalmadan- kendi başına çalışabilir.

1.3.4. Truva Atı

Kendilerini kopyalayabilen, bilgi çalabilen, ana bilgisayar sistemlerine zarar verebilen, bir bilgisayar korsanının hedef bilgisayar sistemine uzaktan erişmesine izin verebilen ve otomatik bir şekilde hareket eden kötü amaçlı programlardır (Cavelty, 2012, s.120). Genellikle kullanıcıların yürütmek isteyeceği yararlı bir program gibi görünür. Ancak yararlı görünüme sahip program, çalıştırıldıktan sonra sistemi etkilemeye başlar ve güvenlik tehdidiyle sonuçlanır. Çoğu zaman kullanıcılar sistemde, saldırganlar için daha önce mevcut olmayan ve izin verilmemiş erişimleri sağlayan 'arka kapı' erişimi açarak siber tehdit aktörlerinin sisteme uzaktan yetkisiz şekilde erişim sağlamalarını ve bilgileri çalmalarını kolaylaştırabilir (Sinopoli, 2012, s. 29). Ayrıca Truva atı virüsleri, virüsler ve solucanlar için bir dağıtım mekanizmasıdır (Edwards, 2006, s. 26).

1.3.5. Casus Yazılımlar

Truva atları gibi kullanıcının izni ve bilgisi olmadan, bir kullanıcının etkinliğini izleme ve bilgilerini toplama amacı taşıyan kötü amaçlı yazılımlardır. Casus yazılım bulaşmış sistemlerden çalınan bilgiler; şifreler, form verileri, e-posta adresleri, kimlik bilgileri, banka hesap bilgileri, bağlı Web kameralarından alınan resimleri ve videoları, bağlı mikrofondan gelen sesleri, özel belgeleri, yazılım lisanslarını ve ağ etkinliği bilgilerini içerebilir (Graham, Howard, & Olson, 2011, s. 224). Bu tür yazılımları üreten firmalar tarafından istihbarat-misyon sistemi olarak da nitelendirilir ve fark edilmeden hedef bilgisayarlarda çalışarak amacına ulaştıktan sonra iz bırakmadan kendini imha eder (Çahmutoğlu, 2020, s. 12). Genellikle ücretsiz reklam yazılımı veya

indirilen deneme sürümleri içerisinde yer alır ve kullanıcı bu ücretsiz yazılım türünü, programı veya uygulamayı yüklediğinde casus yazılım kullanıcının sistemine bilgisi dışında kurulur. Bu tür yazılımlar sisteme yüklendiğinde kullanıcıya sunulan uyarılar, Son Kullanıcı Lisans Sözleşmesi (SKLA) veya gizlilik politikası içerisinde yer almaktadır. Ancak bu politikalar birçok terimin yer alması sebebiyle dikkat edilmemekte ve okunmadan kabul edilmektedir (Öğün & Kaya, 2013, s. 158).

1.3.6. Zombi Bilgisayar Orduları

Robot ve ağ kelimelerinden türetilen ve zombi ordusu olarak da adlandırılan Botnet'ler güvenliği ihlal edilmiş sunucuları, mobil cihazları veya bilgisayarları içeren internete bağlı cihazlardan oluşmaktadır. Kullanıcıların bilgisi dışında, bilgisayarlarını zombi bilgisayara çeviren ve çok sayıda bilgisayarı etkilemek için kullanılan botlar, tehdit aktörleri tarafından uzaktan kontrol edilmekte, dağıtılmakta ve sistem kullanıcının haberi olmadan ve gizlenerek ağ üzerinden otomatik olarak bazı görevleri yerine getirmektedir. Genellikle veri hırsızlığı, sunucu çökmesi, istenmeyen e-postalar gönderme ve kötü amaçlı yazılım dağıtımı, tıklama sahtekarlığı kampanyalarına katılmak gibi toplu saldırıları otomatikleştirmek için bir araç görevi görür (Kaspersky, tarih yok(c)).

Örneğin 2007 yılında bilgi güvenliği tarihinde en çok bilinen kötü amaçlı yazılımlardan biri Zeus veya Zbot olarak bilinen yazılım, virüslü cihazların kullanıcılarından kimlik bilgilerini ve finansal bilgilerini toplamak için kullanılmıştır. Veriler toplandıktan sonra ise siber tehdit aktörleri, Zeus'u daha olası kurbanlara yayan spam ve kimlik avı e-postaları göndermek için botları kullanmıştır. 2009 yılında ise siber güvenlik satıcısı olan Damballa, Zbot'un 3,6 milyon ana bilgisayara bulaştığını tahmin ederken, 2010'da FBI Zbot kampanyasının arkasında olduğundan şüphelenilen bir grup Doğu Avrupalı tehdit aktörlerini tespit etmiştir (Hanna, Lutkevich, & Rob, Botnet, 2021). Zbot sonraki yıllarda ise yeni sürümlerle tekrar ortaya çıkmıştır. 2016 yılında Methbot olarak bilinen yazılım ise genellikle ABD ve Hollanda'da bulunan veri merkezlerinde yaklaşık 800 ila 1200 özel sunucuda çalıştırılarak, çevrimiçi reklamlar için sahte tıklamalar ve video reklamlarının sahte görünümüleri üreterek günlük 3 milyon ila 5 milyon dolar arasında sahte reklam geliri elde etmekteydi (GreenArrow, tarih yok).

1.3.7. Kök Kullanıcı Takımı

Rootkit terimi, UNIX işletim sistemlerinde ana yönetici hesabına atıfta bulunmak için kullanılmaktadır (Symantec, tarih yok). Arka planda çalışan programları temsil eden kök kullanıcı takımlarında, yetkisiz bir kullanıcı erişim sağladığı sistemde varlığını gizlemekte ve yetkili kullanıcıların güvenlik ihlalinin keşfetmesini engellemektedir. Kök kullanıcı takımında bulunan araçlar arasında, siber tehdit aktörlerinin eylemlerini gizlemek ve saldırının izlerini temizlemek için kayıt girdilerini silen araçlar ve aktörün sisteme daha sonra erişim sağlamak için arka kapılan oluşturan araçlar yer almaktadır (Canbek & Sağiroğlu, 2013, s. 127). Rootkitler kendisi ile birlikte sisteme giren zararlı yazılımları, güvenlik uygulamalarında gizleyebilmesi ve donanımları dahil etkileyebilme seviyesinde olması sebebiyle yapı olarak güçlü ve zararlı bir yazılımdır. Dolayısıyla anti virüs programlarını potansiyel olarak atlama yeteneğine sahip ve sürekli gelişen Rootkit gibi araçların varlığı nedeniyle kötü amaçlı yazılımlar daha karmaşık hale gelmektedir.

1.3.8. Mantık Bombaları

Mantık bombaları, tetikleyici bir olay meydana geldiğinde veya belirli bir zamanda programcının, programın yıkıcı bir eylem gerçekleştirmesine neden olan kodu eklediği bir sabotaj biçimidir (GAO, 2004, s. 5). Daha uygun bir örnekte, bir çatışma sırasında bir devlet tarafından, hedef devletin askeri bilgi altyapısına Mantık Bombaları yerleştirebilmesi, hedef devletin askeri olarak yeteneklerini sakatlayabilir (Borah, 2015, s. 459). Kötü amaçlı bilgisayar kodunun başlaması için ayarlanan zaman veya durum sonucunda veriler ele geçirilebilir, yok edilebilir veya kullanılamaz hale getirilebilir. Saatli Bomba olarak da adlandırılan Mantık Bombaları belirlenen zaman veya duruma kadar gizli kalabilmektedir. Ne tür zarar vermek üzere kodlandığı bilinmemekte ve saldırı stratejisinin bir parçası olarak virüs ve solucanları içerebilmektedir. Örneğin Siemens'te elektronik tablo yazılımı sağlayan David Tinley, elektronik tablolardan birine bir mantık bombası yerleştirmiştir. Plan ise kodlanmış mantıksal koşul her sağlandığında, yazılım arıza yapacak ve Tinley onu düzeltmek için çağrılacaktı. Bilgi Teknoloji ekibi tarafından keşfedilen bu durum yaklaşık iki yıl

sürmüştür (AVAST, tarih yok). Belirli bir saatte meydana gelmesine verilebilecek bir örnek ise 1998'de yayılan ve zamanın en yıkıcı kötü amaçlı yazılım saldırı olarak görülen Güney Doğu Asya kökenli Çernobil (CIH) virüsü, Çernobil Faciasının gerçekleştiği tarih olan 26 Nisan'da aktif duruma geçmektedir (Hanna, 2021).

1.3.9. Fidyeye yazılımları

Günümüzde çok sık kullanılan fidye yazılımları bireyler, özel şirketler, kamu kurumları ve ulus devletler olmak üzere tüm kullanıcıları tehdit eden ve gasp için kullanılan bir tehdit haline gelmiştir. Saldırıya uğrayan sistemdeki dosyalar; şifrelenmekte, erişimi engellenmekte ve kullanıcıdan belirtilen süre içinde ödemesi için fidye talep edilmektedir. Tarihte belgelenen ilk fidye yazılımı vakası ise 1989'da e-posta yoluyla dağıtılan AIDS Truva Atı olarak bilinen yazılımdır. Siber tehdit aktörü, kullanıcıların diske erişimini engelleyerek, 189 doların Panama'da belirtilen bir postane kutusuna gönderilmesini talep etmiştir (ESET, tarih yok).

2016 yılında kullanılan virüslü eklere sahip sahte e-postalar ile yayılan Locky, 2017 yılında güvenli olmayan web siteleri aracılığıyla yayılan Bad Rabbit, 2007 yılında 500.00 bilgisayarı etkileyen CryptoLocker, 2016 yılında ortaya çıkan ve kurbanın tüm sabit diskini şifreleyen Petya, 2014 yılında ortaya çıkarak 325 milyon dolar kayba sebep olan CryptoWall, 2017'de 150'den fazla ülkeye yayılan ve Birleşik Krallık'taki devlet hastanelerinin üçte birine saldırarak 92 milyon poundluk hasara sebep olan WannaCry fidye yazılımı örnek olarak verilebilir (Kaspersky, tarih yok(d)).

Türkiye'de ise Crytolocker virüsü en çok görülen fidye yazılımıdır. Genellikle e-fatura içeren sahte mailler yoluyla yayılmakta, kullanıcıların dikkatini çekmek için fatura tutarları yüksek gösterilmekte ve kullanıcıya gönderilen maildeki linke tıklamaya yönlendirilerek ".zip" uzantılı dosyanın indirilmesi sağlanmaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı [UAB], tarih yok).

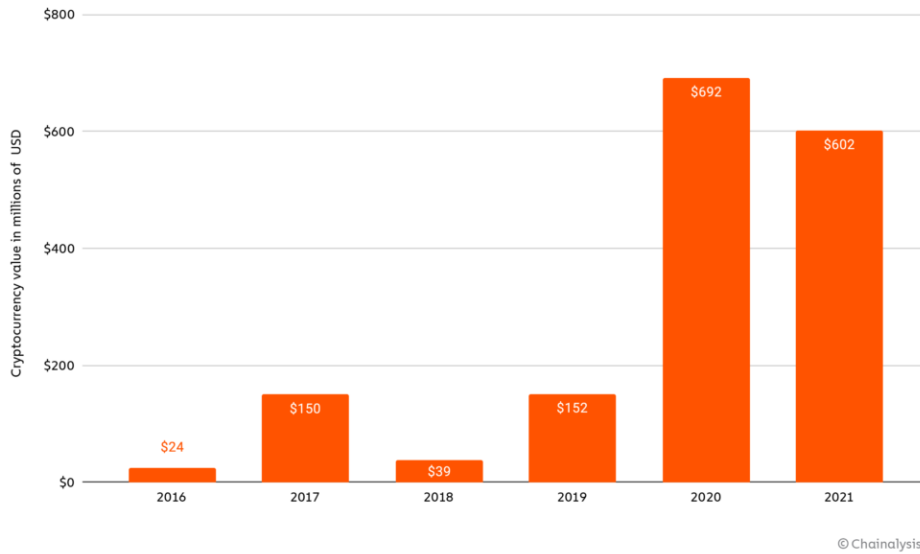
Fidye yazılımları, jeopolitik hedefler doğrultusunda aldatma, casusluk, itibar zedelenmesi, rakip devletin operasyonlarını aksatmaya yönelik kullanılmaktadır. Örneğin Ukrayna Bilgisayar Acil Müdahale Ekibinin (CERT-UA) 13 Ocak 2022'de yaptığı açıklamaya göre Rus hükümeti ile bağlantısının olduğu düşünülen bilgisayar

korsanları tarafından birkaç devlet kurumunun çalışma yeteneğini sekteye uğratılmıştır (CERT-UA, 2022).

Microsoft Tehdit İstihbarat Merkezi (MSTIC) analistleri CyberWarCon, 2021'de "*İran'ın evrimi: İran'ın kötü niyetli ağ operasyonlarında gözlemlenen değişiklikler*" başlıklı oturumunda İran merkezli kötü niyetli ağ operatörleri tarafından kullanılan araçların, tekniklerin ve prosedürlerin kademeli olarak geliştiğinin analizi sunulmuştur (Microsoft, 2021) (Cyberwarcon, 2021). Amerikan güvenlik şirketi CrowdStrike ve Microsoft'taki siber güvenlik analistleri, çoğunlukla ABD, AB ve İsrail'deki kuruluşları hedef alan, İran ile bağlantılı fidye yazılım türlerinin gerçekleştiği bir çok saldırıda, daha çok aksatma ve casusluk faaliyetleri yürüttüğü sonucuna varmıştır.

Tayvanlı yetkililer ise, 2020 yılında ada ulusunun stratejik varlıklarından biri olan Tayvan'ın devlet petrol şirketine yönelik fidye yazılım saldırısının arkasında Winnti olarak bilinen Çinli bilgisayar korsanlarının olduğunu öne sürmüşlerdir (Lyngaas, 2020). Sonuç olarak fidye yazılımları, maliyeti düşük olduğu için rakip devletlere karşı stratejik bir saldırı yöntemi olarak kullanılmaktadır.

Şekil 3: 2016-2021 yılları arasında fidye yazılım saldırıları ile alınan toplam kripto para değerleri



Kaynak: Chainalysis. (2022). As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict. <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/>

Blockchain analiz şirketi Chainalysis, yazılım saldırılarında gasp edilen kripto para birimindeki büyüme sebebiyle 2020 yılını "Fidye Yazılım Yılı" olarak kabul etmiştir. Chainalysis'in sunduğu analize göre, 2021'de 602 milyon dolar fidye yazılımı ödemesi tespit edilmiştir (Chainalysis, 2022).

Rusya merkezli olduğuna inanılan Conti, 2021 yılında sürekli olarak aktif kalan ve en az 180 milyon dolar şantaj yaparak gelir açısından en büyük fidye yazılım türü olarak belirlenmiştir (Chainalysis, 2022). DarkSide ise 2021'in ikinci yarısında 4,4 milyon dolar ödeme aldığı, petrol boru hattı Colonial Pipeline'a yapılan ve bazı bölgelerde yakıt kıtlığına sebep olan saldırıdaki rolü açısından ikinci sırada yer alan dikkate değer bir fidye yazılımı olarak tespit edilmiştir (Chang, 2021).

Colonial Pipeline'a yönelik gerçekleştirilen siber saldırıdan birkaç hafta sonra ABD'nin en büyük sigorta şirketlerinden biri olan CNA Financial'e yönelik gerçekleştirilen fidye yazılım saldırısı, şirket tarihindeki en büyük siber saldırı olarak kaydedilmiştir. Bloomberg'de Kartikay Mehrotra ve William Turton'un raporuna göre CNA Financial ağına, Mart 2021 tarihinde bilgisayar korsanları tarafından eşirim engellenerek verileri çalınmıştır. CNA, 60 milyon dolar talep edilen fidye yazılımı saldırısı sonrasında yaptığı pazarlık ile 40 milyon dolar ödeme sağladığı bilinmektedir (Chang, 2021).

1.3.10. Klavye İşlemlerini Kaydeden Programlar

Keylogger'lar kullanıcıların gizliliği için tehdit oluşturan, tuş vuruşlarını kaydeden ve bilgisayar etkinliğini gizlice izleyen özel bir yazılım ve donanımdır. Fiziksel erişim sağlayarak ya da indirilen programlar aracılığıyla kurulan bu program, bellek ve işlemci kullanımı açısından az yer kaplaması nedeniyle programı izlenemez duruma getirmektedir (Subramanyam, Frank, & Galli, 2007). Özellikle bankacılık işlemleri adına ciddi bir tehdit oluşturan yazılım, bilgisayar ve ATM tuşlarına klavye veya bağlantı noktasında harici bir ek olarak da yerleştirilebilmektedir. Bankacılık işlemleri dışında online oyunlar, sosyal medya hesapları veya e-postalara yönelik kullanılan bu zararlı yazılım, kullanıcıların özel hayat gizliliğinin ihlali konusunda da güvenlik zafiyeti oluşturmaktadır.

Klavye işlemlerini kaydeden programların kurumlar ve kişiler için yasal etik veya rıza dışı olarak belirsiz kullanımları da mevcuttur. Çocukların çevrimiçi ve sosyal etkinliklerini korumak adına ebeveyn denetimi, hile kanıtı için kullanıcının sahip olduğu bir cihazda etkinlik toplayabilmek ve şirkette çalışanların üretkenliklerini izleyebilmek için kullanımlar örnek olarak verilebilir (Kaspersky, tarih yok(e)).

1.3.11. IP Aldatmacası veya Gizlenmesi

İnternet kullanıcılarının sanal ağdaki kimliği IP (Internet Protocol Address) adresi ile belirlenmektedir. Özellikle DDoS saldırılarının kaynağını gizlemek için kullanılan saldırılar, bir bilgisayarın IP adresini maskeleyen eylemdir ve orijinal görünmektedir. Siber suçluların tespit edilemeden cihazlara kötü amaçlı yazılım bulaştırmasını ya da verilerin çalışmasını içeren bu saldırı türünde, başka bir bilgisayar sisteminin kimliğine bürünmek ya da gönderenin kimliğini gizlemek için yanlış ya da değiştirilmiş bir IP adresiyle İnternet Protokolü (IP) paketleri oluşturulur. Saldırgan, alıcı bilgisayar sisteminin paketin meşru bir ağdaki başka bir bilgisayar gibi güvenilir bir kaynaktan geldiğini düşünmesini ve kabul etmesini sağlamak için paket başlığındaki kaynak adresini değiştirmek için ağ düzeyinde araçlar kullanır (Kaspersky, 2022b).

1.3.12. Arka Kapı Açıkları

Arka Kapılar, yazılım firması tarafından oluşturulan yazılımda yaptığı hatalar ile sistemde açıklık olarak var olabilir ya da saldırganlar tarafından çeşitli yöntemler ile sisteme yerleştirilebilir. Arka Kapılar aynı zamanda ulus devletlerin istihbarat veya güvenlik birimlerinin emri doğrultusunda Microsoft gibi işletim sistemi üreticisi şirketler tarafından casusluk faaliyetleri amacıyla oluşturulabilir. Bu konuda dikkate değer bir iddia, NSA'nın Windows işletim sisteminin çeşitli sürümlerinde bir arka kapı oluşturulmasına karıştığı iddiasıdır (Canbek & Sağiroğlu, 2013, s. 126). Tüm Microsoft Windows işletim sisteminde bulunan ve Windows tabanlı uygulamaların güvence altına alınmasını sağlayan Kriptografik Uygulama Programlama Arayüzü olan "Microsoft CryptoAPI" yapısında ikincil anahtar olarak "_NSAKey" yapısının etiketlenmesi, NSA ve istihbarat teşkilatının Windows kullanıcılarının güvenliğini

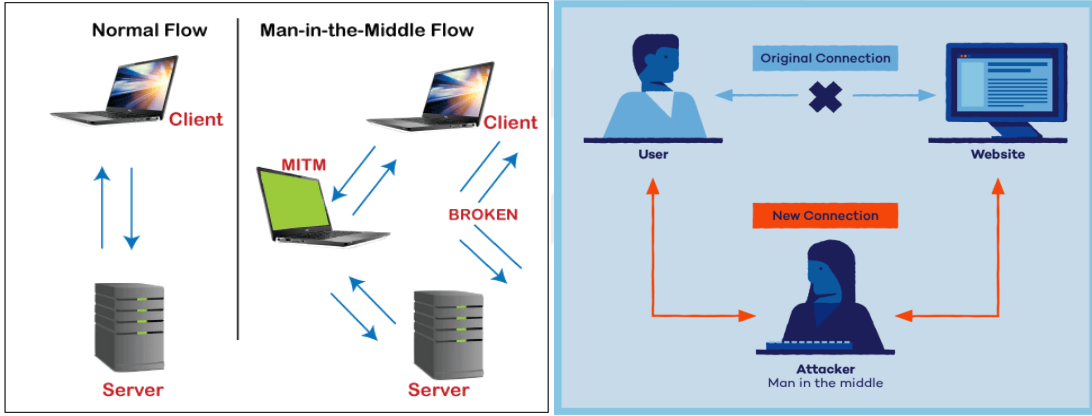
bozmasına izin verdiği ve arka kapı bıraktığı yönünde spekülasyonlara yol açmıştır. Microsoft Sözcüsü Dan Leach, anahtarın NSA'ya ait olduğunu reddederek, _NSAKEY etiketinin kriptografi mimarisinde NSA'nın dışa aktarma standartlarını karşıladığını, hükümetin Microsoft yazılımını kullanarak bilgisayarlarda casusluk yapamayacağını ve kasıtlı olarak arka kapı bırakılmadığını belirtmiştir (CNN, 1999).

Microsoft ve Apple gibi kapalı kaynak işletim sistemlerinde, kullanıcılar bazen verilerinin bu şirketlere veya güvenlik servislerine otomatik olarak gönderilmesi için bir açık kapı oluşturulabileceği konusunda endişeleri dile getirmektedir. Örneğin kaynak kodu herkese açık olduğu için rakip Linux işletim sistemini tercih ettiğini belirten Çin hükümeti, güvenlik servisleriyle birlikte, yabancı üretim işletim sistemlerinde arka kapılar ve hassas bilgilerin sızması olasılığıyla ilgili endişelerini dile getirmiş ve bu endişelere yanıt olarak 2003 yılında Microsoft ile ABD güvenlik servisleri arasında Windows işletim sisteminin kaynak koduna erişim izni veren bir anlaşma imzalamaya sevk etmiştir (CNET, 2003). Sonucunda ise Çin, Microsoft gibi yabancı üretim işletim sistemlerinde zararlı yazılımlar bulunmasından şüphe etmesi ve bilgi güvenliğinin korunması sebebiyle kendi işletim sistemini kurmayı hedeflemiştir. Dikkate değer bir gelişme, 1990'ların sonunda "Red Flag" işletim sistemini oluşturmuştur. Ulusal güvenlik endişelerine ek olarak, Red Flag işletim sisteminin geliştirilmesi maliyetleri düşürmeyi, yerel sanayiye geliştirmeyi ve kurumsal gücü artırmayı amaçlamaktadır (Foster & Goodman, 2000, s. 36). Dolayısıyla Çin, yerel olarak geliştirilmiş bir işletim sistemine sahip olarak, bilgi güvenliği üzerindeki kontrolünü artırmayı ve yabancı teknolojiye bağımlılığı azaltmaya çalışmaktadır. 2000'li yılların başından beri ise Pekin, hem devlet kurumlarını hem de iş sektörünü Unix ve Linux işletim sistemlerini kullanmaya zorlamıştır (Ball, 2011, s. 100). Çin Red Flag işletim sistemine ek olarak, Çin Ulusal Savunma Bilim ve Teknoloji Üniversitesi'nin devlet destekli program tarafından finanse edilerek geliştirdiği işletim sistemi için çalışmalar sürdürerek, Unix tabanlı Kylin işletim sistemini geliştirmiş ve 2007'de ilk tanıtımından bu yana Çin hükümet organları, akademik kurumlar ve diğer kuruluşlar içinde kullanılmaya başlanmıştır (China.org.cn, 2007).

1.3.13. Ortadaki Adam

Gizli dinleme saldırısı olarak da bilinen Ortadaki Adam saldırıları, kötü niyetli saldırganın meşru bir katılımcı olarak istemci (client) ve bir sunucu (server) arasındaki iletişime müdahale etmesi ile gerçekleştirilebilir. Bir başka şekilde, kullanıcı ve uygulama arasındaki bir konuşmada, taraflar birbirleriyle doğrudan ve güvenli bir şekilde iletişim kurduklarına inanırken, saldırganın kendisini iletişim kuran iki taraf arasında konumlandırmasını içermektedir. Kötü niyetli saldırgan iletişime gizlice dahil olarak ve standart bir bilgi alışverişi içerisinde gibi görünerek her ikisinden de verileri çalabilir, değiştirebilir veya veri aktarımını kesebilir (Enisa, tarih yok).

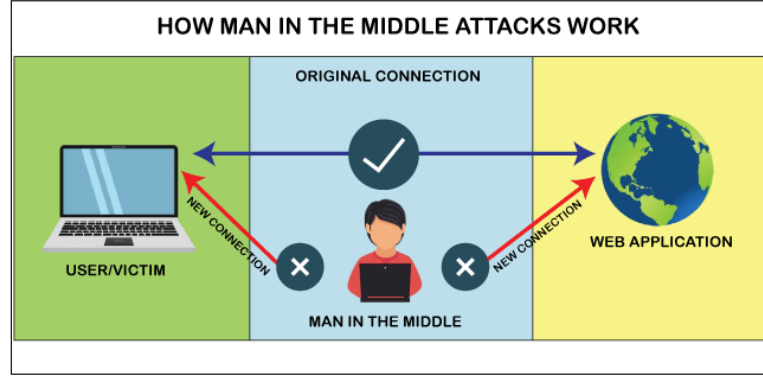
Şekil 4: Ortadaki Adam Saldırısında saldırganın gizli verileri ele geçirmek için kendisini istemci ve sunucu arasında konumlandırması



Kaynak:(<https://www.javatpoint.com/cyber-security-mitm-attacks>),
(<https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/>)

MITM saldırısı casusluk, taraflar arasında kargaşa yaratmak, finansal kazanç sağlamak ve şirketlerin iş süreçlerini aksatmak veya zarar vermek amacıyla kullanılabilir. Örneğin siber tehdit aktörleri, kimlik hırsızlığı veya yasa dışı fon transferleri gibi başka suçları işlemek için kullanılabilecek banka hesap bilgileri, kredi kartı numaraları veya oturum açma kimlik bilgileri gibi gizli verileri çalmaktadır (Panda Security Mediacenter, 2022).

Şekil 5: Siber tehdit aktörünün güvenilir bir web sayfası gibi davranması



Kaynak: <https://www.javatpoint.com/cyber-security-mitm-attacks>

Siber tehdit aktörü, bir istemci ile bir web sitesi sayfasına arasına girerse, Ortadaki Adam saldırısı gerçekleşir. Bu saldırı biçimi birçok farklı yoldan gelebilir. Örneğin, finansal oturum açma uygulamalarında kimlik bilgilerini ele geçirmek için sahte bir bankacılık web sitesi kullanılabilir. Bu durumda kullanıcı ve gerçek bir bankanın web sayfasının ortasında sahte bir site yer alabilir, kurban banka siber tehdit aktörleri ile iletişim kurduğunun farkında varamaz (Java, tarih yok).

1.3.14. Gelişmiş Kalıcı Tehditler

Sisteme sürekli erişim sağlamayı amaçlayan APT saldırıları, yüksek profilli şirketlerdeki ulus devletlerdeki önemli istihbarat bilgilerine, fikri mülkiyet veya ticari sırlara erişim elde etmek gibi belirli amaçlarla yetenekli siber tehdit aktörleri tarafından gerçekleştirilen karmaşık ve hedefli saldırılardır. APT aktörleri, ilk erişimi elde etmek için kimlik avı e-potaları, yazılım güvenlik açıklarından yararlanma, virüslü belgeleri veya bağlantıları kullanma dahil olmak üzere çeşitli taktikler kullanarak hedef sisteme veya ağa kalıcı erişim gerçekleştirirler. Sisteme girdikten sonra, kullandıkları gizli tekniklerle izlerini belli etmemek ve gelecekteki erişim için arka kapılar oluşturur ve sistemi kontrol altına alarak, hedef sistemde fark edilmeden önemli bilgileri çalabilirler (Chen, Desmet, & Huygens, 2014, s. 64).

Ulusal güvenlik verileri, fikri mülkiyet, ticari sırlar gibi rekabet avantajı veya stratejik faydalar sağlama hedefleri bulunan APT saldırıları, genellikle hükümetler veya istihbarat teşkilatları adına çalışan siber paralı askerlere atfedilir. Bu durumda

APT aktörlerinin, hem koordineli bir ekip ile çalıştığını hem de teknik ve finansal açıdan iyi kaynaklara sahip olduğunu göstermektedir (Chen vd., 2014, s. 64).

Icefog APT grubu, 2011'de etkin olan gelişmiş bir casusluk kampanyasına örnektir. Öncelikli olarak Japonya ve Güney Kore'de faaliyet gösteren Batılı şirketlerin tedarik zincirlerine odaklanarak APT saldırıları gerçekleştirilmiştir. Hedefler arasında, devlet kurumları, askeri müteahhitler, denizcilik ve gemi inşa grupları, telekomünikasyon şirketleri, endüstriyel firmaları, yüksek teknoloji şirketleri ve kitle iletişim araçları yer almaktadır (Kaspersky, 2013, s. 3). Bu tür saldırılar genellikle kamuoyuna açıklama yapılmadan gizli tutulur. Saldırının verdiği hasar net bir şekilde bilinmiyor, ancak Icefog saldırısı sırasında hedeflenen şirketlerin çoğu güvenlik açıklarını tespit ederek iyileştirmelerde bulunmuştur.

1.3.15. Kaba Kuvvet Saldırıları

Saldırganların bir ağa girmek için şifre kombinasyonlarını deneme-yanılma veya tahmin yöntemi gibi zorlama yöntemler kullanarak sisteme izinsiz erişim sağlamaya çalıştığı saldırı türüdür. Ağ erişim sağlandıktan sonra siber tehdit aktörleri kişisel verileri çalabilir, sistemi kapatabilir veya kötü amaçlı yazılım yükleyebilir. Kişisel yayın ve yönetim sistemi olan Wordpress'e yönelik 2013 yılında 90.000 IP adresinden gelen kaba kuvvet saldırıları ile farklı zayıf parolalar denenerek yönetici hesaplarına erişim sağlanması "ters kaba kuvvet saldırısına" örnektir (CISA , 2013).

2015 yılında ise Alibaba'nın e-ticaret platformu TaoBao'ya yönelik gerçekleştirilen kaba kuvvet saldırısında ise siber tehdit aktörleri, yaklaşık 99 milyon kimlik bilgisine erişim sağlamıştır. Kullanıcıların genellikle farklı hesaplar için aynı kimlik bilgilerini kullanması nedeniyle bu ihlalden 21 milyon kullanıcı etkilenmiştir (Zoho Corporation, tarih yok). Bu tür saldırılar sonucunda kullanıcıların zayıf şifreler kullanması yasaklanmış ve sağlam şifre gereksinimleri uygulanmıştır.

1.3.16.Sosyal Mühendislik

Siber tehdit aktörlerinin birçoğu manipülatördür. Ancak bu durum onların hepsinin "teknoloji manipülatörü" olduğu anlamına gelmez, bazı siber tehdit aktörleri "insan manipülasyon" sanatını kullanır (Pilette, 2021). Dolayısıyla sosyal mühendislik

saldırılarında siber tehdit aktörleri, insanları psikolojik olarak manipüle ederek, sahte vaatlerde bulunarak ve zayıflıklarını kullanarak ağ kontrolünü ele geçirmeye çalışmaktadır. Kullanılan bu tür psikolojik saldırılarda siber tehdit aktörleri, olmadığı biri olduğuna ikna etmede son derece ustadır. Bu manipülasyon yöntemiyle, yasal çerçevede asla erişmemeleri gereken kişisel bilgilere veya güvenli sistemlere erişim sağlayabilirler (Smith, Papadaki, & Furnell, 2013, s. 249).

Örneğin devlet çalışanı olduğunu iddia eden siber tehdit aktörü, vergilerin vadesinin geçtiğini bildirir ve kredi kartından havale veya EFT ile ödeme yapılması için baskı yapabilir veya ağdaki bir güvenlik açığını düzeltmek için kullanıcıdan oturum açma bilgilerini paylaşmasını isteyebilir. Bu manipülasyondan şüphelenmeyen kullanıcı, giriş bilgilerini paylaşması ile siber tehdit aktörü sisteme erişebilir. Birçok kuruluş, bu tür saldırılar karşısında daha gelişmiş güvenlik sistemleri uygulayarak, saldırganların eylemlerini zorlaştırmaktadır. Ancak kötü niyetli siber tehdit aktörleri, erişim elde etmek için yeni yollar geliştirmeye devam etmekte ve sosyal mühendislik gibi saldırı teknikleri yaygın bir şekilde kullanılmaya devam etmektedir.

1.3.17. Kimlik Avı - Yemleme - Oltalama

Sosyal Mühendislik yöntemi olarak bilinen çevrimiçi kimlik avı, aldatma yöntemi ile siber saldırı gerçekleştirilir. Bu yöntemde, kullanıcı adı, şifre veya bankacılık gibi hassas bilgileri girmek suretiyle kullanıcıların bilgileri sahte kurum adlarıyla oluşturulan bir site aracılığıyla çalınır. Tüm bu tüketici markalar arasındaki ortak faktör, müşterileri ile sürekli olarak e-posta yoluyla iletişime geçmeleri ve kullanıcıların kredi kartı, adres veya şifre doğrulamalarında hassas bilgileri sağlayabilmesidir. Kişisel bilgileri toplamak ve tuzakları dağıtmak amacıyla kullanılan kimlik avı saldırısında siber tehdit aktörleri, sahte kötü niyetli bağlantılar veya mesajlar gönderir ve kullanıcı bilgilerini doğrudan diğer kişilere verebilir (Arachchilage & Love, 2014). İngiltere'deki yazılım şirketi Tessian 2021 verilerine göre kimlik avı saldırılarında en yaygın olarak taklit edilen markaların Microsoft, ABP, Amazon, Adobe Sign, Zoom olduğunu belirlenmiştir (Rosenthal, 2022).

Kötü amaçlı içeriğe sahip, kimlik avı dolandırıcılığına yol açan ve ziyaretçilerin veri gizliliğini ve güvenliğini tehlikeye atan harici bağlantılar genellikle kara listeye alınmaktadır. Google, bu durumda günde 10.000 siteyi kara listeye

almaktadır (Sharma, 2022). Siber tehdit aktörleri ise bu önlem karşısında yeni teknikler öğrendikçe kimlik avı saldırıları daha karmaşık hale gelmekte ve ciddi bir siber güvenlik sorununu oluşturmaktadır.

1.3.18. İstem Dışı Elektronik Postalar

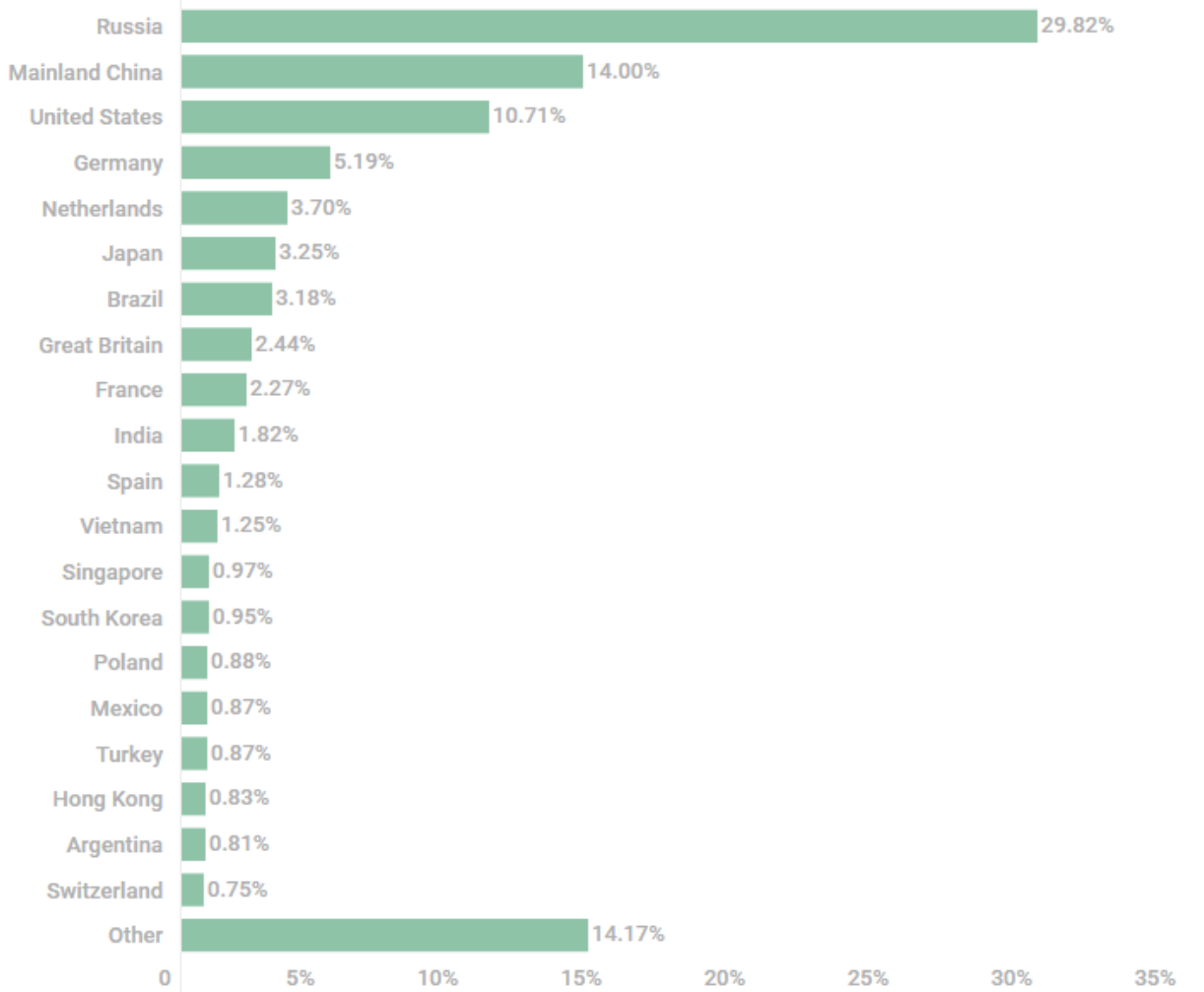
Kişilik haklarını ihlal eden ve talep edilmeyen e-postalar, siyasi ve dini ideolojik görüşlerin yayılması, reklam ve kampanya tanıtımı niteliğinde olmakla birlikte istismar, sahtecilik ve aldatma içerikli ya da bilgisayara zararlı yazılımlar bulaştırmak amacıyla oluşturulmuş botnetlerin dağıtılması için kullanılmaktadır. Dolayısıyla virüs bulaşmış bir bilgisayar, sonrasında daha fazla spam üreten bir ağı (botnetin) robotik bir üyesi (botu) haline gelir (International Telecommunication Union [ITU], 2008). Kaliforniya'daki çok uluslu bir ağ teknoloji şirketi olan CISCO'nun (Cisco Systems) 2021 verilerine göre en fazla istenmeyen kötü amaçlı e-posta alan sektörlerin; perakende, imalat, yiyecek ve içecek, araştırma ve geliştirme teknolojileri olduğu belirtmiştir (Rosenthal, 2022).

Covid-19 döneminde süreçten yararlanan spam kampanyaları ise çok fazla yaygınlaşmıştır. Güvenlik ve bilgi alanına yoğunlaşmış, uluslararası bir yazılım şirketi olan Symantec, halkın virüsle ilgili korkularından yararlanmaya çalışan siber tehdit aktörlerinin gönderdiği e-posta kampanyası analizine göre e-postaların çoğu; kimlik avı, dolandırıcılık ve kötü amaçlı yazılım içeren e-postalardan oluşmaktadır. Bu tür e-postalar finansman teklifi veya sağlık merkezinden gelen bir mesaj gibi görünecek şekilde hazırlanmakta ve böylece kullanıcıların kötü niyetli oluşturulmuş web sayfalarına girmeye teşvik edilmesini sağlamaktadır. Örneğin Dünya Sağlık Örgütünden (WHO) geliyormuş gibi görünen ve salgının önlenmesi amacıyla ücret ödemelerini içeren e-postaların gönderilmesi, koruyucu giysilere olan ihtiyacın artması sebebiyle cerrahi maske tedarikçisinden geldiği iddia edilen e-postalar veya bağışıklık sistemini güçlendiren ilaçların sahte kampanyalarla tanıtılması gibi vakalar süreç içerisinde yaşanmıştır (Thaware, 2020).

2022 yılında yaşanan Rusya Ukrayna savaşında ise Ukrayna'ya yardım olarak para kabul ediyormuş gibi görünen sahte bağış siteleri ve e-postalar yaygın olarak görülmüştür. Bu siteler ve e-postalar, tanınmış kişilere ve insanı yardım kuruluşlarına atıfta bulunarak, alıcıyı kripto para işlemleri yoluyla takip etmek banka işlemlerine

göre daha zor olduğu için Bitcoin cüzdanına para transferi yapılmasını teklif etmiştir (Securelist, 2023).

Şekil 6: 2022 Spam Kaynakları



Kaynak: Securelist. (2023). *Spam and phishing in 2022*. <https://securelist.com/spam-phishing-scam-report-2022/108692/>

Kaspersky'nin 2021 verilerine göre küresel e-posta trafiğinin %45,56'sı istem dışı elektronik postalarından oluşmaktadır. İstenmeyen e-postaların %24,77'si Rusya'dan, %14,12'si Almanya'dan gönderilmiştir. Üçüncü ve dördüncü sırada ise ABD %10,46 ve Çin %8,73 oranlarına sahiptir (Shcherbakova & Kulikova, 2022). 2022 verilerine göre ise küresel e-posta trafiğinin ortalaması %48,63'e yükselmiştir. İstenmeyen e-postaların %29,82'si Rusya'dan, %14,00'ü Çin'den gönderilmiştir.

Üçüncü ve dördüncü sırada ise ABD %10,71 ve Almanya %5,19 oranlarına sahip olarak yer değiştirmiştir (Securelist, 2023).

1.3.19. Yapay Zeka (AI) Destekli Siber Saldırıları

Verileri hızlı bir şekilde ele geçirme, hızlı analiz etme veya siber tehditlerden korunmak için kurulan programları duraklatma yeteneğine sahip AI saldırıları, kullanıcı veya programcı hatasının bir sonucu olarak geleneksel siber saldırılardan farklıdır. Son teknoloji ürünü olan yapay zeka sistemleri, fiziksel nesnelere ya da kritik yapılara giderek daha fazla uyumlu hale getirildiğin için bu tür saldırılar toplumda, kuruluşlarda ve ülke güvenliği üzerinde etki oluşturmaktadır. Örneğin güvenlik açığını temsil eden bir yapay zeka saldırısında, trafikte dur işaretinin üzerinde birkaç parça bant yerleştirerek kendi kendini süren bir arabanın gözünde dur işaretini yeşil ışığa dönüştürebilir ve bir kazaya sebep olabilir (Comiter, 2019, s. 3).

Özellikle askeri ve istihbarat bağlamlarında gerçekleştirilen AI saldırıları, siber silah olarak kullanılma potansiyeline sahiptir. Yapay zeka ve makine öğreniminin boru hatlarına, otonom silahlara ve askeri sistemlere entegrasyonu ile birlikte birçok ülke, askeri operasyonlarda yapay zekanın kullanımına ilişkin araştırma ve geliştirme çalışmalarını artırmıştır (Comiter, 2019, s. 49). Dolayısıyla askeri alandaki yapay zekanın gelişimi, devam eden bir silahlanma yarışına ve yapay zekanın askeri angajmanların stratejik ve taktik yönlerine dahil edilmesine yol açmıştır (Upchurch, 2018). Kenneth Payne *"savaş karar verme ile ilgilidir ve AI her şeyden önce karar vermeyi kolaylaştıran değil, karar veren teknolojidir"* argümanı ile Soğuk Savaşta süper güçler arasındaki nükleer cephanelik ve stratejinin geliştirilmesi arasındaki ilgi çekici paralellikleri vurgulamaktadır (Payne, 2018).

1.3.20. Şebeke Trafiğinin Dinlenmesi

Telefon görüşmesi, anlık mesajlaşma veya video konferansları gibi özel iletişimlerin yetkisiz siber saldırganlar tarafından ele geçirilmesi ile bilgi hırsızlığı meydana gelmektedir. Bir çeşit gizli dinleme metodu olan Evaesdropping; bilişim sistemlerinin veri taşımada kullandığı ağlara girilerek veya yaydığı elektromanyetik

dalgaların yakalanarak verilerin elde edilmesi ile gerçekleştirilir (Altunok & Vural, 2011, s. 78).

IP üzerinden ses video veya mesaj gönderilmesi ve şifreleme kullanılmayan VoIP (İnternet Protokolü Üzerinden Ses İletişimi) sistemleri bu tür yetkisiz kişilerin aramaları kesmesini kolaylaştırmaktadır. 2009 yılında VoIP uygulamalarından biri olan Skype'ı hedefleyen Trojan Peskyspy (Trojan:Win32/Peskyspy.A) isimli bir truva atı piyasaya sürülmüştür. Bu truva atı, Skype konuşmalarından ses verilerini yakalamasına ve yerel olarak ".mp3" dosyaları olarak kaydedilmesine izin vererek kendisini bağlamak için Windows API'lerini kullanmıştır. Truva atı, Skype ile ses cihazı arasındaki ses verilerini yakalayıp, Skype tarafından uygulanan herhangi bir şifreleme mekanizmasından bağımsız olarak sesi toplayabilir (Microsoft, 2009).

1.3.21. SQL Enjeksiyonu

SQL (Structured Query Language - Yapılandırılmış Sorgu Dili) sadece veritabanlarını veya veri akışını yönetmek, sorgulamak, tasarlamak ve değiştirmek için kullanılan geliştirilmiş bir sorgu dilidir. SQL Enjeksiyon, veri tabanı altyapısına sahip sistemlerde yaygın bir biçimde görülen, kurumların ve ulus devletlerin kritik verilerini çalmak veya değiştirmek için kullanılan siber güvenlik tehdididir. Bir çok web uygulaması ve web sayfası verilerini SQL veritabanlarında depolar ve siber tehdit aktörleri veritabanındaki açıkları kullanarak SQL sorgusunun eklenmesi veya "enjekte edilmesi" ile saldırılarını gerçekleştirirler (The Open Web Application Security Project [OWASP], tarih yok). Saldırı sonrasında ise oluşan en yaygın riskler; kimlik bilgilerinin, e-posta adreslerinin, oturum açma bilgilerinin çalınması ve verilerin siber tehdit aktörleri tarafından Dark Web üzerinden satışa çıkartılmasıdır (Turhost, 2021).

1.3.22. Kripto Hırsızlığı

Kripto para madenciliği yapmak için verilerin yer aldığı bilgi işlem gücünün yetkisiz kullanımı ile gerçekleştirilen Cryptojacking, blok zincir (blockchain) ve kripto para madenciliğindeki artış sebebiyle hem literatürde hem de siber saldırı sınıfında nispeten yeni ve etkili bir tehdit olarak ortaya çıkmıştır. Kripto para birimi (cryptocurrency) ya da "madeni para", fiziksel formu ve merkezi olmayan bir defter

tarafından kontrol edilen, katılımcıları arasında serbestçe aktarılabilen dijital bir para sistemidir. Fiziksel formda para transferleri, para çekme ya da yatırma işlemleri bankanın veri tabanında yer alır. Ancak kripto para birimlerinde merkezi olmayan bir veri tabanı mevcuttur, hükümet veya bir banka tarafından desteklenmez. Dolayısıyla kripto para birimindeki anonim yapı, para biriminin ne kadarının dolaşıma gireceğine karar veren bir düzenleyici kurumun olmadığı anlamına gelmektedir (AlwareBytes, tarih yok). Cryptojacking ile uğraşan siber tehdit aktörleri de saldırılarını genel olarak Monero, Ethereum ve Zcash gibi anonimliği yüksek kripto param birimlerine odaklanarak gerçekleştirirler (Turhost, tarih yok).

Kripto hırsızlığı saldırılarının diğer kötü niyetli saldırılara benzerliği; amaçlarının kar elde etmek olmasıdır. Farklılığı ise kullanıcıdan tamamen gizli kalacak şekilde tasarlanan Cryptojacking, yetkisi olmayan elektronik cihazlar, ağ sunucuları ve internet tarayıcıları gibi çeşitli cihazlarda kontrolü ele geçirerek, kripto madenciliği yapmak için sisteme arka planda çalışan kod yükler. Bu yöntem ile çaldıkları kripto para birimlerini dijital cüzdanlarına aktarmaktadırlar. Örneğin 2017'de piyasadaki en popüler kripto hırsızlığı yazılımı olan Javascript tabanlı CoinHive, çoğu web sitesinin arka planına yerleştirilerek ve ziyaretçilerin işlem gücünü doğrudan paraya çevirebilecek bir kripto madenciliği komut dosyasını başlatmıştır (Porter, 2019). Kötü niyetli bir bot veya truva atı gibi kötü amaçlı yazılıma benzer bir kod ile çalışmakta olan CoinHive, web sayfasını ziyaret eden kullanıcının tarayıcısı üzerinden işlemci gücü paylaşmakta ve bu yöntem ile ziyaretçinin sitede gezindiği süreçte Monero¹ madenciliği yapılmaktaydı (KrebsOnSecurity, 2018). 2019'da kapatılan CoinHive'in JavaScript madenci kodunu çalıştıran yaklaşık 32.000 web sitesi olduğu ve tüm kripto hırsızlığı kampanyalarından yaklaşık %60'lık paya sahip olduğu bilinmektedir (Moffitt, 2019).

2017 ve 2018 yıllarında kripto para birimindeki artış sebebiyle kripto hırsızlığı da artmış ve tüm mobil cihazlar, endüstriyel kontrol sistemleri, kritik altyapılar ve bulut alt yapısında ortaya çıkmıştır. RedLock Bulut Güvenlik İstihbaratı (SCI) ekibi,

¹Monero, 2014 yılında merkezi olmayan açık kaynaklı bir kripto para birimi olarak oluşturulmuştur. Bitcoin'den farkı Monero basit bir bilgisayar aracılığı ile çıkarılabilirken, Bitcoin madenciliği özel ve pahalı donanımlar gerektiren cihazlar ile çıkarılabilmektedir.

parola koruması olmadan internet üzerinden erişilebilir yüzlerce Kubernetes² yönetim konsolu tespit etmiştir. Bu örnekler arasında İngiliz çok uluslu bir sigorta şirketi olan Aviva'ya, dünyanın en büyük SIM kart üreticisi olan Gemalto'ya ve Tesla'nın potansiyel olarak hassas bilgiler içeren veritabanına yönelik kripto para madenciliği yapıldığı keşfedilmiştir (RedLock, 2018). 2021'in ikinci yarısında büyük kripto hırsızlıkları toplam 681 milyon dolara mal olmuştur (CipherTrace, 2021).

1.4. Siber Uzayda Faaliyet Gösteren Aktörler ve Aktörler Arası İlişkiler

21. yüzyılda savaş alanı giderek siber uzaya doğru ilerlemektedir. Siber uzayda uluslararası ilişkilerin tüm aktörleri, belirli hedefler doğrultusunda uluslararası normları çiğneyerek siber suç girişiminde bulunmaktadır. Weedon, Nuland ve Stamos (2017) çeşitli aktörler tarafından erişilebilir hale gelen bilgi operasyonlarını *"...organize aktörler (hükümetler veya devlet dışı aktörler) tarafından iç veya dış siyasi duyarlılığı çarpıtmak için, çoğunlukla stratejik veya jeopolitik bir sonuç elde etmek için yapılan eylemler"* olarak tanımlamıştır. Siber saldırı araçlarını doğrudan veya dolaylı olarak kullanan her aktör cihazlara, işlem gücüne, bilgi işlem kaynaklarına ve bilgilere erişime farklı motivasyonlarla önem verir. Genel olarak, her tür siber aktörün birincil motivasyonu vardır (The Canadian Centre for Cyber Security, 2021). Bu motivasyonlar arasında, ekonomik ve siyasi çıkarlar, ideolojik nedenler, casusluk, sabotaj veya yıkıcı amaçlar bulunabilmektedir.

Gerçek ve tüzel kişilerin her geçen gün siber alandaki müdahalelerinin artması sebebiyle, siber uzayda faaliyet gösteren aktörlerin sınıflandırmasında bir kesinlik bulunmamaktadır. Temel olarak ulus devlet aktörleri ve devlet dışı aktör olmak üzere iki grupta sınıflandırılabilir. Bir veya daha fazla egemen devletin yargı yetkisine tabi olan devlet dışı aktörler; bilgisayar korsanlarını, organize suç gruplarını, siber paralı askerleri, terörist grupları içerebilir. Devlet aktörleri ise diğer egemen devletleri hedefler, ancak siber saldırılardaki taktik, teknik ve prosedürleri, devlet dışı aktörlerle

² Kubernetes konsolu, uygulama kapsayıcılarının, sanallaştırılmış yazılımların ve bazı bulut tabanlı hizmetlerin dağıtımını, ölçeklenmesini ve çalışmasını otomatikleştirmek için kullanılır. Google'ın açık kaynaklı Kubernetes sistemi, dünya çapında sayısız kurumsal oyuncu tarafından güvenli bir şekilde kullanılmaktadır, ancak bu durumda, güvenli olmayan bir konsol, erişim kimlik bilgilerini Tesla'nın Amazon Web Hizmetleri (AWS) ortamına ifşa etmiştir. <https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/>

benzerlik göstermektedir (Sims, 2011, s. 3). Çalışmada literatür taraması sonucu Amerika Birleşik Devletleri, Çin Halk Cumhuriyeti, Rusya Federasyonu, Kuzey Kore ve İran dahil olmak üzere birçok ulus devletin siber savaş yeteneklerinin mevcut olduğu sonucuna varılmıştır. Bu bölümde siber uzayda faaliyet gösteren aktörleri anlamak için kavramsal bir çerçeve sunulması amaçlanmıştır.

1.4.1 Ulus Devlet Aktörleri

Ulus devlet aktörleri genellikle illegal faaliyet gösteren, siber paralı askerlerden veya kiralık bilgisayar korsanlarından seçilen ve "hack lisanslarına" sahip kişilerden oluşmaktadır. Bu kişiler hedef hükümetler, kuruluşlar veya bireylere yönelik saldırı gerçekleştirmek için silahlı kuvvetlerden, istihbarat birimlerinden veya diğer devlet kontrol aygıtlarından talimat alabilmektedirler (Pawlicka, Choras, & Pawlicki, 2021a, s. 2). Ulus devlet aktörleri, devlet sponsorluğunda faaliyet gösterdikleri gibi siber ordular veya alanında uzmanlaşmış personeller olarak hükümetin ilgili birimlerinde doğrudan istihdam edilebilmektedir (Culafi, 2021).

Ulus devlet tehdit aktörlerinin profili, siber uzayda faaliyet gösteren diğer aktörlerden farklılık göstermektedir. Potansiyel olarak en uzman programcılardan oluşan ekiplere ve en gelişmiş donanımlara sahip aktörlerdir (Klimburg & Healey, 2012). Misyon odaklı ve hedeflerine ulaşmakta çok ısrarcı olan ulus devlet aktörleri, kendi hükümetlerinin yasal yönergeleri dahilinde çalıştıkları için eylemleri sebebiyle yargılanma endişesi taşımamaktadırlar (Spitzner, 2022).

2020 Microsoft Dijital Savunma Raporuna göre siber uzayda ulus devlet aktörlerinin ortak amaçları, siber casusluk faaliyetiyle diğer ulus devletlerin istihbarat bilgilerine erişim sağlamak ve sonrasında bilgilere erişimi kesintiye uğratmak veya imha etmektir. Ortak teknikleri ise kimlik bilgisi toplama, kötü amaçlı yazılım ve sanal özel ağ açıklarından yararlanma olarak belirlenmiştir (Lambert, 2021, s. 52). Bu tür saldırılar, hedeflenen ulus devletin kritik altyapılarına, savunma sistemlerine, üretim tesislerine, endüstriyel tasarımlarına veya hükümet kurumlarına erişim sağlamayı içermektedir. Temmuz 2020'de ABD Adalet Bakanlığı, Çin'i Covid-19 aşılı geliştiren laboratuvarları hedef alan bilgisayar korsanlarına sponsor olmakla suçlaması, devlet destekli olduğu iddia edilen siber saldırı örneklerinden biridir. İddianameye

göre suçlanan şahıslar, Çin Halk Cumhuriyeti Devlet Güvenlik Bakanlığı (Chinese Ministry of State Security - MSS) ile birlikte hareket etmekteydi (BBC, 2020).

Nisan 2018'de ABD İç Güvenlik Bakanlığı (United States Department of Homeland Security - DHS), Federal Soruşturma Bürosu (Federal Bureau of Investigation - FBI) ve Birleşik Krallık Ulusal Siber Güvenlik Merkezi (National Cyber Security Centre - NCSC), Rusya tarafından gerçekleştirilen siber faaliyetler hakkında ortak bir uyarı metni yayınlamıştır. Ortak bildiride, Rus hükümeti destekli bilgisayar korsanlarının hükümetleri, özel şirketleri ve kritik altyapı sağlayıcılarını hedef alarak, casusluk, fikri mülkiyet hırsızlığı, kurban ağlarına kalıcı erişimi sürdürmek ve potansiyel olarak gelecekteki saldırı operasyonlarına temel oluşturmak için güvenliği ihlal edilmiş yönlendiriciler kullandığı belirtilmiştir (NCSC [National Cyber Security Centre], 2018).

1.4.1.1 Devlet Destekli Gelişmiş Kalıcı Tehdit Aktörleri

Devlet destekli gelişmiş kalıcı tehdit (Advanced Persistent Threat - APT) aktörleri, ulus devletler tarafından doğrudan bir istihbarat teşkilatının birimleri veya dolaylı olarak paravan şirketler aracılığıyla, devlet tarafından desteklenen ve casusluk yeteneklerine sahip tehdit aktörleridir. Bu aktörler, belirli hedeflere ulaşmak için karmaşık ve sürekli bir şekilde çalışmakta ve çoğu zaman siber tehdit aktörleri ve devlet destekli aktörler arasında kullanılan taktikler, teknikler ve prosedürler (TTP) benzerlik gösterebilir. ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency - CISA) tarafından Ocak 2022 tarihli belgede, Rusya Devlet Destekli APT aktörlerinin kullandığı TTP'ler incelenmiştir. Bu belgede, siber tehdit aktörleri ve devlet destekli aktörlerin arasında benzer davranışların sıkça sergilendiği görülmektedir (CISA [Cybersecurity and Infrastructure Security Agency], 2022). Bu durum hem siber tehdit aktörlerinin hem de devlet destekli aktörlerin, hedeflere yönelik sızma, ağ keşfi, arka kapı, kötü amaçlı yazılım kullanımı, hedef sistemin güvenliğini sağlayan Güvenlik Duvarı (Firewall), SIEM (Security Information and Event Management, EDR/XDR (Endpoint/Extended Detection and Response) gibi uygulamaların korumasını etkisiz hale getirerek sistemin komuta ve kontrolünü tümünden ele geçirme ve diğer saldırı teknikleri gibi benzer TTP'leri benimseyebildiğini göstermektedir (Kadir, 2022).

Siber tehdit aktörleri, ulus devletlerin politika planları hakkında bilgi sahibi olabilmek için düşünce kuruluşları ve hükümet kuruluşları arasındaki bağlantıdan faydalanarak istihbarat operasyonları yürütmektedirler. 2020 Microsoft Dijital Savunma Raporuna göre ulus devletler, sivil toplum kuruluşları ve düşünce kuruluşları %80 oranında en çok hedeflenen sektörler arasında yer almaktadır. Siber saldırılarda en çok hedef alınan ülkenin %46 oranında ABD olduğu belirtilen raporda, en yüksek saldırı oranlarına sahip devletler ise Rusya, Kuzey Kore, İran ve Çin olarak belirtilmiştir (Lambert, 2021, s. 55).

Aralık 2020'de Rus hükümetinin desteklediği iddia edilen APT26 grubu, Teksas merkezli yazılım şirketi SolarWinds'e yönelik bir tedarik zinciri saldırısı gerçekleştirmiştir. Siber tehdit aktörleri, SolarWinds'e ait Orion platformunun güvenlik açığından faydalanarak sisteme bir arka kapı yerleştirilmesi ve müşterilerin yazılımı güncellemesiyle etkinleştirilen bu siber saldırı, son 10 yılın en büyük siber saldırısı olarak nitelendirilmiştir. Sonucunda ise ABD devlet kurumları dahil olmak üzere kamu ve özel sektördeki birçok kuruluşu tehlikeye attığı açıklanmıştır (Botelho, 2022). Bir diğer örnek ise APT10 olarak bilinen ve MSS adına hareket eden bir devlet destekli APT aktörünün, Avrupa, Asya, ABD'deki şirketlerin ve kurumların fikri mülkiyet ve hassas ticari verileri hedef alan kötü niyetli bir siber saldırı kampanyasını yürütmek için hareket ettiğini 2018 yılında Birleşik Krallık müttefikleriyle birlikte duyurmuştur (NCSC, 2018a).

2021 yılında NCSC, 2020'den beri Çin hükümeti ile bağlantıları olan Zirconium, Judgment Panda ve Red Keres olarak bilinen APT31 grubunun, Finlandiya parlamentosu dahil birçok Avrupa ülkesinin devlet kurumlarına, siyasi kişilerine, müteahhitlerine ve hizmet sağlayıcılarına yönelik siber saldırılar gerçekleştirdiği değerlendirmesinde bulunmuştur (NCSC, 2021). Aynı şekilde Birleşik Krallık, Ocak 2021'de dünya çapında çeyrek milyondan fazla sunucuyu etkileyen Microsoft Exchange Server'a yönelik gerçekleştirilen saldırının arkasında, Çin hükümeti destekli Hafnium grubunun olma olasılığının yüksek olduğuna karar vermiştir. Birleşik Krallık dışında ABD, NATO, AB, Yeni Zelanda, Kanada, Avustralya, Japonya da Microsoft Exchange Server'a yönelik saldırılarda Çin'i sorumlu tutmuş ve Çin Halk Cumhuriyeti'nin siber uzaydaki sorumsuz ve istikrarsızlaştırıcı davranışından dolayı *"kötü amaçlı siber faaliyet ve sorumsuz devlet davranışı"* atfetmiştir (The White House, 2021).

Devlet destekli APT gruplarının siber suçlara karışmasındaki diğ er bir amacı ise finansal kazanç elde etmektir. G un umuzde Kuzey Kore destekli olmasıyla tanınan ve en aktif APT gruplarından biri Lazarus, kripto para borsalarını ve finansal hizmet şirketlerini hedef alarak ger ekleştirdiğı saldırılarla bilinmektedir. CISA, FBI ve ABD Hazine Bakanlıđının kripto para hırsızlığı ile ilgili siber tehdidi vurgulamak i in yayınladığı Nisan 2022 tarihli a ıklamada; Nisan 2022 itibariyle Kuzey Kore destekli Lazarus grubunun, Kuzey Kore rejimini desteklemek amacıyla fon oluřturmak ve aklamak i in kripto para teknolojisi firmalarının, oyun şirketlerinin ve borsaların g venlik a ıklarından yararlanma eylemine devam edeceğı belirtilmiřtir (CISA, 2022a).

1.4.1.2 Siber Ordular

Siber ordular, ulusal g venlik ve savunma stratejilerinin bir par ası olarak faaliyet g sterirler. Ulus devletler i in siber saldırıları organize etmenin ve siber savunma oluřturmanın iki yolu vardır; talimatları takip eden devlet dıřı akt rleri  cret karřılığında iře almak ya da siber saldırılara ayrılmıř kendi resmi departmanlarını oluřturmaktır.  zellikle ulus devletler, siber uzayda yařanan rekabet gereğı siber saldırı yeteneklerini artırmak i in siber ordulara ve alanında uzman personellere  nemli yatırımlar yapmaktadır.

Siber orduların g revi,  lkelerin siber g venlik ve siber savař yeteneklerini geliřtirmek, h k metin kritik altyapısını etkin bir řekilde koruyabilmek, siber stratejilerin geliřtirilmesine iliřkin y n belirlemede yardımcı olmak, ulusal siber tehdit analizlerini y r tmek, siber tehdit akt rlerini izlemek, gerektiğinde karřı saldırı yapmak ve d řman bir  lkeye siber saldırı bařlatabilmek i in istihbarat toplamaktır. Ayrıca bu ordulardaki siber savunma sistemleri, i  ve dıř tehditler yoluyla tehlikeye karřı askeri ve h k met ađlarının g venliđinin sađlanması i in bir savunma rol ne sahiptir (Aschmann, Vuuren, & Leenen, 2015, s. 2).

D nyada resmi ve gayri resmi olarak faaliyet g steren bir ok siber ordu mevcuttur. Resmi olarak ABD, Rusya, Almanya,  in, İsrail, İran ve Kuzey Kore'nin siber ordularını oluřturduğı bilinmektedir. Diğ er ulus devletler ise siber alandaki eylem planları ve caydırıcılık stratejileri ile g venlik odaklı savunma pozisyonu oluřturmaktadır (Korhan, 2017, s. 87). Bu dođrultuda geleneksel kara, deniz, hava ve

uzay savaş alanlarının dışında siber uzayın savunulması görevi ile ABD 2010'da, ABD Siber Komutanlığını (US Cyber Command - USCYBERCOM) kurmuştur. Çin'in siber ordu kabiliyeti ise Çin Halk Kurtuluş Ordusu (HKO) bünyesinde birçok siber güvenlik uzmanı göreve almasıyla artmaktadır. Rusya'da resmi bir siber ordu yoktur, ancak Federal Güvenlik Servisi (FSB), Dış İstihbarat Servisi (SVR) ve Askeri İstihbarat Kurumu (GRU) bünyesinde siber yapılanmalar mevcuttur.

Devlet dışı aktörlerin siber orduları ise hükümetler veya ordular tarafından işe alınarak, uluslara veya özel kuruluşlara karşı bağımsız olarak siber saldırılar gerçekleştirmektedir. Devlet dışı aktörlerin siber ordularına örnekler ise; Pakistan Siber Ordusu (PCA), Bangladeş Siber Ordusu, Birleşik Krallık merkezli M16 Hacker Ekibi, ABD web sitelerine odaklanan K9 Network Cyber Army, Fransa'da Vupen olarak bilinmektedir (Aschmann vd., 2015, s. 4).

1.4.2. Devlet Dışı Aktörler

1980'lerde düşük seviyeli siber saldırı eylemlerinde bulunan devlet dışı aktörler, 21. yüzyılda geleneksel olmayan siber silahları kullanarak asimetrik savaş yürütmekte ve kritik altyapıya yönelik ciddi hasarlar vererek yıkıcı etkilere yol açabilecek beceri ve uzmanlığı kazanarak uluslararası sistemde önem kazanmaya devam etmektedir. Özellikle ulus devlet kaynakları veya diğer destek biçimleri, devlet dışı aktörlerin siber uzayda dikkate değer bir şekilde güç potansiyelini daha da artırabilir (YRIS [The Yale Review of International Studies], 2017).

Devlet dışı aktörler ideolojileri, organizasyon yapısı, motivasyonları ve yetenekleri açısından aralarında büyük farklılıklar gösterebilmektedir. Çünkü bir devlete veya şirkete zarar verebilecek devlet dışı aktörler, finansal kazanç elde etmek isteyen bireysel bilgisayar korsanları, terörist gruplar, hacktivistler, casusluk girişiminde bulunabilecek eğitimli korsanlar veya siber paralı askerler olabilir. Sadece askeri hedefler peşinde değil, finansal kazanç, politik düşünce, dini motivasyon gibi farklı amaçlar doğrultusunda eylemlerini gerçekleştirebilirler. Devletler tarafından yönlendirilebilir ve teşvik edilebilir veya devletin siyasi oluşumlarıyla ilgili herhangi bir duruma şiddetle karşı çıkabilirler (Bussolati, 2015, s. 106).

1.4.2.1. Hacktivistler

Hackivist gruplar politik veya ideolojik motivasyonlar tarafından yönlendirilen gruplardır. Birçoğu idealizm tarafından motive edilmiş, genelde solcu, anti-kapitalist, şirket karşıtı bakış açılarına sahip ve politik konulardan ilham alarak gündem odaklı siyasi sorunları protesto etmek veya sosyal değişimi teşvik etmek amacıyla siber saldırı faaliyetlerini yürütmektedirler (Jones, 2022). Yaygın olarak hizmet reddi (DoS), web sitesi tahribatı (website defacement) ve kişisel verilerin yayılmasını içeren sızıntı (doxing and leaking) yöntemlerini kullanmaktadırlar.

Hizmet reddi saldırısı; hackivistlerin protesto aracı olarak kullandığı yöntemlerden biridir. Örneğin Anonymous, 2013 yılında ABD hükümetini yabancı devletlerde savaş suçları işlemekle suçlayarak hükümet politikasını protesto etmek amacıyla 130'dan fazla bankanın web sitesini ve dokuz büyük hükümet sitesine yönelik "OpUSA" saldırısını başlatmıştır. Hedefler arasında Pentagon, Ulusal Güvenlik Ajansı (National Security Agency- NSA), FBI, Beyaz Saray, Bank of America, Capital One ve TD Bank gibi bankaların ve kurumların web siteleri yer almıştır. (Bloomfield, 2013).

Sızıntı; bilgisayar korsanlarının muhaliflerin veya kamuya mal olmuş kişilere karşı etkili olabilecek gizli belgelerin ve kişisel verilerin yayınlanması yöntemidir. Özellikle büyük şirketler veya hükümetlerde üst düzey kişilerin görevden alınması amacıyla elde edilen hassas verilerin internet ortamında herkese açık olarak paylaşımını gerçekleştirebilmektedirler. 2015 yılında Crackas With Attitude (CWA) olarak bilinen genç hackivist grubunun bir üyesi, Filistin'i desteklemek amacıyla ABD kolluk kuvvetlerinin ve hükümet yetkililerinin 2.000'den fazla kişisel bilgilerinin bulunduğunu iddia ettiği bir liste yayınlamıştır (Bicchierai, 2015). 2011 yılında ise saldırı, FBI'nın yayınladığı bültende sızıntı adı verilen siber teknik aracılığıyla kimlik hırsızlığı ve taciz riski altında olduğunu değerlendirmiştir. Rapora göre Anonymous ve LulzSec aleyhinde sosyal veya politik olarak motive edilmiş bir mesajı iletmek için suç işleyen bilgisayar korsanlarının Twitter ve İnternet Aktarmalı Sohbet (IRC) kanallarında kolluk kuvvetleri ile ilgili bilgileri yayınladığı belirtilmiştir (FBI, 2011).

Web sitesi tahribatı; bir sitenin içerik veya görsel olarak görünümünü değiştirmek yöntemidir. Özellikle çevrimiçi anket sonuçlarını çarpıtmaya yönelik veya

siyasi kampanyaların uygulanabilirliğine yönelik tahriflerde bulunmak için uygulanmaktadır.

1.4.2.2. Siber Teröristler

Terör örgütleri internet ortamında korku yaratmak, propaganda yapmak, işe alım süreçlerini yürütmek, finansman sağlamak dışında, rakip ulus devlet aktörlerine karşı siber saldırı yeteneklerini geliştirmektedir. Diğer siber suçluların aksine, siber teröristlerin niyetleri sadece hassas verilerden yararlanmak değil, aynı zamanda sosyal düzeni istikrarsızlaştırmak için kritik altyapıyı hedef alarak can kaybını veya ciddi ekonomik kayıpları içerebilen daha ciddi ve kalıcı hasarları hedeflemektir (Swearnin, 2019, s. 48).

Örneğin El Kaide terör örgütü 2012 yılında yayınlanan bir videoda, siber yeteneklerini geliştirerek ABD'ye karşı "*elektronik cihad*" yürütme niyetini ilan etmiştir. Terör örgütü hem ABD hükümet ağlarına hem de elektrik altyapısı dahil olmak üzere diğer kritik altyapılara yönelik siber saldırılar başlatması için "*gizli mücahitlere*" çağrıda bulunmuştur. UNSCYERCOM üst düzey yetkilisi Rear Adm. Samuel Cox, El Kaide ajanlarının ABD ağlarına karşı siber saldırılar düzenlemek için aktif olarak gelişmiş siber silahlar aradıklarını ve bunu yapmak için uzman bilgisayar korsanlarından yetenek satın alabilecekleri konusunda uyarıda bulunmuştur (Cloherty, 2012).

2016 yılında ABD'de, Kosova vatandaşı olan 20 yaşındaki Ardit Ferizi (diğer adıyla Th3Dir3ctroY), IŞİD'e maddi destek sağlamak ve yetkisiz bilgi edinme sebebiyle 20 yıl hapis cezasına çarptırılmıştır. Mahkeme bilgilerine göre Ardit Ferizi, 1.300 ABD askeri üyesine ve hükümet yetkilisine ait kişisel bilgileri, eski IŞİD üyesi Junaid Hussain'e verdiği ve 11 Ağustos 2015 tarihinde İslam Devleti Hacking Birimi (ISHD) adına Junaid Hussain'in kişisel bilgileri içeren bir belgeyi "*ölüm listesi*" şeklinde Twitter'da yayınladığı belirtilmektedir. Terörist grupların yeteneklerinde bir artış görüldüğünü gösteren bu olay Ocak-Nisan 2021 tarihleri arasında ABD Ulusal Güvenlik Başsavcı Yardımcısı olan John P. Carlin tarafından "*terörizm ve bilgisayar korsanlığının birleşiminden kaynaklanan çok gerçek ve tehlikeli ulusal güvenlik siber tehdidini ilk kez gördüğümüzü temsil ediyor*" şeklinde değerlendirmiştir (DOJ [Department of Justice], 2016).

Tel Aviv Üniversitesi'ne bağlı Ulusal Güvenlik Araştırmaları Merkezi'nin web sayfasında yayınlanan bir çalışmada, 2014 yılında İsrail - Gazze çatışması sırasında İranlı bilgisayar korsanları ve Hizbullah ile bağlantılı olduğu anlaşılan, hem kamu hem de özel kuruluşların hassas verilerini çalmayı amaçlayan kötü amaçlı yazılım bulunduğu açıklanmıştır (Siboni & Kronenfeld, 2014).

2017'de ise Hamas ajanları, sahte sosyal medya profilleri oluşturarak İsrailli askerlerin cep telefonlarına sahte bir arkadaşlık uygulaması indirmesini sağlamıştır. Kötü amaçlı yazılım yüklemek için bir araç olan bu sahte uygulama Hamas'ın, İsrail Savunma Kuvvetleri (IDF) biriminde gerçekleşen eğitim tatbikatları ve operasyonel planlar hakkında bilgi almak için aramalarını, mesajlarını ve e-postalarını izlemesine olanak sağlamıştır (Holmes, 2018).

Sonuç olarak terör örgütleri karşı oldukları ulus devletlerin ve örgütlerin ağlarına zarar vermeyi, hizmetlerini ve operasyonlarını aksatmayı, bilgi toplamayı, gelir elde etmeyi amaçlamaktadır ve etkilerini artırmak için kötü amaçlı yazılım veya casus yazılım gibi saldırgan siber saldırı yeteneklerini aktif olarak geliştirmektedirler (Swearnin, 2019, s. 48).

1.4.2.3. Organize Siber Suçlular

Organize siber suçlular, bilişim ve iletişim teknolojilerinin sunduğu fırsatlarla küresel erişim sağlayarak finansal kazanç sağlama amacı taşımaktadır. Birçok organize suç grupları, internet kumarı gibi çevrimiçi suç pazarlarından yararlanmak, kişisel kimlik bilgilerini çalarak kredi kartı sahtekarlığı gerçekleştirmek, sahte kimlikler kullanarak terörizm gibi ciddi suç türlerini finanse etmek, insan ticaretini kolaylaştırmak, Dark Net'i kullanarak yaban hayatı kaçakçılığı yapmak, uluslararası yasaları ihlal eden uyuşturucuların yasadışı dağıtımını ve satışını kolaylaştırmak, silah kaçakçılığı gibi geleneksel organize suç faaliyetlerini gerçekleştirmek ve organizasyon sağlamak için ağ teknolojilerini kullanmaktadır (UNODC [United Nations Office on Drugs and Crime], 2019). Ayrıca dijital para birimlerini kullanarak suçluların yasadışı fonlarını saklama sürecini de gerçekleştirmektedirler. Özellikle sahte isim veya paravan şirket hesapları, Bitcoin tabanlı dijital para birimleri veya kartlar, yasa dışı kumar siteleri, çevrimiçi oyun siteleri ile kara para aklama sürecini yürütmektedirler (UNODC, 2019).

Örneğin Ağustos 2002-Kasım 2004 arasında faaliyet gösteren ve Dark Net ağının öncüsü olan ilk organize siber suç grubu Shadowcrew, kredi kartı sahtekarlığı, sahte kimlik belgelerinin üretimi ve satışı dahil olmak üzere çok çeşitli suç faaliyetlerini teşvik eden 4.000 üyeli uluslararası bir organizasyon olarak bilinmektedir. Kimlik avı ve spam yöntemleri ile 1,5 milyon çalıntı kredi kartının numarasının ticaretini yaptığı ve kredi kartı şirketlerine, finans kurumlarına ve kart sahiplerine 4 milyon doları aşan kayıplara yol açtığı bilinmektedir (DOJ, 2003). Shadowcrew'un bir parçası olan Albert Gonzales ise 2010'da TJX, Heartland Payment Systems, Barnes & Noble, Office Max ve Citibank gibi şirketleri hedef alarak bilgilerini çalmaktan 20 yıl hapis cezasına çarptırılmıştır (Kovacs, 2014).

Sonuç olarak 2000'lerin başında ticaret ve finans veri tabanlarının çevrimiçi hale gelmesi yeni suç türlerini ortaya çıkartmıştır. Siber uzayda meydana gelen tüm bu suç faaliyetlerinin yaklaşık %80'inin bir tür organize faaliyetten kaynaklandığı tahmin edilmektedir (BAE Systems Detica, 2012). Siber uzayın sınır tanımaz ve anonim doğası, dünyanın farklı yerlerinde ortak bir amaç veya çıkarları paylaşan bireylerin birleşerek suç ağları oluşturmaya olanak vermekte ve bu suç grupları kanun yaptırımlarından kaçınmak için taktiklerini ve tekniklerini geliştirmektedir (UNODC, 2010).

1.4.2.4. Siber Paralı Askerler

Siber saldırı yeteneklerine sahip uzman bilgisayar korsanlarından oluşan siber paralı askerler, teknik becerilerini ulus devletlere, özel şirketlere ve bireylere mali kazanç karşılığında sunmaktadır. Hacktivistler veya hacker grupları daha sınırlı büyüklüklere sahip ve gayri resmi bir yapıya sahipken, siber paralı askerler askeri operasyonları planlama, yürütme ve koordineli bir şekilde hareket etme yeteneğine ve istikrarlı yapılara sahiptir (Bussolati, 2015, s. 115). Devlet desteği aldıklarında ise istihbarat teşkilatı veya kolluk kuvvetlerinin desteği ile çalışabilmektedirler. Ancak ulus devletlerin, siber paralı askerden yararlanabilir olmasından dolayı, devlet aktörleri ve devlet destekli aktörler arasında ayırım yapmak gerekir.

Örneğin 2013 yılında keşfedilen "Icefog", tedarik zincirini hedefleyen, APT saldırıları gerçekleştiren, "*saldır ve çalıştır*" operasyonları yürütmek için işe alınan siber paralı askerler olarak bilinmektedir (Iovan & Iovan, 2016). Özellikle Güney Kor

ve Japonya'daki devlet kurumlarını, askeri ve savunma müteahhitlerini, denizcilik ve gemi inşa gruplarını, telekomünikasyon ve uydu operatörlerini, endüstriyel ve yüksek teknoloji şirketlerini hedef alarak çeşitli kaynaklara erişmek için hassas belgeleri, şirket planlarını, kimlik bilgilerini ve parolalarını ele geçirmek için faaliyet göstermiştir.

1.4.2.5. Siber Milisler

Geçici veya kalıcı olarak oluşturulabilen ve hükümet meseleleri ile ilgilenen siber milisler, kimliklerini gizli tutarak siyasi bir amaca ulaşmak için siber saldırı yeteneklerini kullanabilen bir grup gönüllü olarak tanımlanmaktadır. Devletin kontrolü altında, devletin siber gücünün bir uzantısı olabilmekte ya da ulusal güvenlik için bir tehdit haline gelebilmektedirler (Ottis, 2020). Siber saldırılara yanıt vermek için gönüllü bilgisayar korsanlarının işe alındığı Estonya'da siber milislere istihdam sunulmakta, hastanelere, bankalara, askeri üslere veya oylama sistemlerine yönelik bu tür saldırılarla başa çıkmak için eğitilmektedirler (Pawlicka, Choras, & Pawlicki, 2021, s. 848)

Çin'de ise araştırmacılara göre siber milislerin sayısı 10 milyonu aşan bir sayıya ulaşmış bulunmakta ve Çinli bilgisayar korsanları, herhangi bir siyasi kriz sırasında çok hızlı bir şekilde harekete geçmeleri ve saldırımları ile tanınmaktadırlar (Lyll, 2018). 1 Nisan 2001'de Amerikan EP-3 gözetleme uçağı ile Çinli bir savaş uçağının arasındaki çarpışmadan kısa bir süre sonra misilleme olarak gönüllü bilgisayar korsanlarının katılımı ile iki ulus devlet arasında siyasi güdümlü siber saldırılar başlatılmıştı. Çinli bilgisayar korsanları tarafından ABD Sağlık Bakanlığı, ABD Çalışma Bakanlığı, ABD Maden Kaynakları İdari Bürosu gibi hükümet sitelerinin yanı sıra Kaliforniya Enerji Departmanı'nın sitesi, imalat firmaları ve küçük işletmelere yönelik geniş bir siber saldırı gerçekleştirilmiştir (FoxNews, 2015). Bu gayri resmi siber saldırılar, açıkça Pasifik'in her iki tarafındaki bilgisayar korsanlarının işi olsa da, politik olarak motive olmuş bilgisayar korsanlarının ne kadar hızlı harekete geçebileceğinin ve ülkeyi saldırılara karşı savunmak için siber milislerin etkisinin bir örneği olarak görülmektedir (Applegate, 2011, s. 17).

1.4.2.6. Bilgisayar Korsanları

Siyah Şapkalı Bilgisayar Korsanları (Black-hat hackers) ; Kötü amaçlı yazılımları üreterek ve siber saldırı tekniklerini kullanarak ağlara erişim sağlayabilen, güvenlik açıklarından yararlanarak sistem güvenliğine zarar verebilecek kapsamlı deneyime sahip kişiler, siyah şapkalı bilgisayar korsanları olarak tanımlanmaktadır. Büyük veri ihlallerinin arkasındaki bu siber saldırganlar finansal kazanç elde etmek, verileri yok etmek veya değiştirmek, siber casusluk faaliyetleri yürütmek veya sadece eğlence amaçlı yasaları çiğnemektedirler. Kredi kartı, oturum açma bilgileri, sosyal güvenlik numarası dahil olmak üzere büyük şirketler veya hükümetler tarafından tutulan kişisel ve finansal bilgilerin çalınmasında rol oynamakta ve çoğu zaman bu bilgilerin Dark Web üzerinden satışını sağlamaktadırlar (Rafter, 2022). En ünlü siyah şapkalı bilgisayar korsanları arasında ise FBI'ın "*En Çok Aranılan Listesine*" giren ilk bilgisayar korsanı olma ayrıcalığına sahip Kevin Mitnick'tir. ABD'de ulusal savunma uyarı sistemi dahil Motorola, Nokia, Novell, Fujitsu, Sun Microsystems ve Güney Kaliforniya Üniversitesi'ndeki bilgisayarlara yönelik korsanlık faaliyetleri gerçekleştirmiştir. 1989'da ABD merkezli bir bilgisayar üreticisi olan Digital Equipment Corporation'ın (DEC) ağını hackleyerek 1 milyon dolarlık özel yazılımları çalması üzerine tutuklanmıştır (Christensen, 1999). 2000 yılında serbest bırakıldıktan sonra beyaz şapkalı bilgisayar korsanı olarak bilgi güvenliği sektöründe lider bir konumda faaliyet göstermeye başlamıştır (Mitnick Security, tarih yok).

Beyaz Şapkalı Bilgisayar Korsanları (White-hat hackers); Genellikle şirketler ve devlet kurumları için ücretli çalışan beyaz şapkalı korsanlar, sistem güvenliğini sağlamak için yasal olarak bilgisayar korsanlığı yoluyla, güvenlik açıklarını bulmaya çalışan ve iyileştirme için önerilerde bulunan sertifikalı güvenlik uzmanlarıdır. Örneğin Charlie Miller 2008 yılında Apple'ın güvenlik açıklarını keşfederek ün kazanmış ve ABD Ulusal Güvenlik Ajansında etik bilgisayar korsanı olarak görev almıştır (Kaspersky, tarih yok).

Gri Şapkalı Bilgisayar Korsanları (Grey-hat hackers); Sistemdeki güvenlik açıklarını sistem sahiplerinin bilgisi dışında ve yasal olmayan yollar ile tespit eden gri şapkalı bilgisayar korsanları, sistem açıklarını iyileştirmek için genellikle ücret talep etmektedirler. Siyah şapkalı bilgisayar korsanları kadar kötü niyetli olmayan bu saldırganlar güvenlik açıklarını yasa dışı olarak kullanmazlar veya başkaları ile

paylaşmazlar (Kaspersky, tarih yok). 2013 yılında Mark Zuckerberg'in Facebook sayfasını hackleyen Khalil Shreateh iyi bilinen gri şapkalı bilgisayar korsanlarından biridir. Herhangi bir kullanıcının sayfasında izni olmadan gönderi paylaşımı yapılmasına izin veren bir açığı düzeltmeye zorlamak amacıyla yaptığı bu eylemden sonra Facebook, bu güvenlik açığını düzeltmiştir (Rafter, 2022).

1.4.2.7. Senaryo Çocukları

Bilgisayar korsanları kadar yetenekleri gelişmemiş olan senaryo çocukları, siber güvenlik açıkları konusunda daha az deneyimlidir ve kendi kötü amaçlı yazılımlarını geliştirme ve üretme konusunda teknik bilgilere sahip değildir. Kullandıkları siber saldırı yöntemlerini öğrenmekle ilgilenmezler, bunun yerine bir ağa veya sisteme sızmak için başkaları tarafından yazılmış ve internette buldukları kötü amaçlı yazılımları kullanarak gerçekleştirmesi kolay saldırıları rastgele kullanmaktadırlar (Lutkevich, 2021). Kullandıkları yöntemlerin nasıl çalıştırıldıkları ve sebep oldukları zarar hakkında çok az bilgi sahibidirler. Motivasyonları ise eğlenmek, kaos yaratmak, dikkat çekmek veya kötü ün kazanmaktır. Örneğin 2015 yılında yaşları 15 ile 18 arasında değişen altı genç Lizard Squad'ın Lizard Stresser aracını kötü niyetli bir şekilde kullanarak web sunucularına yönelik DDoS saldırıları gerçekleştirdikleri için tutuklanmıştır. Lizard Stresser aracını, anonim kalmak için Bitcoin gibi alternatif ödeme hizmetleri kullanarak satın alan şüphelilerin, ulusal bir gazeteyi, bir okulu, çevrimiçi oyun şirketini hedef aldıkları bilinmektedir (Gibbs, 2015).

1.4.2.8. İnternet Trolleri

Trolleme davranışını neyin oluşturduğuna, eylemlerin arkasındaki motivasyona ve amaçlarına ilişkin çeşitli ve birbirinden çelişkili tanımlamalar mevcuttur. Çoğu araştırmacı trollemenin büyük ölçüde çevrimiçi oyun alanına indirgemekte ve genel olarak internet ortamında sözlü ve davranışsal olan her türlü kötü niyetli çevrimiçi davranışı tanımlamak için kullanmaktadır (Cook, Schaafsma, & Antheunis, 2017). Aldatıcı ve uydurma içerikleri yayma aracı olarak birçok kişi ve kuruluş tarafından kullanılan trollük, hedef kişiler veya firmalar için olumsuz sonuçlar doğurabilecek

manipölasyonun kasıtlı kullanımını içermektedir (Papez & Veer, 2017). Avustralya Enstitüsü'nün 2019'daki araştırmasında trolleme ve çevrimiçi kötüye kullanımın Avustralya'da ekonomik olarak sağlık maliyetleri ve gelir kaybı açısından 3,7 milyar dolara mal olduğu tahmin edilmiştir (The Australia Institute, 2019).

Trollerin alt grubu olarak ortaya çıkan, amacı çatışma ve aldatma yaratan kullanıcı hesaplarından oluşan "*siyasi trollerin*" ise niyetleri, siyasi sürece zarar vermek ve siyasi sistemde güvensizlik yaratmaktır (Addawood, Badawy, Lerman, & Ferrara, 2019, s. 15). Birçok siyasi trol grubu, kamuoyunu manipüle etmek için çeşitli sosyal medya ağları üzerinde çalıştırılan "*siyasi botlar*" oluşturmaktadır (Woolley & Howard, 2016, s. 4885). Aynı şekilde nefret kampanyaları yürüten ve sahte haber yayan hem bireysel hem de devlet destekli trol grupları da mevcuttur. Örneğin 2016 ABD seçimlerinde Rusya'nın kamuoyunu etkilemek için sosyal medya uygulaması olan Twitter'da belirli adayları desteklemek, siyasi olarak taraflı bilgileri yaymak veya "sahte haberler" enjekte etmek için trol hesapları ve siyasi botları kullandığı iddiası söz konusudur (Addawood vd., 2019). Ocak 2017 tarihli ABD İstihbarat Topluluğu Değerlendirmesinde (Intelligence Community Assessment-ICA), İstihbarat Topluluğu, Rusya Devlet Başkanı Vladimir Putin'in 2016 yılında ABD başkanlık seçimlerini hedefleyen etki kampanyası emrettiği, Hillary Clinton'ın kampanyasına zarar verme ve Donald Trump'ın kampanyasına yardım etme çabalarının olduğu belgelenmiştir (CIA, FBI, & Press, 2017).

1.4.2.9. İçerideki Siber Tehdit Aktörleri

Günümüzde kurum ve kuruluşların siber güvenlik planlamalarında dikkate alması gereken tek siber tehdit, dışarıdaki saldırganlardan değildir, içerideki siber tehdit aktörleri de farklı sektörler için önemli bir sorundur. Bu sorun kurum içerisindeki sistemlere ve verilere meşru erişimi kötüye kullanarak, kişisel kazanç için veya ihmalden kaynaklı hassas verileri sızdıran, değiştiren veya silen kişilerden kaynaklanmaktadır (Rosenthal, 2022a). Ponemon Enstitüsünün 2022 yılında hazırladığı İçeriden Tehditlerin Maliyeti: Küresel Rapor'un ortaya koyduğu gibi, içeriden tehdit olayları son iki yılda %44 artış göstermiştir ve olay başına maliyet üçte bir oranında artarak 15,38 milyon olarak ulaşmıştır (Ponemon Institute, 2022).

Covid-19 pandemisi sürecinde birçok sektör kısmi kapanma yaşamış veya çalışanlar işten çıkartılmıştır. Bu durum ise kötü amaçlı içeriden tehdit aktörlerinin çoğalmasına sebep olmuştur. Örneğin Mart 2020'de tıbbi cihaz paketleme şirketinin eski çalışanı olan Christopher Dobbis, eski işverenin paket nakliye sistemine sızarak, 120.000 nakliye kaydını silmiş ve tıbbi ekipmanların hizmet sağlayıcılarına ulaştırılmasında önemli gecikmeler yaşanmasına sebep olmuştur (DOJ, 2020).

Kişisel kazanç için gerçekleştirilen örneklerden biri ise 2018 yılında şirketin güvenlik açıklarına ilişkin içeriden edildiği bilgileri kullanarak Ukrayna vatandaşlarına kredi hizmeti sunan bir finans şirketinden elde ettiği 100 GB'a yakın veriyi, 4.000 dolarlık pazarlık fiyatına satmaya çalışan şahıs, Ukrayna Siber Polis Departmanındaki memurlar tarafından tutuklanmıştır (Cimpanu, 2018)

2018 yılında ise FSB, ülkenin önde gelen nükleer laboratuvarı olan ve Rus ordusu tarafından sürekli koruma altında tutulan izole edilmiş Sarov şehrindeki Rusya Federal Deneysel Fizik Araştırma Enstitüsü'nde (RFNC-VNIIEF) çalışanlar, Rusya'nın en güçlü süper bilgisayarlarından bazılarına erişimlerini kötüye kullanarak Bitcoin madenciliği girişiminde bulunmuşlardır (Cimpanu, 2018a).

1.5. Siber Unsurlar : Kritik Altyapılar

Kritik altyapı, hükümet tarafından hayati olan toplumsal işlevlerin, sağlık hizmetlerinin, güvenliğin, ekonomik ve sosyal refahın sürdürülebilmesi için bir ülkede bulunan varlık, sistem veya bunların bir bölümünü tanımlamak için kullanılan terimdir. (Official Journal of the European Union, 2008). Tüm bu işlevlerin sürdürülememesi, bir devletin temel toplum hizmetlerini yürütme kabiliyetini ciddi şekilde işlevsiz hale getirerek uzun bir süre boyunca ekonomik, siyasi ve sosyal istikrarsızlığı meydana getirebilmektedir.

Ulusal siber güvenlik stratejilerinin belirlenmesi kapsamında birçok ülke tarafından hazırlanan stratejik planlarda, farklı kritik altyapıları içeren sektörler belirlenmiştir (Kurnaz & Karatepe, 2019). Hükümetler özellikle internete bağlı ve siber tehditler karşısında savunmasız sektörleri kritik ulusal altyapı olarak değerlendirmektedir. Örneğin ABD hükümeti tarafından tanımlanan tarım ve gıda, ticari tesisler, iletişim, finansal hizmetler, sağlık, bilgi teknolojisi dahil toplam 16

kritik altyapı türü açıklanmıştır. ABD'de kritik altyapı olarak belirlenen sektörlerin tamamı, işlevlerini yerine getirebilmek için internete bağlı olması sebebiyle siber saldırılara karşı hassas olduğu ileri sürülmektedir (Çifci, 2012, s. 13).

Şekil 7: Kritik Altyapı Sektörleri

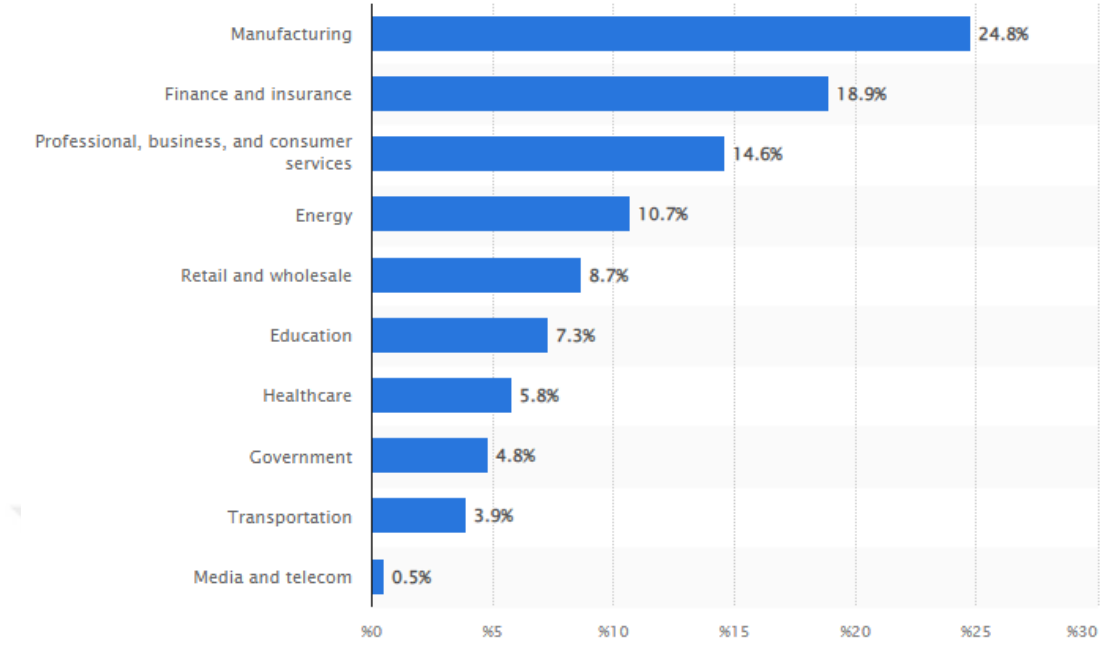


Kaynak: <https://www.gao.gov/products/gao-23-105806>

16 temel sektör; enerji (elektrik üretimi, iletimi ve dağıtımı, petrol ve doğal gaz tesisleri), su ve atık su (su temini, arıtma ve dağıtım sistemleri), iletişim (telekomünikasyon altyapısı, internet sağlayıcıları, haberleşme ağları), ulaşım (havaalanları, limanlar, demiryolları, köprüler, tüneller, karayolları), finans (bankalar, ödeme sistemler, borsalar, finansal kurumlar), sağlık (hastaneler, sağlık hizmeti sağlayıcıları, tıbbi cihazlar veya sistemler), acil servis, gıda ve tarım (gıda üretimi, tarım tesisleri, gıda dağıtım ağı), savunma sanayi (askeri tesisler, stratejik silah sistemleri), kimya (kimyasal üretim tesisleri, tehlikeli maddelerin depoları), nükleer enerji (nükleer santraller, nükleer yakıt tesisleri), ticari ve devlet tesisler (hükümet daireleri, adalet sistemi, acil durum hizmetleri), kritik imalat, baraj, bilgi teknolojisi (yapay zeka, robotik, IoT) şeklinde sıralanmaktadır.

Fiziksel zarar verme amaçlı kullanılan siber saldırı araçları, hükümet sistemlerini veya birçok kritik altyapıları hedef almaktadır. Kritik altyapı sistemleri arasındaki karşılıklı bağımlılıklar da göz önüne alındığında tehlike olasılığı, sektörler arasında kademeli bir etki gösterebilecek şekilde risk ortamını artırmaktadır (CISA, 2016, s. 3).

Şekil 8: Sektöre Yönelik Siber Saldırı İstatistikleri



Kaynak: Statista. (2023a). Distribution of cyber attacks across worldwide industries in 2022. <https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/>

2022 yılında yapılan bir analize göre, imalat sektörü dünya genelinde önde gelen sektörler arasında en yüksek siber saldırı payına sahip olmuştur. İncelenen yıl boyunca, finans ve sigorta sektörü ise yaklaşık %19'luk pay ile ikinci sırada yer almıştır.

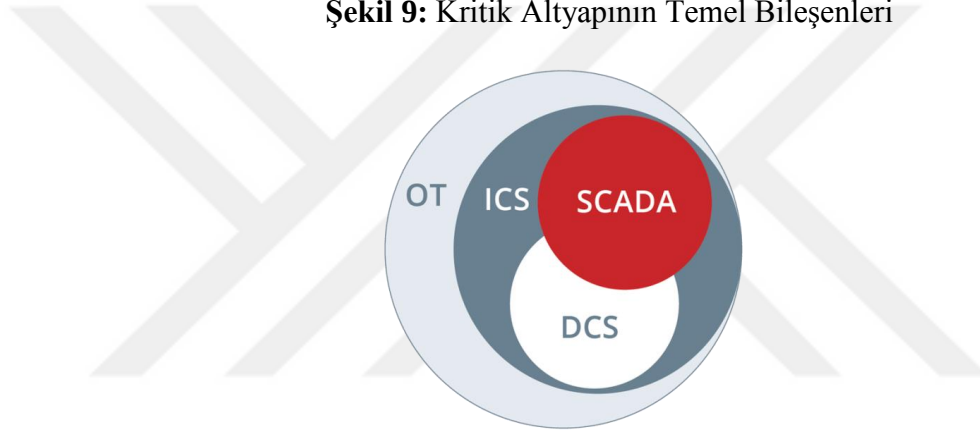
Tüm kritik altyapı sistemleri, giderek artan bilgi odaklı ortamda faaliyet gösteren bilgi teknolojileri (BT) altyapısına büyük ölçüde bağımlı hale gelmektedir. Bununla birlikte, kritik altyapılara yönelik siber saldırılar yapıldığı, bu kritik altyapıların kontrolünün siber tehdit aktörleri tarafından ele geçirildiği, çalışamaz hale getirildiği ve kritik altyapılarda yer alan hassas bilgilerin çalındığı birçok vaka yaşanmıştır (Ünver & Canbay, 2010, s. 98). Bu saldırılara ek olarak ulus devletler arasındaki gerilimler ve çatışmalar neticesinde siber saldırı araçlarının konvansiyonel saldırıyı desteklemek için kullanıldığı vakalar da mevcuttur.

1.5.1. Kritik Altyapının Temel Bileşenleri (ICS, DCS, SCADA, OT)

Kritik altyapının temel bileşenleri; Endüstriyel Kontrol Sistemi (ICS), Denetletici Kontrol ve Veri Toplama Sistemi (SCADA), Dağıtılmış Kontrol Sistemi

(DCS) ve Operasyonel Teknolojidir (OT). Tüm bu sistemler, kritik altyapı tesislerinin süreçlerini izlemek ve kontrol etmek için kullanılan karmaşık ve otomatik kontrol sistemleridir. Ancak bu sistemlerin çoğu, onlarca yıl önce siber güvenlik düşünülmeden tasarlanmıştır. Bu nedenle, bu sistemler siber tehdit aktörlerinin saldırılarında en savunmasız noktalardan biri haline gelmiştir. Kritik altyapının en zayıf noktası haline gelen bu sistemlere yönelik gerçekleştirilen siber saldırılar sonucunda, bu sistemlerdeki güvenlik açıklarından faydalanılarak arıza süresinin uzamasına veya tesislerin kapatılması gereken acil durumlara sebep olan vakalar yaşanmıştır.

Şekil 9: Kritik Altyapının Temel Bileşenleri



Kaynak:[https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/#:~:text=Industrial%20Control%20System%20\(ICS\)%20is,belts%20in%20a%20mining%20operati on](https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/#:~:text=Industrial%20Control%20System%20(ICS)%20is,belts%20in%20a%20mining%20operati on)

Operasyonel Teknoloji (OT), fiziksel süreçleri ve kritik altyapıyı izlemek, kontrol etmek ve yönetmek için programlanabilir donanım, yazılım ve ağ sistemlerini kapsayan genel bir terimdir. İmalat, elektrik üretimi, petrol ve doğal gaz, lojistik, madencilik, su, otomasyon sistemleri gibi birçok kritik altyapının fiziksel süreçlerinin izlenmesinden, üretimdeki cihazların kontrol edilmesine kadar çok çeşitli görevleri yerine getirmektedir. Örneğin bina yönetim sistemlerini, yangın kontrol sistemlerini ve fiziksel erişim kontrol mekanizmalarını içermektedir (National Institute of Standards and Technology [NIST], 2018).

Tarihsel olarak, kritik altyapılarda iki tür kontrol sistemi kullanılmıştır: uzak alandaki verileri hızla toplayan Denetleyici Kontrol ve Veri Toplama Sistemleri (SCADA) ve otomatikleştirilmiş üretim süreçlerini yöneten Dağıtılmış Kontrol Sistemleri (DCS) (Kesler, 2011, s. 16).

Endüstriyel kontrol sistemlerinin yazılım tabanlı unsurlarından olan SCADA'nın temel amacı, sensörler ve cihazlar tarafından sağlanan verileri toplama, izleme ve analiz etmektir. SCADA sistemler, genellikle uzaktaki bir merkezi kontrol noktasından, geniş coğrafi alanlara yayılan endüstriyel tesislerin süreçlerini yönetmek için kullanılır ve uzak bölgelerdeki süreçlerin durumu izlenerek, gerekli müdahaleler yapılabilir ve veriler analiz edilerek operasyonel kararlar alınabilir (Aissa, Rabai, Abercrombie, Mili, & Sheldon, 2014). Örneğin doğal gaz ve elektrik enerjisinin dağıtımı gibi hizmet sağlayan tesislerin tek bir merkezden izlenebilmesi ve kontrolünün yapılması için kullanılmaktadır. Bir sistem genelinde sensörler, iş istasyonları ve diğer ağ bağlantılı cihazlar arasında gerçek zamanlı ve iki yönlü veri akışı sağlanmaktadır (Lehto, 2022). İlk tasarlandığı dönemlerde, güvenlik yerine operasyonel gereksinimler dikkate alınarak sadece kontrol ve veri bilgilerini taşımak için ilkel seri protokoller ve iletişim altyapıları kullanılmıştır (Chandia, Gonzalez, Kilpatrick, Papa, & Shenoi, 2007). Dolayısıyla herhangi bir güvenlik mekanizması olmadan tasarlanan SCADA protokolü ciddi güvenlik sorunlarını meydana getirmektedir. Siber tehdit aktörleri de kritik altyapının çoğunu çalıştıran SCADA sistemlerindeki güvenlik açıklarından yararlanmaktadır.

DCS sistemi, denetçileri, sensörleri, operatörleri ve sistemi kontrol eden motorları birbirine bağlayan bir bilgisayar sistemidir. SCADA sistemi verileri toplamaya öncelik verirken, DCS sistemleri süreçlerin merkezi kontrolüne odaklanır. Kontrol ağı olarak adlandırılan ve merkezin beyni olan DCS, üretime dayalı olarak otomatik kararlar alabilir. Örnek olarak, bir elektrik santralindeki DCS, sıcaklığın yüksek olduğu günlerde değişen elektrik talebine karşılık verebilmek için birden fazla türbinin buhar üretim kapasitesini otomatik olarak artırabilir, dış hava sıcaklıkları soğuduğunda ve talep azaldığında kapasitesini azaltabilir (ControlStation, 2018).

Endüstriyel Kontrol Sistemi (ICS), endüstriyel ortamlarda ve kritik altyapılarda bulunan Denetleyici Kontrol ve Veri Toplama Sistemi (SCADA) ve Dağıtılmış Kontrol Sistemi (DCS) gibi çeşitli kontrol sistemlerini içeren genel bir terimdir. İmalat gibi endüstriyel bir amaca ulaşmak için birlikte hareket eden elektrik, mekanik, hidrolik gibi kontrol bileşenlerinin kombinasyonlarından oluşmaktadır (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014, s. 2-1).

1.5.2. Enerji Sektörü

Enerji sektörünün alt yapısı üç bölüme ayrılmaktadır; elektrik, petrol ve doğal gaz. Enerji altyapısı, diğer sektörlerin temel hizmetlerini sunmak için enerjiye bağımlılığı sebebiyle en kritik ve karmaşık altyapılardan biridir. Ayrıca enerji altyapısı son derece otomatiktir; elektrik üretimi, dağıtımı ve iletimi süreçleri SCADA veya DCS gibi karmaşık enerji yönetim sistemleri kullanılarak kamu hizmetleri ve bölgesel şebeke operatörleri tarafından kontrol edilmektedir (Department of Homeland Security [DHS], 2014).

Enerji arzının olmaması, ekonominin ve sosyal yaşamın düzgün işleyişi üzerinde büyük etki yaratabilmektedir. Enerji sektöründeki hızlı dijitalleşmenin ardından, enerji sistemlerinin siber güvenliğinden ve enerji teknolojisindeki jeopolitik rekabete kadar sektörün dijital güvenlik endişeleri hem ulusal hem de uluslararası kamusal ve özel alanlara nüfuz etmiştir (Goldthau, Westphal, Bazilian, & Bradshaw, 2019).

Enerji sektörüne yönelik önemli vakalardan biri *Shamoon Virüsü*'dür. 15 Ağustos 2012'de Suudi Arabistan'ın ulusal petrol ve doğal gaz şirketi olan Saudi Aramco'ya yönelik gerçekleştirilen siber saldırının hemen ardından 30.000'den fazla bilgisayar hasar görerek kullanılamaz hale getirilmiştir (Reuters, 2012). Siber saldırıda, Suudi Arabistan'daki petrol, doğal gaz üretimini ve yapılan petrol ihracatını aksatma amacıyla "*Shamoon*" (W.32.Disttrack) adı ile bilinen, bilgisayarların sabit disklerinden verileri silerek imha etmek için tasarlanan bir bilgisayar virüsü kullanılmıştır. Saldırı sonrasında ise Saudi Aramco, hasarın ofis bilgisayarlarıyla sınırlı olduğunu ve teknik operasyonlar için kullanılan sistemleri etkilemediğini bildirmiştir (Meer, 2015). Dolayısıyla saldırı Suudi Arabistan'ın petrol ve doğal gaz akışını fiilen bozmayı başaramamıştır. Ancak saldırı başarılı olsaydı, Suudi Arabistan'ın petrol endüstrisine ve ekonomisine ciddi zararlar verebilir, dünya petrol rezervinin önemli bir bölümünü kontrol ettiği için bu tür bir kesinti küresel enerji piyasalarında da ekonomik sorunları beraberinde getirebilirdi.

Saldırıyı kendilerini "*Adaletin Keskin Kılıcı*" (Cutting Sword of Justice) olarak tanıtan İranlı bir grup hacker, "*insanlığa karşı işlenen suçlardan*" dolayı Suud rejimine misilleme yaptıklarını iddia ederek üstlenmiş olsa da, ABD istihbarat kaynakları, güvenlik firmaları, çeşitli uzman ve yazarlar operasyonu doğrudan İran hükümetine

atfedilmesi konusunda mevcut iddialarda bulunmuştur. (Council on Foreign Relations [CFR], 2012). Ancak Aramco veya Suudi Arabistan hükümeti tarafından hiçbir ülke açıkça suçlanmamıştır.

Shamoon virüsü, bölgede siyasi çatışmaların olduğu dönemde kullanılmış ve ardından siber saldırılar yaygınlaşmıştır. Nitekim 27 Ağustos 2012'de ise dünyanın en büyük doğal gaz üreticilerinden biri olan ve bilgisayar virüsü tarafından hedef alınan ikinci Orta Doğu enerji şirketi Katarlı RasGas hedef alınarak sistemleri çevrim dışı duruma getirilmiş ve gözler tekrar Tahran'ın siber yeteneklerine yönelmiştir (Hall & Blas, 2012).

1.5.3. Barajlar Sektörü

Baraj projelerini, setleri, hidroelektrik santrallerini, kasırga bariyerlerini, maden atıklarını, endüstriyel atık barajlarını ve seyir kilitlerini içeren barajlar sektörü, çok çeşitli ekonomik, çevresel ve sosyal faydalar sağlamakta ve ulusal çıkarlarda hayati bir rol oynamaktadır. 1943'de II. Dünya Savaşı sırasında Alman Möhne ve Eder Barajları, 1952'de Kore Savaşı sırasında Kuzey Kore Sui-Ho barajı, hidroelektrik tesisi ve çok sayıda küçük ölçekli yerel saldırılar dahil olmak üzere, barajlara yönelik fiziksel saldırıların tarihsel örnekleri mevcuttur (Schoolmeesters, tarih yok). Fiziksel tehditlerden korunmakla daha çok ilgilenen barajlar sektörü, günümüzde siber saldırılarla karşı karşıya olan sektörlerden biridir.

Yangınla mücadele kapsamında acil servis müdahalesinden, ulaştırmada, gıda ve tarımda, bir topluluğun su temininden, sulama ve sel kontrolünden sorumlu olan barajlar, siber saldırıların hedefi haline gelmekte ve saldırılara karşı savunmasız olabilmektedir. Su seviyesi veya su kalitesi ile ilgili anormalliklere karşı uyarı kontrol sisteminin siber saldırılara maruz kalması, yerel su kaynağına ciddi zararlar verebilir (Dennis, Rajtmajer, & Grady, 2020). Örneğin bir siber tehdit aktörü, bir hidroelektrik barajındaki BT sistemlerini desteklemek için sözleşmeli bir mühendislik firmasına gönderdiği kimlik avı e-postaları aracılığıyla topladığı bilgiler ile mühendislerin sistemine erişim sağlayabilir. Sonucunda ise barajdaki su çıkışlarını maksimum yüksekliğe gelmesi için komut verebilir ve kontrolsüz bir su çıkışına sebep olabilir. Bu ani çıkış ise hidroelektrik santralindeki türbinlere zarar verebilme ve aynı zamanda evlere, işyerlerine doğru su baskınına sebep olma ihtimalini barındırmaktadır (Laux &

Honea, 2018). Dolayısıyla, barajlara yönelik büyük ölçekli siber saldırılar, topluluk geneline, işletme sahiplerine, sigortacılara ekonomik olarak büyük kayıplar yaşatabilir. Barajlar sektöründe Maroochy Shire Olayı ve New York Barajı'na yönelik siber saldırı önemli iki vaka olarak verilmiştir.

Maroochy Shire Olayı; Avustralya Queensland'da yer alan, günde ortalama 35 milyon litre atık su arıtan 880 kilometrelik yerçekimi kanalizasyonuna sahiptir. 2000 yılında Maroochy Shire için çalışan Vitek Boden istifa ettikten bir süre sonra Maroochy Shire Belediyesi'nin kanalizasyon sistemini kontrol eden bilgisayarlara yasa dışı erişim sağlamış ve kanalizasyon pompa istasyonlarının işleyişinde arızalara sebep olabilecek bir siber saldırı gerçekleştirmiştir. Saldırı sonrasında pompalar çalışması gereken zamanda çalışmamış, alarmlar merkezi bilgisayarlara rapor verememiş ve merkezi bilgisayar ile pompa istasyonları arasında iletişim kesilmiştir (Abrams & Weiss, 2008). 265.000 galon arıtılmamış atık su kanalizasyondan, yerel parklara ve nehirlerle bırakılmasıyla, vahşi yaşamın son bulmasına ve doğa rezervlerinin yok edilmesine sebep olmuştur (Cohen, 2021).

Boden'in işlediği suç dünya çapında BT güvenlik uzmanlarının ilgi odağı haline gelmiştir. Çünkü Maroochy'nin kontrol sistemi, siber güvenlik düşünülerek tasarlanmamıştır. Boden'in Maroochy'nin kontrol sistemine girme kolaylığının, herhangi bir siber saldırganın tüm şehirlerde gaz veya elektrik tedarikini kolayca bozabileceğini yansıtmıştır. Maroochy'deki kanalizasyon pompalarını kontrol eden bilgisayar sistemi ve endüstriyel kontrol sistemleri, neredeyse tüm endüstrilerin ve altyapıların üzerine inşa edildiği bir temeldir (Levi, 2016).

New York Barajı Siber Saldırısı; ABD Adalet Bakanlığının 2016 yılında hazırladığı iddianameye göre, İran İslam Devrimi Muhafızları Kolordusu üyelerinden olan Hamid Firoozi, 2013 yılında Bowman Avenue Barajı'nın SCADA sistemine izinsiz erişim sağlamış ve su seviyeleri, su sıcaklığı, akış hızlarının kontrol edilmesinden sorumlu olan savak kapısının durumu dahil Bowman Barajının işleyişi hakkında bilgileri elde etmiştir. Bu durum Firoozi'nin Bowman Barajındaki sistemi manipüle etmesine izin vermiş olsa da, Firoozi'nin sisteme siber saldırısı sırasında, barajın savak kapısı rutin bakım için manüel olarak devre dışı bırakıldığı için sistem zarar görmemiştir (DOJ, tarih yok, s. 14).

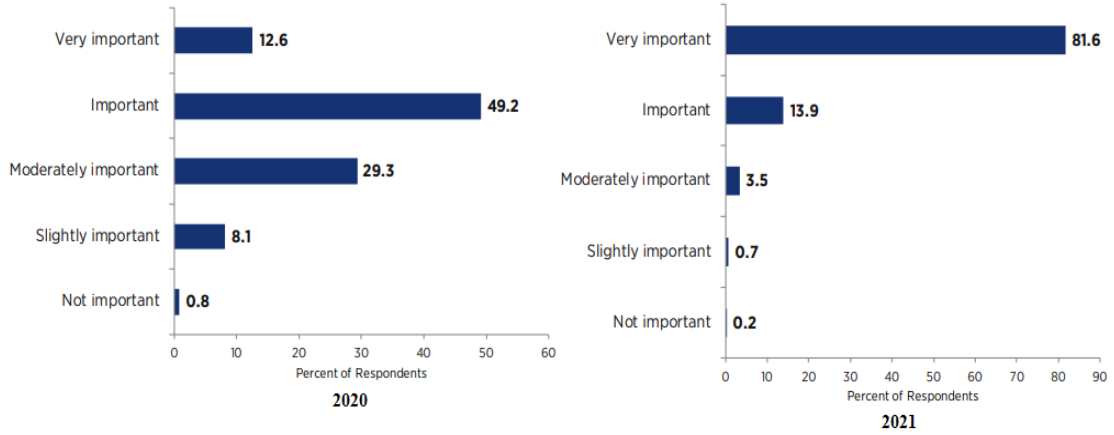
Bu tür vakalarda genellikle bilgi değil, operasyonlar kontrol edilir ve potansiyel olarak bu saldırıların etkisi daha büyüktür. Çünkü operasyon teknolojisine yönelik saldırılar, bilgi teknolojisi saldırılarından farklıdır, çünkü operasyon teknolojisine yönelik saldırılar, fiziksel yıkım yaratabilmektedir (Thompson, 2016).

1.5.4. Finansal Hizmetler Sektörü

Finans sektöründeki kuruluşlar, kredi kartları, mevduat, vasiyet, mülk, tapu ve diğer kritik bilgileri elektronik olarak tutmaktadır. Siber tehdit aktörleri hırsızlık yoluyla kar elde etmek için finans sektörüne yönelmektedirler. Ulus devletler ise politik nedenlerle, ticari casusluk veya hassas verileri elde etmek için finans sektörünü hedef almaktadır (Carter, 2017, s. 14). Günümüzde yaşanan sürekli dijital dönüşüm, mobil bankacılığın yaygınlaşması, karmaşık tedarik zinciri sistemi ve COVID-19'un etkisiyle değişen çalışma alanındaki uygulamalar, siber tehdit aktörlerinin yararlanabileceği saldırı alanlarını genişletmekte ve hassas verileri elde etme fırsatını artırmaktadır. Finans sektörünün siber güvenliğine yönelik tehditler hem iş yapma becerisine zarar verebilmesi nedeniyle operasyonel açıdan hem de şirketlerin itibarı açısından riskler oluşturmaktadır.

IBM X-Force tarafından yapılan araştırmaya göre, finans ve sigorta kuruluşları 2021 yılında gerçekleşen saldırıların %22'sinin hedef noktasındaydı. Bu saldırıların %70'i bankalara, %16'sı sigorta kuruluşlarına ve %14'ü diğer finans kuruluşlarına yönelik gerçekleştirilmiştir. Sunucu erişim saldırıları (%14), fidye yazılımları (%10), kimlik avı saldırıları (%46), güvenlik açıklarından yararlanma (%31), kaba kuvvet saldırıları ve VPN erişimi finans ve sigorta şirketlerine karşı gerçekleştirilen siber saldırılarda gözlenmiştir (International Business Machines [IBM], 2021, s. 44).

Şekil 10: Banka için siber güvenli riski ne kadar önemli? 2020 - 2021



Kaynak: (https://www.csbs.org/sites/default/files/2020-09/cb21publication_2020.pdf),
(<https://resources.gabankers.com/e-Bulletin/2021/Oct.%208/CSBS%20Community%20Bank%202021%20Survey.pdf>)

Devlet Bankası Denetçileri Konferansı (Conference of State Bank Supervisors - CSBS) tarafından Eylül 2021'de gerçekleştirilen ankete göre, siber güvenlik riski %80'inden fazlası tarafından "çok önemli" olarak değerlendirildi; bu sonuç önceki yıl rapor edilenden %60 fazla orandaydı (FRS, CSBS, FDIC, 2021, s. 35).

Bangaleş Banka Soygunu; 4 Şubat 2016'da siber tehdit aktörleri, Bangladeş Merkez Bankasının bilgisayar ağını hedef almıştır. Dünya çapındaki finans kuruluşları arasında uluslararası para transferleri için güvenli mesajlaşma sistemi olan Bankalararası Finansal Telekomünikasyon Derneğindeki (Society for Worldwide Interbank Financial Telecommunication - SWIFT) güvenlik açıklarından yararlanan siber tehdit aktörleri, bankadaki toplam 951 milyon doları çalma girişiminde bulunmuştur. Siber saldırı, bankadaki döviz transferlerinin kayıtlarını basmak için kullanılan bir yazıcının bozulmasıyla başlamıştır. Siber tehdit aktörleri, dünyada birçok bankanın aralarında büyük miktarda para transfer etmek için geliştirdikleri SWIFT sistemine erişim sağlamış ve kendilerini banka çalışanları gibi göstererek New York'taki Bangladeş Merkez Bankası'nın dolar rezervlerini sakladığı ABD Merkez Bankasına hesaptaki tüm paranın çekilmesi talimatını vermiştir (BBC, 2021). Soygunun fark edilmesi ise siber tehdit aktörlerinin, Bangladeş ve New York arasındaki zaman farkını ve tatil günlerini hesaba katması stratejisiyle üç gün gecikmiştir. Bu süreç içerisinde, Manila merkezli Rizal Commercial Banking Corporation'a (RCBC) 81 milyon dolar başarıyla aktararak çalınmıştır (Banka, 2021). Kaspersky dahil olmak üzere farklı BT güvenlik şirketlerinden araştırmacılar

tarafından yürütülen araştırmada 2016 yılında Bangladeş Merkez Bankası'ndan 81 milyon dolarlık kayba sebep olan siber saldırı, üretim şirketlerine ve medyaya saldırmasıyla tanınan Kuzey Koreli Lazarus Grubuna atfedilmiştir (Kaspersky , 2017). Nathan P. Shields isimli FBI müfettişinin beyanına göre, Lazarus Grubu Mart 2015'ten beri Bangladeş Bankası'nın bilgisayar sistemlerinde görünmüş ve kullanılan IP adreslerinden ilki Kuzey Kore'nin başkenti Pyongyang'da bir şirkete kayıtlı, ikincisi ise Çin'de bir şirkete ait Kuzey Kore tarafından kiralanmış veya kullanılmış olan IP adresleri bloğu olarak belirlenmiştir (DOJ, 2008). 2018 FBI raporuna göre 2015'ten 2018'e kadar benzer yöntemler ve "*sulama deliği saldırıları*" kullanılarak çeşitli ülkelerdeki birkaç bankaya erişim sağlanarak en az 1 milyar dolarlık hırsızlık girişimi gözlemlenmiştir (DOJ, 2018).

Ababil Operasyonu; Eylül 2012'de, Izz ad-Din al-Qassam'ın Siber Savaşçıları adlı bir grubun, ABD finans kurumlarını hedef alan siber saldırısı, politik nedenlerle gerçekleştirilmiş bir siber saldırı örneğidir. İran nükleer programını durdurma amaçlı, Washington'ın İran Merkez Bankası ve diğer kuruluşlara ekonomik yaptırımlar uyguladığı dönemde yürütülen Ababil Operasyonu'nda, Bank of America, Wells Fargo, Capital One, BB&T, HCBS ve diğer ABD finans kurumlarının web siteleri ve çevrimiçi bankacılık platformlarını hedef alan DDoS saldırıları kullanılmıştır (Perlroth & Hardy, 2013). ABD'de ticari işlevleri geçici olarak kesintiye uğratan siber saldırı sonucunda, banka web siteleri devre dışı bırakılmış, müşterilerin hesaplarına çevrimiçi olarak erişimi engellenmiş ve saldırıları etkisiz hale getirmek için çalışan bankalara on milyonlarca iyileştirme maliyetine neden olan etkili bir kampanya yürütülmüştür (DOJ, 2016a). Saldırının sorumluluğunu üstlenen Izz ad-Din al-Qassam ise, Hz. Muhammed ile alay eden İslam karşıtı bir videoya misilleme olarak bankalara saldırdığını ilan etmesine rağmen uzmanlar saldırıyı, İran nükleer zenginleştirme ekipmanını devre dışı bırakan, ABD ve İsrail'e atfedilen Stuxnet saldırısına misilleme olarak değerlendirmiştir (Nakashima, 2012).

1.5.5. Gıda ve Tarım Sektörü

Tarihsel olarak gıda ve tarım sektörü, siber tehdit aktörleri için kayda değer bir hedef olmamıştır. Çok uluslu tarım işletmelerinin yükselişinden önce, dünyadaki gıda ve tarım üretiminin çoğu küçük çiftçiler ve yerel bir topluluğa hizmet eden çiftçiler

tarafından sağlanmaktaydı. Ancak tarımla ilgili teknolojik ilerlemeler sonucunda gıda ve tarım sektörü, siber saldırıların giderek daha fazla hedefinde olan kritik altyapı sektörleri arasında yer almaya başlamıştır (Bowcut, 2021). Bu durum ile ilgili Eylül 2021 yılında FBI gıda ve tarım sektörünü potansiyel siber tehlikelere karşı uyarmak için *Özel Sektör Bildirimi* yayınlamıştır. Bildiriye göre fidye yazılımlarının hedefi olan gıda ve tarım işletmeleri, fidye ödemeleri, üretkenlik kaybı ve iyileştirme maliyetlerinden kaynaklanan önemli mali kayıplara maruz kalmaktadır. Ayrıca büyük şirketler de özel ve kişisel verilen çalınmasıyla ve fidye yazılımı saldırısından kaynaklanan itibar kaybıyla karşı karşıya kalmaktadır (FBI, 2021). Dolayısıyla gıda ve tarım sektörüne yönelik saldırılar operasyonların aksaması, finansal kayıplara neden olması ve gıda tedarik zincirinin olumsuz etkilenmesi gibi sonuçlara sebebiyet vermektedir.

Gıda ve tarım sektöründeki siber saldırılar, küçük çiftlikler, büyük üreticiler, marketler, restoranlar da dahil olmak üzere sektör genelindeki tüm işletmeleri hedef alabilmektedir. Ayrıca sektörün, temiz sulama için su ve atık su sektörüne, ürün ve hayvanların taşınması için ulaşım sektörüne, üretim ve gıda işlemede kullanılan ekipmanlara güç sağlamak için enerji sektörüne, gübreleme için kimya sektörüne ihtiyaç duymaktadır (Ribeiro, 2022). Dolayısıyla otomatik ve bağlantılı sistemler kullanılması ve sektörün akıllı teknolojileri benimsemesi, gıda ve tarım sektörüne yönelik saldırı yüzeyini artırmaktadır.

NEW Cooperative Fidye Yazılımı Saldırısı; 20 Eylül 2021'de ABD'nin Ortabatı eyaletlerinden biri olan Iowa merkezli çiftlik hizmetleri sağlayıcısı NEW Cooperative'e yönelik, gıda tedarik zincirlerini ve hayvan besleme programlarını yönetmek için kullanılan bilgisayarlarını kilitleyen siber saldırı gerçekleştirilmiştir. Saldırıda Rusya'ya bağlı BlackMatter isimli siber saldırganlar kooperatiften çaldıklarını iddia ettiği faturalar, araştırma ve geliştirme belgeleri, toprak haritalama teknolojisinin kaynak kodu dahil olmak üzere kooperatifin verilerini yayınlamakla tehdit ederek 5,9 milyon dolarlık fidye ödemesi talep etmiştir (Bogage & Reiley, 2021). NEW Cooperative ise tehdidi kontrol altına alabilmek için sistemlerini kapatarak önlem almaya çalışmıştır.

NEW Cooperative, çiftçilerin hasatlarını en üst düzeye çıkarma yolunda tavsiyeler sağlayan teknolojiye sahiptir. Ayrıca ABD'nin en çok mısır üreten

eyaletinde tahıl depolama asansörleri işletmekte, çiftçilerden mahsul satın almakta, mahsul yetiştirmek için gereken gübre ve diğer kimyasalları satmaktadır (Plume & Bing, 2021). Dolayısıyla şirkete yönelik siber saldırı, üretimi ve tedarik zincirini olumsuz etkilemiş, kapatılan sistemin manuele dönmesi sebebiyle işlemleri yavaşlatmıştır.

JBS USA Foods Saldırısı; Haziran 2021'de Brezilya merkezli dünyanın en büyük et tedarikçisi JBS USA Foods'a yönelik, et tedarik zincirinin büyük bir bölümünü felce uğratacak fidye yazılımı saldırısı gerçekleştirilmiştir. Saldırı, Colorado, Iowa, Minnesota, Pennsylvania, Nebraska ve Teksas'taki JBS tesisleri dahil olmak üzere on üç et tesisindeki operasyonların durmasına sebebiyet vermiştir. Bu durum ise arz ve talep arasındaki dengeyi bozarak toptan et fiyatlarının yükselmesine, çiftliklerdeki hayvanların pazara çıkarılamamasına ve lokantaların işlenmiş et alamamasına sebep olmuştur (Bowcut, 2021). JBS USA Foods ise istikrarlı gıda arzını sürdürme ihtiyacı nedeniyle, fidye yazılımında talep edilen 11 milyon doları Bitcoin olarak ödemek zorunda kalmıştır (JBS Foods, 2021). FBI yaptığı açıklamada, siber saldırıyı son aylarda rekor düzeyde en büyük fidye yazılımı gerçekleştiren Rusya merkezli olduğuna inanılan REvil'e atfetmiştir (NPR, 2021).

1.5.6. Sağlık Sektörü

Sağlık sektörü, yeni teknolojiler ile tedavi sağlamakta ve hayati önem taşıyan hizmetler sunmaya çalışırken, siber tehdit aktörleri bu gelişmelerle bağlantılı güvenlik açıklarından yararlanmaya çalışmaktadır. Sağlık sektörüne yönelik siber tehditler, hastaların gizliliğini tehlikeye atan kötü amaçlı yazılımlardan, sağlık hizmeti sunan tesislerin hasta bakımı sağlama becerisini bozan DDoS saldırıları veya fidye yazılımlarına kadar uzanmaktadır (Center for Internet Security [CIS], tarih yok). Diğer sektörlerin aksine, sağlık hizmetleri için siber saldırılar finansal kayıp ve veri ihlalinin ötesinde sonuçlar doğurabilmektedir.

Tıbbi cihazlar modern sağlık hizmetlerinde kritik rol oynamaktadır. Belirli bir amaç için kullanılan cihazlar hasta verilerini saklamıyor olsa da, siber tehdit aktörleri hassas verileri tutan bir sunucuya erişim sağlamak için tıbbi cihazları araç olarak kullanabilme yeteneğine sahiptir. Bu cihazların sadece tıbbi uygulamalar için kullanılması nedeniyle, ağ cihazlarında bulunan siber güvenlik sistemleri tıbbi

cihazların tasarımında yer almamaktadır. Dolayısıyla cihazlar sağlık kuruluşlarındaki sistemlere kötü amaçlı yazılımların yüklenebilmesinde aracı olarak kullanılabilir ve sağlık kuruluşlarının hastalara hayat kurtarıcı tedaviyi sağlamasını engelleyebilir.

Sağlık sektörünün hedef alınmasının ciddi nedenlerinden biri uluslararası casuslukla ilgilidir. Eski bir FBI siber uzmanı olan John Riggi sağlık sektörü için, *"tıbbi araştırmalar, yenilikler, kanser çalışmaları, nüfus sağlığı çalışmaları, hassas tıp araştırmaları ve klinik deneylerle ilgili fikri mülkiyet hırsızlığı ve potansiyel olarak askeri kullanım için düşman ulus devletler tarafından hedef alınmaktadır"* açıklamasını yapmıştır. Diğer bir sorun ise, bilgisayar korsanlarının askeri tesislerin yakınındaki hastaneleri hedef alarak askeri personellerin hassas verilerini, hatta nereye konuşlandırılacağı konusunda bilgi alabilme potansiyelleridir. (Farmer, 2019).

İş dünyasındaki liderlerin, politikacıların veya askeri figürlerin tıbbi ayrıntılarını elde etmek içinde sağlık sektörü önemli bir alandır. Örneğin 2018 yılında Singapur hükümetinin sağlık verilerine yasa dışı erişim sağlanmıştır. 1.5 milyon hastanın sağlık verileri ve 160.000 kişinin reçetelerinin ayrıntılarının çalındığı siber saldırı örneğinde, Singapur başbakanı Lee Hsien Loong da verileri çalınan profiller arasındaydı (Vincent, 2018).

Boston Çocuk Hastanesine Yönelik Siber Saldırı; Nisan 2014'te Boston Çocuk Hastanesi, tartışmalı bir velayet davasını protesto etmek için Anonymous tarafından çok sayıda DDoS saldırısına maruz kalmış ve operasyonlarının aksamasına sebep olmuştur. Öncelikle 20 Mart 2014'te Anonymous'a atfedilen tehditkar bir mesaj, 15 yaşındaki bir kızın Massachusetts koruma hizmetleri tarafından gözetimine alınan çocuk velayeti vakasıyla ilgili bilgileri aktarmaktaydı. Siber tehdit aktörleri, davaya dahil olan bazı kişilerin ev ve iş adresleri, e-posta adresleri ve telefon numaraları dahil olmak üzere kişisel bilgilerini yayınlayan sızıntı saldırısı uygulamışlardır (Radware, 2015).

Boston Çocuk Hastanesi, ABD'deki en büyük pediatrik tıbbi araştırma merkezlerinden biridir. Her yıl yaklaşık 24.943 yatan hasta kabulü ve 557.620'den fazla ziyaret kaydetmektedir. Yetkililer, saldırının çocuk hastanesi ağını iki hafta boyunca kesintiye uğrattığını, saldırıyı hafifletme çabalarının 18.000 dolara mal olduğunu ve bağış toplama sistemini devre dışı bırakıldığından bu yana tahmini 300.000 dolarlık ek bağış kaybına neden olduğunu bildirmiştir (Reed T. , 2018).

Anonymous adlı bilgisayar korsanı grubunun üyesi olan Martin Gottesfeld, tartışmalı velayet davasının merkezindeki bir gencin bakımını protesto etmek için hastaneye yönelik gerçekleştirilen siber saldırıdan sorumlu tutularak 10 yıl hapis cezasına çarptırılmıştır (Richer, 2019). Savcılar, saldırının sadece Boston Çocuk Hastanesi'ndeki hasta bakımında kesintiye yol açmadığını, aynı zamanda araştırma yeteneklerini engellediğini ve diğer sağlık tesisleriyle iletişimlerini bozduğunu iddia etmiştir (Alder, 2019). Boston Çocuk Hastanesinin kritik altyapısına yönelik gerçekleştirilen siber saldırı, domino etkisi yaratması nedeniyle önemli bir vakadır.

Johnson & Johnson Güvenlik Açığı; Tıbbi cihaz üreticisi J&J, 2016 yılında uzaktan kan şekeri ölçüm yapan Animas OneTouch Ping isimli insülin pompasındaki bir güvenlik açığı konusunda uyarılmıştır. Siber güvenlik firması Rapid7, OneTouch Ping sisteminin tescilli kablosuz yönetim protokolünde şifreli iletişim yerine açık metin iletişim kullandığını, şifrelenmediği için de sistemin savunmasız olduğunu belirtmiştir. Araştırmacı Jay Radcliffe ise bir siber tehdit aktörünün sistemi yanıltabileceğini, yetkisiz insülin enjeksiyonlarını tetikleyebileceğini ve hasta yaşamını tehdit edebileceğini keşfetmiştir (Beardsley, 2016).

Bu güvenlik açığı, cihaza yetkisiz erişim sağlanabilmesini ve kablosuz olarak iletişim sinyaline müdahale ederek cihazın uzaktan kontrol edilebilmesine izin vermenin mümkün olduğunu göstermektedir (Bradbury, 2017). Dolayısıyla bir bilgisayar korsanı tarafından, J&J hastalarına aşırı dozlarda diyabet ilacı alması için uyaracak şekilde uzaktan yeniden programlanabilir olması tehdidini barındırmaktadır. Şu ana kadar cihazlara yönelik herhangi bir saldırı bildirilmemiş olsa da, J&J'nin diyabet biriminin baş tıbbi görevlisi Biran Levy, Radcliffe'in bulgularını kopyalayabildiklerini ve bir bilgisayar korsanının insülin pompasına 25 fite kadar bir mesafeden yetkisiz insülin almasını emredebileceğini doğrulamıştır (Finkle, 2016). Bu örnek ise siber tehdit aktörlerinin sağlık verileriyle giderek daha fazla ilgilenmeye başladığı dönemde, ürünlerin hastalara ulaşmadan önce siber güvenliğin sağlanmasını vurgulayan bir örnektir.

1.5.7. Acil Servisler Sektörü

Acil Servisler Sektörü, insan kaynaklı ve doğal afetlerden kaynaklanan riskleri önlemek ve azaltmak için ulusların ilk savunma hattını oluşturan hazırlık, müdahale ve

kurtarma hizmetleri sağlayan, eğitimli acil durum personellerinden oluşan bir sektördür (Sweigert, 2017). Acil servis sistemleri, konumu izlemek, filo araçlarını yönetmek ve acil durum müdahale ekiplerinin yeteneklerini artırmak için birçok farklı sistem kullanmaktadır. Bu sistemler gerektiği gibi korunmadığında, siber saldırılara karşı riski artırmaktadır. Ayrıca bu cihazların birbirine bağlı yapısı nedeniyle, bir siber saldırı başladığında ardışık arızalar yaratma olasılığı da yüksektir (McElroy, 2021).

Şekil 11: Acil Servis Alanları



Kaynak: <https://www.cisa.gov/emergency-services-sector>

Baltimore 911 Acil Servisine Saldırı; 2018 yılında Baltimore'un 911 sevk sistemi bir siber saldırı ile karşı karşıya kalmıştır. Baltimore eski belediye başkanı Catherine Pugh, güvenlik ihlalinin ardından sevk görevlilerinin 17 saat boyunca Baltimore'un otomatik sevk sisteminin geçici olarak kapanmasına neden olduğunu bildirmiştir. Baltimore kesintisi sırasında, acil durum desteği için gelen aramalar sevk görevlilerine otomatik olarak aktarılamamış, bunun yerine çağrı merkezi destek personeli tarafından manuel olarak yönetilmesi gerekmiştir (NBC News, 2018). 911 sistemi manuel olarak idare edilebilmiştir ancak vaka çağrılarını kaydetmek, müdahale personellerini etkin bir şekilde göndermek ve sahadaki müdahalecilerin durumunu ve yerini belirlemek için -911, 311 servisleri tarafından kullanılan- Bilgisayar Destekli Sevk (Computer Aided Dispatch - CAD) sistemi 36 saat boyunca tamamen kapatılmıştı. Paris'teki Henry County 911 merkezindeki BT yöneticisi Chad Howard, sistem geri çalışmaya başladığında altı günlük verinin kalıcı olarak kaybedildiğini ve

sistemi kurtarmanın şehre tahmini 20.000 dolar mal olduğunu bildirmiştir (Meehan, 2018).

Albuquerque Polis Departmanına Yönelik DDoS Saldırısı; 2014 yılında Albuquerque Polis Departmanındaki memurların silahlı saldırılara karışması üzerinde Anonymous grubu, olayı protesto etmek için departmanın web sitesine yönelik DDoS saldırıları başlatmıştır. Cumartesi gecesini başlayan ve pazar gününe kadar uzayan siber saldırıda polis departmanının çevrimiçi hizmeti kapatılmıştır. Albuquerque dönem Belediye Başkanı olan Richard Berry yaptığı açıklamada ise siber saldırının başarılı olduğunu onaylamıştır (Fox News, 2015).

1.5.8. Nükleer Reaktörler, Malzemeler ve Atık Sektörü

Nükleer sektörü, vatandaşlara elektrik sağlayan güç reaktörlerinden, kanser hastalarını tedavi etmek için kullanılan tıbbi cihazların üretimi dahil, tarım ve sanayi gibi alanları dolaylı veya doğrudan olarak etkileyebilmektedir. Siber tehdit aktörleri tarafından nükleer sektör altyapısına yönelik siber saldırılar, ICS veya SCADA'yı hedef alabilmekte (Lehto, 2022, s. 30) ve sektör için büyük tehditler oluşturabilmektedir. Özellikle nükleer reaktörü kontrol eden makineleri ve yazılımları çalıştıran ağlara zarar verdiğinde doğrudan fiziksel etkiler yaratabilmektedir.

Nükleer Reaktörler, Malzemeler ve Atık Sektörüne yönelik önemli saldırılardan biri Gundremmingen Nükleer Santraline yönelik siber saldırıdır. Münih'in 120 km kuzeybatısında bulunan Gundremmingen tesisi, çok uluslu Alman enerji şirketi olan RWE (Rheinisch-Westfälisches Elektrizitätswerk Aktiengesellschaft) tarafından işletilmektedir. 2016 yılında nükleer santrale yönelik yapılan siber saldırı sonucunda, nükleer santraldeki ofis bilgisayarlarında çıkarılabilir veri deposu olarak kullanılan 18 adet USB bellekte ve nükleer yakıt çubuklarının hareketini modellemek için kullanılan bir sistemde, "W32.Ramnit" ve "Conficker"³ isimli iyi bilinen virüsler bulunmuştur. RWE, kontrol sistemlerinin internete bağlı olmadığı için virüslerin, tesis için bir tehdit oluşturmadığını ve bu nedenle virüslerin etkinleşmeyeceğini açıklamıştır (BBC, 2016).

³ Ramnit 2010 yılında piyasaya çıkan, veri çalmak için kullanılan bir erişim aracıken, Conficker 2008'de piyasaya çıkan ve oturum açma isimlerini, finansal verileri çalmayı amaçlayan bir virüstür.

1.5.9. Ulaşım ve Lojistik Sektörü

Ulaşım ve lojistik, dünyada en önemli endüstrilerden biridir. Sektör havacılık, deniz taşımacılığı, demiryolları, kamyon taşımacılığı, otomobil ve motorlu taşıtları içermektedir. Ancak sektörde kullanılan sistemlerin çoğu, siber güvenlik düşünülerek tasarlanmayan eski altyapı olması sebebiyle, suçlara karşı en savunmasız sektörlerden biridir. Check Point Research (CPR) raporuna göre Haziran 2020 ile Haziran 2021 arasında, ulaşım sektörü haftalık fidye yazılımı saldırılarında %186 oranında artış yaşamıştır (Check Point, 2021).

Bazı siber tehdit aktörleri lojistik şirketleri için sevkiyat detaylarını, iş ortaklarının ve müşterilerinin kişisel bilgilerini çalarak kar elde etme amacını taşımaktadır. Bu girişimler dışında trafik ışıklarının kesintisi veya demiryolu geçişlerinin kesintisi de fiziksel zarara uğratabilecek ve siber tehdit aktörleri tarafından tasarlanabilecek girişimler arasında sayılabilir (Reed J. , 2022). Ayrıca ulaşım sistemlerinde kullanılan navigasyon gibi ağ bağlantılı cihazların kullanılması da siber tehdit aktörleri için potansiyel saldırı noktası sunmaktadır. Ulaşım sektörüne yönelik İran demiryoluna ve EasyJet'e yönelik siber saldırı önemli vaka örnekleridir.

İran Demiryoluna Siber Saldırı; 9 Temmuz 2021'de Jahan News'in aktardığı habere göre İran'ın demiryolu sistemine yapılan bir siber saldırı, ülke genelinde yüzlerce tren hattının faaliyetlerinin ertelenmesine ve iptal edilmesine sebep olmuş, dijital bilet alım merkezleri, kargo ve yolcu hizmetleri kesintiye uğramıştır (Jahan News, 2021). Saldırı sadece sistemi bozmak için tasarlanmamış, tren istasyonlarındaki ekranlara yolcuların sorunları hakkında daha fazla bilgi alabilmeleri için İran'ın dini lideri Ali Hamaney'in ofisine ait "64411" numaralı telefon ile iletişim kurma talimatlarını gösteren bir trol kampanyasını içermiştir. Tren seferlerinin ertelenmesi yolcuların mağduriyetine yol açarken, hem ekonomik etkilere sebebiyet vermiş hem de trol kampanyası ile manipülatif içeriklerle toplumsal bir etki yaratmıştır.

Demiryolu sistemine yönelik yapılan siber saldırıdan bir gün sonra ise İran'ın ulaştırma bakanlığının web sitesi ve devlet demiryolu şirketinin web sitesine yönelik siber saldırı gerçekleştirilerek web siteleri kapatılmıştır (Greig, 2021). Güvenlik firması SentinelOne, daha önce görülmemiş MeteorExpress isimli "silecek" kötü amaçlı yazılımının yöntem olarak tercih edildiğini ve yazılımın genel olarak verileri silmek için kullanıldığını açıklamıştır (Guerrero-Saade, 2021).

EasyJet Siber Saldırısı; Dünyanın en başarılı düşük maliyetli havayollarından biri olan easyJet, 19 Mayıs 2020'de 9 milyon müşterinin etkilendiği, son derece karmaşık bir kaynaktan gelen bir siber saldırının hedefi olduğunu bildirmiştir. Siber saldırı ile 9 milyon müşterinin e-posta adresine ve seyahat ayrıntılarına, 2.208 müşterinin ise kredi ve banka kartı bilgilerine yasa dışı erişim sağlanmıştır (EasyJet, 2020). Havayolu şirketinin BBC'ye verdiği demeçte, saldırının kapsamını anlamak ve kimin etkilendiğini belirlemenin zaman aldığını, müşterileri ise soruşturma yeterince ilerledikten sonra bilgilendirebildiklerini, böylece hangi kişilerin etkilendiğini ve hangi bilgilere erişilebildiğini açıklamıştır. Saldırının doğası ve nedenleri hakkında ayrıntı vermeyen easyJet, siber saldırganların kimlik hırsızlığında kullanılabilecek bilgilerden ziyade "şirketin fikri mülkiyetini" hedeflediğini öne sürmüştür (Wakefield, 2020).

1.5.10. Telekomünikasyon Sektörü

5G, fiber internet, nesnelerin interneti (IoT)⁴, bulut sistemi⁵, yapay zeka (AI), internet sağlayıcıları, siber güvenlik ve veri gizliliği teknolojileri hem pazar büyüme beklentisi hem de sektörler üzerindeki dönüştürücü etkisi sebebiyle öne çıkan teknolojilerdir (TÜBİSAD, 2021, s. 4). Dijital dönüşümün ön plana çıkması, telekomünikasyon şirketlerinin büyümesi için fayda sağlarken, siber saldırı yüzeyini de artırmaktadır.

Telekomünikasyon şirketleri, hassas verileri iletmek ve depolamak için yaygın olarak kullanılan kritik altyapıyı kurmakta, kontrol etmekte ve işletmektedir. Bu geniş kapsamlı hizmeti siber saldırılar için büyük bir hedef olmasının önünü açmaktadır. Genel olarak doğrudan telekomünikasyon şirketlerini hedefleyen tehditler, DDoS saldırıları, APT saldırıları, cihazlardaki güvenlik açıkları, içeriden tehditler, sosyal mühendislik veya üçüncü tarafların bilgiye erişmesine izin verme riski gibi insan

⁴ IoT, internete bağlı olan ve veri alışverişi yapabilen fiziksel cihazların birbirleriyle iletişim kurabildiği bir ağıdır. Bu cihazlar, sensörler, yazılımlar, elektronik bileşenler ve ağ bağlantıları gibi teknolojileri kullanarak birbirleriyle etkileşim kurabilir, veri toplama, işleme ve paylaşma işlemlerini gerçekleştirebilirler. Bu sayede cihazlar verimliliklerini artırabilir, yeni hizmet ve iş modelleri yaratabilir. Akıllı ev sistemleri, akıllı tarım sistemleri örnek olarak verilebilir.

⁵ Bulut sisteminde, kullanıcı verilerinin yerel cihazlar yerine bulut olarak adlandırılan merkezi bir depolama platformunda barındırılmasıdır. İşletmeler veya bireyler için depolama, yedekleme, işlem gücü gibi hizmetleri sunar ve kullanıcılar internete bağlı olduğu herhangi bir cihazdan verilerine erişim sağlayabilir. Google Drive, OneDrive, Microsoft Office 365, Microsoft Azure örnek olarak verilebilir.

temelli tehditlerdir. Dolaylı olarak ise telekomünikasyon hizmeti alan aboneleri, özellikle Şebeke Servis Sağlayıcıları (NSP) ve İnternet Servis Sağlayıcıları (ISP) müşterilerini hedefleyen tehditlerdir (Kaspersky, 2018).

Devlet kurumları da gizli gözetim kurmak için telekomünikasyon operatörlerinin altyapısına ve uygulamalarına, genellikle uzun süreler boyunca fark edilmeden çalışabilen APT saldırıları düzenlemektedir. Gizli gözetim için hedeflenen iletişim kanalları, telefon hatlarından ve çevrimiçi sohbet uygulamalarından, cep telefonu verilerine kadar her şeyi içermektedir (Deloitte Touche Tohmatsu Limited [DTTL], tarih yok). Telekomünikasyon şirketlerindeki müşteri verileri de bir başka yüksek etkili hedeflerdir. Telekomünikasyon şirketleri genellikle tüm müşterileri hakkında isimler, adresler ve finansal veriler gibi kişisel bilgileri depolar ve bu hassas veriler, müşterilere şantaj, kimlik hırsızlığı, para çalma veya daha fazla saldırı başlatmak için siber tehdit aktörleri tarafından hedef olabilmektedir. Müşterilerin hassas verileri DarkWeb üzerinden satılabilir veya ulus devlet destekli gruplar tarafından rakip ulus devletler hakkında istihbarat toplamak amacıyla kullanılabilir.

LightBasin (diğer adıyla UNC1945); 2016'dan beri sürekli olarak telekomünikasyon sektörünü küresel ölçekte hedefleyen bir bilgisayar korsanı grubudur. Dünya çapındaki cep telefonu ağlarına sızan ve telekomünikasyon şirketlerinden gelen arama kayıtlarına ve mesajlarına erişmek için özel araçlar kullanan LightBasin, CrowdStrike araştırmacılarına göre 2019'dan bu yana en az 13 telekomünikasyon şirketinden mobil ağ verilerini çalmıştır (Harries & Mayer, 2021). CrowdStrike, sunuculara iletişim kurmak için kullanılan dilin Çin devletinin sponsorluğunda görüldüğünü belirtse de, bugüne kadar bilgisayar korsanlarının tam yerini kanıtlayacak önemli bir kanıt bulunamamıştır (Goud, tarih yok).

Bilgisayar korsanlığı grubu, başlangıçta Genel Paket Radyo Servisi (GPRS) ağının parçası olan harici DNS (eDNS) sunucularından yararlanarak telekomünikasyon şirketlerinden birinin güvenliğini tehlikeye atmıştır. Grup, GPRS ağındaki Hizmet Dağıtım Platformu (SDP) sistemleri ve SIM / IMEI sağlamanın yanı sıra, Operasyon Destek Sistemleri (OSS) ve Operasyon ve Bakım Birimleri (OMU) gibi diğer telekomünikasyona özgü sistemleri de hedeflemiştir (Harries & Mayer, 2021).

1.5.11. Kimya Sektörü

2021 tarihli Birleşik Krallık Hükümeti araştırması, siber saldırıların kimya endüstrisinde faaliyet gösteren şirketler için 1.3 milyar Sterlin kayıp yarattığını tahmin etmektedir (U.K. Cabinet Office, 2011, s. 19). Siber tehdit aktörleri, üretimin durması veya hassas verilerin çalınması durumunda kimya sektörünün hem finansal hem de itibar kaybı yaratmak açısından değerli bir hedef olarak görmektedir. Kimya şirketlerini en çok etkileyebilecek siber tehditlerden biri, şirketin fikri mülkiyetinin çalınması ve bir başkasına satılmasını içeren endüstriyel casusluktur (Reynard, 2021).

Yüksek riskli olanlar da dahil olmak üzere çoğu kimya şirketi, internete bağlı cihazlara sahiptir. Bu durum cihaz üreticilerinin, cihazlarına uzaktan iletişim kurabilmesini sağlar ve tesisi işleten sistemlerin kontrolünü ele geçiren siber tehdit aktörlerinin saldırılarına imkan verir (Kramer, 2020). Kimya şirketleri bir siber suçlunun ağlarına sızdığını veya bir siber saldırının gerçekleştiğini, birkaç yıl sonra rakip şirket bir ürünü pazara sunduğu ana kadar fark etmeyebilir. Ayrıca, bir kişinin özel bilgilerini çalmak amacıyla bir kuruluşa katılması da "içeriden tehditleri" beraberinde getirmektedir (Dickinson, 2021).

ABD'deki 3300 kimyasal tesis yüksek riskli olarak sınıflandırılmaktadır (CISA, tarih yok). Listedeki zehirli ve patlayıcı bileşiklerin yanı sıra, salındığında hemen tehlikeli olmayan, ancak çalındığında silaha dönüştürülebilecek kimyasallar da yer almaktadır (Kramer, 2020). Kimya şirketleri, 2008'den beri güncellenmemiş olan ABD'deki Kimyasal Tesis Terörle Mücadele Standartları (Chemical Facility Anti-Terrorism Standards -CFATS) programı tarafından yayınlanan siber güvenlik kılavuzunu takip etmektedir. Sürekli gelişen bir tehdit ortamında eski bir sisteme sahip olmak, kimya sektörünü siber saldırılar için savunmasız bir hedef haline getirmektedir. ABD'deki binlerce kimyasal tesisin, güncel olmayan siber güvenlik rehberliğine dayanması, sadece ekonomik hasara değil, aynı zamanda kimyasal sızıntılara veya patlamalara karşı savunmasız bırakmaktadır (Elliott, tarih yok). Siegfried Group ve Brenntag'e yönelik siber saldırılar kimya sektörüne yönelik gerçekleştirilen siber saldırılara yönelik önemli vaka örnekleridir.

Siegfried Group İsviçre, Almanya, İspanya, Fransa, Malta, ABD ve Çin'de tesisleri bulunan, tablet, kapsül, steril şişe, ampul, kartuş ve merhem gibi kimyasal oluşumların sentezi ve geliştirilmesini içeren aktif medisinal (farmasötik) bileşenler,

ara ürünler ve bitmiş dozaj formları üreten bir kimya şirkettir (Siegfried Group, 2021). 21 Mayıs 2021'de Siegfried'in BT ağlarında kötü amaçlı bir saldırı tespit edilmiştir. Saldırının hemen ardından ise Barselona'da izole edilmiş ağ üzerinde çalışan iki tesis dışında, üretim durdurulmuş, ağ bağlantıları kesilmiş ve BT sistemleri kapsamlı bir incelemeye tabi tutulmuştur (Carpenter, 2021). Adli incelemeler sonucunda ise Siegfried (2021), hiçbir hassas müşteri verisinin ele geçirilmediğini ve BT sistemlerinde kalıcı bir hasarın olmadığını açıklamıştır. Ancak saldırı, iş kesintisinin devam etmesiyle üretim ve gelir eksikliklerine neden olmuştur (Siegfried, 2021).

Brenntag merkezi Almanya'da bulunan, dünya çapında 77'den fazla ülkede 670'den fazla tesisi bulunan kimyasal dağıtım şirkettir. Independent Commodity Intelligence Services (ICIS) En İyi 100 Kimyasal Distribütör raporuna göre Brenntag, Kuzey Amerika için satışta ikinci sırada, Asya Pasifik'te üçüncü sırada yer alan en büyük şirkettir (Independent Commodity Intelligence Services [ICIS], 2020).

Brenntag, Mayıs 2021'de DarkSide fidye yazılımı çetesi tarafından, Kuzey Amerika bölümünü hedef alan bir fidye yazılım saldırısına uğramıştır. Saldırı gerçekleştiğinde anonim bir kaynak tarafından BleepingComputer ile paylaşılan bilgilere göre, DarkSide fidye yazılımı grubu, 150 GB veri çaldığını iddia etmiş ve iddialarını kanıtlamak için çalınan veri türlerinin açıklamasını (mali ve muhasebe bilgileri, insan kaynakları bilgileri, pazarlama ve hukuk sözleşmeleri, projeler, kimyasal formüller) ve bazı dosyaların ekran görüntülerini içeren özel bir şifreli veri sızıntısı sayfası oluşturmuştur (Abrams, 2021). Brenntag, DarkSide fidye yazılım çetesine şifrelenmiş dosyaların şifrelerini almak ve tehdit aktörlerinin çalınan verileri kamuya açık bir şekilde sızdırmasını önlemek için Bitcoin olarak 4.4 milyon dolarlık fidye ödemiştir (Gatlan, 2022).

1.5.12. Kritik İmalat Sektörü

Kritik imalat sektörü, küresel ekonominin en büyük, en çeşitli ve hızla değişen bölümlerinden biridir, dolayısıyla canlı bir imalat tabanı, birçok ülke tarafından genel ulusal güç ve canlılığın önemli bir ölçüsü olarak görülmektedir (Mission Secure, tarih yok). Robotik işgücü, otomasyon, IoT, Endüstriyel Nesnelerin İnterneti (IIoT), akıllı cihazlar, yapay zeka, makine öğrenimi gibi günümüz dünyasında imalat sektöründe

sürmekte olan çok fazla teknolojik değişiklikler, bu alanda rekabet ortamı oluşturmakla beraber getirdiği siber riskler de mevcuttur.

Sektördeki üreticiler hammadde ve birincil metalleri işlemektedir; havacılık ürünleri, savunma, otomotiv, elektronik, inşaat, ambalajlı tüketim malları, ticari gemiler, vagonlar ve bunların destekleyici bileşenlerini üretmektedir. Ayrıca kritik imalat endüstrileri tarafından üretilen ürünler, diğer birçok kritik altyapı sektörü için esastır ve kritik imalat sektöründeki bir arıza, birden fazla bölgedeki diğer kritik altyapı sektörlerinde kademe kesintilere sebep olabilmektedir (CISA, tarih yok(a)).

İngiltere merkezli siber güvenlik şirketi olan Sophos Group'un 2021 yılında, Amerika Kıtası, Avrupa, Orta Doğu, Afrika ve Asya Pasifik bölgelerinde ve toplam 30 ülkede -imalat sektöründen 438 katılımcı da dahil- çeşitli sektörlerden katılımcılar ile bir anket gerçekleştirmiştir. Anket sonuçlarına göre, imalat sektöründeki bir fidye yazılım saldırısını düzeltme faturası, kesinti süresi, cihaz ve ağ maliyeti, kaybedilen fırsat, ödenen fidye ve daha fazlası dikkate alındığında ortalama maliyet 1,52 milyon dolar olarak belirlenmiştir (Sophos, 2021, s. 3).

FACC havacılık şirketi ve önemli otomobil markalarından biri olan Honda, kritik imalat sektöründe görülen önemli siber saldırılara uğramıştır. *FACC Havacılık Şirketine* yönelik siber saldırıda; Boeing ve Airbus gibi büyük havayolu müşterilerine hava yapıları, motor, kabin gibi yedek parça tedarik eden orta ölçekli bir işletme olan Avusturya merkezli havacılık şirketi FACC, 2015 yılında "*sahte başkan olayı*" olarak bilinen bir kimlik avı saldırısına uğramıştır (Reuters, 2016). Siber tehdit aktörü, finans departmanı çalışanına inandırıcı bir e-posta hazırlamak için CEO'nun e-postasına sızmış ve sahte bir satın alma projesi için hesabına 56 milyon dolar aktarılmasını talep etmiştir (Boyle, 2019). Bu tür vakarlarda siber tehdit aktörleri, şirketin e-posta sunucuna girer ve mesajın meşru görünmesini sağlamak için yöneticinin yazma alışkanlıklarını inceler. Saldırı sonrasında ise siber tehdit aktörü, şirket CEO'su Walter Stephan'dan geldiği iddia edilen bir e-postada, parayı bir satın alma projesi için talep ettiğini belirterek şirketi 56 milyon dolar zarara uğratmıştır. FACC Denetim Kurulu ise Walter Stephan'ın görevini ciddi şekilde ihlal ettiği sonucuna vararak Walter Stephan ile birlikte şirketin baş finans görevlisi kişiyi görevinden almıştır. 2016 yılında kamuoyuna duyurulan vaka sonrasında ise FACC'nin hisse senedi fiyatları %17 düşüş göstermiştir (Boyle, 2019).

Honda'ya yönelik siber saldırıda; Haziran 2020'de Japon otomobil üreticisi Honda, dahili sunucularından birinin dışarıdan saldırıya uğradığını bildirmiştir. Şirket saldırı sonrasında, Kuzey Amerika, İtalya, Türkiye ve Japonya'daki diğer operasyonların askıya alınmasıyla birlikte İngiltere'deki tesiste çalışmaların durdurulduğunu doğrulamıştır. Japonya dışındaki üretim sistemlerinde önemli bir etki doğuran bu vakada, siber güvenlik analistleri, saldırının fabrikalar ve enerji santralleri gibi çok çeşitli endüstriyel tesislerin kontrol sistemlerine saldırmak üzere tasarlanmış "Ekans" olarak da bilinen "Snake" fidye yazılımı tarafından gerçekleştirildiğini bildirmiştir (Tidy, 2020). Malware Hunter ekibinde güvenlik uzmanı olan Vitali Kremez, Snake fidye yazılımının önce bir sistemi hedeflediğini, Birim Gölge Kopyası Hizmetini (VSS) kaldırıldığını ve ardından endüstriyel kontrol sistemlerini, sanal makineleri, uzaktan yönetim araçlarını, ağ ile ilgili tüm süreçleri tamamen kapattığını belirtmiştir (Dimitrova, 2020). Bu tür siber silahların daha önce sadece devlet ajanları tarafından kullanıldığı bilinmektedir. Siber tehdit aktörlerinin kullandığı siber saldırı aracı, yalnızca veri çalmak veya iş operasyonlarını bozmak için değil, fabrikaları durma noktasına getirmek veya elektrik şebekelerini kapatmak için de kullanılabilir (Dooley & Ueno, 2020).

1.5.13. Ticari Tesisler Sektörü

Ticari tesisler sektörü, konaklama (oteller, konferans merkezleri, turistik tesisler), açık hava etkinlikleri (kamp alanları, fuarlar), eğlence (sinema, tiyatro, spor salonları, oyun merkezleri) , gayrimenkul (ofis, apartman binaları), perakende (alışveriş merkezleri, e-ticaret platformları, süpermarketler), spor ligleri (federasyonlar) gibi büyük insan kalabalığını çeken ve halka açık erişim ilkesine göre çalışan çok çeşitli tesisleri içermektedir. Bu tesislerin çoğu hükümet ve diğer düzenleyici kurumların minimum müdahalesi ile özel sektöre aittir (CISA, tarih yok (b)).

Ticari tesisler sektörü, pazarlama, mağazacılık, bilet satış ve rezervasyonlar için yaygın bir şekilde teknolojiyi ve interneti kullanır. Web siteleri, mobil uygulamalar, sosyal medya uygulamaları gibi dijital kanallar aracılığıyla tesislerin, çevrimiçi olarak varlık oluşturması, ürün ve hizmetlerini tanıtmaları, müşterilerle etkileşim kurmasını sağlar. Müşterilerle etkileşimin düzene sokulması, iş süreçlerinin düzenlenmesi,

verimliliklerin artırılması ve tesislerin alıřtırılması amacıyla; endüstriyel kontrol sistemleri tesislerin operasyonel süreçlerini izlemek, verileri toplamak, analiz etmek için ve IoT cihazları farklı sensörler ve bağlantılı cihazlar aracılığıyla tesislerdeki ekipmanların durumunu takip etmek ve otomasyon sağlamak için kullanılır. Dolayısıyla yönetilmesi ve güvence altına alınması gereken çok fazla cihaz olduđu için güvenlik riskleri ve potansiyel siber saldırılar, ticari tesisler için fiziksel ve dijital ortamı etkileyebilme düzeyinde gerçekleşebilir (Siddiqui, tarih yok). Özellikle bina yönetim sistemleri, ısıtma, havalandırma ve klima sistemlerinden erişim kontrolüne kadar giderek daha fazla bilgisayarlaşmakta ve bu durum operasyonların büyük bir bölümünü siber saldırılara karşı savunmasız hale getirmektedir. Dolayısıyla internetin kesintiye uğramasına sebep olabilecek herhangi bir siber saldırı, sektörde ekonomik sorunlara sebebiyet verebilir veya otomatikleşmiş bina sistemlerine erişim sağlanması durumunda bina sistemlerinde operasyon kaybına neden olabilir (DHS, 2016).

2013 yılında ABD'de bulunan Target mağazalar zinciri, tatil sezonunda mağazalarından alışveriş yapan müşterilerin toplam 40 milyon kredi ve banka kartı hesabından bilgilerinin ele geçirildiğı bir siber saldırıya uğramıştır. Target, veri ihlalinin toplam maliyetinin 202 milyon dolar olduğunu açıklamıştır (NBC NEWS, 2017). Şirketin yanıt süresi, yasal ücretler, itibar kaybı gibi faktörler şirketlin veri ihlali sonucu maliyet kaybını belirler. Veri ihlalinin tatil sezonunda yaşanması, ihlal sonrasında şirket müşterilerinin güven kaybederek alışverişlerini kesmesi ve siber güvenlik ağlarını yeniden yapılandırma süreci sebebiyle Target'in kazançları büyük oranda düşmüş ve maliyet kaybı ortalamanın üstünde yaşanmıştır.

1.5.14. Devlet Tesisleri Sektörü

Devlet tesisleri sektörü, yurt içinde ve yurtdışında bulunan, eyalet, mahalle ve kabile hükümetlerine ait olan veya kiralanan çok çeşitli binaları içermektedir. Birçok devlet tesisi, ticari faaliyetler veya eğlence faaliyetleri için halka açıkken, kamuya açık olmayan ve son derece hassas bilgileri, prosedürleri ve donanımları içeren tesisler de mevcuttur; özel kullanımlı askeri tesisler, elçilikler, adliyeler, ulusal laboratuvarlar, kritik sistemler, ekipmanlar ve ağlar barındırabilecek yapılar dahildir (DHS, tarih yok).

CISA'nın yayınladığı sektöre özel planda, devlet tesisleri sektörünün alt sektörleri; Eğitim Tesisleri, Ulusal Anıtlar ve Simgeler ve Seçim Altyapısı olarak belirtilmiştir. Eğitim Tesisleri Alt Sektörü, 12. sınıfa kadar olan okulları, yüksek öğrenim kurumlarını ve ticaret okullarını kapsamaktadır. Ulusal Anıtlar ve Simgeler Alt Sektörü, ulusal tarihi yerlerin kaydı ve ulusal tarihi yer işaretlerinin listesi gibi varlıkları, ağları ve sistemleri kapsamaktadır. Seçim Altyapısı Alt Sektörü ise, oy verme yerleri ve seçim sürecini yöneterek sonuçları eyalet ve yerel yönetimler adına raporlamak için kullanılan çeşitli fiziksel ve elektronik varlıkları, seçmen kaydı veritabanlarını, oylama makinelerini ve diğer sistemleri içeren bilgi ve iletişim teknolojilerini kapsamaktadır (CISA, tarih yok (c)). Devlet tesislerinin güvenlik sistemlerine yönelik siber saldırılar, tesislerin, memurların ve halkın korunmasını tehlikeye atabilir ve önemli zararlarla sonuçlanabilir.

2011 yılında, ABD'de hükümet tarafından finanse edilen iki laboratuvarın ağlarına yönelik, internet erişiminin ve web sitesinin kapatılmasına sebep olan siber saldırı gerçekleştirilmiştir. Siber saldırılarda hedef alınan araştırma laboratuvarları; fizik tabanlı araştırmalar yürüten Thomas Jefferson Ulusal Laboratuvarı ve bilgi güvenliği, nükleer silahların yayılmasını önleme ve terörle mücadele alanında araştırmalar yapan Pasific Northwest Ulusal Laboratuvarıdır (Hoffman, 2018). Saldırı sonrasında dahili e-posta ve bazı internet erişimleri geri yüklense de, siber tehdit aktörü tarafından gönderilen kötü amaçlı yazılımlar kaldırılana kadar ve güvenlik açıklarını düzeltmek için yamaların yüklenmesine kadar geçen süreçte dış bağlantılar kapalı duruma getirilmiştir (Jackson, 2011).

1.5.15. Su ve Atık Su Sistemleri Sektörü

Su ve atık su sistemleri, içme suyu sağlayan tesisler ve atık sus hizmetleri sağlayan tesisler olmak üzere ikiye ayrılmaktadır. Su hizmetleri; kaynak suları, arıtma tesisleri, pompa istasyonları, depolama alanları ve kapsamlı dağıtım, toplama ve izleme sistemlerinden oluşmaktadır. İçme suyu veya atık su sistemine yapılan siber saldırılar, ulusun halk sağlığını ve ekonomik canlılığını ciddi bir şekilde etkileyebilecek sonuçlar doğurabilmektedir (Department of Homeland Security [DHS], 2014, s. 50).

İçme suyu hizmetleri; güvenli içme suyu, toplum yaşamının merkezinde yer almaktadır. Dolayısıyla içme suyu hizmetlerinin sağlanamaması, ulus genelinde geniş kapsamlı halk sağlığı, ekonomik, çevresel ve psikolojik etkiler yaratabilir. İçme suyu hizmetleri ayrıca yangından korunma, sağlık hizmetleri, ısıtma ve soğutmayı içeren hizmetler için de yardımcıdır (CISA, 2015, s. 3).

Atık su hizmetleri; Atık su tesisleri evrensel kanalizasyon ve endüstriyel işlemlerden üretilen atık suları arıtmaktadır. Dolayısıyla atık su hizmetlerinin kesintiye uğraması can kaybına, ekonomik etkilere, ciddi halk sağlığı ve çevresel etkilere sebep olabilir.

Su ve atık sus hizmetleri veren işletmelere veya süreç kontrol sistemlerine yönelik siber saldırılar aşağıdaki gösterildiği gibi önemli zararlara sebep olabilir:

- Valfların yetkisiz olarak açılması veya kapatılması, alarmların geçersiz hale getirilmesi, pompaların veya diğer ekipmanların devre dışı bırakılmasıyla arıtma veya nakil süreçlerini bozma,
- Yardımcı programın web sitesinin tahrif edilmesi veya e-posta sistemini tehlikeye atılması,
- Tesisin faturalandırma sisteminde müşterilerin kişisel verilerinin veya kredi kartı bilgilerinin çalınması,
- İşletme girişimlerini veya süreç kontrol sistemlerini devre dışı bırakabilecek fidye yazılımı gibi kötü amaçlı programların yüklenmesi.

Bu saldırılar su ve atık sus hizmetlerinin müşterilere temiz ve güvenli su sağlama kabiliyetini tehlikeye atabilir, müşteri güvenliğini sarsabilir, finansal veya yasal yükümlülöklere yol açabilir (EPA, 2022).

Su ve atık sus sitemlerine yönelik siber saldırılar konusunda Oldsmar Su Tesisi ve San Francisco Körfezi Su Arıtma Tesisine yönelik siber saldırılar önemli iki vakadır.

Oldsmar Su Tesisi; 5 Şubat 2022'de isimsiz bir bilgisayar korsanı, Florida'da yer alan su arıtma tesisinin bilgisayar sitemlerine erişim sağlayarak tesisin operasyonel kontrollerini ele geçirmiştir. Birçok tesis gibi, Oldsmar tesisinde de personelin tesis içindeki koşulları izlemesini ve kontrol etmesini sağlayan bir SCADA sistemi kullanılmaktadır. Kimliği belirsiz siber tehdit aktörleri, SCADA sisteminin yazılımına

erişerek sudaki sodyum hidroksit içeriğini geçici olarak zehirli seviyelere çıkarmayı başarmıştır (Yehoshua, 2019). Oldsmar tesisi, şehrin 15.000 sakini için birincil içme suyu kaynağıdır. Oldsmar Şerifi Bob Gualtieri yaptığı basın açıklamasında, bilgisayar korsanının, sodyum hidroksiti milyonda 100 parçadan, milyonda 11.100 parçaya değiştirdiğini ve bunun potansiyel olarak tehlikeli bir artış olduğunu belirtmiştir (Gualtier, 2021).

Massachusetts Eyaleti Çevre Koruma Departmanı tarafından, Oldsmar su artıma tesisindeki riski önemli ölçüde artıran ve güvenli olmayan davranışlara atıfta bulunacak bir güvenlik tavsiyesi yayınlanmıştır. Oldsmar personelleri, SCADA ağı içindeki sistemleri izlemek ve kontrol etmek için oldukça yaygın olan uzaktan erişim programı TeamViewer'ı kullanmaktaydı. Kimliği belirsiz siber tehdit aktörleri ise TeamViewer aracılığı ile su arıtma tesisinin SCADA kontrollerine erişmiştir. Ayrıca su tesisi personellerinin kullandığı tüm bilgisayarlarda eski bir yazılım olan Windows 7 kullanılmasıyla birlikte, tüm çalışanlar TeamViewer'a erişmek için aynı parolayı kullanmaktaydı (MASS, 2022). Dolayısıyla herhangi bir güvenlik duvarı koruması olmaması, siber güvenlik durumunun tesis için öncelikli olmadığını ve bu sonuçların kaçınılmaz olduğunu göstermektedir.

San Francisco Körfezi Su Arıtma Tesis; 15 Ocak 2021'de bir siber tehdit aktörü, San Francisco Körfez Bölgesi'ndeki bir su arıtma tesisinin sistemine erişerek içme suyunu arıtmak için kullanılan birkaç programı silmiştir. NBC News'in bildirdiğine göre, kimliği belirsiz bilgisayar korsanı, San Francisco Körfez Bölgesi'ndeki belirtilmemiş bir su arıtma tesisine, tesisteki eski bir çalışanın kullanıcı adı ve şifresini kullanarak saldırıyı gerçekleştirmiştir. Kuzey Kaliforniya Bölgesel İstihbarat Merkezi tarafından Şubat 2021'de derlenen ve NBC tarafından elde edilen rapor göre siber tehdit aktörünün, bilgisayarları uzaktan kullanmalarına olanak tanıyan TeamViewer hesabına eriştiği bildirilmiştir. 16 Ocak'ta fark edilen siber saldırıdan sonra tesis silinen tüm programları yeniden yükleyerek çalışanların şifrelerini sıfırlamıştır (Chakya, 2021).

1.5.16. Savunma Sanayi Sektörü

Savunma sanayi üssü, askeri gereksinimleri karşılamak için askeri silah sistemlerinin, alt sistemlerinin veya parçalarının araştırılması ve geliştirilmesinin yanı

sıra tasarım, üretim ve bakım sağlayan dünya çapındaki sanayi kompleksidir (DHS, 2014, s. 13). Diğer sektörler gibi savunma sanayi üssü de BT altyapısına büyük ölçüde bağımlı olmakla birlikte sahip oldukları ağlar, ulusal güvenlik için önemli olan kritik operasyonel varlıkları ve verileri barındırmaktadır. Bu sebeple sektör, DDoS saldırılarına, veri hırsızlığına ve bilgilerin kötü niyetli değiştirilmesine karşı savunmasız hale gelmiştir. Siber tehdit aktörleri, siber casusluk faaliyetlerini genişleterek savunma sanayi üssü firmalarının bilgi ve teknolojilerine erişim sağlamaya çalışmakta, ticari sır ve fikri mülkiyet verilerini çalmaktadır (Lehto, 2022, s. 18). Ulusal güvenliği tehlikeye atabilecek bu tür saldırılar, hükümetin askeri yeteneklerine ve operasyonlarına potansiyel olarak zarar verebilme gücündedir.

Bilgisayar korsanları, özellikle bir hükümetin askeri, teknolojik ve ekonomik avantajlarını sabote etmek için savunma sanayi üssüne karşı fidye yazılımı saldırıları gerçekleştirmektedir. Bu saldırıların arkasındaki siber tehdit aktörleri, genellikle hassas hükümet verilerine, fikri mülkiyet ve ticari sırlara erişimi ödeme gerçekleşinceye kadar engellemektedirler (Mallon, tarih yok).

2001 yılında havacılık şirketi Lockheed Martin tarafından ABD hava kuvvetleri için geliştirilen ve Pentagon'a 300 milyar dolara mal olan proje F-35 saldırı uçağı projesi, ABD hükümetinin şimdiye kadarki en maliyetli silah sistemiydi. İngiltere, Kanada, Avustralya dahil diğer beş ülke projeye imza atarak toplam 4,8 milyar dolar katkıda bulunmuştur (Nasaw, 2009). 2007'de bilgisayar korsanları, ABD'nin en gelişmiş donanımlarından olan F-35 Müşterek saldırı uçağı (Lockheed Martin F-35 Lightning II) dahil Lockheed Martin F-22 Raptor savaş uçağı ve Bell-Boeing V-22 Osprey ile ilgili yüksek düzeyde gizli verileri siber casusluk sonucu ele geçirmiştir (The National Interest [TNI], 2019).

ABD, Çin'in kendi beşinci nesil hayalet uçağını üretmek için F-35 savaş uçaklarında kullanılan teknolojiyi çaldığını iddia etmiştir. Çin'in F-35 saldırı uçağı bilgilerini çalmasıındaki rolüne ilişkin ilk şüphe, eski ABD Ulusal Güvenlik Ajansı çalışanı Edward Snowden'ın 2015 yılında bir Alman yayınına bazı gizli verileri sızdırmasının ardından, Çin'in siber casusluğunun tüm kapsamını göstermesiyle ortaya çıkmıştır (Tiwari, 2022). Alman gazetesi Der Spiegel ile paylaşılan kayıtlar, Çinli bilgisayar korsanlarının F-35 Lightning II ortak savaş uçağı hakkında çok gizli

bilgilere erişilebildiğini göstermekteydi. Belge içeriklerine göre, veri sızıntısı 2007 yılında Lockheed Martin'de meydana gelmiştir (Gady, 2015).

Havacılık alanındaki uzmanlar, uzun zamandır Çin'in beşinci nesil Shenyang J-31 savaş uçağı ve Chengdu J-20'nin tasarımının kısmen F-35'ten aldığını tartışmaktadırlar (Tirpak, 2012). Sonuç olarak ulus devletler, bu tür hassas projeler üzerinde çalışırken siber güvenlik alanındaki ayrıntıları dikkate alması ve boşlukları kapatması ulusal güvenlik için önem taşımaktadır.

1.5.17. Bilgi Teknolojileri Sektörü

Diğer kritik altyapı sektörleri doğası gereği fiziksel iken, BT sektörü güvenliği ve kontrolü daha zor olan sanal ağlardan oluşmaktadır. Bilgi işlem gücü her yıl katlanarak artmakta ve birbirine bağlı cihazlar, iletişim kurup makinelerle talimat göndererek Nesnelerin İnterneti'ni oluşturmakta ve büyük miktarda veriler birikmektedir (ISALLIANCE, tarih yok). Siber tehdit aktörler, siber saldırının etkisinin çok büyük olacağı ve çalınan verilerin değerli olacağı sektörleri hedef almaktadır. Dolayısıyla çok büyük miktarda bilginin, dijital formata dönüştürülmesini sağlayan BT sektörüne yönelik saldırılar, ulusal güvenliğe ciddi bir tehdittir. Ayrıca dijitalleşen günümüz çağında, neredeyse tüm kritik altyapı sektörleri BT sektörüne bağlı olması ve hükümetlerin, kuruluşların ve özel sektörün giderek BT sektörüne daha bağımlı hale gelmesi sebebiyle BT sektörünün hedef alınması, ülke güvenliği, ekonomisi ve genel refahı için kritik öneme sahiptir.

Çevrimiçi etkinliğin çoğu, hükümet etkisinin minimum olduğu özel sektör alanına girmektedir. Hükümet politikalarında askeri sistemleri koruma ihtiyacına yönelik gelişmelere önem verilirken özel sektörün korunması üzerinde durulmamakta ve hatta hükümetin özel sektöre karşı güvenlik standartları sunmasına karşı özel sektörün devlet kontrolüne karşı direnişi söz konusudur. Etzioni (2011) bu konuda, özel şirketlerin bilgisayar sistemlerini daha iyi güvenceye almaları için hükümet kontrollerinin, gönüllü eylemleri teşvik edecek şekilde sunulmadığını savunmaktadır. BT altyapısını güvence altına almak için kullanılan araç ve tekniklerin, yeni teknolojiler ve tehditler ortaya çıktıkça sürekli olarak değiştirilmesi gerekmekte, ülkenin kritik altyapısını güvence altına almak için uğraşan tüm sektörlerin, devlet kurumlarının ve özel sektörün arasında daha fazla işbirliği sağlanmalıdır.

2019'da Hintli BT řirketi Wipro, kendi BT sistemine yönelik bir siber saldırıya uğradığını bildirmiřtir. Wipro'nun müşterilerinin çoęu, özellikle devlet destekli olan sektörler dahil, siber tehdit aktörleri için büyük bir hedef olabilecek sektörleri kapsamaktadır. Diğer endüstriler arasında petrol ve gaz, otomotiv, havacılık, savunma, bankacılık ve saęlık kuruluşları yer almaktadır (O'Flaherty, 2019). KrebsOnSecurity'e (2019) göre, iki güvenilir kaynak Brian Krebs'e anonim olarak yaptığı açıklamada, Wipro'nun sistemlerinin en az bir düzine Wipro müşteri sistemini hedefleyen kimlik avı saldırıları düzenlendiğini ve birkaç ay boyunca müşterilerini hedef almak için kullanıldığını belirtmiştir. řirket yaptığı basın açıklamasında, BT aęında birkaç çalışan hesabında gelişmiş bir kimlik avı saldırısı nedeniyle anormal bir etkinlik tespit ettiklerini ve adli soruşturma firması ile anlařtıklarını duyurmuřtur (Mendonca, 2019).

2. SİBER UZAYDA ULUS DEVLETLERİN YENİ BİR ASKERİ YETENEK OLUŞTURMASI

Ağ bağlantıları, telefonlar ve e-postalar gibi tüm iletişim sistemleri üçüncü bir kişi tarafından izlenebilen elektronik aktarımlara dayanmaktadır. Ulus devletler de tüm bu iletişim sistemlerinden toplanılan diplomatik, askeri ve ticari bilgilerle, potansiyel rakipler karşısında müzakere masasında veya savaş alanında avantaj elde etmektedir (Stokes, Lin, & Hsiao, 2011, s.2) .

Siber uzay, teknolojinin sonucu olarak yeni bir savaş alanına dönüşmüş ve ulus devletleri bu alandaki yeteneklerini geliştirmeye ve güçlendirmeye sevk etmiştir. Soğuk Savaş sonrası dönemde fiziksel kritik altyapılara yönelik siber saldırılar, demokratik süreçleri etkilemek için siber uzayda gerçekleştirilen manipülasyonlar ve siber casusluk gibi siber uzay kaynaklı tehditlerin artması sonucu ulus devletlerin tehdit algılamaları değişmiş, siber güvenlik, ulusal güvenliğin bir parçası ve hatta ulusal güvenlik önceliği haline gelmiştir. Dolayısıyla savunma, saldırı ve istihbarat toplama alanlarında geliştirilen siber yetenekler, ulus devlet gücü için yeni bir araç haline gelmiş ve siber savunmanın ulusal güvenlikteki rolü artmıştır. Ulus devletler ise vatandaşlarını, ordularını, istihbarat birimlerini, kamu kurumlarını siber uzay kaynaklı tehditlerden korumak için hem siber savunma hem de siber saldırı alanlarında kapasitelerini geliştirmek için siber güvenlik eylem planlarını oluşturmaya başlamıştır. Ulus devletler eylem planları çerçevesinde siber güvenlik alanında farklı siber tehditlerden sorumlu kurumlar inşa etmiş, siber uzmanlar ve akademisyenler yetiştirilmesi konusunda girişimlerde bulunmuştur.

Siber uzay siyasi, ekonomik ve askeri bir alan olarak algılanmasının yanı sıra ulus devletler tarafından diplomatik bir alan olarak da algılanmaktadır. Tıpkı diğer diplomatik girişimlerde olduğu gibi siber diplomaside de ortak tehditlere karşı devletlerin kendi güçlü yönlerinden ve uzmanlıklarından yararlanarak siber güvenliklerini geliştirmek ve gelişen siber tehditleri ele almak için stratejik ortaklıklar kurmayı, ortak eylem geliştirmeyi ve işbirliği yapmayı gerektirmektedir. Dolayısıyla siber yeteneklerini geliştiren ulus devletler, diğer yandan siber diplomasi girişimleriyle uluslararası toplumu, gelecekte siber operasyonlara karşı güçlendirmekte yardımcı olmaktadır. Ancak ulus devletlerin yeni kozu olan siber diplomasi, aynı zamanda yeni bir ulusal güvenlik tehdidine de dönüşebileceğinden, diğer devletlerin siber diplomasi

faaliyetlerini takip etmesi ulusal güvenliğe önemli katkılar sağlayabilir (Kotik, 2015, s. 74).

Sonuç olarak ulus devletler siber uzayda, siber stratejiler formüle etmekte ve siber faaliyetleri denetlemek, siber saldırı, siber savunma ve istihbarat yeteneklerinin geliştirilmesine yatırım yapmakta, bu doğrultuda yetkili kurum ve kuruluşlar oluşturmaktadır. Çalışmanın bu bölümünde, siber uzayda askeri yeteneklerini geliştirmekle aktif olarak ilgilenen dört oyuncuya odaklanılmıştır: ABD, Rusya Federasyonu, Çin Halk Cumhuriyeti ve İran İslam Cumhuriyeti. Ulus devletlerin yaklaşımları farklılık gösterse de, strateji belgelerinde savunma önlemlerine odaklanma, saldırı yetenekleri ve bilgi savaşı gibi ortak temalar ortaya çıkmaktadır. Bu ulus devletlerin siber yeteneklerini, strateji belgelerini ve kurumlarını anlamak, onların motivasyonları, hedefleri ve gelişen siber uzay ortamındaki potansiyel etkileri hakkında değerli bilgileri sağlamaktadır. Siber uzay gelişmeye devam ederken, politika yapıcılar, stratejisiler, araştırmacılar ve siber güvenlik uzmanları için ulus devletlerin siber uzaydaki faaliyetlerini yakından izlemek ve analiz etmek çok önemlidir. Bu bilgi, etkili savunma stratejileri, uluslararası işbirliği çabaları ve aktörlerin oluşturduğu potansiyel riskleri ve tehditleri azaltmak için siber güvenlik önlemlerini geliştirilmesi konusunda bilgi sağlayabilir. Ek olarak bilgilerin çoğu istihbarat değerlendirmelerine tabi olduğundan ulus devletlerin siber yeteneklerinin ve operasyonlarının tam kapsamını ve doğasını analiz etmenin zor olabileceğini not etmek önemlidir. Dolayısıyla ulus devletlerin siber faaliyetlerini anlamak ve değerlendirmek için açık kaynaklı istihbarat bilgileri, siber güvenlik olay raporları, hükümet açıklamaları ve resmi belgelerinden yararlanılmaktadır.

2.1. Amerika Birleşik Devletleri'nin Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri

Siber güvenliğin çeşitli yönlerini ele alarak birçok yasa çıkartan ABD, dünya çapında siber güvenlik politikası ve stratejisi geliştirmede öncü olmuştur. Sovyetler Birliği'nin resmi olarak dağılması ve Soğuk Savaşın sona ermesiyle birlikte ABD'de ulusal güvenlik tehditleri yeniden değerlendirilmeye başlanmıştır. Değerlendirmeler neticesinde ise bilgi-iletişim teknolojisinin zayıf noktalarına odaklanılarak, siber terörizm dahil tüm asimetrik tehditlerin ve ABD'nin kritik altyapısını hedef alan

saldırıların önlenmesinin gerekliliği raporlara yansımaya başlamıştır. Ulusal güvenliğe yönelik yeni tehditleri içeren türden ilk rapor ise 1993 yılında Savunma Bakanı tarafından kurulan Ortak Güvenlik Komisyonu tarafından yayınlanmıştır. Savunma Bakanı William J. Perry ve Merkezi İstihbarat Direktörü R. James Woolsey'e sunulan 1994 tarihli "*Güvenliği Yeniden Tanımlamak*" raporunda komisyon, bilgi sistemlerinin güvenliğini son on yılın ve muhtemelen gelecek yüzyılın en büyük güvenlik sorunu olarak gördüğünü ve bu alanda ciddi risklerin bulunduğu konusunda bilincin yetersiz olduğunu bildirmiştir (Joint Security Commission [JSC], 1994, s. 1).

Siber güvenlik ile ilgili en etkili rapor ise Ekim 1997'de yayınlanmıştır. Eski General Robert T. Marsh'ın başkanlığındaki "*Kritik Altyapı Koruma Komisyonu Raporu*", ABD'nin kritik altyapıyı koruma çabalarının temelini oluşturmuştur. Raporda kritik altyapının güvenliğinin ve sürekliliğinin sağlanması acil bir öncelik olarak değerlendirilmiş ve Amerikan ulusunun kritik altyapıya bağımlılığı nedeniyle ulusal güvenlik merceğinden bakılmasının gerekliliği vurgulanmıştır (President's Commission on Critical Infrastructure Protection [PCCIP], 10, s. vii).

2.1.1. Temel Belgeler ve Stratejiler

1997 yılında yayınlanan "*63 No'lu Başkanlık Direktifi (Presidential Directive-63)*", ABD'nin kritik altyapılarını tanımlayan ve daha sonra hazırlanacak olan strateji belge ve doktrinlere kaynak oluşturan ilk resmi belge niteliği taşımaktadır (Tirrell, 2012, s. 23). Belgede telekomünikasyon, enerji, bankacılık ve finans, ulaşım, su sistemleri, hem devlet hem de özel acil servisleri içeren kritik altyapı sınıflandırması yapılmış, hem fiziksel hem de siber alanda kritik altyapı sistemlerindeki güvenlik açıklarının ortadan kaldırılması için gereken tüm önlemlerin alınması tavsiye edilmiştir (Federation of American Scientists [FAS], 1998, s. 10).

2000 yılında hazırlanan *Bilgi Sistemleri İçin Ulusal Plan (National Plan for Information Systems Protection Version 1.0)*, siber güvenlik alanında hükümetin tek başına çözüm sunamayacağını ve kamu-özel sektör işbirliğine olan ihtiyacı vurgulayan bir strateji sunmuştur. Dönem Başkanı Clinton "*Hedefimizi hükümet düzenlemeleriyle zorunlu kılamayız, her sektör kilit sistemlerini korumak için hangi uygulamaların, prosedürlerin ve standartların gerekli olduğuna kendisi karar vermelidir*"

açıklamasıyla bilgi-iletişim güvenliğinde araştırma ve geliştirme faaliyetlerine ve kamu-özel sektör işbirliğinin önemine vurgu yapmıştır (FAS, 2000, s. iii).

2003 yılında ABD hükümetinin ilk kapsamlı ulusal siber güvenlik stratejisi olan *Siber Uzayı Güvenli Hale Getirmek için Ulusal Strateji (The National Strategy to Secure Cyberspace)* belgesinde, ulusal siber uzay güvenliği için üç stratejik hedef ve hedefe ulaşmak için beş ulusal öncelik belirlenmiştir:

Stratejik hedefler: (I) Ulusal kritik altyapılara yönelik siber saldırıların önlenmesi, (II) Olası siber saldırılara karşı ulusal güvenlik açığını azaltmak, (III) Meydana gelen siber saldırılardan kaynaklanan hasarı ve kurtarma süresini en aza indirmek

Ulusal öncelikler: (I) Federal bilgisayar sistemleri ve ağlarının güvenliğini sağlamak, (II) Siber saldırılara karşı yanıt sistemi geliştirmek, (III) Tehdit ve güvenlik açığını azaltmak için bir program oluşturmak, (IV) Siber güvenlik için farkındalık ve eğitim programı başlatmak, (V) Uluslararası işbirliği sistemi geliştirmek (The White House, 2003).

2006 yılında *Siber Uzay Harekatları için Ulusal Askeri Strateji (National Military Strategy for Cyberspace Operations)* belgesi, ABD hükümetinin siber uzayı bir savaş alanı olarak gördüğünü resmileştiren bir belgedir. Belgede, siber uzaydaki üstünlüğün, askeri, istihbarat, ticari operasyonlarda ve aynı zamanda hava, kara, deniz, uzay alanlarındaki operasyonları desteklenmesinde kritik bir rol oynadığı ifade edilmekte ve istenen etkileri elde etmenin siber uzay operasyonlarını yürütme yeteneğine bağlı olduğu belirtilmiştir. Bu doğrultuda ABD'nin siber uzayda kontrolü ve üstünlüğü sağlaması için gerekli adımları atmaya yönelik bir çerçeve sunulmuştur (DOD, 2006).

2008 tarihli *Ulusal Savunma Stratejisi'nde (National Defense Strategy)* kritik altyapıya yönelik siber tehditlerin varlığı karşısında siber caydırıcılığa olan ihtiyaç vurgulanmıştır. ABD Savunma Bakanlığı'nın uzun vadede siber tehditlere karşı önemli bir role sahip olduğu, ancak en iyi yeteneğe sahip olmadığı ve görevleri üstlenebilecek uygun bir otorite olmadığı sonucuna varılmıştır (DOD, 2008, s. 7). Ayrıca belgede Çin ile ilgili olarak "*geleneksel avantajlarımızı bozacak teknolojiler geliştirildiği*" vurgusu yapılmıştır. Bahsi geçen teknolojiler arasında Çin'in -bir ülkenin düşman uydu sistemlerini tespit etme, takip etme, etkisiz hale getirme veya yok etme yeteneğini

ifade eden- uydu karşıtı yetenekler ve siber savaş gibi teknolojiler üzerinde çalıştığı belirtilmektedir. Çin dışında devlet dışı aktörlerin de ABD'nin avantajlarını devre dışı bırakacak asimetrik tehdit içeren teknik ve taktikler geliştirdiği ifade edilmektedir (DOD, 2008, s. 22).

2009 yılında yayınlanan *Siber Uzak Politikasının Revizyonu (Cyberspace Policy Review)*, ABD politikalarını ve organizasyon yapılarını değerlendirmek için Başkan Obama'nın talimatı üzerine 60 günlük kapsamlı bir inceleme ile hazırlanmıştır. Belgede, ulusun dijital altyapısının güvenli veya dayanıklı olmadığı, hükümetin büyüyen siber suç ve devlet destekli izinsiz giriş tehditlerini koruyabilme yeteneğinin yetersiz olduğu ve federal hükümetin bu büyüyen siber güvenlik sorunu karşısında etkin bir şekilde örgütlenmediği eleştirileri yapılmış ve sonucunda alınması gereken tedbirler belirtilmiştir. Özellikle bilgi ve iletişim ağlarının, hem ulusal hem de uluslararası düzeyde özel sektöre ait olduğu ve işletildiği için ağ güvenliği konularının, kamu-özel sektör ortaklığının gerekliliği vurgulanmıştır. Bu doğrultuda on tane yakın vadeli, on dört tane uzun vadeli eylem planı oluşturulmuştur (FAS , 2009).

Siber güvenliğin "*ulusal güvenlik önceliği*" olduğu belirtilen 2010 tarihli *Ulusal Güvenlik Stratejisi'nde (National Security Strategy)*, karşılaşılan siber tehditlerin bireysel suç örgütlerinden organize suç gruplarına, terör ağlarından gelişmiş ulus devletlere kadar geniş çapta varlığından söz edilmiştir. Belgede "*internet ve e-ticaret, ekonomik rekabet gücümüzün anahtarıdır, ancak siber suçlular şirketlere ve tüketicilere yüz milyonlarca dolara ve değerli fikri mülkiyete mal olmuştur*" açıklaması, kaygının siyasiden çok ekonomik doğaya sahip olduğunu göstermektedir (The White House, 2010, s. 27).

2011 yılında ABD'nin ortaklarla ilişki kurma yaklaşımını yansıtan *Siber Uzak için Uluslararası Strateji(International Strategy for Cyberspace)* belgesinde ifade edilen genel amaç; uluslararası ticareti destekleyen ve uluslararası güvenliği güçlendiren bir bilgi ve iletişim altyapısını teşvik etmek için siber uzayda; ortaklıkların sürdürdüğü, hukukun üstünlüğünün desteklendiği ve devletlerin sorumlu davranış normlarına uyması gerektiği bir ortamın oluşturulmasıdır. Strateji bu amacı, ortaklıkların güçlendirilmesi için 'diplomasi', caydırıcılık kabiliyetinin geliştirmesi için 'savunma', refah ve güvenliğin sağlanması için 'kalkınma' hedeflerine bölmüştür. Ekonomi, ulusal ağların korunması, kolluk kuvvetleri, askeri, internet yönetimi,

uluslararası kalkınma ve internet özgürlüğü olmak üzere birbirine bağlı yedi faaliyet alanında politika önceliklerine de yer verilmiştir. Ayrıca belgede temel özgürlüklerin korunması, mülkiyete saygı, gizliliğe önem verme, suçtan korunma ve meşru müdafaa hakkı ilkeleri çerçevesinde devletlerin siber uzayda uluslararası yükümlülükleri nasıl yerine getirmesi gerektiği konusunda yol haritası sunulmuştur (The White House, 2011).

2012 yılında ABD'nin gizli tuttuğu *Başkanlık Politika Direktifi 20 - Siber Hareket Politikası* (*Presidential Policy Directive 20 (PPD-20) - U.S. Cyber Operations Policy*), eski NSA çalışanı Edward Snowden tarafından basına sızdırılmıştır. The Guardian tarafından elde edilen söz konusu gizli başkanlık direktifine göre, Barack Obama üst düzey ulusal güvenlik ve istihbarat yetkililerine ABD siber saldırıları için potansiyel denizaşırı hedeflerin bir listesinin hazırlanmasını emretmiştir (Greenwald & MacAskill, 2016).

2015 tarihli Ulusal güvenliğe yönelik riskleri ve tehditlerin ele alındığı *Ulusal Güvenlik Stratejisi'nde* deniz, hava, uzay güvenliğinin yanı sıra siber güvenlik konusunda da değerlendirmelere yer verilmiştir. Özellikle siber güvenlik konusunda, Çin'in devlet destekli siber tehdit aktörlerinin ve özel aktörlerinin ticari kazanç için yürüttüğü siber casusluk faaliyetleri noktasında bir tehdit yarattığı, bu doğrultuda ABD'nin ağlarını korumak için gerekli tedbirleri alarak ticari çıkarlarını koruyacağı belirtilmiştir (The White House, 2015, s. 24).

2015 tarihli *Savunma Bakanlığı Siber Strateji* (*The Department of Defence Cyber Strategy*) belgesinde siber uzay için beş stratejik hedef belirlemiştir. (I) Siber uzay operasyonlarını yürütmek için hazır kuvvetler ve yetenekler oluşturmak, (II) Savunma Bakanlığı ağını, verilerini korumak ve görevlere yönelik riskleri azaltmak, (III) Önemli sonuçlar doğurabilecek yıkıcı siber saldırılara karşı ABD'nin hayati çıkarlarını savunmaya hazır tutmak, (V) Uygulanabilir siber seçenekler oluşturarak, bu seçenekleri çatışmanın tırmanmasını kontrol etmek ve çatışma ortamını şekillendirmek için kullanmayı planlamak, (IV) Ortak tehditleri caydırmak, uluslararası güvenlik ve istikrarı korumak için uluslararası ittifaklar kurmak. Ayrıca siber saldırılara karşı savunma ve caydırıcılık için uluslararası ortaklık üzerine yeni bir vurgu yapılan belgede, özellikle Orta Doğu, Asya Pasifik ve önemli NATO müttefikleri ile bu çabalara odaklanılacağı belirtilmiştir (DOD, 2015a).

2016 tarihli *Başkanlık Politika Yönergesi (Presidential Policy Directive (PPD)-41)* çerçevesinde ABD önemli siber olaylarda hükümet müdahalesini koordine etmek için bir temel kurmuş, olay müdahalesine yönelik ilkeler çerçevesinde federal hükümet içinde kamu ve özel sektör arasında yakın koordinasyonun gerekliliği vurgulanmıştır (The White House, 2016).

Donald Trump'ın başkanlık yaptığı dönemde tehdit algılamaları çerçevesinde oluşturulan 2017 tarihli *Ulusal Güvenlik Strateji'nin* birçok bölümünde siber güvenlik konusunda tehditler ve alınacak önlemlere yer verilmiştir. Belgede alınacak önlemler çerçevesinde, siber saldırılara karşı hızlı yanıt verebilmek için saldırıları atfetme yeteneğine yatırım yapılacağı, kritik altyapının ve verilerin bütünlüğünü korumak için siber araçların çatışma temelinde geliştirileceği ifade edilmiştir. Siber tehdit aktörlerinin yasa dışı faaliyetleri için çevrimiçi pazarlar ve kripto para birimleri gibi araçları kullanma yeteneğini bozmak amacıyla soruşturma araçlarının kullanılacağı ve diğer ülkeleri bu suçlara yardım etmekten sorumlu tutulacağı belirtilmiştir. Tehdit algılamaları çerçevesinde ise Rusya'nın dünya çapında kamuoyunu etkilemek amacıyla siber saldırı operasyonlarını kullandığı ve bu operasyonlar doğrultusunda ise devlet destekli medya aracını, üçüncü taraf araçlarını ve ücretli sosyal medya kullanıcılarını (troller) kullanarak gizli istihbarat operasyonları gerçekleştirdiği ele alınmıştır (The White House, 2017).

2018 tarihli *Ulusal Siber Strateji (National Cyber Strategy of the USA)* belgesinde kritik altyapıyı güçlendirme, kamu-özel sektör koordinasyonu, devlet ağlarının güvence altına alınması ve uluslararası ittifakın kurulmasının önemi, diğer belgelerde olduğu gibi tekrar vurgulanmıştır. Ancak Trump yönetiminin diğer yönetim planlarıyla benzerlikler taşımasına rağmen alınacak tedbirler daha "saldırgan" olarak nitelendirilebilmektedir. Belgenin "*Güç Yoluyla Barışı Korumak*" başlıklı III. sütununda, siber uzayın artık ulusal gücün diğer unsurlarından ayrı bir politika kategorisinde görülmeyeceğini ve siber operasyon kullanımının ulusal gücün her unsuruna entegre edileceği ifadeleri yer almaktadır. Bölümde amaç ise siber uzayda ABD'nin üstünlüğünü korurken, siber uzayda istikrarsızlaştırıcı ve ulusal çıkarlara aykırı davranışların tespiti yapılması, azaltılması ve caydırılması olarak belirlenmiştir (The White House, 2018, s. 20). Dolayısıyla Trump yönetimi, savunma teknolojilerini güçlendirmeye ve güvenlik ihlallerinin etkisini en aza indirme çalışmalarına odaklanmaya devam etmek yerine, saldırgan siber operasyonlarını

hızlandırma yönünde ifadelerde bulunmuştur. Yeni hedef, "önleyici siber saldırılar" yoluyla düşmanları caydırmak ve diğer ulusların ABD hükümetinin misilleme gücünden korkmasını sağlamaktır (Wolff, 2018).

2018 tarihli *Savunma Bakanlığı Siber Stratejisinde (Department of Defense Cyber Strategy)*, tehdit algılamaları çerçevesinde Çin'in ABD kamu ve özel sektör kurumlarında sürekli olarak casusluk faaliyetleri yürüterek ABD'nin ekonomik canlılığını aşındırdığı, Rusya'nın demokratik süreci etkilemek için bilgi operasyonlarını kullandığı, Kuzey Kore ve İran'ın da ABD çıkarlarını tehdit etmek için kötü niyetli siber saldırı faaliyetlerinde bulunduğu açıklanmıştır. Bu doğrultuda ise kriz veya çatışma durumunda, silahlı çatışma eşiğinin altına düşen siber saldırı ve istihbarat faaliyetleri dahil olmak üzere ABD, ulusal güvenliğine tehdit oluşturabilecek tüm eylemler karşısında siber uzay operasyonlarının yürütüleceğini açıklanmıştır. Savunma Bakanlığı ulusal stratejinin yürütülmesine yardımcı olacak beş tane strateji yayınlamıştır: daha yıkıcı bir güç oluşturmak, siber uzayda rekabet etmek ve caydırmak, ittifakları güçlendirmek ve ortaklıkları genişletmek, departmanda reformlar gerçekleştirmek, siber yetenekler yetiştirmek (DOD, 2018).

2021 tarihli *Ülkenin Siber Güvenliğinin Geliştirilmesine İlişkin Başkanlık Yürütme Emri (Presidential Executive Order on Improving the Nation's Cybersecurity)*, siber tehdidi tanımlama, caydırma, koruma, tespit etme ve yanıt verme çabalarının geliştirilmesi yönünde önemli yatırımlar yapmak için gerekli şartları belirlemektedir. Hükümet ve özel sektör arasındaki bilgi paylaşımının geliştirilmesinin tekrar vurgulandığı başkanlık emrinin 5. bölümü çerçevesinde 2002 tarihli İç Güvenlik Yasası'nın (6 U.S.C. 451) 871. maddesi uyarınca siber tehdit faaliyetlerini ve güvenlik açıklarını gözden geçirilmesi ve değerlendirmesinden sorumlu Siber Güvenlik İnceleme Kurulunun oluşturulacağı belirtilmiştir (The White House, 2021a).

2022 tarihli *Ulusal Güvenlik Strateji Belgesinde*, günümüz dünyasında giderek dijitalleşen kritik altyapının siber saldırılar karşısında savunmasız kaldığı ve "Rusya gibi ülkeler tarafından" ülkelerin vatandaşlara hizmet sunma yeteneklerini baltalamak için kullanıldığı vurgulanmıştır. Belgede Japonya, Hindistan ve Avustralya ile QUAD çerçevesinde siber güvenlik dahil birçok tehdit konusunda yakın işbirliği içinde çalışıldığı, uluslararası hukuk fiziksel dünyada olduğu gibi dijital dünyada da geçerli olduğunu kabul eden, BM Genel Kurulu tarafından onaylanan "siber uzayda sorumlu

devlet davranışının" uygulanmasının teşvik edileceği açıklanmıştır (The White House, 2022).

2.1.2. Amerika Birleşik Devletleri'nin Siber Güvenlik Ulusal Organizasyon Yapısı

ABD'de siber güvenlik alanında yetkili tek bir kurumun olmaması, ABD'nin siber güvenliğe verdiği stratejik önemi gösterse de, oluşturulan ulusal organizasyon karmaşık bir yapıya sahiptir. Öncelikle tüm hükümet departmanları kendi ağ sistemlerinin korunmasından sorumludur ve birçoğunun sorumlu olduğu kritik altyapı sektörlerinde özel sorumlulukları vardır. Özellikle 1945-1991 yılları arasında SSCB-ABD rekabetinin gösterdiği etkiyle birlikte ABD siber güvenlik konusunu askeri alan içerisinde değerlendirmeye başlamış ve FBI bünyesinde politikalar belirlemiştir. Soğuk Savaş sonrası dönemde ise değişen güvenlik anlayışının çeşitlenmesi ve Çin ve Rusya'nın siber uzayda güçlenmesi ABD'nin siber güvenlik anlayışına etki etmiş ve yıllar içerisinde temel kurumlar yenilenerek gelişme göstermiştir (Kızılay, 2020, s. 40).

2.1.2.1. ABD Savunma Bakanlığı

ABD Savunma Bakanlığı'nın (Department of Defense-DOD) siber faaliyetleri ve misyonu, 2015 tarihli Savunma Bakanlığı Siber Stratejisi belgesinde üç ana görevle tanımlanmıştır: (I) Savunma Bakanlığı ağlarının, sistemlerinin ve bilgilerinin korunması için siber güvenlik operasyon yeteneklerini geliştirmek; (III) ulusu hedefleyen ve '*önemli sonuçları olan*' siber saldırılara karşı savunma yeteneğini geliştirmek; (II) askeri operasyonlara ve acil durum planlarına destek sağlamak. Bu amaç doğrultusunda Savunma Bakanlığı, Savunma Bakanlığı Bilgi Ağı'nı (Department of Defense Information Network-DoDIN) güvenli bir şekilde işletmek için sürekli olarak ağ savunma operasyonları yürütmektedir. Ayrıca ABD çıkarlarına yönelik siber saldırılar, -can kaybı, mülk hasarı, ciddi ekonomik etkiler veya olumsuz dış politika sonuçları gibi- *önemli sonuçlara* sebep olabilecek saldırılar karşısında, Savunma Bakanlığı karşı siber operasyonlar gerçekleştirilmek ABD ordusuna talimat verebilme yetkisine sahiptir (DOD, 2015a, s. 4).

Savunma Bakanlığı bünyesinde oluşturulan kurumlar ABD hükümetinin ulusal güvenlik stratejisinin önemli bir ayağını oluşturmaktadır. Bu bağlamda Savunma Bakanlığı'nın siber güvenlikteki operasyonel rol ve sorumlulukları, ABD Siber Komutanlığı (United States Cyber Command-USCYBERCOM), Ulusal Güvenlik Ajansı (National Security Agency-NSA), Savunma Bakanlığı Siber Suç Merkezi (Department of Defense Cyber Crime Center-DC3), Savunma Bilgi Sistemleri Ajansı (Defense Information Systems Agency-DISA) aracılığı ile gerçekleştirilmektedir (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, s. 20).

2.1.2.1.a. ABD Siber Komutanlığı

Savunma Bakanlığı'nın (USCYBERCOM) siber güvenlik konusunda en yetkili organizasyonu USCYBERCOM'dur. Fort Meade Maryland'de bulunan ve NSA karargahı ile aynı yerde bulunan ABD Stratejik Komutanlığı (USSTRATCOM) altında, birleşik bir alt komutanlık olarak kurulmuştur. 21 Mayıs 2010 tarihinde kurulan USCYBERCOM aynı yıl içerisinde 31 Ekim 2010'da tam hareket kabiliyetine ulaşmıştır. Askeri siber uzay operasyonlarını yürütmede birincil sorumluluğa sahip olan USCYBERCOM, Savunma Bakanlığı'nın bilgi ağlarının operasyonlarını ve savunmasını yürütme, koordine etme, senkronize etme görevlerine sahiptir (DODa, 2010).

USCYBERCOM'u oluşturan alt bileşenler ise 2009 yılında oluşturulmuştur. Bu alt bileşenler, USCYBERCOM'un çeşitli askeri kolların siber yeteneklerini birleştiren ve koordine eden bir merkez olarak çalışmasını sağlar. (United States Cyber Command [USCYBERCOM], tarih yok). Bunlar;

1. *ABD Ordusu Siber Komutanlığı (ARCYBER)*; ABD Ordusu'na ait ve USCYBERCOM'un yer karargahı olarak görev yapan birimdir. Ağ savunması, ağ saldırısı ve siber operasyonlar gibi görevleri yerine getirmektedir.
2. *Filo Siber Komutanlığı (FLTCYBER)*; ABD Donanması'na ait olan ve donanmanın siber kapasitesini yöneten birimdir. Deniz operasyonları, ağ güvenliği ve siber saldırılarla mücadele gibi görevleri yerine getirmektedir.
3. *Hava Kuvvetleri Siber Komutanlığı (AFCYBER)*; ABD Hava Kuvvetleri'ne ait olan ve hava kuvvetlerinin siber yeteneklerini yöneten

birimdir. Hava operasyonları, ağ savunması ve siber istihbarat gibi görevleri yerine getirmektedir.

4. *Deniz Piyadeleri Siber Uzay Komutanlığı (MARFORCYBER)*; ABD Deniz Piyadeleri'ne ait olan ve deniz piyadelerinin siber yeteneklerini yöneten birimdir. Deniz piyade operasyonları, ağ güvenliği ve siber savunma gibi görevleri yetine getirmektedir.

2012 yılında USCYBERCOM'un eylem kolu olan *Siber Görev Gücü (Cyber Mission Force-CMF)*, ABD ulusal çıkarlarını savunmak için siber uzay operasyonlarını yönlendirme ve koordine etme misyonu çerçevesinde oluşturulmuştur. Savunma amaçlı siber uzay operasyonlarını yürütmek, siber güvenliği sağlamak ve sürdürmek, Savunma Bakanlığı Bilgi Ağı'nın Ordu bölümünün ağlarını korumak CMF'nin temel görevleridir (U.S. Army Cyber Command, 2022).

Siber Ulusal Görev Gücü (Cyber National Mission Force-CNMF), ABD hükümetine yönelik bir siber saldırıya tepki gösteren üç USCYBERCOM kuvvetinden biridir. *Savaş Görev Gücü (Cyber Combat Mission Force -CCMF)*, ABD'yi savunmak için siber tehdit aktörlerini caydırmak ve gerektiğinde saldırmak için siber uzay operasyonlarını planlamakta ve yönlendirmektedir. CCMF, askeri siber yeteneklerini içeren bir birimdir ve saldırıda bulunan siber tehdit aktörlerine karşı misilleme yapmak ve caydırıcılık sağlamak için çalışmaktadır. *Siber Koruma Gücü (Cyber Protection Force - CPF)* ise ABD hükümetine ait bilgi ve iletişim ağlarını korumakla, siber tehditlere karşı dirençli hale getirmekle, siber saldırılara karşı önlemler almakla, ağları izlemekle ve savunma sistemlerini güncel tutmakla görevli bir birimdir (United States Cyber Command [USCYBERCOM], tarih yok).

2.1.2.1.b. Ulusal Güvenlik Ajansı

ABD Savunma Bakanlığı'nın ulusal düzeydeki istihbarat teşkilatı olan Ulusal Güvenlik Ajansı (National Security Agency-NSA), siber güvenlik paylaşımı ve analizinde gerekli uzmanlığa ve kaynaklara sahip savunma odaklı bir organizasyondur. Toplumun dijital ağlara bağımlılığı, veri ve ağlara yönelik artan sayıdaki tehditler, teknolojinin terör örgütleri tarafından kullanılması ve ulus devlet destekli siber saldırıların artması NSA için yeni görev tanımlamalarının oluşmasına yol açmıştır (National Security Agency [NSA], 2012). Bu bağlamda NSA'nın şifre oluşturma ve

şifte kırma yetenekleri, küresel izleme, veri toplama, veri analizi, dijital adli tıp araştırmaları, karşı istihbarat, siber istihbarat, tehdit istihbaratı analizi, sinyal toplama ve teknik siber güvenlik uzmanlığı ABD hükümetinin genel siber güvenlik misyonuna farklı katkılar sunmaktadır (Darıcılı, 2017, s. 8).

Ayrıca ABD Sinyal İstihbarat Topluluğu (Intelligence Community -IC) ile iletişimi daha sağlıklı yürütebilmek adına NSA direktörü aynı zamanda USCYBERCOM'un da şefi olarak "çift şapkalı" görev yapmaktadır (Gallagher, 2013).

Ulusal Güvenlik Operasyon Merkezi (National Security Operations Center-NSOC) ve NSS/CCS Tehdit Operasyonları Merkezi (National Security Agency / Central Security Service Threat Operations Center -NTOC) ise NSA'nın küresel operasyonlarının bir parçası olarak faaliyet gösteren ve 7 gün 24 saat çalışan iki büyük merkezidir. 1960'larda Orta Doğu'daki gerilimler, Arap-İsrail Savaşı, SSCB'nin Çekoslovakya'yı işgali ve Kuzey Kore'nin deniz harekatı sırasında Amerikan casusluk gemisi USS Pueblo'yu ele geçirmesi gibi çeşitli uluslararası krizler, NSA'nın bu coğrafi bölgeler için ayrı ofisler oluşturmaya yönlendirmiş ve dünya genelinde neler olduğunu tam anlamak için birden fazla ofisten anında bilgi almanın önemini göstermiştir. Kuruluş aşamasında olduğu 1969 yılında Kuzey Kore ABD Donanmasına ait EC-121 keşif uçağını düşürdüğünde büyük bir kriz baş göstermiş ve NSA'nın krizlere hızlı yanıt vermezini koordine etmek için tek bir özel izleme merkezi kurulmasını gerektirmiştir. Bu nedenle 1968'de Ulusal Sinyal İstihbaratı İzleme Merkezi (National SIGINT Watch Center-NSWC) olarak kurulmuş ve 1973'te Ulusal Sinyal İstihbaratı Operasyon Merkezi (National SIGINT Operations Center - NSOC) olarak yeniden adlandırılmıştır (Johnson, 1995, s. 469). Dolayısıyla NSOC, dünya genelindeki NSA ofislerinden gelen bilgileri analiz eder, durumu değerlendirir ve ilgili karar mercilerine anında bilgi sağlar. Böylece NSA'nın uluslararası krizlere hızlı ve koordineli bir şekilde yanıt vermezi ve bilgi akışını sağlaması amaçlanmaktadır.

2004 yılında NSA Genel Müdürü Michael Hayden tarafından ABD bilgi sistemlerine yönelik dış tehditleri değerlendirmek, müdahale etmek ve raporlamak için ortak bir bilgi güvenliği ve sinyal istihbaratı (SIGINT) girişimi olarak NSA/CSS Tehdit Operasyonları Merkezini kurmuştur (National Security Agency [NSA], 2012). Bu bağlamda NTOC, siber tehditleri tahmin etmek, ortaya çıkartmak, uyarmak ve

ilişkilendirmek için hem bilgi güvenliği hem de sinyal istihbaratı yeteneklerini kullanmaktadır (Office of the Director of National Intelligence [ODNI], 2013, s. 18).

2.1.2.1.c. Savunma Bakanlığı Siber Suç Merkezi

Savunma Bakanlığı'nın bir bileşeni ve federal siber güvenlik merkezi olan Savunma Bakanlığı Siber Suç Merkezi (Department of Defense Cyber Crime Center-D3C), Savunma Bakanlığı'nın siber suç soruşturması, dijital adli tıp ve siber güvenlik için önde gelen kuruluşu olarak hizmet vermektedir. Ayrıca kurumlar arası ve uluslararası işbirliğini destekleyen bir Saha Operasyon Ajansıdır. Savunma Bakanlığı'nı hedef alan siber suçlara yönelik soruşturma yürütmek; bilgisayarlardan, mobil cihazlardan ve diğer dijital kaynaklardan elektronik kanıtların toplanmasını, analiz edilmesini ve korunmasını içeren dijital adli tıp uzmanlığı ile değerli istihbaratı ortaya çıkarmak ve soruşturmaları desteklemek için gelişmiş adli tıp tekniklerini uygulamak; güvenlik açıklarını belirlemek için siber tehdit istihbaratı toplamak ve analiz etmek; siber güvenlik teknolojilerini ve yeteneklerini geliştirmek; Savunma Bakanlığı çalışanlarının, kolluk kuvvetlerinin ve uluslararası ortakların siber yeteneklerini ve bilgilerini geliştirmek için özel eğitim programı sağlamak; devlet kurumları ve endüstri ortakları ile işbirliğini teşvik etmek başlıca görevleri arasındadır (Department of Defense Cyber Crime Center [DC3], tarih yok). Ayrıca DHS, NSA, FBI ve USCYBERCOM DC3'ten destek almaktadır.

2.1.2.1.d. Savunma Bilgi Sistemleri Ajansı

İletişim sorunları sonucunda kurulan ve daha önce Savunma İletişim Ajansı (DCA) olarak bilinen Savunma Bilgi Sistemleri Ajansı (DISA), ABD Savunma Bakanlığı için çalışan tüm kurumlara, orduya, ulusal düzeydeki liderlere BT ve iletişim desteği sağlayan bir muharebe destek ajansıdır. Savunma Bilgi Sistemleri Ağı (DISN) olarak bilinen küresel bir iletişim ağını işletmek; dünya genelinde askeri komutanlıklar, tesisler ve konuşlandırılmış kuvvetler arasında bağlantı kurmak için güvenli ses, video ve veri hizmeti sağlamak; güvenli iletişim altyapısı ve ağ hizmetleri ile Savunma Bakanlığı'nın komuta ve kontrol sistemlerini desteklemek; yapay zeka, makine öğrenimi ve gelişmiş iletişim teknolojileri gibi BT yeteneklerini araştırmak,

değerlendirmek ve test etmek; Savunma Bakanlığı'nın uydu iletişim sistemlerini yöneterek askeri operasyonlar, istihbarat toplama, komuta ve kontrol amaçları için güvenli küresel bağlantı sağlamak; çok uluslu bilgi paylaşımı ve veri hizmetleri gibi hizmetler sunarak önemli bilgilere erişmesini sağlamak temel görevleridir (Defense Information Systems Agency [DISA], tarih yok).

2.1.2.2. ABD İç Güvenlik Bakanlığı

2002 Ulusal Güvenlik Yasası kapsamında siber güvenlik lideri olarak kurulan İç Güvenlik Bakanlığı'nın (The Department of Homeland Security-DHS) siber güvenlik alanındaki hedefleri; siber güvenliğin sağlanması, kritik altyapıların korunması, hükümetin iletişim ve operasyonel gücünün devamlılığının sağlanması, ulaşım sektörünün korunmasıdır (Başa, 2020).

2.1.2.2.a. Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA)

2007'de kurulan ve DHS'nin siber güvenlik ile ilgili konularını yürüten Ulusal Koruma ve Programlar Müdürlüğü (NPPD), 16 Kasım 2018'de Başkan Trump'ın Siber Güvenlik ve Altyapı Güvenlik Ajansı Yasası ile CISA olarak yeniden organize edilmiştir (Congress.gov, 2018).

ABD'de siber güvenlik ve altyapı korumasını güçlendirmekten, siber güvenlik programlarını koordine etmekten, siber riskleri azaltmaktan sorumlu olan CISA, siber riskleri azaltmak ve siber güvenlik yeteneklerini geliştirmek için federal kurumların izlemesi gereken özel talimatları sunan ilk Acil Durum Yönergesini 22 Ocak 2019'da yayınlamıştır (CISA, 2019). 2018'de kuruluşundan bu yana ilk kapsamlı 2023-2025 CISA Stratejik Planını yayınlamıştır. Stratejik plan, siber uzayın savunmasını ve dayanıklılığını sağlamak için ABD'nin kritik altyapısını, özel sektörünü ve Amerikan halkını hedef alan siber tehdit aktörlerine karşı ulusal çabalara öncülük etmek, ABD'nin kritik altyapısına yönelik riskleri azaltmak ve dayanıklılığını güçlendirmek, tüm ulusun siber operasyonel işbirliğini ve bilgi paylaşımını güçlendirmek üzere planlar ortaya koymuştur (CISA, 2022b).

ABD Bilgisayar Acil Durum Hazırlık Ekibi (United States Computer Emergency Readiness Team - US-CERT), siber tehditlerini ve güvenlik açıklarını

analiz etmek ve azaltmak, olay müdahale faaliyetlerini koordine etmekten sorumlu olarak CISA kapsamında çalışmaktadır. Federal kurumlar, özel sektör, araştırma topluluğu, eyalet ve yerel yönetimler, uluslararası kuruluşlarla birlikte çalışmaktadır (DHS, tarih yok(a)).

Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center - NCCIC), Siber Güvenlik ve İletişim Ofisi (CS&C) bünyesinde 7/24 hizmet veren, federal hükümet, istihbarat topluluğu, yasa uygulayıcı kurumlar ve özel sektör genelinde siber faaliyetlere karşı olay müdahalesi ve yönetim merkezi olarak hizmet vermektedir (DHS, tarih yok(b)). Kritik siber ve iletişim altyapısına yönelik tehditleri analiz ederken, DOD, NSA, ABD Gizli Servisi (USSS), FBI, DOJ, özel sektör, US-CERT gibi federal birimlerden gelen verileri ve müdahale faaliyetlerini koordine etmekten sorumludur (Çifci, 2017, s. 45).

2.1.2.2.b. Siber Güvenlik İnceleme Kurulu

Siber Güvenlik İnceleme Kurulu (Cyber Safety Review Board-CSRB), Başkan Biden'ın 12 Mayıs 2021 tarihli Ulusal Siber Güvenliği İyileştirme konulu 14028 sayılı İcra Emri uyarınca kurulmuştur. Kurul, CISA aracılığıyla yönetilen bağımsız bir kamu-özel danışma organıdır. Önemli siber olaylardan alınan dersleri gözden geçirmek ve özel-kamu sektörlerinde iyileştirmeleri sağlayacak somut önerilerde bulunmak temel görevleri arasındadır (CISA, tarih yok(d)).

2.1.2.2.c. Ulaştırma Güvenliği Ajansı

Ulaştırma Güvenliği Ajansı (Transportation Security Agency-TSA), CISA ile yakın koordinasyon içinde ABD'nin hava ve kara taşımacılığını içeren ulaşım sistemlerinin ağ güvenliğini sağlamakla görevlidir. Hava, kara, demir yolu taşımacılığı sistemlerine ve ilgili altyapıya yönelik siber güvenlik tehdidi konusunda ve kritik boru hatları, sıvılaştırılmış doğal gaz tesislerinin siber güvenliği konusunda güvenlik yönergeleri hazırlayan düzenleyici bir kurumdur (O'Neil & Borgia, 2022).

2.1.2.2.d. ABD Sahil Güvenlik

ABD Sahil Güvenlik (United States Coast Guard - USCG), Amerikan limanlarında, terminallerinde, gemilerinde ve rafinerilerindeki destek sistemlerine, endüstriyel kontrol sistemlerine ve diğer tüm denizcilik sektörüne yönelik siber saldırılara karşı mücadele etmek ve ABD'nin denizdeki çıkarlarını hem yurt içinde hem de yurt dışında korumakla görevlidir (United States Coast Guard [USCG], tarih yok).

2.1.2.2.e. ABD Gizli Servisi

1865'te iç savaşın ardından sahte para biriminin yükselişiyle mücadele etmek için kurulan ABD Gizli Servisi (United States Secret Service-USSS), ülkenin finansal altyapısını korumaya odaklı siber suçları araştırmakla görevlidir. Ağ saldırıları, fidye yazılımı, ATM ve satış noktası sistemlerine saldırı, yasadışı finansman operasyonları, kara para aklama, kimlik hırsızlığı, bilgisayar korsanlığı, sosyal mühendislik gibi Amerikan finans sistemini hedef alarak ülkenin finansal sistemlerinin bütünlüğünü etkileyen siber suçlara odaklanarak, kişileri tespit etmekten, soruşturmadan ve tutuklamaktan sorumlu bir birimdir (DHS, tarih yok(c)).

2.1.2.2.f. Göçmenlik Gümrük Muhafaza - İç Güvenlik Soruşturmaları

ABD İç Güvenlik Bakanlığı'nın soruşturma kolu olan ve sınır kontrolü, gümrük, ticaret, göçmenlik ile ilgili federal yasaların uygulanmasından sorumlu Göçmenlik Gümrük Muhafaza - İç Güvenlik Soruşturmaları (Immigration and Customs Enforcement Homeland Security Investigations - ICE HSI), çeşitli suç faaliyetlerini soruşturmaya yönelik misyonu çerçevesinde siber suçları ele almada da bir role sahiptir. ICE HSI, siber dolandırıcılık, çevrimiçi platformlar aracılığıyla yasa dışı mal ve hizmetlerin dağıtımını, fikri mülkiyet hırsızlığı, çocuk istismarı, kara para aklama ve Dark Web'deki suç faaliyetleri dahil siber tabanlı yerel veya uluslararası siber suçlarda dünya çapında bir kanun uygulayıcı birimdir (FBI, tarih yok). HSI Siber Suçlar Merkezi (Cyber Crimes Center - C3), sınır ötesi siber suç faaliyetlerine ilişkin yerel ve uluslararası soruşturmaları desteklemekte ve bilgisayar tabanlı teknik hizmetler sunmaktadır (U.S. Immigration and Customs Enforcement [ICE], tarih yok).

2.1.2.3. Federal Arařtırma B rosu (FBI)

ABD Adalet Bakanlıęı'nın (Department of Justice - DOJ) bir b l m  olan FBI, ABD'de karřı istihbarattan sorumlu ve siber su ların arařtırılmasında  nemli federal bir kurumdur. "*ABD'yi yabancı istihbarat, casusluk ve siber operasyonlara karřı korumak*" FBI'n  ncelikleri arasında    nc  sırada yer almaktadır (FBI, tarih yok(a)). Dolayısıyla FBI, ABD'nin siber g venlik stratejisini uygulamasında  nemli rol  bulunmaktadır.

2002 yılında kurulan *Siber B l m  (Cyber Division - CyD)*, FBI'n ulusal g venlikle ilgili siber saldırı  abalarında birincil sorumluluęa sahiptir. FBI'n siber su ları arařtırma ve bunlara yanıt verme  abalarına  nc l k etmektedir. ABD'deki mevcut 56 FBI saha ofisinin her birinin  zel ajanları, istihbarat analistleri, dilbilimcileri ve bilgisayar m hendislerinden oluřan en az bir siber g venlik ekibi vardır. En b y k saha ofisleri ise birden fazla siber g venlik ekibine sahiptir ve her bir ekip ulusal siber g venlik ihlalleri,  evrimi i  ocuk pornografisi, fikri m lkiyet hakları ve internet dolandırıcılığı gibi farklı t rdeki siber vakaları arařtırmaktan sorumludur (DOJ, 2011, s. ii).

2008 yılında kurulan *Ulusal Siber Soruřturma Ortak G rev G c  (National Cyber Investigative Joint Task Force - NCIJTF)*, kolluk kuvvetleri, istihbarat topluluęu ve Savunma Bakanlıęı i erisinden 30'dan fazla ortak kuruluřtan oluřmaktadır.  ok kurumlu siber g venlik merkezi olarak NCIJTF, kolluk kuvvetleri, istihbarat teřkilatları ve  zel sekt r kuruluřları arasında iřbirlięini ve bilgi paylařımını kolaylařtırır. ABD h k metinin istihbarat operasyonları ve soruřturmaları da dahil olmak  zere ulusal g venlik siber tehdit arařtırmalarını desteklemek, ilgili bilgileri koordine etmek ve karar vericiler i in istihbarat analizi saęlamakla g revlidir (FBI, tarih yok(b)). FBI, 18 istihbarat topluluęu ve kolluk kuvvetlerini i eren NCIJTF'nin lider kuruluřu ve operasyonel y neticisidir (DOJ, 2011, s. iii).

2.1.3. ABD Siber Diplomasisi

2.1.3.1. Japonya - ABD

Japonya ve ABD, Hint-Pasifik bölgesinde siber güvenliği artan önemi çerçevesinde işbirliğini geliştirmek ve siber güvenlik sorunlarını ele almak için güçlü bir siber diplomasi çerçevesi oluşturmuştur. Çin'in gelişmiş siber yeteneklerini ve siber araçlarını bölgesel siyasi ve ekonomik müdahalede için kullanması, Rusya ve İran'ın devlet destekli APT aktörlerinin bölgede katılımı, ABD'yi bölgede siber uzay konusunda işbirliği yapmaya teşvik etmiştir. Özellikle Biden yönetimi tarafından 11 Şubat 2022'de ana hatlarıyla çizilen Hint-Pasifik Stratejisi, bölgedeki stratejik ortaklıkları derinleştirmenin önemine vurgu yaparken, gelişen teknolojiler, internet ve siber uzayda ortak girişimlerin geliştirilmesinin de önemine vurgu yapılmıştır. Çin'in Hint-Pasifik bölgesinde yoğunlaşan üstünlük mücadelesinden duyduğu endişeyi ve genişleyen etkisinin yarattığı zorlukları kabul eden stratejide, daha geniş bölgesel güvenlik ve ekonomik girişimlerin bir parçası olarak siber güvenlik işbirliğinin önemine vurgu yapılmıştır (The White House, 2022a).

Hint-Pasifik bölgesinde artan rekabet ortamı neticesinde siber uzay, ABD ve Japonya ilişkilerinde önde gelen işbirliği alanlarından biri haline gelmiştir. Tokyo 11 ülke ile siber savunma konusunda ikili diyaloglar kurarak çeşitli ülkelerin savunma makamlarıyla BT forumlarına katılsa da, en uzun ve en yakın uluslararası siber güvenlik ortaklığı ABD ile gerçekleşmiştir (Dominguez, 2022).

19 Nisan 2019'da toplanan Japonya-ABD Güvenlik Danışma Komitesi (SSC) sonucunda iki hükümet, siber uzayda uluslararası hukukun geçerli olduğunu ve belirli durumlarda bir siber saldırının ABD-Japonya Güvenlik Anlaşması'nın V. maddesi uyarınca silahlı bir saldırı teşkil edebileceği konusunda anlaşmıştır (Ministry of Foreign Affairs of Japan, 2019). Japonya-ABD Güvenlik Danışma Komitesi'nin 7 Ocak 2022'de yaptığı toplantıda ise bilgi güvenliğinin daha da artırılması, siber uzayda işbirliğinin derinleştirilmesi ve ittifakın müdahale kabiliyetinin güçlendirilmesi konuları üzerinde durulmuştur. Ayrıca Japonya, siber alanda Japonya Öz Savunma Kuvvetleri'nin (JSDF) yeteneklerini istikrarlı bir şekilde geliştireceğini ve ABD ile JSDF arasındaki siber güvenlik işbirliğinin önemini vurgulamıştır (Ministry of Foreign Affairs of Japan , 2022).

2.1.3.2. Singapur - ABD

Singapur, Asya-Pasifik bölgesinde önemli bir ekonomik ve teknolojik merkez olarak kabul edilmektedir. Dolayısıyla bölgede siber güvenlik tehditlerinin artması ve güvenli bir dijital altyapının korunması, hem ABD'nin hem de Singapur'un ulusal çıkarlarına hizmet etmektedir. Teknoloji alanında güçlü olan iki ülke siber güvenlik teknolojilerinin geliştirilmesi, yeni tehditlere karşı ortaklaşa savunma mekanizmalarının oluşturulması, bilgi paylaşımı ve ortak tatbikatlar için ortak çalışmalar yürütmektedir.

20 Ağustos 2021'de ABD Başkan Yardımcısı Kamala Harris'in Asya ülkesine yaptığı ziyarette bir dizi Mutabakat Zaptı (Memorandum of Understanding-MOU) imzalanmıştır. Bunlardan biri 23 Ağustos 2021'de Singapur Siber Güvenlik Ajansı (CSA) ile CISA arasında, siber tehditler hakkında düzenli bilgi alışverişi, siber güvenlik olaylarına müdahale koordinasyonu, ortak siber güvenlik eğitimi ve tatbikatları gibi alanlarda geliştirmeye yönelik bir anlaşmayı içermektedir. Singapur Savunma Bakanlığı (MINDEF), Singapur Silahlı Kuvvetleri (SAF) ve ABD Savunma Bakanlığı arasında imzalanan ikinci muhtıra ise karşılıklı anlayış ve kapasite geliştirme konusunda işbirliği kurma çabalarını içermektedir (Mahmud, 2021).

Singapur Para Otoritesi (MAS) ve ABD Hazine Bakanlığı'nı içeren üçüncü muhtıra ise ikili kurumsal ortaklıkları güçlendirmeyi amaçlamaktadır. İki kurumun yaptığı açıklamaya göre her iki finans kuruluşunun 2018'den beri siber tehditlerle ilgili bilgi alışverişinde olduğu belirtilmiştir. Anlaşma, siber güvenlik düzenlemeleri, bilgi paylaşımı, tehdit istihbaratı, siber güvenlikte işbirliğini teşvik amaçlı çalışan eğitimi ve sınır ötesi siber güvenlik tatbikatları gibi yetkinlik geliştirme girişimleri dahil birçok çeşitli alanda işbirliğini kapsamaktadır (Yu, 2021).

2021'de siber güvenlik alanında işbirliğini artırmaya yönelik gerçekleştirilen üç anlaşmayı takiben 29 Mart 2022'de ABD ve Singapur'un siber güvenlik konusunda sorunları ortaklaşa ele almak ve kritik altyapının güvenliğini sağlamak amacıyla ABD-Singapur Siber Diyalogu (USSCD) kurulduğu duyurulmuştur (The White House, 2022b).

2.1.3.3. Hindistan - ABD

Hindistan ve ABD, siber güvenlik alanında işbirliği yapmasındaki en önemli neden ortak tehdit görünümüdür. Hem ABD hem de Hindistan, devlet destekli siber casusluk ve siber saldırılar dahil olmak üzere benzer siber güvenlik sorunları ve tehditleriyle karşı karşıyadır. Özellikle Çin ve diğer bazı ülkelerin devlet destekli siber casusluk faaliyetleri iki ülkenin de ulusal tehdit olarak gördüğü bir faktördür. Dolayısıyla siber güvenlik alanında işbirliğini güçlendirmek ve genel stratejik ilişkilerini derinleştirmek, Hint-Pasifik bölgesinde istikrar ve güvenliği teşvik etmenin bir yolu olarak görülmektedir.

11 Ocak 2017 tarihinde Yeni Delhi'de Hindistan Hükümeti Elektronik ve Bilgi Teknolojileri Bakanlığı bünyesindeki Hindistan Bilgisayar Acil Müdahale Ekibi (CERT-In) ve ABD Hükümeti İç Güvenlik Bakanlığı arasında siber güvenlikte işbirliği konusunda Mutabakat Zaptı imzalanmıştır. Daha öncesinde siber güvenlikten sorumlu devletlerin kendi kuruluşları arasında, daha yakın bir işbirliğini teşvik etmek için 19 Temmuz 2011'de bir Mutabakat Zaptı imzalanmıştır. 2011'den bu yana CERT-In ve US CERT arasında, bilgileri paylaşmak ve siber güvenlikle ilgili konuları tartışmak için düzenli görüşmeler gerçekleşmektedir (DQ India, 2017).

11 Nisan 2022'de ABD-Hindistan 2+2 Bakanlar Diyalogu'nda iki ülke siber uzayda ortaya çıkan tehditler hakkında bilgi paylaşımını ve işbirliğini derinleştirmek amacıyla Uzay Durumsal Farkındalık Düzenlemesini imzalamıştır. Ayrıca ortak siber eğitim ve tatbikatları genişleterek, Savunma Yapay Zeka Diyalogu başlatma kararı almıştır (DOD, 2022). Bu strateji her iki ülkenin siber güvenlik uzmanlarının, devlet kurumlarının ve özel sektör kuruluşlarının yeteneklerini geliştirmeye yardımcı olacak girişimlerdir.

2.1.3.4. Polonya - ABD

Güçlü dijital ekonomiye sahip olan ABD ve Polonya, ortak güvenlik endişeleri sebebiyle siber güvenlik alanına işbirliği yaparak siber tehditleri algılama, önleme ve bunlara yanıt verme konusundaki toplu yeteneklerini geliştirmeyi, güvenli dijital ticaret ve yatırımı sağlayarak ekonomik büyümeyi teşvik etmeyi ve kritik altyapılarda dayanıklılığı artırmayı amaçlamaktadır. Ayrıca siber güvenlik, NATO'nun toplu

savunmasının kritik bir yönüdür ve Polonya-ABD arasındaki işbirliği, ittifakın siber yeteneklerini ve dayanıklılığını güçlendirmeye yardımcı olmaktadır.

26 Haziran 2019'da ABD ve Polonyalı askeri yetkililer arasında Varşova'da bir Siber Uzay Savunma İşbirliği Anlaşması imzalanmıştır. Anlaşmanın hükümleri arasında ortak savunma yeteneklerinin güçlendirilmesi ve bilgi paylaşımı yer almaktadır. Bu çerçevede siber tehdit aktörlerinin saldırganlığını caydırmak amacıyla, ABD ve Polonya kuvvetlerinin koordineli olarak savunma amaçlı siber yeteneklerini ve operasyonlarını geliştirmek için birlikte çalışması vurgulanmıştır (U.S. Embassy and Consulate in Poland, 2019).

2.1.3.5. Suudi Arabistan - ABD

ABD Başkanı Joe Biden'ın 15-16 Temmuz 2022 tarihlerinde Suudi Arabistan Krallığı'na yaptığı ziyaret sırasında Suudi Ulusal Siber Güvenlik Kurumu (NCA), ABD İç Güvenlik Bakanlığı, Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) ile siber güvenlik konusunda işbirliği için Mutabakat Zaptı imzalanmıştır. NCA yaptığı açıklamada, Suudi Arabistan ve ABD'nin siber uzayda hayati çıkarlarını korumak için siber güvenlikte ikili işbirliğinin teşvikini hedeflediğini açıklamıştır (Saudi Press Agency [SPA], 2022).

2.1.3.6. AB - ABD

ABD ve AB arasında siber güvenlik ile ilgili girişimler ve işbirliği 2000'li yılların sonlarından bu yana görülmektedir. Bu dönemde, dijital teknolojilerin ve internetin kullanımının artmasıyla birlikte siber güvenlik önemi daha da artmış ve uluslararası düzeyde işbirliği gerekliliği ortaya çıkmıştır. Dolayısıyla siber güvenlik konusunda ortak çıkarlara sahip AB ve ABD, siber tehditlere zamanında müdahale edebilmek için bilgi ve istihbarat paylaşımını kolaylaştırmaya ve siber güvenlik standartlarının oluşturulmasına yönelik işbirliği yapmaktadır. Ayrıca, siber uzayda sorumlu devlet davranışını teşvik etmek, siber tehdit aktörlerinin sorumlu tutulması ve etkili bir şekilde yargılanması için hukuki yardım sağlamak ve bilgi paylaşımı gibi çabaları birleştirerek siber suçlarla mücadelede işbirliği yapmakta ve siber uzayda kurallara dayalı bir uluslararası düzen kurmayı hedeflemektedir.

AB'nin 2013 tarihli Siber Güvenlik Stratejisinde önceliklerinden biri uluslararası bir siber uzay politikası oluşturmak ve siber güvenlikle ilgili konularda uluslararası ortaklarla işbirliği yapmak olduğu belirtilmektedir. Bu belgede *"ikili düzeyde ABD ile işbirliği özellikle önemlidir"* vurgusuyla ABD açıkça bahsedilen tek ülkedir (European Commission, 2013).

Kasım 2010'da Lizbon'da yapılan AB-ABD Zirvesinde iki aktör arasında kurulan Siber Güvenlik ve Siber Suç Çalışma Grubu, siber güvenlik ve siber suç faaliyetlerini geliştirmek ve küresel bir siber güvenlik tehdidiyle mücadeleye katkıda bulunmak adına ABD-AB işbirliği için bir çerçeve görevi görmektedir. Çalışma grubu, siber olay yönetimi ve kritik altyapının siber güvenliği konusunda kamu-özel ortaklığı, siber güvenlik bilincini artırma ve siber suç konuları üzerine odaklanmaktadır. Bu bağlamda çalışma grubu kuruluşundan beri çeşitli siber tatbikatlar yürütmüş, ulusal ve bölgesel siber tatbikatlar hakkında bilgi alışverişinde bulunmuş ve ortaklaşa Ekim ayının "Ulusal Siber Farkındalık Ayı" ilan edilmesini sağlamıştır (The White House, 2014). Ayrıca Siber Güvenlik ve Siber Suç Çalışma Grubunun hedefleri arasında AB ve FBI'nın işbirliği yaparak IP adreslerinin yasa dışı amaçlarla kötüye kullanılmasının önlenmesi, Budapeşte Siber Suç Sözleşmesi'nin AB ve AB dışı devletler tarafından onaylanmasının teşvik edilmesi ve internet üzerinde çocuk cinsel istismarı ve tacizine karşı oluşturulan ittifak kapsamında çocukların çevrimiçi cinsel sömürüsüyle mücadeleyi güçlendirilmesi yer almaktadır (Anagnostakis, 2020).

2014 ABD-AB zirvesinde ise ABD-AB Siber Diyalogu başlatılmıştır. Diyalog çerçevesinde uluslararası siber uzay gelişmeleri, insan haklarının çevrimiçi ortamda desteklenmesi ve korunması, siber uzayda davranış normları, siber güvenlik alanında güven artırıcı önlemler ve mevcut uluslararası hukukun uygulanması, üçüncü ülkelerde siber güvenlik kapasitesi geliştirme konularına odaklanılmıştır (The White House, 2014). Aralık 2022'e kadar AB ve ABD arasında toplam sekiz Siber Diyalog düzenlenmiştir. 15-16 Aralık 2022'e sekizincisi düzenlenen Siber Diyalog'u, Rusya'nın Ukrayna'ya karşı yasadışı askeri saldırısı sonucunda kötüleşen siber tehdit ortamı karşısında, gelişmiş transatlantik işbirliği ve koordinasyon ihtiyacını sağlama ihtiyacı çerçevesinde gerçekleşmiştir. Ukrayna, Batı Balkanlar, Gürcistan ve Moldova'ya yönelik siber saldırılardan çıkarılan derslerin ele alındığı özel bir oturumun ardından AB ve ABD, üçüncü ülkelere yönelik kapasite geliştirme ve siber kriz yönetimi desteği konularında işbirliğini derinleştirme karar almıştır. Ayrıca çok taraflı forumlarda

işbirliği çerçevesinde AB ve ABD, BM'deki işbirliğinin ötesinde, AGİT, Uluslararası Telekomünikasyon Birliği (ITU), İnternet Yönetişimi Forumu (IGF), G20 ve benzer görüşteki kişiler dahil olmak üzere diğer uluslararası ve bölgesel örgütlerde yakın işbirliğine ilgi duyduklarını ifade etmiştir (European External Action Service [EEAS], 2022).

2.1.3.7. İsrail - ABD

İsrail ve ABD'nin Orta Doğu'da güçlü bir stratejik ortaklığı söz konusudur. ABD ve İsrail, ortak çıkarlar, teknolojik uzmanlık ve bölgesel güvenlik endişelerinin birleşimi nedeniyle siber güvenlik alanında işbirliği yapmaktadır. İşbirliğinin temelinde Orta Doğu'daki jeopolitik dinamikler önemli rol oynamaktadır. Bu temel, İran ve Rusya gibi ortak düşmanlardan gelen siber tehditlere karşı koyma konusundaki ortak çıkarlardan kaynaklanmaktadır. İran, ABD ve müttefik ağlarının güvenliğine yönelik bilinen bir tehdittir ve agresif siber operasyonlar yürütme konusunda uzmanlığa ve istekliliğe sahiptir. Rusya'nın da uluslararası topluluk için önemli bir zorluk olarak kabul edilen casusluk, dezenformasyon kampanyaları da dahil olmak üzere bölgedeki çeşitli ülkeleri hedef alan siber operasyonlarda yer aldığı bilinmektedir. Dolayısıyla ABD ve İsrail'in siber güvenlik konusunda işbirliği, İran ve Rusya'nın siber yeteneklerini daha iyi anlayabilme ve bölgedeki siber saldırılara karşı toplu dayanıklılık ve etkili savunma mekanizması geliştirme çerçevesinde şekillenmektedir.

1 Mart 2022'de Tel Aviv'de ABD ve İsrail arasında terörün finansmanıya mücadelede işbirliği, siber alanda araştırma ve geliştirme, ulaşım sektöründe siber güvenlik konusunda işbirliğini içeren bir Mutabakat Zaptı imzalanmıştır. Araştırma ve geliştirme konusunda, 1977'den beri İsrail ve ABD arasında bilimsel işbirliği için yürütülen ve ortak finanse edilen Çift Uluslu Endüstriyel Araştırma ve Geliştirme (Binational Industrial Research and Development - BIRD) programının genişletilmesi ve programa Siber Müdürlüğü eklenmesi planlanmıştır (Keller-Lynn, 2022).

23 Ağustos 2022'de İsrail ve ABD, siber finansal işbirliği için ilk anlaşmasını imzalamıştır. Bu anlaşma siber güvenlik bilgileri ve finans sektörüyle ilgili bilgilerin paylaşılmasını, finansal kurumlarının siber yeteneklerini güçlendirmek için personel

eğitimini ve finansal kurumların dayanıklılığının ölçülebilmesi için ortaklaşa sınır ötesi siber finansal tatbikatlar gerçekleştirmesini öngörmektedir (Bassist, 2022).

ABD Başkanı Joe Biden'ın imzaladığı 2022 mali yılı için Ulusal Savunma Yetkilendirme Yasası (NDAA) kapsamında belirlenen 777,7 milyar dolarlık savunma harcamasının 10,4 milyar doları siber uzay faaliyetlerine ayrılırken 6 milyon doları ABD-İsrail siber güvenlik işbirliği için yapılacak programa hibe edilmiştir. Plana göre hibe programı, İsrail ve ABD'deki özel şirketler, kar amacı gütmeyen kuruluşlar, akademik kurumlar ve devlet kurumları hibe almaya uygun oldukları sürece 5 yıl boyunca 6 milyon dolarlık fon alacaktır (Kogosowski, 2022).

2.2. Rusya Federasyonu'nun Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri

Rusya Federasyonu tarihsel olarak SSCB döneminden günümüze kadar gelen stratejik ve teknolojik aklın etkisiyle, siber kapasitesini hem savunma hem de saldırı yönünde genişletme stratejisi uygulamaktadır (Darıcı, 2017, s. 10). Bazı uzmanlar, Rusya'nın siber yeteneklerinin dünyanın en gelişmişleri arasında olduğunu ve bu alanda önemli kaynaklara ve uzmanlığa sahip olduğunu bilindiğini öne sürmektedir.

Rusya'nın siber yeteneklerinin kökenleri, ülkenin sinyal istihbaratı (SIGINT) ve kriptografiye büyük yatırımlar yaptığı SSCB dönemine kadar izlenebilir. Dolayısıyla Rus siber casusluğu ve bilgi savaşı, Sovyet yönetimi döneminden kalma bir stratejidir. Örneğin, SSCB döneminde, KGB'nin (Komited Gosudarstvennoy Bezopasnosti) dış operasyonlarının önemli bir bölümünün, Batı bloğundaki teknolojik gelişmeleri yakından takip ederek teknolojik casusluk yoluyla bu buluşları SSCB'ye aktardığı bilinmektedir (Darıcı, 2017, s. 10).

Rusya'nın siber stratejinin temeli 1980'lerde Sovyet ordusunda görev yapan ve dijitalleştirilmiş savaşta değişime dikkat çeken ilk kişilerden biri olan Mareşal Nikolai V. Ogarkov tarafından Askeri İşlerde Devrim (Revolution in Military - RMA) programı ile başladığı bilinmektedir. RMA'nın unsurları bilgi odaklı savaş kavramları ve savaş alanı üzerine bilgi hakimiyeti olarak özetlenmektedir (Heickerö, 2010, s. 14). Dolayısıyla bilgi teknolojilerinin 21. yüzyılın en çetin silahları olduğu ve etkilerinin kitle imha silahlarıyla kıyaslanabilir olduğu fark edilmiştir (FitzGerald,

1996). Rus istihbarat servisleri, SSCB'nin dağılmasından sonra siber yetenekleri geliştirmeye devam etmiş ve siber casusluk 1990'ların sonlarında Rus istihbarat teşkilatları için bir öncelik haline gelmiştir. Çoğu araştırmacıya göre Rusya'nın siber yeteneklere büyük yatırımlar yaptığı, ABD ve Çin gibi diğer gelişmiş siber güçlere rakip olduğu ve Rusya'nın artan siber operasyonları ve bilgi savaşı planları, büyüklüğü ve karmaşıklığı nedeniyle dünyanın her bölgesini etkileyen bir strateji olarak görülmektedir.

Ayrıca Rusya'nın strateji belgelerinde teknolojik bir anlam ifade eden siber uzay ve siber güvenlik kelimeleri yerine "*bilgi/enformasyon güvenliği*" ve "*bilgi/enformasyon alanı*" ifadelerini kullanmakta ve teknolojiyi birçok bileşenden sadece biri olarak algıladığını, en önemlisi olarak kabul etmediğini göstermektedir (Gady & Austin, 2010, s. 19). Dolayısıyla bilgi savaşının yalnızca teknolojik kullanımını değil, aynı zamanda sosyal ve politik faktörlerin manipülasyonunu da içeren çok yönlü bir kavram olduğu şeklindeki Rus görüşünü yansıtmaktadır. Rusya, bilgi kontrolünü siyasi hedeflere ulaşmak için kullanılabilecek önemli bir araç olarak görmekte ve siber operasyonları daha geniş bir bilgi savaşı stratejisinin sadece bir parçası olarak görmektedir.

2.2.1. Temel Belgeler ve Stratejiler

"Bilgi güvenliği" ve "bilgi savaşı" ifadelerinin kullanıldığı ilk belge olan 24 Ocak 2000 tarihli *RF Ulusal Güvenlik Konsepti (National Security Concept of RF)*, bilgi güvenliğini ulusal güvenliğin ayrılmaz bir parçası olarak kabul etmekle birlikte, bilgi alanında ulusal güvenliğine yönelik artan bir tehdidin varlığına, Rusya'nın iç ve dış bilgi pazarından çıkarılma arzusunun varlığına değinilmiştir. Bu doğrultuda, bilgi güvenliğinin öneminden ve bu alanda Rusya'nın çıkarlarına yönelik tehditlerin tespitinin yapılması, gerekli tedbirlerin alınarak eylemlerde bulunulmasından bahsedilmektedir. Bilgi güvenliğinin sağlanması için önemli görevler (I) bilgi alanında vatandaşların anayasal hak ve özgürlüklerinin korunması, (II) yerel bilgi altyapısının iyileştirilmesi, korunması ve Rusya'nın küresel bilgi alanına entegrasyonu, (III) bilgi alanındaki muhalefet tehdidine karşı durmak şeklinde sıralanmıştır. Tüm bu tehditlerin zamanında keşfedilmesi için istihbarat ve karşı istihbarat kaynaklarının kullanılması

önemli görülmüştür (Berlin Information Center for Transatlantic Security [BITS], 2000).

9 Ocak 2000 tarihli *RF Enformasyon Güvenliği Doktrini (Information Security Doctrine of the RF)*, ulusal güvenliğin büyük ölçüde bilgi güvenliğine bağlı olduğu vurgusuyla, Rusya'nın siber güç olma hedefini içeren ilk temel belgedir. Belgede Rusya'nın bilgi güvenliğine yönelik iki bölüme ayrılan iç ve dış tehdit kaynakları belirlenmiştir; Rusya'nın bilgi alanındaki çıkarlarına karşı siyasi, ekonomik, askeri istihbarat faaliyetleri, bazı ülkelerin siber uzayda hakimiyet kurma ve RF'nin bilgi alanındaki çıkarlarını ihlal etme çabaları, uluslararası terör örgütlerinin faaliyetleri, önde gelen dünya güçlerinin teknolojik üstünlüğündeki artışı dış tehditler olarak sıralanmıştır. Organize suçların toplum hayatı üzerinde daha fazla etki göstermesi, ulusal bilgi güvenliği alanında sağlam bir devlet politikasının yürütülmesinde kurumlar arasında yetersiz koordinasyonun olması, bilgi alanındaki ilişkileri düzenleyen yasal çerçevenin yetersiz kalması, bilgi güvenliği alanında tecrübeli personel sayısının yetersizliği, bilgi ve telekomünikasyon sistemlerinde ithal donanım/yazılımın kullanılması, sistemlerde donanım ve yazılımlardaki düzenlemelerin ihlal edilmesi başlıca iç tehditler olarak belirtilmiştir (ITU , 2008). Tüm bu tehdit kaynaklar neticesinde bilgi güvenliği konusunda alınacak önlemler belirlenerek hükümet politikasını şekillendirmiştir.

12 Mayıs 2009 yılında imzalanan 2020'ye *Doğru Rus Ulusal Güvenlik Stratejisi (Russia's National Security Strategy to 2020)*, bilgi teknolojisinin artan öneminin hem fırsatlar hem de zorluklar sunduğunu ve siber tehditlerin ulusal güvenlik için ciddi bir endişe haline geldiğini belirtmektedir. Rusya'nın gelecek on yıl için politika oluşturma sürecini şekillendiren belgede, yeni teknolojilerin kullanımı dahil, bilgi güvenliği alanında uluslararası işbirliğine ve güvenliğin sürdürülebilir kalkınma ile yakından ilişkili olduğu vurgulanmaktadır. Bununla birlikte, ulusal güvenliği sağlamak için modern bir orduya geçiş yapmak için silahlı kuvvetlerin organizasyonunu ve yapısını iyileştirme gerekliliğinden bahsedilmektedir (Sophia & Liaropoulos, 2010).

1 Ocak 2011'de RF Savunma Bakanlığı tarafından yayınlanan *Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler (Conceptual Views Regarding the Activities of the Armed Forces of the RF in the Information*

Space), ABD'nin stratejik belgelerinde bahsedilen "siber uzay" kavramının "bilgi alanı" olarak kullanıldığı bir diğer belgedir. Önceki belgelerden farklı olarak bilgi güvenliğinin temel alınarak hazırlandığı belgede, "bilgi savaşı" kavramı "bilgi sistemlerine, süreçlere ve kaynaklara, kritik ve diğer yapılara zarar vermek, politik, ekonomik ve sosyal sistemleri baltalamak, nüfusun kitlesel bir psikolojik manipülasyon amacıyla bilgi alanındaki iki veya daha fazla devlet arasındaki çatışma" olarak tanımlanmıştır. Bilgi güvenliğinin sağlanması amacıyla, Rusya Silahlı Kuvvetleri'nin bilgi güvenliği sisteminin geliştirilmesi; Kolektif Güvenlik Antlaşması Örgütü, Bağımsız Devletler Topluluğu ve Şanghay İşbirliği Örgütü üye ülkeleri ile birinci derecede işbirliğinin kurulması; BM şartı hükümlerine ve uluslararası hukukun normlarına uygun uluslararası bir siber uzay güvenliği anlaşmasının oluşumu için çaba gösterilmesinin gerekliliği vurgulanmıştır (Ministry of Foreign Affairs of the Russian Federation, tarih yok).

2013 tarihli *Gerasimov Doktrini*; Military-Industrial Kruer isimli dergide 27 Şubat 2013'te yayınlanan "The Value of Science in Prediction" isimli makale, RF Genel Kurmay Başkanı Valery Gerasimov tarafından yazılmıştır. Bilgi savaşıyla ilgili kilit noktalara değinilen ve literatürde Gerasimov Doktrini olarak geçen makale, Rusya'nın siber güvenlik konusunda önemli belgeleri arasında yer almaktadır. Resmi olmayan Gerasimov Doktrinine göre Gerasimov, SSCB tarafından geliştirilen savaş taktiklerini stratejik askeri düşünceyle birleştirerek yeni bir modern savaş teorisi ortaya koymuştur (McKew, 2017). Doktrinde "*Savaşın kuralları değişti. Siyasi ve stratejik hedeflere ulaşmak için askeri olmayan araçların rolü büyüdü ve çoğu durumda, etkinlikleri açısından silahların gücünü aşmıştır*" söylemiyle bilgi alanının, düşmanın savaşma potansiyelini azaltmak için geniş asimetrik olanaklar sunduğunu ve stratejik hedeflere ulaşmak için siber yetenekler de dahil olmak üzere mevcut tüm araçları kullanmanın önemini vurgulamıştır (Gerasimov, 2016, s. 24).

Gerasimov Doktrini ile oluşan ilkeler çerçevesinde Rusya, askeri nitelikte olmayan yöntemleri kullanarak, sıcak çatışma süreçlerini daha az can kaybı ve maliyetle yönetmeyi amaçlamıştır. Dolayısıyla siber operasyonlar, Gerasimov Doktrininde önemli bir saldırı aracı olarak rol oynamaktadır. 2014'teki Ukrayna müdahalesi, Gerasimov'un yaklaşımına uygun bir örnek olarak gösterilebilir (Darıcı & Özdal, 2017, s. 126).

12 Şubat 2013 tarihinde Rusya devlet başkanı Vladimir Putin'in onayı ile kabul edilen *RF Dış Politika Konsepti (Concept of the Foreign Policy of the RF)*, Rusya'nın küresel sorunları, bölgesel ve küresel öncelikleri, dış politikasının gelecek dönem hedefleri ve siber güvenlik konusunda bazı değerlendirmeleri içermektedir. Değerlendirmeler çerçevesinde bilgi alanındaki yeni teknolojilerin ulusal güvenlik için bir tehdit oluşturduğu, siber uzayda terör ve diğer suç tehditleriyle mücadele amacıyla bilgi güvenliğinin sağlanmasının, bilgi alanında devlet güvenliğine yönelik iç işlerine müdahale etmeyi amaçlayan ve uluslararası hukuka aykırı siyasi, ekonomik ve sosyal tehditleri önlemek için gerekli önlemlerin alınmasının gerekliliği vurgulanmıştır (Russiaeu.ru, 2008).

2013 Temmuz 2013 tarihli *2020'ye Kadar RF Devlet Politikasının Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri (Basic Principles for States Policy of the RF in the Field of International Information Security to 2020)*, uluslararası bilgi güvenliği alanındaki başlıca tehditleri, Rusya'nın uluslararası bilgi güvenliği alanındaki devlet politikasının amacını ve temel ilkelerini içermektedir. Rusya'nın siber güvenliğe yaklaşımı için geniş bir çerçeve sağlayan ve dijital alandaki stratejik çıkarlarını yansıtan belgede, Rusya'nın büyük dünya güçleri ile rekabet edebilecek bilgi ve iletişim teknolojileri kapasitesini geliştirebilmesi için gerekli şartların oluşturulması, bilgi güvenliği alanında kurumlar arasında işbirliğinin geliştirilmesi ve Rus girişimlerinin teşvik edilmesi temel ilkeler olarak belirtilmiştir. Ayrıca belgede ikili, çok taraflı, bölgesel ve küresel düzeyde uluslararası bilgi güvenliği sisteminin kurulması Rusya'nın devlet politikası önceliklerinden biri olarak kabul edilmiştir (National Security Archive, 2013).

2015 yılında yayınlanan *Rusya Federasyonu Ulusal Güvenlik Konsepti'nde (National Security Concept of the Russian Federation)*, Rusya'nın devlet ve kamu güvenliğine yönelik faşist, aşırılıkçı, terörist, ayrılıkçı ideolojileri yaymak, desteklemek, toplum barışını, siyasi ve sosyal istikrarı tehlikeye atma gibi yasadışı girişimlerin bilgi ve iletişim teknolojileriyle yaygınlaştığı belirtilmiştir. Ayrıca söz konusu tehditler sadece terörist, aşırılıkçı veya faşist grupların girişimleri değil, yabancı ulus devletlerin ve bireylerin istihbarat servislerinin faaliyetlerini de kapsamaktadır. Bu doğrultuda ulusal güvenlik için bilgi güvenliğine hayati önem atfedilen belgede, bilgi alanındaki tehditlerin belirlenmesi, analiz edilmesi ve karşı koyma sistemlerinin iyileştirilmesi devlet ve kamu güvenliğinin sağlanmasının bir

gerekliliği olarak kabul edilmiştir (Instituto Espanol de Estudios Estrategicos [ieee], 2015).

5 Aralık 2016 tarihli RF Bilgi Güvenliği Doktrini'nde (*Doctrine of Information Security of the RF*) bilgi alanında ulusal güvenliğin sağlanmasına ilişkin resmi görüşler yayınlanmıştır. Yabancı devletlerin, ülkenin bilgi altyapısını etkilemek adına bilgi teknolojisi kapasitesini geliştirmesi ve istihbarat faaliyetlerini artırması bilgi güvenliğini etkileyen en önemli olumsuz faktör olarak sıralanmıştır. Devlet ve kamu güvenliği için bilgi güvenliğini sağlamak, Rusya'nın ulusal egemenliğini, siyasi ve sosyal istikrarını, toprak bütünlüğünü, temel hak ve örgütleri korumakla eş görülmektedir. Rusya'nın kritik bilgi altyapısını barış zamanında, doğrudan bir saldırı tehdidi durumunda ve savaş zamanında sorunsuz bir şekilde işletilmesini sağlamak, bilgi teknolojileri sektörünü geliştirmek, üretim, araştırma, bilim ve teknoloji topluluğuna destek vermek stratejik hedefler arasında yer almaktadır (Security Council of Russia Federation [SCRF], 2016).

2017 yılında yayınlanan 2030 Rusya Federasyonu'nda Bilgi Toplumunun Gelişimi Stratejisi (*Strategy for the Development of the Information Society in the RF for 2017 - 2030*), Rusya'nın dijital egemenlik kavramını somutlaştıran ve ilk kez kendi topraklarında bilgi yayılımını kontrol etme ve dış etkilerden bağımsız olma isteklerini resmen açıklayan stratejik bir belgedir. Belge Rusya Federasyonu Cumhurbaşkanlığı Bilgi Teknolojisi Uygulaması ve E-Demokrasinin Geliştirilmesi Müdürlüğü tarafından hazırlanmıştır. Önceki strateji belgelerini belirli yerlerde tekrarlayan belgenin önemli bir kısmı dijital ekonomi konusuna ayrılmıştır. Siyasi boyutta ise devletin kendi topraklarında, internet üzerindeki denetiminin genişletilmesi ve kritik bilgi altyapısında kullanılan yabancı teknolojilerin yarattığı tehditler ele alınmıştır. Bu doğrultuda belgede sunulan çözümler ise dijital egemenlik kavramı çerçevesinde Rus bilgi ve teknolojilerini oluşturmak ve uluslararası düzeyde rekabet edilebilirlik sağlamak, yeni bir teknolojik temel oluşturmak, devletin dijital ekonomi alanında çıkarlarını korumaktır. Rusya'nın bu stratejisi, ülke içinde ve dışındaki yabancı kuruluşlara karşı bir bilgi savaşı yürüttüğü şeklinde yorumlanmaktadır (Centrum Analiz Propagandy i Dezinformacji [CAPD], 2017).

1 Ocak 2018 tarihinde yürürlüğe giren *Kritik Bilgi Altyapısının Güvenliğine İlişkin Federal Yasa (Federal Law on Security of Critical Information Infrastructure)*,

Rusya'nın kritik bilgi altyapısının güvenliğini sağlanması ve hükümete yönelik gerçekleştirilen siber saldırılar karşısında önlemler alınması konusunda çalışmaları düzenlemektedir. Yasallık, süreklilik ve bilgisayar saldırılarını önleme önceliği, kritik bilgi altyapısı güvenliğini sağlamanın ilkeleri olarak belirlenmiştir. Ayrıca yasaya göre kritik bilgi altyapısının güvenliğini sağlama alanındaki yasal düzenlemelerin iyileştirilmesine yönelik teklifler Rusya Federasyonu Başkanına sunulur ve başkanlık tarafından ağ olayları için ulusal bir koordinasyon merkezi oluşturularak ilgili yönetmeliği onaylamasıyla süreç tamamlanır (Kremlin.ru, 2017).

10 Ekim 2019 tarihli *2030'a Kadar Yapay Zeka Geliştirme Ulusal Stratejisi* (*National Strategy for Artificial Intelligence Development Until 2030*), yapay zekanın gelişiminin hızlandırılmasına ve yapay zekanın ekonominin çeşitli sektörlerine entegrasyonuna odaklanmaktadır. Bu alanda araştırma ve geliştirme harcamalarını artırmayı, eğitim programlarına yatırım yapmayı ve yapay zeka kümelerinin gelişimini teşvik etmeye yönelik girişimleri içermektedir. Belgede Rusya'nın yapay zeka teknolojilerini geliştirerek dünya liderleri grubuna girmesi, ülkenin teknolojik bağımsızlığı ve rekabet edebilirliği için bir ön koşul olduğu vurgulanmıştır. Bu hedef doğrultusunda Rusya başbakanı Vladimir Putin, bilim ve teknolojiyi teşvik etmek için devletlerle büyük şirketler arasında ortaklık kurulmasını önermiştir. Ortaklık alanları ise tıp, tarım, endüstri, genom teknoloji, taşınabilir enerji kaynakları, iletim ve depolama tekniklerini içermektedir (Nikolsky, 2019).

2015 yılında yayınlanan Ulusal Güvenlik Stratejisinin yerini alan 2 Temmuz 2021 tarihli *Ulusal Güvenlik Stratejisi*, Rusya'nın ulusal savunmasını, iç bütünlüğünü ve siyasi istikrarını güçlendirmeyi, ekonominin modernleşmesini ve endüstriyel yeteneklerin geliştirilmesini hedeflemektedir. Aynı zamanda Rusya'nın egemenliğini güçlendirmek için içeride ve dışarıda yeteneklerini geliştirmeyi amaçlayan temel bir belgedir (Güler & Shakirova, 2021).

2021 Ulusal Güvenlik Stratejisinde, bilgi güvenliği konusuna ilişkin belirlenen stratejilere, 2015'te olduğundan çok daha fazla öncelik verilmiş ve 2015 belgesinde yer almayan bilgi güvenliği konusuna yer verilmiştir. Belgenin "Bilgi Güvenliği" başlığı altında ayrılan geniş bölümünde; bilgi ve iletişim teknolojilerinin devletlerin iç işlerine müdahale ederek egemenliklerini ve toprak bütünlüklerini ihlal edecek şekilde genişlediği, Rus bilgi kaynaklarına yönelik siber saldırıların sayısının arttığı ve bu

saldırıların çoğunun yabancı devletlerin topraklarından geldiği vurgulanmıştır. Ayrıca Rusya'nın uluslararası bilgi alanındaki girişimlerinin diğer yabancı devletler tarafından engellendiği de belirtilmiştir (Paulo Filho, 2021).

Rusya, bilgi güvenliğini sağlamak amacıyla belirlediği devlet politikaları kapsamında şu hedeflere odaklanmaktadır; (I) Rusya'nın bilgi altyapısında kendi ülkesinde geliştirilen ve üretilen bilgi teknolojilerinin ve ekipmanlarının öncelikli kullanımının öncelikli hale getirilmesi amaçlanmaktadır. Böylece, yerli teknolojilerin güvenlik açısından daha kontrol edilebilir ve bağımsız olmasını sağlayarak bilgi altyapısının güvenliğini artırmayı hedeflemektedir. (II) Siber tehditlere karşı daha etkili savunma mekanizmalarının geliştirilmesi ve hızlı tepki verme kapasitesini artırılması için yapay zeka teknolojileri gibi ileri teknolojileri kullanarak bilgi güvenliği araçlarını geliştirmeyi hedeflemektedir. (III) Yabancı devletlerin teknik istihbarat faaliyetleriyle ulusal güvenliğe zarar vermesini engellemek çeşitli önlemler alınmasını hedeflemektedir (Paulo Filho, 2021).

2.2.2. Rusya Federasyonu'nun Siber Güvenlik Ulusal Organizasyon Yapısı

Bilgi savaşı ve bilgi operasyonları için yetenekler geliştiren, Rusya'nın saldırgan ve savunma amaçlı siber yeteneklerinden sorumlu ve operasyonlarını koordine eden temel kuruluşları FSB, SVR, FSO, Roskomnadzor ve GRU'dur. SSCB'nin dağılmasının ardından Rusya, bilgi güvenliği yeteneklerini geliştirmeye odaklanmış Federal Güvenlik Servisi (FSB) ve Savunma Bakanlığı da dahil olmak üzere çeşitli kurum ve kuruluşlar siber güvenlik çabalarına dahil olmuştur. FSB genel olarak Rusya'daki karşı istihbarat, iç güvenlik ve gözetlemeden sorumludur. SVR, dış istihbarat faaliyetlerini yürüten, insan zekasından sorumludur ve sınırlı siber yeteneklere sahiptir. En aktif birlik olan GRU, siber casusluk ve bilgi savaşını başarılı bir şekilde yürütmek için büyük miktarda kaynağa erişime sahiptir. Roskomnadzor ise ülkenin tüm bilgi, iletişim ve teknoloji ağlarını kontrol eden bir denetleme kurumudur.

2.2.2.1. Federal Güvenlik Servisi

Sovyetler Birliği zamanındaki KGB'nin (Sovyetler Birliği Devlet Güvenlik Komitesi) halefi olarak görülen iç istihbarat servisi Federal Güvenlik Servisi (Federal Security Service-FSB), Rusya'nın siber uzayda gerçekleştirdiği stratejik ve operasyonel faaliyetlerin temelinde yer almaktadır. Odak noktası devlet güvenliği olan FSB'nin iki ana işlevi; istihbarat toplamak ve bilgi güvenliğini sağlamaktır. Rusya'nın yerel bilgi alanının güvenliğini sağlarken, Roskomnadzor (İletişim, Bilgi Teknolojisi ve Kitle İletişim Federal Servisi) ve Minsifri (Dijital Kalkınma, İletişim ve Kitle Bakanlığı) gibi federal kurumlarla da işbirliği içinde çalışmaktadır (Hakala & Melnychuk, 2021, s. 17).

FSB'nin siber uzaydaki yetkileri geniş bir yelpazeye uzanmaktadır. Özellikle 1995 tarihli Operasyonel Arama ve El Koyma Yasası FSB'nin ulusal güvenlik için yetkilerini ve sorumluluklarını artırmıştır. Rus veri trafiğini denetlenmesi, telefon hatlarının dinlenmesi, e-postalara ulaşım, internet gözetimi gibi birçok yetkiler bunlardan birkaçı olarak sıralanabilir. Yasa, FSB'nin yurt içinde olduğu kadar yurt dışında da SVR ile işbirliği içinde istihbarat faaliyetlerini yürütmesini sağlamaktadır (Heickerö, 2010, s. 29).

Rus yasaları, FSB'ye telekomünikasyon verileri, e-posta, web sitesi ziyaretleri, kredi kartı dahil olmak üzere Rus ağlarında iletilen veya alınan tüm verileri toplamak, analiz etmek ve depolamak için Operasyonel Araştırma Faaliyetleri Sistemi'ni (System for Operative Investigative Activities-SORM) kullanma yetkisi vermektedir. 1990'lardan itibaren kullanılan SORM üç çeşit faaliyeti içermektedir. SORM-1 mobil ve sabit telefon aramalarındaki verileri toplamakta, SORM-2 internet ağları üzerindeki verileri toplamakta ve SORM-3 tüm ortamlardaki verileri toplayarak Wi-Fi ve sosyal ağlar gibi tüm ortamlardan bilgi ve istihbarat toplayarak saklamaktadır (Lewis, 2014).

FSB'nin bünyesinde faaliyet gösteren *FSB Bilgi Güvenliği Merkezi - (Information Security Center - TsIB)*, Kaspersky dahil olmak üzere Rus özel siber güvenlik şirketleri arasındaki bağlantıları kullanmaya odaklanmış bir kurumdur (Soldatov & Borogan, 2022). TsIB, Rusya'nın bilgi güvenliği alanında tehditleri tespit etmek, önlemek için çalışmakta ve bilgisayar ağlarının korunması, bilgisayar korsanlarının yakalanması ve internetin dikkatli bir şekilde izlenmesini de sağlamaktadır. İnternette aktif operasyonel çalışmalar yürüten TsIB, bunun için Rus

programcılar tarafından oluşturulan özel arama analitik sistemleri kullanmaktadır (Lenpravda, 2011).

Merkez 16(Centre 16), siber güvenlik arařtırmacıları tarafından "Dragonfly", "Energetic Bear" ve "Crouching Yeti" olarak adlandırılmaktadır (FBI, 2021a). Bu isimler genellikle siber güvenlik arařtırmacıları, medya ve uzmanlar tarafından isimlendirilmektedir. Ayrıca bazı arařtırmacılara göre 2010'da FSB ve SVR'nin elektronik operasyonlar için eğitilen uzmanlarının bir araya gelmesiyle oluşturulmuştur. Ancak FSB ve SVR ile bağlantıları hakkında doğrudan ve resmi bir bilgi bulunmamaktadır. Ana görevi, çevrimiçi alandan veri toplamak, yabancı ülkelerin (özellikle NATO üyelerinin) elektronik iletişimini izlemek, istihbarat toplamak ve yabancı bilgisayar sistemlerine elektronik siber saldırılar gerçekleřtirmektir. "Yabancı Kaynaklardan Elektronik Veri Toplama Dairesi" olarak da adlandırılan 16. Merkez, Ukrayna kuvvetleri tarafından ele geçirilen Rus birliklerine ait bazı belgelerde 'Özel Birim 71330' olarak da isimlendirilmektedir (The Geopost, 2022).

16. Merkezin 2010'dan beri siber operasyonlar gerçekleřtirdiđi, uzun yıllar boyunca Avrupa, Amerika ve Asya'da enerji, sađlık, finans, eğitim kurumlarını ve ulusal yönetimlerin sistemlerini hedeflediđi, 2014'te enerji sektörüne, 2020'de ise havacılık sektörüne karşı önemli siber saldırılar yürüttüğü gözlemlenmiştir. Birleşik Krallık, bu faaliyetlerin 16. Merkez tarafından gerçekleştirildiđini teyit etmiştir (GOV.UK, 2022).

FBI raporuna göre 26 Ağustos 2021'de 16. Merkez üyesi üç kiři, küresel enerji sektöründeki řirketlere yönelik bilgisayarlara izinsiz giriş, elektronik dolandırıcılık ve kimlik hırsızlığı suçlarına karıştıkları iddiası ile suçlanmıştır. Suçlular tarafından Amerikan enerji řirketleri dışında Arnavutluk, Avustralya, Belçika, Brezilya, Çin, Hırvatistan, Norveç, Hollanda, Finlandiya, Güney Kore, İngiltere, Danimarka, İrlanda, İtalya, Hollanda, Pakistan, Singapur dahil olmak üzere 135 ülkede yaklaşık 380'den fazla yabancı řirket hedef alınmıştır. Bu řirketler arasında ise küresel petrol ve doğal gaz řirketleri, nükleer santraller, yenilenebilir enerji řirketleri, kamu hizmetleri, ileri teknoloji firmaları gibi řirketler yer almıştır (FBI, 2021a).

2.2.2.2. Rus İstihbarat Servisi

FSB gibi Rusya Devlet Başkanı'na bağlı olarak görev yapan Rus İstihbarat Servisi (Foreign Intelligence Service - SVR), ülke dışındaki istihbarat faaliyetlerini yürütmek amacıyla KGB'nin devamı olarak kurulmuş dış istihbarat servisidir. SVR'nin yetkileri Dış İstihbarat Hakkında Federal Kanunun 6. maddesi ile tanımlanmıştır. Bu çerçevede SVR, yetkisi dahilinde Rusya'nın sınırları dışında bulunan Rus kurumlarında devlet sırlarını korumaktan, bu kurumların ve kurumda çalışanların korunmasına ilişkin prosedürlerin belirlenmesini sağlamaktan, bilgi ve iletişim sistemlerindeki bilgi hırsızlığını engellemek için sistemler kurmaktan sorumludur (Sluzhba Vneshney Razvedki [SVR], tarih yok).

SVR, Rusya'nın ulusal güvenliği ve çıkarları doğrultusunda yabancı ülkelere istihbarat toplama, analiz etme ve operasyonlar yürütme görevini üstlenmekte, hedef aldığı aktörlere yönelik askeri, siyasi, ekonomik, savunma, bilim ve teknoloji alanlarında istihbarat faaliyetleri yürütmekte ve karar alma süreçlerine katkıda bulunmaktadır. Aynı zamanda stratejik sinyal istihbaratı, askeri ve ticari uydu sistemleri, sabit ve kablosuz iletişim kapasitesine de sahiptir (Heickerö, 2010, s. 30). Siber güvenlik stratejisi kapsamında ise diğer devletlerin bilim ve teknoloji kapasitesini hedef alan siber casusluk operasyonları yürütmekten sorumludur.

SVR, GRU ile birlikte yabancı istihbarat sağlamaktan sorumludur. SVR'nin yurt dışında Belarus, Kazakistan, Tacikistan, Ermenistan, Kırgızistan, Suriye, Küba, Vietnam, Güney Osetya, Abhazya, Kırım ve Transdinyester bölgelerinde GRU ile birlikte ortak kullandığı elektronik ve sinyal istihbaratı toplama merkezleri de bulunmaktadır (Darıcı & Özdal, 2017, s. 128). Siber uzayı yalnızca casusluk için değil, aynı zamanda sabotaj ve bilgi operasyonları için kullanan GRU'nun aksine, SVR çoğunlukla geleneksel casusluk faaliyetlerine odaklanarak yabancı ülkelerdeki devletlere, kuruluşlara, diplomatlara ve politikacılara yönelik istihbarat operasyonları yürütür. SVR genellikle bilgi toplamak ve Kremlin'in politika yapıcılarının planları ve amaçlarını destekleyebilecek stratejik sırları keşfetmek için çalışır (Nakashimave & Timberg, 2020).

APT 29 (Cozy Bear); Batılı siber uzmanlar tarafından Rusya'nın istihbarat topluluğu içinde SVR ile ilişkilendirilen Rus siber casusluk grubu APT29, 2008'den beri faaliyet göstermektedir. Bu grup, bilgisayar ağlarına sızarak hedef ülkelerin

hükümetleri, kurumları ve özel sektör kuruluşlarına yönelik siber casusluk faaliyetleri gerçekleştirmektedir. Aralık 2020'de Teksas merkezli yazılım şirketi SolarWinds'e yönelik gerçekleştirilen tedarik zinciri saldırısı, SVR ile bağlantılı olduğu iddia edilen APT29 birimine atfedilmiştir. 15 Nisan 2021'de yayınlanan Ortak NSA-CISA-FBI Siber Güvenlik Danışmanlığı da SolarWinds tedarik zinciri saldırısını, Rusya'nın dış istihbarat servisi SVR'ye atfetmiş ve geniş kapsamlı siber casusluk kampanyasını yürütmekten sorumlu olduğunu resmi olarak açıklamıştır (CISA, 2021).

2.2.2.3. Rus Askeri İstihbarat Direktörlüğü

Rusya Savunma Bakanlığına bağlı olan Rus Askeri İstihbarat Direktörlüğü (Glavnoye Razvedyvatel'noye Upravleniye-GRU), Rusya'nın dış politikası ve güvenlik politikasında büyük rol oynayan istihbarat teşkilatlarından biridir. İnsan kaynaklı istihbarat, siber istihbarat ve sinyal istihbaratı toplamak GRU'nun görevleri arasındadır. Aynı zamanda savaş alanlarındaki keşiflerden ve Rus kuvvetlerinin operasyonlarından sorumlu askeri bir teşkilat olarak da faaliyet göstermektedir. GRU'nun istihbarat toplama faaliyetleri genellikle düşman ülkelerin askeri birimleri ve savunma sistemleriyle ilgilidir. Bu sebeple GRU hem istihbarat hem de askeri teşkilat yapısı nedeniyle ikili statüye sahiptir (Bowen, 2021). Dolayısıyla GRU, hem sivil istihbarat teşkilatlarıyla hem de Rus ordusuyla yakın bir işbirliği içinde çalışmaktadır.

GRU'nun komutası altında, iletişim ve elektronik istihbaratın gözetlenmesinden sorumlu özel hareket birimleri "*spetznaz*" bulunmaktadır (Heickerö, 2010, s. 31). GRU ve SVR arasındaki fark ise 2006'da bir SVR Korgenerali'nin yaptığı açıklamaya göre SVR siyasi istihbarat toplarken, GRU'nun askeri istihbarat toplamasıdır (Zavershinskiy, 2006).

Rusya'nın 2014'te başlayan Kırım ve Doğu Ukrayna'daki müdahalelerini takiben aynı yıl içerisinde Rusya Savunma Bakanlığı, potansiyel düşmanlarla siber çatışmaları yürütebilmek için bilgi-operasyon birliklerini oluşturmuştur. Yeni siber güçleri eğiten Savunma Bakanlığı merkezindeki bir eğitmene göre öğrenciler, siber saldırı algoritmaları geliştirerek gelecekteki çatışmalara hazırlanmakta ve eğitilen birçok Rus bilgisayar korsanı GRU'ya bağlı araştırma enstitülerinde çalışmaktadır (Astakhov, 2018).

Özellikle son yıllardaki raporlara ve hükümet iddianamelerine göre GRU, Rusya'nın en saldırgan ve kamu istihbarat operasyonlarından bazılarıyla ilişkilendirilmiştir. Örnek olarak GRU, Rusya Kırım'ı ve Doğu Ukrayna'yı işgalinde, Birleşik Krallık'taki eski Rus istihbarat subayı Sergei Skripal'e suikast girişiminde, 2017'de NotPetya kötü amaçlı yazılım saldırılarında, 2018 Olimpiyatlarına karşı gerçekleştirilen siber saldırılarda ve 2016 ABD Başkanlık seçimlerine müdahalede, Alman parlamentosuna (Bundestag) yönelik siber saldırılarda, 2015 Fransız televizyonu TV5Monde'ye yönelik siber saldırı girişiminde, istihbarat ve propaganda operasyonlarında kilit rol oynadığı bildirilmektedir (Bowen, 2021, s. 17).

GRU'nun bir alt birimi olan ve batılı siber araştırmacılar tarafından "APT 28" veya "Strontium veya Fancy Bear" olarak adlandırılan "85. Ana Özel Hizmet Merkezi - Askeri Birim 26165", dünya çapında siber casusluk faaliyetleri yürüten, birçok sektörün ve ulus devletin bilgisayar sistemlerini hedef alarak bilgi toplayan, gelişmiş Rus siber casusluk grubudur. Amerikan hükümeti tarafından hazırlanan iddianamede, Kremlin'in bilgisayar korsanlığı alanında görev yapan GRU birimi olarak tanımlanmaktadır (Poulsen, 2018). Grup, medya ve batı ülkeleri tarafından ABD ve Avrupa'daki sayısız siyasi, kamu ve özel sektör hedeflerine yönelik gerçekleştirilen siber operasyonlarla ilişkilendirilmiştir (Congressional Research Service [CRS], 2022). APT28 biriminin yürüttüğü bilgisayar korsanlığı kampanyası, hükümet ve askeri kurumları, savunma ve silah endüstrisini, siyasi partileri, lojistik şirketleri, enerji firmaları, üniversiteleri, hukuk firmaları ve medya şirketleri dahil olmak üzere çeşitli kuruluşları hedef almıştır (Greenberg, 2021). Örneğin Hillary Clinton başkanlık kampanyasını, Dünya Anti-Doping Ajansını (WADA), ABD nükleer tesisini, Kimyasal Silahların Yasaklanması Örgütü'nü (OPCW) hedef alan saldırılar ve sızıntı operasyonlarını gerçekleştirdiği ABD iddianamelerine konu olmuştur (Greenberg, 2020).

GRU'nun çevrimiçi dezenformasyon ve bilgi işlemleri gibi psikolojik siber operasyonlardan sorumlu olan "72. Özel Hizmet Merkezi - Birim 54777", Rusya'nın ana propaganda birimidir (Congressional Research Service [CRS], 2022). Örneğin 54777 Birimi tarafından yönetilen casuslar sahte hesaplar oluşturarak Rusça ve İngilizce olarak sosyal medya platformlarında, Rus ve Batı yanlısı Ukraynalılar arasındaki ayrımları körüklemeye çalışan girişimlerde bulunmuştur (Troianovski & Nakashima, 2018).

Siber güvenlik arařtırmacıları tarafından verilen diğerk isimleri "Telebots", "Voodoo Bear" ve "Iron Viking" olan "*Birim 74455 - Sandworm*", GRU'nun siber askeri birimi olduđu iddia edilmekte ve bilgi toplamaktan ziyade siber saldırı yeteneklerine sahip olduđu tahmin edilmektedir. Rusya'nın en zarar verici siber saldırılarıyla bağlantılı olduđu iddia edilen Birim 74455, Aralık 2015'te Ukrayna'nın elektrik řebekesine yönelik gerekleřen siber saldırıdan, 2017'de Petya kötü amaçlı yazılımını kullanarak Ukrayna'ya yönelik gerekleřtirdiđi siber saldırıdan, 2017'de Fransa cumhurbaşkanlığı seçimindeki eřitli müdahale operasyonlarından, 2018 Kış Olimpiyatları törenindeki siber saldırılardan ve 2016 ABD Başkanlık seçimleri sırasında alınan e-postaların ve belgelerin koordineli olarak serbest bırakılmasından sorumlu tutulmuřtur (Congressional Research Service [CRS], 2022).

2.2.2.4. Federal Koruma Servisi (The Federal Protective Service - FSO)

FSO, 2003 yılında lağvedilen Federal İletişim ve Enformasyon Ajansı'nın (Federal Agency of Government Communications and Information-FABSI) görevlerinin birçođunu devralmıřtır. Rusya'daki eřitli devlet tesislerine ve personeline fiziksel güvenlik ve koruma sađlamaktan birincil derece sorumlu olan FSO, korunan tesislerdeki bilgi sistemlerinin ve ađlarının güvenliđinin sađlanması da rol oynar. Siber güvenlik alanındaki temel görevleri; yöneticiler ve devlet birimleri arasındaki üst düzey iletişimin güvenli bir řekilde sürdürülebilmesini denetlemek, hükümeti yabancı istihbarat servislerinden korumak ve Kremlin'e gözetleme tesislerinden sinyal istihbaratı sađlamaktır. FSO aynı zamanda Rusya'ya ait nükleer füze sistemini yöneten "kara kutu"dan sorumludur. Ayrıca ülke genelinde kablolu telefon hatlarının izlenmesini, internet, uydu ve kablosuz iletişimin gözetimini de gerekleřtirmektedir (Heickerö, 2010). FSO'nun altında görevli, kripto istihbarat kuruluřu olan Özel İletişim ve Bilgi Servisi (Spetssvyaz), devlet kurumları için özel bilgi sistemlerinin güvenliđini sađlamaktan, yabancı iletişim ve sinyal istihbaratı analizinden sorumludur (Soldatov & Borogan, 2022).

2.2.2.5. Federal İletişim Servisi, Bilgi Teknolojileri ve Kitle İletişimi Denetleme Kurumu

İletişim Bakanlığı'nın altında görev alan Roskomnadzor, esas olarak BT alanında kontrol ve denetim uygulayan yetkili bir kurumdur. Ancak son yıllarda FSB'ye bu alanda giderek daha fazla yetki verilmiştir. Roskomnadzor, ülkenin elektronik medyasını, kitle iletişimini, televizyon ve radyo yayıncılığını, basılı yayın, internet siteleri, bilgi teknolojisini ve telekomünikasyon ağlarını düzenleme ve denetleme görevine sahiptir. İletişim ekipmanlarının doğru ve istikrarlı bir şekilde çalışmasını sağlarken, bu alanda devlet kontrol noktalarının belirlenmesinden de sorumludur (Afanasyeva, Bogatyrev, & Wilke, 2019, s. 5). Ayrıca çocukların gelişimlerine ve sağlıklarına yönelik zararlı bilgilerden uzak tutulması, içerik denetimi, yayın kurallarının uygulanması, kişisel verilerin işlenmesi ve korunması, medya şirketlerinin lisans alması, suç işlenmesi durumunda müdahale etmek gibi Roskomnadzor'un geniş alanda yetkileri de mevcuttur (Roskomnadzor, tarih yok).

2.2.3. Rusya Federasyonu'nun Siber Diplomasisi

2.2.3.1. Hindistan - Rusya

Hindistan ve Rusya uzun zamandır siber uzayı bir işbirliği alanı olarak görmektedir. 2016'da Hindistan'ın Goa eyaletinde gerçekleştirilen BRICS Zirvesi sırasında Hindistan ve Rusya siber uzayda işbirliği, siber terörle mücadele ve kritik altyapının korunması, savunma ve ulusal güvenlik işbirliği konularını kapsayan Bilgi Güvenliğine İlişkin Mutabakat Zaptı imzalamıştır. Bu anlaşma ile Hindistan, hem Rusya hem de ABD ile resmi siber güvenlik çerçevesini kuran tek ulus devlet olmuştur (Digital Watch, 2016). Anlaşma ile Siber Konularda Üst Düzey Diyalog kurulmuş ve siber suçlarla mücadelede işbirliğinin önü açılmıştır.

2018'de gerçekleşen bir toplantıda Hindistan Ulusal Güvenlik Danışmanı ve Rusya Güvenlik Konseyi'nin Bakan Yardımcısı, siber güvenlikte işbirliğinin genişletilmesi ve iki ülkenin ilgili kurumları ve yetkilileri arasında uzun vadeli işbirliği için bir mekanizma kurulmasını tartışmıştır. Ayrıca BM'nin siber uzayda sorumlu devlet davranışına ilişkin normları ve düzenlemeleri koordine etmedeki rolünün de önemi vurgulanmıştır (TASS, 2018).

Aralık 2021'de Hindistan ve Rusya, yazılım hizmetlerinin ve ürünlerinin ortak geliştirilmesi amacıyla hükümet ve özel sektör kuruluşları arasında işbirliği konusunda bir anlaşma yapmıştır. İki ülke siber uzayda bilgi güvenliği tehditlerine, kritik altyapı korumasına ve kanun yaptırımları konusunda etkinliği artırma taahhütlerini vurgulamıştır (Iasiello, 2022).

2.2.3.2. Endonezya - Rusya

Avustralya, Hindistan ve Singapur ile siber güvenlik konusunda görüşmeler gerçekleştiren Endonezya, 2017 yılında Rusya ile gerçekleştirdiği ikili görüşme neticesinde, Rusya'nın uluslararası bilgi güvenliği alanında devlet politikasının temel ilkelerine sahip olması nedeniyle işbirliği yapılmasının gerekliliği belirtmiştir (Radja, 2017). Bu doğrultuda Jakarta ve Moskova hükümeti başta terörizm olmak üzere, ulus ötesi suçlara karşı siber güvenlik konusunda işbirliği geliştirme ve dijital bilgilerin dağıtımını güvence altına alma konusunda işbirliğini yoğunlaştırma kararı almıştır. Siber güvenlik alanında oluşturulması amaçlanan işbirliği, hükümet kurumları dışında Rus ve Endonezyalı şirketler arasında da sağlanması amaçlanmaktadır.

2021 yılında Rusya ve Endonezya bilgi güvenliği alanında işbirliği konusunda resmi olarak hükümetler arası bir anlaşma imzalamıştır. Anlaşma çerçevesinde bilgi ve iletişim teknolojilerinin yasadışı kullanımı, kötü amaçlı yazılımlar ve siber saldırılar hakkında bilgi alışverişinde bulunma, bilgi güvenliği alanında ortak güven artırıcı önlemler geliştirme ve kişisel veriler dahil olmak üzere bilgi korumasını sağlamaya yönelik politikalar geliştirme konusunda anlaşmaya varılmıştır (Metzel, 2021).

2.2.3.3. Ermenistan - Rusya

Ermenistan ve Rusya arasında daha önceki yıllarda dijitalleşme, siber güvenlik, telekomünikasyon ve iletişim alanlarında işbirliği konusunun ele alındığı görüşmeler gerçekleşmiştir. Rusya ve Ermenistan arasında bilgi güvenliğine ilişkin ilk belge ise 19 Nisan 2022'de imzalanmıştır. Belgeye göre bilgi güvenliği alanındaki tehditlere karşı mücadelede, siber suçların tespit edilmesinde ve önlenmesi için veri alışverişinde bulunulması kararlaştırılmış; Bağımsız Devletler Topluluğu, Avrupa Güvenlik ve İşbirliği Teşkilatı, Kolektif Güvenlik Antlaşması Örgütü içerisinde de bilgi güvenliğini

sağlamaya yönelik çabaların genişletilmesinin önemi teyit edilmiştir (TASS, 2022) (Ghazanchyan, 2022).

2.2.3.4. ASEAN ve Rusya'nın Siber Güvenlik İşbirliği

2018 yılında ASEAN ve Rusya'nın yayınladığı Bilgi ve İletişim Teknolojilerinin Güvenliği ve Kullanımı Alanında İşbirliğine İlişkin Bildirisi, siber uzayda sorumlu devlet davranışı kurallarını detaylandırarak, siber güvenlik konusunda ASEAN-Rusya Diyalogu girişiminin değerlendirileceği belirtilmiştir. 24 Eylül 2021'de gerçekleştirilen ASEAN-Rusya Diyalogunun ilk toplantısında, siber güvenlik işbirliği konusu önemli bir konu olarak gündeme gelmiştir. Rusya Dışişleri Bakanlığının yaptığı açıklamaya göre Rusya ve ASEAN üye ülkeleri arasında, bilgi ve iletişim teknolojisi ile ilgili güvenlik konusunda kurumlar arası işbirliğinin uygulanması için bir taslak çalışma planı sunulmuş, bilgi ve iletişim teknolojilerinin suç amaçlı kullanımına karşı kapsamlı bir uluslararası sözleşme ve Uluslararası Telekomünikasyon Birliğinin hazırlanacağı bildirilmiştir (Sharifulin, 2021).

2.3. Çin Halk Cumhuriyeti'nin Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri

Dünyanın en hızlı büyüyen dijital ekonomilerinden biri olan ve en aktif siber savunma kabiliyetlerini geliştiren Çin Halk Cumhuriyeti, siber uzayda tehditler için geleneksel savunma yaklaşımlarından farklı olarak, saldırıya geçmek yerine düşmanın saldırısına direnerek ve onu tüketmeye çalışarak zafer elde etme hedefi çerçevesinde "*aktif savunma*" ilkesini uygulamaktadır. Çin anlayışında aktif savunma, Mao Zedong'un "*saldırıya uğramadıkça saldırmayacağız, ancak saldırıya uğrarsak mutlaka karşı saldırıya geçeceğiz*" fikrine dayanmaktadır (The National Institute for Defense Studies [NIDS], 2020, s. V). Dolayısıyla Mao Zedong'un ideolojik etkisi, ulusal güvenlik ve yerli inovasyona yaptığı vurgudan yararlanılarak Çin'in siber güvenlik stratejisine dahil edilmiştir.

Çin, 1990'ların sonlarından itibaren internet altyapısını hızla geliştirmeyi desteklerken, kendi toplumunun siber uzaya erişimi üzerinde kontrol mekanizmalarını da güçlendirmeye başlamıştır. Genel olarak belgelerinde de görüleceği üzere Çin

hükümeti, siber güvenlik alanında teknolojik gelişmeye, öz sermaye kullanılarak milli ve yerli yazılım-donanım üretimine ve bu üretim süreçlerinin devlet destekli kurum ve kuruluşların desteğiyle sürdürülmesine büyük önem vermiştir (Darıcı & Özdal, 2018, s. 14). Sonuç olarak Çin'de siber güvenliğin tarihi, ülkenin yenilik, bilgi kontrolü ve ulusal güvenlik üzerindeki stratejik odağını yansıtmaktadır. Çin'de internetin benimsenmesi, çevrimiçi etkinliği izlemek, yabancı web sitelerine erişimi kısıtlamak ve uygunsuz veya politik olarak yanlış olduğu düşünülen içerikleri filtrelemek için bir dizi yasal ve teknolojik araç kullanan hükümet tarafından sıkı bir şekilde denetlenmektedir.

2.3.1. Temel Belgeler ve Stratejiler

Çin'in, ekonomik ve sosyal kalkınma planlarını yayınladığı 2001 tarihli *Onuncu Beş Yıllık Planı 2001-2005 (China Tenth Five-Year 2000-2005)*, siber güvenlik yeteneklerine geliştirmeye odaklanmaktadır. Bilgi endüstrisinin ulusal kalkınma için stratejik bir alan olarak tanımlanan planda, yerel bilgi güvenliği altyapısının geliştirilmesine, ulusal bir olay müdahale ağının kurulmasına, siber güvenlik eğitim programının başlatılmasına bilgi teknolojisi üretiminin yaygınlaştırılmasına, bağımsız üretme yeteneğinin geliştirilmesine, hem devlet destekli hem de özel bilgi ve teknoloji alanına büyük ölçekli yerel yatırımlar başlatmaya öncelik vermiştir. Bilgi teknolojisi gibi yeni ve yüksek teknoloji endüstrilerinin yerli gelişiminin teşvik edilmesinin, bu teknolojileri güçlendirmek için yüksek hızlı, geniş bant bilgi ağları, entegre devreleri gibi önemli yüksek teknoloji projelerine destek verilmesinin gerekliliği vurgulanmıştır (The National People's Congress PRC, 2010).

2003 yılında yayınlanan *Belge 27(Document 27)*, afet kurtarma, olay yönetimi ve e-devlet alanlarında güvenlik planları dahil olmak üzere siber güvenlik konusunda önemli politikaları ve ulusal stratejileri belirleyen bir belgedir. Aktif savunma stratejisi fikriyle oluşturulan belge, kritik altyapının korunmasını, bilgi teknolojileri alanında yönetim organlarının işbirliğinin sağlanmasını, yerel teknolojilerin geliştirilmesini desteklemeyi ve bu alana finansman sağlanmasını amaçlamıştır (Raud, 2016, s. 11).

2006 yılında Çin'in 15 Yıllık Bilim ve Teknoloji Planı olarak da bilinen *2006 - 2020 Ulusal Programı (The National Programme for the Development of Science and Technology in the Medium and Long Term 2006-2020)*, özellikle askeri bir amaç

taşımamaktadır. Enerji, su, çevre, tarım, imalat sanayi, ulaşım sektörü, sağlık sektörü, kent gelişimi, kamu güvenliği ve milli savunma konularının ele alındığı belgede, bilgi güvenliğinin önemine ve bilişim sektörünün geliştirilmesi konusundaki planlara önemli bir yer verilmiştir. Teknoloji alanında yerli kaynakların geliştirilmesi, bilgi teknolojisi ürünlerinde kullanım kolaylığının ve maliyet etkinliğinin sağlanması, yeni teknolojilerin ve yerel işletmelerin desteklenmesi, sektördeki rekabet gücünü artırmak için bilgi teknolojisi ürünlerinde yeniliklerin hızlandırılması, yerli tasarım ve üretim kapasitesinin geliştirilmesi, geleneksel endüstrilerin dönüşümünün ve teknolojik yükselişinin teşvik edilmesi sektörlerdeki gelişim yollarının temeli olarak belirlenmiştir. Güvenilir ağlar oluşturma konusunda ise ağ bilgi güvenliği teknolojileri ve ürünlerinin geliştirilmesinin ve bilgi güvenliği için teknik destek sistemlerinin kurulmasının gerekliliği vurgulanmıştır (The State Council PRC, 2005). Dolayısıyla Çin'in 15 Yıllık Bilim ve Teknoloji Planı, bilgi teknolojisi sektöründe gelişimini hızlandıran, yerli yenilikçi kapasite ve yabancı teknolojiye bağımlılığı azaltan ve Çin'in rekabetçi bir yapıya sahip olması için teknoloji odaklı çeşitli planlar sunan bir belge niteliği taşımaktadır (Sergey & Breidne, 2007).

2012'de Danıştay Enformasyon Dairesi (SCIO) tarafından yayınlanan *Yeni Politika Görüşü* (New Policy Opinion - NPO), hedeflenen stratejilerin gerçekleşemediğini göstererek, Çin'in bilgi güvenliği modelinin zayıflıklarına değinmiş ve bilgi teknolojileri alanındaki hedeflenen stratejileri tekrarlamıştır. Özellikle Yeni Politika Görüşü, dijital altyapıda Çin ile gelişmiş ülkeler arasındaki eşitsizliğe, hükümet ve endüstri kuruluşları arasındaki verimsiz bilgi alışverişine, temel teknolojiler üzerinde diğer devletlerin sürekli olarak kontrol payının olmasına, siber uzayda yetersiz stratejik planlamaya ve ağ savunma yeteneklerinin zayıflığına dikkat çekmiştir (Segal, 2012). Bu bağlamda Yeni Politika Görüşü, öncelikle Çin ekonomisine büyük zararlar verebilecek endüstrilerin bilgi ağlarına odaklanarak tüm kritik altyapı sistemlerinin güvence altına alınmasını; nükleer tesisler, havacılık, petrol, gaz, boru hatları, enerji, ulaşım ve kentsel sistemler için endüstriyel kontrol sistemlerinin güçlendirilmesini; Anonymous ve Flame gibi bilgisayar korsanları tarafından genellikle hedef alınan hükümet ve diğer gizli bilgi güvenliği sistemlerinin güçlendirilmesini; Çin vatandaşlarının hassas verilerinin korunmasını önermiştir (Raud, 2016, s. 14).

26 Mayıs 2015 tarihli *Savunma Beyaz Kitabı/Askeri Strateji (China's Military Strategy/Defense White Paper)*, Çin Milli Savunma Bakanlığı tarafından, Çin'in siber yeteneklerini daha da geliştirme politikasıyla oluşturulmuş ilk halka açık ilan edilen ulusal belgedir. Belgeye göre bilgi toplumunun hızlı gelişimi ve savaşın evrimi karşısında ulus devletlerin ulusal güvenlik stratejilerini ve savunma politikalarını aktif olarak düzenlemeleri, askeri kuvvet yapısının yenilenme sürecinin hızlanması Çin'in askeri güvenliğine yeni zorluklar getirmiştir. Dolayısıyla bu yeni koşullar karşısında yeni planlar oluşturulmasının gerekliliği vurgulanmıştır. Siber uzay, askeri güvenlik konusunda gittikçe önemli hale geldiği için ulusal ağ ve bilgi güvenliğinin sağlanması, tüm askeri unsurların ağ teknolojisi ile uyumlu hale getirilmesi, siber savunmanın geliştirilmesi ve siber uzayda uluslararası işbirliğine katılım ile siber saldırıların önüne geçileceği bildirilmiştir (The State Council PRC, 2015).

Büyük fırsatların ve ciddi zorlukların ifade edildiği 27 Aralık 2016 tarihli *Ulusal Siber Uzay Güvenlik Stratejisinde (National Cyberspace Security Strategy)*, siber uzaydan kaynaklanan tehlikeleri bertaraf etmek için barış, güvenlik, şeffaflık ve açıklık, uluslararası işbirliği ve hukuksal düzen ilkeleri çerçevesinde siber operasyonların etkin bir şekilde önleneceği konusunda temel stratejik görevler yer almaktadır. (I) Çin'in siber uzaydaki egemenliğini sürdürmek, bilgi altyapısının güvenliğini korumak için ekonomik, idari, bilimsel, teknolojik, hukuki, diplomatik ve askeri tedbirler dahil her türlü tedbirin alınması, (II) internetin isyan, ayrılıkçı hareketler ve rejimin devrilmesini teşvik edici ve ulusal güvenliğe zarar verici şekilde kullanılması karşısında önlemler alınması, (III) kritik bilgi altyapısının ve önemli verilerin saldırılardan korunması için bilgi altyapısı koruma sisteminin kurulması, uygulanması, caydırıcılığın geliştirilmesi, önleme, erken uyarı ve müdahale sistemlerinin geliştirilmesi, tedarik zinciri güvenlik yönetiminin güçlendirilmesi, devlet kurumlarında kullanılan bilgi teknolojisi ürünlerinin denetimlerinin sağlanması, (IV) Çin'in sosyalist görüşlerini, kültürünü çevrimiçi yayma projesi ve yapıtlarının dijitalleştirilmesinin sağlanması, (V) çevrimiçi terörle mücadele, casusluk ve hırsızlıkla mücadele yeteneklerinin geliştirilmesi ve bu faaliyetlere karşı saldırıların gerçekleştirilmesi, (VI) internet ağının yasal, açık ve şeffaf bir şekilde yönetilmesi, siber güvenlik yasa ve düzenleme sistemlerinin idari denetiminin sağlanması, (VII) kimlik doğrulama, çok seviyeli koruma, risk değerlendirmesi ve sızıntı tespiti, siber güvenlik denetimi, erken uyarı sistemi, acil müdahale mekanizmalarının

iyileştirilmesi, (VIII) siber uzayda uluslararası işbirliğinin güçlendirilmesi Çin'in siber güvenliğini korumak için belirlenen stratejik görevlerdir (Creemers, 2016).

Çin Dışişleri Bakanlığı ve Çin Siber Uzay İdaresi tarafından 1 Mart 2017 tarihinde yayınlanan *Uluslararası Siber Uzayda İşbirliği Stratejisi'nde (International Strategy of Cooperation on Cyberspace)*, Çin'in siber uzayda stratejik hedefleri, eylem planları ve dış ilişkilerinde temel ilkeleri kapsamlı bir şekilde sunulmuştur. Siber güvenlik tehditlerinin diyalog yoluyla ele alınması; devletlerin, uluslararası şirketlerin, sivil toplum kuruluşlarının ve bireylerin işbirliğinin yoğunlaştırılması ve çok taraflı anlaşmalara katılım sağlanması; denetim mekanizmasının belirlenmesinde BM çerçevesinde evrensel kabul edilen normların kabulünün desteklenmesi; güçlü bir dijital ekonominin sağlanabilmesi için siber güvenlik kapasitenin geliştirilmesi; internette kültür çeşitliliğini teşvik edici girişimlerin sağlanması; Kuşak ve Yol Girişimi kapsamında ülkelerle işbirliği yapılması stratejik hedefler arasında yer almaktadır (Shaohui, 2017).

Çin'in siber güvenliğini yöneten ilk temel internet yasası olan, siber uzay egemenliğini en yüksek önceliği olarak kabul eden ve 1 Haziran 2017 tarihinde yürürlüğe giren *Siber Güvenlik Yasası (Cybersecurity Law)*, ülkenin siber ağlarını düzenleyen ve veri koruma, ağ güvenliği ve siber güvenlik gözetimi ile ilgili hükümler içeren kapsamlı bir yasadır. Bu doğrultuda kişisel verilerin, kritik bilgi altyapısının, ağ güvenliğinin korunması, topluma güvenilir ağ hizmetlerinin yayılması, devlete ait olanlar dahil ve diğer tüm verilerin Çin'de depolanması, Çinli yetkililerin bir şirketin şebeke operasyonlarında yerinde kontroller yapması, verilerin işlenmesine yönelik güvenlik önlemlerinin alınması gibi bir dizi girişim ile siber uzay yeteneklerini güçlendirmeyi amaçlamaktadır. Hükümet, siber uzay egemenliğine verdiği önceliğin yanında dijital ekonominin gelişimi için uluslararası siber işbirliğini de aktif olarak desteklemektedir. Sonuç olarak siber güvenlik konusunda mevcut yasa hem güvenlik hem de kalkınma çıkarlarını kapsayan çok boyutlu bir bakış açısını yansıtmaktadır (Qi, Shao, & Zheng, 2018, s. 3). Yasa siber güvenliğin korunmasına ilişkin ulusal politikayı, yaptırım mercilerini, mevzuatın temel ilkelerini belirlerken temel işlevi, belirli siber güvenlik sorunlarını çözmek değil, Çin'in siber güvenlik hukuk sistemini oluşturmaktır (Qi, Shao, & Zheng, 2018, s. 4).

Yasa çerçevesinde, Çin'de faaliyet gösteren yabancı şirketler arasında tartışmalı olan "güvenli ve kontrol" edilebilir olmalarını sağlamak için bir sertifika sürecinden geçmelerini zorunlu hale getirilmiştir. Özellikle önemli ağ ekipmanları ve yazılımların devlet sertifikaları alması gerekmektedir. Ancak bu durum Çin'deki yabancı şirketler için bir tehdit barındırmaktadır. Çünkü Çin'de hükümet, ekonomik planlamalarda kritik rol oynamakta ve hükümet müdahalesi, batılı ülkelerde olduğundan çok daha yaygındır. Dolayısıyla siber güvenlik kapsamında yabancı şirketlerin kritik bilgileri, Çinli firmalara fayda sağlayabilecek şekilde ifşa edilme riski taşımaktadır. Bu durumda yasaya yönelik, Çinli olmayan firmaların Çin'in pazarına erişimini engellemek için ürünlere özel standartlar ve düzenlemeler koyarak Çinli firmaları kayırdığı eleştirileri yapılmıştır (Haour, 2016).

1 Eylül 2021 tarihinde yürürlüğe giren *Veri Güvenliği Yasası (Data Security Law of the People's Republic of China)*, ülke içinde verilerin işlenmesini düzenleyen ve veri güvenliğini destekleyen, kişi ve kuruluşların hukuka uygun çıkarlarını korumak ve devletin güvenliğini korumak amacıyla çıkartılmıştır kapsamlı bir yasadır. Yasa, Çin'de toplanan ve depolanan verilerin ekonomik ve sosyal kalkınmadaki önemine, ulusal güvenlik üzerindeki etkisine ve kamu çıkarlarına göre sınıflandırılmasına ve sınıflandırma düzeyine bağlı olarak saklanması ve aktarılmasını düzenleyen bir sistem sunmaktadır. Ayrıca yasaya göre Çin'de veri işleyen kurum ve kuruluşlar, verilerin hassasiyet düzeyine bakılmaksızın Çin'de depolanan herhangi bir verinin yetkili makamların onayı olmadan, yabancı adli bir makama veya kolluk kuvvetlerine sağlaması da yasaklanmıştır (The National People's Congress PRC, 2021).

14 Kasım 2021'de Çin Siber Uzay İdaresi tarafından yayınlanan *Ağ Veri Güvenliği Yönetimine İlişkin Taslak Yönetmelik (Network Data Security Management Regulation)*, Siber Güvenlik Yasası, Kişisel Bilgileri Koruma Yasası ve Veri Güvenliği Yasası olmak üzere mevcut üç yasanın bölümlerinin uygulanmasına ilişkin özel gereksinimleri belirtmektedir (Cyberspace Administration of China [CAC], 2021). Çin hükümeti topraklarında hem ulusal hem de uluslararası veri işleme faaliyetlerinde bulunan kuruluşlar ve şirketler için veri güvenliğini koruma sistemlerini kurma yükümlülükleri detaylandırılmıştır. Veri işleyiciler, verileri sızıntı, hırsızlık, hasar, kayıp ve yasa dışı kullanıma karşı korumak, veri güvenliği olaylarına müdahale etmek ve suç teşkil eden faaliyetleri önlemek için yedekleme, şifreleme, erişim kontrolü gibi gerekli önlemleri almak zorundadırlar. Bu amaçla yönetmelik içerisinde yeni

hükümler ve yasal gereklilikler yer almıştır (Cyberspace Administration of China [CAC], 2021).

Çin'in yeni siber güvenlik önlemleri incelemesi ülkenin siber güvenlik gözetimini güçlendirmek amacıyla 31 aralık 2021'de yayınlanmış, *Siber Güvenlik İncelemesi İçin Yeni Tedbirler (China Issued New Measures for Cybersecurity Review)* ismiyle yayınlanan yeni önlemler 2022'nin başlarında değiştirilip revize edilmiş ve 15 Şubat 2022'de yürürlüğe girmiştir. Çin Siber Uzay İdaresi (CAC) ve diğer on iki kurumun katılımıyla oluşturulmuş yeni tedbirler, siber güvenlik incelemesinin yasal dayanağını, uygulama kapsamını, sorumlu devlet organlarını ve prosedürleri açıklamaktadır. Revizyonlar veri işleme faaliyetleriyle ilgili risklere ve deniz aşırı ülkelerde listelenen Çinli kuruluşlardan kaynaklanan risklere odaklanmıştır. Yeni tedbirler kapsamında, bir milyondan fazla kullanıcının kişisel bilgilerine erişim sağlayabilen ağ platformu şirketlerinin, bilgileri yurt dışında listelemeden önce siber güvenlik incelemesi için başvurmaları gerekmektedir (Zhang, 2022). Eleştirmenler, Çin hükümetinin Çin'de faaliyet gösteren yabancı şirketler üzerinde çok fazla kontrol sağladıklarını öne sürerek tartışmalara yol açmıştır. Ancak destekçiler, veri güvenliğini artırmak ve hassas bilgileri korumak için gerekliliği ve meşruluğunu savunmaktadır.

Kasım 2022'de Çin Devlet Konseyi Bilgi Ofisi tarafından siber uzayda ortak geleceğe sahip bir topluluk oluşturma önerisini sunan ve *Siber Uzayda Ortak Geleceği Olan Bir Toplumu Birlikte İnşa Etmek (Jointly Build a Community with a Shared Future in Cyberspace)* ismiyle yayınlanan Beyaz Kitap, ayrıca Çin'in internet gelişimi ve yönetişimi uygulamalarının başarılarını detaylandırmakta ve siber uzayda uluslararası işbirliğini vurgulamaktadır. Beyaz Kitap, bazı devletlerin siber uzayda hegemonya kurmak ve diğer devletlerin iç işlerine müdahale etmek amacıyla internet ve bilgi teknolojilerini kullanarak geniş çapta siber hırsızlık ve gözetleme faaliyetleri yürüttüğü konusunda uyarıda bulunmuştur (China's State Council Information Office, 2022).

Çin'in internet ve teknoloji alanındaki gelişimine dair sunulan bilgiler Beyaz Kitapta ayrıca öne çıkarılan bir konudur. Bu doğrultuda, Çin'in 2021 yılına kadar dijital ekonomisinin değeri 6,3 trilyon dolara ulaştığı, GSYİH'sının %39,8'ini oluşturduğunu, Haziran 2022 itibarıyla ülkede 1,05 milyar internet kullanıcısına ev sahipliği yapmanın yanı sıra dünyanın en büyük 5G ağına ev sahipliği yaptığını, 1,85

milyon 5G baz istasyonu, 455 milyon 5G cep telefonu abonesiyle 5G standartlarında dünya liderlerinden biri haline geldiğini belirtmiştir. Ayrıca Beyaz Kitaba göre Çin, tarımsal üretim dahil çeşitli ekonomik ve sosyal sektörlerde 5G, Nesnelerin İnterneti (IoT), yapay zeka (AI) gibi yeni teknolojileri ve uygulamalarını güçlendirmekte ve internet erişiminin tüm yoksul bölgelere kadar genişletmektedir.

Beyaz Kitapta, Çin'in Kuşak ve Yol Girişimi (Belt and Road Initiative) çerçevesindeki girişimlerine de yer verilmiştir. Çin, bulut bilişim ve yapay zeka teknolojilerinin geliştirilmesi ve uygulanması için yeni girişimler gerçekleştirmekle birlikte, 2020'de Afrika, Orta Doğu, Güneydoğu Asya'daki ülkelerde, Kuşak ve Yol Girişimi'ne katılan ülkelere bulut hizmetleri için destek sağlamaya başlamıştır. Ayrıca Kuşak ve Yol Girişimi'ne katılan ülkeler arasındaki bağlantı için ulusal otoyollar, demiryolları, köprüler, iletişim kabloları ve ağların inşasına yardımda bulunmuştur. Dijital İpek Yolu'nun inşasını desteklemek ve yeni IPv6+ uygulama alanları bulmak için kurumsal iletişim teknolojisi, bilgi teknolojisi, bulut bilişim ve büyük veri teknolojilerinin derinlemesine entegrasyonu ve dönüşümü için küresel bir IPv6+ ağ tabanı oluşturmuştur.

Siber uzayda ortak geleceğe sahip bir topluluk oluşturma girişi konusundaki önerisinde, uluslararası işbirliğine vurgu yapılmaktadır. Siber uzay yönetişimi ve işbirliği konusunda da BM'nin ana kanal rolü oynamasının gerekliliği ve siber uzayda uluslararası kuralların ortaklaşa diyalog mekanizması ile geliştirilmesi önceki belgelerinde olduğu gibi tekrar belirtilmiştir. Ayrıca BM Şartında yer alan egemen eşitlik ilkesinin, siber uzayda uluslararası ilişkileri yöneten temel bir norm olduğu, siber egemenliğe saygı gösterilmesi ve hiçbir devletin siber hegemonya peşinde koşmaması vurgulanmıştır. Ancak küresel fayda sağlamak ve kalkınma topluluğu oluşturmak için Çin, yayınlanan Beyaz Kitap'ta yoksul bölgeler dahil tüm dünyada internet erişiminin genişletilmesi, uygun fiyatlı cihazlar ve hizmetler sağlayan teknoloji sektörünün oluşturulması, fakir ülkelere bazılarıyla ortak olma girişimlerinin altını çizmesi, kendisini siber uzayda lider konumda gördüğünü göstermektedir.

Siber Uzay İdaresinin Uluslararası İşbirliği Bürosu genel müdürü Qi Xiaoxia belgenin tanıtım toplantısında, Beyaz Kitabın ABD ve ortaklarının yayınladığı "İnternetin Geleceği için Bildirge"den temelden farklı olduğunu, ABD'nin siber uzayda

tek taraflı tanımlanmış ilkelerin öne sürülerek uluslararası kuralları ihlal ettiği, bölünme ve çatışma yarattığını ifade etmiştir (Global Times, 2022).

2.3.2. Çin Halk Cumhuriyeti'nin Siber Güvenlik Ulusal Organizasyon Yapısı

Çin'de bilgi teknolojisine ulusal düzeyde odaklanma 1986 yılında Devlet Ekonomik Bilgi Yönetimi Lider Küçük Grubunun kurulmasıyla başlamış, 1999 ve 2001 yıllarında Devlet Bilişim Lider Grubunun (State Informatisation Leading Group-SILG) kurulmasıyla devam etmiştir. 2003 yılında Devlet Ağı ve Bilgi Güvenliği Koordinasyonu Küçük Grubu (State Network and Information Security Coordination Small Group-SNISCSG), SILG altında bir alt grup olarak kurulmuştur. Bu üç grubun temel hedefleri, yerli bilgi teknolojilerini geliştirmek ve bilgi teknolojilerini bir ulusal güvenlik temeline yerleştirmektir (Raud, 2016, s. 11).

2014 yılında Xi Jinping'in başkanlık ettiği İnternet Güvenliği ve Bilgilendirme Lider Grubu (Central Leading Group for Internet Security and Informatisation-CLSGISI) kurulmuştur. Çin'de yeni bir kurumun önceden var olan diğer kurumların görevlerini devralması yaygın olduğundan, CLSGISI bünyesinde SILG ve SNISCSG kurumlarının üyeleri birleştirilmiştir. Görevleri ise siber güvenlik ve bilişimin ana konularını koordine etmesi, siber güvenlik stratejilerini, planlamalarını formüle etmesi ve uygulaması, devlet kurumları arasında internet güvenliğini sağlaması olarak belirlenmiştir (Xinhuanet, 2014).

2.3.2.1. ÇHC Sanayi ve Bilgi Teknolojileri Bakanlığı

ABD İç Güvenlik Bakanlığı'na benzer sorumluluklar taşıyan Sanayi ve Bilgi Teknolojileri Bakanlığı (The Ministry and Information Technology-MIIT), 2008 yılında bilgi teknolojisi gelişimini merkezileştirme girişimi amacıyla ve Çin'in telekomünikasyon, yazılım sektörleri dahil olmak üzere çok çeşitli teknoloji alanlarını ve kurumlarını denetlemek kurulmuştur. MIIT, ülkenin posta hizmeti, internet, kablolu yayın ve iletişim endüstrilerinin geliştirilmesinden, bilgi güvenliğinin korunmasından, yeni teknolojik ve endüstriyel ürünlerin üretilmesi, geliştirilmesi, düzenlenmesi ve yatırımların onaylanmasından sorumlu bir departmandır (The US-

China Business Council, tarih yok). MIIT'nin genel sorumlulukları ağ güvenliğini sağlayarak, potansiyel siber riskleri ve güvenlik açıklarını tespit etmek, düzenli olarak ağ güvenliği için denetimler gerçekleştirmek, siber saldırılara karşı koyma yeteneklerini geliştirmek, acil durum tatbikatlarını organize etmek, cep telefonu virüsleri için önlemlerin geliştirilmesini incelemek, toplumun ağ güvenliği farkındalığını artırmak için eğitimler sağlamak, ITU, APEC, SCO, ASEAN+3 tarafından düzenlenen ilgili tartışmalara katılarak uluslararası işbirliğini desteklemektir (Jingguang, 2011, s. 8-10)

2.3.2.2. Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi/Koordinasyon

Merkezi

2001 yılında kurulan Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi/Koordinasyon Merkezi (National Computer Network Emergency Response Technical Team/Coordination Centre - CNCERT/CC), Çin'de 31 ilde ve belediyede faaliyet gösteren, Sanayi ve Bilgi Teknolojileri Bakanlığı'na bağlı ve kar amacı gütmeyen hükümet dışı bir siber güvenlik teknik merkezidir. 7/24 ulusal acil durum müdahale hattı işleterek ülkenin siber güvenlik politikasını iyileştirmeye ve kritik bilgi altyapısının güvenliğini korumaya çalışmakta, teknik destek ve rehberlik sağlamaktadır. Çin'in ağlarının ve internet altyapısının güvenliğini sağlamak, siber güvenlik olaylarını önlemek için ağ operatörleri, alan adı kayıt kuruluşları, siber güvenlik sağlayıcıları, akademi, sivil toplum, araştırma enstitüleri ve diğer acil müdahale ekipleri ile birlikte çalışmakta ve koordinasyon sağlamaktadır. Ayrıca hem yerel hem de uluslararası ortaklarla bilgi paylaşarak, yardım hattı, e-posta, web siteleri aracılığıyla yurt içi ve yurt dışındaki kullanıcılardan olay raporları alarak tehditleri keşfetmektedir. 2021 yılı itibarıyla 81 ülkede 274 ekiple "CNCERT/CC Uluslararası İşbirliği Ortaklığı" kurmuş; APEC, ITU, SCO, ASEAN, BRICS, diğer uluslararası ve bölgesel kuruluşların faaliyetlerinde aktif olarak yer almıştır (CNCERT/CC, tarih yok).

2.3.2.3. Ulusal Savunma İçin Bilim, Teknoloji ve Sanayi Devlet İdaresi

1998 yılında kurulmuş Ulusal Savunma İçin Bilim, Teknoloji ve Sanayi Devlet İdaresi (State Administration for Science, Technology and Industry for National

Defence -SASTIND), Çin'de ulusal savunma ve askeriye ile ilgili endüstrilere teknolojik destek sağlamaktan sorumlu bir devlet kurumudur. Çin Ulusal Uzay İdaresi, Çin Ulusal Nükleer Kurumu, Çin Atom Enerjisi Kurumu dahil bir dizi kurumu denetler. Başlıca sorumlulukları, nükleer silah, havacılık teknolojisi, silahlanma, deniz taşıtları ve elektronik endüstrilerinin denetimini içermektedir. Ulusal savunma için bilim, teknoloji ve endüstrinin idari ve düzenleyici kurumu olarak, askeri kuvvetler ve ulusal ekonomi ile ilgili kuruluşların ihtiyaçlarına hizmet etmektedir (The State Council PRC, 2014).

2.3.2.4. Kamu Güvenliği Bakanlığı

MIIT teknik yönelimli faaliyetlerde bulunurken Çin'in ulusal polis teşkilatı Kamu Güvenliği Bakanlığı (Ministry of Public Security - MPS), siber suçlarla mücadeleyle odaklanmaktadır. Hükümet tarafından kullanılan ticari ürünlerin denetlenmesinden, yerel istihbaratın yürütülmesinden ve Çin'in Büyük Güvenlik Duvarı'nı işletmesinden sorumludur (Feakin, 2013). Çin Komünist Partisi'nin internet üzerindeki kontrolünün gücü, tehlikeli bulduğu bilgilerin yayılmasını önleme girişimine dayanmaktadır.

Büyük Güvenlik Duvarı (Great Firewall), Çin'de 2008'den beri uygulanan oldukça tartışmalı bir bilgi güvenliği projesidir. Bu proje çerçevesinde Çin hükümeti tarafından uygunsuz ve hassas kabul edilen internet sitelerine, uygulamalara ve içeriğe erişimi düzenlemek için katı güvenlik politikaları uygulanmakta, internet trafiğini kontrol etmek için farklı türde sansür, sitelere erişim engellemesi, sınır ötesi internet trafiğini yavaşlatma ve içerik filtreleme gerçekleştirilmektedir. Çin'in Büyük Güvenlik Duvarı, bugüne kadar birçok yöntemle sürekli olarak gelişmiş; Facebook, Twitter, Wikipedia, Google, Youtube gibi popüler web sitelerine erişimler engellenmiştir. Uygulama, ülkenin internet kullanıcılarının çevrimiçi özgürlükleri üzerinde ciddi bir etki yaratarak Çin'i dünyanın en sıkı şekilde düzenlenen internet rejimlerinden biri haline getirmiştir (Chandel, Jingji, Yunnan, Jingyao, & Zhipeng, 2019). Bu yaygın sansür, Büyük Güvenlik Duvarı'ndan kaçmak için VPN'ler gibi hileli atlatma teknikleri kullanma konusunda ustalaşmıştır. Ancak hükümet, internet üzerinde çok fazla kontrol sahibi olmasını sağlayan yeni teknolojiler geliştirerek 2015'te vatandaşların Büyük

Güvenlik Duvarı'nı atlatmak için kullandığı VPN'lerin çoğunu engellemeye başlamıştır (Economy, 2018).

2018 yılında MPS, ülke genelindeki kamu güvenlik departmanlarıyla birlikte, yaygın bilgisayar korsanı saldırıları, internet işletmelerinin karşılaştıkları güvenlik sorunları, ticaret amacıyla vatandaşların kişisel bilgilerinin çalınması gibi çeşitli siber sorunları ele alan "*Temiz Siber Alan*" uygulamasını başlatmıştır. Bu uygulama ile Çin, hem işletmelerin birincil güvenlik sorumluluğunu sıkı bir şekilde uygulamasını teşvik etmiş hem de yasa dışı suç faaliyetlerini önemli ölçüde azaltmıştır. Sonuç olarak 57.000'den fazla siber suç vakası çözülmüş; 83.000'den fazla siber tehdit aktörü tutuklanmış; 34.000'den fazla internet işletmesi idari cezalara çarptırılmış; 35.000'den fazla kötü amaçlı programlar içeren uygulamalar kanunen kaldırılmış; 20.000'den fazla yasa dışı web sitesi kapatılmıştır. Ayrıca silahların, patlayıcıların, uyuşturucuların, vatandaşların kişisel bilgilerinin çevrimiçi satışına ilişkin önemli yasa dışı bilgilerin miktarı bir önceki yıla göre yaklaşık %30 azalma göstermiştir (Chinese Academy of Cyberspace Studies, 2021, s. 142).

2.3.2.5. ÇHC Devlet Güvenlik Bakanlığı

Çin Devlet Başkanlığı Konseyine bağlı olan Devlet Güvenlik Bakanlığı (Ministry of State Security - MSS), hükümet adına diğer devletlere karşı dış istihbarat, karşı istihbarat ve siyasi güvenlik faaliyetlerini yürütmekle görevlidir. (Yetgin, 2021, s. 33). Çin'in siber uzaydaki güvenlik ortamını şekillendiren önemli bir organizasyon olan MSS, siber casusluk faaliyetleri de yürütmektedir (Yetgin, 2021, s. 43).

MSS tarafından örgütlenen Çinli siber korsanlar, sahte profiller aracılığıyla, kişilerin iş ve kişisel bilgilerinin yer aldığı LinkedIn sosyal medya platformunda -kurumsal ticari sırlar, fikri mülkiyet ve diğer araştırmalar dahil olmak üzere, istedikleri bilgilere erişimi olan kişilerle iletişime geçmeye çalışarak casusluk faaliyetleri yürütmüştür. Çinli siber korsanlar, aralarında hükümet çalışanları, bilim insanları ve şirket yöneticilerinin bulunduğu 4.000 Fransız ile iletişim kurmak için sosyal medya platformlarını -özellikle LinkedIn'i- kullandığı anlaşılmıştır (Wong, 2019). 2015 yılında İngiliz karşı istihbarat kuruluşu MI-5'in çalışanları LinkedIn kullanımına karşı uyarıldığı görülmüş. 2018 yılında ise ABD savunma müteahhitlerinin ve ABD

istihbaratının, LinkedIn aracılığıyla MSS tarafından hedef alındığı anlaşılmıştır (Yetgin, 2021, s. 45).

2020 yılında MSS faaliyetleri ile ilişkili olarak bilgisayar korsanları, ABD merkezli Covid-19 aşısı araştırma geliştiricisi olan biyoteknoloji şirketi Moderna'yı veri çalmak amacıyla hedef aldığı açıklanmıştır. ABD Adalet Bakanlığı ise bu konuda Çinli iki vatandaş hakkında iddianame yayınlayarak, Moderna'ya yönelik keşif saldırısı düzenlediğini belirtmiştir. İddianameye göre 2009 yılına kadar uzanan bir süreçte Çinli bilgisayar korsanları savunma, enerji, ilaç, tıbbi cihaz, yazılım geliştirici sektörlerindeki şirketlere yönelik birçok siber saldırı gerçekleştirmiştir. Hedefler arasında ABD dışında, Avustralya, Güney Kore, Belçika, Almanya, Japonya, Hollanda, İspanya, Birleşik Krallık da bulunmaktadır (DOJ, 2020a).

2.3.2.6. Halk Kurtuluş Ordusu Genelkurmay Başkanlığı

Çin Genelkurmay Başkanlığı bünyesinde faaliyet gösteren Halk Kurtuluş Ordusu Genelkurmay Başkanlığı (People's Liberation Army General Staff Department - PLA GSD), siber savaş yürütmekten ve Çin'in siber uzaydaki çıkarlarını savunmaktan sorumludur. Ayrıca siber operasyonlar ve bilgi güvenliği ile ilgili çeşitli departmanları ve kuruluşları denetlemektedir. Denetimi altındaki, Genel Kurmay Başkanlığı Üçüncü Departmanı (3PLA) sinyal istihbaratından (SIGINT), Genel Kurmay Bakanlığı Dördüncü Müdürlüğü (4PLA) elektronik istihbarattan (ELINT), Stratejik Destek Gücü (SSF) aktif savunma konseptinin merkezinde yer almakta ve Çin'in siber uzay alanlarındaki askeri yeteneklerini entegre etmekten sorumludur.

2.3.2.6.a. Genel Kurmay Başkanlığı Üçüncü Departmanı

Sinyal istihbaratından sorumlu Genel Kurmay Başkanlığı Üçüncü Departmanı (The Third Department - 3PLA), hem yerel hem de uluslararası çeşitli iletişim ağlarından sinyallerinin toplanmasını ve analizini sağlamaktadır. Tüm hava, kara, deniz kuvvetlerinde, yurtdışındaki büyükelçiliklerde, diğer tesislerdeki iletişim trafiğini izlemek için geniş bir altyapıyı denetlemekte, Çin genelinde kapsamlı bir sinyal toplama sistemini sürdürmekte, yabancı orduların telekomünikasyonlarını izlemekte ve toplanan askeri bilgilere dayanarak istihbarat üretmekle görevlidir (Krekel, 2009, s. 30) (Pike, 2000). Haberlerde sık sık yer almasına rağmen 3PLA,

MSS dahil olmak üzere diğer yerli istihbarat birimleriyle olan etkileşimleri hakkında gizemliliği koruduğu için yerel kurumlar arasındaki koordinasyonu ve bilgi paylaşımının ne derecede olduğu sorusunu açık bırakmaktadır (Raud, 2016, s. 22). Ayrıca 3PLA, Ulusal Bilgi Güvenliği Teknolojisi Araştırma Merkezi, Bilgi Güvenliği Araştırma Enstitüsü, PLA İletişim Güvenliği Araştırma Enstitüsü gibi ağ savunması ile ilgili çeşitli kurumları yönetmektedir (Stokes, Lin, & Hsiao, 2011, s. 5).

2.3.2.6.b. Genel Kurmay Başkanlığı Dördüncü Departmanı

Üçüncü Departman daha çok ağ savunmasından sorumluyken HKO'nun ağ saldırısı görevi Genel Kurmay Başkanlığı Dördüncü Departmanı'nda (The Fourth Department-4PLA) yer almaktadır. Dolayısıyla elektronik istihbarattan PLA4, geleneksel olarak ulusal düzeyde elektronik savaş veya bilgisayar ağı saldırısından sorumludur. Radar sistemleri, elektronik harp teçhizatı ve diğer elektronik sinyallerin toplanması ve analizi konusunda uzmanlaşmış olan departman, yabancı askeri yetenekler ve faaliyetler hakkında istihbarat da toplamaktadır (Costello, 2016).

2.3.2.6.c. Stratejik Destek Gücü

2015 yılında HKO'nun örgütsel yapılanmasında bir dizi reform hareketleri başlamıştır. Reform hareketleri sonucunda en önemli değişikliklerden biri ise Stratejik Destek Gücü'nün (Strategic Support Force-SFF) oluşturulması olmuştur. Araştırmacılara göre SFF'nin kurulması hem HKO için kritik bir dönüm noktası olarak değerlendirilmekte hem de teşkilatlanma yapısı ve misyonu hakkında sınırlı şeffaflığa sahip olduğu belirtilmektedir. SFF, saldırı ve savunmaya odaklı bilgisayar korsanlarından oluşan "siber birlikler"; keşif ve navigasyon uygulamalarına odaklanan "uzay birlikleri"; düşman radarını ve iletişimini karıştırarak bozmaktan sorumlu "elektronik savaş gücünden" oluşmaktadır (Costello, 2016a). Dolayısıyla HKO, Çin'in ulusal güvenlik çıkarlarını korumak için saldırı ve savunma önlemlerinin kullanılmasını vurgulayan aktif savunma kavramında önemli bir rol oynayan SFF aracılığıyla, uzayla ilgili varlıkların üzerinde kontrolünü sağlamıştır.

SFF uzayın, siber uzayın ve elektronik alanların askeri kullanımını sağlamak için "*stratejik bilgi desteği ve stratejik bilgi operasyonları*" yürütmekten sorumludur.

Stratejik bilgi destek rolü, teknik istihbarat toplama, uzay ve nükleer alanlarda savunmayı desteklemeyi içermektedir. Bilgi operasyonları rolü ise düşmanın operasyonel sistemlerini çalışamaz hale getirmek ve düşmanın savaş komuta sistemlerini sabote etmek için uzay, siber uzay ve elektronik savaşın koordineli bir şekilde kullanılmasını içermektedir (Costello & McReynolds, 2018).

2.3.2.7. Çin Siber Uzay İdaresi

Çin Halk Cumhuriyeti Devlet Konseyi'ne bağlı olarak faaliyet gösteren ve 2013 yılında kurulan, gözetim ve kontrol kurumu Çin Siber Uzay İdaresi(Cyberspace Administration of China - CAC), siber uzay güvenliğinden ve internet içerik düzenlemesinden sorumludur. Siber Uzay İdaresinin başlıca işlevleri; web siteleri, sosyal medya platformları ve diğer internet hizmetleri dahil olmak üzere çevrimiçi içerik etkinliklerini denetlemek ve düzenlemek, çevrimiçi yayınlanacak haberlerle ilgili idari onay sağlamaktır (Thomson Reuters, tarih yok). Uluslararası siber bağlantılı faaliyetlerde Çin'i temsil ettiği için çevrimiçi faaliyetlerin etkilendiği tüm devlet ve özel sektör üzerinde denetleyici ve düzenleyici bir yetkiye sahip olmanın da ötesinde, Çin'deki verilerle ilgili önemli yasal çerçeveleri hazırlamaktan sorumlu ve yargı yetkisine de sahiptir (Horsley, 2022).

CAC'ye bağlı olan Siber Güvenlik İnceleme Ofisi (Cybersecurit Review Office-CRO), siber güvenlik inceleme sistemlerini ve standartlarını belirlemek ve siber güvenlik faaliyetlerini incelemelerini organize etme sorumluluğuna sahiptir (CAC, 2021a).

Çin'in siber uzay konusunda düzenleyici ve denetleyici birçok kurumu gibi CAC'nin düzenleyici yaklaşımı, çevrimiçi içerik üzerindeki katı denetimi, ifade özgürlüğü ile mahremiyet üzerindeki etkisi nedeniyle eleştirilmektedir. Bununla birlikte kurumlar, Çin hükümetinin sosyal istikrarı, ulusal güvenliği sağlama ve siber uzayda vatandaşlarının çıkarlarını koruma konusundaki bakış açısını ve stratejisini yansıtmaktadır.

2.3.3. Çin Halk Cumhuriyeti'nin Siber Diplomasisi

2.3.3.1. ABD - Çin

2000'li yılların başından günümüze kadar, siber casusluk faaliyetleri ABD-Çin arasındaki ilişkileri giderek daha fazla gergin hale getirmiştir. Özellikle şirket ve hükümet ağlarına yönelik izinsiz girişler ve ticari sırların siber hırsızlığı gibi konularda iki ülke karşılıklı olarak birbirine suçlamalarda bulunmuştur. Ayrıca 2013 yılında yaşanan Edward Snowden'ın Çin dahil olmak üzere çeşitli ülkeleri, işletmeleri ve bireyleri hedef alan siber casusluk faaliyetleri de dahil olmak üzere ABD hükümeti tarafından yürütülen kapsamlı gözetim programlarını ortaya çıkaran NSA belgelerini ifşa etmesi ve 2009 yılından beri ABD'nin Hong Kong ve Çin'e karşı kötü amaçlı siber faaliyetler yürüttüğü iddiası da ABD-Çin siber güvenlik ilişkilerini daha da olumsuz etkilemiştir (Murray, 2013). Siber uzayın gelişimi boyunca yaşanan Snowden olayı, yıkıcı bir güvensizliğe neden olmuştur. Bu olaydan sonra ulus devletler kendi siber güvenliklerinin kırılganlığını fark etmeye ve siber kapasitelerini geliştirerek stratejik çıkarlarını korumaya daha fazla önem vermeye başlamıştır.

Snowden sızıntılarını takiben, 19 Mayıs 2014'te ABD Adalet Bakanlığı, beş Çin destekli askeri bilgisayar korsanını, ABD nükleer enerji, çelik ve alüminyum endüstrisinde toplam altı Amerikan kuruluşuna yönelik ekonomik amaçlı siber casusluk faaliyetleri yürütmekle suçlamıştır (Rollins, 2015). Bu olayların ardından 2015'te ABD Başkanı Obama ve Çin Devlet Başkanı Xi Jinping arasında yapılan ABD-Çin Siber Güvenlik Anlaşması'nın yapıldığı görüşmede ekonomik amaçlı siber casusluk asıl gündem konusu olmuştur. Anlaşma çerçevesinde iki hükümette şirketlere veya ticari sektörler için rekabet avantajı sağlamak amacıyla ticari sırları ve fikri mülkiyetin siber saldırı eylemlerinde bulunmayacağı veya desteklemeyeceği konusunda işbirliğinin sağlanmasını amaçlamıştır (The White House, 2015a). Anlaşma ekonomik siber casusluğun azaltılması yönünde temel olarak görünse de siber saldırıların karmaşık doğası hem atıf sorununa sebep olmakta hem de boşluklar oluşturmaktadır. Çünkü her iki hükümet de anlaşma çerçevesinde ekonomik amaçlı siber casusluğu desteklemeyeceğini belirtmiş olsa da, olası siber faaliyetlerin hükümet tarafından desteklenmediğini iddia etmeleri için siber uzayda bir açık her zaman mümkündür.

Obama döneminde ABD ve Çin arasındaki siber gerilimi azaltmak ve karşılıklı anlayış geliştirmek için anlaşma yapılmış olsa da, 2017 yılında Donald Trump yönetimi göreve geldiğinde siber işbirliği konusunda daha sert tutumlar izlemiştir. Trump, Çin'i siber saldırılarda rol almakla ve veri hırsızlığı gerçekleştirmekle suçlayarak, Çin'e karşı daha sert önlemler almıştır. Trump'tan sonra yönetime gelen Joe Biden ise Çin ile siber işbirliği konusunda daha dikkatli ve eleştirel bir yaklaşım sergilemeyi, Çin'in siber saldırılar ve siber casusluk faaliyetlerine yönelik eleştirileri sürdürmektedir. Genel olarak ticaret savaşının bir parçası olarak ABD, Çin'e karşı siber saldırıları kınayan ve karşı önlemler alan politikaları benimsemiş, daha çok ABD'nin güvenliğine ve çıkarlarına odaklanarak siber uzayda mutlak üstünlük aramaya başlamıştır. Çin'in bu sert politikalara karşı siber yaklaşımı ise genel olarak ulusal çıkarlarını korumaya odaklanmak, siber uzayda daha fazla küresel yönetim ve normlar oluşturmak, kendi ulusal siber yeteneklerini güçlendirerek siber uzayda bağımsızlığını artırmayı hedeflemektedir.

2.3.3.2. Rusya ve Çin

Rusya ve Çin arasındaki önemli işbirliği alanlarından ve ortak görüşlerinden biri, internet üzerinde daha fazla devlet kontrolünün savunulması ve siber uzayda ulusal egemenlik kavramının teşvik edilmesidir. Her iki ülke de ulus devletlerin kendi sınırları içinde interneti kendi yasa ve politikalarına göre düzenleme ve yönetme hakkına sahip olması gerektiğini öne süren "siber egemenlik" fikrine desteklerini ifade ettirler (Weber, 2020). Ayrıca iki ülke, küresel siber güvenlik normlarını ve düzenlemelerini şekillendirmede, Batılı yaklaşımların hakimiyetine karşı bir duruş sergilemekte, çok kutuplu ve kapsayıcı bir siber uzay normlarının oluşturulmasına devletlerin daha belirgin rolünün olması gerektiğini vurgulamaktadır.

Siber uzay için yeni bir küresel düzen inşa etmeyi amaçlayan Rusya ve Çin, 2009 yılında Şanghay İşbirliği Örgütü çerçevesinde uluslararası bilgi güvenliği alanında işbirliği anlaşması imzalamış. 2014'te Ukrayna krizinin ardından yakınlaşan Çin-Rusya ilişkileri neticesinde 2015 yılında Rusya ve Çin arasında "Siber Uzay İçin Saldırmazlık Paketi" olarak adlandırılan, siber uzayda saldırmazlık konusunda karşılıklı güvence, işbirliği ve siber egemenliği savunan ikili bir anlaşma imzalanmıştır. Ayrıca siber uzayda uluslararası hukuk normlarının oluşturulması ve yaygınlaştırılması için

her iki ülkenin de işbirliği yapması vurgulanmakta. Bu çerçevede Birleşmiş Milletler, Uluslararası Telekomünikasyon Birliği, Şanghay İşbirliği Örgütü, BRICS gibi örgütler aracılığıyla siber egemenlik ve işbirliği desteklenmektedir (Wei, 2016). Özellikle Rusya ve Çin'in siber egemenlik konusuna verdiği destek, uluslararası sistemde ve siber uzayda ABD hakimiyetine meydan okumayı yansıtan stratejik bir destektir.

Nisan 2016 Moskova'da gerçekleşen ilk Rusya-Çin Bilgi ve İletişim Teknolojileri Geliştirme ve Güvenlik Formu, siber uzaydaki işbirliğini daha da derinleştirmiştir. Haziran 2016'da ise siber uzayda ulusal egemenliğe saygı ilkesinin savunulduğu, bilimsel ve teknolojik işbirliğini geliştirmeyi, bilgi ve iletişim teknolojileri konusunda ortak araştırma ve geliştirme yapmayı, iki ülke arasında sektörler arası alışverişi teşvik ederek siber uzay alanında işbirliğini güçlendirmeyi, vatandaşların internet üzerindeki yasal haklarını korumayı, internetin terör ve suç faaliyetlerini yürütmek için kullanımına karşı mücadele etmeyi taahhüt eden ortak bir bildiri yayınlanmıştır (China.org, 2016).

Çin, bilgi kontrolüne ilişkin kuralcı politikaları ile tanınan bir devlettir. Rusya ve Çin'in siber işbirliği derinleşirken Rusya, internet üzerinde daha fazla kontrol sağlayabilmek için büyük ölçüde Çin'den yardım almaktadır. Rusya ise Çin ile işbirliğinin ardından Çin'in Büyük Güvenlik Duvarı'nın unsurlarını, ülkenin internet filtreleme ve kontrol sistemi olan "Ru Net'e" dahil etmek için çalışmıştır (Soldatov & Borogan, 2016). Bu doğrultuda Rusya'nın diğer bir girişimi, Rus kullanıcı verilerinin Rus topraklarında saklanması talep eden yasayı ihlal ettiği gerekçesi ile LinkedIn'e erişimi engellemesi girişimidir (Walker, 2016). Ayrıca Rusya'nın telekomünikasyon ve internet sağlayıcılarının kullanıcı verilerini altı ay ve meta verileri üç yıl boyunca saklamasını gerektiren Yarovaya Yasası olarak bilinen önlemin uygulanmasında gerekli kapasiteyi geliştirmelerine yardımcı olmak adına Çin menşeli çok uluslu şirket Huawei ile görüşmelerde bulunduğu bildirilmiştir (Soldatov & Borogan, 2016).

Rusya ve Çin, ekonomik amaçlı siber casusluk faaliyetlerinde birbirlerini hedef almamak için devam eden bir anlaşmaya sahiptir. Sonuç olarak Rus-Çin siber uzay işbirliği; siber uzayda ABD hakimiyetine ve ABD'nin internet yönetim ilkelerine muhalefet olma temelinde ve Rusya'nın, Çin'de uygulandığı gibi ulusal siber uzay üzerinde kontrole sahip olma isteği çerçevesine şekillenmektedir.

2.3.3.3. Avustralya - Çin

21 Nisan 2017'de Avustralya ve Çin, siber güvenlik işbirliğini genişletmek için siber güvenlik anlaşması imzalamıştır. Anlaşma çerçevesinde iki ülke, rekabet avantajı sağlamak amacıyla gizli ticari bilgilerin ve fikri mülkiyetin siber saldırı eylemleriyle hedef alınmayacağını ve desteklenmeyeceğini taahhüt etmektedir. Ayrıca her iki ülke, Birleşmiş Milletler Hükümet Uzmanları Grubu'nun siber uzayda sorumlu devlet davranışı normları ve siber raporlarına uygun hareket etmek ve siber güvenlik konularını ele almak üzere bir bilgi paylaşım mekanizması oluşturulması konusunda anlaşmıştır (Astakhov, 2018) (Australian Government Department of Foreign Affairs and Trade [DFAT], 2017).

Siber güvenlik işbirliği anlaşmaları dünya çapında ivme kazansa da bu tür anlaşmaların etkisi tartışılmaktadır. Çünkü devletler anlaşma çerçevesinde karşılıklı taahhütlerde bulunsalar da anlaşmaya yönelik ihlaller sıklıkla yinelenmektedir. Örneğin 2022'de Avustralya hükümetine yönelik üç ay boyunca süren Red Ladon isimli Çin devlet destekli siber tehdit aktörlerinin gerçekleştirdiği iddia edilen siber saldırının sonucunda, savunma ve enerji sektöründeki hassas bilgilerin ele geçirildiği, Avustralya'nın Güney Çin Denizi'ndeki operasyonlarıyla ilgili bilgi toplamak için Avustralyalı medya şirketlerinin ve savuma kurumlarının hedef alındığı bildirilmiştir (Davis, 2022). Bu tür ihlaller karşısında ise ulus devletler farklı ittifaklar içerisine girmektedir. Ekim 2022'de Japonya ve Avustralya askeri, istihbarat ve siber güvenlik işbirliğini kapsayan yeni bir ikili güvenlik anlaşması imzalamıştır. Anlaşma Çin'in geniş çapta suçlandığı tehditler içerisinde yer aldığı "*ekonomik baskıya ve dezenformasyona direnme*" konusundaki işbirliğine atıfta bulunmaktadır (Mcdonough, 2022).

2.3.3.4. Endonezya - Çin

2021 yılında Endonezya ve Çin hükümeti arasında siber güvenliğin ve teknolojik işbirliğinin geliştirilmesi konusunda bir mutabakat zaptı imzalanmıştır. Anlaşma çerçevesinde taraflar siber uzayda devlet egemenliğine saygı ilkesini, işbirlikçi ve şeffaf bir internet yönetim sistemini, düzenli bir siber uzay girişimini ve BİT gelişimini destekleyeceklerini taahhüt etmiştir. Çinli araştırmacılara göre mutabakat zaptının, ABD'nin ulusal güvenlik tehdidi oluşturduğu iddiasıyla Çinli

teknoloji firmalarını kapatmaları için siyasi müttefikleri üzerindeki baskıyı artırdığı bir dönemde imzalandığı için büyük önem taşıdığı belirtmekte ve ABD baskısına karşı koymak amacıyla Çin'in ortaklarıyla birlikte düzenlediği hükümet düzeyindeki karşı saldırılarından biri olarak değerlendirilmektedir (Global Times, 2021). Siber güvenlik uzmanları için Huawei'nin 5G teknolojisinin, Endonezya'daki 5G altyapısının gelişimini hızlandıracağı, ABD baskılarına rağmen Endonezya'nın tarafsız davranması gerekliliği vurgulanmaktadır. Bu doğrultuda ise Endonezya Ulusal Siber ve Kriptografi Ajansı ve Çin Siber Uzay İdaresi 29 Temmuz 2022'de siber güvenlik konusunda işbirliğini derinleştirmeyi amaçlayan bir anlaşma imzalamıştır (Cyberspace Administration of China [CAC], 2022).

Avustralya Stratejik Politika Enstitüsü araştırma raporuna göre, bilgi ve iletişim teknolojisi konusunda büyük bir eksikliğin mevcut olduğu Endonezya, siber suçlara karşı en savunmasız ülkelerden biri olarak değerlendirilmiştir. Bu doğrultuda Endonezya, bilgi ve iletişim teknolojisindeki açığı kapatmak için Çin ile ortaklık kurmuş ve 2020'de Huawei, Endonezya'da dijital eğitim programı çerçevesinde eğitim merkezlerine, burslara ve atölyelere büyük yatırımlar yapmıştır (Cyber Security Connect, 2022). Huawei'nin dijital yetenek programını, Çin'in Kuşak ve Yok Girişimleri çerçevesinde önemli bir ülke olan Endonezya'daki yumuşak güç çabalarının bir parçası olarak değerlendirebilmek mümkündür.

2.3.3.5. Şanghay İşbirliği Örgütü ve Siber Diplomasi

1996'da Kazakistan, Kırgızistan, Rusya, Çin ve Tacikistan taraflarıyla oluşturulan, 2001'de Özbekistan'ın, 2017'de Hindistan ve Pakistan'ın, 2021'de İran'ın katılımıyla üye sayısı dokuzaya çıkan Şanghay İşbirliği Örgütü (ŞİÖ), birçok alanda işbirliğini teşvik etme, iyi komşuluk ilişkilerini güçlendirme, bölgede barışı, güvenliği ve istikrarı sağlama hedefini taşımaktadır. Siber uzayın kritik altyapılar üzerinden doğrudan bir etkisi söz konusu olduğu için ŞİÖ içerisinde ulaşım ve enerji altyapıları kritik bir önem taşımakta ve siber güvenlik önemli bir konu haline gelmektedir (Alcantara, 2018, s. 550). Dolayısıyla ŞİÖ, bilgi güvenliği ve dijital egemenlik konusunda bölgesel uzlaşma sağlanması için bir platform görevi görmekte, Çin ve Rusya'nın siber uzay stratejisi çerçevesinde alternatif bir siber uzay vizyonu oluşturmak amacıyla çok taraflı işbirliği yaklaşımı içerisinde yer almaktadır.

2009 yılında ŞİÖ üye devletleri, uluslararası bilgi güvenliğinin sağlanması alanında işbirliği anlaşması yapılmasına karar vermiştir. Anlaşmanın ikinci maddesi çerçevesinde uluslararası bilgi güvenliğinin sağlanması alanındaki tehditler tespit edilmiştir;

Bilgi silahlarının geliştirilmesi, kullanılması ve bilgi savaşına hazırlık, bilgi terörizmi, bilgi suçu, bilgi alanının/siber uzayın diğer devletlerin çıkarlarına ve güvenliğine zarar verecek şekilde kullanılması, diğer devletlerin siyasi, sosyal ve ekonomik sistemlerine zarar veren bilgilerin yayılması, küresel ve ulusal bilgi altyapısının güvenli ve istikrarlı işleyişine yönelik tehditler Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2009).

ŞİÖ üye devletleri, siber güvenlik konusundaki diğer girişimlerini, 2011 ve 2015 yıllarında BM Genel Kurulu'na sunulan, -devletlerin bilgi alanında hak ve sorumluluklarını belirlemeyi ve uluslararası davranış normlarının oluşturulmasını amaçlayan- bir yasa taslağı ile göstermiştir. Ancak yasa taslakları, siber uzayda aşırı devlet kontrolü algısı yaratması sebebiyle reddedilmiştir (Alcantara, 2018, s. 553).

Rusya-Ukrayna çatışması, Hindistan'ın Pakistan ve Çin ile yaşadığı sınır sorunları, Çin'in Orta Asya'da genişleyen teknoloji altyapısı, ŞİÖ içerisinde siber güvenlik konusunda dönüşümlere sebebiyet vermiştir. Bu dönüşümlerden ilki Hindistan'ın Avustralya, Hindistan, Japonya ve ABD'nin katılımıyla kurulan QUAD ortaklarıyla özellikle siber uzay alanında daha yakın işbirliği yapması olmuştur. QUAD üye devletlerinin Dışişleri Bakanları, Çin, Rusya ve İran kaynaklı devlet destekli siber tehditlere yanıt olarak 2022'de önemli bir fidiye yazılımı bildirimini yayınlamış, bölgesel siber altyapının güvenliğini sağlamada ve siber suçla mücadele etmede işbirliği yapma taahhütlerini göstermiştir (Roy, 2022). Bu dönemde Çin hükümeti, Hindistan'ın Orta Asya ve Avrasya'daki etkisini azaltmayı amaçlayarak Pakistan'ı bölge için yeni dijital merkez olarak tanıtmaya girişiminde bulunmuştur. Tencent ve Huawei gibi Çinli şirketler, özellikle Çin-Pakistan Ekonomik Koridoru (CPEC) projesi gibi girişimler aracılığıyla Pakistan ile aktif bir şekilde işbirliği yapmaktadır (Jindal, 2022).

2.4. İran İslam Cumhuriyeti'nin Ulusal Siber Güvenlik Stratejileri, Savunma ve Caydırıcılık Kabiliyetleri

İran'ın siber uzay yetenekleri, ABD, Çin, Rusya gibi teknolojik olarak daha gelişmiş ulus devletlerle karşılaştırıldığında daha az gelişmiş durumda olsa da Tahran,

siber uzayın kilit oyuncularından biri haline gelmiştir. İran, siber uzayın dış ve iç tehditlere karşı korumak için yıllar boyunca ulusal bir siber güvenlik stratejisi uygulamıştır. Siber saldırı yeteneklerini geliştirmek amacıyla da İran Cumhurbaşkanı Hasan Ruhani'nin siber uzay faaliyetlerine ayrılan bütçeyi artırmaya yönelik girişimlerde bulunmasının yanı sıra, Rusya ve Çin'den de siber uzay savunması için teknik yardım almaktadır (Defense Intelligence Agency [DIA], 2019, s. 36). Yurt içi yatırımların yanı sıra Rusya ve Çin ile işbirliği, İran'ın hem savunma hem de saldırı amaçları için siber yeteneklerini geliştirmeye odaklandığını yansıtmaktadır.

İran İslam Cumhuriyeti, baskın liderler, güçlü bir askeri yapı ve güçlü ulusal kültürel kimlik olmak üzere üç temel özellik tarafından yönlendirilmekte ve ulusun stratejik gelişiminde önemli unsurlar olarak kabul edilmektedir (Spadoni, 2019). Dolayısıyla İran rejiminin siber uzay alanındaki temel amaçları; ülkenin kritik altyapısını ve hassas verilerini siber saldırılara karşı korumak, ülke içindeki çevrimiçi faaliyetleri izlemek ve denetlemek, özellikle muhalif unsurların ve rejime karşı çıkan bireylerin tüm siber faaliyetlerini durdurmak ve rejime karşı olanlara yönelik saldırgan siber operasyonlar yürütmektir. 2009 Yeşil Hareket Protestoları, İran'ın siber operasyon yeteneklerini artırmak ve siber uzayın kontrolünü sağlamak için öncülük etmiş, 2010 yılında İran'ın nükleer programına yönelik gerçekleştirilen Stuxnet siber saldırısı ise İran'ın siber uzayda saldırı ve savunma yeteneklerini geliştirme ihtiyacını stratejik bir öncelik olarak kabul etmesini tetikleyen bir dönüm noktası olmuştur (United Against Nuclear Iran [UANI], 2022). Dolayısıyla bu olayların ardından Tahran, 2011 yılında teknoloji geliştirmek, altyapı kurmak, bilgisayar uzmanları yetiştirmek için 1 milyar dolar yatırım yaparak siber uzayda savunma ve saldırı yeteneklerini geliştirmek adına girişimlerine başlamıştır (Katz, 2011).

Sonuç olarak İran'ın siber uzaydaki savunma programının temelde iki hedefi vardır. Birincisi, Stuxnet gibi bir başka saldırıyı, Duqu ve Flame gibi virüslerin İran ağlarına sızmasını önlemektir. İkinci hedefi ise İran kamuoyundan kaynaklanan bilgi ve hizmetleri gözetleme ve sansür yoluyla rejimin hayatta kalmasını sağlamaktır (Siboni & Kronenfeld, 2012, s. 77). Dolayısıyla İran, siber uzay kabiliyetlerini sadece dış tehditlere karşı değil, yerel tehditlere karşı da caydırıcı bir silah olarak geliştirmeyi amaçlamaktadır.

2.4.1. Temel Belgeler ve Stratejiler

İran'ın *Ulusal Bilgi Ağı Projesi (National Information Network-NIN)*, İran vatandaşlarına güvenli ve yerleştirilmiş internet hizmetleri sağlamayı amaçlayan, küresel internetten bağımsız çalışacak şekilde tasarlanmış İran hükümeti kontrolündeki bir ağıdır. İran rejiminin bakış açısına göre ulusal internet ağının kurulması ve İran siber uzayının küresel siber uzaydan ayrılması, rejimle örtüşmeyen Batılı unsurların İran ağına sızmasını önlemek, siber saldırılara ve siber casusluğa karşı savunma yetenekleri oluşturmada kilit bir öneme sahiptir. Bu nedenle İran ağı, rejim tarafından teşvik edilen Şii Müslüman normlarıyla çalışacak ve hükümetin ağ içeriklerini tamamen kontrol etmesini ve denetlemesini sağlayacak şekilde tasarlanmıştır. Bu doğrultuda kontrolü tamamen devlet elinde olan, Çin'in "Büyük Güvenlik Duvarı" ve Rusya'nın "RuNet" projelerine benzer bir şekilde İran'ın "Ulusal Bilgi Ağı Projesi", 2010 yılında İran Bilgi ve İletişim Bakanlığı tarafından ilk olarak "temiz, helal internet" fikri ile ortaya çıkartılmıştır (Çahmutoğlu, 2021, s. 7). 2013 yılından bu yana ise İran hükümeti Ulusal Bilgi Ağı'nı geliştirmek için büyük yatırımlar yaparak ve projeyi resmileştirerek kontrolü altına aldığı internet altyapısı ile ağ içeriklerini filtrelemekte, iletişimi kısıtlamakta ve kullanıcıların hangi platformları kullanabileceklerini kontrol ederek küresel interneti izole etmektedir (Grace, 2020).

Dünya Çapında Ağ'dan (World Wide Web) izole edilmiş, millileştirilmiş ve helal internet olarak adlandırılan proje çerçevesinde;

1. 2013 yılında Gmail, Hotmail, Yahoo gibi e-posta hizmetlerine alternatif olarak devletin denetimini de kolaylaştıracak şekilde tasarlanan, kullanıcıların tam adlarını, kimlik numaralarını, adreslerini ve posta kodlarını vererek şifresiz bir şekilde oluşturacakları ulusal e-posta hizmetini (@post.ir) açmıştır.
2. 2012 yılında İran Devlet Yayın Kurumu içerik üreticileri için YouTube benzeri, ancak denetimli ve katı kurallar çerçevesinde kullanılabilen "Aparat" adında bir web sitesi oluşturmuştur.
3. "Padvish" adlı yerel bir anti-virüs sistemi geliştirilerek yabancı anti-virüs yazılımlarının kullanımı yasaklanmıştır.
4. Skype ve Google Talk gibi seslendirme uygulamalarının kullanımı engellenmiştir.

5. Devlet denetimini ve siber uzay sansürleri karşısında alternatif olarak kullanılan VPN ve TOR gibi ara sunucu ağlarının kullanımı yasaklanmıştır (Siboni & Kronenfeld, 2014).

Tüm bu önlemler, İran hükümetinin bilgi akışını kontrol etme ve vatandaşlarının çevrimiçi faaliyetleri üzerinde bir düzeyde sansür ve gözetim sağlama çabalarına katkıda bulunmaktadır.

Ağustos 2020'de İran Silahlı Kuvvetleri Genel Kurmay Başkanlığı tarafından yayınlanan *Siber Alana Uygulanabilir Uluslararası Hukuka İlişkin Bildirisi*, uluslararası hukukun siber uzayda nasıl uygulanacağına ilişkin görüşlerini özetlemektedir. Bildiri siber uzayın devletler tarafından barışçıl bir şekilde kullanılması gerektiğini, "egemen eşitlik" ilkesine dayalı olarak tüm devletlerin siber uzay alanında sorumlu bir şekilde hareket etme yükümlülüğünü belirtmekle birlikte, "*her devletin sahip olduğu kaynak ve teknolojiler nedeniyle ortak ancak farklı sorumlulukları olduğu*" vurgulanmıştır (Nournews, 2020).

Bildirinin egemenlik ilkesini konu alan II. maddesinde, bölgesel egemenlik ve yargı yetkisinin siber uzayın tüm unsurlarını kapsayacak şekilde genişlediği ve başka bir devletin kontrolündeki siber yapılara (kamu veya özel), yasa dışı müdahale içeren siber uzay operasyonlarının devlet egemenliğinin ihlali sayılacağı belirtilmiştir. Ancak bildiri, siber uzayda egemenliğin nasıl uygulanacağına rehberlik edebilecek bir açıklama sunmamaktadır. Müdahale etmeme ilkesini içeren III. maddesi, ilkenin uluslararası teamül hukuku kapsamında bir kural olarak statüsünü hatırlatarak, siber eylemlerle seçimleri manipüle etmek ve seçimlerden önce kamuoyunu etkilemek gibi yasa dışı müdahale sayılabilecek bazı eylemlere örnekler verilmiştir. Kuvvet kullanımı ve siber saldırıları içeren IV. maddesinde ise İran, can ve mal kaybına sebebiyet verebilme potansiyeline sahip siber operasyonların kuvvet kullanımı teşkil ettiğini, kuvvet kullanmama ilkesini ihlal ettiğini ve siber operasyonların konvansiyonel silahlı saldırı eşiğine gelmesi durumunda meşru müdafaa hakkının varlığını belirtmiştir (Nournews, 2020).

İran'ın siber uzay ile ilgili sunduğu her görüş, ABD ve diğer Avrupa devletlerinin görüşleriyle örtüşmese de batılı olmayan ancak büyük bir siber güç sayılan İran, siber uzay konusuna yapıcı bir şekilde katıldığını ve uluslararası yasal normların mümkün olduğunca siber uzaya uygulanabileceğini bildiride göstermiştir.

28 Temmuz 2021'de oylamaya sunulan *Siber Uzay Kullanıcılarının Korunmasına İlişkin Yasa Tasarısı (Bill for the Protection of Cyberspace Users)*, uluslararası ağ trafiğinin ve iletişim altyapısının sıkı denetimini İran Silahlı Kuvvetlerine devretmektedir. Yasa çerçevesinde yabancı teknoloji şirketlerinin İran'da kayıtlı yasal bir temsilci bulundurmasını, İran'da bağlantı kurabilmek için hükümetin belirlediği kriterlere uymalarının gerekliliğini ve şirketlerin internet kullanıcılarını izleme ve çevrimiçi alanları sansürleme konusunda İran hükümetiyle işbirliği yapmasının gerekliliğini vurgulamaktadır. Tasarının yasalaşması halinde 19. maddesi çerçevesinde, gazetecilerin ve muhaliflerin alabileceği bilgiler üzerinde potansiyel olarak daha fazla kontrol sağlayabilmek amacıyla VPN'lerin ve diğer internet ara sunucusu (proxy) hizmetlerinin üretimi, satışı ve dağıtımı suç sayılacaktır (Committee to Protect Journalists [CPJ], 2021).

Tartışmalara yol açan yasaya karşı toplumun ve bazı milletvekillerinin karşı çıkması, yasanın üç kez düzenlemesini zorunlu hale getirmiştir. Sonucunda ise yasa taslağının özel bir komite tarafından gözden geçirilmesi ve İslam Cumhuriyeti Anayasası'nın 85. maddesi uyarınca parlamentodan nihai olarak onay alana kadar üç veya beş yıl deneysel olarak uygulanmasına karar verilmiştir (Article19 , 2021).

Hükümetin kriterlerine uymayan ve işbirliği yapmayı reddeden şirketler, alternatifler oluşturulana kadar bant genişliği kısıtlamasına⁶ tabi tutulacağı ve ardından tamamen sansürlenmesi öngörülmektedir. Bu durumda Ulusal Bilgi Ağı'nda İran'ın kendi platformlarına yönlendirme yapması beklenmektedir (Article19, 2021). Uluslararası hizmetlere erişimi kesintiye uğratacak, çevrimiçi ifade özgürlüğüne ve kullanıcıların mahremiyet haklarına darbe indirecek bu yasa çerçevesinde Google, Instagram, Twitter ve Amazon gibi küresel hizmetler dahil olmak üzere, rejimin kriterlerini karşılamadığı taktirde İran'da engellenebilecek, gerekli görüldüğüne internet üzerinde kontrol sağlayabilme ve erişimi kesebilme, yetki çerçevesinde muhalefeti bastırmanın bir yöntemi olarak endişe verici görülmekte ve eleştirilmektedir.

⁶ Bant genişliği kısıtlaması, özellikle fotoğraf, sesli not, video veya arama paylaşımı gibi daha fazla internet verisi gerektiren kullanımlarda kullanımı zorlaştırmak için internet platformlarına erişimi kasıtlı olarak kesintiye uğratmaktır.

2.4.2. İran'ın Siber Güvenlik için Ulusal Organizasyon Yapılanması

İran İslam Cumhuriyeti Kolluk Kuvvetleri (NAJA), İran İstihbarat ve Güvenlik Bakanlığı (MOIS), İran İslam Devrim Muhafızları Ordusu (DMO), Siber Güvenlik Komutanlığı, Siber Güvenlik Yüksek Kurulu, bu kurumların altında oluşturulan askeri ve sivil hükümet organları ve İran Siber Ordusu gibi vekil teşkilatlar İran'ın siber saldırı yeteneklerini ve siber politikalarını belirleyen temel kurumlardır. Ulus devletler genellikle istihbarat kurumlarına siber operasyonları doğrudan yürütmesi için yetki vermektedir. Buna karşılık İran'ın siber operasyonları konusunda yetkili iki istihbarat örgütü ise MOIS ve IRGC'dir.

2.4.2.1. İran Siber Polis

İran Siber Polis (Iran Cyber Police-FATA), 2011'de İran İslam Cumhuriyeti Kolluk Kuvvetlerinin bir birimi olarak siber suçları önlemek, araştırmak ve mücadele etmek amacıyla ulusal ve uluslararası standartlara dayalı olarak kurulmuştur. FATA, siber suçların ne şekilde soruşturulması gerektiği ve siber suçları caydırmak için kullanılabilecek teknik uygulamalar konusuna odaklanmaktadır. Amacı ise ulusal ve dini kimliği, topluluk değerlerinin korunması, siber uzayda ulusal otoritenin sağlanması, siber operasyonlara karşı ulusal kritik altyapının, ekonomik, sosyal, ulusal egemenliğin korunmasını sağlamaktır (Sajedi & Ariani, 2014).

FATA, ağ kullanıcılarının kişisel bilgilerini vermesini gerektiren kişi ve kuruluşlar için yeni yönergeler sunarak siber suç eylemlerini tespit etmeye ve dava açmaya çalışmaktadır. Dolayısıyla FATA'nın en önemli faaliyeti, internet kullanıcılarını kontrol altına almaktır. Örneğin Ocak 2012'de FATA, internet kafeteryaları için kullanıcıların kafeterya sahipleri tarafından altı ay boyunca saklanacak kişisel bilgilerin yanı sıra, ziyaret ettikleri web sitelerinin, kullanıcı IP adreslerinin, günlük dosyalarının, internet kullanım gün ve saatlerinin bir kaydını sağlamalarını gerektiren yeni yönergeler yayınlamıştır. Ayrıca kafeterya sahiplerinin, kapalı devre televizyon kameraları kurması ve kayıtları alt ay boyunca muhafaza etmesi gerekmektedir (IFMAT, tarih yok). Tüm bu önlemlerin vatandaşlara yönelik gerçekleştirilebilecek bilgi hırsızlığından endişe duyulması nedeniyle uygulandığı belirtilse de, 2009 yılındaki seçimlerden sonra başlayan Yeşil Hareket sonrasında, dijital ortamdaki suçlarla mücadele adına kurulan FATA'nın asıl amacı, ulusal

güvenliğe tehdit oluşturabilecek kişilerin izlenmesi olduğunu göstermektedir (Çahmutoğlu, 2021, s. 16).

2.4.2.2. İran Siber Uzay Yüksek Konseyi (Supreme Council of Cyberspace-SCC)

Siber Uzay Yüksek Konseyi (Supreme Council of Cyberspace-SCC) 7 Mart 2012'de İran'ın dini lideri Ayetullah Hamaney'in kararı ile Hamaney'e bağlı olarak, İran rejiminin internet politikasını oluşturmak ve denetlemek amacıyla kurulmuştur. Hamaney tarafından atanan kişilerden oluşan konsey, internet politikasını koordine etme, uygulama, onaylama ve veto etme yetkisine sahiptir. Konsey'e verilen yetkiler çerçevesinde kararları yasal olarak bağlayıcıdır ve faaliyetleri İran Parlamentosu tarafından engellenemez (Small Media, 2014). Konseyin amacı, İran hükümetinin ve vatandaşlarının siber uzayın pozitif yönlerinden yararlanmasını ve olumsuz yönlerinden korunmasını sağlamaktır. Bu doğrultuda Konsey, internet sansürü ve filtreleme politikalarını yürütmektedir. Sansür uygulamasından ve hükümet organları arasında yer alan Saldırgan İçerikleri Belirleme Komitesi ve DMO Siber Savunma Komutanlığını kontrol etmekten sorumludur (Aryan, Aryan, & Halderman, 2013).

Konsey, Hamaney'in doğrudan liderliği altında faaliyet gösteren iletişim, teknoloji, araştırma, bilgi, kültür, yayın, polis, istihbarat ve DMO Başkomutanı ve liderlerini dahil eden üst düzey yetkililerden oluşan bir organizasyondur (The Office of the Supreme Leader , 2011). Yalnızca siber uzay ile ilgili politikalardan sorumlu bir üst organizasyonun oluşturulması İran'ın siber güvenliği, ulusal güvenliğin merkezinde bir konuma getirdiğini göstermektedir.

2.4.2.3. Ulusal Siber Uzay Merkezi

Siber Uzay Yüksek Konseyi'nin denetimi altında faaliyet gösteren Ulusal Siber Uzay Merkezi'nin (National Cyberspace Center-NCC) görevi, İran halkının internet denetimlerini atlamak için kullanılan VPN'lere (Sanal Özel Ağları) ve proxy kullanımını engelleyerek, İran vatandaşlarının Batı medya içeriklerine erişimini engellemesidir (U.S. Department of the Treasury , 2018). İran hükümeti tarafından

yayınlanan 2013 NCC Tüzüğüne göre NCC, İran ve düşmanları arasında "*kültürel bir savaşa hazırlanmak*" ile görevlidir (Congressional Research Service [CRS], 2020).

2.4.2.4. Ulusal Pasif Sivil Savunma Örgütü

İran İslam Cumhuriyeti Silahlı Kuvvetleri'nin özel alt birimi olarak faaliyet gösteren Pasif Sivil Savunma Örgütü (National Passive Defense Organization-NPDO), İran'ın ulusal kritik altyapısını siber tehditlere karşı korumaktan sorumlu, yarı askeri bir kurumdur (Lewis, 2019). Kuruluşunun ilk yıllarında NPDO, İran-İrak Savaşı'ndan elde edilen deneyimden yola çıkarak İran'ın kritik altyapısını geliştirmeye odaklanmıştır. Bugün ise İran'da internet ve sosyal medya kullanımının hızla artması ve askeri olmayan yeni araçlara dayanan ekonomik savaş modellerinin oluşması karşısında NPDO'nun faaliyetleri ve rolleri de genişlemiştir. Bu bağlamda NPDO'nun ana rollerinden biri "*İran'ın ulusal altyapısına karşı düşman devletler veya düşman devletler tarafından desteklenen gruplar dahil tüm ulusal siber ve siber olmayan tehditleri caydırmak, önlemek ve etkili bir şekilde karşı koymaktır*" (Nadimi, 2018). Rejimin otoriter doğası göz önüne alındığında ulusal tehditler kapsamında, popüler mesajlaşma uygulaması Telegram, yaygın yolsuzluk ve adaletsizliğe karşı halk protestolarını kışkırtmaktan sorumlu tutulmuştur (Katman, 2021, s. 444).

2.4.2.5. Siber Savunma Komutanlığı

Siber Savunma Komutanlığı (Cyber Defence Command), Kasım 2010'da gerçekleşen Stuxnet saldırısının hemen ardından İran İslam Cumhuriyeti Ordusu Müşterek Kurmay Başkanlığı'nın bir alt bölümü olan Pasif Sivil Savunma Teşkilatı'nın denetiminde savunma odaklı kurulmuş bir kurumdur. Pasif Sivil Savunma Örgütü başkanına göre Siber Savunma Komutanlığı, siber tehditlere karşı ülkenin ve kritik altyapısının güvenliğinden sorumludur (Neu, 2013). Savunma yönelimli bir merkezi örgüt olan Siber Savuma Komutanlığı, karşı siber saldırı faaliyetlerinde yer almamaktadır (Siboni & Kronenfeld, Iran and Cyberspace Warfare, 2012, s. 82).

2.4.2.6. Besic Siber Uzay Konseyi

DMO'ya bağılı Besic örgütü, siber uzayda da faaliyete geçerek 2010 yılında Besic Siber Uzay Konseyini (Basij Cyberspace Council) kurmuştur. Besic, öncelikle İran yanlısı propaganda yaratmaya odaklanarak içerik üretmeleri için İranlı vatandaşları işe almakta, eğitmekte ve rejim yanlısı bilgisayar grupları kurmaktadır. Ayrıca medyada, büyük forum sitelerinde, yurt içinde ve yurt dışındaki web sitelerinde rejimi destekleyen konuşmalar ve metinler hazırlamaktadır (Esfandiari, Basij Members Trained To Conquer Virtual World, 2010).

İran siber savunma stratejisi çerçevesinde, sivillerin işe alındığı nadir ülkelerden biri olma özelliği taşımaktadır. Besic Siber Uzay Konseyi'nin üyelerinin çoğunluğu alt sosyal sınıflara ait ve uzman olmayan bireylerden oluştuğu için en önemli siber eylemleri arasında bilgisayar ve internet kullanımı, blog yazma becerilerine sahip olmasıdır. Ayrıca rejim lehine çevrimiçi gönderiler oluşturmak amacıyla gönüllülerden oluşan örgütün kurulması için üniversiteler ve ilahiyat okullarıyla olan bağlantılar kullanılmıştır. Bu projenin bir parçası olarak Besic Örgütü içerisinde ücretsiz sınıflar açılmış ve birçok web blogu oluşturulmuştur. Yetkililerin eğitimlerden sonra üyelerden beklentisi ise İran İslam Cumhuriyeti liderini ve rejimi destekleyerek, rejimi eleştirenlere karşı düşük düzeyde saldırı ve sızma faaliyetleri gerçekleştirmeleridir (Bastani, tarih yok).

2.4.2.7. İran Siber Ordusu

2010 yılında DMO tarafından oluşturulduğu iddia edilen İran Siber Ordusu (Iran's Cyber Army - ICA), kurulduktan sonra birçok internet kullanıcılarını tutuklamıştır. DMO henüz İran'ın Siber Ordusu'nun sorumluluğunu resmi olarak üstlenmemiştir ancak DMO ve İstihbarat Bakanlığı tarafından desteklendiği ve finanse edildiği tahmin edilmektedir (U.S. Government Publishing Office, 2016, s. 7). Bir takım DMO yetkililerinin, İran Siber Ordusunun faaliyetlerine ve bu organizasyonla olan bağlantılarına atıfta bulunduğu söylemler mevcuttur. Örneğin Nisan 2011'de DMO'daki dini liderin eski temsilci yardımcısı Mojtaba Zolnoor, İran'ın "Siber Ordu"yu kullanarak "düşman bölgesini" ele geçirmeyi başardığını ifade etmiştir. Daha öncesinde ise DMO'nun siyasi ofisinin eski başkanı Yadollah Javani, İran'ın dünyanın en büyük beşinci siber ordusuna sahip olduğunu söylemiştir (Bastani, tarih yok).

Besic Siber Uzay Konseyi üyelerinin aksine daha gelişmiş operasyonlara katılan İran'ın Siber Ordusu, bilgi teknolojisinde son derece yetenekli uzmanlardan, kimlikleri bilinmeyen profesyonel bilgisayar korsanlarından oluşan bir organizasyondur. İran Siber Ordusu'nun gelişmiş teknik yetenekleri sayesinde şimdiye kadar birçok yabancı merkezli medya kuruluşunun yanı sıra Twitter ve Batı'daki bazı hükümet siteleri, İran Siber Ordusu tarafından hacklenmiştir. Web sitelerinde kullanıcıları İran yanlısı mesajlar içeren web sitelerine yönlendirme sorumluluğunu üstlendiğinde uluslararası dikkatleri üzerine çekmiştir. (Bastani, tarih yok). Örneğin Şubat 2011'de Amerika'nın Sesi (VOA) web sitesinin alan adının ele geçirilerek siber saldırıya uğraması İran Siber Ordusuna atfedilmiştir (Connell, 2014, s. 10).

İran Siber Ordusu'nun dikkat çeken ilk faaliyeti ise, Yeşil Hareket sürecinde protestolar sırasında Twitter'ı uzun saatler boyunca devre dışı bırakmayı başarmış olmasıdır. Ayrıca İran Siber Ordusu'nun, muhalefet faaliyetlerini destekledikleri gerekçesiyle uluslararası basın kuruluşlarına yönelik siber saldırılar düzenledikleri de iddia edilmektedir. Bu çerçevede 1 Mart 2012'de İran'ın BBC Farsça Servisi'ne düzenlenen siber saldırının arka planında İran Siber Ordusu'nun olduğu iddia edilmektedir (BBC, 2012).

2.4.2.8. DMO Elektronik Harp ve Siber Savunma Örgütü

JANGAL olarak da bilinen DMO Elektronik Harp ve Siber Savunma Örgütü (IRGC Electronic Warfare and Cyber Defence Organization- IRGC EWCD Organization JANGAL), DMO bünyesinde uzmanlaşmış bir birimdir (U.S. Department of the Treasury, 2018). JANGAL'ın amacının, İran'ın askeri ve ulusal güvenlik hedeflerini destekleyen elektronik harp operasyonlarını yürütmek olduğu iddia edilmektedir. Hakkında detaylı bilgi bulunmayan bu örgüte, İran'daki Net Peygard Samavat gibi siber güvenlik şirketlerinin teknik destek ve danışmanlık hizmeti verdiği bilinmektedir (Çahmutoğlu, 2021, s. 15). Dolayısıyla JANGAL'ın birinci odak noktası, sinyal istihbaratı ve elektronik gözetleme dahil olmak üzere elektronik harp yetenekleri ve teknolojiler geliştirmektir. Bu yetenekler, İran'ın askeri operasyonlar sırasında düşman iletişim sistemlerini, radar sistemlerini ve diğer elektronik cihazları bozmasını sağlamaktadır.

2.4.2.9. İran Ulusal Bilgisayar Acil Durum Müdahale Ekibi

MAHER olarak da bilinen ve 2008 yılında kurulan İran Ulusal Bilgisayar Acil Durum Müdahale Ekibi (Iran Computer Emergency Response Team Centre - CERT), olay müdahale ve koordinasyon ekibi, değerlendirme ve analiz ekibi, izleme, veri toplama ve güncelleme ekibi, bakım ve destek ekibi, kötü amaçlı yazılım ve güvenlik açığı analiz ekibi, eğitim ekibinden oluşmaktadır (Radkani, 2013). Kurum siber tehditleri tespit etmek, önlemek, ulusal siber altyapıyı korumak, olaylara müdahale faaliyetlerini koordine etmek ve güvenlik açıklarını tespit etmekle görevlendirilmiştir. Ayrıca görevleri çerçevesinde siber güvenliğin sağlanması için yönergeler sunmakta, diğer devlet kurumlarıyla faaliyet göstermekte ve destek sağlamaktadır. Bilgi ve İletişim Teknolojileri Bakanlığı, 2019 yılında İran Ulusal Bilgisayar Acil Durum Müdahale Ekibi'nin 37 milyonu ülke içinde ve 375 milyonu yurt dışında olmak üzere toplam 412 milyon kötü amaçlı siber saldırısını tespit ettiğini ve engellediğini açıklamıştır (Government of the Islamic Republic of Iran, 2020).

2.4.3. İran'ın Siber Diplomasisi

2.4.3.1. Rusya-İran

2015 yılında Tahran ve Moskova hükümetleri, ortak tehditler ve düşman devletlere karşı siber savunma motivasyonu çerçevesinde birlikte çalışmayı amaçladıkları bir anlaşma yapmıştır. Bu işbirliğinde hem istihbarat alışverişine hem de tehditlere karşı ortak savunmaya odaklanılacağı vurgulanmıştır (Tasnim News, 2015). 2015 yılındaki varılan işbirliğini takiben 2016'da Rusya ve İran arasında düzenlenen çalışma toplantısında, BİT alanında ortak projelerin ve işbirliğinin geliştirilmesi için ikili bir çalışma grubunun oluşturulmasının, BİT sektöründe Rus ve İranlı şirketler arasındaki işbirliğini geliştirmek için önemli bir araç olacağı gündem konusu olmuştur. Ayrıca toplantıda yazılım alanında "*tek taraflı Batı egemenliğini*" sona erdirmek için işbirliği yapılması da kabul edilmiştir (Ministry of Digital Development, Telecommunications and Mass Media of the RF, 2016).

2017'de Rusya Devlet Başkanı Vladimir Putin ile İran Cumhurbaşkanı Hasan Ruhani arasındaki görüşmeler neticesinde, iki ülke arasında iletişim ve bilgi teknolojisi alanında işbirliğine ilişkin bir Mutabakat Zaptı imzalanmıştır. Mutabakat Zaptı, sadece

iletiřim ve biliřim sektörünün gelişimine yönelik deęil, aynı zamanda telekomünikasyon, geniş bant internet erişimi, internet yönetiřimi, aę güvenlięi, e-ticaret, e-devlet, e-posta hizmetleri, 4G ve 5G aęları, nesnelerin interneti, uluslararası internet baęlantısı alanlarında işbirlięinin geliştirilmesi öngörülmektedir (Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 2017). Görüşmede ek olarak, Rusya İletişim ve Kitle İletişim Bakanı olan Nikolai Nikiforov İran tarafına, 2014 yılı başında Rusya devlet dairelerin tarafından Rus yazılımının satın alım payının %20 olduğunu ve 2017 yılında %60 oranına yükseldiğini bildirmiştir. Rusya devlet kurumlarının yabancı sunucular yerine yerli Rus sunucularını kullanmaya başladığı konusundan bahsederken, Rusya'nın kendi sunucularını ve teknolojilerini Tahran'daki devlet kurumlarına ve devlete ait şirketlere sunma teklifinde bulunmuştur (Ministry of Digital Development, Telecommunications and Mass Media of the RF, 2017).

26 Ocak 2021 tarihinde Rusya Dışışleri Bakanı Sergey Lavrov ve İran Dışışleri Bakanı Mohammad Javad Zarif, siber güvelik ve BİT alanında bir işbirlięi anlaşması imzalamıştır. Anlaşma siber güvenlik işbirlięi, teknoloji transferi, teknik yardım, bilgi ve istihbarat alanlarındaki işbirlięi genişletmeyi içermektedir (Defence Media [DFNC], 2021). Esas olarak anlaşma, İran ve Rusya'nın ABD'ye karşı ortak düşmanlık, batının özgür bir internet sağlama hedefine karşı çabaları yoğunlaştırma ve batılı teknolojilere olan bağımlılıęı azaltma arzusuyla motive edilerek savunma amaçlı oluşturulmuştur. Bu doğrultuda gerçekleştirilen işbirlięi çerçevesinde gelecekte iki devlet, siber saldırı yeteneklerini ve istihbarat paylaşımına odaklanacaktır (Negi, 2022).

3.4.3.2. Çin - İran

2019 yılında İran'ın İletişim ve Bilgi Teknolojileri Bakanı ve Çin'in Sanayi ve Bilgi Teknolojileri Bakanı arasında gerçekleşen görüşmede iki taraf bilgi teknolojisi alanında işbirliğini artırma, siber uzaydaki tehditleri araştırma ve savunma oluşturmak için ortak bir çalışma grubu kurma konusunda anlaşmaya varmıştır. İran tarafı görüşmede, ABD'nin iki büyük Çinli şirket olan ZTE ve Huawei'ye yönelik yasaklarına eleştirilerde bulunmuş, "*ABD'nin siber uzaydaki hegemonyasını yapay*

zeka gibi yeni teknolojilerle yayarak modern sömürgeciliği başlattığı" açıklamasını yapmıştır (Mehr News Agency, 2019).

2021 yılında İran ve Çin, ABD tarafından uygulanan farklı düzeylerde yaptırımlar altındayken, askeri işbirliğine ek olarak İran'ın enerji, teknoloji, üretim kapasitesi ve sağlık gibi kilit sektörlerinde önemli Çin yatırımlarını içeren kapsamlı bir "25 Yıllık Stratejik Anlaşma" imzalanmıştır. Çin ve İran arasındaki ekonomik ve kültürel etkileşimi içeren 400 milyar dolarlık anlaşma aynı zamanda İran'ın Kuşak ve Yol girişimine katılmasının önünü de açmaktadır (TRT World, 2022). Ekonomik ve askeri işbirliğini içeren 25 yıllık anlaşmada siber güvenlik konusundaki işbirliğine değinilmiştir. Anlaşmanın Çin ile yapılan siber işbirliğine odaklanan bölümünde, İran için ulusal bir internet oluşturmak için iki ülkenin birlikte çalışacağı belirtilmiştir (Esfandiari, 2020).

2.5. Stratejik Siber Vakalar

Stratejik siber vakaların incelenmesi, dijital çağda gelişen savaş ortamını anlamak, güvenlik açıklarının keşfedilmesi ve savunma stratejilerinin geliştirilmesi açısından önem taşımaktadır. Çalışmanın bu bölümünde ele alınan vakaların analizliyle, siber savaşın geçmişten bugüne nasıl evrildiği, küresel güvenlik ve uluslararası ilişkiler üzerindeki geçmiş, şimdiki ve gelecekteki potansiyel etkileri tartışılmaktadır. Bu bağlamda siber eylemlerin ilk belirtilerine ve çatışma zamanında bilgi savaşının gelişimine ışık tutan Körfez Savaşı, Kosova Savaşı, İsrail-Filistin çatışmaları sırasında tanık olunan siber saldırılar, 2007 ve 2008 yıllarında Estonya ve Gürcistan'a yönelik gerçekleştirilen siber saldırılar incelenecektir.

2.5.1. Körfez Savaşı

Bir savaşı kazanmak için düşmanın bilgi ve iletişim hedeflerini kontrol etmenin gerekliliği, II Dünya Savaşı'ndan sonra dönüşmüştür. Hedefleri bombalayarak fiziksel zarara uğratmak yerine, hackleyerek uzaktan etkisiz hale getirme fikriyle günümüzde siber saldırılar daha karmaşık bir hal almıştır. 1990-1991 yılları arasında Irak'ın Kuveyt'i işgal etmesiyle başlayan Körfez Savaşı'nda siber güvenlik, o dönemde henüz günümüzdeki kadar gelişmemiş olsa da bazı siber eylemler gerçekleşmiştir. Bilgisayar

ağları, Birinci Körfez Savaşı'nda önemli bir rol oynayarak, daha önce görülmemiş düzeyde bilgi, istihbarat ve silah gücü sağlamıştır. Körfez Savaşı sırasında, siber operasyonlar ilk kez savaş alanında uygulanmıştır. Bu savaşta Hollanda'dan bir grup bilgisayar korsanı tarafından Pentagon'un ağ sisteminin, son derece şiddetli bir siber saldırıya uğradığı, yüzlerce Amerikan gizli belgesi ve bilgileri, bilgisayar korsanları tarafından ağ üzerinden çalınarak Irak'a verildiği iddia edilmektedir (Li & Zhang, 2022, s. 169). Eski bir savunma politika müsteşarı olan Alan D. Campen "*Bu savaş temel olarak önceki tüm çatışmalardan farklıydı, çünkü sonuç insanların ve silahların performansı kadar üstün bilgi yönetimine de bağlıydı*" ifadeleriyle Körfez Savaşı'nın ilk bilgi savaşı olduğunu kabul etmektedir (Whitehead, 1999, s. 18).

2.5.2. Kosova Savaşı

Küreselleşen, internet çağı çatışmalarında, bilgisayarı ve internet bağlantısı olan herkes potansiyel bir savaşçıdır. Siber savaşın ne zaman başladığına dair net bir tarih yoktur, ancak 1999'da Kosova'da önemli bir dönüm noktası yaşanmıştır (The Atlantic Council of the United Kingdom , tarih yok). Çünkü Kosova Savaşı, bilgi savaşının ve savaşta teknolojinin kullanımının geliştiği bir dönemde meydana gelmiştir.

NATO'nun hava harekatı başladıktan sonra, Kara El gibi çok sayıda Sırp yanlısı ve Batı karşıtı bilgisayar korsanı, NATO'nun askeri operasyonlarını aksatmak amacıyla NATO'nun internet altyapısını hedef almıştır. NATO'nun web sitelerine ve bilgisayar sunucularına yönelik siber saldırıların yanı sıra aynı yöntemlerle, ABD ve Birleşik Krallık'ın internet altyapısı da DDoS ve virüs bulaşmış e-posta yoluyla tahrif edilmiştir. ABD'de Beyaz Saray'ın web sitesi tahrif edilmiş ve Birleşik Krallık bazı veritabanı bilgilerinin kaybedildiği bildirilmiştir (Geers, 2018). NATO'nun Yugoslavya üzerindeki harekatının başlangıcında, Yugoslav bilgisayar korsanlarına Rus bilgisayar korsanlarının yardım ettiği, Belgrad'daki Çin Büyükelçiliğinin bombalanmasından sonra ise Çinli bilgisayar korsanlarının Yugoslav ve Rus bilgisayar korsanlarından oluşan birleşik güce katıldığı iddia edilmektedir (Milosevic, 2014).

Savaş sürecinde Belçika'nın Brüksel kentindeki NATO karargahının web sunucusuna odaklanmış bir siber saldırı, bilgisayar korsanları için bir propaganda zaferine dönüşmüş ve NATO'nun halkla ilişkiler web sitesi birkaç gün boyunca

kesintiye uğratılmıştır (Geers, 2018). Saldırı, NATO'nun e-posta sunucusunu günde 2.000 mesajla dolduran ve birkaç gün sunucu kesintisine yol açan Yugoslavya kaynaklı bir e-posta saldırısını içermektedir. E-postada kullanılan virüsün yirmi beş türü olduğu tespit edilmiştir. Ayrıca NATO sözcüsü Jamie Shea, Yugoslavya'nın başkenti Belgrad'daki bilgisayar korsanlarının NATO internet sitesine "Ping bombardımanı stratejisi" olarak bilinen saldırıyı düzenlediğini ve eşzamanlı bir e-posta selinin NATO'nun e-posta sunucunu başarıyla kapattığını belirtmiştir. Saldırının ardından NATO, bilgisayar sunucularının ve ağının güvende kalmasını sağlamak amacıyla sistemi yükseltmeye çalışırken, Belgrad'da başlayan ağ saldırıları dünyanın diğer bölgelerine yayılmayı başararak uluslararası ağ sistemlerini etkilemiştir (Verton, 1999). Ateşkes 9 Haziran 1999'da sağlanmış, BM kararı ile NATO ve Yugoslavya arasındaki çatışma sona ermiştir. NATO savaş sürecinde askeri açıdan başarı göstermiş olsa da siber uzayda yetenekleri sınırlı kalmıştır.

2.5.3. İsrail - Filistin

Soğuk Savaş sırasında, Orta Doğu genellikle askeri silahlar ve taktikler için bir deneme alanı olarak hizmet etmiştir. Aynı durum internet çağında, siber savaş içinde geçerlidir. Ekim 2000'de, üç İsrail askerinin kaçırılmasının ardından, bir siber saldırıyla Hizbullah web tahrip edilmiş ve içeriği İsrail bayrakları ve İsrail milli marşının yer aldığı bir ses dosyasıyla değiştirilmiştir. Sonraki İsrail yanlısı saldırılar, Filistin Ulusal Yönetimi, Hamas ve İran da dahil olmak üzere İsrail'e düşman olarak algılanan askeri ve siyasi kuruluşların web siteleri siber saldırılarla hedef alınmıştır. Filistin yanlısı bilgisayar korsanlarının bu saldırılara misillemesi ise hızlı ve kapsam olarak çok daha çeşitliydi. Yanıt olarak bilgisayar korsanları, İsrail Bankası, e-ticaret siteleri ve Tel Aviv Menkul Kıymetler Borsası'nın yanı sıra telekomünikasyon, medya ve üniversiteler de dahil olmak üzere İsrail'in siyasi, ekonomik ve askeri hedeflerini siber saldırıyla tahrip etmiştir (Geers, 2018).

2000 yılından bu yana, Orta Doğu'da yaşanan siber saldırılar, genellikle sahada yaşanan çatışmalarla birlikte görülmeye başlamıştır. 2006'da, İsrail ve Gazze arasındaki başka bir krizin ortasında, Filistin yanlısı bilgisayar korsanları Bank Hapoalim, Bank Otsar, Ha-Hayal, BMW Israel, Subaru Israel ve McDonalds Israel dahil olmak üzere yaklaşık 700 İsrail internet alanını kapatmıştır (Geers, 2018). 2008-

2009 Gazze Şeridi'ndeki Dökme Kurşun Operasyonu sırasında İsrail hükümetinin birkaç web sitesi siber saldırıya uğramıştır (Roscini, 2014, s. 8).

2012'de ise İsrail'in Savunma Sütunu Operasyonu sırasında Gazze'deki hava saldırılarına ve internet kesintisine yanıt olarak Anonymous ve diğer bilgisayar korsanları tarafından İsrail'in Cumhurbaşkanlığı sitesine 10 milyon, Dışişleri Bakanlığı'nın sitesine 7 milyon ve Başbakanın sitesine 3 milyon siber saldırı denemesi yapılmıştır. Dönemin Maliye Bakanı adını vermek istemediği bir sitede yalnızca bir bilgisayar korsanlığı girişiminin başarılı olduğunu bildirmiştir. Bu durumda İsrail'in baş istihbarat yetkilisi Carmela Avner "*Savaş üç cephede yaşanıyor. Birincisi fiziksel, ikincisi sosyal ağlar dünyasında ve üçüncüsü siber*" dediği aktarılmıştır (Scheer, 2012).

2.5.4. Estonya Siber Saldırısı

Nisan 2007'de Estonya'nın başkenti Tallinn'deki Sovyet döneminden kalma bir Sovyet Savaş Anıtı'nın (Bronz Asker Heykeli) taşınmasının ardından Estonya, yirmi iki gün süren koordineli bir siber saldırının hedefi olmuştur. Heykelin taşınması, Estonyalı siviller ve Rus azınlıklar arasındaki gerilimi tetiklemiştir. Estonyalı siviller için heykel Rusya'nın Estonya üzerindeki baskısını temsil ederken, Rus azınlıklar için heykelin Tallinn'in dış mahallelerine taşınması, etnik kökenlerinin marjinalleşmesini temsil etmektedir. Bu gerginliğin ardından Nashi Youth Group tarafından Estonya'nın Rusya Büyükelçisi önünde kitlesel bir protesto ve Nashi Youth Group Komiserleri Sergei Markov, Kostantin Goloskokov ve onların takipçileri tarafından başlatılan bir siber saldırı izlemiştir (Handayani & Christianti, 2021, s. 49).

Saldırıları Estonya'nın temel elektronik altyapısını hedef almıştır. DDoS ile Estonya hükümetinin web sitelerine müdahale edilmiş ve bilgisayar korsanları belirli siteleri tahrip ederek kullanıcıları Sovyet askerlerinin görüntülerine yönlendirmiştir (O'Connell, 2012). Halka açık web siteleri ve e-posta gibi kritik olmayan hizmetler hedef alınırken, internet bankacılığı, DNS gibi hayati hedeflere odaklanan bu saldırılar hiçbir kuruluş veya devlet tarafından üstlenilmemiştir. Ancak bu siber saldırıların Estonya ve Rusya arasındaki siyasi çatışmayla bağlantılı olduğu açıktır (Ottis, 2008).

Saldırılarda hedef hem kamu hem de özel sektöre yönelik gerçekleştirilmiştir ve Estonya nüfusunun büyük çoğunluğu bu saldırılardan etkilenmiştir. Ülkenin birçok bakanlıklarının web siteleri, siyasi partileri dahil, özel sektör kurumlarından olan ticari bankalar, telekomünikasyon operatörleri, internet servis sağlayıcıları, küçük işletmeler, ülkenin altı büyük haber kuruluşundan üçü ve Estonya'nın iki büyük bankası DDoS tarafından hedef alınmıştır (Traynor, 2007).

Estonya'da vatandaşların %40'ı her gün çevrimiçi olarak gazete okumakta, banka işlemlerinin %90'ından fazlası internet bankacılığı üzerinden yapılmakta, mobil telefonlardan birçok günlük işlemlerin ödemelerini gerçekleştirmekte ve oylama sistemi çevrimiçi olarak uygulanmaktadır (Davis, 2007). Saldırı, e-posta sunucuları ve ana bilgisayarların arızalanmasına, DNS sunucularının aşırı yüklenmesine ve yönlendiricilerin zarar görmesine sebep olurken, 10 Mayıs'ta Estonya'nın en büyük bankası olan Hansabank, çevrimiçi hizmetine bir saatten fazla süreyle kapatmak zorunda kalmış ve 300 şüpheli internet adresine erişimi engelleyerek yaklaşık 1 milyon ABD doları değerinde kayba neden olmuştur (Colatin, 2007). Ayrıca Estonya, hedef olduğu siber saldırıların ardından sorumluları bulmak için bir soruşturma başlatmıştır. Ancak Kremlin kaynaklı siber saldırıların delilleri yetersiz olduğundan siber operasyonların Rusya tarafından gerçekleştirildiği kanıtlanamamıştır (Ottis, 2008). Dolayısıyla saldırgan tam olarak tanımlanamadığı veya kanıtlanamadığı için meşru müdafaa veya geri misilleme işletilememiştir.

2.5.4. Gürcistan Siber Saldırısı

Estonya'da yaşanan siber saldırı büyük hasarlarla siber uzayda başlamışken, Gürcistan'a yönelik gerçekleştirilen siber saldırılar 2008 Rus-Gürcü savaşı sırasında başlamıştır. Geleneksel silahlı çatışma sırasında, internetin sivil kullanımına müdahale etmek için gerçekleştirilen ilk siber saldırı olarak bilinmektedir. Sıcak çatışma her ne kadar bir hafta sürmüş olsa da, Gürcistan'ın hükümet siteleri, medya siteleri ve ticaret sitelerine DDoS saldırıları yaklaşık bir ay sürmüştür (O'Connell, 2012).

Devlet siteleri, haber ajanslarının web siteleri ve iç iletişim araçları olmak üzere siber saldırıların üç ana hedefi vardı. Gürcistan Cumhurbaşkanlığının, Dışişleri Bakanlığının, Savunma Bakanlığının ve parlamentosunun da içinde olduğu yüz Gürcü web sayfası DDoS ve SQL Injection yöntemi ile siber saldırılara uğrayarak arızalı hale

getirtilmiştir. Daha önce de belirtildiği gibi, askeri müdahaleyle eş zamanlı olarak gerçekleştirilen ilk siber saldırı olma özelliğini taşıyan bu siber saldırı vakasında, Rus hükümetinin bu siber saldırıları gerçekleştirdiğine dair resmi bir kanıt olmamasına rağmen, bilgisayar korsanları kasten özellikle Rus propagandasını yayarak Rusya'nın çıkarları doğrultusunda hareket etmeye çalışmıştır (Napetvaridze & Chochia, 2019, s. 161). Gürcistan Dışişleri Bakanlığı tarafından yapılan açıklamada, Rusya'nın bir "siber savaş" kampanyası yürüttüğü belirtilmiştir. Moskova hükümeti ise, bu saldırılarda herhangi bir rolü olmadığını belirterek suçlamaları reddetmiştir (Synovitz, 2008).

Gürcistan 2008 tarihinde, Estonya hükümeti kadar elektronik hizmetlere bağlı olmadığı için çok fazla tahribat görmemişti. Ancak bazı analistler tarafından saldırıların Gürcistan hükümetinin konumunu önemli ölçüde zarflattığını ifade edilmiştir (Swaine, 2008). Ayrıca Gürcistan'ın bu dönemde devlet politikaları içerisinde siber güvenlik eylem planı, siber alanın güvenliğini sağlamaktan sorumlu devlet kurumları veya özel kurumlar, siber alan ile ilgili ceza kanunları ve yetenekleri mevcut değildi (Napetvaridze & Chochia, 2019, s. 162).

3. SİBER UZAYDA ÇOK ULUSLU ŞİRKETLER

Siber uzayın hızlı genişlemesi, küreselleşen günümüz dünyasını dönüştürmüş ve çok uluslu şirketlerin dinamiklerini şekillendirmede oynadığı rolün daha yakından incelenmesini gerektirmiştir. Endüstri 4.0, tüm sektörler, teknolojik yenilikler, çok uluslu şirketler ve devletler arasındaki rekabet dinamikleri ve küresel jeopolitik ortamı yeniden tanımlamıştır. Endüstri 4.0 ilerlemeleriyle gelişmeye devam ederken, çok uluslu şirketlerin faaliyetlerini, girişimlerini ve geleceğini şekillendirmeye katkıda bulunmaktadır. Eşzamanlı olarak ulus devletler, kritik altyapıların siber güvenliğini acil bir ulusal güvenlik sorunu olarak kabul etmekte, siber uzayı ekonomik ve teknolojik üstünlük için bir rekabet alanı olarak kullanmakta ve kendilerini sektörlerde lider olarak konumlandırmak için rekabet etmektedir. Bu bağlamda endüstri paydaşları arasında yer alan müşteriler, çalışanlar, şirket sahipleri, rakip şirketler, tedarikçiler, toplum, finansörler ve devletler bu dönüştürücü çağda inovasyon, güvenlik ve küresel rekabet gücünü dengeleyen stratejiler geliştirmektedir.

Çok uluslu şirketlerin etkisi, faaliyet gösterdikleri sektörlerin ötesine uzanmakta ve siber uzayda ulus devletler üzerinde etkileri bulunmaktadır. Hükümetler, çıkarlarını destekleyen ve koruyan politikalar geliştirerek, genellikle çok uluslu şirketlerin ekonomik ve stratejik değerini kabul etmektedir. Örneğin, hükümetler kritik altyapıyı ve ulusal güvenlik çıkarlarını korumak için çok uluslu şirketlerle aktif olarak siber güvenlik işbirliklerinde bulunurlar. Ek olarak, çok uluslu şirketler tarafından üretilen vergi gelirleri ve istihdam olanakları, ulus devletlerin genel ekonomik gelişimine katkıda bulunur.

Siber uzayda çok uluslu şirketlerin çoğalması, ulus devletler arasındaki çıkarlara ve rekabete yol açmaktadır. Pazar hakimiyet, teknolojik gelişmeler ve fikri mülkiyet hakları üzerinde rekabete, stratejik çatışmalara ve siber güvenlik tehditlerine yol açmaktadır. Ulus devletler, rekabet avantajı elde etmek ve ekonomik çıkarlarını korumak için siber vekiller aracılığıyla siber casusluk ve siber saldırı faaliyetlerinde de bulunmaktadır. Siber saldırıların yanı sıra ulus devletler, ittifaklar yoluyla veya kısıtlayıcı dış politikalar aracılığıyla rakip bir jeopolitik güce karşı önlemler alabilmektedir.

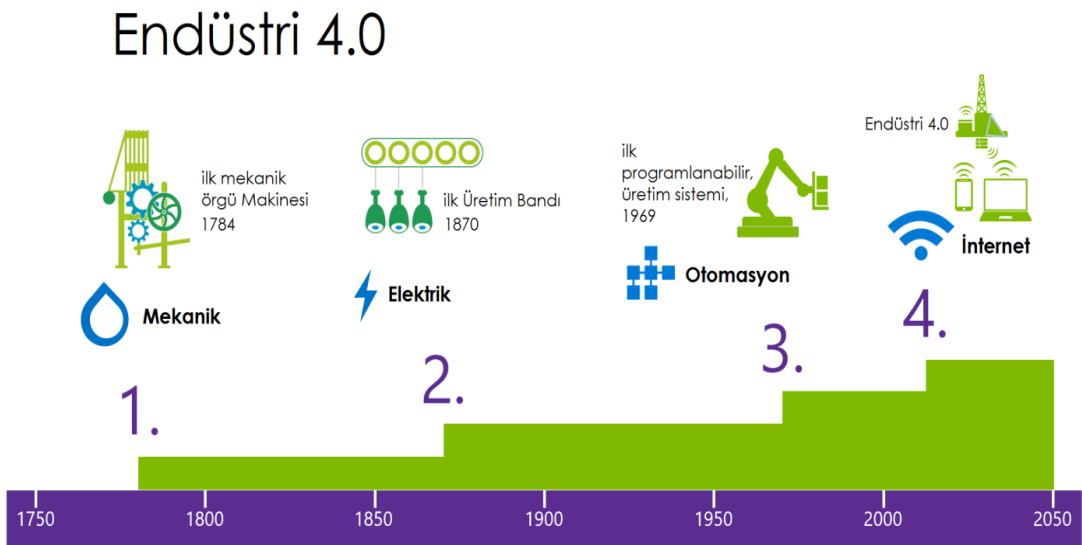
İnovasyon ve teknolojik ilerlemelerin küresel çatışmalar, rekabetler ve stratejik karar verme üzerindeki derin etkisi göz önünde bulundurularak, bu araştırma

teknolojik gelişmeler bağlamında ulus devletler arasındaki çıkarları ve rekabetleri derinlemesine incelemektedir. Aynı zamanda çok uluslu şirketlerin hayati rolünü ve ulus devletlerle etkileşimini de inceleyerek siber uzayın dinamikleri hakkında bilgiler sağlamaktadır. Otomotiv, finans, telekomünikasyon, bilgi ve iletişim teknolojileri, enerji sektörlerine odaklanan bu çalışma, çok uluslu şirketlerin siber uzaydaki önemini ve siber uzaydaki etkinin kapsamlı bir şekilde anlaşılmasını sağlamayı amaçlamaktadır.

3.1. Endüstri 4.0

Teknolojinin hızlı gelişimi, Endüstri 4.0 olarak bilinen yeni bir endüstriyel dönüşüm çağını başlatmıştır ve siber uzayda çok yönlü bir etki yaratmıştır. Alman endüstrisi ile ilgili sıklıkla kullanılan ve Dördüncü Sanayi Devrimi'ni ifade eden Endüstri 4.0 terimi, ilk olarak 2011 yılında Hannover Fuarı'nda kullanılmıştır. Genel olarak siber-fiziksel sistemlerin ve dijital teknolojilerin endüstriyel sistemlere ve fiziksel ekipmanlara entegrasyonunu, geleneksel üretim yönteminden bilgisayar ve internet destekli yeni üretim modeline geçişi sağlayan bir teknoloji projesi olarak başlamıştır (Akçacı, 2017, s. 53).

Şekil 12: Endüstri 4.0'ın Evrimi



Kaynak: Tecim, V. (tarih yok). Endüstri 4.0. <https://vahaptecim.com.tr/endustri-4-0/>

Endüstri 4.0 öncesinde toplum, art arda mekanik çağını, elektrik çağını ve bilgi teknolojileri çağını yaşamıştır. Hayat standartlarının gelişmesiyle birlikte toplum; insan ve hayvan gücü gibi doğal güçler yardımıyla yapılan işlerin makine gücü ile gerçekleştirilmesi, elektrikle güç sağlama süreci ve bilgi teknolojileri kullanımında deneyim kazanmıştır. Dördüncü sanayi devrimi sırasında devrim niteliğinde bir araç olan internetin üretim sürecine derinden dahil olmasıyla birlikte, endüstriyel kontrol süreçlerinin daha akıllı hale gelmesi ve üretimin dijitalleşmesi, insanların ürünleri üretme şeklini tamamen değiştirmiştir. Sanayi devriminin geçirdiği her evrimin içeriği farklı olsa da amaçları, üretim verimliliğini artırmak ve süreçteki üretim maliyetlerini azaltmak için üretici faktörlerin gelişimini desteklemektir (Zhou, Liu, & Liang, 2016, s. 172).

Dijital dönüşüm, üretimde ileri teknolojilerin geliştirilmesini ve kullanılmasını sağlayarak, Dördüncü Sanayi Devrimi'nin yolunu açmıştır. Endüstri 4.0, insanların, makinelerin ve siber-fiziksel sistemlerin birbirine bağlı bir sistemde işbirliği içinde çalıştığı akıllı fabrikaları ifade etmektedir. Endüstri 4.0'ın temel önermesi de şirketlerin, yeni teknolojiler aracılığıyla akıllı ağlar oluşturarak fiziksel ve dijital alanın birleştirilmesiyle insanları, makineleri ve sistemleri birbirine bağlamasını sağlamaktır. Bu bağlamda günümüzde geleneksel üretim ve ürünlerinin geçirdiği dönüşüm, üretim sürecinde milyarlarca makine ve sistem birbirleriyle iletişim kurarak, bilgi paylaşarak ve birbirini kontrol ederek gelişme göstermektedir. Sembol ürünler olarak akıllı telefonların, endüstriyel robotlar, elektrikli ve bağlantılı arabaların, akıllı elektrik sistemlerinin üretimi Endüstri 4.0'ın başlıca çıktılarıdır (Ermağan, 2022). Bu örnekler hem fiziksel bir ürün olarak ortaya çıkarlar hem de yazılım ve internet desteği sayesinde tüketiciye ve endüstriye yönelik yenilikçi ve rekabetçi çözümler sunarlar, aynı zamanda veri paylaşımı, bağlantılılık, konfor ve maliyet desteği sağlar.

Şekil 13: Endüstri 4.0 Teknolojileri



Kaynak: <https://www.otonomfabrika.com/endustri-4-0-teknolojileri-bilesenleri/>

Aksahan'a (2021) göre, Endüstri 4.0 ile başlayan dijital dönüşüm, her alanda uygulanabilen dijital bir alanda verilerin gözlemlenmesi ve toplanması için gerekli siber altyapının hazırlanmasını içermektedir. En basit tanımıyla akıllı cihazların birbiri ile haberleşmesini sağlayan **Nesnelerin interneti teknolojisi**, akıllı sensörlerden gelen verileri kullanarak birbirleriyle iletişim kurabilen akıllı cihazlardan oluşmakta, yapay zeka ve veri analitiği gibi diğer teknolojiler için önemli bir girdi görevi gören çeşitli kaynaklardan veri toplanmasını kolaylaştırmaktadır. Nesnelerin interneti tarafından sağlanan büyük verilerin toplanıp güvenli bir şekilde saklandığı şeffaf bir veri tabanı sistemi olan **blok zinciri teknolojisi** dijitalleşmenin temelinde yer almaktadır. **Yapay zeka teknolojisine** sahip sistemler, saklanan geçmiş verileri işledikten sonra kendi kendine öğrenerek sonuç çıkaran ve geleceğe yönelik tahminlerde bulunan bir teknolojidir. Yapay zeka sistemleri, çok büyük verileri analiz ederek, süreçleri otomatikleştirebilir ve akıllı kararlar alabilir. **Büyük veri** ise binlerce sensörle ortaya çıkmaktadır. Ancak büyük veri, tamamen kaliteli bir veri bütünlüğünü içermemektedir. **Büyük veri analitiği**, yüksek kaliteli verilerin yapay zeka ile çalışan sistemlere iletilmesi için kullanılan analiz yöntemlerinin tümünü içerir. **Bulut bilişim** sistemlerinde, büyük veri analitiği çalıştırılarak verilerin işlenmesini ve analiz edilmesini sağlar. Ayrıca ölçeklenebilir depolama ve bilgi işlem gücü sağlayarak işletmelerin büyük hacimli verilere verimli bir şekilde erişmesine ve bunları analiz etmesine olanak tanır. **Simülasyon** oluşturmak ve sistemi gözlemlemek için ise Dijital

İkiz teknolojisi ortaya çıkmıştır. Nesnelerin interneti ve bulut bilişim teknolojilerinden toplanan veriler, fiziksel nesnenin tüm özelliklerine sahip bir dijital ikizin veya sanal bir kopyanın oluşturulmasında önemli rol oynamaktadır. **Sanal gerçeklik teknolojisi**, simülasyonu oluşturulmuş 3 boyutlu sanal ortamlarda giyilebilir teknolojiler aracılığıyla gerçeklik hissinin yaşanmasını sağlamakta ve bu deneyimle tehlikeler ve riskler azaltılmaktadır. **Eklemeli imalat** olarak da bilinen 3D baskı teknolojisi, prototip, kalıp yapımı ve parça imalatında kullanılarak üretim süresini kısaltmak için kullanılır ve fiziksel nesnelerin dijital tasarımlara dayalı olarak katman katman üretilmesini sağlar. Bahsi geçen tüm teknolojilerin ortak açığı olan **siber güvenlik**, ağları, cihazları, sistemleri, veri gizliliğini ve hatta bireyleri koruyan, tüm dijital ekosistemin bütünlüğünü ve güvenliğini koruma ihtiyacı ile birlikte sürece paralel gelişen Endüstri 4.0'ın diğer önemli bir çıktısıdır (Aksahan, 2021).

Endüstrinin dijital dönüşümü, yeni teknolojilere dayanmaktadır. Endüstri 4.0'da 9 teknoloji dahil çeşitli teknolojileri kullanarak siber-fiziksel bir ortam oluşturmak için bilgi teknolojisi ve operasyonel teknolojiyi birleştirmektedir. Endüstri 4.0'ın merkezinde yer alan bu teknolojiler; bilişim teknolojileri, telekomünikasyon, bilgisayarlı makineler, robotlar, otonom araçlar, gelişmiş tıbbi cihazlar, tarım, uzay ve havacılık teknolojisi, enerji, finans, ulaşım gibi birçok kritik altyapıya entegrasyonunu zorunlu kılmaktadır. Dolayısıyla Endüstri 4.0, insan yaşamının tüm sektörlerini ve yönlerini kapsamlı bir şekilde etkilemiş, teknolojiye, küresel pazarda ve toplumda birbirine bağlı bir değişim meydana getirmiştir.

Tablo 2: Endüstri 4.0'da üretim değişiminin gelişimi

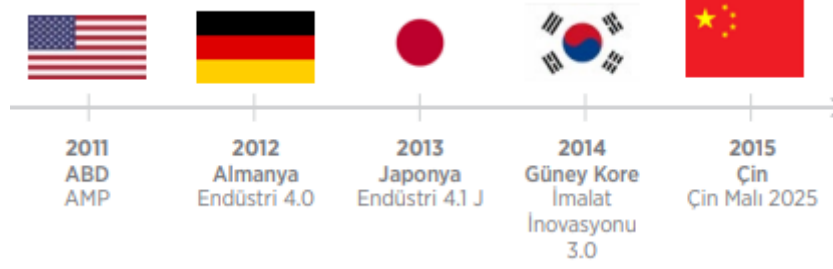
Geliştirme Eğilimleri	Gelişim Eğiliminin İçeriği
"Fiziksel"den "bilgi"ye	Siber-fiziksel sistemler, fiziksel dünyayı ve bilgi dünyasını entegre hale getiren Endüstri 4.0'ın çekirdeğidir, bu nedenle gelecekteki üretim daha fazla bilgi odaklı olacaktır.
"Kamu"dan "özel"e	Gelecekteki üretim, kullanıcıların ihtiyaçlarına göre daha fazla odaklanacak, kullanıcılar daha fazla kişiselleştirilmiş ürünlere ihtiyaç duyacak, bu nedenle büyük ölçekli üretim, küçük ölçekli üretim özelleştirmesine dönüşecek.
"Donanım"dan "yazılım"a	Gelecekteki üretim, ürünlerin katma değerini oluşturmak, hizmetleri ve çözümleri genişletmek için yazılım yoluyla desteklenecek daha büyük miktarda yazılıma ihtiyaç duyar.
"Kablolu"dan "kablosuz"a	Sensör ağları, mobil iletişim ağı ve diğer ağlar gibi endüstriyel üretim sürecinde giderek daha fazla kablosuz ağ yer almaktadır. Kablolu ağlara göre kablosuz ağlar daha kullanışlı daha düşük maliyetlidir.
"Küçük veri"den "büyük veri"ye	Geleceğin üretimi çok çeşitli verilere dayanacak, büyük verilerle daha akıllı ürünler yaratılacak.

Kaynak: (Zhou, Liu, & Liang, 2016, s.10)

3.1.1. Ulus Devletlerin 4.0 Stratejileri

Gelişmiş ülkeler için imalat, Gayri Safi Milli Hasıllarında (GSMH) hayati bir rol oynamaktadır. Yeni teknolojilerin gelişmesiyle birlikte, akıllı endüstriyel ekipmanlar, küresel üretimin temeli olacak şekilde geliştirilmekte ve Dördüncü Sanayi Devrimi'ni benimsemiş ülkeler, yeni sanayi devrimi çerçevesinde gelişimini destekleyecek politikalar ve yeni üretim modelleri ortaya koymaktadır (Zhou vd., 2016, s. 172).

Şekil 14: Dördüncü Sanayi Devrimi Hangi Ülkede Ne Zaman Başladı?



Kaynak: <https://www.ttgiv.org.tr/tur/images/publications/606ad2c302d2a.pdf>

Dünya Ekonomik Forumu ve danışmanlık firması McKinsey ile işbirliği içinde yayınlandığı "Küresel Deniz Feneri Ağı: Büyüme için Operasyonları Yeniden Tasarlamak" adlı raporuna göre; şu anda Dördüncü Sanayi Devrimi teknolojilerini kullanan liderler olarak görülen dünya çapında 69 fabrikadan 20'sine Çin, 19'una AB üye ülkeleri, 7'sine ABD, 2'sine Japonya ev sahipliği yapmaktadır (Betti & Boer, 2021, s. 8-9).

3.1.1.1. Almanya - Endüstri 4.0

Dördüncü Sanayi Devrimi'nin öncüsü olan Almanya, 2011 yılında Endüstri 4.0 Stratejisi (Industry 4.0) olarak bilinen "*Yüksek Teknoloji Stratejisi 2020*" ile bilim ve endüstri arasındaki bağların artırılmasını hedeflemiş ve bu kapsamda 200 milyon avro bütçe oluşturmuştur (Yıldız, 2018, s. 554). Yapay zeka temelli "*Akıllı fabrikaları*" teşvik etmeye odaklanan strateji, fabrikaları, müşterileri, Ar-Ge'yi birbirine bağlayan bir üretim sistemini oluşturmak için büyük şirketlerin ve KOBİ'lerin üretimde IoT ve siber-fiziksel sistemleri uygulayarak işbirliği yapmasını hedeflemektedir (Moon, Chung, & Choi, 2018, s. 27). Özellikle Bosch, Siemens, Mercedes, BMW gibi dev markaların hem ülke gelirine hem de ülke istihdamına sağladığı katkılar, Almanya'nın Endüstri 4.0 girişimindeki öncü konumunu göstermektedir (Yıldız, 2018, s. 554).

3.1.1.2. ABD - Gelişmiş İmalat Ortaklığı

2011'de ABD, 21. yüzyılda üretim liderliğine yönelik hazırladığı yeni teknolojilere yatırım yapmak için endüstriyi, akademisyenleri ve federal hükümeti bir araya getirmeyi amaçlayan "*Gelişmiş Üretim Ortaklığı (Advanced Manufacturing Partnership - AMP)*" politikasını başlatmıştır. İmalat endüstrisi kapsamında

oluşturulan strateji, yüksek kalite üretim yapmak ve küresel rekabet gücünü artırmak için gelişen teknolojilere odaklanmaktadır.

500 milyon dolar yatırım yapılan projede, (I) yerli üretim kapasitelerinin oluşturulması, ürünlerin imalatında kullanılan yerli üretim kapasitelerinin geliştirilmesi, (II) gelişmiş malzemelerin üretim süresinin azaltılması, ürünlerin imalatında kullanılan gelişmiş malzemelerin daha hızlı üretilebilmesi, (III) ürünleri test etmek için gereken süreyi önemli ölçüde azaltacak yeni teknolojilerin geliştirilmesi, (IV) yeni nesil robot biliminde ABD'nin liderliğinin sağlanması ve bu alandaki gelişmelere odaklanması, (V) üretim sürecinde enerji verimliliğinin artırılması için önlemler alınması temel amaçlar olarak belirlenmiştir (The White House, 2011a, s. V). ABD, 2014 yılında ise üretimdeki yeniliklerin ilerlemesini, personel eğitimini ve endüstriyel ortamı şekillendirmeyi teşvik etmek amacıyla yenilenmiş AMP 2.0 politikasını oluşturmuştur (Manufacturing USA, 2014).

ABD'nin Dördüncü Sanayi Devrimi stratejisinde General Electric (GE) başarılı bir uygulama örneğidir. GE'nin stratejik yenilikçi modeli ise Endüstri 4.0 yerine "*Endüstriyel İnternet*" olarak tanımlanmaktadır (Evans & Annunziata, 2012). GE, "Bağlantılı Sanayi Şirketi" olma başarısını elde etmiş, bulut ve yapay zekayı uygulayarak üretim sürecini yönetmeyi başarmıştır. 2014 yılında GE dahil olmak üzere Cisco System, Intel, AT&T, IBM, Microsoft bir araya gelerek Endüstriyel İnternetin büyümesini hızlandırmak, uygulanmasında işbirliği yaparak standartları oluşturmak ve uluslararası imalat endüstrisini geliştirmek için "Endüstriyel İnternet Konsorsiyumu" kurmuştur (Moon vd., 2018, s. 28).

3.1.1.3. Japonya - Endüstri 4.1J ve Yeni Robot Strateji Planı

Endüstri 4.1J, Japon Sanal Mühendislik Topluluğu (VEC), Nippon Telgraf ve Telefon Şirketi (NTT) İletişim şirketleri tarafından başlatılmıştır. Endüstri 4.1J, dünyanın dört bir yanındaki üretim tesislerini birbirine bağlamak için bir bulut sistemi kurmayı hedeflemektedir (Chien, Hong, & Guo, 2017 , s. 552). Bu sistemde ilk olarak ilgili verileri toplamak için kontrol sistemi kullanılacak, ikinci olarak veriler kaydedilerek bulut platformuna toplanacak, üçüncü olarak analiz gerçekleştirilecek ve son olarak uzmanlar olay tespiti, arıza nedenlerinin analizi ve üretimin yenilenmesi, güvenlik iyileştirmesi için öneriler sunarak iyileştirmeler gerçekleştirecektir. "4.1."

güvenlik seviyesinin Endüstri 4.0'dan daha yüksek olduğu ve "J" Japonya'ya ait olduğu anlamını taşımaktadır (Science and Technology Law Institute, tarih yok).

Dünyadaki en fazla sayıda robota sahip Japonya, robot teknolojisinde bir dünya lideri sayılmaktadır. Robot teknolojisindeki lider konumu daha da güçlendirme hedefiyle Japonya, 2015'te Yeni Robot Stratejisini duyurmuştur. Japonya'nın yeni robot stratejisi üç temel hedef ortaya koymaktadır: *"dünya robotik inovasyon üssünü kurmak, dünyanın ilk robot uygulama devleti olmak, dünyanın önde gelen robotunun yeni bir çağına doğru gelişme göstermek"*. Bu üç temel hedefe ulaşmak için ise beş yıllık bir plan geliştirilmiştir: (I) Robot teknolojisi projelerine 100 milyar yen devlet ve özel sektör yatırımı, (II) Robot teknolojisi pazarına yıllık 650 milyar yen yatırımı 2,4 trilyona yükseltmek, (III) Fukuşima'da yeni bir robot test alanı inşa etmek, (IV) Dünya Robot Zirvesi'ni düzenleyerek inovasyonu kolaylaştırmak ve kamu uygulamalarını hızlandırmak, (V) Robotların ilk tanıtımı için maliyetleri %20 oranında azaltmak ve robotların tanıtılmasına yardımcı olmak için insan sayısını 2020 yılına kadar 30.000'e çıkartmak (Ministry of Economy, Trade and Industry (METI) Government of Japan, 2018). Uluslararası Robotik Federasyonu'nun (International Federation of Robotics-IFR) 2022 tarihli raporuna göre, Japonya küresel endüstriyel robot arzının %45'ini üretmektedir. Bu üretim oranı ise Japonya'yı dünyanın en büyük endüstriyel robot üreticisi konumuna getirmektedir (International Federation of Robotics [IFR], 2022).

3.1.1.4. Güney Kore - İmalat Sanayi İnovasyonu 3.0

Güney Kore, dünyada gemi üretimi, otomotiv, elektronik, kimya, çelik ve diğer bazı endüstriler başta olmak üzere küresel imalatla en gelişmiş ülkelerden biridir. Ancak Dördüncü Sanayi Devrimi ile birlikte diğer gelişmiş ülkelerdeki imalat endüstrisinin kademeli olarak artış göstermesi sebebiyle rekabet gücünde ciddi bir düşüş başlamıştır. Böyle bir uluslararası arenada Güney Kore 2014 yılında resmi olarak İmalat Sanayi İnovasyonu 3.0 (Manufacturing Innovation 3.0) stratejisini başlatmıştır. Strateji, imalat ve bilgi teknolojilerinin entegrasyonunu teşvik ederek yeni endüstriler yaratmak, akıllı fabrika kullanımını genişletmek, insansız hava araçları, robotlar, IoT, 3D baskı, büyük veri ile ilgili temel teknolojileri geliştirmek dahil olmak üzere, üretim sürecine yenilik getirmeyi ve imalat endüstrisinde yumuşak gücünü artırmayı amaçlamıştır (Zhou vd., 2016, s. 175).

3.1.1.5. Çin Halk Cumhuriyeti - Çin Malı 2025

Almanya'nın akıllı imalat endüstrisi için Endüstri 4.0 planından ilham alan Çin Malı 2025 (Made in China 2025), dönemin Çin Başbakanı Li Keqiang tarafından Mayıs 2015'te açıklanmıştır. Strateji, Çin'in ileri teknoloji endüstrilerindeki rekabet gücünü artırmayı ve ülkenin üretim mallarını değer zincirinde üst seviyelere taşımayı amaçlayan stratejik bir plandır. Yabancı teknoloji bağımlılığını azaltma, yerli üretim alternatifleriyle yabancı teknolojilerin değiştirilmesi ve Çinli yüksek teknoloji üreticilerinin küresel hakimiyetini teşvik etme isteği doğrultusunda Çin Malı 2025 stratejisini ana hedefleri, temel çekirdek bileşenlerin ve önemli temel malzemelerin yerli üretimini 2025'e kadar %70'de çıkartmak ve 2049 yılına kadar küresel pazarlarda hakim bir süper güç olmaktır (Springborg, 2018).

ABD, diğer gelişmiş ülkelerdeki politika yapıcılar ve güvenlik uzmanları, Çin'in ileri teknolojide baskın bir oyuncu olma çabalarını giderek artan bir şekilde ulusal güvenlik sorunu olarak görmektedir. Çünkü Çin'in, küresel pazarlarda baskın bir konuma ulaşma çabası; Batılı şirketleri ve teknolojileri satın almaya yönelik yatırımları; birçok Batı, Amerika ve Asya bölgesindeki ülkelerle ikili anlaşmalar yoluyla ekonomik katkılarda bulunması; Çin ürünlerinin daha düşük maliyeti olması ve bu durumun da ulusal şirketlerin bu ürünlerle rekabet etmesini zorlaştırması nedeniyle Çin Malı 2025 tehdit olarak ve ticaret savaşının temeli olarak görülmektedir.

ABD hükümeti, Çin'in kendi yüksek teknoloji imalat sektörünü hızla geliştirmek için yabancı teknoloji firmalarına yatırımını artırmayı planladığı Çin Malı 2025 politikasını, yabancı yatırıma yönelik ayrımcı muamele gösterdiğini, zorunlu teknoloji transferine sebep olduğunu, projenin fikri mülkiyet hırsızlığına ve siber casusluğa dayandığını savunarak kınamıştır (McBride & Chatzky, 2019). Bu doğrultuda 2018'de ABD istihbarat teşkilatları, Çin'in ABD firmalarını hedef alarak gerçekleştirdiği satın almaların, ABD için benzeri görülmemiş bir tehdit oluşturduğunu açıklamıştır (Masters, McBride, & Berman, 2023). ABD Ticaret Temsilcisinin 22 Mart 2018'de yayınladığı "Bölüm 301" raporunda, Çin'in politika hedefleri doğrultusunda ABD ticaret ağlarına siber casusluk faaliyetleri düzenlediği, bu siber saldırılar aracılığıyla Çin hükümetinin çeşitli ticari sırlara, teknik ve hassas verilere erişim elde ettiği iddia edilmektedir (Office of the US Trade Representative [USTR], 2018, s. 153).

Bir ulus devletin endüstrilerde hakimiyet arayışı çerçevesinde, tüm tedarik zincirini kontrol edebilme, fiyatları manipüle edebilme, temel kaynaklara erişimi kısıtlayabilme veya kritik teknolojilerin geliştirilmesi ve üretilmesi üzerinde etkili olabilme potansiyeli, rakip ulus devletler tarafından endişelere yol açmaktadır. Genel olarak politika yapıcılar, Çin'in küresel tedarik zincirinin kritik sektörlerini kontrol etme hırsından ve endüstrinin rakip jeopolitik gücün kontrolü altına girme olasılığından endişe duymaktadır. Çünkü bu endişeler diğer ülkelerdeki endüstrilerin tedarik ürünleri için Çin'e bağımlı hale geldiği, güvenlik açıkları yarattığı ve potansiyel olarak ulusal güvenliklerini ve ekonomik rekabet güçlerini baltaladığı bir duruma yol açabilir. Örneğin kobalt endüstrisi, akıllı telefonlar, yenilenebilir enerji sistemleri, elektrikli araçlar gibi birçok elektronik cihazda kullanılan lityum pillerin üretimi için önemlidir. Bu hammaddeye olan talep artmaya devam ettikçe sürdürülebilir kobalt arzını güvence altına almak çok daha önemli hale gelmektedir. Çin ise büyük bir kobalt üreticisi olan Demokratik Kongo Cumhuriyeti gibi ülkelerde kobalt madenciliğine aktif olarak yatırım yapmaktadır. Bu durum Çin'in kobalt tedariklerini kontrol etme ve potansiyel olarak fiyatları manipüle etmeye veya bu kritik hammaddeye erişimi kısıtlama becerisine ilişkin endişeleri artırmaktadır.

3.1.2. Siber Uzayda Endüstri 4.0 ve Siber Casusluk

Siber uzay, artan teknolojik gelişmelerin bir sonucudur. İletişim ve bilgisayarlı sistemler küresel bir imalat ortamı oluşturmak için birbirine bağlanmakta ve bu doğrultuda siber uzay çeşitli düzeylerde gelişmeye devam etmektedir. Birbirine bağlı sistemler, ağların çoğalması, bilgi trafiğindeki büyüme, yaygın bağlantı düzeyi, mobil uygulamaların çeşitliliği de siber uzayın genişlemesine katkıda bulunmaktadır. Ancak siber uzay, sayısız avantajının yanı sıra yeni tehditleri ve meydan okumaları da beraberinde getirmektedir. Dolayısıyla siber uzaydaki veya dijital ortamdaki bilgilerin sabote edilmesinden, siber uzay yetenekleriyle fiziksel varlıklara zarar verilmesine kadar düşmanca faaliyetler için yeni bir alan sunar. Dolayısıyla siber uzayın kullanımı artıkça, ulusal kritik altyapılara, veri tabanlarına, endüstriyel operasyonlarına, komuta ve kontrol sistemlerine yönelik tehditler ve endüstriyel casusluk faaliyetleri de artmaktadır (Argaman & Siboni, 2014, s. 44).

Bilginin önemine ve değerine odaklanan Bilgi Teknolojileri dallarının yanı sıra Endüstri 4.0'da asıl süreç, güvenlikten önce üretim olmuştur. Genel olarak, bilgi teknolojileri sistemlerinin, operasyonel teknoloji sistemleriyle entegrasyonu Endüstri 4.0'ın başarısı için çok önemlidir (Gönen, Yılmaz, Seda, Karacayılmaz, & Özbirinci, 2021, s. 1150). Dolayısıyla Endüstri 4.0'ın temelinde siber-fiziksel sistemlerin oluşumu mevcuttur. Bu oluşum fiziksel cihazların, endüstriyel internete bağlanmasını sağlayabilir ve böylece fiziksel cihazlar bilgi işlem, iletişim, hassas kontrol ve uzaktan koordinasyon gibi işlevlere sahip olduğunda sanal dünya ve gerçek fiziksel dünya arasında yakın entegrasyon elde edilir. Bununla birlikte Endüstri 4.0'ın sağlaması gereken bir diğer önemli unsur siber güvenlidir. Dördüncü Sanayi Devrimi'ndeki dijital dönüşüm hızı, siber saldırıların her zamankinden çok daha kapsamlı etkilere sahip olabileceğini, üreticilerin ve tedarik ağlarının da siber tehditlerle karşı karşıya olabileceği anlamına gelmektedir. Tedarik zincirleri, fabrikalar, müşteriler ve operasyonlar birbirine bağlandığında, siber tehditlerin oluşturduğu riskler çok daha büyüktür (Deloitte, 2017).

2009'da gerçekleşen Stuxnet saldırısında kötü amaçlı yazılım, USB bellek aracılığıyla bağımsız ağlara yüklenerek, üretim ağlarına otonom bir şekilde yayılmasını sağlamış ve nükleer zenginleştirme tesisindeki santrifüjlerin hızını değiştirerek kontrolden çıkmasına sebep olmuştur. Bu örnek, siber saldırıların birbirine bağlı fiziksel fabrikalarda bir silah olma potansiyelini gösteren önemli bir vakadır (Deloitte, 2017).

Siber casusluk, siber tehdit aktörleri tarafından dijital ortamlardaki bilgilerin haksız yere ele geçirilmesi veya sabote edilmesini içermektedir. Endüstri 4.0 kapsamında imalat sektörünün ticari sır olarak tanımladığı bilgiler, siber casusluğun alanına girmektedir. Siber casusluk, aynı zamanda fabrikaların araştırma ve geliştirme faaliyetleri ve veri tabanları için de bir tehdittir. Endüstri 4.0, çok sayıda akıllı ve bağlantılı iş sürecini barındırdığı için, siber uzayda geleneksel üretime göre daha fazla savunmasızdır. Endüstri 4.0 tabanlı imalat şirketleri için ürün bilgileri ve teknik özellikler gibi üretim altyapısına ilişkin belirli bilgilerin siber casusluk yöntemleriyle çalınması çok olasıdır (Ateş, Bostancı, & Güzel, 2020, s. 41).

Siber uzayın önemli casusluk aracı haline gelmesi, yabancı istihbarat servisleri, devlet destekli siber tehdit aktörleri veya şirketlerin rekabet gücü ve ekonomik kazanç

elde etme çerçevesinde, diğer ulus devletlere ve şirketlerine karşı teknolojik gelişimin bir parçası olarak faaliyetler yürütmesinden kaynaklanmaktadır. Devletler arasındaki siber uzay casusluğu hakkında çok fazla bilgi ortaya çıkmıştır. Özellikle ABD ve Çin arasındaki siber çatışmalar, endüstriyel casusluğun genel olarak devletlerin küresel hakimiyet çabasının birincil aracı haline geldiğini ve ekonomi savaşlarında bir silah olarak hizmet ettiğini göstermektedir (Argaman & Siboni, 2014, s. 44).

ABD'nin Siber Uzayda Dış Ekonomik Casusluk raporuna göre Rusya, Çin ve İran, ABD'nin ticari sırlarını ve teknolojik verilerini potansiyel hırsızlığıyla bağlantılı en yetenekli aktif üç siber aktör olarak belirlenmiştir (National Counterintelligence and Security Center [NCSC], 2018).

Mayıs 2022'de bir ABD merkezli siber güvenlik firması olan Cybereason, Çin hükümeti tarafından desteklendiği iddia edilen bir bilgisayar korsanlığı grubunun üç kıtada fikri mülkiyet hırsızlığı ve endüstriyel casusluk faaliyetlerini ortaya çıkardığını açıklamıştır. Bu faaliyetler, ABD, Avrupa ve Asya'daki teknoloji ve üretim şirketlerini hedef alan patent ve ürün ayrıntıları, kaynak kodları, teknoloji planları ve üretim talimatları gibi hassas verilerin elde edilmesine yönelik çabaları içermektedir (Ben-David, 2022).

3.2. Otomotiv Sektörü

3.2.1. Endüstri 4.0'ın Otomotiv Sektörüyle Entegrasyonu

Yıllar boyunca otomotiv endüstrisinde çok sayıda yenilikler yaşanmıştır; 1886'da Avusturyalı Karl Benz tarafından içten yanmalı bir motorla çalışan ilk araba, 1908'de dünyanın montaj hattında üretilen ilk otomobili Ford Model T, 1921'de kablosuz elektrikle çalışabilen çakmaklar, 1930'da araba radyosu, 1949'da araba anahtarları, 1953'te klima, 1958'de sürücünün gaz pedalını kullanmadan sabit bir hızı korumasını sağlayan hız sabitleyici, 1959'de emniyet kemerleri, 1960'da elektrikli camlar, 1969'da otomatik ön cam silecekleri, 1971'de kilitlenmeyi önleyici fren sistemi, 1984'te CD çalarlar, 1988'de hava yastıkları, 1996'da bağlantılı arabalar (General Motors bir kazada 911'i arama yönlendirmesi için bağlantılı arabaları piyasaya sürmüştür), 2000'de GPS uydulu navigasyon sistemi, 2001'te bluetooth, 2003'te otomatik park etme (Toyota sürücülerin paralel park etmesine yardımcı Akıllı

Park Yardımı teknolojisini ilk kez piyasaya sürmüştür), 2014 Tesla tarafından otomatik pilot icat edilmiştir (Jardine Motors Group, tarih yok).

Dijitalleşme süreci, yeni ve değişkenlik gösteren fikirlerle birlikte, ağ ile kalıcı bir bağlantıyı da gerektirmektedir (Haas & Möller, 2017). Endüstri 4.0 ile otomotiv endüstrisi, mekanik tabanlı üretimden yazılım tabanlı bir üretime geçerek dijital dönüşüm olanaklarını genişletmiştir. Büyük dijital dönüşüm geçiren otomotiv endüstrisinin geleceğinde *bağlantılı arabalar, otonom sürüş, paylaşımlılık ve elektrikli araç teknolojisi*⁷ temel yapı taşlarını oluşturmaktadır.

3.2.2. Otomotiv Endüstrisinde Uluslararası Rekabet Gücü ve Etkileri

Endüstri 4.0'ın yönlendirdiği hızlı teknolojik yenilik, otomotiv sektörüne hakim olan çok uluslu şirketlerin ortaya çıkmasına ve rekabetin otomotiv sektörü üzerinde bir etki yaratmasına neden olmuştur. Dolayısıyla otomotiv sektöründeki çok uluslu şirketler, inovasyonu yönlendirmek, üretim süreçlerini optimize etmek ve rekabet avantajı elde etmek için ileri teknoloji sistemlerine milyarlarca dolar yatırım yapmakta, küresel erişimlerini ve AR-GE yeteneklerini geliştirmekte, dijitalleşmeye ve yazılım geliştirmeye daha fazla odaklanmaktadır. Otonom sürüş uygulamaları, bağlantılı araçlar, araç paylaşım modelleri gibi değişiklikler ve teknolojik gelişmeler, rekabetle karşı karşıya kalan otomobil üreticilerinin inovasyon zorunluluğunu şekillendirmektedir (Organisation for Economic Cooperation and Development [OECD], 2017). Aynı zamanda Endüstri 4.0, otomotiv sektöründe ekonomik hakimiyet ve teknolojik liderlik için ulus devletler arasındaki rekabeti yoğunlaştırmış ve hükümetler, ulusal otomotiv endüstrilerini desteklemek için inovasyon ekosistemlerini, üretim yeteneklerini güçlendirmeye, doğrudan yabancı yatırımı çekmeye odaklanmıştır.

En değerli ve en güçlü 100 otomobil markasını sıralayan marka değerlendirme danışmanlığı Brand Finance'in Otomotiv Endüstrisi 2022 raporuna göre (Brand Finance, 2022);

⁷ACES teknolojisi; Automation, connectivity, electrification, sharing

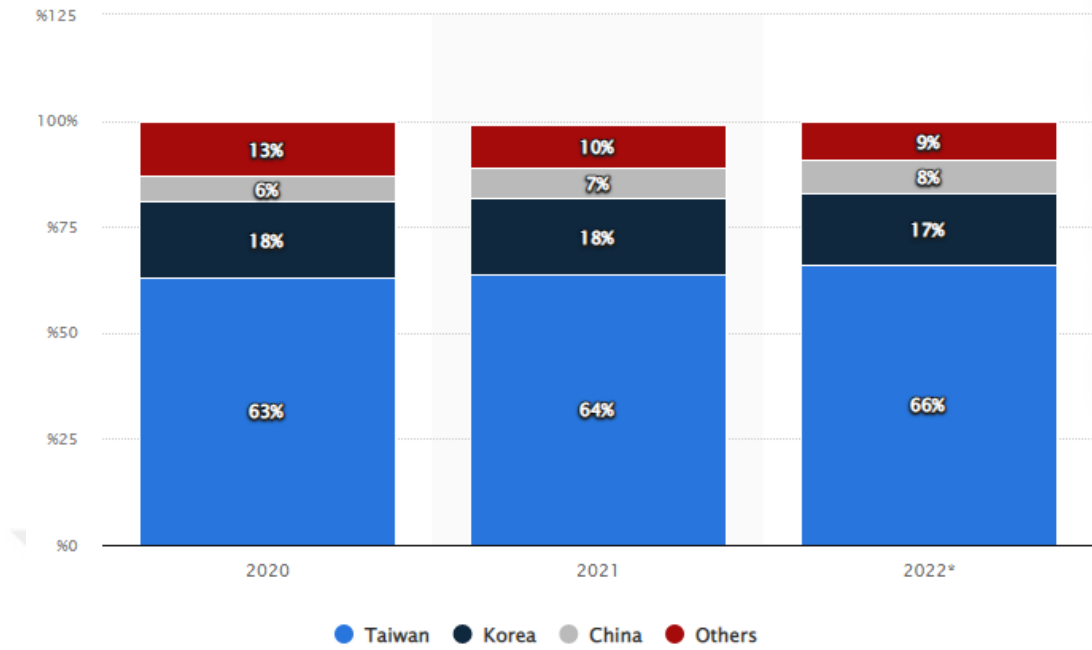
- ABD markası Tesla, Covid-19 salgını boyunca tüm otomobil markaları arasında *en büyük büyümeyi yaşamış*, 2020'den beri %271 oranında marka değerini artırmış ve 2022'de marka değerini 46,0 milyar dolara yükseltmiştir. Ayrıca 2021 yılı boyunca Tesla, Çin pazarında rekabetini güçlendirmek için 2020'de Çin'de kurulan Gigafactory Şanghay'da teslimatlarını artırmıştır. Küresel çip krizi sebebiyle yeni model piyasaya sürmeyeceğini duyuran Tesla, tam otonom sürüş yazılımına ve üretim kapasitesini artırmaya odaklanacağını bildirmiştir.
- Çinli otomobil markaları ise *en hızlı büyüyen* ilk on markanın sekizini oluşturmakta (Great Wall, BYD, Song, Qin, Tang, NIO, Dongfeng, WEY) ve dünya çapında satılan çoğu elektrikli aracı üretmektedir. Özellikle marka değerini %109 artırarak 2,6 milyar dolara ulaşan otomotiv şirketi Great Wall, Tayland'da önümüzdeki üç yıl içerisinde dokuz elektrikli araç modelini piyasaya süreceğini duyurmuştur. Ayrıca Great Wall, Tayland'ı ASEAN bölgesine genişleme stratejisi çerçevesinde önemli bir üs olarak kullanmayı planlamaktadır.
- Japon markası Toyota, 64,3 milyar dolar marka değeri ile *en değerli otomobil sıralamasında* birinci sırada yer almaktadır. Giderek artan elektrikli araç pazarında geri kalan Toyota, 2030 yılına kadar 3,5 milyon elektrikli araç satma hedefi doğrultusunda 35 milyar dolar yatırım yapacağını duyurmuştur.
- Diğer Japon markaları, marka değeri 28,2 milyar dolar olan Honda ve 14,6 milyar dolar olan Nissan *en değerli araba markaları sıralamasında* ilk on da yer almaktadır.
- Alman markası Mercedes-Benz, 2021 yılına göre marka değerini %4 artırarak 60,4 milyar ABD dolarına yükseltmiş *en değerli ikinci marka ve en değerli Avrupa markası* olmuştur. Elektrikli araç satışını ise 2022 yılında %90 oranında artırmıştır.
- Diğer Alman otomobil markaları Volkswagen, BMW ve Audi ise marka değerinde kayıplar yaşayan otomobil markalarıdır. Sektördeki devam eden çip krizi ve yasal zorluklar sebebiyle elektrikli üretim yöntemlerine geçmek zorunda kalan markalar, üretimde geri çekilme yaşamıştır.
- İtalyan markası Ferrari, 100 üzerinden 90,9 Marka Gücü Endeksi puanı ile dünyanın *en güçlü otomobil markası* seçilmiştir.

3.2.2.1. ip Endüstrisindeki Krizin Otomotiv Sektörüne ve Siber Uzaya Etkisi

Günümüzün dijital dünyasını oluşturan, imalatı zor ve yüksek teknoloji ürünü olan mikroip, yonga veya yarı iletkenler olarak adlandırılan ipler, askeri operasyonlar dahil füzelerden, yapay zeka donanımlı araçlara, modern elektronik cihazlara, telekomünikasyon ve otomotive kadar birçok endüstrinin beynini oluşturmaktadır. Ayrıca pek çok sektörde üretim, dünyada en çok ticareti yapılan dördüncü ürün olan iplere baėlıdır (Nuroėlu, 2022). Dolayısıyla ip üretimi, modern teknolojilerin ayrılmaz bir parçası olduğundan, birçok ülkenin endüstriyel yeteneklerinde çok önemli bir faktördür.

Artan ihtiyaçlar, jeopolitik gerilimler, doğal afetler, artan hammadde fiyatları, Covid-19 salgını gibi birkaç olayın bir araya gelmesi sonucu, güçlü talep ve sınırlı arzdan kaynaklı küresel ip kıtlığı yaşanmıştır. 2012 yılında dünya ip endüstrisinden elde edilen gelirler 300 milyon dolar iken, 2021 yılında 583,5 milyar dolara ulaşmıştır. 2022 yılında dünya ip üretiminde %66 Tayvan, %17 Güney Kore ve %8 ile Çin lider konumdadır (Nuroėlu, 2022).

Şekil 15 : 2020'den 2022'ye kadar dünya çapında yarı iletken gelir payı



Kaynak: <https://www.statista.com/statistics/1230946/semiconductor-foundries-market-share-by-country-worldwide/>

2021'de küresel çip krizi, dünya genelindeki otomobil üreticilerini 11,3 milyon araç üretimini iptal etmek zorunda bırakmıştır. 2022'de ise şirketlerin 3,8 milyon aracın üretimini etkilediği tahmin edilmektedir (Bove, 2022). Araştırmacılar, şirketlerin yarı iletkenler için önemli yatırımlar yaptığını ancak 2023 yılı dahil olmak üzere yarı iletkenlerde yapısal eksiklikler olacağını ve krizin devam edeceğini öngörmektedir.

Küresel çip krizinin çok uluslu otomotiv şirketlerine etkileri;

- Dünyanın en çok satan otomobil üreticisi Toyota ve Toyota tarafından üretilen Lexus, 2021'in sonlarında çip kıtlığı nedeniyle dünya çapındaki araç üretimini %40 oranında azaltmış, Şubat 2022'de çip krizi sebebiyle üretim tahminini 500 bin azaltarak 8,5 milyon adede düşürmüştür (BBC, 2022). Ayrıca Toyota Japonya'daki müşterilerine arabalarını, tek bir elektronik anahtarla göndermeye başlayarak, kullandığı çip sayısını azaltmak amacıyla ikinci anahtarı mekanik versiyonu ile değiştirmiştir.
- Diğer bir Japon markası Honda, Mart 2022'de küresel çip krizi ve jeopolitik belirsizlik sebebiyle iki yerel fabrikada üretimini %10 azaltacağını açıklamıştır (Reuters, 2022). Ekim 2022'de ise Honda

ikinci kez, Japonya fabrikalarından birinde üretimi %40, ayrı bir montaj fabrikasında faaliyetlerini %30 azaltacağını duyurmuştur (Bove, 2022).

- Kasım 2022'de Nissan, sektörde devam eden çip kriziyle ilgili tedarik zinciri aksamalarından kaynaklı, Titan ve Frontier kamyonetlerinin yanı sıra Altima Sedan için kasım ayında bazı üretim günlerini azaltacağını açıklamıştır (Shepardson, 2022).
- Elektrikli araç lideri Tesla'nın çip krizi nedeniyle Çin'de üretilen Model 3 ve Model Y arabalarının direksiyon raflarında bulunan iki elektronik kontrol ünitesinden birini çıkarmaya karar vermiştir (Reuters, 2022a).
- Amerikan otomobil firması Ford, Mart 2022'de yaptığı açıklamada, Avrupa'daki araç üretiminin ve siparişlerinin, çip kıtlığının yanı sıra Ukrayna'daki savaştan etkilendiğini duyurmuştur. ABD'li otomobil üreticisi, çoğunlukla küresel çip kıtlığı sebebiyle Almanya'da iki bölgede fabrikalarını durduracağını, İspanya'nın Valensiya kentinde üretilen S-Max ve Galaxy araçları için yeni sipariş almayı bırakacağını açıklamıştır (Reuters, 2022b).

3.2.2.2. Rusya-Ukrayna Savaşı ve Küresel Otomotiv Endüstrisine Etkileri

Rusya, otomobil, kamyon, minibüs, otobüs ve motor üreten birçok otomobil üretim tesisine ev sahipliği yapmaktadır. Rusya'nın 24 Şubat 2022'de Ukrayna'yı işgal etme kararı ardından yaptırımlar ve sınırdaki teslimat sebepleriyle, fabrikaların ülkedeki parça üreticilerinin tedarik sürecini durdurmasına, devam eden küresel çip krizinin daha da kötüleşmesine, hem savaşan ülke hem de komşu bölgelerin üretim hacimlerinde düşüş yaşanmasına, bazı otomobil üreticilerinin fabrikasına durdurmasına yol açmış ve Rusya'nın otomobil sektöründe ciddi bir daralma yaşanmıştır.

- Birçok otomobil üreticisi Rusya'ya araç ihraç etmeyi durdurmuştur. Etkilenen otomobil şirketler arasında Volkswagen, Mercedes-Benz, BMW, Honda, Toyota, Volvo, Nissan, Land Rover ve Ford yer almaktadır.
- Üretim Doğu Avrupa'da kesintiye uğramıştır. Çek Cumhuriyeti'nde Hyundai, Volkswagen ve Toyota; Beyaz Rusya'da Stellantis; Polonya'da Ford,

Volkswagen, Stellantis; Slovakya'da Kia, Peugeot, Land Rover, Audi, Porsche, Seat, Skoda, Volkswagen üretimi durdurmuştur.

- Kanada merkezli otomotiv parça üreticisi Magna International, Rusya'daki faaliyetlerini durdurmuştur (Silberg, 2022).

Rusya ve Ukrayna, otomobil parçaları ve çip endüstrisi için gerekli olan önemli neon, paladyum, platin, nikel, helyum, kripton gibi birçok gazın ve değerli metalin büyük ve önemli üreticileridir. Çatışma sebebiyle, değerli metal fiyatları %10 ile %30 oranında artış göstermiş ve bu oran araç fiyatlarına da yansımıştır. Özellikle Ukrayna, dünyanın neon gazı arzının çoğundan sorumlu olduğu için çiplerin geliştirilmesinde önemli rol oynamakta ve küresel çip krizini etkilemektedir (Financial Times, 2022).

3.2.2.3. Çin - Tayvan Krizinin Otomotiv Endüstrisine Etkisi

ABD, Tayvan, Güney Kore, Japonya, Avrupa ve Çin, çip endüstrisinde giderek artan bir şekilde gelişme ve büyüme göstermektedir. Ancak hiçbir ülke, çip endüstrisinde "teknolojik egemenlik" veya "kendi kendine yeterlilik" elde edemediği için tüm üretim süreci boyunca karşılıklı bağımlılıklar sürmektedir (Kleinhans & Baisakova, 2020, s. 5). Dolayısıyla çip endüstrisindeki bu parçalanmış üretim yapısı, jeopolitik rekabeti beraberinde getirmektedir. Özellikle çip endüstrisi, Çin ile ABD arasında süregelen teknolojik rekabetin merkezinde yer almaktadır. Bu doğrultuda, her iki ülke de ihracat kontrollerinin uygulanması yoluyla kendi etkilerini artırmak ve güç sağlamak için aktif olarak çaba göstermektedir. Dünyanın en büyük çip üreticisi olan Tayvan Yarı İletken Üretim Şirketi'ne (Taiwan Semiconductor Manufacturing Company-TSMC) ev sahipliği yapan Tayvan ise bu rekabette önemli bir odak noktası olarak ortaya çıkmakta. Washington'daki Stratejik ve Uluslararası Çalışmalar Merkezi'nde araştırmacı olan Scott Kennedy'ye göre TSMC, "*gezegendeki en önemli şirket*" olarak tanımlanmıştır (Asia Financial, 2022). Artan ABD-Çin teknoloji rekabeti ve küresel çip krizi, Tayvan'ın çip endüstrisinde önde gelen küresel tedarikçisi olma rolünü her iki ülke için de stratejik ve ekonomik açıdan önemli hale getirmektedir.

Çin'in küresel çip tedariki için kilit bir ülke olan Tayvan üzerinde açıkça ifade edilen toprak iddiası, gerekirse askeri güç kullanma durumu söz konusudur (Kamasa, 2022). Ancak küresel çip üretim kapasitesi, Tayvan ve Güney Kore dahil olmak üzere Asya'da yoğunlaştığı için, Çin ve Tayvan arasında olası bir askeri çatışma, küresel çip

üretimini daha da etkileyecek ve küresel bir ekonomik krizin yaşanmasını tetikleyecektir. Bu senaryo göz önüne alındığında, Çin'in Tayvan ile çip ticaretini kısıtlamak ve kendi ekonomisini tehlikeye atmak için sınırlı teşvikleri mevcuttur (The Central News Agency [CNA], 2022).

3.2.2.4. Çip Stratejileri

Hükümetler yarı iletken endüstrisinin ekonomik ve teknolojik önemini kabul ederek, ulusal çip üretimini teşvik edecek stratejik yaklaşımlar geliştirmeye başlamıştır. Özellikle ABD, Çin, Tayvan, Japonya ve Güney Kore gibi ülkeler, yarı iletken sektöründe kendi ulusal yeteneklerini desteklemek için politikalar geliştiren önemli ulus devletler olarak ortaya çıkmıştır.

ABD Başkanı Joe Biden, *"Yarı İletken Üretimi için Faydalı Teşvikler Oluşturma ve Bilim Yasası 2022'yi (Creating Helpful Incentives to Produce Semiconductors - CHIPS and Science ACT 2022)"* imzalayarak yerli yarı iletken üretimini artırmak için 50 milyar dolar yatırım yapılmasını teklif etmiştir. Ayrıca yasa, finansman alan şirketlerin, Çin'de çip kapasitesinin maddi olarak genişletilmesini içeren önemli işlemlerde bulunmasını 10 yıl boyunca yasaklamıştır (The U.S. Department of Commerce, 2022). Yasa, ABD'nin çip endüstrisindeki bağımlılığı azaltmak, rekabet gücünü artırmak amacıyla ve tedarik zincirindeki kesintilere karşı yaptığı bir müdahale olmakla birlikte, çip endüstrisinde Çin'e karşı bir çevreleme politikası oluşturmak ve Çin'e karşı endüstriyel, teknolojik ve askeri üstünlüğün sağlanması amacını da taşımaktadır.

ABD, Mart 2022'de ticaret ve ulusal güvenlik gerekçesiyle Çin'de üretilen çiplere bağımlılığın azaltılması dahil, çip endüstrisindeki tedarik zincirlerinin direncini artırmayı amaçlayan stratejinin bir parçası olarak ABD, Güney Kore, Japonya ve Tayvan'ın dahil olduğu *"Dörtlülük Çip İttifakını (Chip 4)"* önermiştir. Girişim hükümetlere ve şirketlere, tedarik zinciri güvenliğini artırmayı, iş gücünü geliştirmeyi, araştırma ve geliştirme politikaları konularında tartışmaları yönlendirmeyi ve koordine etmeyi amaçlayarak, tasarımdan üretime kadar çip endüstrisindeki tedarik zincirini oluşturmak için her bir katılımcının gücünü birleştirme amacını da taşımaktadır. Ancak Çin'in olası misilleme tehdidi, Tayvan'ın hükümetler arası bir oluşuma dahil edilmesi konusundaki tereddütler ve Güney Kore ile Japonya arasındaki

uzun süredir devam eden gerilimler⁸ çip ittifakının toplanma çabalarını engellemektedir (Financial Times, 2022a). Ayrıca Çin, ittifak üyeleri için büyük bir elektronik eşya pazarıdır. Hükümet verilerine göre Çin, dizüstü bilgisayarlara yönelik toplam küresel talebin %70'ini, küresel mobil telefon talebinin %80'inden fazlasını oluşturmaktadır. 2021'de Çin'in başlıca tedarikçileri olan ABD ve Güney Kore 350 milyar dolar değerinde çip ithal etmiştir. Dolayısıyla Çin'in tedarik zincirinden dışlanması, ABD ve diğer ittifak ülkelerinin firmalarının mali durumlarına ve karlarına önemli ölçüde zarar verecektir (Gargeyas, 2022). Diğer bir durum ise pazar rekabeti içerisinde yer alan çok uluslu şirketler, ticari rakipleriyle teknolojik bilgi paylaşımına karşıdır. Özellikle bu endişe çip endüstrisinin önemli üreticileri olan Tayvanlı ve Güney Koreli şirketler arasında daha güçlüdür.

Çin, çip üretmek ve ithal edebilmek için büyük ölçüde yabancı teknolojiye bağımlı bir ülkedir. Bu doğrultuda yüksek teknoloji ve ileri düzeydeki çip üretimini gerçekleştirebilmek için özellikle yabancı teknoloji şirketlerinden teknoloji transferi ve lisans anlaşmaları yoluyla faydalandığı bilinmektedir. Teknoloji sektörünü desteklemek için yılda 300 milyar doların üzerinde ithalat yapan Çin, dünyanın en büyük çip tüketicilerinden biri konumundadır (Reuters, 2020). Otonom, elektrikli ve yapay zeka destekli tasarımda ve üretimde daha fazla gelişme gösteren Çin'in çip talebinde artış söz konusudur. Dolayısıyla çip endüstrisindeki gelişim, ekonomik ve ulusal güvenlikle bağlantılı hale geldiği için yabancı teknolojiye bağımlılığın azaltılması ve yerli çip endüstrisinin güçlendirilmesi Çin'in stratejik hedefleri arasında yer almaktadır.

Çin Devlet Konseyi'nin çip endüstrisine yönelik oluşturduğu 2014 tarihli Ulusal Entegre Devre Endüstrisini Teşvik İlkeleri, 2030'a kadar 150 milyar doların üzerinde yatırım yaparak açığı kapatmak amacıyla bazı girişimlerden bahsetmektedir. Teşvik yönergelerinin yayınlanmasıyla Çin'in çip endüstrisine yönelik çabaları hızlanmıştır. Öncelikle 21 milyar dolarlık devlet destekli finansmanla Ulusal Entegre Devreler Endüstrisi Geliştirme Yatırım Fonu (Büyük Fon) kurulmuştur. Fonun yatırımcıları arasında Çin Maliye Bakanlığı, devlete ait Çin Kalkınma Bankası, China Tobacco, Pekin, Şanghay ve Wuhan belediyelerinin yatırım araçları dahil olmak üzere çeşitli devlete ait şirketler yer almaktadır. Büyük Fon kurulduğunda, Çin'in devlet

⁸ ayrıca bkz. <https://www.bbc.com/news/world-asia-49330531>

planlamacılarının temel odak noktası, sıfırdan kendi kendine yeten bir endüstri inşa etmek için gereken temel teknolojilerden ziyade çip üretimi yer almıştır (Financial Times, 2022b). Ancak 2022 yılında bazı üst düzey yöneticilerin, yolsuzluk iddiaları sebebiyle tutuklanması fonun yatırım faaliyetlerini etkilemiştir.

Çin'in 14. Beş Yıllık Planı, ülkenin 2021-2025 dönemi için teknolojik iyileşmeye ve çip endüstrisindeki yeniliklere odaklanan bir dizi hedef ve planları içermektedir. Bu plan, Çin'in çip endüstrisinde bağımsız ve kontrol edilebilir bir endüstri hedefine ulaşma amacını belirtmektedir. Yerli çip üretimini teşvik etmek, yüksek teknoloji yeteneklerini geliştirmek, araştırma ve geliştirme faaliyetlerini desteklemek ve çip tedarik zincirinin güvenliğini sağlamak gibi stratejik hedefleri içermektedir (Central Cyberspace Affairs Commission, 2021).

Çin Mali 2025 stratejisinde ise 2025 yılına kadar çip endüstrisinde %70 kendi kendine yeterliliğe ulaşma hedefi belirlenmiş ve endüstrilerin 300 milyar dolardan fazla devlet yatırımı ile destekleneceği, bütçenin 130 milyar dolarının çip endüstrisine ayrılacağı açıklanmıştır (Springborg, 2018). Sonuç olarak devlet yatırımı ve ülkenin yabancı çip üreticilerine olan bağımlılığı azaltma hedefiyle kurulan, Çinli yarı iletken üretici şirketleri Şanghay merkezli Hua Hong, Yangtze Memory Technologies Corp (YMTC) ve Semiconductor Manufacturing International Corporation (SMIC) gibi yerel çip üreticileri hızla büyüme gösterse de, Çin günümüzde hala çiplerin tasarım ve temel ekipmanları konusuna yabancı yatırımcılara bağımlılığını sürdürmektedir.

Üretimini Tayvan üzerinde yoğunlaştırmış olan TSMC, Çin'in çip tedariki için en büyük pazardır. Dolayısıyla hem ABD'de pazar gücünü artırmak hem de Çin'de pazarını korumak için dengeleme stratejisini izlemektedir. TSMC'nin 2021 yılında ABD'de 12 milyar dolarlık girişim ile kurulacak olan tesisinin temeli atılmış ve tesisin 2024'te 5 nanometre çip üretmeye başlaması planlanmaktadır. TSMC'nin 8,6 milyar dolarlık yatırım ile kuracağı diğer tesis ise Sony ve Japonya hükümetinin girişimiyle 2024 yılında hizmete girmesi beklenmektedir (Asia Financial, 2022).

Dünyada en iyi yarı iletken tedarikçisi SK Hynix ve Samsung'a ev sahipliği yapan Güney Kore, çip endüstrisinde egemen bir devlet olmak ve kaynaklarını güçlendirmek amacıyla stratejiler geliştiren bir ülkedir. Bu doğrultuda 2022 yılında, çip tasarım firmalarının satın alımlarına 300 milyar won (230 milyon dolar) yatırım yapacağını açıklayan Güney Kore, plan kapsamında 2024'ten 2030'a kadar otomobil

iplerinin geliřtirilmesine ynelik giriřimlerine 950 milyar won ve 2029 yılına kadar yapay zeka ipleri geliřtirmek iin 1.25 trilyon won yatırım yapmayı amalamaktadır (Suk-yeol, 2022). lkenin en byk ip reticisi ve Tayvanlı TSMC'nin rakibi olan Samsung Electronics ise 2030 yılına kadar yatırımlarını 171 trilyon won'a ıkaracağını duyurmuřtur (Samsung News, 2021).

Japonya Kasım 2022'de Toyota ve Sony'nin de aralarında bulunduėu sekiz nde gelen Japon řirketi tarafından "Rapidus" ismiyle kurulan ve 480 milyon dolar yatırımla ip endstrisinde 2027'ye kadar yerli retim oluřturma stratejisini aıklamıřtır (NTV, 2022).

3.2.3. Siber Uzay ve Otomotiv Endstrisi

Otomotiv sektrnde yeni dijital hareketlilik, otonom srř, baėlantılı ve paylařımlı arabalar, internet ile kalıcı bir baėlantı gerektirir ve aracı ok karmařık bir siber-fiziksel sisteme dnřtrr (Haas & Mller, 2017, s. 635). Araların elektrikle alıřması, kullanıcıların uzaktan ynetimi, src mdahalesi olmadan basın oluřturabilen fren sistemleri, baėımsız olarak ynlendirilebilen direksiyon, GPS gibi konum belirleme sistemleri, kablosuz yazılım gncelleme, 5G baėlantısı gibi belirli zellikler, dijitalleřen gnmz otomotiv endstrisinde giderek daha yaygın hale gelmektedir. Teknoloji alanındaki her yeni geliřme, kullanıcı deneyiminde devrim yaratmakla birlikte yeni bir siber saldırı alanı amaktadır. nk aėa baėlı otomobillerin fren sistemleri, ara kilitleme ve motor dahil tm fiziksel sistemler uzaktan kontrol edilebilir ve izlenebilir hale gelmiřtir (Kapur, 2022). Ara aėa baėlandığı srete oluřabilecek herhangi bir gvenlik aığı sonucunda mřterilerin can ve mal gvenliėi tehlikededir. Aracın fren sistemini devre dıřı bırakma, sunucudan veri hırsızlıėı, řarj altyapısına saldırılar, verilerin bozulması, trafik veya GPS verilerindeki ihlaller bu tehlikelere rnek olarak verilebilmektedir.

2015 yılında iki gvenlik arařtırmacısının internet zerinden gerekleřtirdiėi tatbikat sonucunda Cherokee Jeep'teki Wi-Fi baėlantısı aracılıėıyla direksiyonun uzaktan ynlendirilebilmesi, frenlerinin devre dıřı bırakılabilmesi ve motorun durdurulabilmesi gibi ciddi sonular gzlemlemiřtir (Drozhzhin, 2015). nemli bir mřteri deėeri sunan bu sistemler byk miktarda veri retmektedir. Morgan Stanley'e gre otonom aralar, bir iPhone telefonun 3.000 yıldan fazla kullanımına eř deėer

oranda saatte 40 terabayt veri üretebilecek kapasiteye sahiptir (Naughton, 2021). Dolayısıyla otomotiv sektörünün dijital dönüşümü ve sunduğu yenilikler, siber saldırılara karşı duyarlılığı zorunlu kılmış ve siber güvenlik konusu otomotiv sektöründeki her alanı ilgilendirmeye başlamıştır.

3.2.3.1. Otomotiv Endüstrisinde Siber Saldırıları

Bağlantılı araçlar için siber güvenlik ve veri yönetimi platformu olan Upstream'in 2022 Küresel Otomotiv Siber Güvenlik Raporuna göre 2023 yılına kadar 775 milyon bağlantılı arabanın yollarda olacağı tahmin edilmektedir (Upstream Security, 2022). Ayrıca raporda otomotivle ilgili 900'den fazla siber olaya dayanarak bir takım sonuçlar elde edilmiştir;

- Otomotiv sektörüne yapılan siber saldırıların sıklığı 2018 yılından 2021'e yılına kadar %225 artış göstermiştir.
- 2010 ile 2021 arasında bildirilen siber saldırıların %84,5'i uzaktan, %15,5'i ise hedefe fiziksel erişim gerektirmekteydi.
- 2020'de %49,3 olan Siyah Şapkalı hackerler tarafından gerçekleştirilen saldırıların %54,9'u 2021 yılında görülmüştür
- 2010-2021 yılları arasında en çok saldırı kategorileri; veri ihlali (%39.9), araba hırsızlığı (%27.9), araç kontrol sistemleri (24.2), hizmet kesintisi (%18.2), dolandırıcılık (%4.2), araba sistemlerinin manipülasyonu (%4), konum takibi (%2), politika ihlali (%1.5) olarak belirlenmiştir.
- Anahtarsız giriş ve anahtarlık saldırıları, tüm araç hırsızlıklarının %50'sini oluşturmaktadır. Siyah Şapkalı bir bilgisayar korsalarının sinyali alıp yeniden üretebilmesi için kötü niyetli aktörlerin yalnızca anahtarlığa yakın olmasının yeterli olduğu tespit edilmiştir.

3.2.3.2. Otonom Araçlara Yönelik Siber Tehditler

Çok az insan müdahalesiyle çalışan otonom araçlar, sensör ve kamera kullanarak ayrıntıları okur ve otomobilin çevresinden gelen bilgileri analiz ederek kendi kendine performans gösterir. Kullanılan sensörler, yoldaki işaretleri, radar sistemini, trafik ışıklarını, hava koşullarını, GPS ve göz önünde bulundurulması

gereken diğer tüm riskleri ve hesaplamaları okumak için tasarlanmıştır. Geleneksel arabalarda insanlar tarafından alınan kararları almak için veri toplamak, analiz etmek ve aktarmak için yapay zeka tabanlı yazılımlara göre çalışmaktadır (European Union Agency for Cybersecurity [ENISA], 2021). Bu sistemin ana işleyişi, verilerin sürücü ile araç, araç ile çevresi arasındaki iletişimi ve kendi sistemleri arasındaki veri aktarımıyla sağlanır (Upstream Security, 2022) ve otonom aracın çarpışmalardan kaçınmasına, doğru navigasyon sağlamasına, yayaları ve engelleri tanımasına, çevreyi algılamasına olanak tanır (Giordani, 2021). Bu sistemler, tüm bilgi ve teknoloji sistemleri gibi aracın düzgün çalışmasını tehlikeye atabilecek saldırılara karşı savunmasızdır. Otonom bir araç belirli girdilere yanıt vermediğinde tehlikeli bir durum ortaya çıkabilir. Bu iletişimleri korumak, güvenli tutmak, hassas bilgileri ve kritik sistemleri dijital saldırılardan koruma uygulaması da siber güvenliğin rolüdür.

Otonom bir aracın neden olduğu bilinen ilk kaza 2016 yılında Tesla tarafından açıklanmıştır. Kaza, 40 yaşındaki Joshua Brown'ın Tesla Model S'yi otoyol sürüşü sırasında, arabayı kontrol edebilen oto pilot ayarına almasının ardından meydana gelmiştir. Tesla yaptığı açıklamada, parlak bir gökyüzü sebebiyle, otomobilin sensör sisteminin otoyoldan geçen büyük beyaz tekerlekli bir kamyonu ayırt edemediğini ve fren sisteminin devreye girmediğini belirtmiştir (Tesla, 2016).

Arabalarda önemli bir sensör olan GPS'ler de siber tehdit aktörlerinin saldırıları için bir alan oluşturmaktadır. Otonom araçlar, bir haritayı analiz ederek en kısa rotayı belirlemek için GPS kullanmaktadır. Ancak GPS sistemi, otonom araçlarda saldırganların yararlanabileceği güvenlik açıkları oluşturur. Bu durumda ise siber tehdit aktörleri iki tür saldırı gerçekleştirebilir; kimlik sahtekarlığı ile sinyallerin GPS alıcısını şaşırtarak aracın yanlış yöne sürüklenebilmesi ve aracın GPS sinyallerini almamasını sağlamak için aynı anda çok daha güçlü sinyallerin kullanılması (Giordani, 2021).

3.2.3.3. Bağlantılı Araçlara Yönelik Siber Tehditler

Kodlardan oluşan ve internet bağlantısı içeren bağlantılı teknoloji, araç performansını, konforunu ve güvenilirliğini büyük ölçüde geliştirmiştir. Günümüzde bağlanabilirlik, otomobiller dahil birçok ürünün merkezinde yer almaktadır. Araç üreticileri, tüketicilerin artan talepleri doğrultusunda, araçlara iletişim sistemler, dijital

araç bilgi sistemleri, yerleşik Wi-Fi ve akıllı telefon uygulamalarıyla araç kontrolü gibi dijital özellikleri entegre etmektedir. Bu dijital özellikler, sürücülere ve yolculara daha fazla konfor, güvenlik ve eğlence sunmayı amaçlamaktadır (Panda, 2017).

Canlı izleme, uzaktan çalıştırma, durdurma, sıcaklık kontrolü, bakım planlaması, otonom sürüş sağlayan IoT özellikli cihazlarla donatılmış araçlar, güvenlik saldırılarına karşı savunmasızdır (Çakal, Kara, & Aydos, 2021). Çünkü araç, halka açık internet erişimi olan bir ağa bağlandığında, belirli bilgileri ve verileri paylaşımına sunar. Dolayısıyla kişisel verileri içerebilecek bu bağlantı ve veri paylaşımı, araçları siber saldırılar karşısında daha savunmasız hale getirmektedir.

Arabalar, kullanıcıların arabaları etrafında değilken bile yönlendirme yapmasına izin veren mobil uygulamalar sayesinde akıllı telefonlara bağlanmaktadır. Mobil uygulamalar aracılığıyla araçlar uzaktan çalıştırma, kilitleme, kilidini açma, aracın konumunu ve durumunu izleme gibi özelliklerle daha rahat kontrol edilmesini sağlamaktadır. Bu uygulamalar, kullanıcıların kritik işlevleri dünyanın her yerinden rahatça kontrol edebilmesine olanak tanımakta ve aynı zamanda bilgisayar korsanlarının da yararlanabileceği ek bir siber saldırı yüzeyi oluşturmaktadır. Bu sebeple 2010 ile 2021 yılları arasında otomotiv sektöründe görülen siber saldırıların %7,3'ü mobil uygulamalar aracılığı ile gerçekleşmiştir (Upstream Security, 2022, s. 39).

2016 yılında oto pilot ayarında giden bir Tesla'nın karıştığı ilk ölümcül kazasından sonra Çinli teknoloji devi Tencent tarafından yönetilen Keen Security Lab'daki güvenlik araştırmacıları, Tesla Model S arabalarında siber tehdit aktörlerinin aracı uzaktan bir konumda kontrol etmesine izin verebilecek birkaç güvenlik açığı keşfetmiş ve düzeltilmesine yardımcı olmuştur. Ekip, Tesla Model S'in uzaktan kumandasını 12 mil mesafeden ele geçirerek, elektronik olarak kontrol edilebilen özelliklere müdahalede bulunabilmiştir. Güvenlik açığını gösteren bir videoda uzmanlar, aracın ışıklarını, camlarını, koltuklarını, açılır tavan panelini, araç içi ekranları kontrol edebilmiştir. Ayrıca araç hareket halindeyken frene basmak, bagajı açmak, yan aynaları ayarlamak ve ön cam sileceklerini etkinleştirmek gibi işlemleri gerçekleştirebilmiştir (Keen Security Lab of Tencent , 2016). Saldırı, araç web tarayıcısı kullandığında gerçekleşebilmekte ve aracın fiziksel olarak kötü amaçlı bir Wi-Fi bağlantı noktasına yakın ve bağlı olmasını gerektirmekteydi. Gözlemlenen

güvenlik açığı sonucunda Tesla, kablosuz olarak sunduğu bir yazılım güncellemesi ile güvenlik açığına bir çözüm sunmuştur (Solon, 2016). Bu keşif, araçların siber saldırılar karşısında ne kadar savunmasız olduğunu ve güvenlik açıklarının potansiyel etkilerini gösteren önemli bir örnektir.

3.2.3.4. Elektrikli Araçlara Yönelik Siber Tehditler

Elektrikli araçlar, elektrikli şarj istasyonundaki güvenlik açıklarından etkilenebilirler ve bu güvenlik zafiyetleri birden fazla elektrikli şarj istasyonu bileşenini etkileyebilir. Elektrikli araçlar pilleri şarj etmek için şebekeye bağlandıklarında siber saldırılara karşı diğer araçlara göre daha savunmasızdır. Elektrikli araç sektöründeki profesyoneller arasında yapılan bir ankette her 5 kişiden 2'si (%39) IoT tabanlı elektrikli araç altyapısındaki güvenliğin, kuruluşların üstesinden gelmesi gereken en büyük zorluk olarak belirtmiştir (Eseye, 2021, s. 4).

Georgia Üniversitesi'ndeki araştırmacılar, bir şarj istasyonu aracılığıyla bir elektrikli araca yönelik gerçekleştirilen saldırının sadece şarj istasyonunun kendisini değil, aynı zamanda araç kontrol sistemini ve ona bağlı herhangi bir altyapıyı etkileyebileceğini ve bu durumda da frenlerin devre dışı bırakılması, farların söndürülmesi veya direksiyon hakimiyetinin devralınması gibi tehditlere yol açabileceğini keşfetmiştir (Michaux, 2021).

Temmuz 2021'de yapılan bir araştırma, bir dizi elektrikli araç şarj cihazında çok sayıda güvenlik açığı tespit edildiğini ortaya koymuştur. Tespitler sonucu, bir siber tehdit aktörünün şarj cihazlarını uzaktan açma ve kapama, şarj kablosunu kilitleme veya kilidini açma, şarj cihazını kalıcı olarak devre dışı bırakma, araç sahibinin erişimini engelleme, araç sahibinin kimliğini çalma ve ardından kendi aracını ücretsiz olarak şarj etme gibi yeteneklere sahip olabileceği keşfedilmiştir (Upstream Security, 2022, s. 34). Tüm bu güvenlik açıkları, bilgilerin çalınmasında ve milyonlarca aracı etkileyebilme potansiyeli taşımaktadır.

Elektrikli araç korsanlarının çoğu, şirketlerin güvenlik sistemlerini test etmek için tuttuğu beyaz şapkalı bilgisayar korsanlarından oluşmaktadır. Beyaz şapkalı bilgisayar korsanları, üreticilerin zayıflıklarını bulmasına ve düzeltilmesine yardımcı olmak için sistemlere girmektedir. Ancak günümüzde siyah şapkalı bilgisayar

korsanları ekonomik ve politik temelli yasadışı siber saldırılarda bulunmaya başlamıştır. Örneğin Şubat 2022'de şarj cihazları için parça teminin sağlayan Ukraynalı bir şirket⁹, Rusya'nın Moskova'dan Saint Petersburg'a uzanan M11 otoyolundaki şarj cihazlarının kontrol sistemlerindeki bir arka kapıyı kullanarak devre dışı bırakmış, Ukrayna yanlısı ve Rusya devlet başkanı Vladimir Putin'e yönelik eleştirel mesajlar gösterecek şekilde programlanmıştır (Massie, 2022).

3.2.3.5. Otomobil Şirketlerine Yönelik Siber Tehditler

Otomotiv sektöründeki ihtiyaç duyulan siber güvenlik sadece arabaların teknolojik gelişimleriyle ilgili değildir. Günümüz çağında tüm şirketler, siber tehdit aktörlerinin hedefi haline gelmiştir. Dolayısıyla otomotiv sektöründeki dijitalleşmeyle hem araç sistemi hem de üretim tesisleri, kötü niyetli siber saldırı riskiyle karşı karşıyadır. Olası siber saldırılar karşısında araç güvenliğinde, tüm üretim tesislerinde, şirket içi operasyonlarda ve tedarik zincirlerinde son teknoloji siber savunma sistemi geliştirmesi gerekmektedir. Otomobil şirketlerine yönelik en çok görülen siber saldırı türleri ise fidye yazılım saldırıları, kaba kuvvet saldırıları ve kimlik avı saldırılarıdır.

Geleneksel BT ortamlarında en başarılı ve karlı saldırı tekniği olan fidye yazılım saldırıları genellikle, işletmeleri gasp etmek amacıyla şirketlerin sunucularını hedef alır. Sunuculara erişim sağlandığı takdirde sistemler kontrol edilebilir ve araçlara yönelik saldırılar kolaylaşabilir. Fidye yazılımı saldırısına uğrayan işletme, talep edilen ödemeyi gerçekleştirmezse siber tehdit aktörleri tüm verileri, verilerin şifresini çözmek için kullanılan şifreleme anahtarlarını silmekle veya yayınlamakla tehdit edilmektedir. Ayrıca bir fidye yazılımı, aracın bilgi-eğlence sisteminin bağlı olduğu bir web hizmetine veya USB bağlantısına gönderilebilir ve otomotiv yazılımındaki bir güvenlik açığından yararlanılarak aracın sistemine kurulabilir. Yüklenen fidye yazılımı ise aracın ana bileşenlerini kilitler ve komuta kontrol şifreleme yoluyla fidye ödemesi yapılana kadar kullanılamaz hale getirilebilir (Lee, Woo, Song, Lee, & Lee, 2020). Özellikle son birkaç yıldır Asya ve Avrupa'da çok sayıda Orijinal Ürün Üreticisi (OEM) fabrikalar, otomobil üretim süreçlerinin aksamasına yol açan saldırılara maruz kalmıştır (Upstream Security, 2022, s. 39).

⁹ M11 otoyoluna yapılan elektrikli araçlar için şarj istasyonlarını yapan şirket Rus olsa da, şarj istasyonlarının üretiminin çoğunu Ukrayna'daki Auto Enterprise isimli parça tedarikçisinden sağlanmıştır. Dolayısıyla parçaları üretenler arka kapı kullanarak siber saldırı eylemini gerçekleştirebilir.

Otomobil üreticisi Kia Motors America (KMA), bir şifre çözücü ve çalıntı verileri sızdırmama karşılığında 20 milyon dolar değerinde 404 Bitcoin talep eden DoppelPaymer çetesi tarafından bir fidye yazılım saldırısına uğramıştır (Abrams, 2021).

Şubat 2021'de Doğu Avrupalı araba paylaşım hizmeti sağlayıcısı CityBee, bir fidye yazılım saldırısı yoluyla önemli bir güvenlik ihlali yaşamıştır. Bu saldırı sonucunda araların şirketin müşterilerinin de bulunduğu yaklaşık 110.000 kişinin kişisel verileri ele geçirilmiş ve ardından çevrimiçi bir hacker sitesine sızdırılmıştır. Çalınan veriler, Kullanıcı adları, kişisel kimlik numaraları, telefon numaraları, e-posta ve ev adresleri, sürücü belgesi numaraları ve şifrelerini içermektedir (Holroyd, 2021).

2020'de Honda, "Ekans" olarak bilinen bir kötü amaçlı yazılım saldırısı yaşamıştır. Bu kötü amaçlı yazılım Honda'nın bilgisayar sistemlerine başarılı bir şekilde sızmış ve Kuzey Amerika, Türkiye, İtalya ve Japonya da dahil olmak üzere dünya genelinde birçok bölgede yaygın üretim kesintilerine yol açmıştır. Saldırı, tüm telefon sistemlerinin tamamen kapanmasına ve çalışanların bilgisayarlarına erişimin kısıtlanmasına neden olmuştur. Ekans kötü amaçlı yazılımının, özellikle makineleri kontrol etmekten, yetkisiz erişim elde etmekten ve ardından kritik verileri şifrelemekten sorumlu sistemleri hedef alarak üretim süreçlerinde aksamalara neden olduğu düşünülmektedir (Baggott, 2020). Honda 2017 yılında da WannaCry fidye yazılımı saldırısına uğradığında da üretimi geçici olarak durdurmak zorunda kalmıştır.

1 Mart 2022'de Toyota'nın önemli plastik parça ve elektronik bileşen tedarikçisi Kojima Endüstrisi, sunucusundaki bir dosya hatasından sonra cihazı yeniden başlatmak istediği sırada sisteme virüs bulaştığını ve tehdit mesajı aldığını bildirmiştir. Şirkete yönelik yapılan saldırı sonucunda Toyota, Japonya'daki 14 yerel fabrikasındaki 28 hattın tamamında üretimi durdurma kararı almıştır. Bir günlük üretimin durdurulması sonucunda ise 13.000 aracın üretiminin etkilendiği ve aylık üretimde %5'lik bir düşüşe sebep olduğu açıklanmıştır (Dooley & Ueno, 2022). Siber saldırının kaynağı net olmamakla birlikte, Ukrayna'nın işgali sonrasında Japonya'nın Rusya'ya yönelik ekonomik ve mali yaptırımlar uygulamak için Batılı müttefiklere katılmasının hemen ardından gerçekleşmesi Rusya'yı şüpheli göstermiştir.

Siber tehdit aktörlerinin doğrudan sisteme girerek erişim elde ettiği kaba kuvvet saldırıları, sistemin güvenlik açıklarını hedeflemektedir. Otomotiv sektöründe yapay

zeka, makine öğrenimi ve işlemcilerin gelişimi sayesinde daha karmaşık hale gelen saldırı bir türüdür (Bocetta, 2022).

Kimlik avı saldırısındaki senaryoda, otomotiv endüstrisindeki büyük şirketlerin çalışanlarına kötü amaçlı ekler içeren e-postalar gönderilmekte ve çalışanlar bu e-postaları açıp bir bağlantıya veya eke tıkladığında kullanıcının bilgisayarlarında kötü amaçlı kod aktif duruma gelmektedir. Bu durum ise potansiyel olarak siber tehdit aktörlerinin bir bilgisayar ağı üzerinden denetlenmeden dolaşmasına ve hassas verileri aramasına olanak tanır (Lindsey, 2019).

2021 yılında Audi ve Volkswagen markalarının, ABD ve Kanada bayilerinde 2014 ve 2019 yılların arasında satış ve pazarlama için toplanan müşteri verilerine yetkisiz bir üçüncü taraf müdahalesi gerçekleşmiştir. Ehliyet numarası, doğum tarihi, kimlik numarası, satın alma ve kiralama uygunluk verileri, hesap veya kredi kartı verilerinin ihlal edildiği siber saldırıda 3,3 milyondan fazla müşteri etkilenmiştir (Shepardson, 2021).

Otomotiv endüstrisinin siber uzayı hangi düzeyde etkilediği problemi çerçevesinde (P_{1a}), ileri teknolojilerin araçlara entegrasyonu yoluyla siber uzayı giderek daha fazla benimsediği ve bunun sektörlere hem olumlu hem de olumsuz etkileri olduğunu söyleyebiliriz. Çip krizinin siber boyutunda, otomotiv endüstrisindeki çip krizi, araçların üretim ve tedarik zincirini sekteye uğratmıştır. Rusya-Ukrayna Savaşı ve Çin-Tayvan krizi otomotiv endüstrisine kadar uzanan jeopolitik etkiler de söz konusudur. Dolayısıyla siber uzay, ülkelerin siber saldırıları kritik altyapıyı bozmak ve stratejik avantajlar elde etmek için bir araç olarak giderek daha fazla kullanılmasıyla modern savaşta önemli bir rol oynamaktadır. Altyapının hayati bir bileşeni olan otomotiv sektörü, jeopolitik krizlerin yaşandığı dönemlerde siber saldırıların hedefi haline gelebilmekte. Genel olarak otomotiv endüstrisinin siber uzaydaki etkisi büyüktür. Gelişmiş bağlanabilirlik, gelişmiş özellikler ve verimlilik kazanımları açısından faydalar sağlar, ancak aynı zamanda siber güvenlik, veri gizliliği ve jeopolitik gerilimler sorunları nedeniyle zorlukları da ortaya çıkartır.

3.3. Finansal Hizmetler Sektörü

3.3.1. Endüstri 4.0'ın Finansal Hizmetler Sektörüne Entegrasyonu

Tüm dünyada dijital gelişimin etkisiyle gelişen finansal hizmetler sektörü, Endüstri 4.0'ın gücünden yararlanan sektörlerden biridir. Finans sektörü, ürün veya hizmet rekabetinin yoğun olduğu dinamik bir sektördür ve sektörde faaliyet gösteren şirketler, rakiplerinden daha iyi performans göstermek için sürekli büyüme ve dönüşüm gerçekleştirme çabası içerisinde. ATM ve internet bankacılığı uygulamalarının ardından rekabet, hizmetlerin dijital kanallardan sunulmasına olanak sağlayan dijital bankacılık ve finansal teknoloji alanında devam etmektedir. Hızlı şehirleşme, akıllı teknolojilerin benimsenmesi, mobil bankacılık, dijital ödemeler, şirketlerin teknolojileri benimsemeleri ve hizmetlerine entegre etmeleri ihtiyacını zorunlu hale getirmiştir.

Risk değerlendirmesi, dolandırıcılık tespiti, finansal veri analitiği, varlık yönetimi, çevrimiçi işlemler, sanal asistan, dijital finans, dijital denetim vb., şirketlerin finansmanını yönetmek için - Nesnelerin interneti, bulut bilişim, büyük veri, robotik süreç otomasyonu, yapay zeka gibi- Endüstri 4.0 teknolojilerinin entegrasyonunu gerekli kılmaktadır (Bisht vd., 2022). Teknolojinin finansal hizmetlere entegrasyonu daha fazla müşteri odaklı hizmetlerin sağlanmasını, maliyetleri düşürülmesini, etkinliğin, verimliliğin ve faydanın artırılmasını, işlemlerin hızlandırılmasını, finansal hizmetlere 7/24 erişilebilirliği, robotik ve yapay zeka kullanımının artmasını, sohbet botlarının kullanımı yoluyla uygun maliyetli müşteri desteğinin sağlanmasını beraberinde getirmiştir. Bu entegrasyon aynı zamanda FinTech (Finansal Teknoloji) gibi yeni iş alanlarına ve blok zinciri teknolojisinden yararlanan akıllı sözleşmelerin uygulanmasına yol açmıştır.

Finans sektöründe yapay zeka analitiği aracılığıyla toplanan veriler, müşteri beklentilerine göre kişiselleştirilmiş ürün ve hizmet sunulmasına, insan etkileşimi olmadan finansal işlemlerin otomatikleştirilmesine olanak sağlamaktadır. Nesnelerin interneti teknoloji, şirketlerin kullanıcılar hakkında anlık veri toplaması için kullanılmakta ve internete bağlı olan nesneler (akıllı telefon, akıllı saat, yüzük, gözlük gibi çeşitli nesnelerin interneti teknolojisi içeren) üzerinden elde edilen veriler işlenerek, kullanıcılar hakkında bilgiye dönüşmektedir. Akıllı sözleşmeler ise blok zinciri teknolojisinin altyapısı üzerinden, üçüncü taraf kişi ve kurumlar olmadan

bankacılık, tedarik zinciri, sađlık, gayrimenkul ve vatandaşlık hizmetleri gibi alanlarda daha az maliyetli ve hızlı gerçekleştirilen dijital anlaşmalardır (Kaymak, 2019). Blok zinciri teknolojisi, kurumların ve kişilerin bankalara, hükümete veya diğer araçlara ihtiyaç duymadan işlem yapmasına olanak tanıyan, merkezi olmayan, değiştirilemez, işlemlerde veri koruması ve düşük maliyet sağlayan siber para birimleri veya kripto para birimlerinin temelini oluşturan bir teknolojidir (Varma, 2019). Kripto para birimlerinin ortaya çıkışı, uluslararası işlemlerin yürütülmesi için basitleştirilmiş bir çerçeve sunarak, aynı zamanda tek kutuplu bir ekonomik sistemden çok kutuplu bir ekonomik sisteme geçişe yol açmıştır. Böylelikle bireyler ve işletmeler, dijital para birimlerinden yararlanarak, geleneksel finansal araçları, kurumları ve engelleri aşarak, artan kolaylık, hız ve verimlilikle sınır ötesi işlemler gerçekleştirebilir (International Monetary Fund [IMF], 2020, s. 2). Ekonomik etkinin çeşitlendiğı günümüz dünyasında, kripto para birimlerinin ortaya çıkışı küresel ekonomik düzenin devam eden dönüşümüne katkıda bulunmaktadır.

3.3.2. 1929'dan Günümüze Dijitalleşen Finansal Hizmetler Sektörü

Finansal hizmetler sektörünün dijitalleşmesi, tarihi olaylar, teknolojik gelişmeler ve düzenleyici reformlarla şekillenmiştir. Dijitalleşen finansal hizmetler sektörünün 1919 Büyük Buhranı'ndan günümüze kadar gelişiminin analizini sunan çalışmanın bu bölümünde, II. Dünya Savaşı, 2008 mali krizi ve Bitcoin'in ortaya çıkışı gibi önemli tarihi olayları inceleyerek, bunların finans sektörü üzerindeki etkilerine ve ardından finansal hizmetlerin dönüşümünü açıklamaktadır.

İki savaş arasındaki dönemde, küresel ekonomik liderliğin ve işbirliğinin olmaması, savaş tazminatı ve kredilerin geri ödemeleri için yapılan baskı, sisteme liderlik edecek ve uygulanabilir bir kurtarma planının olmaması, uluslararası istikrar ve güveni yeniden tesis edecek kadar güçlü bir devletin yokluğu toparlanmanın önünde büyük bir engel olmuştur. 1924'ten sonra ABD'nin Avrupa'ya verdiği krediler, altta yatan ekonomik kırılganlıkları ve biriken küresel dengesizlikleri maskeleyemeye hizmet etmiştir. 1929'da Büyük Buhran yaşandığında tüm zayıflıklar açığa çıkmış ve dünya ekonomisini etkilemiştir (World Trade Organization [WTO], 2013, s. 46). Dow Jones Sanayi Ortalaması, Ağustos 1921'de 63'ten artarak Eylül 1929'da 381'e yükselmiştir. 24 Ekim 1929'da yaklaşık 13 milyon hisse senedi işlem görmüştür. J.P. Morgan ve

diğer birkaç banka pazarlara olan güveni geri kazanmak ve bankacılık sistemini kurtarmak için hisse senedi satın almış, ancak başarısız bir sonuç vererek hisse senetlerinde artışa yol açmıştır (Social Welfare, 2011). 28 Ekim 1929'da piyasalar yeniden açıldığında, rekor sayıda hisse senedi işlem görmüş ve borsa %22'den fazla değer kaybetmiştir. 28 Ekim 1929 Kara Pazartesi, Dow Jones Sanayi Ortalaması yaklaşık %13 düşüş yaşamış, 16 milyondan fazla hisse senedinin işlem gördüğü ertesi gün Kara Salı'da ise yaklaşık %12 bir düşüş yaşayarak Kasım ayı ortasına kadar değerinin neredeyse yarısını kaybetmiş ve 1932 yılına kadar düşüş devam etmiştir (Federal Reserve [FED], tarih yok).

Bu krizin etkisi, hisse senedi sahibi olmayan tarafları bile etkilemiş, kısa vadeli sermayeyi artıramayan işletmeler, çalışanlarını işten çıkartarak maliyeti düşürmüş, işsizlik artmış, stoklar artmaya başlamış ve bu durum fiyatların daha da düşmesine sebep olarak daha fazla işletmenin iflas etmesine neden olmuştur. Büyük oranda hisse senedine yatırım yapan bankalarda büyük miktarda para kaybetmiş ve bankacılık sistemine olan güven kaybedilmiştir. Bu süreçte FED daraltılmış para politikasıyla kriz döneminde para ve kredi arzını yanlış yöneterek faiz oranlarını yükseltmiş ve kredi almayı daha da zorlaştırmıştır. 1931 yılına gelindiğinde 2.294 Amerikan bankası iflas etmiş, 11 milyon insan işsiz kalmış ve bu durum II. Dünya Savaşı'na kadar devam etmiştir (Hughes, 1999).

Büyük Buhran'ın ekonomik çöküşü, finansal sistemdeki ciddi kusurları ortaya çıkararak düzenlemelerin ve gözetimin temelden yeniden değerlendirilmesine yol açmıştır. ABD hükümeti, 1933 tarihli Menkul Kıymetler Yasası ve Bankacılık Yasası (Glass-Steagall Yassı) gibi birkaç önemli düzenleyici önlem yürürlüğe koymuştur. Bu reformlar, finansal piyasalarda güveni yeniden tesis etmeyi, yatırımcıları korumayı ve bankacılık sisteminin istikrarını sağlamayı amaçlamaktaydı (FED, 1993) (U.S. Securities and Exchange Commission, 1993). Doğrudan dijitalleşme ile ilgili olmasa da, bu düzenleyici değişiklikler gelecekteki teknolojik gelişmeler ve finansal hizmetlerin dijitalleştirilmesi için temel oluşturmuştur.

Bugün kullanılan dijital teknolojilere benzer olmasa da, otomasyona ve elektronik işlemlerin gerçekleştirilmesine yönelik ilk adımlarda Büyük Buhran döneminde başlamıştır. Örneğin telgraf ve teleprinter sistemlerinin yükselişi, iletişim hızını ve doğruluğunu geliştirerek finansal bilgilerin daha hızlı iletilmesini sağlamıştır.

Özellikle teleprinter, vazgeçilmez bir ofis ekipmanı haline gelmiş ve finans piyasalarındaki tüccarların en son fiyatları takip etmelerini sağlamıştır (Science Museum, 2018). Sonuç olarak 1929 Büyük Buhran, o dönemde gelişmiş dijital teknolojilerin olmaması sebebiyle daha dolaylı ve temel bir şekilde de olsa, dijitalleşen finansal hizmetler sektörü üzerinde önemli bir etkiye sahiptir.

Yaşanan ekonomik güvensizlik ve ticaret savaşı siyasi güvensizliği besleyerek siyasi aşırılığın yükselmesine, güvenliğin azalmasına, yeniden silahlanma yarışına sebep olmuş ve nihayetinde II. Dünya Savaşı'nın yolunu açmıştır. 1944'ten sonra yaşanan gelişmeler ise uluslararası finans sisteminin doğasını derinden değiştirmiştir. Ticari ve ekonomik bağlar üzerine kurulu ortaklıkların yeni bir dünya savaşını engellemeye yardımcı olacağı teorisi ile 1944'te düzenlenen Bretton Woods konferansında kurulan IMF ve Dünya Bankası, küresel finansal sistemin şekillenmesinde önemli bir role sahiptir. Dünya Bankası, uzun vadeli yatırım projeleri, kurum inşası ve yoksulluğu azaltma gibi konulara odaklanarak hükümetlere finansman, politika takviyesi, teknik yardım sağlar ve geliştirmekte olan ülkelerde özel sektörü güçlendirmeyi amaçlar. IMF, uluslararası para sistemini istikrara kavuşturmaya hizmet ederek, dünya para birimlerinin izlenmesini sağlar ve üye ülkelerdeki ekonomiyi takip eder, ödemeler dengesinde güçlük çeken ülkelere kredi verir ve üyelere yardım sağlar (The World Bank, tarih yok). Savaş sonrasında küresel ölçekte finansal piyasaların gelişmesine ve bölgesel bütünleşmeye katkı sağlayan Dünya Bankası ve IMF'nin yanı sıra, bölgesel ölçekte Afrika Kalkınma Bankası, Asya Kalkınma Bankası, Avrupa Kalkınma Bankası, Amerikalılar Arası Kalkınma Bankası gibi Bölgesel Kalkınma Bankaları kurulmuştur (Brundtland Commission, 1987). Bu bankalar, uluslararası ticaret ve finansla artan odaklanma çerçevesinde sınır ötesi işlemlerde ve dijital finansal hizmetlerde gelecekteki gelişmelerin önünü açmıştır.

Savaş, uzun vadede finansal hizmetler sektörünün dijitalleşmesi üzerinde önemli bir etki yaratmıştır. Hükümetler ve askeri kuruluşlar, iletişim, kriptografi ve veri işleme için ileri teknolojileri geliştirmeye yatırım yapmaya başlamış ve bu teknolojik gelişmeler, finansal hizmetler sektöründe gelecekteki dijitalleşme çabalarının temelini atmıştır.

1929 Büyük Buhranı, İkinci Dünya Savaşı ve 2008 mali krizinden bu yana bankacılık düzenlemeleri riskleri azaltmak ve müşterileri korumak için sürekli değişim

ve gelişim göstermeye başlamıştır. Finansal kırınlıkları ortaya koyan krizlerin sonucunda ulus devletler, geleceği göz önüne alarak düzenleme tedbirlerini almaya başlamış ve finansal tarih önemli ölçüde değişmiş, hem uluslararası kurumlar kurulmuş hem de şirketler kurumsallaşmıştır. Toplumun büyük mali kurumlara ve fiziki paraya olan güveninin yok olduğu dönemlerde, yeni bankalar krizden fayda sağlayarak halka yenilenmiş bir bankacılık deneyimi sunmaya başlamıştır. Özellikle daha fazla şeffaflık, kullanıcı dostu yönler ve daha kolay kullanım sayesinde dijital bankacılık girişimi dünyanın bir çok yerinde yaygınlaşmaya başlamıştır. Dolayısıyla finansal kurumlar, operasyonel ve mülkiyet açısından giderek daha fazla küresel hale gelmiş ve birçok büyük banka, daha da büyük bankalar oluşturmak için birleşmiştir.

Dijital bankacılığın geliştiği bu dönemde şeffaf, gizli ve güvenli bir işlem ağı esasıyla oluşturulan blok zinciri teknolojisi ve kripto paralar da ulus devletlerin, çok uluslu şirketlerin ve bireylerin ilgisini çekmiştir. Özellikle kripto para biriminin ilk örneği Bitcoin (BTC), ilk çıktığı dönemde piyasa değeri olarak çok düşük bir ücret karşılığında alınması dikkatleri üstüne çekmemesine neden gösterilmiştir. Teknolojik altyapının gelişmesi ve uygun altyapının oluşmasıyla birlikte bir ihtiyaç olarak BTC'nin değeri şu anda, kripto para birimleri arasında en yüksek piyasa değerine sahiptir ve hem yatırımcıların hem de politika yapımcıların ilgisini çekmektedir (Yetgin & Baştuğ, 2022, s. 48).

3.3.3. Finansal Teknolojinin Gelişimi

20. yüzyılın sonlarında ve 21. yüzyılın başlarında teknolojik gelişmeler ve internetin yükselişi, finansal hizmetler dünyasında devrim yaratmış ve sektör giderek rekabetçi bir hale gelmiştir (Sohail & Shanmugham, 2003). Uluslararası transferler, elektronik bankacılık, kredi kartlarının yükselişi, banka operasyonlarını desteklemek için tasarlanmış ATM'lerin ortaya çıkışı ve POS, telefon bankacılığı, dijital hizmet kanalları olan internet bankacılığı ve mobil bankacılık sistemleri gibi teknoloji destekli devrimler yaşanmıştır.

Teknolojik gelişmelerin de yardımıyla bankalar, müşteri memnuniyetini artırmaya odaklanan bir strateji benimsemiştir. Yaygınlaşan müşteri odaklı hizmet anlayışı, azalan işletme maliyeti, rekabetçi piyasa yapısı ve tüketicilerin bankacılık ürünlerine hızlı, etkin ve verimli bir şekilde ulaşabilir olması, yetersiz hizmet alan veya

uzak bölgelerdeki bireylerin ve işletmelerin finansal hizmetlere erişmesini sağlaması sonucunda web tabanlı bankacılık ürünlerine olan talep artmıştır (Şanlı & Hobikoğlu, 2015).

ATM (Automated Teller Machine); Bankacılık işlemlerinin doğrudan şubeden yapılmasına ilave olarak 1967 yılında ilk ATM'nin kurulması nakit para çekme, para yatırma, para transferi, elektrik ve kredi kartı faturalarının ödenmesi ve diğer finansal işlemlerin gerçekleştirilmesini sağlayan yenilikçi bir hizmet olarak ortaya çıkmıştır. İlk ATM, John Shepherd-Barron tarafından geliştirilmiş ve ilk olarak Londra'daki Barclays Bank'ta kurulmuştur (Konheim, 2016).

POS (Point of Sale); 1879'da çalışan hırsızlığını durdurmak amacıyla nakit işlem miktarını kaydeden otomatik olmayan bir yazarkasanın icadından sonra, 1906'da işlemlerin hızlı bir şekilde gerçekleştirilmesini sağlayan elektrikle çalışan bir yazarkasa icat edilmiştir. 1973 yılına gelindiğinde ilk POS sistemleri piyasaya sürülmüş ve IBM ilk bilgisayar tabanlı elektronik yazar kasayı duyurmuştur. 2000'li yıllarda ise bulut teknolojisinin POS sitemine entegre edilmesiyle POS sistemi dijital bir dönüşüm geçirmiştir. Çünkü her işlemin verileri ve müşterilerin bilgileri, yerinde bir sunucuya olan ihtiyacın ve maliyetin azaltılmasıyla bulut depolama alanına saklanmaktadır (BooksPOS, tarih yok). İşletmeler için kayıt tutmak kolaylaşmış ve otomatik sistem yardımıyla her işlem yönetilebilir hale gelmiştir.

Kredi Kartı; 1914'de Western Union, "Metal Para" adı verilen ilk tüketici kredi kartını piyasaya sürmüştür. Ancak modern kredi kartları gibi kullanılabilen metal para, piyasaya sürüldüğü dönemde daha sınırlı ve yalnızca seçkin müşteri grupları tarafından kullanılabilmekteydi (Western Union, 2019). 1920'lerde petrol şirketleri ve otel zincirleri gibi bireysel firmaların, şirket satış noktalarında yapılan alışverişler için müşterilere kart vermesiyle ABD'de yaygınlaşmaya başlamıştır. 1950'de ilk evrensel kredi kartı olan Diners Club Card piyasaya sürülmüştür. 1953 yılına gelindiğinde İngiltere, Kanada, Küba ve Meksika'daki işletmeler, Diners Club Card'ı uluslararası kabul görmüş ilk ödeme kartı olarak kullanmaya başlamıştır (Diners Club International, tarih yok). Diners Club Card'ın ortaya çıkmasından kısa bir süre sonra, Chase, Capital One ve Bank of America gibi büyük bankalar tarafından kredi kartları verilmeye başlanmıştır. Bank of America, 1958'de Kaliforniya'daki birkaç müşterisine ilk kredi kartlarını göndererek kullanıma sunan ilk banka olmuştur (Murray, 2022).

Günümüzde fiziksel kredi kartları dönüşmekte, tüketiciler dijital bankacılık seçeneklerine yönelmekte ve sanal kredi kartları popülerlik kazanmaktadır. Sanal kredi kartları, çevrimiçi alışverişlerde kullanılmak üzere fiziksel kartlara eklenerek yeni bir kart numarası oluşturularak kullanılmaktadır. Farklı bir kredi kartı numarasına sahip gibi görünen sanal kredi kartları, fiziksel kartlardan farklı olarak ek bir güvenlik katmanı sağlamaktadır (Murray, 2022).

SWIFT (Society for Worldwide Interbank Financial Telecommunication); 1973'te Belçika'da 15 ülkeden 239 banka, uluslararası para transferlerinin gerçekleştirilmesi için kullanılan iletişim ağı SWIFT'i kurmuştur. SWIFT, dünya genelindeki finansal kurumlar arasında güvenli, hızlı ve standartlaştırılmış iletişimi sağlamaktadır. 1977 yılında mesajlaşma faaliyetlerini hayata geçiren SWIFT, bir yıl içinde 10 milyon mesajı, 1983 yılına gelindiğinde 52 ülkeden 1.000'den fazla kullanıcıya hizmet vererek, 46.9 milyon mesajı işlemiştir. Günümüzde ise SWIFT, 200'den fazla ülke ve bölgeyi kapsayan, dünya çapında 11.000'den fazla kuruma hizmet veren küresel bir finansal altyapıya dönüşmüştür (Swift, tarih yok). Dijitalleşme SWIFT'in rolünü ve işleyişini de etkilemiştir. SWIFT ile gerçekleştirilen para transferleri manuel süreçlerden geçerken, dijitalleşme ile birlikte otomatikleştirilmiş ve daha hızlı işlemler mümkün hale gelmiş, aynı zamanda veri analitiği ve risk yönetimi çözümlerini geliştirmiştir.

Çevrimiçi bankacılık veya internet bankacılığının ilk versiyonu 1981'de, New York City'deki Citibank, Chase Manhattan, Chemical Bank ve Manufacturers Hanover bankaları tarafından sabit telefon kabloları aracılığıyla müşterilerinin kişisel hesaplarına uzaktan erişim sağlamasıyla ev bankacılığı hizmeti olarak başlamıştır. İnternet aracılığı ile çevrimiçi bankacılığa dönüşüm ise Ekim 1994'te Stanford Federal Kredi Birliği'nin bankacılık hizmetlerine yönelik ilk web sitesini kurmasıyla başlamış ve tüm müşterilerine çevrimiçi bankacılık sağlayan ilk finans kurumu olmuştur (Zeybek, 2018, s. 83).

1990'lı yılların ortalarında finans kurumları internet bankacılığı hizmetini hayata geçirmek için adımlar atarken, birçok tüketici güvenlik konusundaki endişeleri sebebiyle internet üzerinden parasal işlem yapmak konusunda tereddüt göstermiştir. Bu dönemde Amerika Online, Amazon.com ve eBay gibi şirketler elektronik ticaretin

yaygın olarak benimsenmesini sağlamıştır (Keivani, Jouzbarkand, Khodadadi, & Sourkouhi, tarih yok).

Mobil Bankacılık; Çevrimiçi bankacılığın bir uzantısı olan mobil bankacılık, finansal işlemlerin gerçekleştirilmesi için mobil cihazların kullanımını ifade etmektedir. Mobil bankacılıkta hizmetler, mobil uygulamaların kullanıma sunulmasından önce SMS ve metin yoluyla gerçekleştirildiği için SMS Bankacılığı olarak bilinmektedir. Mobil web ve kablosuz uygulama protokolünün (WAP) piyasaya sürüldüğü 1999 yılında müşterilere ilk mobil bankacılık platformu sunulmuştur (Sorbet, 2022).

2000'li yılların başında iOS ve Android işletim sistemli akıllı telefonların gelişmesiyle birlikte mobil bankacılık uygulamaları da gelişmiştir. Bankaların müşterileri çekmek için uygulamalarına gelişmiş özellikler eklemesiyle, kolay erişilebilirliğe sahip uygulamalar müşteriler için daha cazip hale gelmeye başlamıştır. Özellikle Apple, 2007'de ilk iPhone'u piyasaya sürdüğünde, sadece iletişim kurma biçiminde devrim yaratmakla kalmadı, aynı zamanda bu yeni teknolojik cihaz, akıllı telefonlardaki bankacılık hizmetlerini kolaylaştırarak ve basitleştirerek mobil bankacılığın gelişimini hızlandırmıştır (Sorbet, 2022). Sonucunda birçok şirket ve finans kurumu geleceğe tamamen farklı şekilde bakmaya başlamış ve teknolojinin getirdiği fırsatları değerlendirmiştir.

Dijital Bankacılık / Neobanka; Teknolojinin her bankacılık faaliyetine uygulandığı dijital bankacılık, mobil bankacılıkta olduğu gibi fiziksel bir yerde olma zorunluluğunu ortadan kaldırır ve tüm hizmetin çevrimiçi olarak sunulmasını sağlar. Ancak erişim açısından mobil bankacılık, yalnızca Android veya iOS işletim sistemi olan mobil cihazlar veya internet üzerinden uygulamalar aracılığıyla işlem yapmaya izin verir. Dijital bankacılık ise internet bağlantısı veya uyumlu bir cihaz yardımıyla birden çok yol sunarak bankacılık işlemi yapmaya olanak tanır (Volenik, 2023).

İsviçre ve Singapur'da merkezleri bulunan Sygnum Bank, dünyanın ilk dijital varlık bankası olarak küresel erişime sahiptir. Sygnum, kurumsal ve özel nitelikli yatırımcılara, şirketlere, bankalara ve diğer finansal kurumlara dijital varlık sisteminde yatırım yapma yetkisi vermektedir (Sygnum Bank, 2021).

2005 yılında ING Direct¹⁰, Kanada'da President's Coice Financial, İngiltere'de HSBC Direct ve First Direct gibi fiziksel şubesiz faaliyet gösteren bankalar hizmetlerini öncelikle çevrimiçi olarak sunmaya başlamıştır (Candemir, 2020, s. 83).

Avrupa'da kurulan ilk faizsiz ve tamamen dijital banka Albaraka Türk tarafından geliştirilen Insha, Almanya'da dijital katılım bankacılığı hizmetleri vermeye başlamıştır (Papuççıyan, 2018). 2020 yılında faaliyet gösteren ve İngiltere'de Müslüman toplum için kullanıma sunulan Niyah, ülkede piyasaya sürülen ilk İslami dijital bankacılık uygulaması ve etik finansal pazar platformu olarak dijital bankacılık hizmetiyle faaliyet göstermektedir. Platform, dijital banka hesapları, banka kartları, yatırımlar, küçük ve orta ölçekli işletme finansmanını içeren faizsiz bankacılık ürünlerini içermektedir (Eyidilli, 2020).

Dijital bankacılık yapay zeka ürünü olan sohbet robotlarını da içermektedir. Örneğin Capital One'ın Eno uygulaması, hızlı bilgi sunan ve kredi kartı ödemeleri, hesap görüntüleme gibi görevleri 7/24 yürüten sanal bir asistandır (Capital One, tarih yok).

Dijitalleşme doğası gereği dijital olan temel ürünlerde ve değer zincirlerinde köklü bir dönüşüme yol açmıştır. Dijital bankacılık ürünlerinin pazara sunma süresi kıaldıkça, binlerce FinTech girişimi ve diğer banka dışı kuruluşlar, ödemelerde bankacılığın tüm alanları için oluşturulan yeni ürünler, hizmetler ve iş modelleri gelişmektedir (Gasser vd., 2017).

Finansal Teknoloji (FinTech); Terim olarak "finans-finance" ve "teknoloji-technology" kelimelerinin birleşiminden oluşan FinTech, finans sektörünün dijitalleşmesini tanımlamak için kullanılan bir terimdir ve finansal faaliyetleri iyileştirmek, hızlandırmak ve verimliliğini artırmak için mobil merkezli bilgi ve iletişim teknolojisini kullanan gelişmekte olan bir endüstri olarak kabul edilmektedir (Kim, Park, Choi, & Yeon, 2015 , s. 137).

FinTech girişimleri, müşteri ihtiyaçlarına fayda sağlamak için aracıyı ortadan kaldıran gelişmiş iş modelleri ve teknoloji destekli ürün veya hizmet sunarak tüketicilerin finansal işlemlerinin şeklini değiştirmektedir. E-ticaret alanındaki internet tabanlı teknolojiler, çevrimiçi ödemeler ve para transferi, kredi alma, sigorta

¹⁰ ING Direct, 2012 yılında Capital One'a devredilmiştir (ING, 2012)

oluřturma, kripto yatırımı, dijital cüzdanlar, uluslararası işlemler, tasarruf ve yatırım, güvenlik çözümünde kullanılan yüz tanıma veya parmak izi uygulamaları gibi finansal hizmetleri sağlamak ve dijitalleřtirmek için en modern teknolojilerin kullanılmasını içermektedir. Bu teknolojiler, otomasyon, yapay zeka, makine öğrenimi, büyük veri, veri analitiđi, bulut biliřim, blok zinciri, robo-danışmanlık, nesnelerin interneti gibi yeni teknolojiler içermektedir (Dapp, 2014, s. 5).

Bazı uzmanlara göre, bankamatiklerin ortaya çıktığı 1960'lı yıllar, FinTech oluşumunun başlangıcı olarak görölmektedir. Aslında FinTech küresel teknoloji şirketlerinin ve yeni çevrimiçi hizmetlerin yayılmasıyla aynı anda ortaya çıkmıştır. Örneđin 1998'de çevrimiçi para transferiyle ödeme yapılmasını sağlayan PayPal (O'connell, 2020), geleneksel ödeme yöntemlerine dijital bir alternatif sunan, kullanıcıların bir banka hesabı veya kredi kartına ihtiyaç duymadan çevrimiçi para göndermesine ve almasına izin veren öncü FinTech şirketlerinden biridir.

Dijitalleşme, finans sektöründe ödeme sistemlerinde yeni ürün ve hizmetlerin ortaya çıkmasını da sağlamaktadır. Kolay ödeme hizmetlerinin öncülüğünde mobil ödemenin yaygınlaşması, FinTech hizmetleri arasında en hızlı büyüme gösteren girişimdir. Apple tarafından -sadece ABD'de kullanılabilen- "Apple Pay" ve "Apple Cash", Google tarafından "Google Pay" hizmetinin oluşturulması, kolay bir şekilde mobil ödeme uygulamasının şekillenmesini sağlamıştır. Google, satılan Android telefonlara önceden yüklenmiş Google Pay uygulamasını oluşturmak için Verizon, AT&T ve T-Mobile gibi telekomünikasyon şirketleri ile işbirliği yapmıştır (Chuen & Teo, 2015, s. 2).

FinTech hizmetleri arasında yer alan ve büyüme gösteren diğeri bir girişim, temassız ödeme yöntemidir. ABD ve İngiltere'de Amazon'un kasiyersiz ve nakit işlemsiz süpermarketi Amazon Go girişimi FinTech başarılarından biridir. Amazon Go mağazasında, tüketiciler mobil cihazlarındaki Amazon uygulamasını tarattıktan sonra alışveriş yapmaktadır. Mağaza genelinde stratejik olarak yerleştirilmiş kameralar, gelişmiş bilgisayar görüşü ve makine öğrenimi yazılımı, tüketicilerin alışveriş etkinliklerini izleyerek, alınan her ürünü otomatik olarak Amazon hesaplarındaki sanal alışveriş sepetine eklemektedir. Tüketiciler, mağazadan çıktıktan sonra ise Amazon, satın alma işlemi için bir makbuz göndermektedir (Günen, 2019).

Ödeme kolaylığı sağlayan diğer bir uygulama Mastercard Kimlik Kontrolü (Identity Check Mobile), telefonlardaki parmak izi tarayıcısı veya bir öz çekim (selfie) fotoğrafı ile yüz tanıma teknolojisi aracılığıyla kimlik doğrulayarak ödeme işlemini gerçekleştirmesini sağlamaktadır. Kullanıcıların bu sistemden yararlanabilmeleri için önce uygulamayı indirmesi ve daha sonra şirkete yüz biyometrik verilerini göndermesi gerekmektedir (Mastercard, 2016).

Finansal işlemler için gelişmiş yapay zeka yönlendirmeli ve insan benzeri kullanıcı desteği sağlayan sohbet botları/sanal asistanlar da, finans sektöründe soruları -özellikle tekrarlayan müşteri sorularını- saniyeler içerisinde çözebilen ve 7/24 hizmet verebilen bir teknolojidir. Örneğin Bank of America'nın yapay zeka özellikli sanal finans asistanı olan Erica, piyasaya sürüldüğü 2018 yılından beri yaklaşık 32 milyon müşteriye, makine öğrenimi, gelişmiş analitik ve bilişsel mesajlaşma kullanarak günlük finansal ihtiyaçlarında yardımcı olan bir teknolojidir. Erica, Bank of America müşterilerinin ihtiyaç duyduğu alanlardaki -nakit akışı, yaklaşan faturalar, işlem geçmişi, hesaptaki bakiyeler gibi- bir dizi veriyi değerlendirerek sorularına destek sağlamaktadır (Bank of America, tarih yok).

3.3.4. Finansal Teknoloji Şirketleri

Finansal teknoloji şirketleri, mevcut finansal şirketler tarafından sağlanan finansal hizmetlerin kullanımını geliştirmeyi veya değiştirmeyi amaçlayan, gelişmekte olan yazılım projelerinden ve köklü teknoloji şirketlerinden oluşmaktadır (Alduhaidahawi, Zhang, Salam, Sebai, & Harjan, 2020). The Brainy Insights tarafından hazırlanan rapora göre küresel finansal teknoloji pazarının büyüklüğü 2021'de 115,34 milyar dolardır. Dijital ödemelerin ve cüzdanların artan kullanımı ve teknoloji tabanlı çözümlere yapılan artan yatırımlarla, 2022'den itibaren %36,2'lik yıllık büyüme oranıyla, 2030 yılına kadar 936,51 milyar dolara ulaşması beklenmektedir (The Brainy Insights, 2021).

3.3.5. Çin, ABD ve Avrupa'da Geleneksel Bankalar ve Finansal Teknoloji Şirketleriyle İşbirliği

Bankalar, finansal teknoloji şirketleriyle işbirliğine girme konusunda giderek daha aktif hale gelmektedir. Geleneksel bankalar ve finansal teknoloji şirketleri arasındaki karşılıklı yarar sağlayan işbirliği, bankaların basit veri tabanlı finansal ürünlerinin kalitesini artırmasını, yenilikçi çözümler oluşturmasını ve maliyetlerini düşürmesine olanak tanımaktadır (Romanova & Kudinska, 2016). Bu işbirlikleri, finansal hizmetlerin daha iyi ve kapsamlı bir şekilde sunulmasını sağlamaktadır.

Ulus devletler, finansal sistemlerinde teknolojik ilerlemeleri teşvik etmek için rekabet etmektedir. Bu doğrultuda güvenli ödeme sistemleri, çevrimiçi bankacılık platformları ve dijital işletmeleri destekleyen düzenleyici çerçeveler sunarak ve sağlam bir dijital finansal altyapı geliştirerek işletmeler ve yatırımcılar için sektörü çekici hale getirmeyi hedeflemektedir. Dolayısıyla ulus devletlerin finans endüstrisi, teknolojik ilerlemeler, değişen tüketici davranışları ve hükümetin inovasyona verdiği desteklerin etkisiyle FinTech hızlı bir büyüme yaşamıştır.

Çin'de geleneksel finansal kurumlar, büyük teknoloji şirketleriyle ortaklık kurma stratejisi izlemektedir. Örneğin Alipay'ın ana şirketi olan Ant Group, dijital finansal hizmetler sağlamak için Çin'deki geleneksel bankalarla işbirliği yapmaktadır. Dünyanın en büyük bankalarından biri olan Çin İnşaat Bankası (China Construction Bank), Ant Financial ve Alibaba ile stratejik bir ortaklık imzalayarak, mevcut ödemelerini ve e-ticaret işini yürütmek amacıyla Ant Financial teknolojisini ve Alibaba platformlarını kullanmaya başlamıştır (McKinsey, 2018).

WeChat Pay'in arkasındaki şirket olan Tencent, Bank of China da dahil olmak üzere çeşitli geleneksel bankalarla ortaklıklar kurmuştur. Bu işbirlikleri sayesinde Tencent, mobil ödeme platformunu bu kurumların bankacılık uygulamalarına entegre ederek müşterilerinin sorunsuz bir şekilde ödeme yapmasına, para transfer etmesine ve ek finansal hizmetlere erişmesine olanak tanımaktadır. 2015 yılında Tencent ve kentsel ticaret bankası Bank of Beijing 1,6 milyar dolarlık çevrimiçi bankacılık anlaşması başlatmıştır. Aynı zamanda ortaklığının sonucunda, bankanın, kullanıcıların hastanelerde tıbbi bakım ve diğer hizmetleri almak için çip özellikli bir kart kullanmasına izin veren Jingyitong girişimine odaklanacağını açıklamıştır (Reuters, 2015).

ABD'nin en büyük bankalarından biri olan *JPMorgan Chase*, 2016 yılında çevrimiçi bir borç verme platformu olan OnDeck ile bir ortaklık kurmuştur. Bu ortaklık sayesinde JPMorgan Chase, küçük işletme kredilendirme sürecini kolaylaştırmak ve basitleştirmek için OnDeck'in teknoloji platformuna erişim elde etmiştir. Ortaklık stratejisi ile ilerleyen JPMorgan bir ipotek finansal teknoloji şirketi olan Roosfity ve güvenli mesajlaşma uygulaması olan Symphony dahil birkaç finansal teknoloji şirketi ile ortaklık kurarak dijital stratejisini oluşturmaktadır (McKinsey, 2018).

Bir yatırım bankacılığı şirketi olan *Goldman Sachs*, 2019'da Apple Card'ı piyasaya sürmek için Apple ile işbirliği yapmıştır (Goldman Sachs, 2019). Goldman Sachs aynı zamanda Square, Bluefin Payments, Bill Trust, Revolution Money gibi alternatif finans şirketlerine önemli yatırımlar yapmıştır.

Küresel bir bankacılık kurumu olan *Citigroup*, mobil bankacılık hizmetlerinin geliştirilmesinden sorumlu bir Citi FinTech birimi kurmuştur (Macheel, 2015). Citigroup, müşterilerine mobil cihazlarını kullanarak temassız ödeme yapma olanağı sunmak için Google Pay ile ortaklık kurarak, müşterilerinin kredi veya banka kartlarını Google Pay platformuna bağlamasına ve katılımcı satıcılarda güvenli ödemeler yapmasına olanak sağlamıştır (Citi, 2020).

Önde gelen kredi kartı düzenleyicisi American Express, 2020'de kart sahiplerine küçük işletme kredileri sunmak için çevrimiçi bir borç verme platformu olan Kabbage ile ortaklık kurmuştur. 2023 yılında ise American Express, küçük işletmeler için bir dizi dijital nakit akışı yönetimi aracı olan American Express Business Blueprint'i piyasaya sürmüştür. Business Blueprint, şirketin 2020'de satın aldığı alternatif borç verme girişimi olan Kabbage'den geliştirdi ve piyasaya sürülmesiyle Kabbage markası artık kullanımdan kaldırıldı. Platform, nakit akışını yönetmelerine, kredi almalarına, faturaları ve satıcılara ödeme yapmalarına, hesap bakiyelerini kontrol etmelerine, çekleri yatırmalarına, kart ödemelerini kabul etmelerine ve daha pek çok şeye yardımcı olarak küçük işletme sahiplerinin yükünü hafifletmeyi hedeflemektedir (Muhn, 2023).

Avrupa'da ise Almanya'nın en büyük bankalarından biri olan Deutsche Bank, Alman FinTek şirketi Traxpay ile ortaklık kurarak tedarik zinciri finansmanını genişletmeyi amaçlamıştır (Deutsche Bank, 2020). Deutsche Bank, açık bankacılık ve

mevduat piyasası çözümlerinde uzmanlaşmış FinTech şirketi olan Deposit Solutions ile ortaklık kurmuş, 2019 yılında ise Deutsche Bank, Deposit Solutions'ın %4.9 hissesini satın almasıyla dijital bir platform olarak faaliyet gösterme niyetini açıklamıştır (Deutsche Bank, 2019).

Lüksemburg merkezli Banking Circle ise Avrupa'da anında ödeme hizmetini başlatmak için Avrupa'nın önde gelen yüksek teknoloji şirketi SIA (Studio Informatico Associato) ile işbirliği kurmuştur. Ultra hızlı ağ altyapısına sahip olan SIA ile ortaklığı sonucunda, Avrupa finans kuruluşlarının ve şirketlerinin tavan limiti 100.000 avro olarak belirlenmiş tutarla 7/24, saniyeler içinde ödeme yapmaları sağlanmaktadır (Banking Circle, 2021).

Hollanda'nın en büyük üçüncü bankası olan ABN AMRO, kullanıcılarının tekrarlı ödemelerini ve aboneliklerini yönetmeleri için Danimarkalı FinTech şirketi Subanio ile işbirliği yaparak kullanıcıların ödemelerini çevrimiçi olarak gerçekleştirebilmelerini sağlamıştır (Hamann, 2021).

İspanyol çok uluslu bir banka olan BBVA, 2015 yılında İngiltere merkezli bir dijital banka olan Atom Bank'ın %29,5'lik hissesi içi 45 milyon Sterlin yatırım yapmıştır. BBVA'nın yatırımı, Atom Bank'ın dijital bankacılık platformunu geliştirmesine ve hizmetlerini genişletmesine yardımcı olmuştur. Ayrıca BBVA, ABD'de insanların bankacılık ve para hakkında düşünme şeklini değiştiren bir teknoloji şirketi olan Oregon merkezli Simple'ı satın almıştır. Buna ek olarak, 100 milyon dolarlık BBVA Ventures fonu ile önde gelen FinTech işletmelerine yatırım yapmıştır (Atom Bank, 2015).

3.3.6. Çin'de Dijitalleşen Bankacılık

Çin'de finansal hizmetler piyasası uzun süre devlet tarafından düzenlendiği ve finansal teknolojilerin gelişmesi risklerle ilişkilendirildiğinden, finansal hizmetler alanında yeniliklere ihtiyaç duyulmamıştır. Ancak ekonomideki karşılıklı birbirine bağımlılık, bankacılık sektöründeki liberal reformlar, toplumun teknolojik gelişimi ve Çin halkının bilgiye erişim seviyesinin artması daha gelişmiş finansal araçlara olan ihtiyacı beraberinde getirmiştir (Gupta & Xia, 2018). Özellikle Çin'de değişen duruma ilk tepki veren e-ticaret şirketleri olmuştur; AliPay'i oluşturan Alibaba ve WeChat'i

oluşturan Tencent başarılı örnekler olarak sunulabilir (Guliev, Khubaeva, Chernysheva, & Kolesova, 2021). Günümüzde Çin hükümeti dijital ekonomiyi güçlü bir şekilde destekleyen bir ülkedir ve dijital bankaların kurucuları ve geliştiricileri ise WeChat, Baidu, Taobao ve Xiaomi gibi güçlü holdinglerdir.

Çin Halk Bankası, 2014 gibi erken bir tarihte merkez bankası dijital para birimini incelemeye başlamış ve kendi Dijital Para Birimi Enstitüsünü kurmuştur. 2019'un sonlarında ise Çin Halk Bankası yetkilileri, merkez bankasının dijital para biriminin üst düzey tasarımını, standartlarını ve operasyonel testini tamamladığını açıklamıştır (Huang, 2020). Ancak Çin'in dijital para birimi araştırmasında diğer tüm büyük ekonomilerden daha ileride olmasına rağmen, dijital parasının pazara girmesi için önünde ekonomik ve politik zorluklar mevcuttur.

Çin'de dijital banka ve FinTech örnekleri;

- Çin'deki ilk dijital banka Tencent'in oluşturduğu WeBank, Çin'de en fazla varlığa, net kara ve en çok krediye sahip en büyük dijital bankadır (Osawa, 2019). Tencent bir sosyal ağ yazılımı olan WeChat ile piyasaya girmiştir.
- Finans ve ticaret hizmetlerini tek bir şemsiye marka altında birleştiren Alibaba'ya bağlı Ant Group, 2004'te çevrimiçi ödemeler için Alipay uygulamasını başlatmıştır (McKinsey, 2018).
- 2017'de Citic Bank ve arama motoru Baidu'nun ortak girişimi ile kurulan Çin'deki ilk devlet kontrollü dijital banka Aibank, tüketicilere ve küçük işletmelere çevrimiçi kredi sağlamaya başlamıştır (Volenik, 2022).

3.3.7. Avrupa Birliği'nde Dijitalleşen Bankacılık

Avrupa'da bireylere ve şirketlere sunulan çok sayıda bankacılık çözümü vardır. AB'nin dijital bankacılık alanında yapılacak düzenlemeler için Eylül 2020'de Avrupa Komisyonu, rekabetçi bir AB finans sektörü için gelecek yıllarda finans sektörünü şekillendirecek "*Dijital Finans*" ve "*Perakende Ödemeler*" stratejisini yayınlamıştır. Komisyon, söz konusu stratejilerin yanı sıra "*kripto paralar*" ve "*dijital dayanıklılık*" ile ilgili iki farklı yasa tasarısını aynı gün yayınlayarak, dört farklı stratejiyi "Dijital Finans Paketi" adıyla kamuoyuna sunmuştur. Özellikle "*Finansın geleceği dijital*"

mottosuyla başlayan Dijital Finans Stratejisi, Avrupa'nın finansın dijital dönüşümünü nasıl destekleyeceği konusunda bir çerçeve sunmakta ve dört ana öncelik belirlemektedir:

(I) Dijital Tek Pazar'a geçiş, (II) Dijital inovasyonu kolaylaştırmak için AB düzenleyici çerçevesini uyarlamak, (III) Veriye dayalı inovasyonu teşvik etmek için Avrupa finans veri merkezi oluşturmak, (IV) Finansal sistemin dijital operasyonel dayanıklılığını artırmak ve dijital dönüşümle ilgili zorlukları ve riskleri ele almak (Altaş, 2020, s. 29).

AB'de dijital banka ve FinTech örnekleri (Almay, 2022);

- 2012'de kurulan Bunq, Hollanda'da dijital olarak faaliyet gösteren ilk bankadır ve SWIFT transferlerinde kullanılmaktadır.
- 2009'da İrlanda'da kurulan CurrencyFair, pahalı ve yavaş olan sınır ötesi transfer sorununu çözmek amacıyla İrlanda'da kurulmuştur.
- 2011'de Finlandiya'da serbest meslek sahipleri için oluşturulan Holvi, küçük ve orta ölçekli işletme sahiplerinin faturalama ve raporlama gibi iş fonksiyonlarının basitleştirilerek büyümelerine yardımcı olmak amacıyla oluşturulmuştur.
- 2013'te Almanya'da kurulan Alman neobankası N26, sık seyahat edenler ve göçmenler için özel olarak geliştirilmiş bir bankadır. Dünyanın her yerindeki ATM'lerden ücretsiz para çekme, seyahat sigortası oluşturma gibi hizmetler sunmaktadır.
- 2015'de kurulan Curve, Avrupa'da ve eski AB üyesi İngiltere'de yaşayan müşterilerine e-para hizmetleri sunan Londra merkezli bir finansal teknoloji şirkettir. Birden fazla banka kartını tek bir yerde işlenmesini sağlamak ve paraya çevrilebilen puan toplama gibi ödüller sunan işlevlere sahiptir.
- 2017'de kurulan Bnext, 2020 yılında İspanya Merkez Bankası tarafından resmi olarak banka lisansına sahip olmuştur. Kredi ve sigorta hizmetlerine ek olarak Bitcoin ve Ethereum hesaplarını açma hizmeti de sunmaktadır.
- 2019'da Alman bankası Nuri, Solarisbank ile karşılıklı işbirliği yaparak geleneksel ulusal para birimini Bitcoin ve Ethereum gibi kripto para desteğiyle birleştirerek ilk gerçek kripto para bankasını oluşturmayı amaçlamıştır. Bitcoin ve Ethereum kripto para birimlerinden ikisini satın alma seçeneğine ek olarak kullanıcılara Avro ile işlemlerini gerçekleştirmeyi sunmaktadır.

- 2015'te İsveç, Norveç ve Danimarka'da 325.000'den fazla müşterisi olan Danimarka bankası Lunar, ilk pan-İskandinav bankasını oluşturmak amacıyla kurulmuştur.

3.3.8. ABD'de Dijitalleşen Bankacılık

ABD'nin finansal hizmetler sektörü, küresel finansal sistemi için temel oluşturmaktadır. ABD dolarının uluslararası finansal sistemdeki etkisi ve fiili küresel rezerv para birimi olması, ABD'nin ulusal güvenlik stratejisi için kritik bir alandır ve bu alandaki etkisini korumak ve rekabetçi kalabilmek için finansal hizmetler sektöründe dijitalleşmeye olan yatırımlarını artırmaktadır.

ABD, dijital para birimi ve blok zincirindeki gelişmeleri yakından takip etmesine rağmen, ABD dolarının dijital formu olan "merkez bankası dijital para birimi" konusunda daha şüpheci durmaktadır. 2016'da Federal Rezerv Bankasının dijital para birimlerini incelediği bir finansal teknoloji grubunda "FedCoin" fikri önerilmiş olsa da, ABD hükümeti tarafından ilgi görmemiştir. ABD'nin dijital para biriminde izlediği strateji büyük olasılıkla, diğer ülkelerdeki dijital para birimlerinin finansal kapsayıcılığının ne ölçüde olacağı, siber tehditlere karşı nasıl güvenlik önlemlerinin alınacağı ve finansal krizlerde nasıl etkileneceği konusundaki deneyimleri gözlemleyerek ilerleyecektir (Chorzempa, 2021, s. 106). Çünkü ABD hükümetinin bu stratejisi, dijital para birimi girişimindeki deneme ve yanılma riskini önemli ölçüde düşürecektir. 2022'de Beyaz Saray Bilim ve Teknoloji Politikası Ofisi'nin, merkez bankası dijital para birimi için teknik olanakların sunulduğu raporda, dijital para birimi için birçok faydadan bahsedilse de, henüz ABD hükümeti için hala bir olasılık olarak beklemede kalan bir girişimdir.

2019 verilerine göre JP Morgan Chase, teknoloji harcaması için 11.4 milyar dolar, Bank of America, 10 milyar dolar, Wells Fargo 9 milyar dolar ve Citigroup 8 milyar dolar harcama planlamıştır (Şevlin, 2019).

ABD'de dijital banka ve FinTech örnekleri;

- JP Morgan Chase'in ABD ticari bankacılık işletmesi olan Chase, dijital bankacılık stratejisini benimsemiştir. Chase Mobile Bankacılık ile fatura

ödeme, ödeme planlaması, ülke genelinde para transferi, yatırım dahil birçok hizmet sunmaktadır (Chase, tarih yok).

- JP Morgan Chase, 2019 yılında ödeme işini dönüştürmek için ABD'deki ilk banka destekli kripto para birimi JPM Coin'i piyasaya sürmüştür (Son, 2019).
- Global Finance tarafından 2021 ve 2022 yıllarında Dünyanın En İyi Dijital Bankası seçilen Citi Group, 160'tan fazla ülkede faaliyet göstermektedir. En son teknolojiyi kullanarak oluşturduğu bankacılık platformu CitiDirect ile dijitalleşme sürecinde büyük bir adım atmıştır (Citi Group, 2022).
- ABD'nin dört büyük bankasından biri olan Wells Fargo, bankanın ticari, kurumsal ve yatırım bankacılığı işlemlerinde dijital dönüşümü hızlandırarak, fiziksel şubelerinde azalma strateji izlemektedir. Wells Fargo 2020 ve 2022 yılları arasında fiziksel şubelerini şubelerinin %17'sini kapatmıştır (Blumental, 2023). Dijital bankacılığa geçişle PNC Bank ve Bank of America da yerel şubelerini sırasıyla %15 ve %5'lik oranlarında kapatma yoluna gitmiştir (Blumental, 2023). Bu adım bankaların operasyonel verimliliklerini artırarak fiziksel şube ağlarını azaltma hedeflerine ulaşmalarını sağlamaktadır.
- 2013 yılında kurulan Chime, 13,1 milyondan fazla dijital bankacılık kullanıcısı ile ABD'deki en büyük dijital bankadır. 2025 yılına kadar 22,7 milyon kullanıcıya ulaşması tahmin edilen Chime, tasarruf için yüksek faiz oranı uygulamakta, 60.000'den fazla ATM'ye ücretsiz erişim ve hızlı para yatırma hizmetleri sunmaktadır (Chime, tarih yok).

3.3.9. Finans Sektöründe Siber Saldırıları

Finansal hizmetler; FinTech, mobil bankacılık, dijital start-up'lar ve kripto para biriminin ortaya çıkışıyla birlikte dijital devrimin merkezinde yer almaya başlamıştır. Sektördeki tüm şirketler, hizmetlerini ve rekabetçi konumlarını iyileştirmek, finansal sistemin verimliliğini artırmak için finansal teknolojileri kullanmaktadır. Ayrıca finans sektöründe akıllı cihazlara olan güvenin artması, varlıkların internet üzerinde elektronik ortamda hizmet için sunulması, sektöre yönelik kasıtlı siber tehditlere karşı korunmayı gerektirmektedir (Warren, Kaivanto, & Prince, 2018). Finansal sistemin büyüklüğü nedeniyle önemli bir şirkete yapılan siber saldırı, sektör genelinde büyük

bir etki yaratabilir. Çünkü sektör, hizmetlerine erişimini genişletmek için teknolojiyi kullandığında, hesaplanamayan sayıda yeni bağlantı devreye girmekte ve dijital varlıklar artık küresel olarak yayılmaktadır (Afşar, 2019, s. 147).

Finansal hizmet sektöründeki tehdit aktörleri, amatör bilgisayar korsanlarından profesyonel siber tehdit aktörlerine ve ulus devlet destekli siber tehdit aktörlerine kadar çeşitlilik göstermektedir. Özellikle hem kaynaklara hem çıkarlara sahip olan ulus devletler, finansal kazanç için sistemden yararlanmak istemektedir.

3.3.9.1. Dijital Bankacılıkta Siber Güvenlik Tehditleri

Dijital bankacılık ile ilgili ana sorunlardan biri, çeşitli güvenlik risklerinin varlığıdır. Bu riskler, insanların parasını çalmayı amaçlayan bilgisayar korsanları ve dolandırıcıların suç faaliyetlerinden kaynaklanmaktadır. Çevrimiçi olarak erişilebilen özel bankacılık bilgileriyle, bankalar ve tüketiciler siber güvenlik konusunda tehlikededir. Bu bağlamda finans sektöründe siber güvenlikle ilgili en sık karşılaşılan tehditler: (I) Para çalmak amacıyla kullanıcıların hassas bilgilerinin çalındığı kimlik avı saldırıları. (II) Diğer bir yaygın siber tehdit ise şifrelenmemiş verilerdir. Siber tehdit aktörleri şifrelenmemiş verilere kolayca erişmekte ve bilgilerin kurtarılması için fidye talep etmektedir. (III) Bankalar müşterilere daha verimli hizmet vermek için üçüncü taraf sağlayıcıları ile ortaklık kurmaktadır, ancak zayıf siber güvenliğe sahip e-ticaret platformları siber tehdit aktörleri için hedef haline gelmektedir. (IV) Orijinaline benzer bir web sitesini kullanarak bir bankanın web sitesini taklit etmeyi içeren kimlik sahtekarlığı ise kullanıcıların oturum açma bilgilerini girmelerini sağlamakta ve siber tehdit aktörleri tarafından bilgilerin çalınmasına sebebiyet vermektedir (Day, 2022).

Ekvador'un en büyük özel bankası Banco Pichincha, 2021'de ATM ve çevrimiçi bankacılık uygulamasını çevrimdışı duruma getiren ve müşterilerin bankacılık hizmetlerine erişimini engelleyen bir siber saldırıya uğramıştır. Banka, saldırının diğer sistemlere yayılmasını önlemek için ağların bazı bölümlerini kapatmak zorunda kalmıştır (Abrams, 2021).

Yeni Zelanda Menkul Kıymetler Borsası, bir ağ sağlayıcısına yönelik dört gün süren DDoS saldırısının ardından 2020'de faaliyetlerini durdurmak zorunda kalmıştır. Saldırıdan sonraki işlem gününde bağlantıyı yeniden sağlasa da, piyasa açıldıktan

sonra siber saldırı devam etmiş ve ulusal güvenlik sistemleri etkinleştirilmiştir (The Guardian, 2020).

3.3.9.2. Finansal Hizmetler Sektörüne Yönelik Devlet Destekli Siber Tehdit : Kuzey Kore ve İran Örneği

Kuzey Kore ; Güney Kore İstihbarat Teşkilatı'nın eski direktörü Nam Jae-Joon'a göre, Kim Jong Un, siber yeteneklerin geliştirilmesinin önemini, nükleer silahlarla eşitlemekte ve "*siber savaş, nükleer silahlar ve füzelerle birlikte çok amaçlı bir kılıç*" olarak tanımlamaktadır (Bartlett, 2020). Kuzey Kore, siber yeteneklerin desteklenmesini ulusal bir öncelik olarak görmektedir.

Devlet destekli siber tehditler, genel olarak devlet kurumlarını hedef alırken, Kuzey Kore destekli siber tehdit aktörleri siber kaynaklarının büyük bir bölümünü küresel finans piyasasına yönelik kullanmaktadır. ABD ve BM, Kuzey Kore'ye yönelik ekonomik yaptırımlar uygulayarak, nükleer silah programı ve diğer provokasyon eylemleri nedeniyle uluslararası toplumun güvenliğini tehdit ettiği gerekçesiyle tepki göstermektedir. Bu yaptırımlar, Kuzey Kore'nin uluslararası finansal sistemlere erişimini kısıtlama, dış ticaretini finansal kaynaklarını sınırlamaktadır (UN Security Council, 2023). ABD ve BM'nin ekonomik yaptırımlarının bir sonucu olarak Kuzey Kore, parasal kayıplarındaki açıklarını yasa dışı siber faaliyetler yoluyla elde etmektedir. Dolayısıyla mali yaptırımları ve küresel engelleri atlamak için geliştirdiği siber yeteneklerle çevrimiçi banka soygunları, hileli banka havaleleri, SWIFT işlemleri, kripto para ile ödeme talep eden fidye yazılım saldırıları, kripto para borsalarına yönelik saldırılar gerçekleştirmiştir. Örnek olarak 2013 yılında Güney Kore bankalarına, 2016'da Bangladeş Bankası'na ve 2017'de Tayvan'ın Uzak Doğu Banka'sına karşı SWIFT'i kullanarak gerçekleştirilen siber saldırılardan sorumlu tutulmuştur (Borghard, 2018). Gerçekleştirilen siber suç faaliyetleri ise Çin, Rusya ve Hindistan gibi üçüncü taraf konumlardan yürütülmektedir (Bartlett, 2020).

ABD istihbarat topluluğu, Kuzey Kore'nin kötü niyetli siber etkinliğinden genellikle Gizli Kobra (Hidden Cobra) olarak söz etmekte ve devletin kritik altyapısını doğrudan etkileyen yıkıcı gizli operasyonlar yürütme becerisini vurgulamaktadır (CISA, 2020). Resmi ABD hükümeti açıklamalarına göre 2015 yılından 2019 yılına kadar Kuzey Koreli bilgisayar korsanları Vietnam, Bangladeş, Tayvan, Meksika,

Malta ve Afrika'daki çeşitli bankalardan 1,2 milyar dolar çalmıştır (DOJ, 2021). Ekim 2020 tarihli CISA raporuna göre Şubat 2020'den itibaren Kuzey Koreli bilgisayar korsanları Güney Kore, Japonya, İspanya, Türkiye dahil 38 ülkenin bankalarını hedef almıştır (CISA, 2020a).

BM Güvenlik Konseyi'nin Mart 2021 raporunda, Kuzey Kore'nin denizaşırı hesaplar, paravan şirketler, kripto para birimi gibi sanal varlıklar aracılığıyla uluslararası finansal sistemlere erişmeye devam ettiğini ve elde ettiği yasadışı gelirlerle ülkenin kitle imha silahlarını ve balistik füze programlarını hem doğrudan hem de dolaylı olarak desteklediğini değerlendirmiştir (UN Security Council, 2021).

İran; İranlı bilgisayar korsanları, Aralık 2011'den Mayıs 2013'e kadar ABD'nin finansal kurumlarını hedef alan "Ababil Operasyonu" ismiyle de bilinen ve "İzzedin el-Kassam'ın Siber Savaşçıları" isimli grup tarafından gerçekleştirilen siber saldırılarından sorumlu tutulmuştur. ABD Adalet Bakanlığı iddianamesinde bilgisayar korsanları, 176 gün boyunca Bank of America, Capital One, JP Morgan Chase ve PNC Bank, ING Bank, New York Menkul Kıymetler Borsası ve Nasdaq dahil olmak üzere 46 büyük finans kurumu hedef alarak yüz binlerce müşterinin hesaplarına erişimini engellediği belirtilmiştir (DOJ, 2016b). İstihbarat uzmanları ve bazı analistler saldırının, 2010'da İran'ın nükleer santrifüjlerine yönelik Stuxnet saldırısına misilleme olduğunu belirtmektedir.

3.3.9.3. Siber Aklama ve Siber Terörizm

Bilgi çağının finansal bir yeniliği olan kripto para birimi avantajları ve dezavantajları içinde barındırmaktadır. Dijitalleşen finansal hizmetler sektöründe ödeme işlemleri için gelişen yeni teknolojiler, finans kurumlarını yeni risklerle karşılaştırmıştır. Siber tehdit aktörleri yeni ödeme yöntemleri karşısında, kara para aklamak için oluşan güvenlik açıklarından yararlanarak, yeni teknikler geliştirmiş, kapa para aklama ve terörün finansmanı ile ilgili endişeleri artırmıştır. Çünkü siber tehdit aktörleri, genellikle yasal sorumluluk olmadan ve geleneksel işlemlerden farklı olarak dijital kanallar üzerinden, yüksek finansal işlemleri yapabilecek yöntemleri geliştirmiştir (Kobor, 2007, s. 14).

Terörizm perspektifinden incelendiğinde kripto paraların, siber uzayda iz bırakmadan hareket etmesi, yine devletlerin diğer devletlere siber saldırısında terör örgütlerini finanse etmekte en güvenilir yol olarak görülmektedir (Yetgin & Baştuğ, 2022, s. 53). Kripto para birimlerinin ademi merkezîyet ve anonimlik özellikleri nedeniyle yasadışı işlemler düzenlenemez. Bitcoin de genellikle kara para aklama ve terörizmin finansmanı dahil olmak üzere suç faaliyetleriyle ilişkilendirilir. Federal Rezerv ve Avrupa Merkez Bankası, Bitcoin'in yasa dışı finansman faaliyetlerinde kullanılan bir varlık olduğunu belirtmiştir. Bu nedenle, Bitcoin üzerinde küresel bir düzenleyici konsensüs gereklidir. Bununla birlikte, düzenleyici konsensüsün geliştirilmesi, genellikle finansal teknoloji gelişiminin gerisinde kalarak terörizmi finanse etmek için yeni fırsatlar sunmaktadır (Song, Chen, & Wang, 2023).

Ekim 2015'te, Kara Para Aklama Konulu Mali Eylem Görev Gücü, özellikle kripto para birimlerinin terör finansmanı risklerini analiz eden "Yükselen Terör Finansmanı Riskleri" başlıklı bir rapor yayınlamıştır. Bu rapor, Bitcoin tarafından temsil edilen kripto para birimlerinin, kara para aklama ve terörün finansmanını kolaylaştırarak çeşitli yasa dışı suç faaliyetlerine giderek daha fazla suç ortağı haline geldiğini vurgulamıştır. Dolayısıyla gelişmekte olan teknolojilere dayalı terör finansmanı, terör örgütlerinin dünya çapında anında fon transfer etmesine izin vermekte ve ilgili ülkelerde terörle mücadele finansmanının zorluğunu da artırmaktadır (Song vd., 2023).

Terör örgütleri sahada aldıkları büyük kayıplarla birlikte ekonomik olarak da zorluk çekmiştir. Örneğin Irak ve Suriye'de petrolleri satmasıyla kazanç elde eden terör örgütü DEAŞ, kontrol ettiği toprakları kaybetmesiyle yönünü siber uzayda illegal faaliyetler yürütmeye ve bu alanda büyümeye yöneltmiştir. Özellikle, örgüt, ekonomik kayıplarını telafi etmek için kripto para birimleri üzerinden silah ticareti, bağış toplama faaliyetleri, uyuşturucu ticareti ve Bitcoin talebinde bulunabilecekleri fidye yazılım saldırıları ile ekonomik durumunu düzeltmeye çalışmıştır (Yetgin & Baştuğ, 2022, s. 53).

Siber tehdit aktörleri, e-ticaret platformlarını kara para aklama amacıyla kullanabilmektedir. Özellikle düşük maliyetli ürünlerin satışı gibi yöntemler, para transferlerini gizlemek ve yasadışı faaliyetleri finanse etmek için kullanılabilir.

Örneğin 2017 yılında ABD'de IŞİD üyeleri, yurtdışındaki IŞİD üyelerinden aldığı PayPal ödemelerini gizlemek için popüler bir e-ticaret eBay platformunu kullanmıştır. Bilgisayar yazıcılarını satıyormuş gibi davranarak, gerçekte finansal kaynakları terör saldırılarını finanse etmek amacıyla kullanmışlardır (Mackie, 2017).

Finansal hizmetler sektörünün siber uzayı hangi düzeyde etkilediği problemi çerçevesinde (P_{1b}), finansal hizmetler sektörü, FinTech şirketlerinin yükselişi, dijital bankacılık hizmetlerinin entegrasyonu, geleneksel bankalar ve FinTech şirketleri arasındaki işbirliğinin hızlanmasıyla siber uzayda önemli bir dönüşüm geçirmiştir. Özellikle geleneksel bankalar FinTech şirketleriyle rekabet etmek ve değişen müşteri beklentilerini karşılamak için dijital dönüşümü benimsemiştir. Bununla birlikte, sektör kara para aklama ve siber terörizm gibi siber tehditlerin yarattığı zorluklar dijital çağda önemli bir endişe haline gelmiştir. Kara para aklama ve siber terörizme karşı, hükümetler, düzenleyici kurumlar, finansal kurumlar arasında güçlü siber güvenlik önlemleri uygulamak, potansiyel tehditleri tespit etmek için yapay zeka gibi ileri teknolojiler kullanmak için birlikte çalışmaktadır.

3.4. Telekomünikasyon, Bilgi ve İletişim Teknolojileri Sektörü

3.4.1. Endüstri 4.0'ın Telekomünikasyon ve BİT Sektörüyle Entegrasyonu

Nesnelerin interneti, yapay zeka, robotik gibi dijital teknolojilerin hızlı bir gelişim göstermesinin ve küreselleşmesinin, topluma ve endüstriye önemli değişiklikler getirdiği yeni bir çağdayız (Fukuyama, 2018, s. 47). Bilgi ve iletişim teknolojisinin gelişimi, insanlar arasındaki iletişimin daha basit ve daha hızlı olmasını sağlamaktadır. İnternetin geniş bir nüfuza yayılması, yeni elektronik cihazların ortaya çıkışı, çevrimiçi sosyal ağlar (Twitter, Instagram, Facebook vb.) ve bilgi işlem alanındaki genel gelişmeler, yaşama ve iletişim kurma şeklimizi tamamen değiştirmiştir. Dünyada giderek daha fazla insan günlük aktiviteler için bu teknolojinin kullanımına bağımlı hale gelmektedir. Özellikle akıllı telefonların artışı, insanların alışveriş yapma, finans işlemlerini gerçekleştirme, eğlenme, iletişim kurma şeklinde köklü değişiklikler meydana getirmiştir. Dolayısıyla teknoloji, telekomünikasyon,

medya ve eğlence şirketleri Endüstri 4.0'ın yarattığı değişimin merkezinde yer almaktadır.

Dijitalleşme sürecinde yaşanan değişim ve gelişim karşısında siber saldırılar, giderek daha çok teknoloji sektörünü hedeflemektedir. Siber saldırıların sıklığının ve şiddetinin arttığı bir dünyada şirketler, verilerini ve sistemlerini güvence altına almak için yine teknolojiye güvenmektedir. Aynı zamanda dünya, doğal kaynakların tükenmesi, küresel ısınma, artan ekonomik eşitsizlik ve terörizm gibi küresel ölçekteki zorluklarla giderek daha fazla karşı karşıya kalmaktadır. Bu nedenle, yeni bilgi edinmek için bilgi ve iletişim teknolojilerini kullanarak toplumdaki sorunları çözmenin etkili ve verimli bir yolu olarak fiziksel alan ve siber uzay arasında bağlantı kurarak güçlüklerle çözüm bulunması amaçlanmalıdır (Fukuyama, 2018, s. 47).

3.4.2. Telekomünikasyon ve BİT Sektöründe Uluslararası Rekabet Gücü ve Etkileri

Teknolojiye eğilim artıkça, talep karşısında çok uluslu şirketler kendi alt yapılarını genişletme ve müşteri portföyünü artırma yoluna gitmiştir (Yetgin, 2020, s. 106). Bilgi ve iletişim teknolojilerinde büyüme, temel olarak telekomünikasyon ekipmanı ve hizmetlerindeki büyümeden kaynaklanmaktadır. Bu sektördeki büyüme, çok uluslu şirketler ve ulus devletler arasındaki rekabeti de artırmaktadır. Önde gelen teknoloji ve telekomünikasyon şirketleri, yenilikçi ürünler, hizmetler ve çözümler sunmak için küresel ölçekte rekabet etmektedir. Bu şirketler genellikle önemli bir pazar gücüne sahiptir ve birden fazla ülkede faaliyet göstererek pazar payı için yoğun rekabete yol açmaktadır. Aynı zamanda ulus devletler yerel endüstrilerini, ulusal güvenliklerini korumak ve kritik altyapı üzerinde kontrolünü sürdürmek için kısıtlayıcı politikalar benimsemektedirler. Bu politikalar, ticaret engelleri ve yabancı yatırımlar üzerindeki kısıtlamaları içermektedir. Piyasa rekabetini önlemek için hükümetler tarafından izlenen kısıtlayıcı politikalarda görülen artış, hükümetlerin yerel inovasyonu teşvik etmek ve yerel BİT endüstrilerini desteklemek için oluşturduğu politikalarda da görülmektedir. Bu önlemler, yabancı teknolojilere aşırı bağımlılığı önleme, karşılıklı bağımlılığı tek taraflı bağımlılığa dönüştürme ve küresel pazarda rekabet avantajı sağlama girişimleri olarak görülebilir.

Ulus devletler arasındaki rekabet, ekonomik faktörlerin ötesine geçmektedir. Aynı zamanda teknolojik liderliği, dijital egemenliği, küresel standartları belirleme üzerindeki etkiyi de kapsamaktadır. Bu bağlamda ulus devletler, rekabet avantajı elde etmek ve ekonomik büyümeyi desteklemek için 5G, yapay zeka ve siber güvenlik gibi gelişen teknolojilerde lider olarak konumlandırma hedefinde stratejiler geliştirmektedir. Çalışmanın bu bölümü 5G teknolojisi üzerindeki rekabet; ABD ve Çin arasındaki teknolojik rekabetin temelinde yer alan Apple-Huawei çatışması ve sonucu olarak Huawei'ye yönelik yaptırımlar; küresel tedarik zincirinin temeli olan hammadde temelindeki çatışmalar; Metaverse teknolojisinin gelişimi; Toplum 5.0 kapsamında incelenmiştir.

3.4.2.1. 5G İletişim Ağı ve Uluslararası Rekabet

Cep telefonlarının piyasaya sürüldüğü 1980'li yıllardan bugüne telekomünikasyon sağlayıcıları, kapsama alanını genişletmek, hizmetleri iyileştirmek ve daha fazla kullanıcı çekmek için mobil ağlara yatırım yapmaktadır. Telekomünikasyon sektöründe 4G'den 100 kat daha yüksek iletim hızına sahip bir kablosuz mobil ağ teknolojisi olan 5G (5. Nesil) teknolojisi, dünyanın dört bir yanındaki devletler, devlet dışı aktörler ve teknolojiden sosyal bilimlere kadar değişen farklı çalışma disiplinleri arasında büyük ilgi görmektedir, küresel liderliği sürdürmek için önemli bir anahtar olarak tanımlanmakta ve ulusal güvenliğin güvencesi olarak görülmektedir (Gong, 2021, s. 3).

2018'in sonunda piyasaya çıkmaya başlayan ve savaşın geleceğini dahi değiştireceğine inanılan 5G teknolojisi, farklı sektörlerde yenilikçi hizmetler sağlamakla birlikte, güvenilir bir bağlantı imkanı ile her türlü görsel ve metinsel verilerin hızlı bir şekilde aktarımını sağlamaktadır.

5G ağları, üç ağ katmanından oluşmaktadır: (I) İletişim akışını daha hızlı hale getiren gelişmiş mobil ağ. Örneğin 5G, film indirme süresini 7 dakikadan 6 saniyeye indirmektedir. (II) Otonom araçlarla bağlantı kurulmasını sağlayan son derece güvenilir ve düşük gecikmeli iletişim. Düşük gecikme süresinin kullanılması, bağlantıyı 4G'den 60 veya 120 kat daha hızlı hale getirmektedir. (III) Makinelerin veya cihazların birbirleriyle kablosuz olarak iletişimini sağlayan makine-makine iletişimidir (Tekir, 2020, s.118).

Dijital dönüşüme büyük katkılar sunması beklenen 5G teknolojisi, IoT, yapay zeka, robotik gibi yeniliklerin daha etkili çalışması için ultra güvenilir ve yüksek hızda iletişim ile dijital teknolojiyi sağlayarak; ekonomik, askeri, bilimsel, sosyal, kültürel

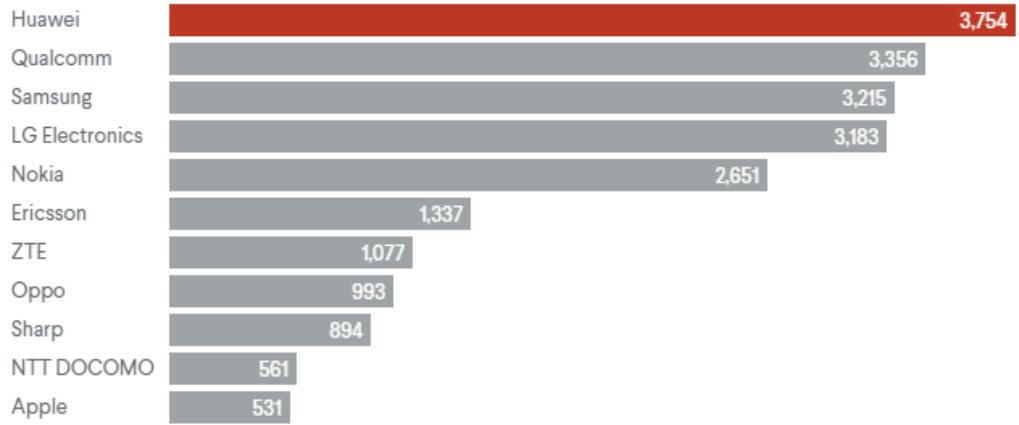
vb. birçok sektöre yansımalarıyla, toplumları, devletleri ve bunlar arasındaki ilişkileri değiştirecek ve dönüştürecek bir teknolojidir (Aydın, 2021, s. 43).

İşletmelerin verilere daha hızlı ulaşmasını ve daha hızlı karar almasını sağlayan bu teknoloji, tarım ve endüstrideki yeniliklerin daha ucuz ve kolay olmasını sağlayarak işletmeler için maliyet tasarrufu, müşteriler için ise daha iyi bir deneyim sağlayacaktır. Ayrıca akıllı şehirler, akıllı okullar, akıllı evler, akıllı otomobiller ve akıllı sağlık merkezleri için daha çok veri alarak ve elektronik cihazların bağlantısını sağlayarak daha verimli ve güvenli bir ortama zemin hazırlayacaktır (Tekir, 2020, s. 118).

5G teknolojisine yönelik toplumsal hayatı kolaylaştıran ve iyileştiren bir etki yarattığı düşüncesine karşı uluslararası tepkiler mevcuttur. Özellikle uluslararası tepkiler, 5G teknolojisinin kanser riski, nörolojik bozukluk ve olumsuz genetik etkiler sebebiyle insan sağlığına tehdit oluşturduğu yönündeki endişelerden kaynaklanmaktadır. 5G karşılığında daha ileri giden endişeler arasında COVID-19 ve 5G arasında bir ilişkinin söz konusu olduğu düşüncesidir. 5G teknolojisinin bağışıklık sistemini zayıflatarak COVID-19'a yakalanmayı kolaylaştırdığını ve doğrudan virüse neden olduğu iddia edilmektedir. Dünya Sağlık Örgütü, 5G'yi güvenli bir teknoloji olarak ilan etse de, uzmanların tümü bu sonuçlara katılmamaktadır (Laurence, 2023).

20. yüzyılda çelik, kömür, otomobiller, uçaklar, gemiler ve seri üretim, ulusal gücün önemli kaynakları arasındayken 21. yüzyılda, ulusal güvenliğin, ekonomik ve askeri gücün, uluslararası rekabetin kaynağı; yeni teknolojiler oluşturma ve kullanma yeteneğindedir (Lewis, 2018). Yeni teknolojilere sahip olan, bilgi ve iletişim teknolojisinin geleceğini yönlendiren, ve küresel standartları belirleyen ulus devletler, dijital çağda avantajlı konuma geçecektir. Bu bağlamda 5G'nin toplum ve ekonomi üzerindeki etkisi hem şirketler arasındaki rekabeti hem de devletler arasında jeopolitik çatışmayı da etkilemektedir (Tekir, 2020, s. 119). Sonucunda da ulus devletler, 5G standartlarının arkasındaki fikri mülkiyetten daha fazla pay alarak, küresel etkisini artırmayı amaçlamaktadır.

Şekil 16: Haziran 2022 itibariyle 5G patent sayısı



Source: IPlytics.

COUNCIL
FOREIGN
RELATIONS

Kaynak: <https://www.cfr.org/background/chinas-huawei-threat-us-national-security>

Küresel olarak analistler, 5G teknolojilerinin birden fazla sektörde 12,3 trilyon dolarlık satış faaliyeti oluşturabileceğini ve 2035 yılına kadar 22 milyon istihdamı destekleyeceğini tahmin etmektedir. Deneyimler, yeni ürünlerle pazara ilk giren şirketlerin, uzun vadeli faydalar sağlayabildiğini ve şirketlerin bulunduğu ülkeler için önemli ekonomik kazanımlar sağladığını göstermektedir (Gallagher, 2019, s. 8). Çinli Huawei, ZTE ve Oppo, Güney Koreli Samsung ve LG, İsveçli Ericsson, Finlandiyalı Nokia, ABD'li Apple, Qualcomm ve diğer AT&T, Verizon, Cisco, Japonyalı Sharp ve NTT DOCOMO çok uluslu şirketleri 5G alanında yatırım yapan öncü şirketlerdir.

3.4.2.2. ABD ve Çin Arasındaki Jeopolitik Mücadelenin Odağı: Apple ve Huawei

Bilgi ve iletişim teknolojileri sektöründeki gelişmeler çok uluslu şirketlerin rekabeti üzerinden hızla ilerlerken ABD ve Çin arasındaki küresel etki alanı odaklı rekabet, "ticaret savaşları" formatından, şirketlerin doğrudan hedef alındıkları "teknoloji savaşları" formatına evrilmiş bulunmaktadır. 2018'de Trump yönetiminin, Çin'in ekonomik yükselişini dizginlemek için belli sektörlerde tarife artışları ve piyasaya giriş kısıtlamaları ile başlattığı mücadele, telefon ekipmanları pazarında yükselişe geçen Huawei çok uluslu şirketinin faaliyetlerinin engellenmesi noktasına kadar ulaşmıştır (Ünay, 2019). Genel tartışmalarda ticaret savaşları, 5G teknolojileri üzerinden tartışılrsa da dijitalleşmenin olduğu her alanda ABD ve Çin arasında gerilim

yaşanmakta, diğer ulus devletler ise yaşanan rekabet ortamında tepkilerini göstermektedir.

2019 yılında Samsung %21,8 pazar payına sahipken Huawei %17.6 ile ikinci sırada yer almış ve %14.5 oranıyla Apple üçüncü sıraya gerilemiştir (Canalys, 2020). Apple ve Huawei örneğinde olduğu gibi bu şirketler arasındaki rekabetin kimi zaman bir ticari savaşa dönüştüğü ve hükümetler arasında siyasi krizlere yol açtığı görülmüştür (Yetgin, 2020 , s. 105). 2023 yılına kadar geçen süreç içerisinde Huawei, ticari casusluk ve Çin ordusu ile işbirliği yapmakla suçlanmıştır. Aynı zamanda Huawei'nin, ABD'nin İran'a yönelik ambargo kararına uymaması gerekçe gösterilerek Huawei'nin mali işler müdür Meng Wanzhou'yu tutuklatmış, Android lisans desteği iptal edilmiş, pazar gücü yasal yollarla ve diplomatik yöntemlerle hem ABD hem de Avrupa pazarıyla kesilmiştir. Sonucunda ise Huawei'nin pazar payı ve geliri büyük bir farkla düşüş yaşamıştır.

Şekil 17: Dünya çapında mobil satıcı pazar payı - Şubat 2023



Kaynak: <https://gs.statcounter.com/vendor-market-share/mobile>

Ticaret anlaşmazlığı olarak başlayan ticaret savaşı, ABD ve Çin arasında 5G, yapay zeka ve yarı iletken gibi temel teknolojilerde liderlik etme savaşına dönüşmüştür. Bu bağlamda çalışmada; Apple ve Huawei çok uluslu şirketleri incelenmiş, ABD ve müttefiklerinin, Huawei'ye karşı faaliyetlerini kısıtlaması ve dijital altyapı sektöründe dışlaması stratejik olarak ele alınmıştır.

3.4.2.2.a. Apple

Apple, 1976'da kuruluşundan günümüze kadar yüksek teknoloji ürünlerinde, bilgisayar donanım ve yazılım üretiminde uzmanlaşmış, Mart 2023 itibariyle 2,54 trilyon dolar bir piyasa değerine sahip çok uluslu bir Amerikan şirkettir (Fool, 2023).

Steve Jobs, Steve Wozniak ve Ronald Wayne, Apple I kişisel bilgisayarını geliştirmek ve satmak için Apple Computer Inc'i kurmuştur. 1977'de şirketin ilk çevrimiçi mağazasını açmasıyla Apple, üç yıl içinde 1 milyar dolar yıllık satışa erişmiş ve coğrafi erişimini genişleterek dünya çapında daha fazla mağaza açmaya başlamıştır. Birkaç yıl öncesine kadar Apple, Amerikan hükümetinin üç katı ve İngiltere'nin iki katından fazla nakit paraya sahipti. 2014 yılında Apple, 157,8 milyar dolarlık nakit ve yatırım bildirirken, Bank of America, Amerikan hükümetinin aynı yıl içinde 48,5 milyar dolarlık rezervi olduğunu bildirmiştir. Aynı yıl içinde Apple, Amazon, Google ve Facebook'un toplamından daha fazla gelir elde etmiştir (Shvartsman, 2023). Apple, günümüzde de dünya verilerine göre en değerli şirket konumdadır. Benzer şirket ve rakiplerin piyasa değerleri ise Nisan 2023 itibarıyla Microsoft için 2,09 trilyon dolar, Amazon için 1,01 trilyon dolar ve Google için 1,35 trilyon dolardır (Fool, 2023).

Apple'ın gelirinin yaklaşık %40'ı ABD'den gelirken Avrupa ve Çin, Apple için diğer iki büyük pazardır. 2018 yılında ABD'den 116,9 milyar dolar gelir elde ederken Avrupa'dan 62,4 milyar dolar ve Çin'den 51,9 milyar dolar gelir elde etmiştir. Ancak 2019 yılına gelindiğinde Çin'den elde ettiği gelir 42,6 milyar dolara ve 2020'de 40,3 milyar dolara düşmüştür (Shvartsman, 2023). Bu süreçte Çin'den gelen gelir düşüklüğü ise Washington ve Pekin arasında gerçekleşen teknoloji savaşlarının ve Apple ürünlerine yönelik bojkotların bir sonucu olarak yorumlanabilir.

3.4.2.2.b. Huawei

1987 yılında -Çin Halk Kurtuluş Ordusu'nda mühendis olarak hizmet vermiş ve Çin Komünist Partisi üyesi- Ren Zhengfei tarafından kurulan Huawei, hızlı bir şekilde büyüyen BİT hizmeti sağlayıcısıdır. Kurulduğu yılda 700 kullanıcıya ulaşan mobil teknolojisi, 1995 yılına gelindiğinde 5,2 milyon kullanıcıya ulaşmıştır. Aynı yıl mobil iletişim teknolojilerinde gelişim sağlamak için Şanghay ve Pekin'de araştırma merkezleri kurmuştur. 1996 yılında ise Çin hükümetinin, yabancı şirketleri için özel ithalat politikalarına son vererek yerli telekomünikasyon şirketlerine açıkça destek vermeye başlaması ve yerel şirketlere daha fazla finansal kaynak sağlaması, Huawei'nin büyümesinde önemli bir rol oynamıştır (Chong, 2020).

1990'ların sonlarında mobil iletişim teknolojilerinde rekabet daha da yoğunlaşmıştır. Bazı çok uluslu şirketler yurt içindeki pozisyonlarını sağlamlaştırdı

ihracata yoğunlaşırken, bazıları doğrudan dış pazara yatırım yapmıştır. Huawei ise teknolojiadaki güçlü yeteneklerine rağmen, kalitesiz Çin ürünleri söylemleriyle karşı karşıya kaldığı için uluslararası pazarda rekabetini güçlendirebilmek amacıyla rakiplerinden çok daha düşük fiyatlar sunmuş ve uygun fiyatlı teknoloji arayan, telekomünikasyon altyapısının yetersiz olduğu ülkelere giriş yapmaya başlamıştır (Chong, 2020). Bu hedef doğrultusunda 1997 yılında Rus pazarına girdikten kısa bir süre sonra, Tayland, Brezilya ve Güney Afrika'da satışlar yapmaya başlamıştır. Fiyatlandırma strateji sayesinde, rakiplerinin fiyatını genel olarak %30 oranında düşürmüştür. 2003 yılında Etiyopya'da 20 milyon dolarlık bir sözleşmeyle, 2005'te Nijerya'da 200 milyon dolarlık bir projeye ve 2006'da Gana, Mauritius, Fas, Kongo ve Kenya'da yapılan sözleşmelerle gelecekteki iş anlaşmalarının temelini atmıştır (Ahrens, 2013, s. 8).

Rusya ve gelişmekte olan pazardaki girişimlerinin ardından Huawei, hedefini gelişmiş pazarlara yöneltmeye başlamıştır. Bu doğrultuda 2001 yılında Huawei, Avrupa'daki ilk büyük satışlarını Hollanda ve Almanya'ya yapmıştır. 2002 yılında Birleşik Arap Emirlikleri'ne yaptığı satışla, ülkeyi 3G'ye sahip ilk Arap devleti haline getirmiştir. 2004 yılında 3G ağını inşa etmek için önce Portekiz'e ve ardından Hollanda'ya büyük bir satış yapmıştır. 2005 yılında British Telecom ve Vodafone ile yaptığı küresel tedarikçi anlaşması ile Huawei uluslararası profilini yükseltmiştir (Ahrens, 2013, s. 9).

Huawei'nin, Batılı şirketlerin göz ardı ettiği Afrika, Orta Doğu, Güneydoğu Asya pazarlarına girmesi ve küresel pazarlara girmeye başlaması, 2000 yılında dönemin Başbakanı Zhu Rongji tarafından -Çin'deki şirketleri, uluslararası pazarda daha rekabetçi hale getirmek amacıyla formüle edilen- küreselleşme politikasının ardından gerçekleşmiştir. Sonuç olarak Çin'in resmi açıklamaları ve politikaları doğrultusunda Huawei, küresel operasyonlarını yürütmekte ve küreselleşme stratejisini başarıyla uygulamaktadır (Tekir, 2020, s. 120). Çin hükümeti 5G ağlarını kendisi oluşturmak yerine, Huawei'nin Ar-Ge yatırımlarına desteği ve küresel pazarlara girmesine olanak tanınması yönünde izlediği stratejiyle, dünyadaki konumunu yükseltmeyi amaçlayan ana hedefleriyle uyumlu kalmasını sağlamıştır (Tekir, 2020).

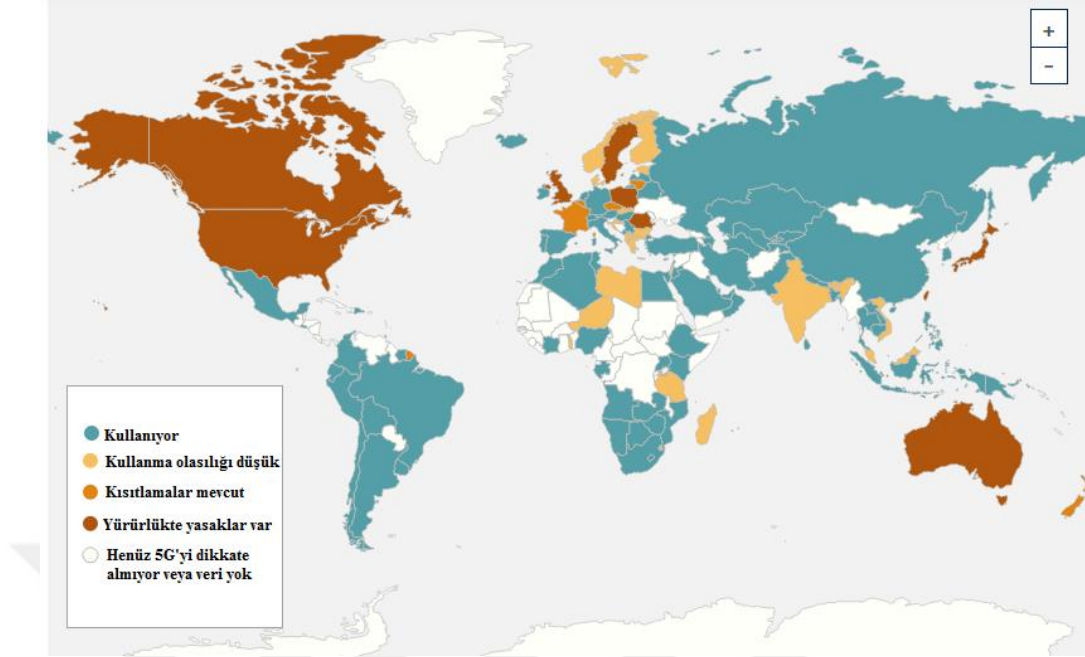
3.4.2.2.c. Dijital Ekonomik Rekabet: 5G Teknolojisi

5G, mevcut dijital sanayileşme çağında çekirdek bir teknoloji olarak ekonomik düzeyde uluslararası rekabeti doğrudan etkilemektedir. ABD ve Çin, gelişmekte olan teknolojilerde, özellikle teknoloji savaşında bir dönüm noktası olan 5G teknolojisinde hakimiyet için rekabet etmektedir.

ABD Savunma Bakanlığı tarafından yayınlanan 5G Ekosistem Raporuna göre Huawei, 2009'da yaklaşık 28 milyar dolar olan küresel gelirini 2018'de 109 milyar dolara yükseltmiştir. Aynı dönemde Ericsson'un geliri 27,9 milyar dolardan 23,9 milyar dolara düşerken, Nokia'nın geliri 57,6 milyar dolardan 26,6 milyar dolara düşmüştür. Huawei, ZTE, Xiaomi, Vivo ve Oppo gibi Çinli teknoloji şirketlerinin pazar payları 2009'da yaklaşık %6'nın altındayken 2018'de %30'un üzerine çıkmış ve ABD pazarındaki kısıtlamalara rağmen hızla büyümeye devam etmiştir. 2009'da gelire göre ilk 10 internet şirketinin tamamı Amerikalıyken, bugün ilk 10 şirketten dördü (Baidu, Alibaba, Tencent, TikTok) Çinli şirketlere aittir (Medin & Louie, 2019, s. 17). Apple ve Google gibi Amerikan şirketleri, refah yaratan ve ulusal serveti hızlı bir şekilde büyüten 4G pazarında lider bir konuma sahip olma fırsatını yakalamıştır. Ancak bugünkü tahminlere göre 5G liderleri önümüzdeki on yılda yüz milyarlarca dolar gelir elde edecek ve Çin 5G teknolojisinde gösterdiği gelişim ABD'nin 4G döneminde gösterdiği başarıyı elde edecektir.

Çin, 5G teknolojisini yaymak için fiber optik kablo ağının erişimini kademeli olarak Asya-Pasifik bölgesinde genişletirken, Avrupa, Afrika, Latin Amerika ve Orta Doğu'da da bu alanda lider olmayı hedeflemektedir. Aralarında Huawei ve ZTE'nin de bulunduğu Çinli şirketler, Belize, Ekvador, Gine ve Solomon Adaları da dahil olmak üzere dünyanın dört bir yanındaki ülkelerde fiber optik kablolar inşa etmek ve 5G teknolojisine sahip olmak için anlaşmalar imzalamıştır (Cheney, 2019, s. 5). Örneğin Huawei, diğer servis sağlayıcılarla karşılaştırıldığında Avrupa'da fiyat rekabetinde öne çıkmaktadır. Avrupa'da 5G konusunda imzalanan sözleşmelerin yarısından fazlası Huawei ile yapılmıştır. Hollanda, 5G teknolojisine sahip olmak için %60'lık fiyat avantajı sebebiyle Huawei'yi tercih ederken, 4G ve 4,5G teknolojisinde dünyanın yarısı Huawei altyapısını kullanmaktadır. Dolayısıyla Avrupa'da 5G altyapısının sağlanması için farklı şirketlere yönelmek hem ülkeler için ek bir maliyete sebep olabilir hem de 5G projelerinin ertelenerek bölgede gelişmesini geciktirebilir (Esen, 2021, s. 103-104).

Şekil 18: Huawei ekipmanlarını 5G ağlarında kullanmaya yönelik resmi yaklaşımlar



Kaynak: <https://www.cfr.org/backgrounders/chinas-huawei-threat-us-national-security>

Gelecekte dünyanın en büyük kaynağının maden veya petrol kaynaklarının değil veri kaynakları olacağı düşünülmektedir. Veri insan faaliyetlerinin bir sonucudur ve zengin bir kaynaktır. Ancak ulus devletlerin verileri doğru analiz ederek kullanıp kullanılmayacağına bağlıdır. 5G teknolojisi üzerindeki rekabetin ulus devletlerin geleceğini belirlemesindeki temel neden ise 5G teknolojisine hakim devletin verileri daha büyük bir servete dönüştürebilme kapasitesine bağlıdır. Amerikalı 5G sağlayıcısı Qualcomm, 5G teknolojisiyle 2035 yılına kadar ABD'nin 3,5 trilyon dolar gelir elde edeceğini ve 22 milyon iş yaratacağını hesaplamaktadır. (Gong, 2021, s. 43-44). Dolayısıyla 5G üzerindeki yarışı kaybetmek, milyarlarca doları ve milyonlarca iş kaybetmek anlamına gelmektedir. 5G teknolojisinde kazanan devlet pazar payını yükseltirken ve daha fazla gelir elde ederken siber yeteneklerini de artıracaktır ve rakip ulus devletlerin dijital verilerinin güvenliği daha fazla risk altında olacaktır.

3.4.2.2.d. Dijital İpek Yolu

Çin, uluslararası arenada dış politika girişimi olan 2013 yılında başlattığı Tek Kuşak Tek Yol veya Kuşak ve Yol Girişimi adıyla bilinen proje aracılığıyla, kalkınma ve fiziki altyapı yatırımlarıyla hem bölgesel hem de küresel bir güç olmak için projeler geliştirmektedir. Proje, Asya, Avrupa, Orta Doğu, Afrika ve Amerika arasında ticareti

artırma, altyapı bağlantılarını geliştirme ve ekonomik işbirliğini güçlendirme hedefiyle sağlam kültürel ilişkilere dayanmaktadır (Çatal & Yılmaz, 2021). Kuşak ve Yol Girişimi, bir dizi proje ve girişimi kapsar, Bunlar enerji altyapısı, limanlar, demiryolları, otoyollar, havalimanları, köprüler, lojistik ağlar, petrol ve gaz boru hatları, iletişim ağları gibi altyapı yatırımlarını içermektedir (Altun, Kurt, & Özbaysal, 2021, s. 84). Bu girişim, Çin'in ekonomik, siyasi ve jeopolitik etkisini küresel ölçekte genişletmeyi, pazar erişimini artırmayı ve ekonomik bağları güçlendirmeyi hedeflerken aynı zamanda ekonomik entegrasyonu teşvik etmeyi amaçlamaktadır.

Çin'in yurt dışında dijital bağlantıyı geliştirmeyi ve küresel teknolojik süper güç olma hedefi kapsamında başlatılan Dijital İpek Yolu Girişimi, Kuşak ve Yol Girişimi'nin bir bileşenidir. Dijital İpek Yolu Girişimi çeşitli dijital bağlantı ve işbirliğini teşvik etmeye odaklanmaktadır. Özetle katılımcı ülkelerde internet bağlantısını iyileştirmek ve dijital hizmetlere erişimi genişletmek için denizaltı kablolarının, fiber optik ağların ve uygu iletişim sistemlerinin inşasını; güvenli çevrimiçi işlemler ve veri koruma için platformlar, düzenlemeler ve standartlar oluşturarak sınır ötesi e-ticareti ve dijital ticareti kolaylaştırmayı; 5G ağları, yapay zeka, büyük veri, bulut bilişim ve siber güvenlik gibi alanlarda işbirliğini, teknoloji transferini ve kapasite geliştirmeyi teşvik etmeyi; akıllı şehirler ve veri merkezleri gibi dijital altyapı projelerinin gelişimini desteklemek için finansman, uzmanlık ve teknik yardım sağlamayı hedeflemektedir (Masduki, Niu, Rochman, & Sulhan, 2021, s. 44).

Dijital İpek Yolu Girişimi'nde en dikkat çeken konu 5G'nin geliştirilmesidir. Çin, yerel teknoloji şirketlerini destekleyerek ve devlete ait olan bankalardan finansman sağlayarak, internet üzerinden veri iletmek için kullanılan fiber optik kablolar ve veri depolamak için kullanılan veri merkezleri inşa etmektedir. Tüm çabalar sonucunda ise 5G teknolojisinin fiziksel altyapısını sağlamada bir dünya lideri olmayı hedeflemektedir (Kitson & Liew, 2019). Ayrıca Dijital İpek Yolu, Avrupalı ve ABD'li rakiplerinden önemli ölçüde düşük maliyetlerle yüksek kaliteli fiber optik sağlayabilen Çinli teknoloji devleri Huawei, Tencent, Alibaba ve ZTE tarafından yürütülmektedir (Masduki vd., 2021, s. 44).

5G teknolojisi, fiber optik kablolar üzerine kurulmakta. Çinli şirketler de denizaltı ve kara optik kablo ağlarını kullanarak Kuşak ve Yol güzergahındaki ülkelerin telekomünikasyon ağları pazarlarına girmeyi başarmış ve bu altyapı planları

sayesinde 5G ağlarının yaygınlaşması hızlanmıştır. Bu program aracılığıyla Çin'in Asya'nın mevcut kablolarının yaklaşık %30'una ve planlanan kabloların %54'üne sahip olmasına izin vermiştir (Masduki vd., 2021). Dolayısıyla Kuşak ve Yol Girişimi'ne katılan ülkeler, Huawei'nin 5G sektöründeki girişimlerinde önemli bir rol oynamaktadır (Tekir, 2020).

Uluslararası deniz altı kablo projeleri alanında Çinli büyük teknoloji şirketlerinin, 2012'den 2015'e kadar (sadece Çin Anakarası, Tayvan, Hong Kong'a bağlanan projelere dahil olarak) %7'sine katıldığı, 2016-2019 yılları arasında bu oranın Güney Çin Denizi dışında gerçekleşecek tüm kablo inşaat projeleriyle %20'ye yükseldiği görülmektedir. Örneğin devlete ait üç büyük ağ operatörü -China Telecom, China Mobile ve China Unicorn- Güneydoğu Asya, Orta Doğu ve Batı Avrupa'yı birbirine bağlayan yeni SeaMeWe-5 denizaltı kablosunun inşasına katılmıştır (Lee, 2017). Diğer bir örnek ise 2017 yılında Exim Bank tarafından alınan 44 milyon dolarlık kredi ve Huawei tarafından sağlanan telekom ekipmanı ile Pakistan üzerinden Gwadar Limanı'na fiber optik kablolar döşenmeye başlanmış ve proje 2020 yılında tamamlanmıştır (Shen, 2018, s. 2691-2693).

Güvenlik açısından bakıldığında, Çin hükümetinin dijital gözetleme eğilimi göz önüne alındığında, fiber optik kablo ağları üzerindeki kontrolünü sağlayarak veri trafiğini izleme, istihbarat toplama ve diğer ülkelerle bağlantıları kesebilme potansiyeli çeşitli siber güvenlik risklerini yaratmaktadır.

3.4.2.2.e. Huawei ve ABD Hükümetinin Müdahaleleri

2020 yılında ABD hükümeti tarafından yayınlanan Ulusal Güvenlik Belgesinde Huawei şirketi, Çin ordusuyla işbirliği yapmakla, Amerikan teknolojisine yönelik ticari casusluk ve fikri mülkiyet hırsızlığı yapmakla suçlanmıştır (Ford, 2020). Bu doğrultuda Trump yönetimi, ABD'ye yönelik ulusal güvenlik tehdidi oluşturabilecekleri için Amerikan şirketlerinin, Huawei ve aynı alanda hizmet veren ZTE ile işbirliği yapmaktan kaçınmalarını bildirmiştir. Ardından ABD hükümeti, Çinli şirketlerin ABD yerel 5G ağına katılmasını yasaklamak için resmi adımlar atmış, ülkede yerleşik kurumların ve federal hükümetin Huawei ile iş yapmasını engellemek için varlık listesine eklemiştir. Yasal güçle Huawei'nin pazar ve teknolojik bağlarını

ABD pazarıyla kesmek amacıyla atılan bu adımın ardından Microsoft, Google, Intel gibi çokuluslu şirketler ile Huawei arasındaki bağlantı kopmuştur (Aydın, 2021, s. 60).

ABD hükümeti, idari ve diplomatik yöntemlerle müttefiklerine karşı da Huawei'yi dışlamaları için söylemlerde bulunmuştur. 2019'da ABD Dışişleri Bakanı Mike Pompeo, İsviçre medyasına verdiği röportajda, Çinli işletmelerle işbirliği yapmanın Çin hükümeti ile işbirliğine eşdeğer olduğunu, Çin'in Huawei ekipmanlarını gözetleme aracı olarak kullanabileceğini ve bu nedenle Huawei ile işbirliğinin veri güvenliği için risk oluşturduğunu savunmuştur. Dolayısıyla Japonya, Kanada, İngiltere, Avustralya ve Yeni Zelanda hükümetleri de Huawei'ye yönelik kısıtlamalar getirmiştir. Bu durumun bir sonucu olarak Alman telekomünikasyon devi T-Mobile'ın, güvenlik endişeleri nedeniyle Huawei ile yaptığı 4,1 milyar dolarlık satın alma sözleşmesini askıya alması örnek olarak verilebilir (Gong, 2021, s. 40-41).

ABD Adalet Bakanlığı savcıları, Çinli teknoloji devi Huawei'nin Mali İşler Direktörü Meng Wanzhou'ya karşı yolsuzluk, teknoloji hırsızlığı ve adalete engel olma gibi bir dizi suçlamalar yöneltmiştir. Huawei ve Meng tüm suçlamaları reddetse de sürecin arka planına bakıldığında, İran yaptırımlarını deldiği gerekçesiyle Meng Kanada'da tutuklanmış ve ardından 10 milyon Kanada doları tazminat ile şartlı serbest bırakılmıştır. Yaşanan dava süresinde ise Çin ekonomisi 2018 yılında 1990'dan bu yana en düşük büyümesini yaşamıştır (Aktan, 2019). ABD hükümeti tarafından bir diğer diplomatik kısıtlama ise Huawei çalışanları ve Çinli şirketlere yönelik vize kısıtlamasıdır (Gong, 2021, s. 41).

Huawei'nin akıllı telefon çiplerinin %90'ından fazlasını tedarik eden TSMC, 2020'de ABD ihracat kontrollerini gerekçe göstererek Huawei ile iş yapmayı durdurmuştur. Huawei, akıllı telefon çiplerinin envanteri tükendiği için yeni çipler almakta zorlanmış ve gelirinde düşüş yaşamıştır. 2021'de şirket, 2019 seviyelerine göre %23 düşüşle 95 milyar dolar gelir bildirmiştir (Berman, Maizland, & Chatzky, 2023).

2021 yılında ABD yönetimine gelen Joe Biden ise Huawei'ye yönelik daha da kısıtlayıcı yasaklar getirmiştir. Kasım 2021'de Biden, Huawei ve ZTE'nin ABD düzenleyicilerinden ekipman yapım lisansları almasını engellemeyi amaçlayan bir yasa tasarısı imzalamıştır. 2022'de Federal İletişim Kurulu, Huawei ve ZTE tarafından ABD'de üretilen bazı iletişim ekipmanlarının, ulusal güvenlik riskini gerekçe göstererek satışını yasaklayan yeni kuralları kabul etmiştir. Ocak 2023'te ise Biden

yönetimi, ABD şirketlerine Huawei'ye mal ihraç etmeleri için lisans vermeyi durdurmuştur (Berman vd., 2023).

ABD hükümetinin teknolojik rekabette Çinli şirketlere yönelik müdahalede bulunmasının itici güçlerinden en önemlisi ekonomik çıkarlar ve ulusal güvenlik kaygılarıdır. Ulus devletlerin endişeleri, Çin'in istihbarat teşkilatları ve Çinli teknoloji şirketleri ile arasındaki bağlantıya dayanmaktadır. Çin hükümetinin Huawei'yi casusluk yapmak için kullanmasına dair kamuya açık bir kanıt sunulmamıştır. Ancak Çin'in 2017 yılında yayınladığı Ulusal İstihbarat Yasasında, vatandaşların ve şirketlerin devletin istihbarat çalışmalarını desteklemesini, yardım etmesini, işbirliği yapmasını bir şart olarak göstermesi ve Çin Komünist Partisi'nin özel şirketler üzerindeki etkisini artırmak için devlet şirketleri ve yerel yönetimlerin özel şirketlere, özellikle teknoloji şirketlerine yatırım yapması bu algının temel dayanaklarından. Algılanan veya gerçek olan bu durumda, Huawei'nin 5G teknolojisinde lider konumda olduğu takdirde, barış veya çatışma zamanında Çin istihbarat servisleri ve Çin ordusu tarafından Huawei ekipmanlarının kontrol edilebileceğine ve kullanıcıları gözetlemek için kullanabilme yeteneği ihtimaline dair endişeler mevcuttur. Huawei ise verilerin hükümete verilmeyeceği, bunun bir zorunluluk olmadığını iddia etmektedir. Çin'in endüstriyel casusluk ve devlet tesislerini hedef alma konusundaki kötü ünü, Batı'ya karşı eksi yöndeki algısı, küresel bir güç olma arzusu, devlet olarak ulusal teknoloji endüstrisi üzerindeki hukuki ve siyasi baskısı hükümet ve şirketler arasındaki bağları temsil ettiğinin algısını yaratmakta ve batılı ülkeleri tedirgin etmektedir.

3.4.2.3. Telekomünikasyon Endüstrisindeki Küresel Tedarik Zincirinin Temeli : Hammadde

Telefonun temel bileşenlerini oluşturmak için hammadde tedarikinden başlayan bir süreç vardır. Telekomünikasyon endüstrisindeki ana katılımcılar arasında bileşen tedarikçileri, telefon ekipmanı üreticileri, telekomünikasyon ağ servis sağlayıcıları, müşteriler ve düzenleyiciler yer almaktadır. Telefon ekipman üreticileri, bileşen tedarikçilerinden hammadde temin eder, kendi araştırma ve geliştirmelerini yürütür, cihazları tasarlar ve dağıtım kanallarını oluşturur (Zhu & Pasadilla, 2015, s. 314).

Şekil 19: Akıllı telefonlar içerisinde bulunan madenler



Kaynak: <https://www.madenprofesyonelleri.com/akilli-telefonlar-icerisinde-bulunan-madenler/>

Siber uzayda oluşan tehditlerden biride tedarik zincirindeki etik sorunlardır. Cep telefonu satışları 2000'li yılların başından bu yana önemli ölçüde artmış ve satışın sürekli artmasına ek olarak, üreticiler ekran boyutlarını, kameralarının kalitesini ve işlevini sürekli artırma eğilimi göstermiştir. Cep telefonları dışında, rüzgar santralleri, LED ekranlar, güneş enerjisi santralleri gibi belirli yüksek teknoloji ekipmanlarının üretimi için değerli madenler yüksek talep görmektedir. Aynı zamanda bazı değerli madenler dünyanın sadece belirli ülkelerinde görülmektedir. Dolayısıyla hammaddeler, modern ekonomilerin ve jeopolitik rekabetin vazgeçilmez bir parçasıdır. Yenilikçi teknolojinin ve dijitalleşmenin sonucunda da hammadde talebi önemli ölçüde artmakta ve üretim aşamasında olumsuz etkilere sebep olmaktadır. Bu olumsuz etkilerin başında ise silahlı çatışmalara sebep olması ve işçi hakları ihlalleri yer almaktadır. Demokratik Kongo Cumhuriyeti ve Bolivya olmak üzere iki örneklem üzerinden hammadde konusunda bölgesel çatışmalar incelenmiştir.

3.4.2.3.a. Çatışma Mineralleri : Demokratik Kongo Cumhuriyeti

Toprakları doğal kaynaklar açısından zengin ve kara kütlesi bakımından Afrika'nın en büyük ikinci ülkesi olan Demokratik Kongo Cumhuriyeti, çatışma mineralleri olarak bilinen kalay, tungsten, tantal ve altın açısından da zengindir. Bu

minerallerin tümü elektronik cihazlarımızda bulunmaktadır. Örneğin kalay, metal bileşenleri birbirine lehimlemek için kullanılırken tantal, elektrik enerjisini depolayan kapasitörlerde kullanılır. Telefonu titreten bileşenlerde tungsten, devre kartı konektörlerinde ise altın kullanılır (Brigham, 2023). Demokratik Kongo Cumhuriyeti'nde bulunan çatışma mineralleri istikrarsızlığa da katkıda bulunmaktadır. Bu madenler, özellikle çok sayıda silahlı grubun ana finansman kaynağını oluşturdukları için uluslararası ilişkilerde önemli bir konudur. Uluslararası Af Örgütü'ne göre, maden bölgelerindeki çatışmaların temel nedenleri de madenlerdir (Kroutchinin & Baudrier, 2019, s. 5).

Örneğin lityum ve kobalt gibi elementler, akıllı telefonlarda, dizüstü bilgisayarlar ve elektrikli arabalarda güç sağlamak için kullanılan pillerdeki temel bileşenlerdir. Demokratik Kongo Cumhuriyeti, bu iki element açısından da zengin bir ülkedir. Kobalt, her yıl Apple, Google, Dell, Microsoft ve Tesla tarafından satılan milyonlarca üründe kullanılan şarj edilebilir lityum pillere güç sağlamak amacıyla gerekli olduğundan, kobalt talebi her geçen yıl katlanarak artmaktadır. 2019 yılında Apple, Google, Dell, Microsoft ve Tesla, insan hakları şirketi olan International Rights Advocates tarafından, Demokratik Kongo Cumhuriyeti'nden 14 ebeveyn ve çocuk adına Washington DC'de açılan bir davada sanık olarak gösterilmiştir. İlk kez teknoloji şirketlerinin madencilikte yaşanan ölümlerle ilgili yasal zorluklarla karşı karşıya kaldığı mahkemenin belgelerinde Apple, Google, Dell, Microsoft ve Tesla'nın kobalt tedarik zincirlerinin denetleme ve düzenleme yetkisine tabi olduğunu ancak bunu yapmayarak müşterilerinin madendeki ölümlere ve yaralanmalara katkıda bulunduğunu iddia etmektedir. Sanıklar ise iddialarını reddederek, madenlerin sorumlu bir şekilde tedarik edildiğini açıklamıştır (Kelly, 2019).

2010 yılında ABD'de kabul edilen Dodd-Frank Yasası, şirketlerin çatışma minerallerinin kullanımını açıklamalarını zorunlu hale getirmiştir. Yasa, tedarik zincirini izlemek için çalışan özel kuruluşların da ortaya çıkmasına neden olmuştur. Örneğin, Apple, Microsoft, Tesla, Intel, Samsung ve diğer yüzlerce çok uluslu şirket, sorumlu bir şekilde kaynak sağladıklarından emin olmak için bağımsız bir denetimden geçen izabe tesislerinin ve rafinelerin bir listesini tutan Sorumlu Mineraller Girişimi'nin (Responsible Minerals Initiative) üyeleridir (Brigham, 2023). Bu doğrultuda Apple 2021 tarihli çatışma mineralleri raporunda 2009'dan beri üçüncü taraf denetimine katılmayan, madenlerin sorumlu bir şekilde tedarik edilmesi için

gereklilikleri karşılamayan 163 izabe tesisini ve rafineyi tedarik zincirinden çıkardığını bildirmiştir (Apple Inc., 2021, s. 11).

3.4.2.3.b. Lityum Üçgeni : Bolivya, Şili, Arjantin

Küresel lityum yataklarının yaklaşık %56'sı Lityum Üçgeni olarak anılan Bolivya, Şili ve Arjantin'de bulunmaktadır. Bu ülkeler arasında Bolivya, dünyadaki en fazla lityum rezervine sahip bir ülkedir. Ayrıca Bolivya, telefonlarımıza, bilgisayarlarımıza, elektrikli araçlarımıza güç sağlayan piller için önemli bir bileşen olan lityum madenini ve diğer kaynakları millileştirme hedefi sebebiyle en büyük darbelerden birini yaşamış bir ülkedir. 21. yüzyılın altını olarak nitelendirilen lityum, Bolivya'nın And Dağları'nın yüksek kesimlerinde yer alan ve büyük ölçüde kullanılmayan Salar de Uyuni tuz düzdüklerinin, dünyada bilinen rezervlerin %25 ila %45'ini içerdiği, bunun dışında kalan yerlerde ise toplam %70'ine sahip olduğu tahmin edilmektedir (Atkins, 2019).

Bolivya, bağımsızlığını kazandığı 1825 yılından 2019 yılına kadar geçen 194 yılda 190 darbe girişimine tanık olmuştur. Yönetimi her seferinde güç kullanılarak değiştirilen ve genellikle çok uluslu maden şirketleri adına ordu tarafından yürütülen darbelere maruz kalan Bolivya, 2019 yılında "*insanlığın en kötü düşmanı ABD kapitalizmidir*" (Atkins, 2019) söyleminde bulunan Evo Morales'e yönelik gerçekleştirilen 191. darbeyi yaşamıştır. Morales, ülkenin doğal kaynaklarının ulus-ötesi şirketlere değil, kendi ülkesine fayda sağlamasını amaçlamış bir liderdir. Bu amaç doğrultusunda Morales, kamuya ait olan doğal kaynak endüstrilerden elde edilen parayı kullanarak, sömürülen ülkesine ekonomik ve sosyal demokrasi getirmek ve büyük bir yoksulluğu ortadan kaldırmak için birçok projede yer almıştır. Ekonomi ve Politika Araştırmaları Merkezi tarafından toplanan verilere göre, Bolivya'daki ekonomik büyüme, 2006-2019 Morales hükümeti döneminde Latin Amerika ve Karayipler bölgesindeki oranın iki katı artmış, GSMH'si ise 2,957 oranından ortalama %3,2 büyüme ile 4,287 oranına yükselmiş ve yoksulluk içinde yaşayan nüfusun yüzdesi 2018'de %60'ken %35'e düşmüştür (Arauz, Weisbrot, Bunker, & Johnston, 2019 , s. 5).

Morales girişimleri doğrultusunda, Hintli Jindal Steel, İsviçre merkezli Glencore, İngiliz-Arjantin kökenli Pan American, Kanada merkezli South American

Silver gibi güçlü çok uluslu maden şirketlerinin madencilik faaliyetlerinin birkaçını engellemiş ve sözleşmeleri feshetmiştir (Prashad, 2019). Ayrıca Morales'in batılı çok uluslu şirketlerle anlaşma yapmaması ve Çinli şirketlerle ortak olma kararı, hükümeti daha savunmasız hale getirmiş, Bolivya'yı ABD ve Çin arasındaki rekabetin içine sokmuştur. Morales'in Bolivya'da gerçekleştirdiği girişimler bir kalkınma modeli olarak kabul edilmesi gerekirken, hükümetin yanlış hareket ettiğine dair suçlamaların ardından sokak protestoları ve şiddet baş göstermiş, askeri bir darbeyle hükümet devrilmiştir. Sonucunda ise Bolivya bugün hala Güney Amerika'daki en yoksul ülke olmaya devam etmektedir.

Darbe sonrasında en çok öne çıkan fikirlerden biri, ABD dış politikası esasına dayanarak Suriye'deki petrol sahalarını ele geçirmek ve kontrol altında tutmak için Suriye'de kendi silahlı kuvvetlerinin konuşlandırılmasını gerçekleştirdiği gibi Bolivya'da doğal kaynakları kontrol etme arzusuyla hareket ettiği iddiaları ortaya çıkmıştır. Bu doğrultuda Bolivya'daki askeri darbe, ABD'nin kritik ve küresel bir kaynak olan lityum üzerinde kontrolünü sağlama amacıyla kendi silahlı kuvvetlerini konuşlandırmak yerine, darbe yoluyla rejim değişikliği için CIA tarafından tasarlanmış bir planın izlenmesiyle gerçekleştirilmiştir. Elon Musk, 24 Temmuz 2020'de Twitter'da Bolivya'nın lityum kaynaklarını elde edebilmek adına ABD hükümetinin desteği ile darbenin organize edildiğini ifade eden bir tweet'e yanıt olarak "*kimi istersek onu darbeleriz!*" yazısını paylaşmış ve yasadışı bir şekilde görevinden alınan Morales'e yönelik gerçekleştirilen darbeye atıfta bulunmuştur (Sweeney, 2020). Jeanine Anez liderliğindeki darbe yönetimi, Tesla dahil olmak üzere çok uluslu şirketlerin Bolivya'nın lityum rezervlerinden yararlanmaya davet etme planları duyurulmuş, dönemin eski Dışişleri Bakanı Karen Longaric'in Elon Musk'a yazdığı 31 Mart 2020 tarihli mektupta da "*sizin ve şirketleriniz ülkemize sağlayabileceği her türlü iş birliği minnetle karşılanacaktır*" ifadeleri yer almıştır (Sweeney, 2020). Tüm bu söylemler ise darbe sonrasında en çok öne çıkan fikirleri destekler nitelikte görünmektedir.

3.4.2.4. Metaverse

1992'de Neal Stephenson tarafından yazılan Snow Crash adlı romanında ilk kez tanıtılan (Joshua, 2017) ve "Evrenin Ötesi" olarak tanımlanan Metaverse, kodlarla desteklenerek sanal ve fiziksel dünyayı daha fazla birbirine bağlamaktadır. Sosyal

etkileşimler, eğitim, küresel siyaset ve yeni ekonomilerin inşa edilmesi dahil birçok alanda etki gösteren Metaverse, özellikle küresel teknoloji şirketlerinin eylemlerine, ulus devletlerin yatırımlarına, kamusal uygulamalarına ve siyasi faaliyetlerine yön vermekte ve yeni fırsatlar sunmaktadır (Yetgin & Özkan, 2022 , s. 209).

Bilgi ve iletişim teknolojileri perspektifinden bakıldığında Metaverse, 21. yüzyılın en büyük teknoloji devrimi ve internetin bir sonraki evrimsel adımı olarak nitelendirilmektedir. Dijital altyapısının merkezinde bağlantı, bilgi işlem ve yapay zeka bulunan Metaverse, sanal gerçeklik (VR), artırılmış gerçeklik (AR), nesnelerin interneti, 5G, blok zinciri, bulut bilişim, 3D, insan-makine etkileşimi, dijital para birimi, Web 3.0 ve daha fazlasını içeren birkaç farklı teknolojinin bir araya gelmesinin sonucudur.

3.4.2.4.a. Çok Uluslu Şirketlerin Metaverse Stratejileri

Çok uluslu şirketler için Metaverse teknolojisi, önemli bir rekabet alanıdır. Şirketler Metaverse vizyonuna yatırım yaparak, daha geniş kitleye ulaşmakta ve siber uzayda dijital ayak izi bırakmaktadır. Çok uluslu şirketlerin sanal dünyalara yatırım yapması ve özellikle son dönemde Metaverse teknolojisinin ön plana çıkarılması, şirketlerin politikalarının Endüstri 4.0'a geçme isteğinden, Endüstri 4.0'ın oluşturacağı olanakların farkına vararak Metaverse'ü yeni yatırım alanı olarak görerek yeni bir pazar payında yer almak istemesinden kaynaklanmaktadır. Özellikle 2019'da başlayan ve bütün dünyayı etkisi altına alan Covid-19 pandemi sürecinin etkisiyle hayat tarzları önemli oranda değişmeye başlamış ve yeni iş kolları oluşmaya başlamıştır. İnsanların evlerine kapanması ve evden çalışma süreci, siber uzayın çok fazla yeteneği kaldırdığı ve bünyesinde barındırdığını keşfettirmiş ve böyle bir düzen içerisinde siber uzaya yatırım yapmak büyük şirketler için en öncelikli iş olmuştur (Yetgin & Baştuğ, 2022, s. 26-27).

ABD'de Amazon, Google, Meta, Roblox, Facebook, Epic Games, Disney, Snapchat (Bitmoji), Nvidia, Microsoft (Microsoft için Mesh), Decentraland, Apple; Çin'de Tencent (Kings Metaverse), Alibaba, ByteDance, NetEase, Zqgame, Wondershare; Güney Kore'de, Samsung, SK Telecom, Urbanbase, Metaverse Alliance; Japonya'da Sony, Hassilas, GREE, Avex; İngiltere'de Sotheby's, Maze Theory; Fransa'da Stage11; İtalya'da Gucci çok uluslu şirketleri Metaverse vizyonuna yatırım

yapmış ve ürün geliştirmiş şirketlere örnektir (Lopez-Diez, 2021, s. 302). Çalışmada Metaverse vizyonunda rekabet edebilirliği yüksek Microsoft, Apple, Meta ve Samsung çok uluslu şirketlerinin Metaverse girişimleri örnek olarak incelenmiştir.

Metaverse vizyonunu geliştirebilecek yazılım ve donanıma sahip önemli bir şirket olan *Microsoft*, yatırımlarıyla önemli ürünler sunmakta ve stratejiler geliştirmektedir. Özellikle oyun teknolojisi ve araçlarına yatırım yapan Microsoft, Ocak 2022'de "Call of Duty", "Warcraft", "Candy Crush", "Diablo" gibi dünya çapında ünlü oyunların üreticisi ve eğlence içeriği yayıncısı Activision Blizzard Anonim Şirketini 68,7 milyar dolara satın alacağını duyurmuştur. İşlemler sona erdiğinde ise Microsoft, Tencent ve Sony'nin ardından gelir bakımından dünyanın üçüncü büyük oyun şirketi olacaktır (Microsoft, 2022).

Microsoft'un diğer önemli bir Metaverse girişimi ise 2020'de yaşanan Covid-19 salgınının ofis çalışmaları üzerindeki etkisiyle başlayan "Microsoft Teams için Mesh (Mesh for Teams)" uygulamasıdır. 2022'de kullanıma sunulan uygulama, iş toplantısı ve eğitim gibi durumlarda farklı fiziksel konumdaki bireylerin üç boyutlu holografik deneyimlerle, siber uzayda buluşmayı ve işbirliğini sürdürme deneyimini sunmaktadır (Yetgin & Özkan, 2022 , s. 212).

Apple, marka erişimini yeni tüketicilere genişletmek için hem erken dönemde hem de gizli olarak Metaverse teknolojisinden yararlanarak ürünlerini geliştirmektedir. 2014 yılında Apple, müşterileri için giyilebilir teknoloji olan "Apple Watch" adını verdikleri ürünü geliştirmiştir. 2015 yılında ise iPhone 6s satışlarını artırmak için Apple, Metaverse vizyonundan yararlanmış, telefonun sanal gerçeklikle uyumlu bir sürümünü geliştirerek iPhone 6s satışlarında %30'luk bir artış elde etmeyi başarmıştır (Bushell, 2022, s. 26). App Store'da yüzlerce artırılmış gerçeklik tabanlı uygulamanın bulunması, artırılmış gerçeklik gözlükleri ve sanal gerçeklik başlıkları üzerine çalışmalar yürütüyor olması, yeni nesil kulaklıklarının hem artırılmış gerçeklik hem de sanal gerçekliği destekliyor olması Apple'ın diğer Metaverse ürün ve hizmetlerine örnektir.

Sosyal medya devi *Facebook*, Metaverse vizyonu ile tüm iş modelini yeniden şekillendirmesi, 28 Ekim 2021'de Facebook'un CEO'su ve kurucusu Mark Zuckerberg'in şirketin adını Meta Platforms Inc. olarak değiştireceğini ve bir Metaverse şirketi olacağını duyurmasıyla başlamıştır. Meta'nın şirket ismini

değiştirmesindeki en önemli etken, aynı teknolojinin birden fazla ticari versiyonunun oluşturulmasıyla tek kazanç yerine birden çok kazancın elde edilmesine olarak sağlama isteğidir. Meta şirketi, ilk olarak Meta ismini benimseyerek, farklı bir sosyal ağ modeline geçtiğini duyurmasının ve yeniliklerini kullanıcılarına aktarmasının ardından hisse değerleri artmıştır. Ayrıca, ilerleyen süreçte Metaverse'de gerçekleştirilecek bütün eylemler için aracılık eden yeni teknolojik ürünlerin satışı ve pazarlanmasında ürünlere lisanslama yoluyla ek kazanç elde etme stratejisine de başvurmuştur (Yetgin & Baştuğ, 2022, s. 28) Ayrıca Meta, toplam on milyar dolar harcama ile dijital ürün ve hizmetler doğrultusunda çalışmalarını genişleteceğini de duyurmuştur (Bushell, 2022, s. 33). Meta'nın merkezi olan Horizon Home, Meta Quest ve Project Cambria sunulan ürünler arasındadır.

Andorid telefon pazarının önemli ismi olan *Samsung*, New York City'de bulunan Samsun 387 isimli mağazasını sanal olarak "Samsung 837X" ismi ile Metaverse platformu olan Decentraland'da kurmuş ve Şubat 2022'de Galaxy S22'nin ilk tanıtımı dahil, yeni nesil Galaxy S modellerinin tanıtımını, 100 bini aşkın kişinin katılımı ile Samsung 837X'de gerçekleştirmiştir (Yetgin & Özkan, 2022 , s. 2012).

Latin Amerika bölgesindeki ülkeler, Metaverse vizyonunu oluşturan teknolojileri geliştirmek için çalışmaktadır. Ancak bu teknolojiyi tam olarak dağıtmak için bağlantı kapasitesinin yetersizliği ve sınırlı ağ altyapısı sebebiyle Latin Amerika'da bu teknolojinin uygulanması biraz daha yavaş olsa da aldığı yatırımlarla gelişmelerini sürdürmektedir. Aralık 2022'de Samsung, Latin Amerika bölgesindeki müşterileri hedefleyen Metaverse projelerine 35 milyon dolardan fazla yatırım yapacağını açıklamıştır. Bu hareketin arkasındaki amaç, markanın dijital büyüme ve pazarlama stratejisinin bir parçası olarak genç kitleleri çekmesine ve onlarla bağlantı kurmasına yardımcı olmaktır (Goschenko, 2022).

3.4.2.4.b. Ulus Devletlerin Metaverse Stratejileri

Teknolojik gelişmeler sebebiyle devletlerin, giderek daha dijital hale gelen ve coğrafi sınırları aşan dünyaya uyum sağlama zorunluluğu doğmakta ve devletlerin rekabet seviyelerini etkilemektedir. Hükümetler, artırılmış gerçeklik, sanal gerçeklik ve dijital ikizler gibi Metaverse teknolojisinin ekonomik, sosyal, kültürel ve politik hedeflerine ulaşmak için gerekli olduğunun farkına varmaktadır. Bu doğrultuda bir ilki

temsil eden, Karayiplerin en doğusunda 430 km² yüz ölçümü ile küçük bir ada devleti olan Barbados, diplomatik misyonunu genişletmek ve dünyanın geri kalanı ile ilişkiler kurmak amacıyla -uluslararası hukuka ve Viyana Sözleşmesine uygun olacağını açıklayarak- ilk Metaverse büyükelçiliğini Kasım 2021'de Metaverse platformu olan Decentraland ile anlaşma imzalayarak açmıştır. Ancak Barbados'un oluşturduğu dijital büyükelçiliğinin başarısı, diğer ulus devletlerinde Metaverse platformuna katılmasına bağlı olacaktır (Yetgin & Özkan, 2022 , s. 211-212).

Güney Kore hükümeti tarafından da Metaverse için ulusal olarak önemli ve somut adımlar atılmıştır. Ulusal Metaverse stratejisi için Güney Kore, 2021'de "Metaverse Alliance"ı başlatmıştır. Ülke, dijital dönüşümü kolaylaştırmak için 2022 bütçesinden yaklaşık 8 milyar dolar ayırmıştır. BİT ve Gelecek Planlama Bakanlığı ve Ulusal BT Sektörü Teşvik Ajansı, K-Metaverse olarak adlandırılan devasa bir proje başlatmıştır (Kshetri, 2023, s. 139). Şehir hizmetleri için sanal platformlar oluşturmak amacıyla 2021'de başkent Seul için ekonomik, kültürel, turizm, eğitim ve vatandaşlık hizmetlerini içeren ve yaklaşık 2,8 milyar avro yatırım yapılan "Metaverse Seoul" projesini duyurmuştur (Yetgin & Özkan, 2022, s. 211).

Birleşik Arap Emirlikleri'nin Yapay Zekadan Sorumlu Devlet Bakanı 2022'de, Metaverse stratejisinin turizm, eğitim, devlet hizmetleri, emlak gibi konulara odaklanacağını, meta veri deposunun, ülkenin kültürünü ihraç etme fırsatlarını değerlendirmek için bir görev gücü başlatma planını duyurmuştur (UAE Moments, 2022). BAE Ekonomi Bakanlığı ise hükümetler, küresel şirketler ve halkın bağlantı kurması, işbirliği yapması ve idari işlerin verimliliğini artırmak amacıyla Metaverse'de genel merkezini açmıştır. Ayrıca Bakanlığın, Meta evrendeki diğer ülkelerle ikili anlaşmalar imzalaması için ileri teknolojilerle destekleneceği bildirilmiştir (UAE Moments, 2022a). Temmuz 2022'de BAE'nin en kalabalık şehri Dubai için dünyanın ilk 10 Metaverse ekonomisi arasına girmesini amaçlayan Dubai Metaverse Stratejisi başlatılmıştır. Hedefi ise, 1.000'den fazla blok zincir ve Metaverse şirketini şehre çekmek ve 2030 yılına kadar 40.000'den fazla sanal işi desteklemektir (Kshetri, 2023, s. 140).

Çin'de ise internet ve teknoloji alanında uygulanan katı kurallar ve sansürler sebebiyle Metaverse teknolojisinde nasıl gelişim göstereceği tartışma konusudur. Bu sebeple Çin hükümeti Metaverse stratejisinde dünyanın geri kalanından farklı bir

strateji izlemektedir. Dolayısıyla hükümet kripto para birimlerinin kullanımı, oyun bağımlılığı, yetkisiz sınır ötesi veri hırsızlığı, hileli yatırım planları gibi olumsuz etkileri değerlendirerek, dış dünyayla bağlantılı ama kendi yöntemleri ile strateji geliştirme eğilimindedir. Çin'de Metaverse stratejisi, 2021'de Devlet Güvenliği Bakanlığı'nın 11. bürosu olan Çin Çağdaş Uluslararası İlişkiler Enstitüsünün "*Chinaverse*" girişimini başlatmasıyla gündeme gelmiştir (Liu, 2022). Ayrıca finansal ve ticari merkez olan Şanghay, en gelişmiş Metaverse stratejileri için önemli bir şehirdir. Temmuz 2022'de Şanghay, Metaverse gelişimine 1,5 milyar dolar yatırım yapmayı planladığını duyurmuştur. Şehirde on lider şirket geliştirmek ve Metaverse sektöründe yüz küçük ölçekli firma geliştirerek 2025 yılına kadar yüz adet Metaverse ürününü piyasaya sürmesi ve 52 milyar dolar değerinde bir Metaverse ekonomisi kurulması beklenmektedir (Kshetri, 2023, s. 138).

3.4.2.5. Toplum 5.0

İnsanlık tarihine baktığımızda, toplumların farklı aşamaları tanımlanmaktadır: insan gruplarının doğa ile uyumlu bir şekilde yaşadığı ve avcılıkta ustalaştığı Avcı Toplumu (Toplum 1.0), yeni tarım tekniklerinin gelişmesiyle ve ulus inşasına dayalı grupların olduğu Tarım Toplumu (Toplum 2.0), sanayi devrimi ile başlayan Sanayi Toplumu (Toplum 3.0), bilginin önem kazandığı Bilgi Toplumu (Toplum 4.0). Bilgi ve zekanın üretimi, teknoloji yardımıyla insanlar tarafından yapıldığı Toplum 4.0'ın üzerine inşa edilmiş ve insan merkezli bir toplumu hedefleyen, siber ve fiziksel dünyayı tamamen birleştiren Toplum 5.0 aşamasının amacı ise bilgi ve zekanın makineler aracılığıyla üretilerek insanlara sunulmasıdır (Kurter, Temizkan, Yılmaz, & Yetgin, 2021, s. 18).

Japonya tarafından büyüme stratejinde çok önemli bir rol oynayan Toplum 5.0, 2016'da Japon kabinesi tarafından kabul edilen 5. Bilim ve Teknoloji Temel Planında bir kavram olarak sunulmuştur. Kavramın arkasındaki niyet, bilgi ve iletişim teknolojilerinden sonuna kadar yararlanarak fiziksel alan ve siber uzayı birleştiren bir girişim aracılığıyla gelecekteki toplum için insanlara zenginlik getirecek bir "*süper akıllı toplum*" projesidir (Deguchi vd., 2020, s. xi).

Toplum 5.0 projesi, siber uzayın ve fiziksel alanın entegrasyonuna vurgu yapmaktadır. Toplum 5.0 söz konusu olduğunda, siber uzay sadece çok büyük

miktarda veri alışverişi için kullanılan bir alan anlamına gelmemektedir. Aynı zamanda bilgisayar ağları tarafından sorunları analiz etmek ve fiziksel alandaki sorunlara yönelik çözümleri modellemek için oluşturulan bir alan anlamına da gelir (Deguchi vd., 2020, s. 3). Özellikle yaşlı nüfusunun artması, doğum oranının ve genç nüfus oranının azalması ulusal olarak üretim gücünün ve kaynakların yetersizliği noktasında yeni sorunları beraberinde getirmekte ve endişe yaratmaktadır. İnsan merkezli bir toplum yaratma çabasının yanı sıra çeşitli toplumsal sorunların çözümünü de içeren Toplum 5.0 vizyonundaki siber ve fiziksel alanın entegrasyonu sayesinde hem ekonomik kalkınmanın hem de toplumsal zorlukların çözümünün sağlandığı, tarım, gıda, sağlık, finans, enerji, doğal afet gibi tüm ihtiyaçlarının karşılandığı, refah seviyesi yüksek bir toplum yaratmak amaçlanmıştır.

Toplum 5.0 kapsamında öngörülen önemli uygulamalardan biri doğal afetlerin önlenmesi ve erken koruyucu müdahalelerin yapılması üzerinedir. Bu bağlamda afetlerden etkilenen alanların uydulardan, hava denetim radarlarından veya insansız hava araçlarından ya da sensör verilerine dayalı hasar bilgilerinden ve otomobillerden alınan yol hasarı bilgilerinden elde edilen verilerin büyük veri platformlarına yapay zeka tabanlı analizler yoluyla anında müdahale edilmesi mümkündür. Bu sayede afetlerden etkilenenlerin yerleri anında tespit edilerek, sağlık, gıda, hijyen ve barınma ihtiyaçları hızlı bir şekilde temin edilebilmekte, kurtarma robotları kullanımı ile enkazlar daha güvenli bir şekilde taranabilmekte, yolların kapandığı durumda malzeme lojistiği insansız hava araçları ile sağlanabilmektedir. Menşe ülkesi olması itibarıyla insan merkezli Toplum 5.0 projesi kapsamında Japonya'da 157 bölgede kamu-özel-akademi ortaklığında toplam 229 adet akıllı şehir projesi faaliyete geçirilmiştir (Arı, 2021, s. 470).

Toplum 5.0'ın tarım ve gıda sektöründe de uygulama alanları mevcuttur. Sensör teknolojisi ve nesnelerin interneti sayesinde meteorolojik veriler, ürün büyüme verileri ve piyasa verileri, gıda eğitimleri gibi bilgilerden oluşan büyük veri niteliğindeki verilerin yapay zeka ile analiz edilmesi sonucu pek çok işlemde yüksek verim sağlanmaktadır. Tarım işlerinde sürücüsüz traktör aracılığıyla iş gücünden tasarruf ederek, insansız hava araçları aracılığıyla mahsul verilerinin toplanmasını otomatikleştirerek, hava tahmini ve su verilerine dayalı olarak su yönetimini daha yüksek performanslı hale getirerek emek tasarrufu sağlayan ve yüksek verim sağlayan,

ürünleri tüketicilere istendiği zamana ulaştırarak değer zincirini güçlendiren "akıllı tarım" uygulamaları son dönemde oldukça yaygınlaşmıştır (Arı, 2021, s. 472).

Yaşam kalitesini artırmak adına hasta-doktor-makine işbirliğini oraya koyan mobil uygulamalar, giyilebilir teknolojilerle, yapay zeka uygulamalarıyla kendini gösteren "akıllı sağlık" kavramı da Toplum 5.0 ile birlikte ortaya çıkmıştır (Büyükgöze & Dereli, 2019, s. 179-180).

3.4.3. Siber Uzay ve BİT Sektörü

İnternet, dünya genelinde topluma yayın yeteneği sunmakta, bilgi yayma mekanizması olarak görev yapmakta, coğrafi konuma bakılmaksızın bireyler ve bilgisayarlar arasındaki bağlantı göreviyle işbirliği, örgütlenme ve etkileşim için bir ortam sağlamaktadır. İnternet kavramı, 1960'ların sonlarında ARPA (Gelişmiş Savunma Araştırmaları Projeleri Birimi) tarafından geliştirilen ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı) ile doğmuştur. İnternetin ve modern siber çağın başlangıcı olan ARPANET, Soğuk Savaş döneminde yaşanan nükleer savaş tehdidi sebebiyle ABD tarafından geliştirilen savunma amaçlı bir projedir. (Singer & Friedman, 2014, s. 34) 1957'de Sovyetler Birliği tarafından uzaya fırlatılan Sputnik 1 nedeniyle ABD, Sovyetler Birliği'nin uzaydan saldırmasından ve iletişim ağını yok etmesinden endişe duyması sebebiyle bir nükleer saldırı durumunda ABD'de iletişim ağını aktif tutmak için bilgisayarların birbirine bağlanmasını sağlayan ARPA Ağı kurulmuştur. 1989 yılına gelinliğinde CERN'de (Avrupa Nükleer Araştırma Merkezi) görevli olan Tim Berners-Lee, HTML (Hyper Text Markup Language-Hiper Metin İşaretleme Dili) işaretleme dilini geliştirmesinden sonra WWW (World Wide Web-Dünya Çapında Ağ) sistemi kurulmuştur (Fitzpatrick, 2017).

İnternet, ortaya çıktığı andan itibaren özgür ve açık bir alan olarak düşünülmüştür (Hawkins, 2016, s. 3). Ocak 2023 itibariyle, dünya nüfusunun %64,4'üne denk gelen 5,16 milyar internet kullanıcısı bulunmaktadır. Bu oran içerisinde 4,76 milyarı sosyal medya kullanıcılarıdır (Statista , 2023).

Çalışmanın bu bölümünde veri güvenliğinin ve istihbaratın dijital alanda ne kadar önemli olduğunu ve sosyal medya şirketlerinin kritik süreçlerde nasıl bir rol oynadığını ele almak için Cambridge Analytica skandalı ele alınmıştır. Devletleri,

şirketleri ve bireyler tehdit eden internet ortamının güvenlik açıkları, Dark Web ve Deep Web üzerinden örneklerle açıklanmıştır. Sektör üzerindeki siber saldırılar ise Amerikalı teknoloji şirketi Microsoft, İngiltere merkezli telekomünikasyon şirketi Vodafone, Alman telekomünikasyon şirketi T-Mobile, Amerikan eğlence şirketi Sony Pictures üzerinden örneklerle ele alınmıştır.

3.4.3.1 Çevrimiçi Sosyal Ağlar ve Siber Tehditler

Çevrimiçi Sosyal Ağlar, dünya çapında milyonlarca insanın etkileşimine olanak sağlayan bilgi sistemleridir. Twitter, YouTube, Facebook, LinkedIn, Google gibi popüler olan sosyal ağlar, toplumun siyasi, ekonomik ve sosyal bağlantılarını, seslerini ve aracılıklarını hızlandırma potansiyeline sahiptir ve ilişki geliştirme, bireysel deneyimlerin paylaşılması, farklı hizmetlerin sunulması gibi amaçla hizmet etmektedir (Rehman, 2019). Hızla büyüyen ve çeşitli faydalar sunan çevrimiçi sosyal ağlar, siber güvenlik endişelerini de beraberinde getirmektedir. Verilerin gizlilik ihlalleri, internette bıraktığımız veri izleri üzerinden üçüncü taraflar tarafından gerçekleştirilen veri madenciliği ve uygulamaların kullanıcılardan istediği resim veya konum gibi kişisel bilgilere erişim izni ile gerçekleştirilebilecek kötü amaçlı yazılım saldırıları siber güvenlik tehditlerine örnektir.

Dijitalleşen günümüz dünyasında kişisel verilerin gizliliği ve kişisel verilerin izinsiz kullanımı siber uzayda önem kazanmış bir konudur. İnternet üzerinden gerçekleştirilen her faaliyet, vatandaşların birçok kişisel bilgilerini gözler önüne sermekte ve bu bilgiler hem politik hem de ticari amaçlarla kullanılabilir (Bozkanat & Çömlekçi, 2020, s. 40). Sosyal ağ tarihindeki en büyük veri sızıntılarından biri Cambridge Analytica skandalı, küresel siyaseti etkilemek için bilgi ve iletişim teknolojilerinin nasıl manipüle edilebileceğini ve kişisel kullanıcı verilerinin siyasi amaçlarla nasıl kötüye kullanılabileceğini gösteren örnek bir vakadır.

Londra merkezli veri analitiği yapan ve siyasi kampanyaların çevrimiçi olarak potansiyel seçmenlere ulaşmasına yardımcı olan Cambridge Analytica, seçmen profillerini oluşturmak için çevrimiçi bilgiler ve anket dahil olmak üzere birçok kaynaklardan gelen verileri birleştirerek seçmenleri hedefleyen projeler geliştirmiştir. Örneğin özel reklamlardan etkilenebilecek olan seçmen davranışını tahmin etmek için

bir bilgisayar programı kullanarak seçim kampanyalarında stratejik adımları belirlemekteydi.

Cambridge Üniversitesinde akademisyen olan Aleksandr Kogan, 2013 yılında kişilik testi içeren "this is your digital life" aldı bir uygulama geliştirmiştir. Uygulama, Facebook hesabına sahip ve ABD'li seçmenler arasından yaklaşık 300.000 kullanıcıya psikolojik bir profil oluşturulması için soruları yanıtlamaya yönlendirmiştir. Sonuçlar kaydedildikten sonra kullanıcıların Facebook hesaplarından kişisel verilerini ve arkadaşlarının verilerini toplamıştır (Meredith, 2018). Kısa bir süre içinde Cambridge Analytica, milyonlarca ABD seçmeninden oluşan, siyasi inançları ve kişilik özelliklerini belirleyen algoritma ve veri tabanına sahip olmuştur.

Facebook'tan toplanan veriler, Donal Trump'ın 2016 başkanlık seçimlerinde Hillary Clinton'a karşı yürüttüğü başarılı kampanyada önemli bir rol oynamıştır. Trump kampanyası, 2016 seçimleri sırasında veri işlemlerini yürütmek, reklamlarla hedeflenecek seçmenleri belirlemek, kampanyanın nerede durdurulacağını ve konuşmalarda neler söyleneceği gibi stratejik iletişime yardımcı olmak için Cambridge Analytica'yı işe almıştır (Sherr, 2018). Federal Seçim Komisyonu dosyalarına göre, Trump kampanyası tarafından Cambridge Analytica'ya 5,9 milyon dolar ödeme yapılmış, bu ödemenin 5 milyon doları televizyon reklamlarını satın almaya ayrılırken, geri kalanı ekibe verilmiştir (Federal Election Commission [FEC], 2016).¹¹ Michigan, Wisconsin ve Pennsylvania eyaletlerinden hedef seçmenleri belirleyen şirket, çok az bilinen bir Facebook özelliği "Dark Post" uygulamasını kullanmıştır. Uygulama sosyal medyada hedeflenen seçmenlerin alışkanlıklarına ve dijital parmak izlerine dayalı olarak oluşturulan ve sadece hedeflenen seçmenler tarafından görülebilen kişisel reklam yayınlamasını içermektedir. Siber saldırı olarak nitelendirilebilecek bu girişim, Trump'ın üç eyalette 77.000 oy almasını sağlamıştır (Rehman, 2019).

Kogan'ın geliştirdiği uygulama aracılığıyla kullanıcı verileri, Facebook'un rızası olmadan Cambridge Analytica ile paylaşılmıştır. Bu nedenle Facebook politikalarını ihlal etmesi sonucunda uygulama, Facebook tarafından yasaklanmış ve 87 milyon kullanıcıdan toplanan tüm verilerin yok edilmesi istenmiştir (Nieva, 2018).

¹¹ Ayrıca bkznz: ayrıntılı diğer ödemeler:

https://www.fec.gov/data/disbursements/?data_type=processed&committee_id=C00580100&recipient_name=cambridge+analytica&two_year_transaction_period=2016&min_date=01%2F01%2F2015&max_date=12%2F31%2F2016

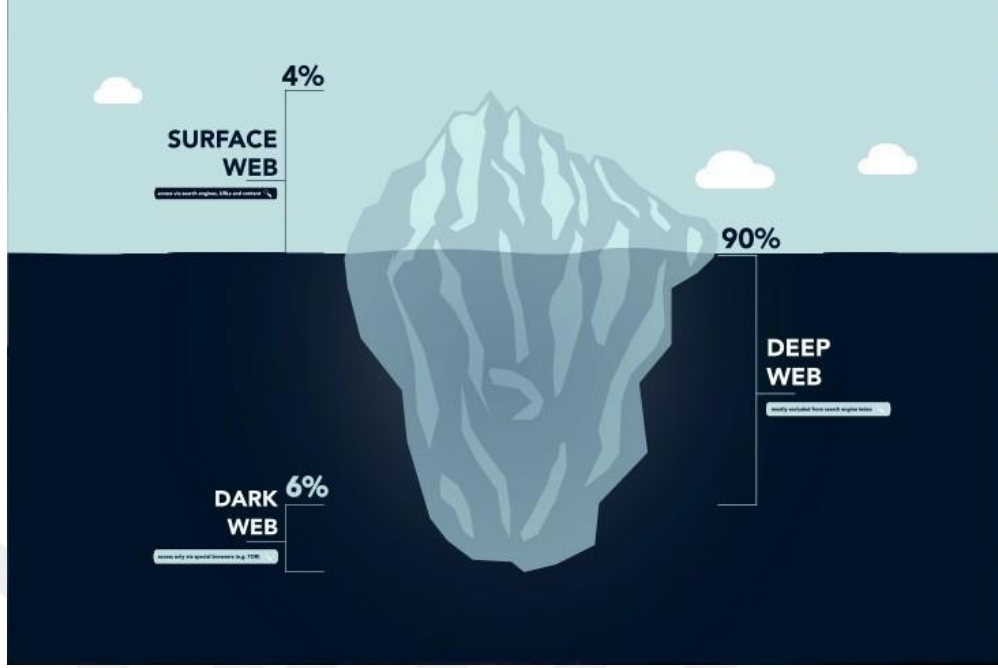
21 Mart 2018'de ise Facebook, büyük miktarda bilgiye erişimi olan uygulamaları araştıracağını, şüpheli etkinlik içeren herhangi bir uygulamayı denetleyeceğini ve kişisel bilgileri kötüye kullanan herhangi bir uygulama geliştiriciyi tespit edeceğini açıkladıktan sonra yüzlerce uygulamayı askıya almıştır (Wong, 2019). Ayrıca süreç içerisinde Facebook, çok sayıda dava, ABD, İngiltere, AB hükümet soruşturmaları, boykot kampanyası ve piyasa değerinde keskin düşüşle karşı karşıya kalmıştır. ABD Federal Ticaret Komisyonu'nun, Facebook'a yönelik verdiği 5 milyar dolarlık pazar cezası, tüketicilerin gizliliğini ihlal ettiği için herhangi bir şirkete verilen en büyük ceza ve dünya çapında şimdiye kadar uygulanan en büyük veri güvenliği cezasından yirmi kat daha büyüktür (Federal Trade Commission [FTC], 2019).

Cambridge Analytica'nın milyonlarca sosyal medya kullanıcısının kişisel verilerini yasa dışı bir şekilde elde ettiği haber ortaya çıktığında, Avrupa ve ABD'deki düzenleyici kurum ve medya, kişisel kullanıcı verilerini koruma ve güvence altına alma konusundaki yetersizliğini sert bir şekilde eleştirmiş ve büyük verilerin siyasi kazanç için olası kötüye kullanımı konusunda temel sorunları gündeme getirmiştir (Neudert & Marchal, 2019). Cambridge Analytica 2018 yılında kapansa da, bugün tekniklerinin tekrarlanabilirliği hakkındaki sorular hala devam etmektedir.

3.4.3.2. İnternetteki Siber Tehditler : Deep Web ve Dark Web

İnternetin güvenlik açıklarına sahip olması, anonim yapısı, atıf ve tespitite yaşanan zorluklar, ulus devletlerin her türlü faaliyetini ağlar üzerinden ve kritik altyapılar aracılığıyla yürütmesi nedeniyle başta devletler olmak üzere, şirketlerin ve bireylerin de yaşamlarını tehdit eden bir seviyeye gelmiştir (Çelik, 2018, s. 150).

Şekil 20: İnternetin katmanları



Kaynak: <https://berqnet.com/blog/dark-web-ve-deep-web-nedir>

Popüler arama motorları ve geleneksel web tarayıcıları kullanılarak çevrimiçi içeriklerin kolayca görüntülenebildiği internet bölümü yüzey ağı (surface web) olarak bilinmektedir ve bu alan Google, Yahoo, Bing gibi arama motorlarını kullanarak bulunabilecek tüm web sitelerini içermektedir (Başakçi, 2019).

İnternetin devasa alt bölümü olarak bilinen ve yüzey ağından 500 kat daha büyük olduğu tahmin edilen -Hidden Web (Gizli Web) ya da Invisible Web (Görünmeyen Web) olarak da isimlendirilen- Deep Web (Derin Web), Google gibi standart arama motorları tarafından indekslenemez. Deep Web'e erişim için The Onion Router (Tor) olarak bilinen anonimliği koruyan özel tarayıcılara ve özel olarak yapılandırılmış yazılımlara ihtiyaç vardır. Ortalama bir internet kullanıcısının Deep Web'i kullanmayacağı varsayıldığı için bu ağın kullanımı şüpheli olarak değerlendirilmektedir (Hawkins, 2016, s. 6).

Ancak Deep Web'in kullanımı tamamen yasa dışı olmamakla birlikte, birçok siyasi düşünür, gazeteci, bilim insanı, akademisyen ve özel hayat gizliliğine önem veren sıradan vatandaşlar tarafından kullanabilmektedir. Örneğin Arap Baharı sürecinde mevcut hükümet tarafından internet ve diğer kitle iletişim araçlarındaki kullanımın yasaklanmasının ardından seslerini Twitter ve Facebook üzerinden

duyurmaya çalışan vatandaşların, VPN'in yanı sıra, Tor ile birlikte Deep Web'i aktif bir şekilde kullandığı bilinmektedir (Çelik, 2018, s. 155).

Dark Web (Karanlık Ağ) ise Deep Web içerisinde bulunan, arama motorlarından ve normal internet kullanıcılarından gizlenen, Tor aracılığıyla erişimi mümkün olan bir alandır (Hawkins, 2016, s. 10).

Dark Web tamamen anonimdir ve bu nedenle devlet kurumları veya kolluk kuvvetleri gibi sorumlu kurumlardan gizli kalmak isteyen gruplar tarafından yasa dışı amaçlarla kullanılmaktadır. Dünya çapında anonim kalmak isteyen kullanıcılar için bir merkez haline gelen karanlık ağ, yüksek derecede anonimlik içermesi sebebiyle kötü niyetli kullanıcılar tarafından çocuk pornografisi, kötü amaçlı yazılım, propaganda, terör örgütlerine katılım ve çevrimiçi terör eğitimi almaya teşvik, kişisel bilgilerin satılması, ulus devletlerin politikalarıyla ilişkin bilgilerin ve istihbaratın ifşası, kara para aklama, organ ticareti ve uyuşturucu, silah, insan kaçakçılığına kadar yasa dışı faaliyetler için kullanılmaktadır. Bu tür sistemlerin kullanıcıları, daha fazla korunmak ve gizli kalmak için para işlemlerini, Bitcoin kullanarak gerçekleştirmektedir (Spalevic & Ilic, 2017 , s. 75).

İpek Yolu (Silk Road) ; Anonim Tor ağındaki gizli bir Dark Web özelliğiyle işletilen ve 2011 yılında kurulan Silk Road, kullanıcıların anonim olarak uyuşturucu, sahte kimlikler, kaçak yazılım, kara para aklama gibi yasadışı ürün ve hizmetleri - elektronik olarak oluşturulan izlenemeyen sanal para birimi Bitcoin'i kullanarak alıp satabilecekleri ilk modern ve anonim Dark Web pazarı olarak bilinmektedir. Kurucusu Ross Ulbricht, 2011'den 2013'e kadar sadece bir bilgisayar ve internet yardımıyla milyonlarca dolar gelir elde etmiştir. 2013 yılında ise FBI, Silk Road web sitesini kapatarak Ulbricht'i kara para aklama, bilgisayar korsanlığı, uyuşturucu kaçakçılığı, Silk Road'u ifşa etmekle tehdit ettikleri için en az beş kişiyi öldürmeye teşebbüsle suçlanmış ve müebbet hapis cezasına çarptırılmıştır (Pace, 2016, s. 3). Ulbricht'in tutuklanmasından ve sitenin kapatılmasının ardından, aynı sitenin yöneticileri Silk Road 2.0'ı karanlık ağda yeniden aktif hale getirmiştir. Ancak aynı yıl içerisinde sitenin sahibi Blake Benthall, FBI tarafından tutuklanmıştır (Knibbs, 2014).

Silk Road sonrası dönemde, birçok Dark Web pazar yerleri gelişmeye devam etmiştir. Tor ağı, kolluk kuvvetlerinin Silk Road'ın arkasında tam olarak kimin olduğunun bulunmasını zorlaştırsa da, bu vaka gelecekteki eylemler için bir zemin

hazırlamıştır. Yasadışı ürün ve hizmetleri içinde barındıran bir endüstri olarak Dark Web pazarları, hükümetler için büyük bir endişe kaynağıdır. Bu nedenle dünyanın birçok yerinde Dark Web pazarlarının büyümesini durdurmak için hükümetler kolluk kuvvetleri ile birlikte çalışmaktadır (Avast, tarih yok).

Black Market Reloaded ; Yasa dışı ateşli silah ve silah ticareti; hukukun üstünlüğünü, polis operasyonlarını ve sivil halkın güvenliğini tehdit eden, şiddeti ve terörizmi körükleyen küresel bir sorundur. Black Market Reloaded, (takma adıyla CherryFlavour) Dark Web üzerinden Bitcoin ile ABD'den Avustralya'ya elektronik cihazların içine gizlenmiş ateşli silahların posta yoluyla satışını yapan bir pazardı. Avusturya dışında, Belçika, Kanada, Danimarka, Fransa, Almanya, İrlanda, Kazakistan, Hollanda dahil olmak üzere yüksek fiyatlarla 70'in üzerinde yasadışı bir şekilde ateşli silah gönderen suçlular, 500 dolara satılan bir tabancayı, Dark Web üzerinden 3.400 dolara satarak kar elde etmekteydi (U.S. Attorney's Office, 2018).

BidenCash; Dark Web'de yer alan ve çalınan kredi ve banka kartı bilgilerinin paylaşıldığı BidenCash adı verilen pazar yeri, 2022 yılında 1,2 milyon kredi kartı bilgilerini internette yayınlarak satışa çıkartmıştır. Bilgileri sızdırılan kartların çoğunun kullanım süresi 2023-2026 yılları arasında ve önemli bir bölümü ABD'de yaşayan vatandaşlara aittir. Bu sızıntıdan etkilendiği kesinleşen diğer ülkeler arasında Kanada, Hindistan, Brezilya, İspanya, Bangladeş, Suudi Arabistan, Birleşik Arap Emirlikle, Malezya, İran dahil olmak üzere dünyanın dört bir yanındaki tüketiciler yer almaktadır (Cyble Research , 2022).

Devlet Dışı Aktörlerin Siber Tehditleri: Terör faaliyetleri, teknolojinin gelişimi ile evrimleşmiş ve internet alanında yoğunlaşmasına zemin hazırlamış, terörist gruplar siber uzayda giderek daha fazla yer almaya başlamıştır. Teröristler, 1990'ların sonlarından beri yüzey ağındaki çeşitli çevrimiçi platformlarda faaliyet göstermeye başlamıştır. Ancak yüzey ağındaki terör içerikli web siteleri ve sosyal medyanın çoğu, terörle mücadele kurumları tarafından izlenmekte ve kapatılmaktadır. Yüzey ağı anonimlik arayan teröristler için izlenebilir, takip edilebilir ve bulunabilir olduğu için teröristleri yeni çevrimiçi platformlar aramaya zorlamıştır (Weimann, tarih yok). Buna karşılık Dark Web, teröristler için anonim olarak eylemlerini meşrulaştıracak, ideolojilerini paylaşabilecekleri, kripto para birimiyle fon toplayabilecekleri, yeni üye

kazanabilecekleri, silah alışverişi yapabilecekleri ve saldırılarını planlayabilecekleri bir platform görevi görmüştür.

Terörist saldırıların gizli bir ağda koordine edildiği uzun süredir bilinmektedir. Özellikle IŞİD'in interneti ve Dark Web'i etkin bir şekilde kullanması daha fazla terörist grubun Dark Web'e yönelmesini sağlamıştır (Sönmez & Çelik, 2020, s. 79). 2015 yılında Paris Operasyonu'nda IŞİD'in birçok internet sitesinin kapatılmasının ardından, Dark Web'e geçiş için gerekli bilgiler Al-Hayat Medya Merkezi'nde (IŞİD medyası) yayınlanmış ve IŞİD faaliyetlerini Dark Web üzerinden devam ettireceğini resmen ilan etmiştir. Ayrıca IŞİD üyeleri, bağlantı kurmanın yanı sıra, sınır kontrollerinde yasal düzenlemelerin artmasıyla birlikte, sahte kimlik ve pasaportlar elde etmek için Dark Web pazar yerlerini de kullanmaktadır (Sönmez & Codal, 2022, s. 5).

Terör örgüleri, kimyasal, biyolojik, radyolojik ve nükleer silahlar için yeterli kaynaklara ve teçhizata erişim için de malzemeleri ve silah üretim konusunda bilgili kişileri işe almak için Dark Web'i kullanmaktadırlar. 2016 Münih saldırısı ve 2015 Paris terör saldırılarının Dark Web üzerinde planlandığı ve silahların bu platform üzerinden satın alındığına dair görüşler ortaya atılmıştır (Paoli, 2018, s. ix).

Teröristler, Dark Web'i bitcoin ve diğer kripto para birimleri gibi sanal para birimlerini kullanarak para toplamak, gizli para transferi yapmak ve yasa dışı silah almak amacıyla da kullanmaktadır. 2014 yılında "Bitcoin ve Cihad Hayır Kurumu" anlamına gelen "Bitcoin wa Sadaqat al-Jihad" başlıklı çevrimiçi olarak yayınlanan makale, cihatçılar için finansal sistem üzerindeki kısıtlamaları atlamanın ve ekonomik desteği kolaylaştırmanın bir yolu olarak Bitcoin'i ve anonim bağış sisteminin nasıl kurulacağına dair açıklamaları içermektedir (Weimann, tarih yok).

Kötü Amaçlı Yazılımlar: Dark Web'in popüler kullanımlarından biri kötü amaçlı yazılımlarla ilgilidir. Kötü amaçlı yazılımların ve güvenlik açıklarının Dark Web üzerinden çevrimiçi satışı, siber güvenlik üzerinde etkili olmaktadır. Dark Web kötü amaçlı yazılımların açıkça ticaretinin¹² yapıldığı bir alan haline gelmiştir (Burgess, 2022).

¹² ayrıca bkzn. Dark Web Fiyat Endeksi 2022; <https://www.privacyaffairs.com/dark-web-price-index-2022/>

3.4.3.3 Şirketlere Yönelik Siber Tehditler

3.4.3.3.a. Microsoft'a Yönelik Siber Saldırıları

Microsoft tarafından üretilen haberleşme yazılımı Microsoft Exchange Server üzerinde Ocak 2021'de küresel siber saldırılar ve veri ihlalleri fark edilmiştir. Bilgisayar korsanları, hedeflenen kuruluşların e-posta sistemlerine erişim sağlayarak hassas verilere erişim sağlamıştır. ABD'de yaklaşık 30.000 kuruluşa, Birleşik Krallıkta 7.000 kuruluşa ait sunucuların yanı sıra Norveç Parlamentosu, Şili Komisyonu, Avrupa Bankacılık Otoritesi dahil toplam 250.000 sunucu saldırıdan etkilenmiştir (Duffy, 2021). Microsoft Tehdit İstihbarat Merkezi tarafından, Çin devleti destekli, çok yetenekli ve sofistike bir siber tehdit grubu olarak tanımlanan Hafnium grubu saldırıdan sorumlu tutulmuştur (Microsoft, 2021a). Temmuz 2021'de ise ABD, Birleşik Krallık, AB, NATO ve diğer Batılı ülkeler ortak bir bildiride, Microsoft Exchange ihlali ve diğer saldırıları gerçekleştirmekle Devlet Güvenlik Bakanlığı'nı (MsS) suçlamıştır (The White House, 2021b).

2022'de siber tehdit grubu olan Lapsus\$, Microsoft'a yönelik gerçekleştirdiği siber saldırıda, Microsoft projelerine ait kaynak kodlarını da içeren 37 GB'lık veriyi sızdırmayı başarmıştır. Sızdırılan dosyalarda Google'ın rakibi Bing arama, Bing haritalar, akıllı kişisel asistan olan ve Siri'nin rakibi olan Cortana gibi projelere ait kodlar yer almaktadır (Kalelioğlu, 2022).

3.4.3.3.b. Vodafone'a Yönelik Siber Saldırıları

Bilgi ve iletişim teknolojileri sektörü, büyük miktarda hassas veriyi iletmek ve depolamak için yaygın olarak kullanılan kritik altyapıyı oluşturdukları, kontrol ettikleri ve işlettikleri için siber saldırılar için büyük bir hedeftir. Özellikle devlet kurumları, gizli gözetim oluşturmak için telekom operatörlerinin altyapısına ve uygulamalarına giderek daha fazla odaklanmaktadır. Gizli gözetim için hedeflenen iletişim kanalları, telefon hatlarından cep telefonu verilerine kadar birçok şeyi içermektedir. Hatta bir ülkenin siber saldırısının başka bir ülkenin liderlerinin mobil cihazları üzerinden iletişim kurmasını engellediği durumlar bile yaşanmıştır (Deloitte, 2020).

2013'te Vodafone Almanya, iki milyondan fazla müşterisinin kişisel verilerinin çalındığı bir siber saldırıya uğramıştır. Müşterilerin adlarının, adreslerinin, banka

hesap numaralarının çalındığı saldırıda, bilgiler şirketin dahili ağında bulunan bir veri tabanından çalınmıştır. Saldırıyı gerçekleştiren siber tehdit aktörünün ise Vodafone içinde çalışan bir kişi olduğundan şüphelenilmiştir (BBC, 2013).

2022'de 4,7 milyon mobil müşterisine hizmet veren Vodafone Portekiz, hem 4G hem de 5G ağlarını etkileyen kötü niyetli bir siber saldırıya uğrayarak ani bir kesintiyle, veri ağlarına, televizyona, SMS ve diğer yanıtlayıcı hizmetlerine, Vodafone 4G ağına bağlı bazı büyük ATM'lerin ağı dahil birçok erişim engellenmiştir. Vodafone Portekiz CEO'su Mario Vaz, siber saldırıyı terörist ve suçlu bir saldırı olarak nitelendirmiştir. Eylemin ardından uzun bir süre sonunda erişimler yeniden sağlanmıştır (McMurtry, 2022).

3.4.3.3.c. T-Mobile'a Yönelik Siber Saldırıları

T-Mobile, Alman telekomünikasyon şirketi Deutsche Telekom bünyesinde faaliyet gösteren Çek Cumhuriyeti, Polonya, Hollanda ve ABD'de bulunan çok uluslu mobil iletişim şirkettir. Son birkaç yıla birden fazla veri ihlaline uğrayan T-Mobile'ın ABD'de faaliyet gösteren telekomünikasyon şirketi T-Mobile USA 2018 yılında, bir siber tehdit aktörünün müşteri isimleri, fatura bilgileri, telefon numaraları, e-posta adresleri, hesap numaraları gibi kişisel verileri sızdığını bildirmiştir. 2020 yılında da saldırganların müşteri ve çalışan verilerine erişim kazandığı iki ihlal daha açıklanmıştır (Gatlan, 2022). Telekomünikasyon şirketi 2021 yılında ise SIM kart saldırısına uğramıştır. SIM kart dolandırıcılığı, sosyal mühendislik kullanılarak hedeflenen telefon numaralarının kontrolünü ele geçirmelerine olanak tanır. Bu saldırıda siber tehdit aktörleri SMS tabanlı çok faktörlü kimlik doğrulamayı atlayarak kullanıcıların çevrimiçi hizmet hesaplarını ele geçirebilir ve kurbanların banka hesaplarına giriş yapabilir. T-Mobile'a yönelik bu saldırıda kullanıcıların kişisel bilgileri, kimlik numaraları dahil olmak üzere müşterilerin hesap bilgilerine erişim sağlandığı ortaya çıkmıştır (Gatlan, 2021). 2022 yılında T-Mobile, Lapsus\$ isimli siber tehdit aktörleri tarafından çalınan kimlik bilgilerinin kullanılarak dahili sistemlere erişim sağlandığını doğrulamıştır (Gatlan, 2022). 2023 yılında da şirketin Amerikan ağlarında "olağandışı etkinlik" fark edilmesi üzerine 37 milyon müşterinin kayıtlarını açığa çıkaran bir veri ihlali yaşamıştır (T-Mobile, 2023).

3.4.3.3.d. Sony Pictures Siber Saldırısı

Sony'nin yan e lence  irketi Sony Pictures, Kasım 2014 yılında fikri m lkiyet verilerini,  irket  alı anlarının ve  st d zey y neticilerinin ki isel verilerini i eren belgelerin  evrimi i olarak sızdırılmasını i eren bir siber saldırıya u ramı tır. Sony Pictures'a y nelik ger ekle tirilen siber saldırı ile ilgili haberler  ıktıktan kısa bir s re sonra saldırının, d nyanın en otoriter devletlerinden biri olan Kuzey Kore tarafından ger ekle tirildi ine dair yaygın iddialar ortaya  ıkmı tır.      saldırı, Sony'nin Kuzey Kore lideri Kim Jong-un'a y nelik kurgusal bir suikast giri imini konu alan The Interview isimli komedi filminin yakla an galasının bir sonucu olarak ger ekle tirilmi tir. Haziran 2014'te Kuzey Kore h k meti, d nemin eski BM Genel Sekreteri Ban Ki-Moon'a yazdı ı bir mektupta, The Interview filmini "*ter rizme destek vermenin yanı sıra bir sava  eylemi*" olarak tanımlayarak filmi kınamı  ve filmin ABD y netiminin deste iyle g sterime girmesi durumunda "*kesin ve acımasız kar ı  nlemler*" alınaca ını bildirmi tir (Beaumont-Thomas, 2014).

Kuzey Kore'nin BM'den destek g rememesi  zerine do rudan Sony'yi hedef alan siber saldırı s reci ba lamı tır. Kendilerine "Barı ın Koruyucuları (Guardians of Peace (GOP))" adını veren grup, Sony genel merkezindeki bilgisayar ekranlarına kafatası resmiyle birlikte taleplerine uyulması gerekti i, aksi takdirde  irketin  ok  nemli sırlarını if a edecekleri bir mesaj bırakmı tır (Sullivan, 2016, s. 439). Kademeli olarak artan saldırılarda  irketin bilgisayar sistemlerine sızılmı , ticari istihbarat,  zel bilgiler, ki isel e-posta adresleri, b t eler, banka havaleleri, stratejik i  planları, rekabet nedeniyle gizli tutulan  nemli bilgilerden yayınlanmamı  film materyallerine kadar  ok  e itli gizli bilgiler internete sızdırılmı tır (Sullivan, 2016, s. 445).  irkete ve  alı anlarına  ok b y k zararlar veren siber saldırıda daha fazla hasarı  nlemek i in Sony, dahili a ını kapatmı  ve filmi g sterimden kaldırmı tır. Kuzey Kore yetkilileri tarafından BM'ye yapılan a ıklamaların t m , Kuzey Kore'nin Sony saldırısının failleri olarak g sterirken FBI, bu saldırıdan Kuzey Kore h k metinin sorumlu oldu u sonucuna varmak i in yeterli bilgiye sahip oldu unu a ıklamı tır. Barack Obama ise yaptı ı a ıklamada Sony'nin filmin g sterime girmesini durdurmakla hata yaptı ını belirterek Kuzey Kore'ye orantılı olarak yanıt verilece ini a ıklamı  ve Sony saldırısını gerek e g stererek Kuzey Kore'ye yeni yaptırımlar uygulamak i in bir y r tme emri imzalanmı tır (Holm, 2017 , s. 27-28). T m tehditlere ra men 25 Aralık 2014'te film g sterime girmi tir.

Telekomünikasyon sektörünün siber uzayı hangi düzeyde etkilediği problemi çerçevesinde (P_{1c}), veri iletimi, cihazlar, ağlar arasında iletişimi sağlar ve çeşitli dijital hizmetler için altyapı sağlaması açısından siber uzayda derin bir etkisi mevcuttur. Bilgi ve iletişim teknolojisi, iş, eğitim, sağlık ve eğlence dahil olmak üzere hayatın çeşitli yönlerini dönüştürmüştür. Bilginin yayılma biçiminde devrim yaratmış, dünyanın farklı yerlerinden insanların gerçek zamanlı olarak iletişim kurmasına ve bilgi paylaşmasını sağlayarak küresel bağlantıyı kolaylaştırmış, işletmelerin çevrimiçi işlemler gerçekleştirmesine, daha geniş müşteri tabanına ulaşmasına ve küresel pazarda faaliyet göstermesine olanak tanıyarak e-ticaretin büyümesini kolaylaştırmış, yeni ekonomik fırsatlar ve endüstriler oluşmasına yol açmıştır. Sonuç olarak 5G gibi teknolojilerin ilerlemesini sağlamış, jeopolitik rekabeti etkilemiş, hammadde talebini artırmış, Metaverse vizyonunun gelişimini kolaylaştırmış, Toplum 5.0 vizyonunu desteklemiştir. Aynı zamanda siber uzayda çeşitli güvenlik zorluklarını da beraberinde getirmiştir. Çevrimiçi sosyal ağlar ve Dark Web'in varlığı, artan bağlantı ve dijital sistemlere bağımlılıkla birlikte siber tehditler, veri ihlalleri, bilgisayar korsanlığı ve kimlik hırsızlığı riskleri de artmıştır.

3.5. Enerji Sektörü

3.5.1. Endüstri 4.0'ın Enerji Sektörüne Entegrasyonu

Petrol endüstrisi, gaz endüstrisi, elektrik endüstrisi, kömür endüstrisi, nükleer enerji endüstrisi ve yenilebilir enerji endüstrisini içeren enerji sektörü; enerjinin üretilmesinden, arıtılmasından ve dağıtılmasından sorumlu bir sektördür. Bu endüstrilerin sınırlı işleyen birçok süreci, son yıllarda gelişen robot teknolojisi ve bilişim teknolojisi gibi sistemlerin sürece entegrasyonu sayesinde insan-makine etkileşimi artmış ve yaşanan dijital dönüşüm dünyaya enerji sağlama şeklinde devrim yaratacak çizgiye ulaşmaya başlamıştır.

Enerji sektöründeki sanayi devrimi, üç ana faktörün baskısı altındadır; (I) Geleneksel olan enerji kaynaklarının tükenmesi (kömür, petrol, gaz); (II) enerji piyasasındaki hızlı değişimler; (III) dijitalleşme ve yeni teknolojik gelişme olanaklarının ortaya çıkması. Endüstri 1.0 kömür ve buhar gücüne dayanmaktaydı, elektrik ve petrol ise Endüstri 2.0'ın merkezinde yer almaktaydı, Endüstri 3.0 ise aktif

gaz geliştirme ve otomasyon ile ilişkilidir (Goosen, Nikitenko, Kagan, & Pakhomova, 2020, s. 2). Endüstriyel süreçlerde dijital teknolojilerin kullanılmasını içeren Endüstri 4.0'a geçiş, enerji sektöründe; enerjinin üretilme, dağıtılma ve tüketim sistemini dönüştürmek için akıllı makinelerden ve yeni teknolojilerden yararlanmak anlamına gelmekte ve otomasyon sistemleri, sensörler ve internet bağlantısı, yapay zeka, bulut bilişim gibi dijital teknolojilerle entegre edilerek enerji sektöründe verimliliği artırmak için büyük bir potansiyel oluşturmaktadır.

Örneğin *büyük veri*, karbon ayak izinin azaltılması ve üretim performansını tahmin etmek için kullanılmaktadır; *endüstriyel nesnelerin interneti*, bir petrol kuyusundan veri toplamak, büyük veri ve yapay zeka ile birleştirerek anında çözüm sağlamak için kullanılmaktadır; *robotik*, sızıntıların erken tespiti sağlamak, su altı kaynağı, açık deniz kuleleri ve boru hatları gibi erişilmesi zor konumlardaki varlıkların denetlenmesini desteklemektedir; *yapay zeka*, bilgi ayıklamada ve kapsamlı resimler oluşturmak için ilgili verileri bulmada kullanılmaktadır; *AR/VR teknolojisi* ise karmaşık görevleri test edecek şekilde kullanılmaktadır (Japan Aramco, tarih yok). Bu teknolojiler, enerji tüketim verilerinin toplanması ve analizini, enerji verimliliğinin artırılmasını, büyük projelerde harcanan sürenin ve ilk petrolün çıkarılmasına kadar geçen sürenin azaltılmasını, üretim ve lojistikte insan faktörünün azaltılmasını, karbon ayak izinin azaltılmasını, tahmine dayalı sorun gidermeyi, maliyetin düşürülmesi ve daha sürdürülebilir bir enerji sistemi oluşturulabilmesi gibi konularda fayda sağlamaktadır.

Şirketleri, ulus devletleri ve uluslararası politikayı etkileyen enerji fiyatlarındaki değişimler ve artan enerji ihtiyacı gözlemlendiğinde, enerji sektöründeki farklı dijital teknolojilerin ve stratejilerin geliştirilmesi, artan enerji ihtiyacını karşılayabilir, temiz, sürdürülebilir ve yenilenebilir teknolojilere dönüşümü destekleyebilir. Dünya Ekonomik Forumu'na göre, petrol ve gaz endüstrisinin dijitalleşmesi tek başına 2026 yılına kadar 1,6 trilyon dolarlık ek gelir sağlayabilir (World Economic Forum [WEF], 2017 , s. 5).

Endüstri 4.0 ile enerji sektöründe, robotik veya uzaktan kumandalı ekipmanlar, uzaktan merkezi kontrol odaları, sondaj kuleleri ve ekskavatörlerin (kazmaç) yüksek hassasiyette konumlandırılması, personel sağlık durumunu izlemek için taşınabilir cihazlar, üç boyutlu modellerin tasarlanabilmesi, jeolojik verileri ve üretim süreciyle

ilgili her şeyi analiz etmek için tahmine dayalı yöntemler ortaya çıkmıştır (Goosen vd., 2020 , s. 7).

3.5.2 Enerji Sektöründe Uluslararası Rekabet Gücü ve Etkileri

Günümüzde enerji endüstrisi, siber uzayın giderek artan bir şekilde hayatımıza girmesiyle büyük bir dönüşüm geçirmektedir. Bu dönüşüm, enerji şirketlerinin dijital girişimleri, bazı politik süreçler, uluslararası krizler ve iklim değişikliği gibi faktörlerin birleşmesiyle şekillenmektedir. Enerji endüstrisinin siber uzaydaki etkisi, uluslararası politikaları da etkilemektedir. Siber uzayda gerçekleştirilen ve ulus devletlerin kritik altyapı statüsündeki enerji sektörüne yönelik siber saldırılar, ülkeler arasındaki gerilimlere ve çatışmalara neden olabilmektedir.

Çalışmada, enerji sektöründeki dijitalleşme trendleri "petrol ve gaz endüstrisi" ve "elektrik enerjisi endüstrisi" üzerinden ele alınmıştır. Özellikle bu iki endüstri içerisinde dijitalleşen ve öncü konumda olan şirketler ve ülkeler detaylı bir şekilde incelenmiştir.

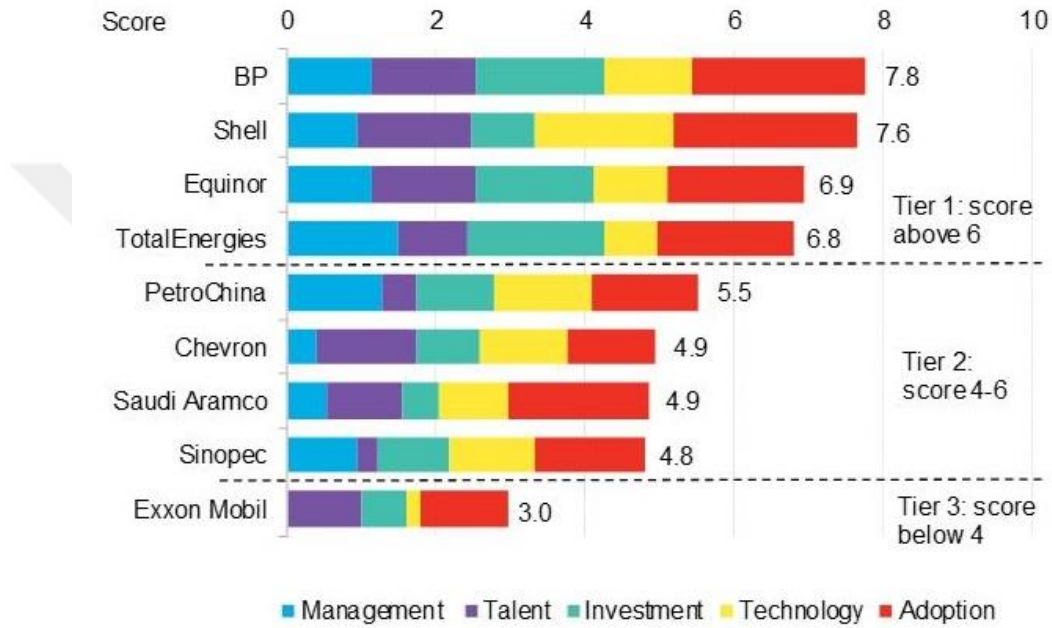
3.5.2.1. Petrol ve Gaz Endüstrisinde Dijitalleşme

Petrol ve gaz sektörü son derece politik bir alandır ve tarih boyunca uluslararası ilişkilerin merkezinde yer almış bir sektördür. Petrol ve gaz, endüstrinin vazgeçilmez bir parçasıdır ve küresel ekonomik büyüme için temel enerji kaynaklarıdır. Diğer sektörlerin yüksek teknoloji ürünlerini verimli kullanması ve dijitalleşmesi, petrol ve gaz endüstrisinin de dijitalleşmenin getirdiği fırsatlardan ve dönüştürücü etkisinden yararlanmasının yolunu açmıştır. Dolayısıyla petrol ve gaz şirketlerinin faaliyet gösterdiği ortamı yeniden şekillendiren büyük toplumsal, teknolojik ve politik eğilimlerin olduğu bir dönemdeyiz. Petrol ve gaz endüstrisindeki dijital dönüşüm, operasyonları kolaylaştırarak üretkenliğin ve karlılığın artmasını sağlayabilir, çalışan güvenliğini artırabilir, çevre kirliliğinin önüne geçebilir ve müşterilerin paradan tasarruf etmesini sağlayarak topluma yardımcı olabilir.

İngiltere merkezli veri analitiği ve danışmanlık şirketi Global Data, "*Petrol ve Gazda Dijitalleşme*" adlı tematik araştırmasında, sektördeki önde gelen ve dijital olarak gelişmiş petrol ve gaz şirketlerini belirlemiştir. Şirketler arasında Birleşik Arap

Emirlikleri merkezli ADNOC (Abu Dhabi National Oil Company), İngiltere merkezli BP (British Petroleum), İtalya merkezli Eni, ABD merkezli Chevron ve ExxonMobil, Norveç merkezli Equinor, İspanya merkezli Repsol, İngiltere - Hollanda ortaklığındaki Royal Dutch Shell, Çin merkezli Sinopec, Suudi Arabistan merkezli Saudi Aramco, Fransa merkezli TotalEnergies yer almaktadır (Global Data, 2022).

Şekil 21: Piyasa değeri ile en büyük petrol şirketlerinde dijital inovasyon skoru 2021



Source: BloombergNEF

Kaynak: <https://about.newenergyfinance.com/blog/will-digital-technologies-become-the-next-competitive-edge-of-oil-majors/>

Petrol ve gazda dijitalleşme, diğer sektörlerde olduğu gibi yapay zeka, bulut bilişim, büyük veri, siber güvenlik, nesnelerin interneti ve robotik gibi dijital teknolojilerin benimsenmesini içermektedir. Araştırmaya göre 2020'de petrol ve gaz sektörü için en büyük üç dijitalleşme önceliği bulut tabanlı uygulamalar (%47), veri platformları (%44) ve yapay zeka (%27) olarak sıralanmıştır (DNV GL, 2020, s. 28). Petrol ve gaz endüstrisinde yapay zeka saha keşiflerini iyileştirmek için kullanılmaktadır. Saudi Aramco, potansiyel keşif sahalarının özelliklerini analiz etmek ve belirlemek için tahmine dayalı yazılım araçları sağlayan Earth Science Analytics'e yatırım yapmıştır. 2019'da Fransız TotalEnergies, saha keşfini kolaylaştırmak için yapay zeka kullanan bir dijital fabrika açma planlarını duyurmuştur. Petrol ve gaz endüstrisindeki mevcut teknolojinin diğer bir örneği, Fransız petrol devine ait

TotalEnergies'in süper bilgisayarı Pangea'dır. Pangea, saniyede beş katrilyondan fazla hesaplama hızıyla dünyanın en güçlü 19. süper bilgisayarı olarak gösterilmektedir (Evans, 2022). Sonuç olarak günümüzde şirketler için veriler ve yapay zeka petrol kadar kritik ve önemli hale gelmiştir.

2018'deki Abu Dabi Uluslararası Petrol Fuarı ve Konferansı'nda (ADIPEC), ADNOC Group CEO'su, Dr. Sultan Ahmed Al Jaber ilk kez "Petrol ve Gaz 4.0" planını sunmuştur. Petrol ve Gaz 4.0'da temel amaç, sektörde daha yüksek değer elde etmek için gelişmiş dijital teknolojiyi kullanmaktır (Emirates News Agency [WAM], 2015).

3.5.2.1.a. Petrol ve Gaz Şirketlerinin Teknoloji Endüstrisi ile İşbirliği ve Girişimleri

2014 yılında yaşanan petrol fiyatlarındaki düşüşün ardından, büyük petrol ve gaz şirketleri maliyetleri azaltmak ve operasyonları iyileştirmek için dijitalleşmeye artan bir ilgi göstermiştir. Enerji sektöründe rekabet gücü büyük ölçüde işbirliği yapma ve esnek piyasa koşullarına uyum sağlama yeteneği ile belirlenir. Büyük enerji şirketleri, yüksek teknoloji endüstrisindeki şirketlerle giderek daha fazla işbirliği yapmaktadır. Çalışmada dijitalleşmenin petrol ve gaz değer zinciri üzerindeki etkisini ve dijitalleşme temasındaki rekabetçi pozisyonlarına genel bir bakış sunmak için farklı menşeli şirketlerin dijitalleşme süreçlerine odaklanılmıştır. Bu kapsamda BP, Shell, Chevron, Saudi Aramco, Eni, Sinopec, TotalEnergies, Gazprom gibi sektörde öncü konumda bulunan şirketlerin dijital dönüşüm girişimlerine ve işbirliklerine yer verilmiştir.

ABD'de özel sektöre ait ve İngiltere'de borsada işlem gören BP, NASA'nın derin uzay araştırmaları için yapay zeka ve bilişsel hesaplamaya dayalı bir girişimi olan Kaliforniyalı şirket Beyond Limits'e 2017 yılında 20 milyon dolarlık yatırım yapmıştır. BP ve Beyond Limits ortaklığının kurulmasındaki temel amaç, BP'nin rezervleri bulma ve geliştirme, ham petrol üretme ve rafine etme, rafine edilmiş ürünleri pazarlama ve tedarik etme faaliyetlerinde yapay zeka yazılımı ile iyileştirmelerin sağlanmasıdır (BP, 2017).

Şekil 22: BP'nin Meksika Körfezi'nde işlettiği platformlar (Argos, Atlantis, Mad Dog, Na Kika, Thunder Horse)



Kaynak: https://www.bp.com/en_us/united-states/home/where-we-operate/gulf-of-mexico/our-platforms.html

2019 yılında jeofizikçi Xukia Shen tarafından oluşturulan ve Meksika Körfezi'nde kullanılan yazılım, BP'nin uzun süre bulunamayacağını düşündüğü bir bölgede ham petrol keşfetmesinin yolunu açmıştır. Ham petrol, süper bilgisayar ile çalışan ve deniz yatağının binlerce metre altındaki kaya katmanlarının yüksek çözünürlüklü 3D görüntülerini üretmek için sismik ses dalgalarının yansımalarını analiz eden Full Waveform Inversion olarak bilinen bir yazılımla bulunmuştur. Aynı yıl içinde BP, Wolfspar adlı yeni sistemik cihazının Thunder Horse sahasında 1 milyar varilden fazla petrolün keşfedilmesini sağladığı bildirilmiştir. Bu teknolojiler ile sahaların yerini belirleyerek ve doğru kuyuların açılmasını sağlayarak keşif saatlerindeki azalmayla yüz milyonlarca dolar tasarruf sağlanabilmektedir (Bousso, 2019).

Amerikan enerji şirketi Chevron'un petrol sahalarındaki dijitalleşme adımlarından en önemlisi, 2017 yılında Microsoft ile yedi yıllık bir ortaklık yaparak Microsoft Azure'un güçlü bulut bilgi işlem ve analitiğinden yararlanmayı hedeflemesidir. Azure, Chevron'un ticari zorluklarını çözen ürünler geliştirmesine, ürettiği verilerle performansını iyileştirmeye yardımcı olmasına ve petrol sahalarının dijitalleşmesine katkı sağlamaktadır (Microsoft, 2017). Günümüzde petrol ve gaz şirketleri, daha verimli ve üretken olmalarına yardımcı olan veri analitiğinin ve büyük verilerin değerini anlamaktadır. Dolayısıyla bu girişimlerle şirketler, kuyulara gömülü sensörler veya makineden makineye aktarılan verilerle çok çeşitli kaynaklardan veri toplayabilir ve rekabet avantajı elde etmek için verilerin analizleriyle faaliyetlerini daha verimli hale getirebilir. Ayrıca sondaj için en uygun yerlerin belirlenmesi

amacıyla Chevron, sismik verileri görselleştirmek ve üç boyutlu saha modelleri oluşturmak için aktif olarak grafik işlemciler geliştirmektedir (Goosen vd., 2020, s. 4).

Dijitalleşmenin bir sonucu olarak petrol keşfi sırasında toplanan veri miktarı büyük ölçüde artmıştır. Çeşitli kaynaklardan toplanan verilerin, analiz edilerek anlamlı bir hale dönüştürülme amacını taşıyan büyük veri, petrol ve gaz şirketleri tarafından kullanılarak stratejik adımlar atmasını sağlamaktadır. Royal Dutch Shell'de bu konuda HP (Helwett-Packard) ile özel bir ortaklıkla oluşturulan fiber optik kabloları kullanarak verilerini, Amazon Web Services tarafından sağlanan özel sunuculara aktarmaktadır. Böylece bir petrol sahasından elde edilen veriler, jeologlara nerede sondaj yapılacağı konusunda daha doğru önerilerde bulunmasını sağlamak için dünyanın dört bir yanındaki binlerce petrol sahasından alınan verilerle karşılaştırılabilir hale gelmektedir (Marr, 2015). Büyük veri sayesinde Shell, 2015 yılında Nijerya'nın en zorlu arazilerindeki bazı petrol sahalarını izlemek için dijital teknolojiye yaptığı 87.000 dolarlık yatırımdan toplam 1 milyon dolarlık bir gelir elde etmiştir (DeGrasse, 2016).

Shell, akıllı sensörler ve internet bağlantılı cihazlar aracılığıyla petrol sahalarında veri toplamaktadır. 2018'de dijital dönüşüm stratejisi çerçevesinde kurumsal bir yapay zeka yazılım sağlayıcısı C3 AI ile kurduğu ortaklıkla, yapay zekayı kullanarak petrol ve gaz rezervlerini keşfetmek için veri analizi yapmaktadır (C3.AI, 2018). Bu veriler, C3 AI üzerinde işlenerek ve yapay zeka algoritmaları kullanılarak analiz edilmektedir. Sonucunda ise Shell'in faaliyetlerinin verimliliğini artırması ve yeni üretim fırsatlarını keşfetmesi amaçlanmaktadır.

Saudi Aramco Dijital Dönüşüm Programı çerçevesinde çeşitli inovasyon merkezleri kurmuştur. Bunlardan en önemlisi 2019 yılında dijital dönüşüm vizyonunu gerçekleştirmek amacıyla kurulan 4IR Merkezi isimli bir yapay zeka merkezidir. En son teknolojiyi keşfetmeye adanmış 2.500 metrekare alana sahip merkez, gelişmiş analitik ve makine öğrenimi çözümlerini geliştirmeye odaklanan büyük bir dikey ekranla çevrilidir. Tesis enerji endüstrisinde, artırılmış gerçeklik ve dronlar gibi yeni nesil teknolojilerin uygulanmasını sağlayan son teknoloji ile tasarlanmıştır. Oluşturulan insansız hava araçları alanı; alevlenme noktalarının incelemesini ve metan gazı tespitini destekleyen hava, toprak ve su altı dronlarının operasyonel kullanımlarını göstermektedir. Bu doğrultuda iş yeri güvenliğini ve yakıt verimliliğini artırma, ham

petrolün kalite çözümünü sağlama, emisyonları ve üretim maliyetini azaltma gibi biz dizi stratejik hedefler belirlenmiştir (Aramco, tarih yok).

Şekil 23: 4IR Merkezi



Kaynak: <https://spfconsoles.com/aramco-chooses-spf/>

Saudi Aramco'nun "Uthmaniyah Gaz Fabrikası" Dünya Ekonomik Forumu tarafından Endüstri 4.0 teknoloji uygulamalarında lider olan bir "Deniz Feneri" üretim tesisi olarak kabul edilmiştir. Uthmaniyah Gaz Fabrikası, dünyanın en büyük gaz işletme tesislerinden biridir ve işletme tesislerinin güvenliğini, verimliliğini ve üretkenliğini artırmak için gelişmiş analitik ve yapay zeka çözümleri kullanılmaktadır. Video görüntülerini yakalayan dijital kasklar ve bilgileri doğrudan merceğe yükleyen gözlükler gibi boru hatlarını ve makineleri incelemek için dronlar ve giyilebilir teknolojilerin kullanılması, fabrikada denetim süresinin %90 oranında kısaltılmasına yardımcı olmuştur (Japan Aramco, tarih yok).

2023 yılında Aramco, şirketin dijital dönüşümünü hızlandırmak için toplam değeri 7,2 milyar dolar olan 100'den fazla anlaşma imzalayarak ortaklıklar kurmuştur. Özellikle dijital ve teknolojik danışmanlık hizmeti sunan Accenture ile olan stratejik dijital ortaklığı, Aramco'nun dijital yetenekler geliştirmesinde kilit rol oynayacağı belirtilmektedir (Ozsevim, 2023).

2020'de Pavia eyaletindeki Ferrera Erbognone'deki Green Data Center isimli dijital teknoloji merkezinde kullanıma sunulan ve saniyede 52 trilyon matematiksel işlem gerçekleştirebilen Eni'nin HPC5 süper bilgisayarı, dünyanın en güçlü süper bilgisayarlarından biridir. HPC5, tüm üretim varlıklarının işletilmesi sırasında ürettiği

büyük verinin kullanılmasına olanak sağlamakla birlikte, enerji kaynaklarına ilişkin süreçleri iyileştirmekte, denizden enerji geliştirmeyi ve manyetik araştırmaları destekleyerek maksimum düzeyde enerji verimliliği elde etmeyi sağlamaktadır (Eni, tarih yok).

Sinopec, diğer şirketler gibi gelişen bilgi teknolojisinden daha iyi yararlanmak, arz, talep ve emisyon gibi faktörleri daha iyi takip etmek için bulut bilgi işlem ve büyük veriden yararlanma gerekliliği çerçevesinde, 2015 yılında Çin menşeli e-ticaret şirketi Alibaba'nın bulut bilişim işletmesi Aliyun (Alibaba Cloud) ile bulut bilişim hizmetleri ve büyük veri analizi sağlamak için bir anlaşma imzalamıştır (Reuters, 2015a).

2002 yılında Sinopec ve Hong Kong merkezli BİT şirketi Pacific Century Cyberworks Limited ile ortak bir girişimle Petro-Cyberworks Information Technology Company Limited (PCITC) adıyla bilgi ve iletişim teknolojilerini temel alan bir kuruluş oluşturulmuştur (Petro-CyberWorks Information Technology Company [PCITC], tarih yok). Sinopec'in akıllı fabrika girişimlerinde ise PCITC ve Huawei ortaklaşa bir işbirliği gerçekleştirmiş ve Smart Factory 2.0'ın temel parçası olan akıllı üretim platformunu ortaklaşa duyurmuştur. Platformun sekiz ana yeteneği mevcuttur; **Merkezi entegrasyon** (akıllı fabrika verilerini ve bilgilerini birleştirir, verilerin kontrolünü ve sistemlerle entegrasyonunu sağlar), **nesnelerin interneti erişimi** (dijital depo, tehlikeli kimyasalların takibi, korozyon ve çevre izleme hizmetlerini sağlar), **BT yönetimi ve kontrolü** (bulut bilişim yönetimi, işletme ve bakım yönetimini sağlar), **optimizasyon** (en iyi tasarım belirleme süreciyle enerji verimliliğini artırmayı, üretim sürecini ve cihaz işlemlerini kolaylaştırmayı sağlar), **paylaşılan hizmetler** (iş ve teknoloji hizmeti bileşenlerini merkezi olarak yönetir, kontrol eder ve bulut hizmetleri sağlar), **veri işleme ve analiz** (üretim analizi, ekipman hatası teşhisi ve ürün kalitesi analizi sağlar), **yapay zeka** (verilerle petrokimya tesisleri için akıllı beyin oluşturmayı sağlar) (Huawei , 2017).

Temmuz 2021'de Sinopec'in ilk dijital petrol ve gaz toplama, taşıma kombine istasyonu olan Shunbei Oilfield Kombine İstasyonunu faaliyete geçirmiştir. İstasyon ham petrol arıtma, doğal gaz arıtma, üretilen su ve kükürt geri kazanımını entegre etmektedir. İstasyonun yıllık işleme kapasitesi bir milyon ton ham petrole ve 380 milyon metreküp doğal gaza ulaşmaktadır. Bir sonraki adımda ise şirket inşa edeceği

faz II projesi ile yıllık doğal gaz işleme kapasitesini 1 milyar metreküpe ulaştırmayı hedeflemektedir (Sinopec, 2021, s. 36).

Total'in yıllık bilgi ve iletişim teknolojilerine harcamasının 2021'de 2,0 milyar dolar olduğu tahmin edilmektedir. Bu harcamaların büyük bir kısmı yazılım, donanım ve BİT hizmetleri almak için kullanılmıştır (Global Data, 2022a).

Total, çeşitli stratejik teknoloji ortaklıkları da önem vermektedir. Örneğin Kasım 2019'da Total ve ADNOC, genel operasyonel verimliliği artırmak, harcamaları azaltmak ve insan müdahalesi olmadan sismik haritalama yapmak amacıyla insansız hava araçlarını ve otonom kara aracını kullanan bir pilot proje başlatmak için bir araya gelmiştir (Global Data, 2022a). Aynı zamanda Mart 2021'de Total ve Microsoft, dijital dönüşümü ilerletmek ve net sıfır emisyonu sağlamak için işbirliği yapmıştır. Microsoft, sürdürülebilirlik hedeflerinin bir parçası olarak 2030 yılına kadar dizel yakıta bağımlılığı ortadan kaldırmayı hedeflemektedir (Total Energies, 2021). Bu hedefi de hem enerji sektöründeki şirketlerin bilgi ve iletişim sektörü ile işbirliğinin gelişmesine katkı sağlamak hem de enerji sektöründeki şirketlerin Microsoft'un yenilikçi girişimlerini kullanmasına olanak tanımaktadır.

Total, 2020'de Paris'te, şirketin dijital dönüşümünü hızlandırmak için birçok veri bilimci ve diğer uzmanları bir araya getirdiği bir Dijital Fabrika (Total Digital Factory) kurmuştur. Dijital Fabrika, Total'in operasyonlarını hem kullanılabilirlik hem de maliyet açısından iyileştirmek için ihtiyaç duyduğu dijital çözümleri geliştirmekle görevlendirilmiştir (Total Energies, 2019).

Dünyadaki diğer ülkelerle karşılaştırıldığında Rusya, doğal gaz ve sıvılaştırılmış doğal gaz üretiminin dijitalleştirilmesine yönelik iş süreçlerinde, proje sayısı, kalitesi açısından ve projelerin gecikmeli uygulaması sebebiyle rakiplerinin gerisinde kalmıştır. Uzmanlara göre, Gazprom'un bir yan kuruluşu olan ve Rusya'nın üçüncü büyük petrol üreticisi olan Gazprom Neft ve onu takiben Rosneft, Rus petrol ve gaz üretiminin dijitalleştirilmesi alanında en başarılı kabul edilen gelişmelere ev sahipliği yapmaktadır (Samylovskaya, Makhovikov, Lutonin, Medvedev, & Kudryavtseva, 2022). Rusya'da Gazprom Neft gibi şirketlerin başarılı dijitalleşme projeleri gerçekleştirmesi, Rusya'nın dijitalleştirme alanında gelecekte daha fazla gelişme göstermesine de yardımcı olabilir.

Gazprom Neft, 2007 yılında kurduğu Bilişim ve Teknik Merkez'i ile birçok proje geliştirmiştir. 2019 yılında 150'den fazla dijital girişim başlatan Gazprom Neft, özellikle Dijital Gaz Projesi ile şirketin gaz alanlarında yapay zeka kullanarak gizli petrol oluşumlarını hesaplamalarına yardımcı olmuştur. Gizli petrol oluşumlarını tespit edebilecek ve bu oluşumların verimli bir şekilde yapılmasını sağlayabilecek proje, Vyngapurovskoye sahasında ek petrol akışı sağlamış ve makine öğrenimi algoritmasını uygulayarak ilk dijital petrolünü üretmiştir. Ayrıca şirket 2025 yılına kadar dijital dönüşümün jeolojik keşif süresini ve maliyetini %30 oranında azaltmayı hedeflemektedir (AK&M, 2020). Yine Ocak 2022'de Gazprom Neft, Moskova'dan 1.500 km uzaklıktaki Orenburg bölgesinde yer alan Yagodnoye sahasındaki kuyuları denetleyerek, artırılmış gerçeklik teknolojilerinin Rusya'daki ilk kullanımına ilişkin pilot testini başarıyla tamamladığını duyurmuştur (Szymczak, 2022).

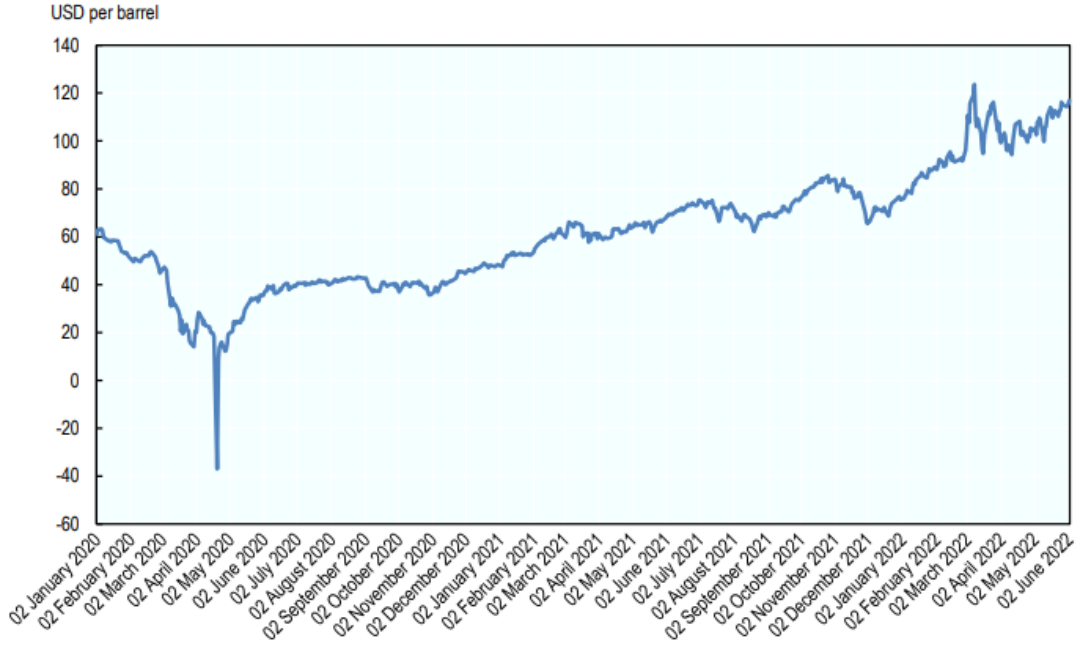
2019 yılında Abu Dabi Ulusal Petrol Şirketi (ADNOC) ve BAE merkezli bulut bilişim şirketi Group 42, özellikle petrol ve gaz endüstrisi için gelişmiş programlama çözümlerini ticarileştirmek için AIQ ortak girişimini kurmuştur. Aynı yıl Gazprom Neft ve ADNOC stratejik işbirliği anlaşması imzalamış ve ortak girişime katılmıştır. Bu girişim ile şirketler, Rusya ve Orta Doğu'da petrol ve gaz endüstrisi için ortaklaşa geliştirilen dijital çözümleri geliştirmeyi ve ticarileştirmeyi hedeflemektedir. Hedefler doğrultusunda şirketler, robotik, makine öğrenimi ve yapay zeka kullanarak petrol ve gaz arama, üretme için araçlar geliştirme taahhüdünde bulunmuştur. Özellikle Gazprom Neft, Orta Doğu'daki kendi dijital optimizasyon çözümlerini tanıtmayı planlamaktadır (Szymczak, 2022).

Tüm dijitalleşmeye yönelik girişimler ve teknoloji şirketleri ile yapılan işbirliği girişimleri, enerji sektöründeki dijital dönüşümü ve rekabeti sağlamakla birlikte, sektörler arasındaki engellerin ve tedarikçiler, üreticiler, tüketiciler arasındaki sınırları kaldırarak daha şeffaf ve verimli bir işbirliği sağlamaktadır.

3.5.2.1.b. Covid-19'un Petrol ve Gaz Endüstrisine Etkisi

2020 ve 2021'de enerji fiyatları, dünya çapında sokağa çıkma kısıtlamaları nedeniyle 2020'de yaşanan önemli ekonomik zorluk ve ardından kısıtlamaların kaldırıldığı 2021'deki ekonomik toparlanmanın etkisiyle değişkenlik göstermiştir.

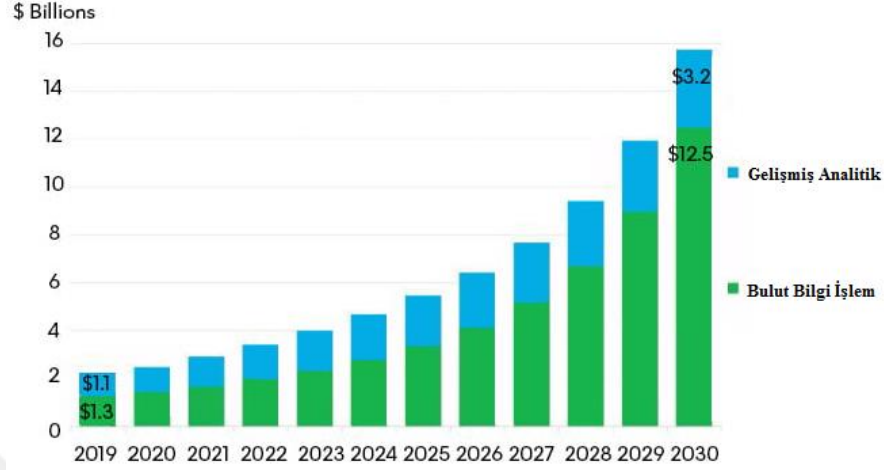
Şekil 24: Ham petrol ürünleri için spot fiyatlar (2020-2022)



Kaynak: <https://www.oecd.org/daf/competition/competition-in-energy-markets-2022.pdf>

Covid-19 salgınının başlangıcında yaşanan ekonomik gerileme, petrol ve gaz talebinin düşmesine neden olarak bazı petrol sahaları ve rafinelerde üretimin durmasına sebebiyet vermiştir. Covid-19 salgınının ilk dalgası sırasında, büyük borsalarda bir varil petrol fiyatı 25 doların altında düşüş göstermiştir. 2022 yılında ise artan talep, jeopolitik olaylar ve tedarik kesintileri sebebiyle 100 doların üzerine çıkmıştır. Hem petrol hem de doğal gaz fiyatları salgın öncesi fiyat seviyelerini aşarken, Avrupa'da doğal gaz fiyatları tüm zamanların en yüksek seviyelerine ulaşarak rekor düzeyde elektrik fiyatlarını etkilemiştir. Doğal gaz fiyatlarındaki artış, elektrik üretiminde ve ısınmada doğal gaz yerine kullanılan ham petrol ve kömür gibi diğer enerji kaynaklarına olan talebin artmasına neden olmuştur. Örneğin, Avrupa'da kömür fiyatları iki kattan fazla artmıştır (OECD, 2022, s. 18).

Şekil 25: BloombergNEF raporuna göre petrol Endüstrisinin gelişmiş analitik ve bulut bilgi işlem harcamaları 2019'da 1,3 milyar dolardan 2030'da 12,5 milyar dolara katlanarak artacağı tahmin edilmektedir



Source: BloombergNEF, CAGR taken from various Gartner and IDC studies

Kaynak: <https://bnef.turtl.co/story/oilandgasdigitalization2020/page/2/1>

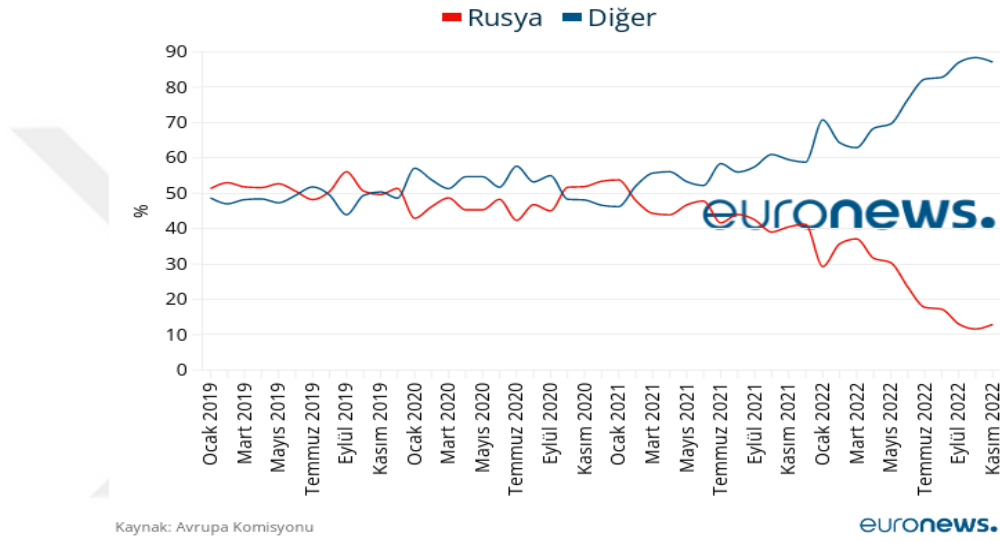
Olumsuz etkilerin yanı sıra, petrol ve gaz şirketleri, rekabetçi kalabilmek için maliyetlerini ve karbon emülsiyonlarını azaltırken, varlıklarının güvenilirliğini ve kullanılabilirliğini artırmak amacıyla operasyonlarını dönüştürmeye çalışmaktadır. Dolayısıyla petrol ve gaz endüstrisindeki dijitalleşme girişimleri üzerinde genel olarak olumlu bir etki yaratmıştır ve kurumsal bulut bilgi işlem, sanal ve artırılmış gerçeklik, dronlar ve blok zinciri tabanlı veri alışverişi dahil olmak üzere hızla olgunlaşan çok çeşitli teknolojilerin uygulanması için fırsatları görmeye başlamıştır (Hansman, Tan, Zhou, & Loh, 2022). Ayrıca Covid-19 sonrası dönemde enerji sektöründeki dijital dönüşüm, temiz bir enerji sisteminin ve yenilenebilir altyapı inşasını teşvik etmek içinde önemli süreçtir.

3.5.2.1.c. Rusya-Ukrayna Savaşının Petrol İhracatına Uluslararası Etkisi ve Norveç'in Artan Petrol İhracatı

24 Şubat 2022'de, aylarca süren gerginliğin ardından Rusya, kuzey, doğu ve güney Ukrayna'da hükümet kontrolündeki bölgelere tam kapsamlı bir işgal başlatmıştır. Covid-19 sonrası ekonomik toparlanmanın ardından gelen bu süreç 2022 yılında enerji piyasasında bir dalgalanmaya yol açmıştır. İşgal sonrasında Rus enerji sektörüne ve hükümetine finansman sağlanmasını yasaklayan kapsamlı bir dizi

yaptırımlar gerçekleştirilmiş, AB ülkeleri ve ABD Rus petrol ve doğalgaz ürünlerinin ithalatını yasaklamıştır (OECD, 2022). Özellikle AB üye ülkeleri Mart 2022'de Versay Deklarasyonu ile Rus fosil yakıtlarına bağımlılığını, mümkün olan en kısa sürede aşamalı olarak sona erdirmeyi taahhüt etmiştir. Rusya'nın Ukrayna'yı işgalinden bir ay önce, Ocak 2022'de AB'ni ithal ettiği doğal gazın %41'i Rusya'dan karşılanmaktaydı. Ancak bu oran Ekim 2022'de %12'ye kadar düşmüştür (European Council, 2022).

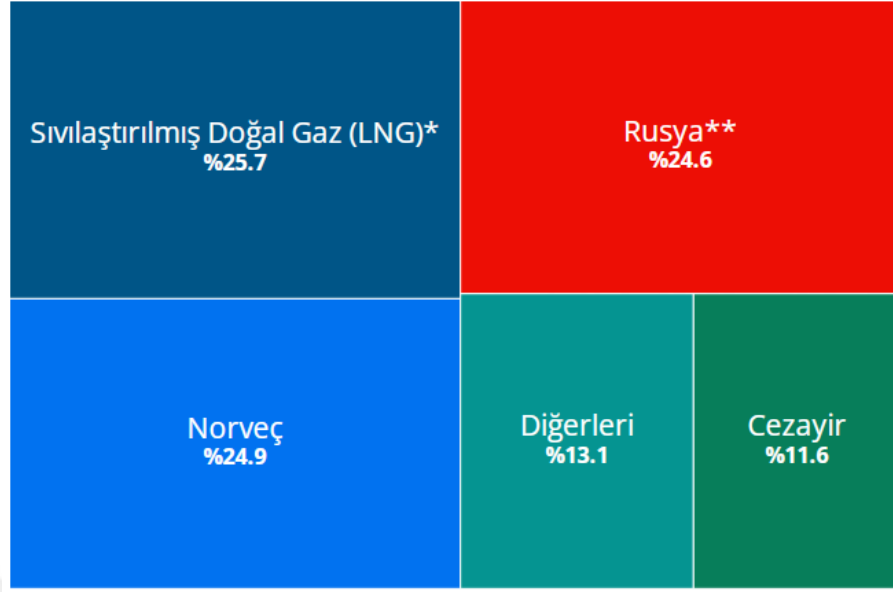
Şekil 26: AB'nin doğalgaz ithalatı Rusya ve diğer, Ocak 2019 - Kasım 2022



Kaynak: <https://tr.euronews.com/2023/02/24/ukrayna-igalinin-yil-donumu-abnin-rusyadan-enerji-ithalati-nasil-degisti>

Rusya ve Ukrayna arasındaki jeopolitik çekişme nedeniyle enerji ithal eden ülkelerin tercihlerinin değişmesi nedeniyle sıvılaştırılmış doğal gaz sektörünün önümüzdeki on yılda önemli bir büyüme kaydetmesi beklenmekte. AB'nin sıvılaştırılmış doğalgaz ithalatında işgal öncesi %50 civarındayken Ocak-Kasım 2022'de bu oran %24,6 oranına gerilemiş ve Norveç'in payı %24,9'a yükselmiştir. Asıl artış ise ABD'den ithal edilen sıvılaştırılmış doğal gazda olmuştur. ABD'den ithal edilen sıvılaştırılmış doğal gaz miktarı 2021 yılına göre Ocak-Kasım 2022 döneminde iki katını aşmıştır. Rusya'dan gelen doğal gaz azalırken ABD ve Norveç'ten ithalatın artmasıyla bu durum telafi edilmiştir (Euronews, 2023). 2022 yılı boyunca Avrupa'da ve özellikle Almanya'da enerji maliyetleri artmış olsa da 2023 ve 2024 yıllarında sıvılaştırılmış doğal gaz ithalatı ile arzın korunacağı, güneş ve rüzgar teknolojilerinde yerli üretiminin artırılacağı belirtilmektedir.

Şekil 27: AB'nin doğal gaz ithalatı (Ocak-Kasım 2022)



Source: Avrupa Komisyonu *Ağırlıklı olarak ABD, Katar ve Nijeryadan; ** Boru hattı + LNG euronews.

Kaynak: <https://tr.euronews.com/2023/02/24/ukrayna-iskalinin-yil-donumu-abnin-rusyadan-enerji-ithalati-nasil-degisti>

Avrupa'nın Rus gaz tedarikinden, ABD, Katar ve diğer satıcılardan sıvılaştırılmış doğal gaz ithalatına geçmiştir. Ayrıca Çin ve Hindistan gibi hızlı büyüyen gelişmekte olan Asya pazarlarının enerji talebinin önümüzdeki on yılda büyük bir artış göstereceği beklenmektedir. Bu süreç içerisinde de dijitalleşme çabaları ve sıvılaştırılmış doğal gaz terminallerinin artırılması için çalışmalar yoğunlaşabilir (Global Data , 2022).

Ukrayna'daki savaşın başlamasından bu yana Norveç'in Avrupa'ya olan gaz ihracatı %10 artmış ve bu tesislerin etrafındaki güvenlikte karada ve denizde sıkılaştırılmıştır. Ekim 2022'de Norveç başbakanı Jonas Gahr Store, uluslararası bir krizde, Norveç'in Avrupa'ya gaz ve petrol ihracatı siber saldırıların hedefinde olabileceği endişesini dile getirmiş ve İskandinav hükümetinin, petrol sektörünü siber saldırılardan korumak için çok yavaş hareket ettiği yönündeki eleştirilerle birlikte, Rusya'nın ülkenin petrol ve gaz endüstrisi için ciddi bir siber tehdit oluşturduğu konusunda uyarılmıştır (Regjeringen.no, 2022). Şubat 2023'te Norveç Ulusal Güvenlik Teşkilatının yaptığı yıllık değerlendirmesinde de, Ukrayna'daki savaşın bir sonucu olarak ve Rusya'nın Avrupa enerji güvenliği üzerindeki baskısı sebebiyle, Norveç'in Avrupa'ya enerji tedarikçisi olmasıyla güvenlik politikasının büyük önem kazandığı ve dolayısıyla Norveç'in petrol ve gaz altyapısı hakkında daha fazla istihbarat girişimleri

olabileceği bildirilmiştir (The Norwegian Police Security Service [PST], 2023, s. 12). Dolayısıyla jeopolitik konumuyla dikkat çeken Norveç hükümeti, siber güvenliği sağlamak için çeşitli önlemler almakta ve uluslararası işbirliği geliştirmektedir.

3.5.2.2. Elektrik Enerjisi Endüstrisinde Dijitalleşme ve Rekabet

Elektrik, farklı yakıt kaynaklarından ve farklı teknolojilerle üretilmektedir: fosil yakıtlar (doğal gaz, petrol ve kömür), nükleer ve yenilenebilir enerji (rüzgar, güneş, hidro, biyokütle). Üretim ise ülkeler arasında önemli ölçüde farklılık göstermekte ve dijitalleşme sürecinde de değişim göstermektedir.

İleri teknolojiler, azalan maliyetler ve yeni pazarların ortaya çıkmasıyla hareket eden enerji sektörü, iklim değişikliği ve enerji güvenliği için kapsamlı etkileri olan yeni bir dijital çağın eşiğindedir. Dolayısıyla dijitalleşme, elektrik endüstrisini derinden dönüştürmektedir. Elektrik santrallerinden iletim şebekelerine ve dağıtım şebekelerinden son kullanıcı cihazlara kadar tüm elektrik altyapısında yaygınlaşan dijital süreç, elektrik sisteminin durumuna ilişkin artan miktarda veriyi kullanıma sunar ve yapay zeka, makine öğrenimi, büyük veri, veri analitiği, IoT, bulut bilişim, robotik gibi araçlarla enerjinin üretimi, iletimi, dağıtımı ve tüketimi hakkında daha iyi kararlar almak için kullanılır (Rossetto & Reif, 2021).

Elektrik üretimi, dağıtımı ve tüketimi arasındaki uyumu, tedarikçiler ve tüketiciler arasında dolaşan elektrik akışının izlenerek değerlendirilmesine izin veren bilgisayar teknoloji çözümlerinden oluşan akıllı sayaçların kullanımı ve akıllı şebekeler hakkındaki tartışmalar dijitalleşme dalgasının örneklerindendir. Dijitalleşme ile birlikte oluşan diğer eğilim ise karbon emisyonunu azaltma süreci olan karbonsuzlaşma/dekarbonizasyondur. Dekarbonizasyon, fosil yakıtların elektrik üretim karışımından kademeli olarak çıkarılmasını ve karbon salmayan diğer enerji kaynaklarına artan bağımlılığı ifade etmektedir. Bu değişim, son yıllarda iklim değişikliğini ve ilgili üretim teknolojilerindeki maliyet düşüşünü ele almak için çoğunlukla yenilenebilir enerji kaynaklarının aldığı güçlü politika desteğini yansıtmaktadır (Rossetto & Reif, 2021).

Dünya, geleneksel fosil yakıt tüketiminden yenilenebilir enerji kaynaklarına doğru kullanım önceliğini değiştirirken, enerji endüstrisi, esas olarak petrol ve kömüre

dayalı altyapılar yerine sürdürülebilir temiz enerji tesislerine daha fazla yatırım yapmaya başlamıştır. Elektrik enerjisi üretiminde rekabet gücünü korumak için petrol, gaz ve kömürle çalışan santrallerin dijital dönüşümle yakıt verimliliğinin ve performansının iyileştirilmesi gerekir. Günümüzde yenilebilir kaynakları daha rekabetçi hale getirmekte ve kömürden daha fazla güç üretmektedir. Sonucunda ise enerji depolamanın maliyeti düşmekte, elektrikli araçlar çoğalmakta, akıllı şebekeler yaygınlaşmaktadır. Dolayısıyla dijitalleşme, enerji tüketim davranışındaki değişiklikler yoluyla enerji sürdürülebilirliğini teşvik eder.

3.4.2.2.a. Avrupa Birliği

2021 verilerine göre AB'deki enerji karışımı temel olarak beş farklı kaynaktan oluşmaktadır: petrol (%34), doğalgaz (%23), yenilenebilir enerji (%17), nükleer enerji (%13), fosil yakıtlar (%12) (EUROSTAT, tarih yok). Avrupa bölgesi artan yenilenebilir enerji üretimi ve endüstriyel sektördeki büyüme nedeniyle küresel dijital enerji hizmeti pazarında önemli bir paya sahiptir. AB, Rus fosil yakıtlarına bağımlılığını sona erdirmek, iklim kriziyle mücadele etmek, enerji güvenliğini sağlamak, rekabetçi bir pazarın gelişimini desteklemek ve herkes için erişilebilir, uygun maliyetli enerji erişimi sağlanabilmesi için dijital enerji altyapısına yatırım yapmaktadır. Bu konudaki ana hedefleri; 2027 yılına kadar tüm ticari ve kamu binalarının çatılarına, 2029'a kadar tüm yeni konut binalarının çatılarına güneş panelleri kurulması; 2030'a kadar net sera gazı emisyonlarını %55 azaltmak; 2030'da %45 yenilenebilir enerji payına ulaşmak; 5G ve 6G bağlantısı, bulut bilişim, IoT cihazları ile desteklenen bir pan-Avrupa enerji veri alanı ve enerji sisteminin dijital ikizleri gibi dijital teknolojilere yatırım yapmak; enerji sistemlerinin siber güvenliğini artırmak; 2030 yılına kadar yollardaki 30 milyon arabayı elektrikli araçlarla değiştirmek (European Council for an Energy Efficient Economy [ECEEE], 2020a) (European Commission, 2023) (European Commission, 2022a). Bu politika çerçevesinde elektrikli araçların satın alımında vergi indirimleri uygulamakta, şarj istasyonlarının altyapısının geliştirilmesi ve elektrikli araç üretimi için teşviklerde bulunmaktadır.

AB üyesi ülkeler, yenilenebilir enerjinin gelişimini desteklemek için belirli stratejiler, planlamalar ve politikalar oluşturmaktadır. Örneğin Fransa Ulusal Enerji

Planı 2030, ülkenin enerji dönüşümü elde etmek için güç üretiminde yenilenebilir enerji kaynaklarının payını artırmaya devam edeceğini belirlemekte ve yenilenebilir enerji kaynaklarının toplam enerji üretiminin %40'ını ve rüzgar enerjisini %20 olarak planlıyor. Almanya ise enerji karışımlarındaki yenilenebilir enerji yüzdesini mevcut %18'den %30'a çıkarmayı hedeflemektedir (Huawei, 2020, s. 3-4).

3.4.2.2.b. Çin Halk Cumhuriyeti

Dünyadaki dijital dönüşüm liderlerinden biri olan Çin'de elektrik iletim şirketi State Grid Corporation of China (SGCC) gibi devlete ait işletmeler ve Huawei gibi özel sektör kuruluşları, ülkenin enerji verimliliği, elektrikli araç şarjı, akıllı ölçüm gibi çok sayıda alanda büyük dijitalleşme gerçekleştirmiştir. Bu doğrultuda SGCC, 2021'de elektrik şebeke altyapısının dijital dönüşümünü hızlandıracaklarını, sırasıyla 2030 ve 2060'dan önce karbon nötrlüğüne ulaşabileceklerini belirterek, fosil yakıtla üretilen gücün payını 2030'a kadar %25'e düşürme planını yayınlamıştır (The China Project, tarih yok). Huawei'nin Yeşil Kalkınma 2030 raporunda, gelecekteki yeşil kalkınmayı güçlendirmek için izlenmesi gereken üç ana yol açıklanmaktadır: (I) dijital altyapının enerji verimliliğinin iyileştirilmesi, (II) elektrik üretiminde yenilenebilir enerji kaynaklarının payının artırılması, (III) yeşil endüstrilerin etkinleştirilmesi. Bu adımlarla elektriğin %50'den fazlasının yenilenebilir enerjiden sağlanacağı ve 2030 yılına kadar tüm yeni binaların 2050 yılına kadar net sıfır karbonla çalışmasının beklendiği öngörülmektedir (Huawei, 2020a). SGCC ve Huawei gibi şirketler ayrıca yapay zeka, büyük veri, blok zinciri, bulut bilişim dahil olmak üzere birçok dijital enerji girişimine yatırım yapmıştır.

3.4.2.2.c. Güney Kore

Güney Kore elektriğin %34,32'si kömürden, %0,41'i petrolden, %27,3'ü nükleerden, %29,19'u sıvılaştırılmış doğal gazdan ve %8,5'i yenilenebilir kaynaklardan üretmektedir Güney Kore'nin 9. Güç Arzı ve Talebi Temel Planı, mevcut yenilenebilir enerji payı %15,1 oranından 2034 yılına kadar %40'a çıkarmayı hedeflemektedir. Plan, 30 yıllık işletme ömrü 2034 yılına kadar sona eren tüm kömüre dayalı elektrik santrallerinin kapatılmasını öngörmektedir (Asia Pacific Energy Portal, 2020).

Dijitalleşmeyi temel alan Kore Enerji Ana Planı 2035 ve Yeşil Yeni Mutabakat 2020 belgeleri de akıllı şebekeleri, akıllı sayaçları tanıtmak ve BİT altyapısını yükselterek enerji verimliliğini artırmayı amaçlamaktadır (Turovets, Proskuryakova, Starodubtseva, & Bianco, 2021, s. 40).

3.4.2.2.d. ABD

ABD'de elektriğinin %60'ını fosil yakıtlardan, %18'ini nükleerden ve %22'sini yenilenebilir kaynaklardan üretmektedir (U.S. Energy Information Administration [EIA], tarih yok). ABD, Kasım 2019'da feshettiğini bildirdiği Paris Anlaşmasına Ocak 2021 itibariyle yeniden katılarak, 2030 yılına kadar emisyonları yarıya indirme, 2035'e kadar emisyonsuz bir enerji sektörü yaratma ve en geç 2050'ye kadar ekonomi genelinde net sıfır emisyona ulaşma yenilenebilir enerji kaynaklarındaki hedefleri arasında yer almaktadır (The White House, 2021c).

3.4.2.2.e. Siber Uzayın İklim Değişikliğine Etkisi

Yüzeysel olarak bakıldığında siber güvenlik ve iklim değişikliği zıt konular gibi görünse de aralarında düşünüldüğünden daha fazla bağlantı vardır. İklim değişikliği, uluslararası ilişkilere konu olan ve enerji endüstrisinin en büyük sorunlarından biridir. Fosil yakıtların kullanımı sonucu açığa çıkan sera gazları, atmosferdeki karbondioksit seviyelerinin artmasına ve iklim değişikliğinin hızlanmasına neden olmaktadır.

Elektrik enerjisinin dijitalleştirilmesi, geleceğin önemli bir parçası ve iklim değişikliğinin hafifletilmesine de olumlu katkılar sağlamaktadır. Enerji endüstrisi siber uzaydaki gelişmeleri kullanarak ve enerji kullanma şeklini iyileştirerek enerji verimliliği artırılabilir ve yenilenebilir enerji kaynakları daha etkili bir şekilde kullanılabilir. Bu da sera gazı emisyonlarının azaltılmasına, enerji sistemlerinin karbondan arındırılmasına ve dolayısıyla iklim değişikliğiyle mücadeleye yardımcı olur. Bu duruma yardımcı olabilecek teknolojiler arasında bilgi ve iletişim teknolojiler, modern sensörler, büyük veri, yapay zeka ve nesnelerin interneti yer almaktadır.

3.5.3. Siber Uzay ve Enerji Sektörü

Petrol boru hatları, petrol sondaj işlemleri, petrol arıtma, elektrik iletim ve dağıtım hatları, doğalgaz depolama tesisleri, basınç regülasyonu, benzin istasyonları, nükleer, fosil yakıt, su barajları, santral tesisler dahil bilgisayar destekli kritik tüm tesislerdeki işlemler giderek birbirine bağlanan bilgisayarlar ve ağlar aracılığıyla faaliyet göstermektedir (Aydın, Barışkan, & Çetinkaya, 2021, s. 152). Dünyada enerji sistemlerinin birbirine artan bağılılığı nedeniyle enerji sektörü, siber saldırılar için en önemli sektörlerden biri haline gelmektedir.

Enerji sistemlerine yönelik meydana gelebilecek siber saldırıların sonucu sadece iş operasyonlarını değil, günlük yaşamı da olumsuz etkileyebilecek düzeydedir: Ülkelerde mevcut rafineler ve nükleer santraller atom bombasına dönüştürülebilir, doğalgaz enerji iletim sistemlerinde basınç artışı oluşturularak doğalgaz boruları havaya uçurulabilir, baraj kapakları açtırılarak şehirler ve tarım arazileri su altında bırakılabilir, şehirleri besleyen trafo merkezlerinde transformatörlerin çeşitli yollarla devre dışı bırakılması sonucunda kısa devre yapmasıyla arızalandırılması ya da trafo yağının yanarak yangına neden olması neticesinde şehirlerin elektriksiz bırakılarak karanlığa gömülmesi ve büyük üretim kayıplarına sebep olunabilir, sağlık, ulaşım, iletişim, ekonomi gibi hayati faaliyetler sekteye uğratılabilir, ülkeler enerji sistemlerine yönelik tehditlere karşı savunmasız hale getirilebilir, kamu düzeni bozulabilir ve ulusal güvenliğin istikrarsızlaşmasına neden olabilir (Aydın vd., s. 161).

Enerjiye olan bağımlılık artıkça siber saldırılarda öncelik, enerji sistemlerine kaymaktadır. Siber güvenlik, karmaşık ve küresel endüstriyel ortamda en üst düzeyde gözetim gerektiren kurumsal ve ulusal stratejik bir sorun haline gelmektedir. Çalışmada kritik enerji altyapısında siber güvenliği desteklemenin artan önemini ortaya çıkartan nükleer enerji, petrol ve gaz, elektrik endüstrisinden örnek vakalar incelenmiştir.

3.5.3.1. Petrol ve Gaz Endüstrisinde Siber Tehditler

Petrol ve gaz endüstrisinde ürünlerin çıkarılabilmesi, taşınması ve rafine edilebilmesi için bir dizi karmaşık sistem ve birbirine bağlı teknolojiler kullanılmaktadır. Bu teknolojiler, enerji hizmetlerinin ve ürünlerinin dağıtımını

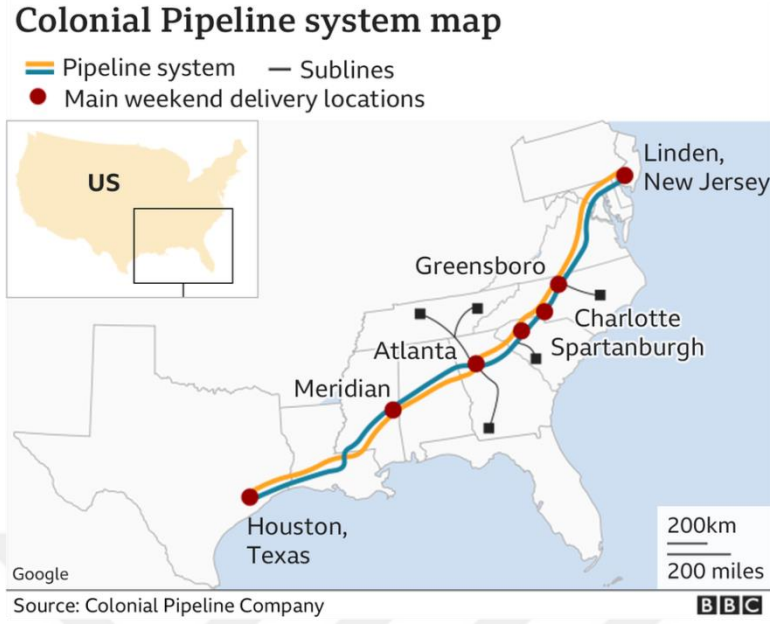
desteklemek için gerekli olsa da, endüstriyel sistemlerin artan dijitalleşmesi siber saldırılara karşı savunmasızlığı da artırmaktadır (World Economic Forum, tarih yok). Dolayısıyla bir petrol ve gaz şirketine yönelik siber saldırı, operasyonel aksamalara, ekonomik kayıplara, itibar zedelenmesi ve çevresel zararlara sebep verebilir.

Petrol ve gaz sektörü, jeopolitik çatışmalarda ulus devlet aktörleri, bilgisayar korsanları ve siyasi, ekonomik veya stratejik çıkarlarla motive olan diğer saldırganlar için bir hedef haline gelmektedir. Örneğin, Ukrayna krizinden hemen önce ABD'de Chevron, Cheniere, Kinder Morgan dahil olmak üzere sıvılaştırılmış doğal gaz üretimiyle uğraşan toplam 21 gaz üreticisi, siber saldırılara maruz kalmıştır (World Economic Forum, tarih yok). Saldırıların devlet destekli olduğuna inanılmakta ancak doğrudan Rusya'ya atıf yapılmamaktadır. Çünkü Ukrayna krizi, ABD'nin enerji politikalarını ve doğalgaz ihracatını etkileyen bir dizi faktöre sahiptir. Rusya'nın Ukrayna'ya doğalgaz ihracatını kesmesi, ABD'nin doğal gaz ihracatının artması için bir fırsat yaratmıştır. Sıvılaştırılmış doğalgaz ihracatı Rusya karşısında alternatif bir enerji sağlamak için önemli bir rol oynamakta. Dolayısıyla ABD'nin sıvılaştırılmış doğalgaz üretimini yapan şirketlerine yönelik siber saldırılar, ABD'nin doğalgaz ihracatını ve enerji politikalarını etkileyerek politik bir durum kazanabilir.

3.5.3.1.a. Colonial Pipeline Siber Saldırısı

ABD'deki rafine petrol ürünleri için en büyük botu hattı sistemi olan Colonial Pipeline'ın yürüttüğü modern operasyon türü son derece dijitaldir. Colonial Pipeline, Teksas Körfezi'nde ülkenin doğu kıyısına 8.850 km boru hattı aracılığıyla günde 2,5 milyon varil benzin, ev ısıtma yağı ve jet yakıtı taşımaktadır.

Şekil 28: Colonial Pipeline Boru Hattı Haritası



Kaynak: <https://www.bbc.com/news/technology-57063636>

Mayıs 2021'de Colonial Pipeline'in boru hattını ve bilgisayar ekipmanlarını etkileyen fidye yazılım saldırısı, tarihteki kritik ulusal altyapıya yönelik en önemli saldırılardan biri olarak nitelendirilmektedir. Saldırının ardından ise Doğu bölgesinin yakıtının neredeyse yarısını sağlayan Colonial Pipeline boru hattı uzun süre ağlarını kapatmış ve ABD yönetimi ülkede acil durum ilan etmiştir. Saldırı, yalnızca şirket içi operasyonların kesintiye uğramasına ve mali kayıplara yol açmamış, aynı zamanda diğer sektörler üzerinde de kademeli bir etki yaratmıştır. Örneği havacılık sektörü, jet yakıtı kıtlığı nedeniyle aksamalar yaşamış, benzin krizi korkusuyla satın alımlar artmıştır. Bu durum ise ABD'deki benzin istasyonlarında fiyatların yükselmesine ve benzin alımlarına 20 dolar sınır getirilmesine sebep olmuştur (Krauss, Chokshi, & San, 2021).

FBI, Colonial Pipeline ağlarının ele geçirilmesinde, Rusya merkezli olduğu düşünülen fidye yazılım çetesi DarkSide'in sorumlu olduğunu doğrulamıştır (FBI, 2021b). ABD Adalet Bakanlığı yaptığı açıklamada, Colonial Pipeline'in fidye yazılım korsanlarına ödediği, değeri 4 milyon dolardan fazla olan 75 Bitcoin'in izini sürerek ödenen fidyenin çoğuna el koyduğunu bildirmiştir. Kolluk kuvvetlerine ve mahkeme belgelerine göre, federal müfettişler fidye yazılım saldırısını gerçekleştiren DarkSide'a ait en az 23 farklı elektronik hesaptan oluşan akışı izleyerek 2,3 milyon dolar değerinde 63,7 Bitcoin'i geri almıştır (Benner & Perlroth, 2021). Bitcoin gibi dijital

para birimlerinin izlenmesi ve geri alınması vakaları nadirdir. Ancak fidye yazılımı büyüyen bir ulusal güvenlik tehdidi haline geldiği ve uluslararası ilişkileri zorladığı için siber güvenlik yetkilileri dijital para akışını izleme konusunda uzmanlıklarını artırmaktadır.

3.5.3.1.b. Avrupa Petrol Rafineri Limanlarına ve Depolama Tesislerine Yönelik Siber Saldırı (Amsterdam-Rotterdam-Antwerp)

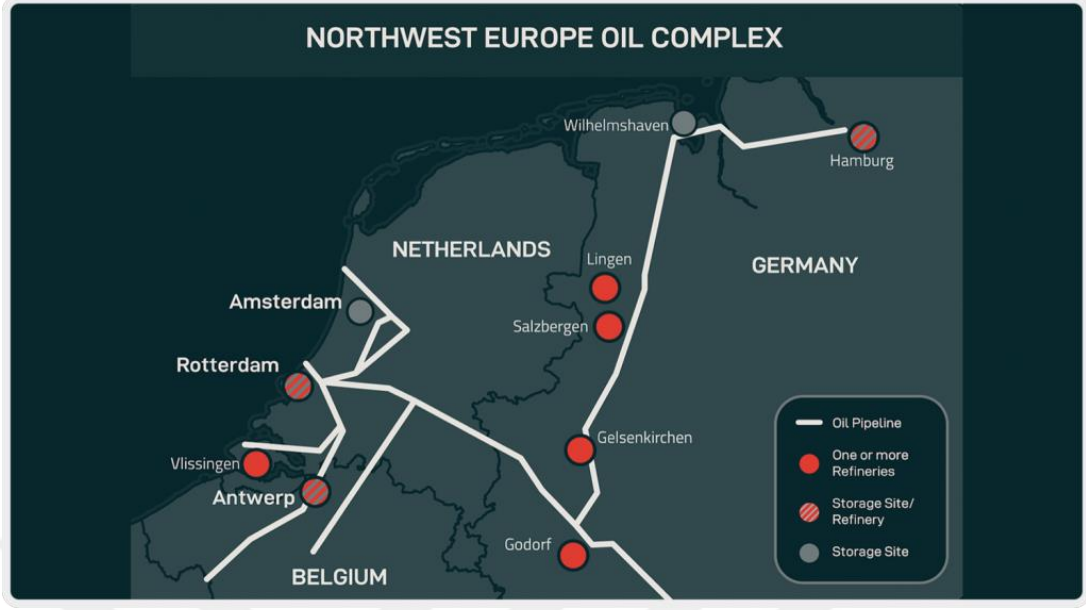
Avrupa'da Amsterdam-Rotterdam-Antwerp'te (ARA) 6 adet ve Almanya'da 11 petrol depolama merkezi dahil olmak üzere, -enerji fiyatlarının yükseldiği dönemde- 2022 yılının başlarında Kuzey Avrupa'daki petrol yükleme tesislerine yönelik gerçekleştirilen siber saldırı, rafine petrol kargo hareketini kesintiye uğratmış, tank çiftliklerinde büyük ölçüde otomatik bir süreçle işleyen yükleme ve boşaltma faaliyetlerinin aksamasına ve kısa vadeli yakıt kıtlığına sebep olmuştur.

29 Ocak 2022'de ilk siber saldırıya uğrayarak BT sistemleri kesilen, Almanya'daki petrol depolama şirketi Oiltanking ve petrol tedarik şirketi Mabanaft'ın yayınladığı ortak bildiride, mücbir sebep¹³ ilan ederek sorumluluklarından muaf tutulmuştur. Özellikle Oiltanking'in tank çiftliklerinin faaliyet gösterememesi nedeniyle, orta ölçekli şirketlerin ve Shell gibi büyük şirketlerin benzin istasyonlarına tedarik sağlanamamış, otomatik olarak gerçekleştirilen faaliyetlerin manuel olarak yapılmasını zorunlu hale getirmiş ve bu durum Kuzey Almanya'da 233 benzin istasyonuna petrol tedarikini etkilemiştir (Scholz & Verfürden, 2022).

Saldırıdan etkilenen diğer şirketler ise Belçikalı Sea-Tank ve Hollandalı akaryakıt depolama firması Evos'tur. Sea-Tank ve Evos, Amsterdam-Rotterdam-Antwerp petrol merkezi içinde ve çevresinde depolama yapmaktadır. Şirketlere yönelik gerçekleştirilen siber saldırı, limanda sorunlara sebep olmuştur. Belçika savcıları ise Rotterdam'dan sonra Avrupa'nın en büyük ikinci petrol limanı olan Antwerp dahil olmak üzere, ülkenin deniz giriş yollarındaki petrol tesislerinin siber saldırıya uğramasıyla ilgili soruşturma başlatmıştır (Payne, 2022).

¹³ Bir şirketin öngörülemeyen ve kendisinden kaynaklanmayan olağan üstü bir durum nedeniyle tedarik sözleşmesinden doğan yükümlülüklerini yerine getiremediği zaman kullanılan acil yasal madde.

Şekil 29: Amsterdam-Rotterdam-Antwerp Rotası



Kaynak: <https://ursaspace.com/blog/dated-brent-goes-dutch/>

Bir Alman gazetesine göre, Alman güvenlik servislerinden gelen ilk rapor, BlackCat fidye yazılımının Almanya'daki siber saldırılarda kullanılan araç olduğunu belirtmiştir. BlackCat, Kasım 2021'de bilgisayar korsanlarının hedef sistemlerinin kontrolünü ele geçirmesine olanak tanıyan bir yazılım aracı olarak ortaya çıkmış ve kısa zamana ün kazanmıştır. Araştırmacılar, BlackCat programcılarının Rusça kullandığını, ancak bilgisayar korsanlarının izlerini gizlemek için genellikle yanlış ipuçları bırakarak yanıltma yöntemi uyguladıklarını belirtmektedir (Scholz & Verfürden, 2022). Ayrıca saldırı, Rusya'nın Ukrayna'yı işgaline giden yolda yaşanan diplomatik gerilim, petrol fiyatlarının en yüksek seviyeye ulaşması ve Avrupa'nın enerji güvenliğine ilişkin derinleşen endişeler gibi jeopolitik krizin mevcut olduğu dönemde gerçekleşmesi manidar karşılanmıştır.

3.5.3.1.c. Saudi Aramco'da Triconex Denetleyici Saldırısı

Dünyanın en büyük ham petrol ihracatçılarından biri olan Saudi Aramco, 2017 yılında petrol ve gaz operasyonlarına zarar verecek ve fabrikada bir patlamaya neden olabilecek Triconex kontrolörlerini kapatmak için tasarlanmış "Triton" isimli kötü amaçlı yazılım saldırısına uğramıştır. Ancak kullanılan koddaki bir kusur güvenlik sistemini tetikleyerek tesisi durma noktasına getirmiş ve saldırının kötü sonuçlar

vermesinin önüne geçmiştir. Triconex kontrolörleri, Amerikan şirketi Schneider Electric tarafından üretilen endüstriyel bir kontrol sistemidir ve nükleer, su arıtma tesisleri, petrol ve gaz rafineleri, kimyasal tesisler dahil olmak üzere dünya çapında 18.000 tesiste kullanılmaktadır. Bu kritik endüstriyel kontrolörler, basınç, sıcaklık ve voltaj gibi özellikleri düzenleyerek ekipmanın güvenli parametreler içinde çalışmasını sağlar. Saldırı sonrasında Schneider, Saudi Aramco, ABD İç Güvenlik Bakanlığı ve Triton soruşturmasına katılan diğer kurumlarla işbirliği yaptığını, gelecekteki saldırılara yanıt vermesine yardımcı olmak için daha fazla kişiyi işe aldığını ve cihazlarında kullanılan ürün yazılım ve protokollerin güvenliğini artırdığını belirterek yanıt vermiştir (Giles, 2019).

Saldırının failleri bilinmemekte, ancak kaynaklara göre son derece karmaşık ve pahalı bir saldırı olması nedeniyle ulus devlet aktörlerinin saldırıyı gerçekleştirdiği düşünülmektedir. Siber güvenlik şirketi FireEye araştırmacıları 23 Ekim 2018'de, siber tehdit aktörlerinin Saudi Aramco'nun ağında bıraktıkları dijital dosyaları bularak diğer dosyaların izini sürmeye başlamıştır. Kötü amaçlı yazılımla bağlantılı işlemleri başlatmak için kullanılan IP adresi ve Kiril alfabesindeki karakterlerden oluşan birkaç isim tespit edilmiştir. İzinsiz giriş faaliyetlerinin, Rus hükümetine ait teknik araştırma kurumu olan *Rusya Merkezi Kimya ve Mekanik Araştırma Enstitüsü* tarafından desteklendiği değerlendirilmiştir. Ancak araştırmacılar enstitünün, Triron'un geliştirilmesine yardımcı olmak için gerekli kurumsal bilgi ve personele sahip olması "muhtemel" olarak değerlendirilmiş, kesinliğine dair özel bir kanıt bulunamadığına dikkat çekmiştir (Mandiant , 2018).

3.5.3.1.d. Norveç'in Petrol ve Gaz Sektöründeki 50 Şirkete Yönelik Siber

Saldırı

2014 yılında Norveç'in petrol endüstrisini hedef alan bir siber saldırı gerçekleştirilmiştir. Norveç devletine ait en büyük petrol üreticisi olan Equino (eski adıyla Statoil) dahil olmak üzere petrol endüstrisindeki 250 şirket risk altındayken 50 şirket saldırının hedefi olmuştur. Siber tehdit aktörleri, şirketlerin ticari ve stratejik bilgilerini ele geçirmek amacıyla, şirket yöneticilerini kötü amaçlı eklere yönlendirmek için hedef odaklı kimlik avı saldırılarını kullanarak bilgisayar ağlarına sızmış ve şirketin verilerine erişim sağlamıştır (The Local, 2014). Saldırı sonucunda ise

şirketlerin çeşitli bilgileri çalınmış ve bu durum petrol endüstrisi açısından büyük bir güvenlik açığı ve itibar kaybı yaratmıştır.

Norveç, Rusya'nın Ukrayna'yı işgalinin ardından Avrupa pazarlarının kilit gaz tedarikçisi olarak önemli bir konumda olması nedeniyle yüksek bir siber saldırı riskinde olduğu düşünülmektedir. Saldırı ile ilgili çok fazla ayrıntı mevcut olmamakla birlikte, Norveç hükümeti saldırının arkasında Rusya'nın olabileceği şüphesiyle konuyu araştırmış ancak kesin bir kanıt elde edememiştir.

3.5.3.2. Nükleer Endüstrisinde Siber Tehditler

Dijital sistemler nükleer tesislerin ayrılmaz bir parçasıdır ve bilgi teknolojisine bağlı sistemler nükleer enerji santralleri için ciddi ve küresel bir tehdit haline gelmiştir. Dolayısıyla nükleer endüstrisi, siber saldırılara karşı savunmasız sektörlerden biridir. Siber saldırılar, nükleer tesislerin kontrol sistemlerine, güvenlik sistemlerine ve hatta nükleer silahların depolandığı yerlere erişim sağlayarak, küresel bir etki yaratacak seviyede nükleer tesislerin çalışmalarını etkileyebilir, yıkıcı bir radyolojik kazaya sebep olabilir ve tesislerin güvenliği üzerinde ciddi bir tehdit oluşturabilir. Bu o kadar tehlikeli kabul ediliyor ki ülkelerin olası bir siber savaşta nükleer sektörünün, yasak bölge olması gündeme gelmiş bir konudur. BM Hükümet uzmanlar grubunun siber uzayda normlar öneren 9 Ağustos 2015 tarihli raporunda ülkelerin kritik altyapıya herhangi bir şekilde zarar vermemeyi kabul etmeleri tavsiye edilmektedir (Collins-Fattedad, DeVito, Goes, Khorenyan, & Milgrim, 2022, s. 27).

Siyasi ve stratejik ortam değiştikçe ve siber yetenekler geliştikçe, askeri nükleer programlara yönelik siber saldırılar büyük bir stratejik risk haline gelebilir, nükleer cephaneliklerin güvenilirliğini baltalayabilir ve çatışmaların tırmanmasına yol açabilir. Uluslararası Atom Enerjisi Kurumu (IAEA), nükleer tesislere yönelik siber saldırıları içeren üç önemli risk senaryosu belirlemiştir (Boulain & Ogilvie-White, 2017):

1. Bir nükleer tesisin komuta ve kontrol sistemini bozan, nükleer veya başka bir radyoaktif malzemenin izinsiz olarak çıkarılmasına yol açan bir siber saldırı; böyle bir saldırı büyük olasılıkla bir terör örgütü, bir devlet veya şirkete şantaj yapmak isteyen bir suç örgütü tarafından gerçekleştirilebilir. Bu

senaryoda siber saldırı, fiziksel erişimle sağlandığı için zor olsa da uygulanabilir bir senaryodur.

2. Bir devlete ait nükleer tesisin komuta ve kontrol sistemlerinin normal işleyişini etkileyen, devre dışı bırakan, nükleer caydırıcılığını felç eden bir siber sabotaj eylemi; devletlerin, terör örgütlerinin, siyasi aktivistlerin (çevreci gruplar gibi) bu tür siber operasyonlardan çıkarları olabilir. Bu yüksek risk senaryosu gerçekleşmiş ve bir ölçüde de başarılı olmuştur. 2010'da ortaya çıkan Stuxnet kötü amaçlı yazılım bu senaryoya örnektir.

3. Hassas nükleer silah bilgilerinin toplanması ve kullanılmasıyla sonuçlanan bir siber casusluk eylemi; bazı nükleer silahlı devletlerde cephanelik ve nükleer savaş başlıklarının teslimatı, mobil sistemler aracılığıyla gerçekleştirilir. Kötü niyetli devlet veya devlet dışı aktörler, bu nükleer savaş başlıklarının konumu ve nakliye programı hakkında hassas bilgilere erişmek ve onları çalmak için siber saldırıları kullanabilir. Ayrıca nükleer silah elde etmek veya radyolojik silahlar geliştirmekle ilgilenen devlet veya terör örgütleri tarafından nükleer silahların tasarımına yönelik bilgilere erişmek için siber saldırılar düzenlenebilir. Bu senaryoya ilişkin vakalara örnek ise Korea Hydro'ya yönelik gerçekleştirilen siber saldırı ve Ekim 2011'de Budapeşte Teknoloji ve Ekonomi Üniversitesi'ndeki bir araştırma laboratuvarını etkileyen Duqu kötü amaçlı yazılımıdır. Stuxnet'e benzeyen ancak farklı bir amaç için kullanılan Duqu kötü amaçlı yazılımı, içeriden birinin desteği olmadan nükleerle ilgili hassas bilgileri elde etmek için kullanılabileceğini göstermiştir.

Nükleer saldırıya sebep olabilecek bir siber saldırı, en büyük felaket içeren senaryo olsa da önünde engeller vardır. Askeri açıdan güçlü devletler gelişmiş askeri siber yeteneklere sahiptir ve barış zamanında başka bir devlete, büyük bir siber saldırı başlatmayı kendi çıkarlarına uygun görenlerin sayısı çok azdır (Gartzke, 2013, s. 63). Bu konuda ABD eski Siber Komutanlığı başkanı General Keith Alexander, yabancı liderlerin ABD'ye yönelik büyük bir saldırının izinin sürüleceğini inandığından ve böyle bir saldırının hızlı ve orantılı bir yanıtı yol açacağından emin olduklarını ifade etmiştir (Farnsworth, tarih yok).

Ayrıca ulus devletler nükleer caydırıcılığı artırmak ve nükleer silah sahibi ulus devletlerin nükleer cephaneliğini sabote etmek için siber araçlar geliştirmektedir. Örneğin Güney Kore, Kuzey Kore'nin nükleer silah programını hedef almak için siber

saldırı silahları geliştirmektedir. Bu doğrultuda Güney Kore, Kuzey Kore'nin seçkin bilgisayar korsanları biriminin oluşturduğu tehdide karşı korunmak için ilk olarak 2010 yılında bir Siber Komutanlık birimi kurmuştur. Amacı ise ulusal ağıları Kuzey Kore kaynaklı siber saldırılardan korumak ve Kuzey Kore'nin nükleer silah geliştirme kabiliyetini bozmaktır (Keck, 2014).

3.5.3.2.a. Stuxnet

Özel olarak hedeflenen, hassas bir şekilde tasarlanmış, teknolojik olarak geliştirilmiş, endüstriyel kontrol sistemlerini hedef alan ve erişim sağlayabilmek için USB bellekler gibi aracı cihazların kullanımını gerektiren bir siber silah olarak 2010 yılında ortaya çıkan Stuxnet, nükleer santrallerdeki siber tehditlerin gerçekliğini ortaya koyan önemli bir vaka çalışmasıdır. Yarısından fazlası İran'da olmak üzere 60.000'den fazla bilgisayara bulaşan Stuxnet, en fazla hasar gören İran'ın dışında Hindistan, Endonezya, Azerbaycan, ABD, Pakistan, Güney Kore, Malezya, Almanya, Avustralya ve İngiltere'de de bulunmuştur (Farwell & Rohozinski, 2011, s. 23). Stuxnet hedefli bir saldırı olsa da diğer ülkeler için bir güvenlik riski oluşturmuş ve nükleer tesislerini siber saldırıya uğratmıştır.

Stuxnet'in ABD ve İsrail tarafından geliştirildiği ve özellikle İran'ın uranyum zenginleştirme yeteneğini sabote etmek amacıyla İran'ın nükleer tesislerini hedef aldığı iddia edilmektedir. Stuxnet, uranyum zenginleştirmek için kullanılan santrifüjlerin çok hızlı dönmesine ve parçalanmasına neden olurken, santrifüjlerin normal çalışıyormuş gibi görünmesi için kontrol mekanizmasına yanlış bilgi göndererek çalıştırılmıştır (Baylon, 2016, s. 215). Fiziksel ve maddi hasarlara yol açan Stuxnet virüsünden etkilenen tesislerden biri de İran'ın Natanz uranyum gazını zenginleştirme tesisine yöneliktir. Sonucunda ise tesiste yaklaşık 1000 santrifüje zarar vererek İran'ın uranyum gazını zenginleştirmek için ürettiği santrifüj sayısının düşmesine ve silah kapasitesine ulaşma kabiliyetinin gecikmesine yol açmıştır (Yetgin & Özkan, 2021, s. 118).

Stuxnet, uluslararası toplumun çoğunluğu tarafından İran'ın nükleer silah edinmesini engellemek amacıyla tasarlanması ve İran'ın nükleer programını engellemek için olası nükleer tesise hava saldırısının sivil kayıplara yol açabileceği ve radyoaktif maddelerin yayılması kötü sonuçlar doğurabileceği sebebiyle olumlu ve güvenli bir yöntem olarak karşılanmıştır (Baylon, 2016, s. 215-216). Etik açıdan

değerlendirildiğinde Stuxnet, egemen bir devlete yönelik saldırı teşkil etmektedir. Ayrıca Stuxnet, siber savaş riskini artıran bir siber silahlanma yarışı başlatmıştır. İran'ın Stuxnet saldırısının ardından kendi siber silah programını hızlandırdığı ve Ababil Operasyonu ismiyle geçen 2011-2013 yılları arasında ABD'nin çeşitli finans kurumlarını hedef alan bir dizi saldırıyı misilleme olarak gerçekleştirdiği tahmin edilmektedir.

Saldırının ABD ve İsrail devletlerine atfedilmesinin sebebi ise;

ABD, İsrail ve uluslararası toplumun çoğunluğu uzun yıllardır İran rejiminin elindeki nükleer silahların bölgeyi istikrarsızlaştıracağına, ABD'nin Orta Doğu'daki en büyük müttefiki olan İsrail'i doğrudan tehdit edeceğine, ABD ve Avrupa için güvenlik riski oluşturacağına inanarak İran'ın nükleer silah üretmesini engellemek için birçok girişimde bulunmuştur (Yetgin & Özkan, 2021, s. 120). 2005 yılında Mahmud Ahmedinejad İran Cumhurbaşkanı olarak göreve gelmesiyle uranyum zenginleştirme faaliyetleri hız kazanmış ve bu durumda 2006 yılında BM Güvenlik Konseyi İran'a uranyum zenginleştirme faaliyetlerini durdurma çağrısını yasal olarak bağlayıcı hale getirmiştir. Ancak İran'ın ilgili faaliyetleri durdurulmaması sebebiyle İran'ı ekonomik olarak etkileyen yaptırım uygulaması kabul edilmiştir. 2010 yılına kadar İran'a yönelik yaptırım kararları sert bir şekilde uygulanırken gerçekleşen Stuxnet saldırısı, ABD ve İsrail politikalarının bir uzantısı olabileceği görüşleri hakim olmuştur (Yetgin & Özkan, 2021, s. 117).

3.5.3.2.b. Korea Hydro & Nuclear Power Co. Ltd'ye Yönelik Siber Saldırı

Sony Pictures'a yönelik gerçekleştirilen saldırıyla eş zamanlı olarak 2014 yılında, Güney Kore'de nükleer enerji santralleri işleten Korea Hydro'nun bilgisayar ağına bir siber saldırı gerçekleştirilmiştir. Siber tehdit aktörleri şirketin bilgisayar sistemlerine bulaştırdıkları kötü amaçlı yazılımlar aracılığıyla, 10.000 KHNP çalışanının kişisel bilgilerinin, nükleer santralle ilgili verilerin, tasarım ve kılavuzların, elektrik akış çizelgelerinin çalınmasıyla sonuçlanmıştır (McCurry, 2014).

Seul merkez savcılığında yapılan açıklamada, siber saldırıda kullanılan kötü amaçlı kodlar, çalışma yöntemleri bakımından Kuzey Koreli bilgisayar korsanları tarafından sıklıkla kullanıldığı bilinen "Kimsuky" kötü amaçlı yazılımı ile aynı olduğu,

şüpheli bilgisayar korsanının IP adresinin Çin'in Shenyang kentine kadar takip edildiği ve Shenyang kentinin Kuzey Kore hükümeti tarafından gönderilen siber uzmanlara ev sahipliği yaptığı belirtilmiştir (Yoo-chul, 2014). Siber savaş niyetini açıkça gösteren son eylemleri göz önüne alındığında Kuzey Kore ile yakından bağlantılı olduğuna yönelik bulgular mevcut olsa da, çalışanların mahremiyetine yönelik tehdit içeren saldırıyı Çin ve Kuzey Kore hükümetleri bu iddiayı reddetmiştir.

3.5.3.2.c. Çin Casus Balonu

2 Şubat 2023 tarihinde dijital kamera, radar sistemi, sinyal ve iletişim teçhizatı taşıyan Çin casus balonunun Alaska, Utah, Missouri ve Montana eyaletinin nükleer silah depolama tesislerinin bulunduğu bölge üzerinden geçtiği iddia edilmiştir (Sanger, 2023). Çin casus balonu, Tennessee eyaletindeki çeşitli nükleer araştırma ve üretim tesislerine ev sahipliği yapan Oak Ridge şehrindeki hassas askeri ve sivil araştırma tesisleri üzerinde de görülmüştür. Dışişleri Bakanlığı yetkilileri Çin casus balonunun, hava durumu verilerini toplamak amacıyla değil istihbarat toplamak için donatıldığını, balonun hava durum tespiti için kullanılan balonlarındaki ekipmanla tutarsız olduğunu bildirmiştir. Ayrıca 4 Şubat 2023'te F-22 jetiyle atılan bir füze aracılığıyla düşürülen Çin casus balonunu, Halk Kurtuluş Ordusu tarafından yürütülen bir istihbarat toplama programıyla ilişkilendirilmiştir. Yetkililere göre Çin hükümetinin yaptığı, *"büyük bir çaba ile eski bir teknolojiyi modern iletişim ve gözlem yetenekleriyle birleştirerek diğer ulusların orduları hakkında istihbarat toplamak"* ifadesiyle açıklanmıştır (Nakashima, Harris, Hudson, & Lamothe, 2023). Ayrıca Çin'in 2018 yılından beri Japonya, Hindistan, Vietnam, Tayvan ve Filipinler dahil olmak üzere gelişmekte olan ve stratejik ilgi alanı olan ülkelerdeki askeri varlıklar hakkında bilgi toplamak için casus balonlarla faaliyet yürüttüğü iddiaları mevcuttur.

Biden yönetimi casus balonu, egemenliğe ve uluslararası hukuka yönelik açık bir ihlal olarak değerlendirmiş ve Dışişleri Bakanı Antony Blinken yakın bir tarihte Çin'e gerçekleştireceği ziyaretini ertelemiştir. Çin casus balonunun, frekanslar toplayarak özel gözetleme ekipmanı taşıyabileceği tahmin edilmektedir ancak hangi verileri toplayabileceği veya balonun hangi gözetleme yeteneklerine sahip olabileceği hala belirsizliğini korumaktadır.

3.5.3.3. Elektrik Enerjisine Yönelik Siber Tehditler

Dünyadaki birçok ülke elektrik enerjisi sektörünü, işleyen bir toplum için kritik altyapı olarak sınıflandırmıştır. Çünkü bir bölgede yaşanan uzun elektrik kesintisi, toplumun karanlıkta ve hareketsiz kalmasına sebep olacak finans, iletişim, internet, ulaşım, su, sağlık gibi birbirine bağımlı sistemleri de ciddi bir şekilde etkileyecektir.

3.5.3.3.a. BlackEnergy Kötü Amaçlı Yazılımı

23 Aralık 2015'te bölgesel bir elektrik dağıtım şirketi olan Kyiv Oblenagro ve Pyrkarpattya Oblenagro'ya yönelik gerçekleştirilen *BlackEnergy* siber saldırısının ardından, Batı Ukrayna'nın Ivano-Franksick bölgesindeki 220.000'den fazla halk elektrik kesintisi yaşamıştır. Siber tehdit aktörleri, şirket bilgisayarlarına ve SCADA sistemlerine yasadışı erişim sağlayarak 30 trafo merkezinin bağlantısını engellemiş ve hizmet kesintisine sebep olmuştur (Lee, Assante, & Conway, 2016). Bir elektrik şebekesine yönelik yıkıcı bir siber saldırının ilk onaylanmış örneği olan bu vakada, Ukrayna Güvenlik Servisi (SBU) olaydan Rusya'yı sorumlu tutarken, ABD'li siber güvenlik şirketi olan iSight Partners olayı, "*Sandworm*" olarak bilinen bir Rus bilgisayar korsanlığı grubuyla ilişkilendirmiştir (Volz & Finkle, 2016).

BlackEnergy, DDoS saldırıları, spam dosyaları indirmek, siber casusluk, bilgi hırsızlığı veya veri imha saldırılarını gerçekleştirmek amacıyla özellikle enerji endüstrisindeki şirketleri ve SCADA sistemlerini kullanan şirketlere karşı kullanılan bir Truva Atı'dır. Kaspersky'ye göre, Ukrayna saldırısında kullanılan BlackEnergy Truva atı, 2014 yılında dolaşıma girmiştir (Kaspersky, tarih yok(f)). Endüstriyel Kontrol Sistemlerini riske atabilecek işlevlere sahip bu yazılım, hedef kişiye kötü amaçlı bir ek içeren e-posta gönderir ve hedeflenen kişiden belgenin içeriğini görüntülemesi için gönderilen eki çalıştırması talimatını verir (TrendMicro, 2016). Böylece siber tehdit aktörlerinin sistemdeki kimlik bilgilerini bulmalarına, ağ boyunca yanal hareketler gerçekleştirmelerine, merkezlerin SCADA sistemlerine ulaşmalarına izin sağlamaktadır (Miller, 2021).

3.5.3.3.b. Industroyer Kötü Amaçlı Yazılımı

Aralık 2015 yılında 220.000'den fazla kişiyi etkileyen elektrik kesintisi ile ilişkilendirilebilecek bir diğer olay, yaklaşık bir yıl sonra 17 Aralık 2016'da, Kiev şehri ve çevresindeki bölgelerde elektrik kesintilerine sebep olan *Industroyer* isimli kötü amaçlı yazılımı ile bir siber saldırı gerçekleştirilmiştir. Ulusal enerji şirketi Ukrenegro, yaşanan elektrik kesintisinde, Kiev'in elektrik tüketiminin yaklaşık beşte birini kaybettiğini bildirmiştir (BBC, 2017).

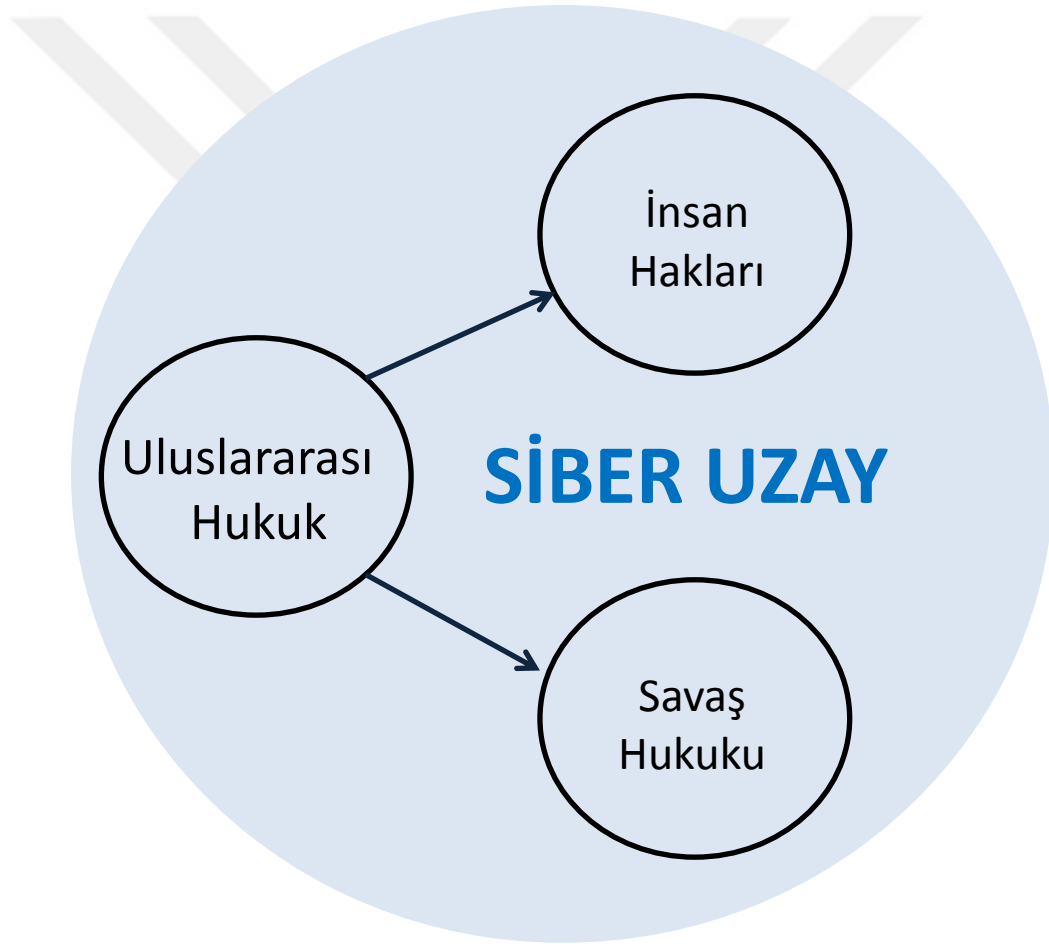
ESET araştırmacıları ise Kiev'i etkileyen elektrik kesintisinden Industroyer adı verilen bir kötü amaçlı yazılımın sorumlu olduğunu ortaya çıkartmıştır. 2017 yılında anti virüs sağlayıcısı ESET araştırmacılarının sunduğu rapora göre Industroyer, Stuxnet'den bu yana Endüstriyel Kontrol Sistemleri için en büyük tehdit olarak tanımlanan kötü amaçlı yazılım, elektrik trafo merkezi anahtarlarını ve devre kesicilerini doğrudan kontrol edebildiği için özellikle tehlikeli bir siber tehdit olarak sınıflandırılmıştır. Bunu yapabilmek için ise kritik altyapı sistemlerinde kullanılan iletişim protokollerindeki zayıflıklardan yararlanılmaktadır. Buradaki sorun ise protokollerin onlarca yıl önce endüstriyel sistemlerin dış etmenlerden izole edilerek güvenlikleştirilmesi düşünülmeden tasarlanmış olmasıdır (Cherepanov, 2017) (ESET, 2017). Dolayısıyla bu tür sistemlerin bozulması, hayati hizmetlerin işleyişini doğrudan veya dolaylı olarak etkileyebilmektedir.

Enerji sektörünün siber uzayı hangi düzeyde etkilediği problemi çerçevesinde (P_{1d}), sektörün siber uzayda entegrasyonu, enerji sektörünü dönüştürme, verimliliği, sürdürülebilirliği ve dayanıklılığı artırma potansiyeline sahiptir. Bununla birlikte ilgili riskleri ve endişeleri ele almak için siber güvenlik önlemleri ve dikkatli veri gizliliği yönetimi gerektirir.

4. ULUSLARARASI HUKUKUN SİBER UZAYDAKİ ROLÜ

Siber uzaya artan güven ve dijital altyapıların birbirine bağılılığı küresel istikrarı sağlama ve insan haklarını koruma konusunda yeni zorlukların ortaya çıkmasına sebep olmuştur. Bu bağlamda uluslararası savaş hukuku ve insan hakları hukuku çerçevesinde siber uzayın önemi yadsınamaz. Dolayısıyla küresel etkiye sebebiyet verebilen siber saldırıların etkilerinin minimize edilebilmesi için uluslararası savaş hukuku ve insan hakları hukukuna uyum gerektirmektedir.

Şekil 30: İnsan Hakları & Savaş Hukuku



Siber saldırılar, konvansiyonel savaş yanında alternatif bir araç olarak sunulan ve gelişmekte olan askeri bir yetenektir. Tüm ulus devletlerin siber saldırı yeteneklerini geliştirmesi de Soğuk Savaş'ın nükleer silahlanma yarışını anımsatan bir siber silahlanma yarışı sayılabilir. Teknolojideki hızlı gelişmeler, savaş ve güvenlik de dahil olmak üzere birçok sektörde devrim yaratma potansiyeline sahipken, sonuçları

dikkatle değerlendirmek ve yasal çerçeveleri buna göre uyarlamak önemlidir. Siber savaş veya siber saldırı olarak nitelendirdiğimiz durumlar teknolojik olarak gelişmiş veya gelişmemiş tüm ulus devletleri alakadar etmektedir. Çünkü siber uzayda rastlantısal veya tasarlanarak gerçekleştirilen herhangi bir saldırı diğer ulus devletleri etkileyebilmektedir. Dolayısıyla Endüstri 4.0, uluslararası hukukta siber silahların uygulanması da dahil olmak üzere çeşitli alanlarda hızlı bir değişikliğin getirilmesini mecburi kılmaktadır (Zahra, Handayan, & Christiant, 2021).

Siber uzayda büyüyen tehditlere karşı savunma stratejilerinde yenilikler ve düzenlemeler yapılmalıdır. Ancak siber güvenlik stratejileri geliştirilirken hükümetler, ulusal egemenliğe ve küresel etkiye öncelik vermektedir. Siber uzayda insan haklarından ve siber güvenlikten söz edilecekse her şeyden önce ortak ilkeler ve prensiplerin benimsenmesi, internet etiğinin oluşturulması ve insan haklarının göz ardı edilmemesi gerekmektedir (Çokbıdık, 2018, s. 147). Çünkü dünya genelinde bireyler, sıklıkla siber uzayla ilgili insan hakları ihlalleri ile karşı karşıya kalarak düşünce özgürlüğü, örgütlenme özgürlüğü, bilgiye erişim ve mahremiyet gibi temel haklarından mahrum bırakılmaktadır. Bu ihlaller hem hükümetlerin kendi ulusuna yönelik kontrol ve gözetim mekanizmalarını yaygınlaştırmasıyla hem de rakip ulus devletlerin birbirlerine yönelik gerçekleştirdiği siber casusluk operasyonlarıyla kendini göstermektedir. Dolayısıyla bireylerin ifade özgürlüğü, kişi güvenliği ve özgürlüğü, özel yaşamın gizliliği ve kişisel verilerin korunması en sık ihlal edilen haklardır. İnternet sansür araçlarındaki son gelişmeler ve Edward Snowden'ın NSA'nın küresel gözetimi hakkındaki açıklamaları, internet özgürlüğünün, anonimliğin ve veri korumasının ne kadar savunmasız olduğunu canlı bir şekilde göstermektedir (Carnegie Council, 2021).

4.1. Siber Uzayda İnsan Hakları İhlalleri

Siber güvenliği tanımlamaya yönelik insan merkezli bir yaklaşım, yalnızca ağların ve hizmetlerin güvenliğini sağlamaya değil, aynı zamanda bu ağların ve hizmetlerin toplumun tüm üyeleri tarafından nasıl güvenli bir şekilde kullanılabileceğine odaklanmak anlamına gelir (Merali & Bavicic, 2022).

İnsan haklarından bahsederken, çoğunlukla BM İnsan Hakları Evrensel Beyannamesi ve Uluslararası Medeni ve Siyasi Haklar Sözleşmesi kapsamında

güvence altına alınan, ifade özgürlüğü, mahremiyet hakkı, düşünce özgürlüğü ve örgütlenme özgürlüğü tüm insanların en temel haklarından bazılarıdır. Hükümetler tarafından alınan bir dizi siber güvenlik yasaları ve önemleri, bu tür hakları doğrudan ihlal ederek veya insanların haklarını ifade etme istekleri üzerinde caydırıcı bir etki yaratarak çevrimiçi konuşma ve ifade özgürlüğü üzerinde olumsuz bir etkiye sebep olabilmektedir

4.1.1. İfade Özgürlüğü

İfade özgürlüğü, hem ulus devletlerin vatandaşlara sağladığı bir güvence hem de uluslararası anlaşmalarda yer alan yasal bir çerçeve olarak ortaya çıkmıştır. İfade özgürlüğü, İnsan Hakları Evrensel Beyannamesinde "*her bireyin müdahale olmaksızın fikir sahibi olma ve ülke sınırları gözetmeksizin bilgi ve fikirleri herhangi bir araçla arama, erişme ve paylaşma hakkı*" olarak tanımlanmaktadır (UN, 1948). 2011 yılında BM Özel Raportörü Frank de la Rue bütün ulus devletleri, siyasi çatışma dönemleri de dahil olmak üzere internet erişiminin her zaman korunmasını sağlamaya çağırması ve 2012'de Cenevre'deki BM İnsan Hakları Konseyinde "insanların çevrimdışı oldukları aynı haklardan çevrimiçi olarak da korunması" gerektiğini dile getirmiştir (Yılmaz, 2026, s. 282).

Bilgiye erişimin önünde engeller varsa veya bilgi kasıtlı olarak manipüle edilmiş veya bozulmuşsa bu durum İnsan Hakları Evrensel Beyannamesine aykırıdır. Bazı durumlarda dünya genelinde hükümetler, çevrimiçi içeriği kısıtlamaya, engellemeye veya gözetlemeye olanak tanıyan, sansür ile basın ve diğer medya özgürlüğünü kısıtlayan yasalar ve yönetmelikler uygulayarak bireylerin mahremiyet, bilgiye erişim ve ifade özgürlüğü hakkını sınırlamaktadır.

Siber savaş bilgi savaşını da içinde barındırmaktadır. Amacı ise siber yeteneklerle, bilgi alanında etkiler yaratmak, bilgiye erişimi değiştirmek, bölünme ve anlaşmazlık oluşturmak, siyasi bir aktöre veya anlatıya yönelik halk desteğini aşındırmaktır. Bu faaliyetler doğrudan ifade özgürlüğü üzerinde etkisi olan eylemlerdir. Bu düşünce tarzı özellikle Çin ve Rusya gibi ülkelerde ön plana çıkmış ve Batı ile Doğu arasındaki farklı siber savaş anlayışının temelini oluşturmuştur (Burton,

2019, s. 122). Çin, Rusya ve İran'ın çevrimiçi ifade özgürlüğüne yönelik kısıtlayıcı yaklaşımları, "siber egemenlik" kavramının savunulması yoluyla uluslararası sahneye yansımıştır. Çevrimiçi ifade özgürlüğü konusundaki tartışmalar, teknoloji yönetişimi hakkında açık ve küresel mi yoksa kapalı ve devlet temelli mi olması gerektiğine dair geniş jeopolitik tartışmaların giderek daha fazla gündemine girmektedir (Moynihan & Patel, 2021).

Suudi Arabistan Siber Suçlarla Mücadele Yasası ve "*kamu yararının, ahlakın ve ortak değerlerin korunmasına*" ilişkin muğlak hükmü, farklı görüşleri dile getiren, kamu görevlilerine hakaret eden veya iktidardaki hükümet dışı güçleri destekleyen yazarları hapse atarak çevrimiçi konuşma ve ifade özgürlüğünü kısıtlamak için kullanılmıştır (Rossini, Green, & Knowledge, 2011, s. 15).

Çin'in Siber Güvenlik Yasası, internet kullanıcılarının ulusal onuru zedeleyen, ekonomik ve sosyal düzeni bozan, sosyalist sistemi devirmeyi amaçlayan bilgilerin yayınlanmasını yasaklamıştır. Yasa çerçevesinde çevrimiçi platformların çalışmasına izin verilebilmesi için devletin koyduğu kısıtlamalara uyması ve siyasi, sosyal ve dini söylemler üzerindeki sert kısıtlamaları uygulamada işbirliği yapması gerekmektedir (Moynihan & Patel, 2021). Eylül 2017'de Siber Uzay İdaresi, Baidu, Tencent ve Weibo'yu "yanlış söylentiler" üzerine yasaklanmış içeriği tespit edemedikleri ve kaldırmadıkları için ülkenin siber güvenlik yasaları çerçevesinde azami para cezalarıyla cezalandırılmıştır (Abrougui, 2019). Aynı zamanda internet servis sağlayıcılarının da talep edildiği takdirde Çin ulusal güvenlik kurumlarıyla işbirliği yapması gerekmektedir. Örneğin, 2017'de Apple, VPN'ler yeni düzenlemelere uymadığı için yasal olarak zorunlu olduğu gerekçesiyle Çin'deki çevrimiçi mağazasından 60 VPN uygulamasını kaldırmıştır (BBC, 2017a).

2017 itibarıyla Çin'in kamuoyunu parti çizgisi çerçevesinde şekillendirmek için istihdam edilen 500.000 ila 2 milyon internet yorumcusu olduğu bildirilmiştir (Moynihan & Patel, 2021). Çin'in bu stratejileri, ifade özgürlüğünü sınırlamakta ve bireylerin doğru bilgiye erişimini engellemektedir.

4.1.2. Özel Yaşamın Gizliliği ve Kişisel Verilerin Korunması

İnsan Hakları Evrensel Beyannamesinde özel hayatın gizliliği, *"hiç kimsenin özel hayatına, ailesine, konutuna veya haberleşmesine keyfi olarak karışamaz, şeref ve adına saldırılamaz. Herkesin bu tür müdahale veya saldırılara karşı hukuk tarafından korunma hakkı vardır"* maddesiyle açıklanmıştır (UN, 1948). Mahremiyet kavramının üç yönü vardır; (I) bir kişiyi çevreleyen yakın fiziksel alanı koruyarak (bölgesel mahremiyet), (II) bir kişiyi fiziksel aramalar veya ahlaki duygusunu ihlal eden bilgiler gibi gereksiz müdahalelere karşı koruyarak (bireysel mahremiyet); (II) kişisel verilerin toplanabileceğini, saklanabileceğini, işlenebileceğini veya seçici olarak dağıtılıp dağıtılmayacağını ve nasıl yapılacağını kontrol ederek (bilgi mahremiyeti) (Fischer-Hübner, 1998, s. 422).

Veri koruma, kişisel verilerin mahremiyeti sağlamak amacıyla korunmasıdır ve mahremiyet kavramının bir parçasıdır. Bireysel bilgi mahremiyeti, Alman Anayasa Mahkemesi tarafından 1983 tarihli Sayım Kararında, bir kişinin kişisel verilerinin açıklanmasını ve kullanılmasını ilke olarak kendi takdirine bağlı olarak belirleme hakkı anlamına gelen *"bilgisel olarak kendi kaderini tayin hakkı"* terimi olarak tanımlanmıştır. Bilgisel olarak kendi kaderini tayin hakkını korumak için, birçok Batılı devletin ulusal mahremiyet yasaları, farklı bilgisayar topluluklarının etik kuralları ve ayrıca uluslararası mahremiyet kılavuzları veya direktifleri (AB Veri Koruma Direktifi, AB Direktifi 1995 vb.) kişisel veriler toplanırken veya işlenirken temel gizlilik ilkelerinin garanti edilmesini zorunlu kılar (Fischer-Hübner, 1998, s. 422).

Küresel bilgi toplumunda mahremiyet ciddi şekilde tehlike altındadır. Ulus devletlerin ortada herhangi bir suç unsuru olmadan, ulusal güvenlik ve terörizm gerekçesini öne sürerek bireyleri izlemesi veya sosyal medya aracılığıyla kişisel bilgilerini izinsiz olarak kullanması gibi durumlar, insan hakları ihlallerine örnektir. Bu ihlaller sadece ulus devletler tarafından değil, özel şirketler tarafından da gerçekleştirilebilir. Örneğin, kişisel bilgilerimizin özel şirketler tarafından depolanması ve şirketler arasında satılması veya izinsiz bir şekilde devlete paylaşılması veri gizliliğini ihlal eden durumlar arasındadır (Yılmaz, 2026, s. 283).

2015 yılında Paris'te gerçekleşen Charlie Hebdo saldırılarından bir hafta sonra, eski İngiltere Başbakanı David Cameron, İngiliz istihbarat teşkilatlarının mesajlara ve

kullanıcı verilerine daha fazla erişim sağlamaması halinde Whatsapp gibi şifreli mesaj servislerinin yasaklanmasını desteklediğini açıklamıştır. Cameron, İngiltere'yi saldırılardan korumanın bir yolu olarak şifreli mesajlara erişimin artırılması gerektiğini vurgulamıştır. Şifreli mesaj hizmetlerinin yasaklanması, siber güvenlik ve çevrimiçi gözetim yoluyla ulusal güvenlik adına hem mahremiyet hakkının hem de çevrimiçi anonimlik hakkının ihlali olarak görülebilir. Mahremiyet hakkı, tüm insanların kendileri hakkında bilgileri, bu bilgilere sahip olmak istemedikleri kişilerin ellerinden uzak tutmalarına izin verir (Rossini, Green, & Knowledge, 2011, s. 15).

Siber Güvenlik Bilgi Paylaşım Yasası (CISA), 2015'te yürürlüğe giren bir ABD federal yasasıdır. Birincil amacı, siber güvenlik tehditleri ve güvenlik açıklarıyla ilgili olarak devlet ve özel kuruluşlar arasında bilgi paylaşımını teşvik ederek siber güvenliği iyileştirmektir (CISA, 2015a). Yasa, özel kuruluşların siber güvenlik tehdidi bilgilerini İç Güvenlik Bakanlığı da dahil olmak üzere çeşitli devlet kurumlarıyla paylaşılmasına olanak tanımaktadır. CISA'nın arkasındaki amaç siber güvenliği artırmak ve kritik altyapıyı korumak olsa da, insan hakları, aşırı gözetim ve mahremiyet üzerindeki potansiyel ihlaline ilişkin endişeler dile getirilmektedir. Ayrıca yasada, siber güvenlik tehditleriyle ilgisi olmayan bilgilerin de toplanmasına ve paylaşılmasına yol açabilecek geniş bir dil kullanılmıştır.

4.2. Siber Uzayda Uluslararası Hukukun Uygulanmasındaki Zorluklar

Gürcistan ve Estonya'ya yönelik siber saldırı örnekleri sosyal, ekonomik ve fiziksel açıdan yıkıcı sonuçlar vermiştir. Rusya ve Gürcistan arasındaki savaşta Gürcistan'a yönelik gerçekleştirilen siber saldırı, konvansiyonel savaşı desteklemek amacıyla bir araç olarak etki göstermiştir. 2007 yılında Estonya'ya yönelik devlet ve banka kurumlarının hedef alındığı siber saldırı hem maddi zarar hem de bireylerin hayati tehlikesini neden olabilecek boyutta gerçekleşmiştir. Siber uzayda gerçekleşen saldırılar, bilişim sistemini doğrudan etkilerken, oluşturduğu zarar sistemlerden hizmet alan kişileri de doğrudan etkilemektedir. Sonuç olarak siber saldırıların doğurduğu sonuçlar toplumu yakından ilgilendirdiği için karşılığında alınacak önlemler uluslararası hukuk ve savaş hukuku alanına girmektedir (Özkan, 2021).

Mevcut uluslararası hukuk normları, devlet faaliyetlerini yönetir. Ancak var olan uluslararası hukuk normlarının mevcut teknolojiye uygulanması, siber saldırıları önlemek veya yönetmek için uluslararası hukuk normlarındaki yasal boşlukları ve zorlukları beraberinde getirmektedir. Ayrıca internetteki iletişim ve ticareti desteklemek amacıyla çeşitli uluslararası hukuk normları mevcut olsa da, bu normlar silahlı çatışma hukuku içerisinde yer almamaktadır. Uluslararası hukukun siber uzayda nasıl uygulanabileceğine dair farklı bakış açıları da, bu alanda anlaşma olasılığını zorlaştırmakta ve kötü niyetli aktörler tarafından istismar edilmek üzere yasal bir boşluk riski doğurmaktadır (Moynihan, 2020).

Uluslararası hukuk, devletlerin diğer devletlerin haklarına aykırı bir eylemler bulunmasına izin vermemelerini sağlamak için izlenilmesi gereken davranış kurallarını sunmaktadır. Ancak siber saldırı konusunda -Avrupa Konseyi Budapeşte Sözleşmesi dışında- herhangi bir anlaşma mevcut değildir. Dolayısıyla bu aşamada, uluslararası kuralların ana kaynağı olarak genel bir devlet uygulaması olan teamül hukukuna güvenilmektedir (Moynihan, 2020).

4.2.1. Kuvvet Olarak Nitelendirilmesi

BM Şartı'nın 2. maddesinin 4. fıkrasına göre *"bütün üyeler, herhangi bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı veya BM'nin amaçlarıyla bağdaşmayan herhangi bir şekilde kuvvet kullanma veya kuvvet kullanma tehdidinden kaçınacaklardır"* ibaresi siber operasyonların bu yasak dahilinde ne ölçüde "kuvvet" olarak nitelendirileceği sorusunu ortaya çıkarmaktadır (Melzer, 2011, s. 6). Çünkü siber saldırıların, sınırları belirli olmayan bir alanda ve anonim olarak gerçekleştirilmesi gibi benzersiz ve karmaşık özellikleri, hukukta uygulama zorluklarına sebep olmaktadır.

BM Şartı'nın 2. maddesinin 4. fıkrasında belirtilen "kuvvet" kullanımı kinetik, kimyasal, biyolojik veya nükleer silahların uygulanmasıyla sınırlı olduğu anlamına gelemez. Zira siber operasyonların saldırı veya savunma amaçlı kullanılması kişilerin yaralanmasına veya ölümüne ya da altyapıların yok edilmesine sebep olabilecek bir kuvvet kullanımını da içerebilir. Bir nükleer güç istasyonunda erimeye sebep olabilecek şekilde bilgisayar sistemlerini etkilemek, büyük şehirlerin elektrik santrallerini devre dışı bırakmak, kötü hava koşullarında havaalanının hava trafik

kontrolünü devre dışı bırakmak amacıyla gerçekleştirilen siber operasyonlar kişilerin ölümlerine, yaralanmasına veya altyapının yıkımı açısından potansiyel olarak kuvvet kullanımını içeren eylemlere örnektir (Melzer, 2011, s. 7).

1974 tarihli 3314 Sayılı BM Genel Kurul Kararı, BM Şartı 2(4)'ü desteklemek için saldırganlığın tanımını detaylandırır: "*Saldırı, bir devlet tarafından başka bir devletin egemenlik, toprak bütünlüğü ve siyasi bağımsızlığına karşı veya bu tanımda belirtildiği gibi BM Şartı ile tutarsız herhangi bir şekilde güç kullanılmasıdır.*" Bu tanıma atıfta bulunarak, saldırganlık ister siyasi ister bölgesel olsun, bir müdahale eylemidir. Ancak 3314 Sayılı BM Genel Kurul Kararı saldırı eyleminden bahsetmiştir ve siber saldırı bunlardan biri değildir. Bununla birlikte, siber silahların evrimi bir savaş veya siyasi baskı aracı olarak kullanılabilir ve yine bu karar, saldırının ne kadar ileri gidebileceğini açıkça sınıflandırmadan, saldırının devam etmesine yol açabilecek bu yeni silahları yeterince ele almakta başarısızdır (Zahra vd., 2021, s. 36).

4.2.2. Meşru Müdafaa

Meşru müdafaa durumu siber saldırılar bağlamında en çok tartışılan konulardan biridir. BM Şartı'nda 51. maddede belirtilen meşru müdafaa durumu için yalnızca silahlı saldırı veya saldırının önemli olması gerekir ve meşru müdafaa'nın yürütüldüğü devlete atfedilebilir olması, kuvvet kullanımının son çare olması, savunmayı sağlamada başarılı olması ve maruz kalınan yaralanma ile orantılı olması şartları sağlanmalıdır. Ancak bilgi teknolojilerinin gelişmesi savaş ve çatışmaların giderek daha fazla asimetrik bir karaktere sahip olduğunu göstermektedir. Dolayısıyla bu koşulların siber saldırı eylemlerine uygulanabilirliği imkansız değilse de zor sayılmaktadır. Örneğin maddi olarak nesnelerde zarar oluşturan İran'a yönelik Stuxnet saldırısında oluşan zarar, 51. madde için geçerli olan "önemli olması" şartını tam olarak karşılamamaktadır (O'Connell, 2012). Ancak uzman gruplarca hazırlanan Tallinn Klavuzu, Stuxnet saldırısının "silahlı saldırı" olarak sınıflandırılabilir yakın bir vaka olduğu konusunda atıfta bulunmuştur. Çünkü fiziksel hasara yol açan bu saldırı silahlı saldırı tanımına girmektedir (Hayward, 2017). Gürcistan ve Estonya örneklerinde ise elektronik sistemleri aksatan DDoS saldırıları, önemli kalıcı hasarlara sebep vermediği için baskın görüş sonucunda silahlı saldırı olarak ilan edilmemiştir.

Egemen bir devletin saldırıya uğradığını hissetmesi durumunda güçlü bir şekilde karşılık vermesi doğal bir haktır. Ancak bir devletin siyasi bağımsızlığına yönelik saldırganlık ifadesi dikkate alındığında, silah olarak "siberin kullanıldığı bir çatışmada, ne tür bir etkinin medyana geldiğine ve silahların nasıl serbest bırakıldığına dikkatlice bakılmalıdır (Zahra vd., 2021, s. 57). Dolayısıyla siber saldırıların, zarar verici sonuçları olabileceğinden BM Şartına göre silahlı olarak nitelendirilme potansiyeline sahip olduğu ve meşru müdafaaanın somut olarak nasıl uygulanacağı konusundaki anlaşmazlık devam etmektedir (Pangrazzi, 2021).

Benzer şekilde, saldırganın büyük miktarda hedef ağlara yönelik DDoS saldırıları genellikle işlevselliği engeller, dolayısıyla şimdiye kadar doğrudan insan ölümlerine veya yıkıma neden olan silahlı saldırı gereksinimini karşılayacak siber saldırı kaydı bulunmamakta. Ayrıca şimdiye kadar DDoS saldırılarına maruz kalan hiçbir devlet, bu saldırıları silahlı saldırı olarak ilan etmemiş olmasının etkisiyle de ileriye dönük olarak silahlı olarak sınıflandırılması pek olası değildir (Hayward, 2017).

4.2.3. Ayırt Etme İlkesi ve Siber Saldırıların Anonim Yapısı

Siber saldırılar sadece devletler tarafından değil, tüm aktörler ve şahıslar tarafından gerçekleştirilebilmesi, bu saldırıların suçun tespitini zorlaştırmaktadır. Bu bağlamda siber saldırılar karşısında savaş hukuku normlarının uygulanabilirliğindeki diğer bir zorluk ise, siber saldırıların gerçekleştiği anda ikna edici kanıtların bulunmasının zorluğudur. Siber saldırıların anonim yapısı göz önüne alındığında saldırıyı yönlendiren kişinin, devletin veya örgütün tanımlanması çok zordur ve saldırı bir duruma veya kişiye atfedilememektedir. Bir eylemde herhangi bir devletin kaynak gösterilebilmesi için, söz konusu eylemin o devlet *de facto* ve *de jure* organları ya da ajanları tarafından gerçekleştirildiğinin ispat edilmesi gerekmektedir (Güntay, 2019, s. 102). Estonya ve İran örneklerinde görüldüğü gibi bilgisayar ağlarına saldıranları tespiti gerçekleştirilememiş ve kuvvet kullanma hakkı (*jus ad bellum*) işletilememiştir.

4.2.4. Gereklilik ve Orantılılık İlkeleri

Gerçekleştirilen siber saldırı eylemin bir örgüt, birey veya devlete atfedilememesi yanında "gereklilik" ve "orantılılık" ilkelerinin karşılanması zorluğunda mevcuttur. Çünkü bu tür karşı saldırıda, savunma amacına ulaşabileceğini kanıtlama sorunu vardır ve bir bilgisayar uygulaması kullanılarak gerçekleştirilen meşru müdafadaki karşı saldırıların amaçlanan hedefle sınırlandırılması zor olacaktır (O'Connell, 2012). Ancak siber saldırıların, silahlı saldırı olarak nitelendirilememesi, uluslararası hukukun bu tür saldırılara yönelik yasası olmadığı anlamına gelmez. Çünkü bir devletin deniz, hava ve kara sahasına, ekonomik alanına yönelik gerçekleştirilen saldırılar "müdahale etmeme ilkesi" gereğince yasaktır.

Orantılılık ve gereklilik ilkelerinin siber saldırılar için uygulanmasındaki ayrıntılar Tallinn El Kitabında açıklanmış olsa da, sivilleri ve sivil nesneler için yeterli değildir.

(I) siber savaşta sivil bir nesneyi askeri hedefe karşı neyin oluşturduğuna ilişkin tanımın uygulanması ve kapsamı, özellikle veriler ve siber sistemlerin işlevselliği açısından belirsizdir; (II) bir saldırıyı neyin oluşturduğunun tanımı kinetik olmayan etkileri yeterince açıklamaz (III) siber savaşta hasarın tanımı ve hasarı hesaplama kılavuzu belirsizdir; (IV) Bir orantılılık analizinde dolaylı etkilerin ne ölçüde dikkate alınması gerektiğinin değerlendirilmesi için bir kılavuz eksikliği vardır (Pascucci, 2017, s. 420).

Uluslararası hukuk normlarının, siber uzayda uygulanabilirliğinin zor olmasının yanında, son yıllardaki giderek artan bir şekilde birçok devlet, mevcut uluslararası hukukun siber uzayda nasıl uygulanacağına yönelik görüşlerini yayınlamıştır.

4.3. Uluslararası Hukukun Normlarının Siber Uzaya Uygulanması

Yönündeki Girişimler

Mevcut uluslararası hukukun, siber alanda devletlerin davranışlarına uygulanabileceği görüşü birçok uluslararası kuruluş ve devlet tarafından kabul edilse de, bazı devletler pratikte yeni kurallara ihtiyaç olduğunu resmi görüşlerle açıklamıştır. Şanghay İşbirliği Örgütü (ŞİÖ) üyelerinden olan Çin, Kazakistan, Kırgızistan, Rusya Federasyonu, Tacikistan ve Özbekistan, BM'ye hitaben Genel Sekretere yazdığı 9 Ocak 2015 tarihli mektupta "*güçlü bir küresel siber güvenlik kültürünün teşvik edilmesi, geliştirilmesi ve güçlü bir şekilde uygulanması gerektiğini kabul ederek, kritik bilgi*

altyapılarını korumaya yönelik ulusal çabaların değerlendirilmesinin" gerekliliği vurgulanmıştır (UN General Assembly, 2015).

Devletlerin iyi niyetli olmayan siber saldırılarına yanıt olarak artan bir şekilde ittifak halinde ve uluslararası hukuk kuralları çerçevesinde hareket edilmesi yönündeki girişimler de artmıştır. Birleşik Krallık Ulusal Siber Güvenlik Merkezi, Rusya'nın askeri güvenlik teşkilatı olan GRU'nun, uluslararası hukuku açıkça ihlal eden ve Rusya dahil bir çok ülkede vatandaşları etkilediği, ulusal ekonomilere ciddi zararlar verdiği siber saldırılar düzenlediğine yönelik açıklamada bulunmuştu. Bu doğrultuda ise Birleşik Krallık ve müttefiklerinin, uluslararası toplumun diğer hükümetlerinin siber saldırılara karşı duracağını ve bunlara yanıt vermek için birlikte çalışacaklarına yönelik atıfta bulunmuştur (NCSC, 2018b).

AB'nin 19 Haziran 2017'de birlik veya üye devletleri tehdit eden siber saldırılara karşı kısıtlayıcı tedbirlere ilişkin konsey kararında; Siber Diplomasi Araç Kutusu (the Cyber Diplomacy Toolbox) aracılığı ile kötü niyetli siber faaliyetlere yönelik birliğin, üye devletlerin ve vatandaşların bütünlüğünü ve güvenliğini siber saldırılara karşı korumaya yönelik artan ihtiyacını teyit ederek, Ortak Dış ve Güvenlik Politikası kapsamındaki tedbirlerin de dahil edildiği, kötü niyetli siber faaliyetlere karşı ortak bir birlik diplomasisinin uygun olduğu bildirilmiştir. Aynı konsey kararında mevcut uluslararası hukuk normlarının siber uzaya uygulanabilirliğinin güçlü bir şekilde desteklenmeye devam edileceği, uluslararası barış ve istikrarı korumak için başta BM Şartı olmak üzere uluslararası hukuka saygı gösterilmesinin şart olduğu da vurgulanmıştır (EU , 2019).

Devletlerin siber saldırılara karşı ittifak yapılmasına yönelik girişimlerin yanında çok sayıda uluslararası kuruluşlar da uluslararası hukukun, devletlerin siber alandaki faaliyetleri için geçerli olduğunu kabul etmiştir. Bu doğrultuda NATO, Temmuz 2016'da siber uzayı bir operasyon alanı olarak kabul etmiş ve siber uzayın havada, karada, denizde olduğu kadar etkili bir şekilde savunulması gerektiğini ve bu nedenle siber uzayın korunmasının Avrupalı devletler için bir ulusal güvenlik önceliği haline geldiğini belirtmiştir (Napetvaridze & Chochia, 2019, s. 160).

2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren 48 maddelik Avrupa Konseyi Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi), siber saldırıların suç

sayılmasını ve toplumun siber suçlara karşı korunmasını belirterek, bu tür suçlarla etkin bir şekilde mücadele edilmesi için hem ulusal hem de uluslararası düzeyde gerekliliğini vurgulamaktadır (Vatis, 2010). Onaylayan devletlerin *"kendi ulusal hukuklarında tanımlaması gereken temel siber suçlar, devletlerin uygulaması gereken soruşturma prosedürleri ve uluslararası işbirliğini geliştirmeye yönelik mekanizmaların"* ele alındığı üç bölümden oluşmaktadır (Council of the Europe, 2001).

20 Kasım 2017 tarihli 14435 sayılı AB Konseyi kararında ise, siber güvenliğin hem uluslararası hukukun üstünlüğü hem de bireylerin insan haklarını ve temel özgürlüklerinin korunması için önemini belirterek, *"BM Şartı'nın tamamı dahil, uluslararası hukukun ve uluslararası insan hakları hukukunun siber uzayda geçerli olduğunu kabul ederek bu yöndeki çabaların korunmasının sağlanmasının gerekliliğine"* vurgu yapılmıştır (Council of the European Union, 2017).

11 Nisan 2017 tarihli Siber Uzayda Sorumlu Devlet Davranışlarına İlişkin G7 Bildirgesi (Lucca Deklarasyonu) de devlet veya devlet dışı aktörler tarafından Bilgi ve İletişim Teknolojilerinin kötü niyetli kullanımının azaltılmasına yönelik tedbirlerin yanı sıra siber uzayda güvenliğin sağlanması için uluslararası işbirliğinin gerekliliğinin vurgulandığı bir belgedir. Bu bilgide, mevcut uluslararası hukukun özellikle BM Şartı'nın, siber uzayda devlet davranışlarına uygulanabilirliğini teyit etmektedir (G7, 2017). Aynı deklarasyonda yine siber saldırıların güç kullanımının eşiğine ulaşabileceği ve silahlı saldırı olarak değerlendirilebileceği, bu durumda da BM Şartı'nın 51. maddesi uyarınca bireysel veya toplu olarak meşru müdafaa hakkının ileri sürülebileceği ifade edilmiştir.

AGİT'in Daimi Konsey 1092. Genel Kurul toplantısında bilgi ve teknolojinin kullanımından kaynaklanan çatışma risklerini azaltmak için aldığı 1202 sayılı kararında, bilgi ve teknolojinin barışçıl kullanımı için devletlerin işbirliği içinde şeffaf ve istikrar sağlama amacıyla hareket edilmesinin gerekliliği vurgulanmıştır. Bunun yanı sıra bilgi ve teknolojinin kullanımında devletlerin BM Şartı, uluslararası sivil sözleşmeler, siyasi haklar, Helsinki Nihai Senedi temel alınarak insan haklarına ve temel özgürlüklerine saygı gösterme sorumluklarının olduğu vurgulanmıştır (OSCE, 2016).

BM bünyesinde BM Güvenlik Konseyi tarafından siber güvenlik konusuna ilişkin bir karar alınmamış olsa da, Genel Kurul tarafından tavsiye niteliği taşıyan bir takım kararlar alınmıştır. 31 Ocak 2003 tarihli "*küresel bir siber güvenlik kültürünün oluşturulması*" amacıyla alınan 57/239 sayılı Genel Kurul kararında hükümetlerin, işletmelerin ve bireysel kullanıcıların bilgi teknolojilerine artan bağımlılığına dikkat çekerek, bu doğrultuda siber güvenlik ihtiyacının arttığını ve yasal zeminin oluşturulmasına ilişkin devletlerin işbirliği sağlamasını, küresel bir siber güvenlik kültürünün oluşturulması vurgulanmıştır (UN General Assembly, 2003).

2009'da Estonya'nın başkenti Tallinn'de NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi (CCDCOE), Uluslararası İnsancıl Hukuk kapsamında siber savaşın nasıl kapsamlı bir şekilde uygulanması gerektiğini tartışarak siber uzayı yöneten uluslararası hukukun ilk kapsamlı incelemesini yapmak için teknik uzmanlardan oluşan "Uluslararası Uzmanlar Grubu" kurmuştur. Üç yıllık sürecin ardından 2013'te ortaya çıkan "Tallinn El Kitabı (Tallinn Manual 1.0)" içerisinde egemenlik, devlet sorumluluğu, insancıl hukuk ve tarafsızlık hukuku, 1899 Lahey Sözleşmesi ve 1949 Cenevre Sözleşmesi birlikte ele alınmıştır. Söz konusu kitapta "*bir devlet tarafından başka bir devlette bulunan siber altyapıya yönelik siber operasyonların, o devletin egemenliğini ihlal ettiği*" ve uluslararası hukukun ihlali anlamına geldiği sonucuna varılmıştır (Schmitt, 2018). Ek olarak meşru müdafaa konusunda, silahlı saldırı tanımıyla tutarlı bir tanım olan "*insanları yaralayan veya öldüren mülke zarar veren veya tahrip eden herhangi bir güç kullanımının*" silahlı saldırı şartını karşılayacağı konusunda ortak bir görüş ortaya atmışlardır (Hayward, 2017). Ancak Tallin El Kitabı, Uluslararası Adalet Divanı Tüzüğü Madde 38'e göre bir uluslararası hukuk kaynağı sayılmamaktadır (Zahra vd., 2021, s. 58).

"Tallinn El Kitabı 2.0" ise uluslararası hukukun siber alana uygulanmasına ilişkin sunulan analizlerin ikinci baskısı olarak 2017 yılında ortaya çıkmıştır. Siber uzay genellikle sınırsız bir "*küresel ortak alan*" olarak tasvir edilerek devlet egemenliği, devletlerin siber uzay üzerinde uyması gereken genel uluslararası hukuk ilkeleri, siber alan üzerinde yargı yetkisi, uluslararası hukuk kapsamında devletlerin sorumlulukları, devlet dışı aktörlerin siber eylemlerinin durumu, bireylerin hakları ve devletlerin bu haklara yönelik yükümlülükleri, deniz hukuku/hava hukuku/uzay hukuku/uluslararası telekomünikasyon hukuku alanlarında siber operasyonların

yürütülmesine ilişkin sorunları, devletlerin anlaşmazlıkları barışçıl şekilde çözümünün siber faaliyetler içerisinde de geçerli olduğu, siber alanda müdahale etmeme yasağı, siber yollarla güç kullanımına ilişkin sorunlar, BM Güvenlik Konseyi'nin siber operasyonların barış için bir tehdit oluşturduğunu belirleme hakkını, siber operasyonlara yönelik silahlı çatışma yasalarının uygulanabilirliği konularını içeren yirmi bölümden oluşmaktadır (Tropeano, 2019).

NATO'nun Ocak 2020 tarihli "Siber Uzay Operasyonları İçin Müttefik Ortak Doktrini" siber uzaydaki hareket özgürlüğünün karada ve denizdeki kontrol kadar önemli olduğunu vurgulayarak, BM Şartındaki Silahlı Çatışma Hukuku ilkelerinin silahlı bir çatışma sırasında yürütülen siber operasyonlar için geçerli olmasını ifade etmiştir (NATO, 2020, s. 21).

Uluslararası hukuk normlarının siber saldırılar veya operasyonlar üzerinde geçerli olup olmadığı açık bir tartışma konusudur. Ancak savaş hukuku çerçevesinde silah, araç ve savaş yöntemlerinin kullanımının sınırlanması gibi silahlı çatışmalar sırasında da yürütülen siber operasyonlar için geçerli olduğu konusu Uluslararası Adalet Divanı tarafından da belirtilmiştir (Rodenhauser, 2021).

Şimdiye kadar "siber uzayda sorumlu devlet davranışı" paradigmasında çığır açan bir gelişme olmamıştır, ancak uluslararası hukukun mevcut çerçevesinin siber uzay için geçerli olduğu yönünde genel olarak kabul gören görüşler mevcuttur (Nakashidze, 2020). Sonuç olarak uluslararası hukuk normlarının siber uzaya uygulanıp uygulanmayacağından ziyade asıl sorun, nasıl uygulanacağı konusudur. Ayrıca siber saldırıların yakın geleceği konusunda büyük olasılıkla nükleer savunmaya benzeyeceğini ifade edebiliriz. Bu durumda artan eğilim, ulusların siber savunma sistemlerini diğer ulusların siber saldırılarını caydırmanın bir yolu olarak geliştirmesi olacaktır (Swanson, 2010).

Sonuç olarak her devlet için geçerli olan kurallara ve ortak bir sisteme sahip olmak gelişmiş, az gelişmiş veya gelişmekte olan tüm ülkelerin çıkarıdır. Ancak bir devletin siber saldırıları başka bir devletin egemenliğini ihlal edebilir mi ve devletlerin siber alanda başka bir devlet tarafından uluslararası hukuk ihlaline karşı önlemleri alabilir mi veya alabilirse hangi koşullarda gibi konularda şu anda devletler birbirleriyle çelişmektedir. Bu gibi uluslararası hukuk kapsamına girmesi gereken

konular üzerinde bir uzlaşmaya varılamaz ise kötü niyetli aktörler tarafından istismar edilebilecek bir yasal boşluk doğmakta.

Siber alanda neyin uluslararası örf ve adet hukuku oluşturduğuna dair görüş birliği zaman alacaktır. Devletlerin siber operasyona yönelik yaklaşımları çıkarları doğrultusuna şekillendiği için ortak hareket edilmesini ve bütünlük sağlanmasını zorlaştırmaktadır. Buna rağmen BM'de bu konudaki tartışmalarda görüş ayrılığı olsa da, zamanla kapsayıcı ve küresel hale gelen katılım sağlanabilir.

Devletler ve uluslararası örgütler için önemli olan, belirli siber saldırılardan kimin sorumlu olduğunu belirlemenin verimli yollarını bulmak ve sürekli gelişen siber saldırı sorunlarına yönelik daha şeffaf ulusal politikalar oluşturulması olmalıdır. Siber saldırılar doğrudan insanlara yönelik olmasa da, dolaylı yoldan hem maddi açıdan hem de ölümcül sonuçlara sebep verebilecek potansiyele sahiptir. Dolayısıyla silahlı çatışma grubunda sınıflandırılabilmesi için siber saldırıların etkileri incelenmelidir.

5. ARAŞTIRMANIN YÖNTEMİ VE SWOT ANALİZİ

5.1. Araştırmanın Yöntemi

I. Öncelikle araştırmanın modeli çizilmiştir.

II. Araştırmamızın modeli üzerine genişletilmiş model oluşturulmuştur.

III. Modele dayanarak araştırmanın iki temel problemi oluşturulmuş ve bu iki temel problemlerin alt problemleri bulunmaktadır.

IV. Problemlere yönelik içerik analiz yöntemi uygulanarak bulgular elde edilmiştir.

İçerik analizleri; araştırılan bilginin geniş kitlelere yayılması ve gelecek araştırmaların, politikaların, uygulamaların ve kamu algısının şekillendirilmesinde önemli bir role sahip olan araştırma sentezleridir (Çalık & Sözbilir, 2014, s. 34). Yöntem, doğrudan yazılı belgelerden elde edilen verileri veya içeriği araştırmak ve analiz etmek için uygulanabilir. İçerik analizinde, temel amaç toplanan verileri açıklamaya yardımcı olacak kavramlara ve ilişkilere erişmektir. İçerik analizi sürecinde asıl yapılan işlem, benzer verileri belirli kavramlar ve temalar etrafında birleştirerek, bunları okuyucunun anlayabileceği bir şekilde düzenlemek ve yorumlamaktır. İçerik analizinin aşamalarını incelemeye başlamadan önce ise kullanılan terimleri tanımlamak önemlidir (Karataş, 2015, akt. Yıldırım ve Şimşek, 2008).

Norshahida Noor Zeri ve Noor Nirwandy Mat Noordin'in "Framing Cyberterrorism: A Content Analysis of The New York Times" isimli makalesi, siber terörizm hakkındaki New York Times gazetesinde yayınlanan içeriği analiz etmektedir. Bu makale, içerik analiz yöntemini kullanarak belirli bir konuyu incelemek ve çıkarımlarda bulunmak için örnek olarak verilmiştir. Makalede, içerik analiz yöntemi kullanılarak 2010 ve 2016 yılları arasında The New York Times gazetesinde yer alan siber terörizm ile ilgili haberler tespit edilmiş, siber terörizm teriminin nasıl çerçevelendiği, haber medyası tarafından bildirilen siber terör tehdit türleri ve bu çerçevede ne tür anlamlar taşıdığı araştırılmıştır. Bu çerçevede "cyberattack", "cyberterrorism", "cyberterror", "cyberwarfare" ve "cyberthreat" terimleri etrafında bir anahtar kelime taraması yapılarak, ABD ve diğer ülkelerdeki güncel olaylarla ilgili

haberlerden, teknoloji haberlerinden, fikir yazılarından, siber terörizmin kurgusal filmleri ve eleştirileri dahil özel raporlardan yararlanılmıştır. Araştırmanın bulgularında ise siber terörizm ile ilgili önemli miktarda içerik olduğu, medyanın yeni terörizm biçimine önemli oranda ilgi gösterdiği ve medya tarafından gelecekteki tehdide ilişkin endişelerin ifade edildiği, incelenen anket çalışmalarında %70 oranında siber terörizmin "önemli bir tehdit" oluşturduğu ve The New York Times gazetesinin siber saldırıları öne çıkarmaya hevesli olduğu anlaşılmıştır (Zeri & Noordin, 2017).

İçerik analizi birçok amaç için kullanılmaktadır. Çalışmada ulus devletlerin ve çok uluslu şirketlerin siber uzay üzerindeki odak noktalarını ve etkilerini ortaya çıkartmak amacıyla içerik analiz yöntemi kullanılmıştır. Bu çerçevede ABD, Çin, Rusya ve İran ulus devletlerinin hükümet raporları ve ulusal strateji belgeleri, AB Komisyonu, AB Konseyi, BM Güvenlik Konseyi, BM Genel Kurulu, Uluslararası Adalet Divanı, NATO'nun konuyla ilgili raporları ve kararları incelenmiştir.

Çok uluslu şirketler çerçevesinde ele alınan otomotiv endüstrisi, finansal hizmetler sektörü, telekomünikasyon sektörü ve enerji sektörünün siber uzaya etkilerinin incelenmesi için ilgili web siteleri, finansal raporlar ve endüstriye özgü yayınlardan yararlanılmıştır. Siber güvenlik şirketleri arasında Ustream Security, Kaspersky Lab, Keen Security Lab, Krebs On Security, McKinsey, Mitnick Security'nin ilgili raporlarından ve açıklamalarından yararlanılmıştır.

1. Otomotiv endüstrisinde rekabet karşılaştırması yapmak için Brand Finance'in Otomotiv Endüstrisi 2022 raporundan, çip krizinin otomotiv endüstrisine etkisini incelemek için BBC, Reuters, Financial Times, Asia Financial, The Central News Agency haber sitelerinden, hükümetlerin otomotiv endüstrisi ve çip krizi konusundaki girişimleri için ABD, Çin, Tayvan, Güney Kore ve Japonya'nın resmi hükümet açıklamalarından yararlanılmıştır.
2. Finansal hizmetler sektörünün gelişimini anlamak için Apple, Google, Verizon, AT&T, T-Mobile, Alibaba, Amazon, Baidu gibi teknoloji şirketlerinin; Çin menşeli China Construction Bank, Bank of China, Bank of Beijing; ABD menşeli Bank of America, JP Morgan Chase, Goldman Sachs, Citigroup, American Express, Wells Fargo; Almanya menşeli Deutsche Bank; Lüksemburg merkezli Banking Circle; Hollanda menşeli ABN AMRO;

İspanyol menşeli BBVA gibi geleneksel bankaların finansal teknoloji şirketleri ile işbirlikleri ve girişimleri incelenmiştir.

3. Telekomünikasyon sektöründe 5G teknolojisindeki rekabeti anlayabilmek için Çinli Huawei, ZTE ve Oppo, Güney Koreli Samsung ve LG, İsveçli Ericsson, Finlandiyalı Nokia, ABD'li Apple, Qualcomm ve diğer AT&T, Verizon, Cisco, Japonyalı Sharp şirketleri özelinde inceleme yapılmıştır. Ayrıca ABD ve Çin arasındaki Jeopolitik mücadelenin odağını anlayabilmek için Apple ve Huawei çok uluslu şirketleri ayrıntılı incelenmiştir. Metaverse teknolojisi için Samsung, Apple, Microsoft, Meta çok uluslu şirketlerinin girişimleri örnek olarak seçilmiştir.

Bilgi ve iletişim teknolojileri sektörüne yönelik siber tehditleri daha net anlayabilmek için T-Mobile, Vodafone, Microsoft, Sony Pictures çok uluslu şirketlerine yönelik siber saldırılar ele alınmıştır.

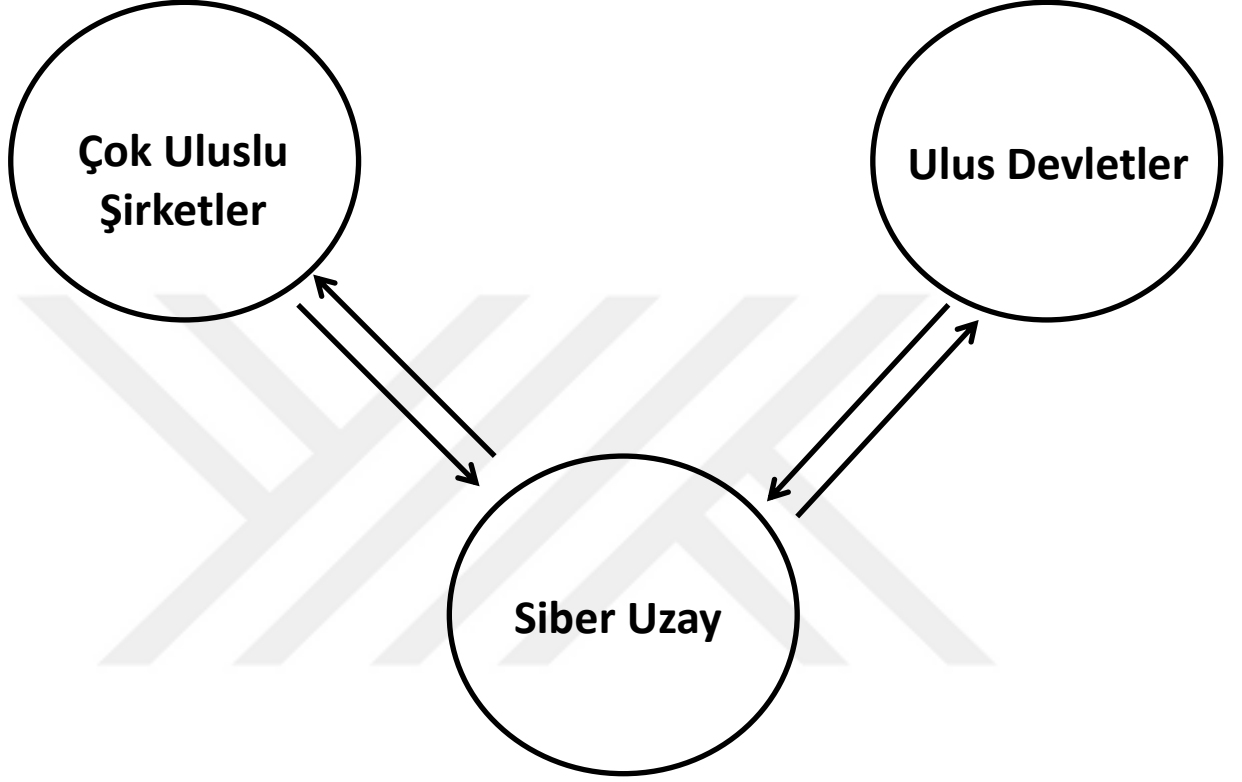
4. Enerji sektöründeki rekabeti ortaya koyabilmek için Birleşik Arap Emirlikleri merkezli ADNOC (Abu Dhabi National Oil Company), İngiltere merkezli BP (British Petroleum), İtalya merkezli Eni, ABD merkezli Chevron ve ExxonMobil, Norveç merkezli Equinor, İspanya merkezli Repsol, İngiltere - Hollanda ortaklığındaki Royal Dutch Shell, Çin merkezli Sinopec, Suudi Arabistan merkezli Saudi Aramco, Fransa merkezli TotalEnergies çok uluslu enerji şirketleri ayrıntılı olarak incelenmiştir. Enerji sürdürülebilirliği, dekarbonizasyon girişimleri ve fosil yakıtlara bağımlılığı azaltmak için AB, Çin, Güney Kore ve ABD'nin resmi yaklaşımları ele alınmıştır.

İçerik analizi sonucunda elde edilen bulgulara uygun olarak belirlenen temalarla çok uluslu şirketler ve ulus devletler için SWOT analizinde örneklendirilmiş ve SWOT analizi ile elde edilen bulgular araştırmanın daha iyi anlaşılması için tartışılmıştır. SWOT analizi, belirli alanlarda organizasyonların rekabet avantajlarını, olumsuz iç faktörleri, stratejik ve taktiksel tehditleri belirlemek ve bu tehditlerden kaynaklanan kayıpları zamanında önlemek için kuruluşun politik, ekonomik, teknolojik, sosyal faktörlerinin kapsamlı bir şekilde incelenmesini içeren bir araştırma yöntemidir. Bu analiz, araştırmanın güçlü yönlerini, zayıflıkların, fırsatların ve tehditlerin kapsamlı bir şekilde açıklamayı amaçlar (Shevchenkoa, Shevchenko, Zhdanova, Spasiteleva, & Negodenko, 2021)

5.2. Araştırmanın Modeli

Şekil 31'de bu çalışmanın modeli gösterilmiştir.

Şekil 31: Araştırmanın Modeli



Kaynak: Şekil yazar tarafından oluşturulmuştur.

Araştırmanın ana hipotezleri (*Çok uluslu şirketlerin siber uzayda etkisi hangi düzeydedir? (P₁) ve Ulus devletlerin siber uzayda etkisi hangi düzeydedir? (P₂)*) bu bölümde çözümlenmiştir. Çok uluslu şirketlerin ve ulus devletlerin siber uzayda "bilgi, güç, hız, güvenlik" temalarıyla etkisi söz konusudur.

Siber Uzay & Çok Uluslu Şirketler: Siber uzay, çok uluslu şirketler için büyük bir bilgi kaynağıdır. Şirketler, siber uzay aracılığıyla pazarlar, müşteriler ve rakip şirketler hakkında büyük miktarda veri toplayabilir, analiz edebilir. Bu, şirketlerin bilinçli iş kararları almalarını, değişen trendlere uyum sağlayabilmelerini ve yenilikçi iş stratejilerini geliştirmeleri sağlar. Ayrıca çok uluslu şirketler genellikle çevrimiçi bilgi paylaşım platformları kurarak küresel işgücü arasında işbirliği ve bilgi alışverişinde bulunabilirler.

Siber uzay, çok uluslu şirketlere güçlü bir rekabet avantajı sunmaktadır. Şirketler, dijital pazarlama, e-ticaret, müşteri ilişkileri yönetimi gibi alanlarda siber uzayı kullanarak küresel çapta varlık göstermektedir. Geniş kaynakları ve küresel erişimleri, çevrimiçi pazarlara hakim olmalarını ve dijital ekosistemleri şekillendirmelerini sağlamaktadır. Çok uluslu şirketler, çıkarlarını savunarak ve dijital ortamı şekillendirerek siber uzayla ilgili düzenlemeleri, standartları ve politikaları etkileyebilir. Ekonomik nüfuzları sayesinde, hükümetlerle müzakere etme ve çeşitli ülkelerdeki dijital altyapının gelişimini etkileme gücü elde etmektedirler.

Siber uzay, çok uluslu şirketlerin güvenliği için hem fırsatlar hem de zorluklar yaratmaktadır. Siber saldırılar, veri ihlalleri, bilgisayar korsanlığı ve fikri mülkiyet hırsızlığı gibi siber tehditler için yeni yollar sağlar. Bu doğrultuda çok uluslu şirketler, değerli varlıklarını korumak ve verilerinin bütünlüğünü, gizliliğini sağlamak için güçlü siber güvenlik önlemleri almak zorundadır. Sunduğu fırsatlar arasında ise çok uluslu şirketler, şifreli iletişim, güvenli ağlar ve gelişmiş kimlik doğrulama sistemleri dahil birçok gelişmiş güvenlik önlemleri için siber uzayı kullanmaktadır.

Siber uzay, çok uluslu şirketlerin benzeri görülmemiş bir hızda çalışmasını sağlayarak iletişimi, karar vermeyi ve işlemsel süreçleri kolaylaştırır. İnternet ve dijital teknolojiler ile çok uluslu şirketler, ticari operasyonlarını sınırlar ötesinde anında yürütebilir. Bu hız, tedarik zinciri yönetimini geliştirir, e-ticaret ve diğer platformlar aracılığıyla ürün ve hizmetlerin küresel ölçekte hızla sunulmasını sağlar.

Siber Uzay & Ulus Devletler: Ulus devletler dijital alanda bilginin büyümesine katkıda bulunan Ar-Ge, eğitim ve teknolojik gelişmelere yatırım yapmaktadır. Hükümetler genellikle yeni teknolojilerin geliştirilmesine ve siber uzayda bilgi paylaşımına yol açan inovasyon ve siber güvenlik araştırmalarını teşvik eden girişimleri finanse eder.

Ulus devletler, uluslararası ilişkilerde güç ve etki uygulamalar için siber uzayda faaliyet göstermektedir. Hakimiyetlerini savunmak veya stratejik hedeflerini takip etmek için casusluk, gözetleme ve siber saldırılar gibi çeşitli faaliyetlerde bulunmaktadır. Siber yetenekler, kritik altyapıyı hedef alabildikleri, iletişim ağlarını bozabildikleri veya hassas bilgileri çalabildikleri için ulus devletlere güçlerini yansıtmak için araçlar sağlamaktadır. Ayrıca ulus devletler, dijital dünyayı yöneten

kuralları, normları ve yönetim yapılarını şekillendirmeye çalışmaktadır. Bu etki mücadelesi, uluslararasıdaki güç için daha geniş rekabeti yansıtır ve internet özgürlüğü, veri gizliliği ve devletler arasındaki güç dengesi gibi konular üzerinde etkileri vardır.

Ulus devletler, siber güvenliğin sağlanmasında ve siber tehditlere karşı savunmada çok önemli bir rol oynamaktadır. Hükümetler siber güvenlik stratejileri oluşturur, kaynakları tahsis eder ve ulusal siber uzayın korunmasında sorumlu kurumlar inşa eder. Bu doğrultuda kritik altyapıyı korumakta, siber suçlarla mücadele etmekte ve güvenlik risklerini azaltmak için istihbarat operasyonları yürütmektedirler. Diğer yandan siber uzayın birbirine bağlı doğası, ulusal güvenliğe yeni zorluklar getirmektedir. Devlet destekli siber saldırılar, bilgisayar korsanlığı ve diğer suç faaliyetleri hükümetlerin ve vatandaşların mahremiyeti için önemli tehditler oluşturabilmektedir. Ulus devletler, güvenlik önlemlerini hem yurtiçinde hem de uluslararası siber tehdit ortamını ele alacak şekilde sürekli olarak uyarlamalıdır.

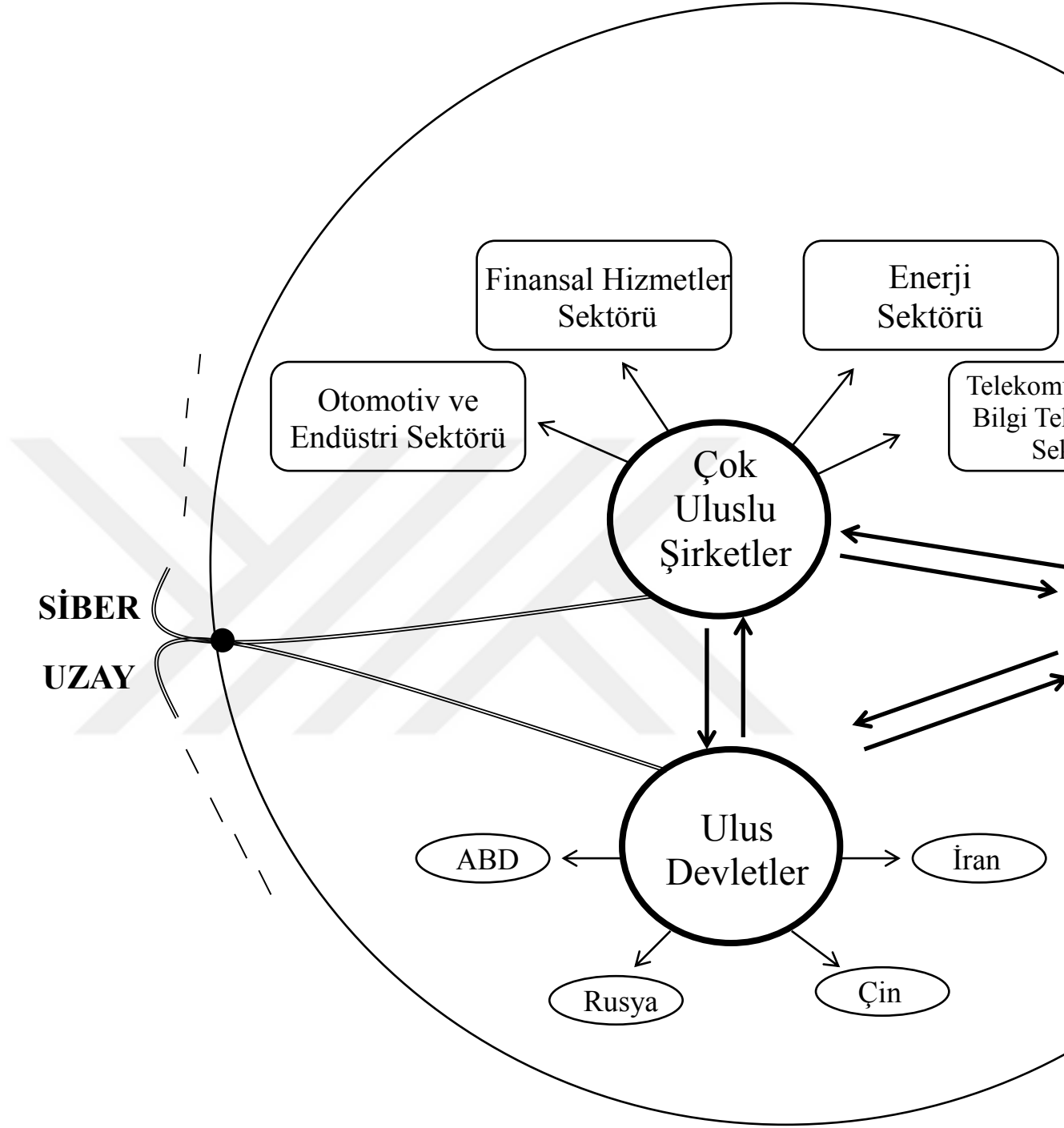
Siber uzay, ulus devletler için hızlı iletişim, işbirliği ve karar alma olanağı sağlar. Bilgiler anında paylaşılabilir ve ortaya çıkan zorluklara veya fırsatlara hızlı yanıt verilmesinde olanak tanır. Hükümetler, politikaları yaymak, vatandaşlarla etkileşim kurmak ve birden fazla kurum arasındaki faaliyetleri koordine etmek için siber uzayı kullanmaktadır. Ayrıca siber uzaydaki teknolojik gelişmelerin hızı, ulus devletler için hem fırsatlar hem de zorluklar sunmaktadır. Yapay zeka ve blok zinciri gibi gelişen teknolojiler, yönetim, ekonomi ve güvenliğin çeşitli yönlerinde devrim yaratma potansiyeline sahiptir. Devletler, rekabetçi kalabilmek ve ortaya çıkan tehditleri etkili bir şekilde ele almak için teknolojik değişimin hızına uyum sağlamalıdır.

5.3. Araştırmanın Genişletilmiş Modeli

Siber uzayda çok uluslu şirketlerin ve ulus devletlerin etkilerinin yanı sıra çok uluslu şirketler ve ulus devletler arasında da siber uzayda karşılıklı bir ilişki söz konusudur. Aynı şekilde uluslararası hukukun da siber uzayda etkisi söz konusudur.



Şekil 32: Araştırmanın Genişletilmiş Modeli



Kaynak : Şekil yazar tarafından oluşturulmuştur.

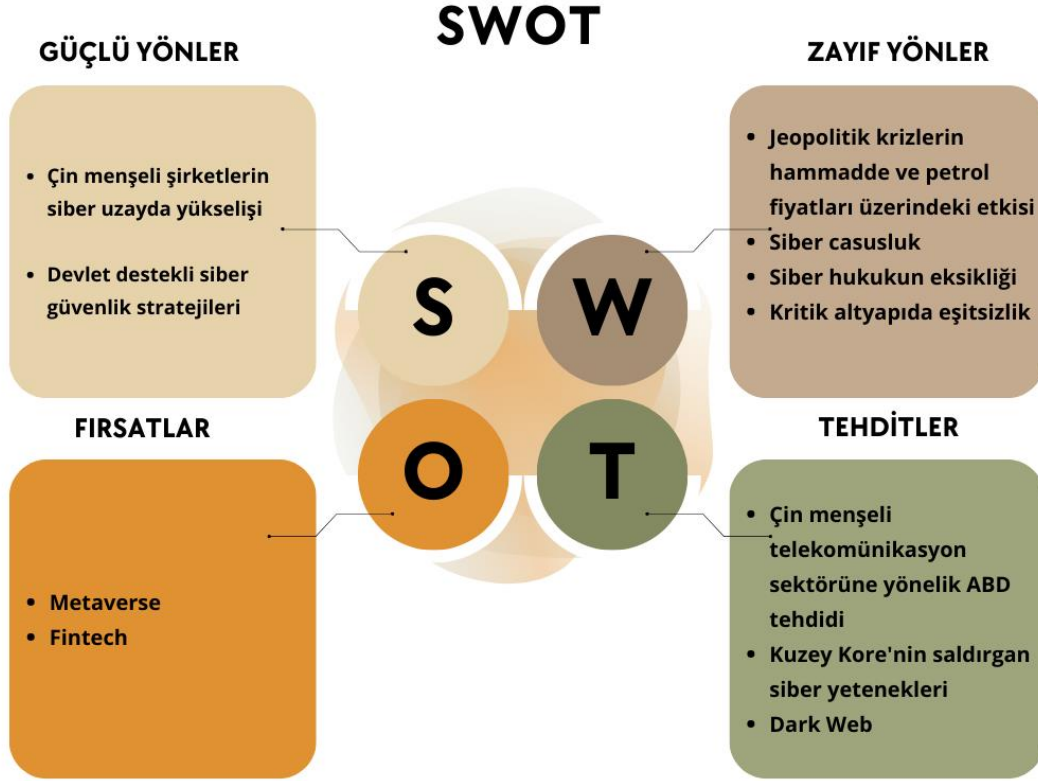
Uluslararası hukukun; çok uluslu şirketler ve ulus devletler açısından siber alandaki ilişkilerine yönelik anlaşılabilmesi önemlidir. Ancak siber hukuk diyebileceğimiz bu tartışma sahası hukuki anlamda uluslararası normlar çerçevesinde henüz yeterli bir düzeye ulaşamamıştır. Araştırmanın modeline hukuki yöne dair sorunsal da taşınmıştır. Böylelikle genişletilmiş bir model uygulanmıştır.



5.4. Ulus Devletler için SWOT Analizi

Şekil 33'te şirketler ile ilgili SWOT analizi şekli verilmiştir.

Şekil 33: Devletler SWOT Analizi



5.4.1. Güçlü Yönler

Çin Menşeli Şirketlerin Siber Uzayda Yükselişi; Kara, deniz, hava ve uzay dışındaki beşinci rekabet alanı olarak siber uzay, küresel stratejik bir rekabet alanı haline gelmiştir. Dünya ekonomisi sadece ulus devletler tarafından değil, aynı zamanda çok uluslu şirketler tarafından da şekillenmektedir. Bu çok uluslu şirketler ticareti yönlendiren, gelir oluşturan, araştırma ve geliştirmeyi desteleyen ulusal ekonomik gücün kritik unsurlarıdır. Çin hükümeti de siber uzayda dijital güç olma hedefiyle çok uluslu şirketlere çeşitli sübvansiyonlar, teşvikler ve politikalar sağlayarak bilgi ve iletişim teknolojileri endüstrisini aktif olarak desteklemektedir. Bu destek Çin menşeli teknoloji şirketlerinin gelişmesine yardımcı olmaktadır. Ayrıca Çin'deki işçilik maliyetlerinin diğer ülkelere nispeten düşük olması, Çinli BİT

şirketlerine ürünleri daha düşük maliyetle üretmesi ve satmasına olanak tanıyarak hem iç pazarda hem de küresel pazarda maliyet avantajı sağlamaktadır. Tüm bu etkenler Çinli BİT şirketlerinin büyük ölçekte hızlı üretim sağlayan iyi gelişmiş bir üretim üssüne sahip olmasını, hızlı inovasyonları ve değişen pazar taleplerine hızla uyum sağlama yeteneklerini olumlu yönde etkilemesini sağlamaktadır.

Çin hükümetinin, teknolojik yeteneklerini geliştirmesine yönelik Huawei'ye araştırma ve geliştirme için verdiği maddi desteği, ABD'nin küresel teknoloji endüstrisindeki hakimiyetine bir meydan okuma olarak görülmektedir. 2022 verilerine göre ABD dışında 170 ülke ve bölgede faaliyet gösteren Huawei özellikle 5G endüstrisinde, Verizon ve Qualcomm gibi ABD menşeli şirketlere büyük bir rakip olarak görülmektedir (Huawei, tarih yok).

Xiaomi, Oppo ve Huawei gibi Çinli BİT şirketleri, Çin'deki düşük işçilik maliyetleri nedeniyle ürünleri daha düşük maliyetle üretilip sattıkları ve benzer ürünleri daha rekabetçi bir fiyat noktasında sunabildikleri için küresel pazarda büyük bir avantaj elde etmiştir. Dünyanın en değerli ilk 20 teknoloji şirketi arasında yer alan 207,92 milyar dolar piyasa değerine sahip -dünyanın en büyük e-ticaret devlerinden biri- Alibaba ve 395,33 milyar dolar piyasa değerine sahip -en büyük oyun şirketlerinden biri- olan Tencent gibi Çinli BİT şirketleri de önemli oranda iç pazara sahip olmakla birlikte teknolojik uzmanlıkları sayesinde küresel olarak genişleme fırsatını yakalamıştır (CompaniesMarketCap.com, 2023).

Devlet Destekli Siber Güvenlik Stratejileri; BİT alanındaki teknolojik gelişmelerin hızlı gelişimi, fırsatların yanı sıra yeni tehditleri de beraberinde getirmekte ve ulus devletler için siber altyapıya daha fazla bağımlı hale gelmesine neden olmaktadır. Dolayısıyla hükümetler toplumun ve ekonominin işleyişi için önemli varlıklar olarak nitelendirilen kritik altyapıların karşı karşıya olduğu siber güvenlik riskleriyle mücadele etmek için ulusal siber güvenlik ve savunma stratejileri geliştirmektedir.

Ulus devletler, ulusal çıkarları ve ulusal güvenlik öncelikleriyle uyumlu olarak siber güvenlik stratejileri geliştirme yetkisine sahiptir. Ulus devletler siber güvenliğe yönelik çok çeşitli yaklaşımlar benimsemiş olsa da, genel olarak; caydırıcı, önleyici, düzenleyici, iyileştirici, tespit edici amaçlarla oluşturulan kurumlar ve strateji belgeleri ile askeri siber operasyonlar yürütmeyi, siber suçlarla mücadele etmeyi, siber güvenlik

yeteneklerini geliřtirmeyi, kritik altyapı korumasını ve siber diplomasi oluřturulmasını hedeflemektedir. Bu doęrultuda siber tehdit ortamına gre uyarlanmış stratejiler; siber gvenlik teknolojilerine ve yeteneklerine yatırım yapılmasını, lkelerin siber gvenlikle ilgili uluslararası kuruluşlar, zel sektr ve dięer lkelerle iřbirlięi yapmasını, siber saldırıları caydırmak veya siber saldırılara karřı yanıt vermek iin saldırgan siber yetenekler geliřtirmesini iermektedir.

Her lkenin kendi ulusal ıkarları, jeopolitik kaygıları ve i politikaları tarafından ynlendirilen siber gvenlik stratejileri konusunda kendine zg bir bakıř aısı vardır. ABDnin siber strateji belgelerinde genellikle hkmet ve zel sektr iřbirlięine vurgu yapılmaktadır. Trump ynetimi dneminde, nleyici siber saldırılar yoluyla saldırgan siber operasyonları hızlandırma, siber caydırıcılık gcn artırma ve siber misilleme yeteneęini geliřtirme gibi stratejiler belirlenmiřtir. ABD'nin hayati ıkarlarını savunma amacıyla belirlenen siber stratejiler, siber saldırılara hızlı yanıt verme yeteneęi iin saldırıları izleme veya atfedebilme kapasitesine yatırım yapma, evrimii pazarlar ve kripto para birimleri gibi araların kullanımını engellemek iin soruřturma aralarını kullanma, ortak tehditlere karřı caydırıcılıęı glendirmek ve uluslararası gvenlięi korumak iin uluslararası ittifaklar oluřturma gibi prensipler zerine kurulmuřtur. Ayrıca, devletlerin siber uzaydaki uluslararası ykmllklerini nasıl yerine getireceęi konusunda meřru mdafaa ilkesi erevesinde yol haritaları belirleme hedefi de bulunmaktadır.

in, en hızlı byyen dięital ekonomiye sahip olmasının yanı sıra, siber gvenlik stratejisinde temel olarak devlet desteęiyle yerli yksek teknoloji endstrilerini teřvik etme ve yerli yazımı-donanım retimine ncelik verme yaklařımını benimsemiřtir. Bu stratejiyle, in hkmeti siber uzaydaki egemenlięini koruma, internetin rejimi tehdit edici veya ulusal gvenlięe zarar verici řekilde kullanılmasını engelleme, in'in sosyalist ideolojisini evrimii platformlarda glendirmek, siber uzaya eriřimi kontrol altına tutmak amacıyla denetleyici mekanizmaları glendirme, yabancı web sitelerine eriřimi kısıtlama ve politik olarak kabul edilmeyen ierięi filtreleme gibi stratejik hedeflere odaklanmıřtır. Bu hedefler erevesinde in, Byk Gvenlik Duvarı aracılıęıyla siber uzayı kontrol altında tutmaktadır. Ayrıca in'de faaliyet gsteren yabancı řirketlerin siber saldırılara karřı nem almak iin devletten sertifika alma, gvenli ve kontrol edilebilir bir řekilde faaliyet gsterme zorunluluęu bulunmaktadır.

İran'ın ulusal güvenlik stratejilerinin oluşturulmasında baskın liderler, güçlü bir askeri yapı ve güçlü kültürel kimlik baskın unsurlar olarak kabul edilmektedir. Dolayısıyla İran rejiminin siber uzay alanındaki temel amaçları ülke içindeki çevrimiçi faaliyetleri izleme ve kontrol etme, içerik filtreleme, rejime karşı çıkan muhalif unsurların örgütlenme ve iletişim kurma yeteneklerini engelleme, ulusal güvenliklerini korumak için saldırgan siber yeteneklerini geliştirmektir. Ayrıca vatandaşları küresel siber uzaydan ayıran, Şii Müslüman normlarına uygun, hükümetin ağ içeriklerini tamamen kontrol etmesini sağlayan ve yerli internet hizmetleri sunmayı amaçlayan proje çerçevesinde rejimle örtüşmeyen Batılı unsurların İran ağına sızmasını önleme, siber saldırı ve siber casusluğa karşı savunma yetenekleri oluşturmada kilit önemdedir.

Rusya'nın siber strateji belgelerinde, bilgi güvenliğini sağlama, yerli bilgi altyapısını geliştirme, uluslararası işbirliği kurma, uluslararası hukuka uyum, siber tehditlerle mücadele ve dijital egemenlik çerçevesinde devletin kendi topraklarındaki internet üzerinde denetiminin genişletilmesi gibi hedefler önemslenmektedir. Ayrıca Rusya siber stratejilerinde stratejik hedeflere ulaşmak ve ulusal çıkarlarını korumak için siber yetenekler de dahil olmak üzere çeşitli araçların kullanımını vurgulamaktadır. Dolayısıyla Rus hükümeti, Gerasimov Doktrini çerçevesinde, rakip bir ulus devletlerin kritik altyapısını, iletişim ağlarını veya bunlardan yararlanabilecek asimetrik faaliyetler yürüterek savaşma potansiyelini zayıflatmak için geleneksel ve askeri olmayan araçlara izin veren bilgi alanının asimetrik doğasını kabul etmektedir.

5.4.2. Zayıf Yönler

Jeopolitik Krizlerin Hammadde ve Petrol Fiyatları Üzerindeki Etkisi; Son 5 yıldır yaşanan jeopolitik krizler sırasında hammadde ve petrol arzını etkileyebilecek bazı önemli riskler ve kırılmalıklar arasında; askeri çatışmalar, ticari anlaşmazlıklar, bölgesel yaptırımlar ve siyasi istikrarsızlar sayılabilir. Bu zorluklar arz ve talep üzerindeki etkileri nedeniyle yaşanan hammadde kıtlığı ve petrol fiyatlarındaki yükselme hem işletmeler hem de tüketiciler üzerinde önemli etkiler yaratabilmektedir. Arz kesintilerinin yanı sıra, jeopolitik krizler belirli emtialara, özellikle de arz kesintisi riski varsa altın veya petrol gibi güvenli liman olarak görülen alanlara yönelik talebin artmasına neden olabilir, etkilenen bölgelerde hammadde ve petrol tedarikinde aksamalara ve kur dalgalanmalarına yol açabilir. Latin Amerika, Afrika ve Orta Doğu

gibi büyük madencilik ve hammadde üretiminin olduğu ülkelerinde yaşanan herhangi bir siyasi kriz, birçok hammaddenin arzının kesintiye uğramasına ve arzın azalmasını etkileyerek endüstrilerdeki üretimi etkileyebilmektedir. Örneğin 2020'de İran'da Kasım Süleymani suikastı, petrol piyasalarına duyarlılığı artırmış ve jeopolitik konuları yeniden gündeme getirmiştir (Kumar, 2020).

2022'de Rusya'nın Ukrayna'yı işgali ve ardından Rusya'ya yönelik ekonomik yaptırımlar petrol, gaz ve bazı tarım ürünlerinin fiyatlarının artmasına, Rusya'da üretilen bazı endüstriyel uygulamalarda kullanılan (inşaat, elektronik cihaz, uzay araçları, nükleer reaktörler, gıda, uçak ve diğer taşıtlar vb.) önemli metaller arasında yer alan alüminyum, nikel, paladyum gibi hammaddelerin ticaretinin ve küresel piyasaların ciddi bir şekilde etkilenmesine neden olmuştur. Rusya-Ukrayna Savaşı ve ABD-Çin arasındaki ticaret savaşları örnekleriyle yaşanan jeopolitik krizlerin yanı sıra, Covid-19 salgını, artan hammadde fiyatları, çeşitli elektronik ve diğer endüstrilerde kullanılan iletken çip krizine sebep olmuştur.

Jeopolitik krizlerin siber uzayda oluşturduğu zayıflık ise hammadde ve petrol fiyatları üzerindeki etkisini, muhtemelen bu ürünlerin üretimi ve dağıtımında yer alan kritik altyapı ve ulaşım sistemlerine yönelik siber saldırı riskini, siber casusluk, piyasa manipülasyonu, fidye yazılım saldırıları riskini içermektedir. Dolayısıyla devlet destekli aktörler veya diğer siber tehdit aktörleri jeopolitik krizler, küresel tedarik zincirlerinde hammadde ve petrol sevkiyatını kesintiye uğratabilecek siber saldırılara yol açabilir, hammadde ve petrol üretimi veya nakliyesi ile ilgili hassas bilgilerin çalındığı siber casusluk eylemi gerçekleştirebilir, dijital altyapıya yönelik saldırılarla boru hattı veya rafineriye yönelik bir siber saldırıyla önemli fiziksel hasara yol açabilir ve fiyatları etkilemek için yanlış bilgi ile piyasaları manipüle edilebilir.

Siber Casusluk; Son 30 yılda, devlet destekli ve devlete bağlı olmayan siber tehdit aktörlerinin aktif olarak siber casusluk faaliyetlerini kullanması, siber uzayda büyüyen ve önemli bir tehdit oluşturmaktadır. Ulus devletler ve çok uluslu şirketler için siber casusluğun oluşturduğu tehdit, potansiyel siber tehdit aktörlerinin, motivasyonlarını, amaçlarını, siber yeteneklerini ve hassas bilgilere erişim elde etmek için kullanabilecekleri yöntemleri belirlemeyi içermektedir. Bu tehditler, siber casusluğa karşı savunmasız hale getirebilecek -ağ güvenliğindeki zayıf yönler, içeriden

gelen tehditler, üçüncü taraf güvenliğindeki zayıflık, şifreleme ve veri koruma eksikliği gibi- zayıflıkları da beraberinde getirmektedir

Siber casusluk yapan ulus devlet destekli siber tehdit aktörleri, siyasi, ekonomik ve askeri amaçlarla motive olmaktadır. Askeri planlar, hükümet sırları veya kritik altyapı gibi hassas bilgileri hedef alan ulus devlet destekli siber tehdit aktörleri, önemli kaynaklara ve gelişmiş siber araçlara sahiptir ve bu durum onları güçlü bir tehdit haline getirmektedir. Siber casusluk faaliyetleri yürüten ulus devletler genellikle, kritik altyapıya, hükümetin resmi ağlarına ve rakip ulus devlet menşeli çok uluslu şirketlere karşı büyük ölçekli ve hedefli siber saldırılar gerçekleştirmelerine izin veren, gelişmiş teknolojik yeteneklere ve önemli kaynaklara sahiptir. Siber casusluk faaliyetlerinin atfedildiği ve devlete bağlı siber tehdit aktörlerinin bulunduğu ulus devletlerden bazıları Çin, Rusya, Kuzey Kore ve İran'dır.

1996-1997 yılları arasında gerçekleşen Moonlight Maze saldırısı, Rus hükümetine veya Rus devlet destekli siber tehdit aktörlerine atfedilen ve ABD'yi hedef alan devlet destekli ilk büyük çaplı siber casusluk operasyonlarından biri olarak bilinmektedir. Siber saldırıda NASA, Pentagon, üniversitedeki sistemler, silah laboratuvarları, ABD Enerji Bakanlığı ve birkaç Amerikan devlet kurumu hedeflenmiştir. Gizli bilgilerin veri ihlaline yönelik iki yıllık bir süre boyunca gerçekleştirilen saldırıda, silah yönlendirme sistemleri, deniz istihbarat kodları, teknik araştırmalar, askeri haritalar, askeri donanım tasarımları, şifreleme teknikleri ve Pentagon'un savaş planlamasıyla ilgili veriler çalınmıştır (Westby, 2020). Infrastructure Defence'nin baş yöneticisi James Adams, "*çalınan bu bilgilerin değeri on milyonlarca- belki de yüz milyonlarca- dolardır. Bilgiler, en yüksek teklifi verene satılmak üzere internet üzerinden Moskova'ya gönderildi*" ifadelerinde bulunmuştur (FAS, 2000a). Saldırılarda Rus hükümeti sorumlu tutulmuş, ancak Moskova'daki bir IP adresi dışında ABD suçlamalarını destekleyen çok az somut kanıt elde edilmiştir. Bu büyük siber casusluk operasyonunun önemi ve çalınan bilgilerin hassas doğası nedeniyle kanıtlar gizli tutulmuştur.

Siber Hukukun Eksikliği; Siber uzayda uluslararası kabul görmüş hukuk kurallarının bulunmaması kötü niyetli siber aktörler tarafından istismar edilebilecek bir yasal boşluk oluşturmaktadır. Bu zayıflık siber saldırıların atfedilmesine yönelik

zorlukları ortaya çıkarmakta, insan hakları ihlallerine kapı açmakta, siber saldırı olasılığı artırmakta ve ulus devletler arasında güveni zedelemektedir.

Siber uzayda net yasal sınırların olmaması, siber tehdit aktörlerinin ulus devletlere, kritik altyapıya ve çok uluslu şirketlere yönelik siber saldırılar başlatmasını kolaylaştırmakta ve ulus devlet destekli aktörlerin veya diğer tehdit aktörlerinin siber saldırılar gerçekleştirmesi için cesaretlendirmektedir. Bu saldırılar ulusal güvenliğe, ekonomiye ve sosyal düzene önemli zararlar vermektedir. Siber hukukun ve açık kuralların yokluğunda, uluslar siber saldırılara karşı askeri çatışmaya dönüşebilecek misillemeyi tercih edebilir ve bu durum uluslararası sistemi istikrarsızlaştırabilir. Ayrıca siber saldırılar için net bir yasal standartlar oluşturulmadığından, siber saldırıların atfedilmesi zorlaşmaktadır. Bu durumda siber saldırıların belirli bir aktöre atfedilmesi daha zor hale gelir ve sorumlu tarafa karşı misilleme veya cezai önlemler almasını zorlaştırır.

2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren 48 maddelik Avrupa Konseyi Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi), 20 Kasım 2017 tarihli 14435 sayılı AB Konseyi kararı, 11 Nisan 2017 tarihli Siber Uzayda Sorumlu Devlet Davranışlarına İlişkin G7 Bildirgesi (Lucca Deklarasyonu), AGİT'in Daimi Konsey 1092. Genel Kurul toplantısında bilgi ve teknolojinin kullanımından kaynaklanan çatışma risklerini azaltmak için aldığı 1202 sayılı kararı³¹ Ocak 2003 tarihli "*küresel bir siber güvenlik kültürünün oluşturulması*" amacıyla alınan 57/239 sayılı BM Genel Kurul kararı, NATO'nun Ocak 2020 tarihli "Siber Uzay Operasyonları İçin Müttefik Ortak Doktrini" gibi bilgi ve teknolojinin barışçıl kullanımı ve siber uzayda güvenliğin sağlanması için uluslararası işbirliğinin gerekliliğinin vurgulandığı, mevcut uluslararası hukukun özellikle BM Şartı'nın siber uzayda devlet davranışlarına uygulanabilirliğinin ve yasal zeminin oluşturulmasının vurgulandığı bir çok karar alınmıştır. 2009'da Estonya'nın başkenti Tallinn'de NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi (CCDCOE), Uluslararası İnsancıl Hukuk kapsamında siber savaşın nasıl kapsamlı bir şekilde uygulanması gerektiğini tartışarak siber uzayı yöneten uluslararası hukukun ilk kapsamlı incelemesi sonucunda oluşturduğu Tallinn Manual 1.0 ve 2017'de Tallinn Manual 2.0 olarak ikinci baskısı sunulan el kitabı uluslararası hukukun siber alana uygulanmasına ilişkin analizler sunmaktadır. BM Güvenlik Konseyi'nin 2178 (2014) ve 2396 (2017) sayılı kararları da üye devletlerin, teröristlerin teknoloji ve iletişimi terör eylemleri için kullanmasını

önlemek amacıyla ulusal önlemler alınırken aynı zamanda uluslararası işbirliği içinde hareket edilmesinin gerekliliğini vurgulamaktadır (UNCCT, tarih yok).

İnsan hakların çerçevesinde ise BM İnsan Hakları Evrensel Beyannamesi ve Uluslararası Medeni ve Siyasi Haklar Sözleşmesi kapsamında güvence altına alınan, ifade özgürlüğü, mahremiyet hakkı, düşünce özgürlüğü ve örgütlenme özgürlüğü tüm insanların en temel hakları arasındadır. Ancak hükümetlerin uyguladığı siber güvenlik yasaları, insan hakları ve özgürlükleri üzerinde olumsuz bir etki yaratmakta ve doğrudan bir ihlal oluşturmaktadır.

Siber hukukun oluşturulamaması, insan haklarının daha geniş ölçekte ihlal edildiği durumlar yaratmaktadır. Bu ihlalde bireylerin mahremiyet haklarının korunamamasından daha kötü oluşacak senaryo, ulus devletlerin kritik altyapılarına yönelik gerçekleştirilen bir siber saldırıda bireylerin yaşam hakları ihlal edilebilir. Sağlık sistemleri, finansal hizmetler veya elektrik şebekeleri gibi kritik altyapıların zarar görmesi toplumda önemli kayıplara yol açmaktadır. Örneğin 2007'de ilk modern siber saldırı niteliği taşıyan Avrupa'nın en kablolu ülkesi olarak bilinen Estonya'ya karşı gerçekleştirilen saldırı sonucunda büyük bir mağduriyet yaşanmıştır. Devlet kurumları, finansal sistemler, ulaşım sistemleri çökmüş ve Avrupa ülkeleri Estonya'ya konvansiyonel savaş sonucundaki zararların iyileştirilmesi sürecinde yardım etmiştir. Ancak siber saldırı sonucunda yaşanan veri kayıplarının iyileştirilmesi için etkili bir süreç yürütülememiştir. Özellikle siber saldırılar sonucu veri kaybı yaşandığında, bu kayıpların hukuki süreçleri yetersiz kalmakta ve uluslararası arenada etkin bir koruma mekanizması bulunmamaktadır. Ulus devletler ve uluslararası örgütler tarafından bu konu zaman zaman ele alınmış olsa da, veri kaybı gibi siber saldırı sonuçlarının cezalandırılması konusunda henüz bağlayıcı kararlar ele alınmamıştır.

Kritik Altyapıda Eşitsizlik; Kritik altyapı teknolojisi için küresel bir ağ altyapısının olmaması, siber güvenlik açısından çeşitli zorluklar ve zayıflıklar sunmaktadır. Dolayısıyla ulus devletlerin kritik altyapı teknolojilerinin siber güvenlik hazırlığı, siber güvenliğe yatırım düzeyi, altyapının karmaşıklığı ve siber tehditlerin karmaşıklığı gibi faktörlere bağlı olarak büyük ölçüde değişiklik göstermektedir. Ülkelerin kritik altyapılarının ve siber güvenliklerinin kalitesine göre kesin olarak sıralama yapmak zordur. Bununla birlikte, bazı ülkelerin diğerlerine göre daha zayıf kritik altyapıya ve siber güvenlik sistemlerine sahiptir.

Zayıf kritik altyapıya sahip ülkelerin örneklerinden biri İran'dır. İran, 2010 yılında ülkenin nükleer programına zarar veren Stuxnet virüsü de dahil olmak üzere, uzun bir süre çok sayıda siber saldırılarla karşı karşıya kalmıştır. Ayrıca elektrik şebekesi dahil olmak üzere zayıf kritik altyapısı nedeniyle de eleştirilmektedir. Ukrayna 2017'de ülkenin altyapısına önemli ölçüde zarar veren NotPetya kötü amaçlı yazılım saldırısı da dahil olmak üzere birçok büyük siber saldırının kurbanı olmuş ve enerji sektörü de dahil olmak üzere kritik altyapısıyla ilgili zorluklarla karşı karşıya kalmıştır. Venezuela, Bangladeş, Yemen, Haiti, Suriye, Somali gibi ülkeler de yıllar içinde çok sayıda siber saldırıyla karşı karşıya kalan ve zayıf kritik altyapıyla mücadele eden ülkeler arasındadır.

Gelişmiş kritik altyapıya sahip ülkeler arasında yer alan Singapur, kritik altyapı koruması ve siber güvenlik alanında dünya lideri olarak tanınmaktadır. Ülkenin ulusal bir siber güvenlik stratejisi ve kritik altyapının korunması için çalışan Siber Güvenlik Ajansı adıyla özel bir devlet kurumu mevcuttur. Almanya, Japonya, ABD, İngiltere, Çin de siber güvenliğe büyük yatırımlar yapan, gelişmiş kritik altyapı koruma programına, gelişmiş ulusal siber güvenlik stratejisine, siber güvenlik yasalarına ve kritik altyapının korunması için çalışan özel devlet kurumlarına sahip ülkeler arasındadır.

5.4.3. Fırsatlar

Metaverse; Metaverse, çok uluslu şirketler ve ulus devletler için çeşitli potansiyel fırsatların yanı sıra, bu yeni sanal dünyanın ekonomik etkisi ve gelir yaratma olasılıklarını kapsayan bir fırsat içermektedir. Ulus devletler, ekonomik kalkınmayı yönlendirmek için Metaverse platformunda sanal işletmeler ve istihdam fırsatları yaratarak hem dijital ekonomilerin büyümesine katkıda bulunabilir hem de GSYİH'larını artırabilir ve yeni gelir kaynakları yaratabilir. Fırsatlar doğrultusunda daha fazla yatırımı çekmeye yardımcı olabilecek iyileştirilmiş küresel markalaşmanın yanı sıra vatandaşlara yeni çevrimiçi hizmetlere ve kamusal alanlara erişim de sağlamaktadır. Ayrıca ulus devletler, kültürlerini ve miraslarını tanıtmak için Metaverse platformunu kullanmaktadır. Geleneklerini, tarihlerini ve sanatlarını sanal müzeler ile sergileyerek kültürel kimliklerini koruyan ve geliştiren sanal alanlar yaratabilme imkanına sahiptir. Sanal müzelere ek olarak Metaverse platformu, ülkeler

arasındaki diplomatik ilişkiler ve şirketler arasında işbirliği çabaları, zirve toplantıları ve müzakereler için sanal platform görevi görmektedir.

Fintech; Ulus devletler, Fintech endüstrisindeki gelişmekte olan işletmelere destek sağlayarak, yenilikçiliği ve girişimciliği teşvik eden politikalar oluşturarak ulusal ekonomik büyümeyi destekleyebilir, blok zinciri ve yapay zeka gibi teknolojilerin kullanımıyla hükümetlerin finans sektörünü daha etkin bir şekilde düzenlemesine yardımcı olabilir, özellikle finansal işlemleri izlemek, dolandırıcılığı tespit etmenin ve uyumluluğu iyileştirmenin yanı sıra veriler ve analizler sağlayarak riskleri daha etkin bir şekilde yönetmek için araçlar geliştirebilir. Uluslararası ticaret ve yatırım üzerindeki olumlu etkisi ise sınır ötesi işlemlerin maliyetini ve karmaşıklığını azaltmaya yardımcı olabilmesi ve çok uluslu şirketler için nakit akışının iyileştirilmesi için yeni finansman seçeneklerinin sunulmasıdır içermektedir. Genel olarak finansal süreçleri iyileştirmek, maliyetleri düşürmek ve rekabet avantajı elde edilebilmesi için birçok fırsat sunar.

5.4.4. Tehditler

Çin Menşeli Telekomünikasyon Sektörüne Yönelik ABD Tehdidi; Çin ve ABD ilişkileri 21. yüzyılın en önemli ikili ilişkilerini temsil etmektedir. ABD ve Çin arasındaki jeopolitik çatışma, "teknoloji savaşları" adı altında yeni bir çatışma türüne doğru kaymasıyla sonuçlanmıştır. Bu çatışma ABD hükümetinin, Çin'in teknolojik gelişimini sınırlama ve Çinli şirketlerin kilit sektörlerde baskın oyuncular haline gelmesini engellemeye yönelik daha geniş çabaların bir parçası olarak Huawei gibi şirketlerin doğrudan hedef alınmasını içermektedir.

Ulus devletlerin endişesi, Çin'in 2017 Ulusal İstihbarat yasası uyarınca, tüm Çinli şirketlerin ve kuruluşların yasal olarak Çin hükümeti adına istihbarat çalışması yürütülebilme analizinden kaynaklanmaktadır. Bu analize göre istihbarat toplamak ve fikri mülkiyeti çalmak için Huawei'nin 5G ağlarını kullanma yeteneği olduğu ve şirketin hükümet taleplerine boyun eğebileceği ve bir ülke üzerinde baskı uygulamak için ağları devre dışı bırakabileceği konusunda endişeleri beraberinde getirmektedir.

ABD hükümetinin, Huawei'yi ABD şirketlerinin hükümet onayı olmadan Huawei ile iş yapmasını fiilen yasaklayan Varlık Listesi'ne alması, Huawei

alıřanlarına ynelik diplomatik kısıtlamalar getirmesi, in hkmetinin řirket zerindeki potansiyel etkisine iliřkin endiřeler nedeniyle mttefiklerini Huawei'nin 5G aęlarına katılımını sınırlamaya aęırması, Huawei'yi ABD'nin İran'a ynelik yaptırımlarını ihlal etmekle suçlaması, Biden ynetiminde ABD řirketlerinin ip retimi iin kullanılan ekipmanları zel bir lisans almadıkları srece belli inli reticilere satmalarını engelleyen yeni ihracat kontrolleri yayınlaması, akıllı telefon iplerinin byk bir oranını tedarik ettięi TSMC'nin ABD ihracat kontrollerini gereke gstererek in ile iřbirlięini durdurması, ABD mdahaleleri arasında yer almaktadır. zellikle ihracat kontrolleri yasası erevesinde in'in Wuhan kentinde, lkenin yabancı ip reticilerine olan baęımlılıęı azaltma hedefiyle kurulan dnyanın en byk szleřmeli ip reticisi Yangtze Memory Technologies Corporation (YMTC) dahil olmak zere 36 inli ip reticisinin ABD ip teknolojisine eriřimi kısıtlanacak řekilde geniřletilmiřtir.

Huawei, in hkmetiyle iddia edilen baęları ve teknolojisini siber casusluk iin olası kullanımı konusundaki endiřeler nedeniyle ABD, hem ekonomik ıkarlar hem de ulusal gvenlik kaygıları neticesinde Huawei'nin pazara giriřini kısıtlama abalarında birka mttefikin desteęiyle pazar eriřimini kısıtlayarak kendi ekonomisini glendirme fırsatı bulmuřtur. in ekonomisi byk lde ihracata baęımlı olduęu iin, ABD pazarındaki kısıtlama ekonomisine zarar vermektedir. Ayrıca in'in ABD rnlerine ulusal alternatifler geliřtirme abaları, teknolojik uzmanlık ve temel bileřenlere eriřim eksiklięi nedeniyle engellenmektedir.

ABD mttefiklerinden gelen kısıtlamalar arasında; Hindistan'ın gelecek projelerde Huawei ekipmanının kullanımını ařamaları olarak kaldırma kararı, Fransa'nın telekomnikasyon operatrlerinin sresi dolduęunda Huawei ekipmanlarının lisanslarını yenilemeyeceęi ve řirketin lkedeki varlıęını ařamalı olarak kaldırma kararı, Vietnam'ın Huawei'yi tamamen olmasa da 4G ve 5G aęlarında kullanımını kaldırma kararı, İtalya'nın Huawei ile telekomnikasyon saęlayıcısı Fastweb arasında Huawei'yi 5G aęının tek tedarikisi olarak kullanılmasına dair anlařmayı veto etmesi, Kanada'nın Huawei'yi 5G aęlarından ıkarma kararı yer almaktadır. Belika, Hırvatistan, Finlandiya, Yunanistan, Norve, Portekiz, Singapur ve İřpanya ise Huawei'ye karřı aleni bir duruř sergilememiř olsa da 5G aęlarını kurmak iin Huawei'nin rakipleri arasında yer alan Ericsson ve Nokia ile szleřme yapmayı tercih etmiřtir (Sacks, 2021).

Kuzey Kore'nin Saldırgan Siber Yetenekleri; Rejimin devamlılığını sağlama, dış müdahalelerden bağımsız bir ulus haline gelme ve Kore'yi Kuzey Kore hükümetinin kontrolü altında birleştirme hedefiyle politikalar yürüten Kuzey Kore'nin saldırgan siber yetenekleri, uluslararası güvenlik için önemli bir tehdit oluşturmaktadır. Ülkenin siber operasyonları siyasi ve ekonomik hedeflerine ulaşmak için önemli bir araç olarak gördüğüne inanılmakta ve bir dizi yüksek profilli saldırı yapmakla suçlanmaktadır.

Kuzey Kore'nin, kuruluşları, bireyleri ve rakip ulus devletlerin operasyonlarını bozmayı hedeflediği kötü amaçlı yazılımlar geliştirdiği ve dağıttığı bilinmektedir. 2017'de yine Kuzey Kore destekli Lazarus grubuna atfedilen WannaCry fidye yazılım saldırısı, dünya çapında yüz binlerce bilgisayarı etkileyerek büyük bir maddi hasara sebep olmuştur. Genel olarak, Kuzey Kore'nin saldırgan siber yetenekleri ve faaliyetleri, savaş eşiğini geçmeden ülkelerin ekonomilerine ve ulusal güvenliklerine önemli zararlar verdiğini ve uluslararası toplum için önemli bir tehdidi temsil ettiğini göstermektedir.

Dark Web; Dark Web, siber tehdit aktörleri, teröristler ve devlet destekli casuslar tarafından yasa dışı faaliyetleri yerine getirmek ve çeşitli siber suç türleri için en zorlu ve izlenemez bir pazar yeridir. Bu sebeple ulus devletler ve çok uluslu şirketler için oluşturduğu birçok potansiyel tehdit vardır.

Dark Web üzerinde faaliyet gösteren siber tehdit aktörleri hassas bilgileri çalmak, kritik altyapıları bozmak, casusluk yapmak veya siber saldırılar başlatmak için ulus devletleri ve çok uluslu şirketleri hedef alabilmektedir. Bu siber tehdit aktörleri, belirli bir ulus devletin çıkarlarına zarar vermeye çalışan devlet destekli veya devlet dışı aktörler olabilir. Ayrıca Dark Web, aşırılık yanlısı grupların hükümetlere ve vatandaşlarına yönelik saldırılar planlamaları için bir platform sağlar. Dark Web hem ateşli silahlar, patlayıcılar ve kimyasal silahlar gibi yasa dışı silahlar için bir pazar yeri hem de uyuşturucu ve insan kaçakçılığının satışı, dağıtımı için bir merkezdir. Dolayısıyla bu tehditlerden etkilenen ulus devletler ve vatandaşlar üzerinde önemli sosyal, ekonomik ve politik etkiler doğurabilmektedir.

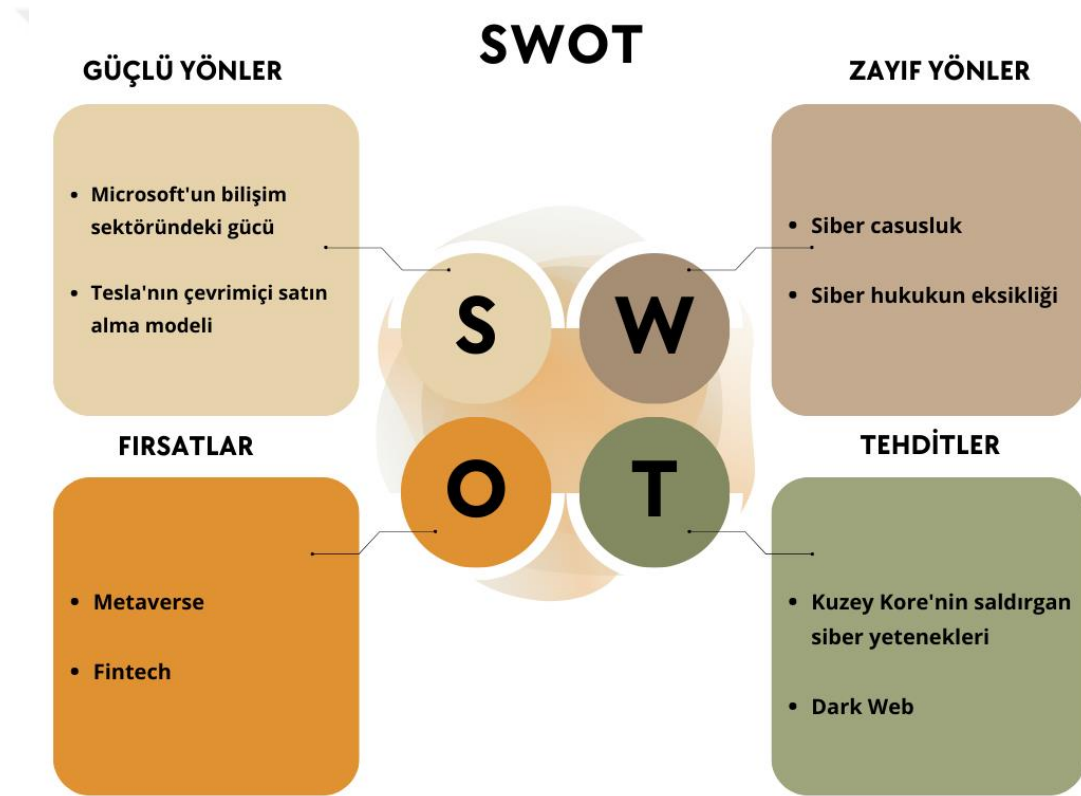
Dark Web'de özellikle terör örgütleri ulusal güvenlik için büyük bir tehdittir. El Kaide IŞİD gibi terör örgütleri, Dark Web'i propaganda yapmak, para toplamak ve üye kazanmak için kullandığına dair veriler bulunmaktadır. Örneğin 2014 yılında çevrimiçi

olarak yayınlanan "Bitcoin wa Sadaqat al-Jihad" (Bitcoin ve Cihad Hayır Kurumu) makalesi, Bitcon'i ve anonim bağış sistemini kullanarak cihatçı grupların finansal sistemdeki kısıtlamaları aşma ve ekonomik desteği kolaylaştırma stratejilerini ele almaktadır.

5.5. Çok Uluslu Şirketler için SWOT Analizi

Şekil 34'te şirketler ile ilgili SWOT analizi şekli verilmiştir.

Şekil 34: Şirketler SWOT Analizi



5.5.1. Güçlü Yönler

Microsoft'un Bilişim Sektöründeki Gücü; Apple, piyasa değeri açısından ilk sırada yer alan ve Microsoft'tan daha büyük şirket olsa da, Microsoft kendisini, Apple, Amazon, Meta ve Google dahil olmak üzere diğer piyasa değeri yüksek teknoloji şirketlerinden çeşitli yönlerden ayırmaktadır. Apple tüketici donanımına (iPhone, iPad, Mac) güçlü bir vurgu yaparken, Amazon e-ticaret ve bulut bilgi işlemde hakim bir konumdadır. Google, arama, çevrimiçi reklamcılık ve internet hizmetlerinde

uzmanlaşırken, Meta öncelikle sosyal medyaya ve sanal gerçeklik gibi girişimlere odaklanır.

Dünyanın en ünlü ve en büyük bir piyasa değerine (2,09 trilyon dolar) sahip Amerikan çok uluslu teknoloji şirketlerinden biri olan Microsoft, yazılım ve bulut bilişim teknolojisinde küresel pazar lideridir. Windows işletim sistemi, Microsoft Office programları, bulut bilişim platformu Azure, Office 365, Dynamics 365, uzaktan çalışma çözümü Microsoft Teams, Mesh, sanal asistan Cortana gibi çeşitli yazılım ürünleri ve hizmetleri geliştirerek, 1975 yılından beri teknoloji endüstrisinde güçlü bir pazar varlığı oluşturmuş ve önemli bir aktör olmuştur. Bu ürünler hem kişisel hem de profesyonel ortamlarda vazgeçilmez olmakla birlikte, Microsoft, özellikle otomotiv, enerji ve finans sektörleri de dahil olmak üzere çeşitli sektörlerdeki çok uluslu şirketler için lider bir dijital stratejik ortak haline gelmiştir. Yenilikçi teknolojileri ve hizmetleri sayesinde Microsoft, çok uluslu şirketlerin operasyonlarında daha fazla dijitalleşme ve verimlilik elde etmelerini sağlarken, aynı zamanda kendi pazarlarında büyüme ve rekabet gücünü artırmıştır.

Microsoft, çeşitli şirketleri satın almasıyla ve çeşitli alanlara yatırımlarda bulunmasıyla yeni teknolojilerle de ilgilenmektedir. Örneğin Sony'nin PlayStation oyun konsoluna rekabetçi bir şekilde Microsoft tarafından oluşturulan Xbox (Microsoft, tarih yok) oyun konsolu donanımı ile eğlence ve oyun sektöründe de öncü olmayı hedeflemektedir.

Yazılım geliştirme projeleri için web tabanlı bir kod deposu hizmeti olan GitHub'ı 7,5 milyar dolara satın alması (Microsoft, tarih yok(a)), sosyal iş ağı sitesi LinkedIn'i 26,2 milyar dolara satın alması (Microsoft, tarih yok(b)), dünya oyunu olan Minecraft'ı 2,5 milyara satın almasıyla (Microsoft, tarih yok(c)) yeni gelir akışları elde etmiştir. Aynı zamanda Microsoft'un çeşitli kullanıcı tabanlarından faydalanmasına ve kritik sektörlerdeki varlığını güçlendirmesine olanak sağlamıştır.

Microsoft'un ABD'deki ekonomik etkisi ise son derece önemlidir. Şirketin ülkedeki yatırımları, ekonomik büyümeyi artırmaya yardımcı olmakta ve ülkenin GSYİH'sına katkı sağlamaktadır. Ayrıca Microsoft, ABD'deki hükümet kurumlarındaki, özel ve kamu şirketlerindeki bilgi işlem ihtiyaçlarına güvenilir çözümler sunmaktadır.

Tesla'nın çevrimiçi satın alma modeli; Covid-19 salgını sırasında birçok sektör salgının etkisinden olumsuz etkilenmiş ve dünya çapındaki fabrikaların çoğu kapanmıştır. Özellikle pandemi sürecinde yaşanan sokağa çıkma kısıtlaması sebebiyle küresel otomobil satışları düşmüş ve otomotiv endüstrisinin tamamı Covid-19 pandemisi sürecinde büyük bir gerileme yaşamıştır. Ancak bu koşullar altında elektrikli araç pazarında lider bir marka olan Tesla, üretim ve satışlarında artış sağlayarak sipariş hacmini büyütüştür. Şirketin operasyonlarının çoğu virüsten büyük ölçüde etkilenmemiş ve 2020'nin ilk çeyreğinde 88.496 araba satmıştır. 2020'den beri %271 oranında marka değerini artırmış ve 2022'de marka değerini 46,0 milyar dolara yükseltmiştir. Bu oran yerleşik otomobil üreticileri tarafından bildirilen rakamların daha üstündedir. General Motors, Ford Motor, Fiat Chrysler ABD satışlarının 2020'nin ikinci çeyreğinde %30 ve daha fazla düştüğünü bildirirken, Tesla %5'lik bir düşüş yaşamıştır (Boudette, 2020).

Tesla'nın satış modeli, pandemi sırasında çevrimiçi satış ve teslimat stratejisine dayanmaktadır. Çevrimiçi mağaza modeline dayalı stratejisi, müşterilerin evlerinden çıkmadan araçlarını satın almalarına ve teslim almalarına olanak sağlamıştır. Farklı bölgeler için eve teslim hizmetiyle satın alma ve satın alım sonrasında şarj etme gibi ihtiyaçlara yönelik çevrimiçi danışmanlık hizmetleri sunması, Tesla'nın Covid-19 pandemisi sırasında üretimde pozitif satış büyümesi elde etmesini sağlamıştır.

Fransız danışmalık firması Brand Finance'ın 2023 tarihli araştırmasına göre Tesla, şu anda 66,2 milyar dolar değerindeki markasıyla dünyanın en değerli otomobil markası olan Mercedes-Benz ve Toyota'yı geride bırakmıştır. Elektrikli otomobil üreticisi sıralamasında ise sırasıyla 58,8 milyar dolar ve 52,5 milyar dolar değerindeki Mercedes ve Toyota'dan daha yüksek bir değere sahiptir (BrandFinance, 2023). ABD'de elektrikli otomobil pazarı, satılan tüm elektrikli araçların yarısından fazlasını oluşturduğu için Tesla'nın hakimiyetindedir.

5.5.2. Zayıf Yönler

Siber Casusluk; Çok uluslu şirketler ticari sırları, mali bilgiler, müşteri verileri, diğer gizli ve özel bilgiler nedeniyle hedef alınabilir ve genellikle değerli fikri mülkiyet, ticari sırlar ve finansal verilere sahip oldukları için siber casusluk faaliyetlerine karşılan devlet destekli ve diğer bağımsız aktörlerden gelen önemli

tehditlerle karşı karşıyadır. Hedef alınan şirketin ağlarına yönelik siber saldırılar, şirketin önemli mali kayıplarla ve itibar zedelenmesiyle sonuçlanabilmektedir.

GhostNet, bireyleri, kuruluşları ve hükümetleri gözetlemek için kullanılan büyük ölçekli bir elektronik casusluk programı olarak bilinmektedir. Saldırıda virüs içerikli ekler ve web sitesi bağlantıları içeren e-postalar kuruluşlara gönderilmiş ve virüs açıldıktan sonra siber tehdit aktörleri tarafından ana bilgisayar arka planda ele geçirilerek veri gönderme alma gibi faaliyetlere izin verilmiştir. Siber tehdit aktörleri, ağırlıklı olarak Güneydoğu Asya'daki hükümetlere odaklanarak, iki yıllık bir süre içinde 103 ülkede 1295 bilgisayarı gözetleyerek veri ihlalleri gerçekleştirmiştir. 10 aylık araştırma sürenin sonunda İran ve Endonezya da dahil olmak üzere birçok ülkenin dışişleri bakanlıklarında, Hindistan, Güney Kore, Tayvan, Portekiz, Almanya ve Pakistan büyükelçiliklerinde dinlenen bilgisayarlar tespit edilmiştir ve siber tehdit aktörlerinin Çin'de yerleşik olduğu doğrulanmıştır (Glaister, 2009).

Siber Hukukun Eksikliği; Çok uluslu şirketler açısından siber hukukun eksikliği şirketlere yönelik ve topluma yönelik ayırabiliriz. İlk olarak şirketlere yönelik durumda güçlü siber yasaların eksikliği, siber saldırılara, veri ihlallerine ve fikri mülkiyet hırsızlığına karşı savunmasız bırakabilmekte ve siber tehdit aktörlerini sorumlu tutmak için yetersiz mekanizmalara sahip olmasına neden olmaktadır. Örneğin finansal hizmetler sektöründe siber güvenlik açığı finansal istikrar için açık bir tehdittir. IMF'nin 51 ülkeyi kapsayan bir anketine göre, yükselen piyasalar ve gelişmekte olan ekonomiler açısından çoğu mali denetçi siber güvenlik düzenlemeleri getirmemiş ve bunları uygulamak için kaynak oluşturmamıştır. Merkez bankalarının %56'sının finans sektörü için ulusal bir siber stratejisi bulunmamakta, %42'i özel bir siber güvenlik veya teknoloji risk yönetim yönetmeliğine sahip değil, %68'i uzmanlaşmış bir risk birimine sahip değil, %64'ü siber güvenlik önlemlerinin test edilmesini ve uygulanmasını zorunlu hale getirmemekte, %54'ü özel bir siber olay raporlama biriminden yoksun ve %48'inin siber suç düzenlemeleri mevcut değildir (Adrian & Ferreira, 2023).

Teknolojiye artan güven ve çok uluslu şirketler tarafından yürütülen büyük miktarda veri, yeni zorluklar ve güvenlik açıkları yaratmaktadır. Kişisel verilerin çok uluslu şirketler tarafından toplanması, saklanması ve kullanılmasıyla ilgili potansiyel riskleri vurgulayan en önemli vakalardan biri Cambridge Analytica skandalıdır. Firma,

milyonlarca Facebook kullancısının kişisel bilgilerini izinleri olmadan toplamış ve analiz etmiştir. Veriler ise 2016 yılında ABD başkanlık seçimleri ve Birleşik Krallık Brexit referandumu gibi siyasi kampanyalar sırasında hedefli kampanyalar oluşturmak için kullanılmıştır. Dolayısıyla bireylerin mahremiyetini korumak ve verilerin şirketler tarafından kötüye kullanılması çerçevesindeki yasalarda önemli zayıflıklar görülmektedir.

5.5.3. Fırsatlar

Metaverse; Metaverse tanıtım, markalaşma ve pazarlama için benzersiz bir ortam sağlamaktadır. Çok uluslu şirketler için fırsatlar, Metaverse aracılığıyla gelişmiş müşteri ilişkileri ve küresel bir kullanıcı kitlesine ulaşma becerisini içerebilir. İşletmelere ürünleri ve hizmetleri sanal bir ortamda test etmeleri için yeni fırsatlar sunarak, maliyetleri düşürmeye ve verimliliği artırmaya yardımcı olabilir. Ayrıca Metaverse, yeniliği hızlandırmaya ve üretkenliği artırmaya yardımcı olabilecek yeni işbirliği ve bilgi paylaşımı biçimleri sağlayabilir.

Metaverse'ün gelişmekte olan bir dijital ortam olduğunu ve potansiyelinin tamamının henüz gerçekleştirilmediğini not etmek önemlidir. Bu nedenle Metaverse'ün tam potansiyelini ortaya çıkarmak için gerçekleşmesi muhtemel olanaklarını ve durumları rakiplerden önce keşfederek bir stratejinin belirlenmesi gerekmektedir.

Fintech; Geleneksel bankalardan daha hızlı değişime uyum sağlayan ve modern pazarlama kanallarını kullanan Fintech sektörü, finansal hizmet sağlayıcıları ve tüketiciler arasındaki etkileşimi daha kolay hale getirerek, müşterilerin finansal işlemlerini daha hızlı ve verimli bir şekilde gerçekleştirmelerini sağlar. Geleneksel bankacılık ve ödeme sistemlerine kıyasla, yetersiz hizmet alan müşteriler dahil herkes tarafından erişilebilir düşük işlem maliyeti sunar. Blok zinciri gibi yeni teknolojileri kullanarak kullanıcıların finansal işlemlerini daha güvenli ve şeffaf olmasına yardımcı olur ve yapay zeka, makine öğrenimi gibi teknolojiler aracılığıyla da finansal hizmet sağlayıcılarının daha verimli operasyonlar gerçekleştirmesine olanak sağlar. Geliştirilen mobil uygulamalar ve sanal asistanlar aracılığıyla müşterilerin daha kolay işlem yapmasını sağlar. Fintech şirketleri, dijital ödemeler, borç verme, sigorta ve para yönetimi gibi alanlarda yenilik yaparak finans sektöründe önemli ilerlemeler kaydetmiştir. Dolayısıyla mobil ve çevrimiçi bankacılığın yükselişyle birlikte

bankalar, dijital bankaların ve Fintech girişimlerinin artan rekabetiyle karşı karşıya kalmaktadır. Küresel FinTech endüstrisinin önümüzdeki yıllarda hızla gelişmeye devam etmesi ve hem yeni başlayanlar hem de sektördeki tüm aktörler için sayısız fırsatlar sunması beklenmektedir.

FinTech, finansal hizmetlerin iyileştirilmesi ve ekonomik büyümenin hızlandırılması açısından ulus devletler ve çok uluslu şirketler için önemli fırsatlar sunmakta ve finansal teknoloji endüstrisindeki potansiyel pazar ve büyüme fırsatlarını içermektedir. Fintech, kırsal veya düşük gelirli bölgelerde geleneksel bankacılık işlemlerini gerçekleştiremeyen nüfuslara mobil ödeme ve dijital bankacılık hizmetlerinin sunulmasını sağlayarak, finansal hizmetlere erişimin genişletilmesini içermektedir.

5.2.4. Tehditler

Kuzey Kore; Kuzey Kore'nin 2014 yılında Sony Pictures'ı hedef alan siber saldırı göz önüne alındığında hem stratejik avantaj elde etmek amacıyla hükümetlerden, askeri kuruluşlardan ve ileri düzey bilgi içeren özel şirketlerden hassas bilgileri çalmak amacıyla hem de savunma, imalat ve ileti teknoloji gibi belirli hedeflere yönelik ekonomik siber casusluk yürüttüğü sonucuna varabiliriz.

Kuzey Kore'nin nükleer silah geliştirme faaliyetlerini finanse etmek ve yaptırımlardan kaçınmak amacıyla enerji şebekeleri ve finansal hizmetler gibi kritik altyapıya karşı saldırgan siber operasyonlar düzenleme kabiliyetine sahip olduğuna inanılmaktadır. 2016 yılında Bangladeş Merkez Bankası'na yönelik siber saldırıda, Kuzey Kore destekli Lazarus grubu ile bağlantılı olduğu iddia edilen siber tehdit aktörleri, küresel bir finansal mesajlaşma ağı olan SWIFT'in kimlik bilgilerini ele geçirerek işlemlerle 81 milyon dolar çalmıştır. Ayrıca Kuzey Kore'nin kripto para borsalarını ve kullanıcıları kendi ekonomik kazancı için dijital para birimlerini çalmayı hedeflediği de bilinmektedir.

Dark Web; Çok uluslu şirketler, özel bilgileri, ticari sırları ve finansal verileri çalmaya çalışan siber tehdit aktörleri tarafından sıklıkla hedef alındıklarından, Dark Web tehditlerine karşı savunmasızdır. Özellikle Dark Web üzerinden faaliyet gösteren siber tehdit aktörleri, dolandırıcılık ve kimlik hırsızlığı gibi eylemleri şirketler ve

bireyler için önemli mali kayıplara neden olabilmekte ve ulusal güvenlik için bir tehdit oluşturabilmektedir. Örneğin Black Market Reloaded, Dark Web üzerinden Bitcoin aracılığıyla Avustralya, ABD, Hollanda Almanya, Fransa dahil birçok ülkeye elektronik cihazların için yerleştirilmiş ateşli silahların posta yoluyla satışını gerçekleştiren ve 500 dolara satılan bir tabancayı, Dark Web üzerinden 3.400 dolara satarak kar elde eden bir pazar olarak bilinmektedir.



SONUÇ

Çok uluslu şirketlerin ve ulus devletlerin siber uzay üzerindeki etkisini anlamaya odaklanan araştırmalar, günümüzün dijital çağında büyük önem taşımaktadır. Siber uzaya katılımlarını, güç dinamiklerini ve siber uzayın çeşitli boyutları üzerindeki etkilerini inceleyerek, aktörler arasında karmaşık etkileşime ve bunun sonucunda ortaya çıkan sonuçlara ilişkin önemli bulgular elde edilmektedir. Bu bilgi, bilgiye dayalı karar verme, etkili dijital yönetim, güçlü siber güvenlik uygulamaları ve bireylerin, toplumların ve ulusların benzer şekilde çıkarlarını korurken dijital devrimin tüm potansiyelinden faydalanmak için gereklidir.

Siber uzayın ve dijitalleşmenin yararları toplumun her düzeyinde kendini göstermektedir. Finans, endüstri, eğlence, iş yaşamı, savaş, rekabet gibi birçok sektör ve alanda uygulamaları dönüştürmüş, yapay zeka, bulut bilişim, nesnelerin interneti, artırılmış gerçeklik gibi Endüstri 4.0'ın tüm unsularının gelişimini hızlandırmıştır. Bununla dönüşüm, hem olumlu ve olumsuz sonuçlarla birlikte kendini göstermiş hem de siber güvenlik, siber savunma ve siber savaş konularında artan farkındalık ihtiyacına yol açmıştır. Dolayısıyla siber uzaya artan güven, iki ucu keskin kılıç olarak tanımlanabilecek bir saha yaratmıştır.

Siber uzay, hem süper güçler hem de daha küçük devletler tarafından kullanılan etkili bir araç haline gelmiş ve tüm ulus devletlerin kendilerini eşit düzeyde bulabilecekleri asimetrik savaş modelini oluşturmuştur. Askeri yeteneklerdeki eşitsizlikler nedeniyle siber uzayda dinamikler değişmekte ve daha küçük devletler, daha güçlü ulusların güvenlik açıklarını hedeflemek için siber yeteneklerini kullanmaktadır. Bununla birlikte, siber uzay asimetrik savaş için fırsatlar sunarken, süper güçler ile daha küçük devletler arasındaki güç eşitsizliklerini tamamen ortadan kaldırmadığına dikkat etmek önemlidir. Büyük ulus devletler daha gelişmiş siber yeteneklere ve kaynaklara sahip olduğu için siber uzayın şekillenmesinde hala önemli bir rol oynamaktadır.

Bir ulus devlet için siber egemenlik, bilginin stratejik bir kaynak olması nedeniyle yüksek önceliğe sahiptir. Kritik altyapıyı korumak, siber tehditlerle mücadele etmek ve siber barışı sağlamak ulusal güvenlik için elzemdir. Bilgiyi korumak, telekomünikasyon, endüstri, ekonomi, hükümet ve ordu dahil olmak üzere

ulus içindeki çeşitli sektörlerin işleyişi için hayati önem taşımaktadır. Dolayısıyla siber uzayın kullanımı, birden fazla tehdidi beraberinde getirerek, devletleri dijital altyapılarının savunması için siber güvenliğe öncelik vermeye ve potansiyel siber savaşa karşı saldırı ve savunma yeteneklerini geliştirmeye sevk etmektedir. Siber savaş durumu birçok araştırmacı için bir efsane gibi görünse de, siber uzayda dünyanın farklı bölgelerinden güçlü aktörlerin karıştığı vakalar, siber savaşın gerçekliğini göstermektedir. Siber savaş, özellikle ekonomik ve politik güçlerin temelini oluşturan dijital altyapılar açısından, devletlerin iç ve dış egemenliğine yönelik bir tehdit oluşturmaktadır.

Çok uluslu şirketler, siber uzayda inovasyon ve teknolojik ilerlemeleri yönlendiren ekonomik güç merkezleri olarak hizmet vermektedir. Geniş kaynakları, araştırma yetenekleri, platformları ve hizmetleri geliştirerek dijital ortamı şekillendirmektedir. Dolayısıyla çok uluslu şirketlerin siber uzayın teknolojik gidişatını şekillendirmede, ekonomik büyümeyi desteklemede ve endüstriler genelinde dijital dönüşümü yönlendirmede oynadığı rol önemlidir.

Araştırmada ele alınan ABD, Çin, Rusya ve İran açısından bilişim sektöründe ve jeopolitik çerçevede siber uzaydaki rekabetleri, devlet destekli siber güvenlik stratejilerinin oluşmasını gerekli kılmıştır. Bunun yanında Metaverse alanında Microsoft, Samsung ve Apple gibi çok uluslu teknoloji şirketlerinin girişimleri ve Fintech alanında finansal teknoloji şirketleriyle işbirliği yapan JPMorgan, Goldman Sachs, Citigroup, Deutsche Bank, BBVA ve Bank of Beijing gibi çok uluslu finans kurumlarının rekabette ön planda olduğu ve bununla ilgili çok önemli fırsatların meydana geldiği anlaşılmıştır. Kuzey Kore ve İran gibi ülkelerin saldırı yeteneklerinin, telekomünikasyon veya finans gibi hayati sektörlerle yönelik saldırılarının ve Dark Web'in varlığının önemli bir tehdit oluşturduğu anlaşılmıştır. Ayrıca Çin ve ABD arasındaki ticaret savaşlarında Çinli telekomünikasyon şirketlerine yönelik getirilen kısıtlamaların incelenmesiyle ABD'den Çin'e yönelik bir tehdit algısının varlığı sonucuna varılmıştır. Bu yönüyle uluslararası hukukun güçlendirilmesi ve ilgili devletlerin birbiri arasındaki rekabetteki bu yönüyle siber casusluk gibi faaliyetlerin daha denetlenebilir ve daha hukuki olarak gözlemlenebilir olarak ele alınması BM barış ve güvenli misyonuna daha yakın bir yaklaşım olarak görülecektir.

Siber yeteneklerin kullanımını kontrol edebilecek merkezi bir otoritenin bulunmaması, siber savaşın ortaya çıkmasına ve bireysel, örgütsel ve küresel düzeylerde çeşitli siber stratejilerin geliştirilmesine yol açmıştır. Ancak gelişmiş siber güvenlik yeteneklerine sahip ulus devletler tarafından uygulananlar da dahil olmak üzere ulusal siber stratejilerinin, siber tehdit aktörlerinin faaliyetlerini caydırma, düzenleme veya engellemede yetersiz kaldığı kanıtlanmıştır. Bunun nedeni, siber uzayın ulusal çıkarların gözetilebileceği bir alan sunduğu algısı ve kullanıcı faaliyetlerini denetleyen merkezi bir kontrol biriminin olmamasından kaynaklanıyor olabilir.

Sonuç olarak, siber tehdit aktörleri tarafından devletlerin, şirketlerin ve bireylerin veri havuzlarına izinsiz girişler, veri tabanlarına yapılan başarılı saldırılar devam etmektedir. Bu mevcut durumlar ise uluslararası ilişkilerde ekonomik, siyasi ve güvenlik konusunda etkiler göstermektedir. Hukuksal çerçevede ise bireysel, devletsal ve kurumsal unsurlar içerisinde boşlukları meydana getirmektedir.

KAYNAKÇA

- Abrams, M., & Weiss, J. (2008). *Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia*. MITRE. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf adresinden alınmıştır
- Abrams, L. (2021). *Kia Motors America suffers ransomware attack, \$20 million ransom*. <https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/> adresinden alınmıştır
- Abrams, L. (2021). *Chemical distributor pays \$4.4 million to DarkSide ransomware*. <https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/> adresinden alınmıştır
- Abrams, L. (2021). *Cyberattack shuts down Ecuador's largest bank, Banco Pichincha*. <https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/> adresinden alınmıştır
- Abrougui, A. (2019). *Chinese law and state security requirements stunt companies' progress in 2019 RDR Index*. <https://rankingdigitalrights.org/2019/07/17/chinese-law-and-state-security-requirements-stunt-companies-progress-in-2019-rdr-index/> adresinden alınmıştır
- Addawood, A., Badawy, A., Lerman, K., & Ferrara, E. (2019). Linguistic Cues to Deception: Identifying Political Trolls on Social Media. *Thirteenth International AAAI Conference on Web and Social Media* (s. 15-25). California: Association for the Advancement of Artificial Intelligence.
- Adrian, T., Ferreira, C., (2023). *IMF Blog*. <https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards> adresinden alınmıştır
- Afanasyeva, A., Bogatyrev, S., & Wilke, N. (2019). *ADVANT Beiten*. <https://www.advant-beiten.com/sites/default/files/downloads/Information%20Technologies%20in%20Russia.pdf> adresinden alınmıştır
- Afşar, A. (2019). Finansal Hizmetler Sektöründe Siber Güvenlik . *Dijital Dönüşüm ve Finans* (s. 141-161). içinde Detay Yayıncılık.

- Ahrens, N. (2013). *China's Competitiveness, Myth, Reality, and Lessons for the United States and Japan*. Washington, DC: Center for Strategic & International Studies (CSIS).
- Akçacı, T. (2017). Endüstri 4.0 ve İnovasyon Göstergeleri Kapsamında Türkiye Analizi. *ASSAM Uluslararası Hakemli Dergi*, Sayı:7, 50-72.
- Aktan, S. (2019). *ABD'den Huawei'ye yeni suçlamalar: Çinli teknoloji devi neden hedefte?* . <https://tr.euronews.com/2018/12/12/huawei-veliahtinin-tutuklanmasi-gelecegin-dunyasi-icin-oylanan-satrancin-bir-parcasi-mi> adresinden alınmıştır
- Aksahan, F. (2021). Industry 4.0 in the Oil and Gas Industry. *Honeywell Forge*.
- AK&M. (2020). *Gazprom Neft earns RUB 7.2 billion in economic effect from advanced technologies and business process optimization*. <https://www.akm.ru/eng/news/gazprom-neft-earns-rub-7-2-billion-in-economic-effect-from-advanced-technologies-and-business-proces/> adresinden alınmıştır
- Altun, N., Kurt, İ., & Özbaysal, T. (2021). Adım Adım Yeni Dünya Düzeni: Çin BKBY Projesi. *Gümrük Ticaret Dergisi*, 8(26), 81-93.
- Aissa, A. B., Rabai, L. A., Abercrombie, R. K., Mili, A., & Sheldon, F. T. (2014). Quantifying Availability in SCADA Environments Using the Cyber Security Metric MFC. *2014 9th Annual Cyber and Information Security Research Conference (CISRC)*. Oak Ridge .
- Alduhaidahawi, H. H., Zhang, J., Salam, M., Sebai, M., & Harjan, S. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science*, 9(6), 123-133.
- Alcantara, B. T. (2018). SCO and Cybersecurity: Eastern Security Vision for Cyberspace. *International Relations and Diplomacy*, 6(10), 549-555.
- Alder, S. (2019) *10 Year Jail Term for Boston Children's Hospital Hacker*. <https://www.hipaajournal.com/10-year-jail-term-for-boston-childrens-hospital-hacker/10> adresinden alınmıştır
- Almay, R. (2022). *Europe's Most Popular Digital Banks - What Should We Know About Them?* <https://ergomania.eu/europes-most-popular-digital-banks-what-should-we-know-about-them/> adresinden alınmıştır
- Altaş, G. (2020). Avrupa Birliği Dijital Finans Stratejisi. *Gösterge*, 29-42.
- Altunok, E., & Vural, A. F. (2011). Bilişim Suçları. *Denetim*, Sayı:8, 74 - 84.

- AlwareBytes. (tarih yok). *Cryptojacking – What is it?*.
<https://www.malwarebytes.com/cryptojacking> adresinden alındı
- Anagnostakis, D. (2020). The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. *Journal of Cyber Policy*, 6(2), 243-261.
- Antoniuk, D. (2022). *DDoS attacks surge in popularity in Ukraine — but are they more than a cheap thrill?* <https://therecord.media/ddos-attacks-surge-in-popularity-in-ukraine-but-are-they-more-than-a-cheap-thrill> adresinden alınmıştır
- Applegate, S. (2011). Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare. *IEEE Security and Privacy Magazine*, 9(5), 16-22.
- Apple Inc. (2021). *Conflict Minerals Report 2021*. California.
- Arachchilage, N. A., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance. *Computers in Human Behavior*, Vol:38, 304-312.
- Arauz, A., Weisbrot, M., Bunker, A., & Johnston, J. (2019). *Bolivia's Economic Transformation: Macroeconomic Policies, Institutional Changes, and Results*. Washington, DC: Center for Economic and Policy Research.
- Aramco. (tarih yok). *Technology Depeloment Our Digital Innovation Centers* .
<https://www.aramco.com/en/creating-value/technology-development/in-house-developed-technologies/digitalization/our-digital-innovation-centers> adresinden alınmıştır
- Argaman, S., & Siboni, G. (2014). Commercial and Industrial Cyber Espionage in Israel. *Military and Strategic Affairs*, 6(1), 43-58.
- Arı, E. S. (2021). Süper Akıllı Toplum: Toplum 5.0. *Dokuz Eylöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 23(1), 455-479.
- Article19 . (2021). *Iran: Parliament's "Protection Bill" will hand over complete control of the Internet to authorities* . <https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/> adresinden alınmıştır
- Aryan, S., Aryan, H., & Halderman, J. A. (2013). *Internet Censorship in Iran: A First Look*. Washington, DC: Free and Open Communications of the Internet [FOCI].
- Aschmann, M., Vuuren, J. J., & Leenen, L. (2015). Cyber Armies: The Unseen military in the grid. *International Conference on Cyber warfare and Security*, (s. 1-11). Skukuza.

- Asia Financial. (2022). *China War Risk Sees Taiwan's TSMC Moving Fabs to US, Japan* . <https://www.asiafinancial.com/china-risk-sees-taiwans-tsmc-moving-chip-fabs-overseas> adresinden alınmıştır
- Asia Pacific Energy Portal. (2020). *Republic of Korea: 9th Basic Plan for Power Supply and Demand (BPLE) (2020-2034)*. <https://policy.asiapacificenergy.org/node/4314> adresinden alınmıştır
- Astakhov, D. (2018). *What is the GRU? Who gets recruited to be a spy? Why are they exposed so often?*. Meduza: <https://meduza.io/en/feature/2018/11/06/what-is-the-gru-who-gets-recruited-to-be-a-spy-why-are-they-exposed-so-often> adresinden alınmıştır
- Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(1), 238-244.
- Ateş, E. C., Bostancı, E., & Güzel, M. S. (2020). Security Evaluation of Industry 4.0: Understanding Industry 4.0 on the Basis of Crime, Big Data, Internet of Thing (IoT) and Cyber Physical Systems . *Güvenlik Bilimleri Dergisi*, Sayı:9, 29-50.
- Atkins, C. (2019). *Bolivia coup against Morales opens opportunity for multinational mining companies*. <https://www.peoplesworld.org/article/bolivia-coup-against-morales-opens-opportunity-for-multinational-mining-companies/> adresinden alınmıştır
- Atom Bank. (2015). *Atom and BBVA in strategic partnership*. <https://www.atombank.co.uk/newsroom/atom-and-bbva-in-strategic-partnership/> adresinden alınmıştır
- Australian Government Department of Foreign Affairs and Trade [DFAT]. *High-Level Security Dialogue with China: Joint Statement*. <https://www.dfat.gov.au/news/media/Pages/high-level-security-dialogue-with-china-joint-statement> adresinden alınmıştır
- AVAST. (tarih yok). *What Is a Logic Bomb? How to Prevent Logic Bomb Attacks*. <https://www.avast.com/c-what-is-a-logic-bomb> adresinden alındı
- AVAST. (tarih yok). *A Guide to the Silk Road Dark Web*. <https://www.avast.com/c-silk-road-dark-web-market> adresinden alınmıştır
- Aydın, Ö. (2021). 5. Nesil Mobil İletişim Teknolojisi ve Uluslararası Yansımaları. *Teknoloji ve Uluslararası İlişkiler* (s. 41-65). içinde Ankara: Nobel Akademik Yayıncılık .
- Aydın, H., Barışkan, M. A., & Çetinkaya, A. (2021). Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi. *Güvenlik Bilimleri Dergisi*, 10(1), 151-174.

- Baggott, J. (2020). *Car manufacturer Honda targeted in cyber attack after computers infected*. <https://cardealermagazine.co.uk/publish/car-manufacturer-honda-targeted-cyber-attack-computers-infected/194934> adresinden alınmıştır
- Ball, D. (2011). China's Cyber Warfare Capabilities. *Security Challenges*, Vol:7, No:2, 81-103.
- Banka, N. (2021). *Explained: The story of how North Korea hackers stole \$81 million from Bangladesh Bank*. <https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/> adresinden alınmıştır
- Bank of America. (tarih yok). *See what Erica can do*. <https://promotions.bankofamerica.com/digitalbanking/mobilebanking/erica> adresinden alınmıştır
- Banking Circle. (2021). *Banking Circle chooses SIA to launch Instant Payments Service in Europe*. <https://www.bankingcircle.com/banking-circle-chooses-sia-to-launch-instant-payments-service-in-europe-0710413> adresinden alınmıştır
- Bartlett, J. (2020). *Exposing the Financial Footprints of North Korea's Hackers*. Center for a New American Security.
- Bassist, R. (2022). *Israel-US sign cybersecurity agreement*. Al-Monitor. <https://www.al-monitor.com/originals/2022/08/israel-us-sign-cybersecurity-agreement> adresinden alınmıştır
- Bastani, H. (tarih yok). *Structure of Iran's Cyber Warfare*. l'Institut français d'analyse strategique [IFAS]. <http://www.strato-analyse.org/fr/spip.php?article223> adresinden alınmıştır
- Başa, Ş. (2020). *ABD İç Güvenlik Bakanlığı*. [http://www.safakbasa.com.tr/yuklenen_akademik_calismalar/40-ABD_IC_GUVENLIK_BAKANLIGI_\(SUNUM\).pdf](http://www.safakbasa.com.tr/yuklenen_akademik_calismalar/40-ABD_IC_GUVENLIK_BAKANLIGI_(SUNUM).pdf) adresinden alınmıştır
- Başakçi, G. (2019). *Surface, Deep ve Dark Web Nedir?* BGA Security : <https://www.bgasecurity.com/2019/08/surface-deep-ve-dark-web-nedir/> adresinden alınmıştır
- Baylon, C. (2016). Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare. *Ethics and Policies for Cyber Operations* (s. 213-29). içinde Springer International Publishing .
- BBC. (2012). *Cyber-attack on BBC leads to suspicion of Iran's involvement*. <https://www.bbc.com/news/technology-17365416> adresinden alınmıştır

- BBC. (2013). *Vodafone Germany hack hits two million customers*. <https://www.bbc.com/news/technology-24063621> adresinden alınmıştır
- BBC. (2016). *German nuclear plant hit by computer viruses*. <https://www.bbc.com/news/technology-36158606> adresinden alınmıştır
- BBC. (2017). *Ukraine power cut 'was cyber-attack'*. <https://www.bbc.com/news/technology-38573074> adresinden alınmıştır
- BBC. (2017b). *Apple 'pulls 60 VPNs from China App Store'*. <https://www.bbc.com/news/technology-40772375> adresinden alınmıştır
- BBC. (2020) *US charges Chinese Covid-19 research 'cyber-spies'*. <https://www.bbc.com/news/world-us-canada-53493028> adresinden alındı
- BBC. (2021). *Lazarus soygunu: Kuzey Koreli bilgisayar korsanları, Bangladeş Merkez Bankası'ndan 1 milyar dolar çalmaya ne kadar yaklaştı?* . <https://www.bbc.com/turkce/haberler-dunya-57554598#:~:text=Gelgelelim%20Amerikan%20Federal%20Soru%C5%9Fturma%20B%C3%BCrosu,sistemli%20%C3%A7al%C4%B1%C5%9Fmalar%C4%B1n%C4%B1n%20sonucunda%20hayata%20ge%C3%A7irildi.> adresinden alınmıştır
- BBC. (2022). *Global chip shortage: Toyota profits fall as production hit*. <https://www.bbc.com/news/business-60313571> adresinden alınmıştır
- Beardsley, T. (2016). *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*. <https://www.rapid7.com/blog/post/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/> adresinden alınmıştır
- Beaumont-Thomas, B. (2014). *North Korea complains to UN about Seth Rogen comedy The Interview*. <https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco> adresinden alınmıştır
- Ben-David, R. (2022). *US-Israeli cyber firm uncovers 'massive' Chinese-backed industrial espionage ring*. <https://www.timesofisrael.com/us-israeli-cyber-firm-uncovers-massive-chinese-backed-industrial-espionage-ring/> adresinden alınmıştır
- Benner, K., & Perlroth, N. (2021). *By Katie Benner. U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack*. New York Times. <https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html> adresinden alınmıştır

- Berlin Information Center for Transatlantic Security [BITS]. (2000). *2000 Russian National Security Concept*. <https://www.bits.de/EURA/natsecconc.pdf> adresinden alınmıştır
- Berman, N., Maizland, L., & Chatzky, A. (2023). *Is China's Huawei a Threat to U.S. National Security?* Council on Foreign Relations .
- Betti, F., & Boer, E. d. (2021). *Global Lighthouse Network: Reimagining Operations for Growth*. World Economic Forum.
- Bicchierai, L. F. (2015). *Teenage Hackers Say They've Doxed More Than 2,000 Government Employees*. <https://www.vice.com/en/article/9a39v7/teenage-hackers-say-theyve-doxed-more-than-3500-government-employees> adresinden alındı
- Bisht, D., Singh, R., Gehlot, A., Akram, S. V., Singh, A., Montero, E. C., . . . Twala, B. (2022). Imperative Role of Integrating Digitalization in the Firms Finance: A Technological Perspective. *Electronics*, 11(19), 1-16.
- Bloomfield, A. (2013). *Anonymous OpUSA: Massive Cyber Attack Planned For Tuesday Against Government and Banks*. <https://www.mic.com/articles/40149/anonymous-opusa-massive-cyber-attack-planned-for-tuesday-against-government-and-banks> adresinden alındı
- Blumenthal, J. (2023). *3 of Philadelphia's largest banks continue trimming footprints, shuttering additional branches*. <https://www.bizjournals.com/philadelphia/news/2023/05/18/wells-fargo-pnc-bank-of-america-branch-closures.html> adresinden alınmıştır
- Bocetta, S. (2022). *The Risk of Cybersecurity Threats Continues To Grow for the Auto Industry*. <https://www.globalsign.com/en/blog/cybersecurity-threats-auto-industry> adresinden alınmıştır
- Bogage, J., & Reiley, L. (2021). *Russian hackers target Iowa grain co-op in \$5.9 million ransomware attack*. Washingtonpost. <https://www.washingtonpost.com/business/2021/09/21/new-cooperative-hack-ransomware/> adresinden alınmıştır
- BooksPOS. (tarih yok). *A brief History of POS*. <https://www.bookspos.com/history-of-pos-system-why-is-it-relevant-today/> adresinden alınmıştır
- Borah, C. K. (2015). Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake. *Strategic Analysis*, 39(4), 458-560.
- Borghard, E. (2018). *Protecting Financial Institutions Against Cyber Threats: A National Security Issue*. Carnegie Endowment for International Peace .

- <https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324> adresinden alınmıştır
- Botelho, B. (2022). *SolarWinds breach news center*. <https://www.techtarget.com/searchsecurity/essentialguide/SolarWinds-breach-news-center> adresinden alındı
- Boudette, N. E. (2020). *Tesla Shines During the Pandemic as Other Automakers Struggle*. <https://www.nytimes.com/2020/07/02/business/tesla-sales-second-quarter.html> adresinden alınmıştır
- Boulanin, V., & Ogilvie-White, T. (2017). *Cyber Threats and Nuclear Dangers. PolicyBrief, No.17*.
- Bouso, R. (2019, 01 18). *After billion-barrel bonanza, BP goes global with seismic tech*. <https://www.reuters.com/article/us-bp-seismic-focus-idUSKCN1PC0HF> adresinden alınmıştır
- BP . (2017). *Caltech startup, Beyond Limits secures investment of \$20 million from BP Ventures*. <https://www.bp.com/en/global/corporate/news-and-insights/press-releases/caltech-startup-beyond-limits-secures-investment-of-20-million-from-bp-ventures.html> adresinden alınmıştır
- Bozkanat, E., & Çömlekçi, M. F. (2020). *Yeni Medya Çalışmalarının Geleceği ve Büyük Veri Kaynaklı Riskler: Bir Delfi Çalışması . Istanbul University Journal of Communication Sciences, Vol:58, 73-64*.
- Brand Finance. (2022). *Automotive Industry 2022* .
- Brundtland Commission. (1987). *Our Common Future*. Oslo: Oxford University Press.
- Bove, T. (2022). *The chip shortage claims another victim as Honda cuts 40% of vehicle production in Japan* . <https://fortune.com/2022/09/22/chip-shortage-honda-japan-production-cutbacks/> adresinden alınmıştır
- Bowcut, S. (2021). *Cybersecurity in the food and agriculture industry*. <https://cybersecurityguide.org/industries/food-and-agriculture/> adresinden alınmıştır
- Bowen, A. S. (2021). *Russian Military Intelligence: Background and Issues for Congress*. Congressional Research Service (CRS): <https://sgp.fas.org/crs/intel/R46616.pdf> adresinden alınmıştır
- Boyle, K. (2019). *How One Email Cost a Company \$56 Million*. <https://www.cyberriskopportunities.com/how-one-email-cost-a-company-56-million/> adresinden alınmıştır

- Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. O. D. Jens, K. Govern, & C. Finkelstein içinde, *Cyberwar: Law and Ethics for Virtual Conflicts* (s. 102-126). Oxford University Press.
- Bradbury, D. (2017). *4 Ways Johnson & Johnson Is Leading the Fight Against Cyberattackers*. <https://www.jnj.com/innovation/johnson-and-johnson-leading-fight-to-prevent-cyberattacks> adresinden alınmıştır
- BrandFinance. (2023). *Tesla dépasse Mercedes-Benz et Toyota pour prendre la pole position en tant que marque automobile la plus valorisée au monde*. <https://brandfinance.com/press-releases/tesla-depasse-mercedes-benz-et-toyota-pour-prendre-la-pole-position-en-tant-que-marque-automobile-la-plus-valorisee-au-monde> adresinden alınmıştır
- Brigham, K. (2023). *How conflict minerals make it into our phones*. <https://www.cnbc.com/2023/02/15/how-conflict-minerals-make-it-into-our-phones.html> adresinden alınmıştır
- Brown, G. D., & Metcalf, A. O. (2014). Easier Said Than Done: Legal Reviews of Cyber Weapons. *Journal of National Security Law & Policy*, 7(15), 115-138.
- Burgess, J. (2022). *Malware and Exploits on the Dark Web*. Queen's University Belfast.
- Bushell, C. (2022). *The Impact of Metaverse on Branding and Marketing - A Study of How Individuals and Celebrities Use Metaverse as a Brand Extension, and the Implications for Marketing*. London: Westminster Business School.
- Burton, J. (2019). Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation. *Baltic Journal of European Studies*, 9(3), 116-133.
- Büyükgöze, S., & Dereli, E. (2019). Toplum 5.0 ve Dijital Sağlık. *Güncel Sağlık Bilimleri Çalışmaları II* (s. 13-27). içinde Ankara: Akademisyen Kitapev .
- C3.AI. (2018). *Shell Selects C3.ai as Strategic AI Software Platform*. <https://c3.ai/shell-selects-c3-ai-as-strategic-ai-software-platform/> adresinden alınmıştır
- CAC. (2021a). *Cybersecurity Review Measures (Revised, Draft for Comment)*. http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm.
- Canalys. (2020). *Global smartphone market Q4 and full year 2019*. <https://www.canalys.com/newsroom/canalys-global-smartphone-market-q4-2019> adresinden alınmıştır

- Canbek, G., & Sağıroğlu, Ş. (2013). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 22(1), 121-136.
- Candemir, G. (2020). *Bankacılık Sektöründe Yeni Trendler ve Teknolojik Gelişmeler: Fintek Sektörü Üzerine Bir Uygulama*. İstanbul: Marmara Üniversitesi Doktora Tezi.
- Canfil, J. K. (2016). Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity. *The Cyber Issue*, 70(1), 217-226.
- Capital One. (tarih yok). *Meet Eno*. <https://www.capitalone.com/digital/eno/> adresinden alınmıştır
- Carnegie Council. (2021). *A Human Rights Approach to U.S. Cybersecurity Strategy*. <https://www.carnegiecouncil.org/media/article/a-human-rights-approach-to-u-s-cybersecurity-strategy> adresinden alınmıştır
- Carpenter, G. (2021). *Siegfried starts to ramp up production after cyber attack*. <https://www.cphi-online.com/siegfried-starts-to-ramp-up-production-after-news112548.html> adresinden alınmıştır
- Carter, W. A. (2017). Forces Shaping the Next Generation of Cyber Threats to Financial Institutions . *SWIFT INSTITUTE* .
- Cavelty, M. D. (2012). The militarisation of cyber security as a source of global tension. D. Möckli içinde, *STRATEGIC TRENDS 2012 Key Developments in Global Affairs* (s. 103-124). Zurich: Center for Security Studies.
- Center for Internet Security [CIS]. (tarih yok). *Cyber Attacks: In the Healthcare Sector*. Center for Internet Security Blog Posts. <https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector> adresinden alınmıştır
- Centrum Analiz Propagandy i Dezinformacji [CAPD]. (2017, 05 25). *Analysis of the Russian "Strategy for the Development of an Information Society"*. <https://capd.pl/en/analyses/185-analysis-of-the-russian-strategy-for-the-development-of-an-information-society> adresinden alınmıştır
- CERT-UA. (2022). *Фрагмент дослідження кібератак*. Computer Emergency Response Team of Ukraine. <https://cert.gov.ua/article/18101> adresinden alındı
- Central Cyberspace Affairs Commission. (2021). *Translation: 14th Five-Year Plan for National Informatization*. <https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/> adresinden alınmıştır

- Chakya, D. (2021). *50,000 security disasters waiting to happen: The problem of America's water supplies.* NBC News. <https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206> adresinden alınmıştır
- Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., & Zhipeng, Z. (2019). The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. Guilin: IEEE.
- Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M., & Shenoi, S. (2007). Security strategies for scada networks. *Critical Infrastructure Protection*, 253, 117–131.
- Chainalysis. (2022). *As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict.* <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/> adresinden alındı
- Chang, B. (2021). *One of the biggest US insurance companies reportedly paid hackers \$40 million ransom after a cyberattack.* Business Insider. <https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5> adresinden alındı
- Chase. (tarih yok). *Chase Mobile Banking.* <https://www.chase.com/business/mobile-login> adresinden alınmıştır
- Check Point. (2021). *Ransomware attacks continue to Surge, hitting a 93% increase year over year.* <https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/> adresinden alınmıştır
- Chen, P., Desmet, L., & Huygens, C. (2014). A Study on Advanced Persistent Threats. *IFIP International Conference on Communications and Multimedia Security*, 63-72.
- Cheney, C. (2019). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. *Issues & Insights Working Paper, Vol:19*.
- Cherepanov, A. (2017). *WIN32/INDUSTROYER A new threat for industrial control systems.* ESET.
- China.org.cn. (2007). *Computer Server Operating System Developed.* <http://www.china.org.cn/english/China/191263.htm> adresinden alınmıştır
- China.org. (2016). *Joint statement between the presidents of China and Russia.* http://www.china.org.cn/chinese/2016-06/27/content_38756664.htm adresinden alınmıştır

- Chinese Academy of Cyberspace Studies. (2021). *China Internet Development Report 2019*. Beijing: Springer Singapore.
- China's State Council Information Office. (2022). *Jointly Build a Community with a Shared Future in Cyberspace*. <https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html> adresinden alınmıştır
- Chien, C.-F., Hong, T.-Y., & Guo, H.-Z. (2017). An empirical study for smart production for TFTLCD to empower Industry 3.5 . *Journal of the Chinese Institute of Engineers*, 40(7), 552-561.
- Chime. (tarih yok). *Find ATMs in your network*. <https://www.chime.com/atms/> adresinden alınmıştır
- Chong, G. (2020). *Huawei - Chinese Telecommunications Giant Huawei: Strategies to Success*. Nanyang Technopreneurship Case Centre.
- Christensen, J. (1999). *The trials of Kevin Mitnick*. CNN. <http://edition.cnn.com/SPECIALS/1999/mitnick.background/> adresinden alındı
- Chorzempa, M. (2021). China, the United States, and central bank digital currencies: how important is it to be first? *China Economic Journal*, 14(1), 102-115.
- Chuen, D. L., & Teo, G. S. (2015). Emergence of FinTech and the LASIC Principles. *Journal of Financial Perspectives*, 3(3), 1-26.
- CIA, FBI, & Press, P. H. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Intelligence Community Assesment.
- CISA. (tarih yok). *Appendix A: Chemicals of Interest (COI)*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/appendix-chemicals-interest> adresinden alınmıştır
- CISA. (tarih yok(a)). *Critical Manufacturing Sector*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/critical-manufacturing-sector> adresinden alınmıştır
- CISA. (tarih yok (b)). *Commercial Facilities Sector*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/commercial-facilities-sector> adresinden alınmıştır
- CISA. (tarih yok (c)). *Government Facilities Sector*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/government-facilities-sector> adresinden alınmıştır

- CISA. (tarih yok(d)). *The Cyber Safety Review Board*. <https://www.cisa.gov/cyber-safety-review-board> adresinden alınmıştır
- CISA. (tarih yok(e)). *Emergency Services Sector*. <https://www.cisa.gov/emergency-services-sector> adresinden alınmıştır
- CISA. (2013). *WordPress Sites Targeted by Mass Brute-force Botnet Attack*. <https://www.cisa.gov/news-events/alerts/2013/04/15/wordpress-sites-targeted-mass-brute-force-botnet-attack> adresinden alınmıştır
- CISA. (2015). *Water and Wastewater Systems Sector-Specific Plan*. <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf>: DHS, EPA.
- CISA. (2015a). *Cybersecurity Information Sharing Act of 2015 Procedures and Guidance*.
- CISA. (2016). *A Reference Guide for the Critical Infrastructure Community. Cybersecurity and Infrastructure Security Agency*. <https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf> adresinden alınmıştır
- CISA. (2019). *Security Agency's Emergency Directive 19-01* . <https://www.cisa.gov/emergency-directive-19-01> adresinden alınmıştır
- CISA. (2020). *Guidance on the North Korean Cyber Threat* .
- CISA. (2020a). *FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks*.
- CISA. (2021). *Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise*. CISA.
- CISA. (2022). *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, Alert (AA22-011A)*. 05 Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/uscert/ncas/alerts/aa22-011a> adresinden alındı
- CISA. (2022a). *TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies, Alert (AA22-108A)*. Cybersecurity and Infrastructure Security Agency: <https://www.cisa.gov/uscert/ncas/alerts/aa22-108a> adresinden alındı
- CISA. (2022b). *CISA Strategic Plan 2023-2025*. Cybersecurity and Infrastructure Security Agency's. https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf adresinden alınmıştır

- Cimpanu, C. (2018). *Former Employee Arrested for Trying to Sell Company's Database for \$4,000*.
<https://www.bleepingcomputer.com/news/security/former-employee-arrested-for-trying-to-sell-companys-database-for-4-000/> adresinden alındı
- Cimpanu, C. (2018a.). *Russian Nuke Scientists, Ukrainian Professor Arrested for Bitcoin Mining*.
<https://www.bleepingcomputer.com/news/cryptocurrency/russian-nuke-scientists-ukrainian-professor-arrested-for-bitcoin-mining/> adresinden alındı
- CipherTrace. (2021). *Cryptocurrency Crime and Anti-Money Laundering Report, August 2021*. <https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/> adresinden alındı
- Citi Group. (2020). *A New Way to Bank Nationwide on Google Pay*.
<https://www.citigroup.com/global/news/perspective/2020/a-new-way-to-bank-nationwide-on-google-pay> adresinden alınmıştır
- Citi Group. (2022). *Citi Named World's Best Digital Bank and Best Corporate/Institutional Digital Bank by Global Finance Magazine*.
<https://www.citigroup.com/citi/news/2022/221026b.htm> adresinden alınmıştır
- Cloherly, J. (2012). *Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'*.
<https://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875> adresinden alındı
- CNCERT/CC. (tarih yok). *National Computer Network Emergency Response Technical Team/Coordination Center of China*.
<https://www.cert.org.cn/publish/english/index.html> adresinden alınmıştır
- CNET. (2003). *China to view Windows code*. <https://www.cnet.com/tech/tech-industry/china-to-view-windows-code/> adresinden alındı
- CNN. (1999). *NSA key to Windows: an open question*. Cable News Network.
<http://edition.cnn.com/TECH/computing/9909/03/windows.nsa.02/> adresinden alındı
- Colatin, T. S. (2007). *Cyber attacks against Estonia (2007)* . CyberLaw.
[https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_\(2007\)](https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)) adresinden alınmıştır
- Collins-Fattedad, S., DeVito, M., Goes, Y., Khorenyan, M., & Milgrim, L. (2022). *Towards A Global Digital Governance Architecture: Mapping Pathways for Cooperation and Inclusion*. United Nations.

- Congress.gov. (2018). *H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018* . <https://www.congress.gov/bill/115th-congress/house-bill/3359> adresinden alınmıştır
- Congressional Research Service [CRS]. (2020). *Iranian Offensive Cyber Attack Capabilities*. <https://sgp.fas.org/crs/mideast/IF11406.pdf> adresinden alınmıştır
- Congressional Research Service [CRS]. (2022). *Russian Cyber Units*. Congressional Research Service . <https://crsreports.congress.gov/product/pdf/IF/IF11718> adresinden alınmıştır
- Connell, M. (2014). *Deterring Iran's Use of Offensive Cyber: A Case Study*. Washington, VA : CNA Analysis & Solutions.
- Comiter, M. (2019). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Commission of the European Communities . (2007). *Towards a general policy on the fight against cyber crime*. Brussels.
- Committee to Protect Journalists [CPJ]. (2021). *Iran's parliament moves forward with troubling bill to further restrict internet*. <https://cpj.org/2021/11/iran-parliament-bill-restrict-internet/> adresinden alınmıştır
- CompaniesMarketCap.com. (2023). *Largest tech companies by market cap*. <https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/> adresinden alınmıştır
- Community Banking. (2020). *Community Banking in the 21st Century 2020* . https://www.csbs.org/sites/default/files/2020-09/cb21publication_2020.pdf adresinden alınmıştır
- Community Banking. (2021). *CSBS 2021 National Survey of Community Banks*. <https://resources.gabankers.com/e-Bulletin/2021/Oct.%208/CSBS%20Community%20Bank%202021%20Survey.pdf> adresinden alınmıştır
- Cook, C., Schaafsma, J., & Antheunis, M. (2017). Under the bridge: An in-depth examination of online trolling in the gaming context. *New Media & Society*, 20(4), 3323-3340.
- Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2009). *The Agreement on the Information Security Area*. <https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf> adresinden alınmıştır

- Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound*, Vol:111, 207-2012.
- Costello, J. (2016). *China's Cyber-Focused Military Unit Emerges from the Shadows*. <https://international.thenewslens.com/article/58081> adresinden alınmıştır
- Costello, J. (2016a). *China Finally Centralizes Its Space, Cyber, Information Forces*. The Diplomat: <https://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/> adresinden alınmıştır
- Council of Europe. (2001). *Convention on Cybercrime*. Budapest: European Treaty Series - No. 185.
- Council of Europe [COE]. (2004). *Details of Treaty No.185*. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185> adresinden alınmıştır
- Council of the European Union. (2017). *Council conclusions: 14435/17* . Brussels.
- Costello, J., & McReynolds, J. (2018). *China's Strategic Support Force: A Force for a New Era*. Washington, D.C: Center for the Study of Chinese Military Affairs.
- Craig, G. (2018). *Dated Brent Goes Dutch*. <https://ursaspace.com/blog/dated-brent-goes-dutch/> adresinden alınmıştır
- Creemers, R. (2016, 12 27). *National Cyberspace Security Strategy*.
- Culafi, A. (2021). *The wide web of nation-state hackers attacking the U.S*. Search Security: <https://www.techtarget.com/searchsecurity/news/252499613/The-wide-web-of-nation-state-hackers-attacking-the-US> adresinden alındı
- Cyble Research . (2022). *'BidenCash' Strikes Again: Over 1.2 Million Compromised Payment Cards Data Leaked* . <https://blog.cyble.com/2022/10/07/bidencash-strikes-again-over-1-2-million-compromised-payment-cards-data-leaked/> adresinden alınmıştır
- Cyberspace Administration of China [CAC]. (2021). *国家互联网信息办公室关于《网络数据安全条例（征求意见稿）》公开征求意见的通知*. http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm adresinden alınmıştır
- Cyberspace Administration of China [CAC]. (2022). *中国国家互联网信息办公室与印尼国家网络与密码局签署网络安全合作行动计划* . http://www.cac.gov.cn/2022-07/29/c_1660713333439712.htm adresinden alınmıştır

- Cyber Security Connect. (2022). *Experts Concerned About China's Cyber Security Interests in Indonesia* . <https://www.cybersecurityconnect.com.au/policy/8063-china-s-interest-in-indonesia-cyber-security-a-concern-experts-say> adresinden alınmıştır
- Cyberwarcon. (2021). Their Own Little War: Iran Adopts Disruptive Ransomware: <https://www.cyberwarcon.com/their-own-little-war> adresinden alındı
- Çahmutoğlu, E. (2020). Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi. *Analitik Politika*, 1(1).
- Çahmutoğlu, E. (2021). *İran'ın Siber Gücü*. Ankara : İram Yayınları.
- Çakal, K., Kara, İ., & Aydos, M. (2021). Cyber Security of Connected Autonomous Vehicles . *Avrupa Bilim ve Teknoloji Dergisi*, Sayı:32, 1121-1128.
- Çalık, M., & Sözbilir, M. (2014). İçerik Analizinin Parametreleri. *Eğitim ve Bilim*, 39(174), 33-38.
- Çatal, S., & Yılmaz, B. A. (2021). Küresel Sistem İçerisinde Çin'in Kuşak ve Yol İnisiyatifi'nin Ekonomipolitik Bir Değerlendirmesi ve Türkiye Üzerindeki Etkileri. *Anadolu Akademi Sosyal Bilimler Dergisi*, 3(3), 567 - 579.
- Çelik, E. (2018). Deep Web ve Dark Web: İnternet'in Derin Dünyası. *Cyberpolitik Journal*, Cilt 2, Sayı 4, 148 - 162.
- Çelik, S. (2018). Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım. *Academic Review of Humanities and Social Sciences*, 1(2), 110 - 119.
- Çelik, Ş. (2013). Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), 137-175.
- Çifci, H. (2012). *Her Yönüyle Siber Savaş*. Ankara: TÜBİTAK.
- Çokbıdık, C. A. (2018). Siber Uzay ve İnsan Hakları. *Cyberpolitik Journal* Vol:3, No:5, 133-157.
- Dapp, T. F. (2014). *Fintech – The digital (r)evolution in the financial sector*. Deutsche Bank .
- Darıcı, A. B. (2017). Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi. *Ulusa: Uluslararası Çalışmalar Dergisi*, (1)1, 1-24.
- Darıcı, A. B., & Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. *Bilig*, Sayı: 83, 121 - 146.

- Darıcı, A. B., & Özdal, B. (2018). Analysis of the Cyber Security Strategies of People's Republic of China. *Güvenlik Bilimleri Dergisi*, 14(28), 1-35.
- Das, R. (2021). *Asymmetric Cyber Warfare*. 06 21, 2022 tarihinde <https://platform.keesingtechnologies.com/asymmetric-cyber-warfare-part-1/> adresinden alındı
- Davis, J. (2007). *Hackers Take Down the Most Wired Country in Europe*. Wired: <https://www.wired.com/2007/08/ff-estonia/> adresinden alınmıştır
- Davis, M. (2022). *Chinese cyber attack on Australia targets defence and energy information in months-long hack*. <https://www.skynews.com.au/australia-news/chinese-cyber-attack-on-australia-targets-defence-and-energy-information-in-monthslong-hack/news-story/23f55f01c93e7b5827f20bf48cfdef67> adresinden alınmıştır
- Day, J. (2022). *Cybersecurity In Digital Banking: Everything You Need To Know*. <https://stefanini.com/en/insights/articles/cybersecurity-in-digital-banking-everything-you-need-to-know> adresinden alınmıştır
- Defense Information Systems Agency [DISA]. (tarih yok). *DISA's Mission Partner Support*. <https://disa.mil/About/Our-Work/Mission-Partners> adresinden alınmıştır
- Defense Intelligence Agency [DIA]. (2019). *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance*. Tehran: Islamic Republic of Iran Broadcasting (IRIB).
- Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M., & Tani, S. (2020). What Is Society 5.0? *Society 5.0, A People-centric Super-smart Society* (s. 1-23). içinde Tokyo: Springer Open.
- DeGrasse, M. (2016). *Pumping profits: Shell saves \$1M with IoT*. <https://www.rcrwireless.com/20160415/internet-of-things/pumping-profits-shell-saves-1m-iot> adresinden alınmıştır
- Deloitte Touche Tohmatsu Limited [DTTL]. (tarih yok). Global Cyber Executive Briefing; Telecommunications: <https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/Telecommunications.html> adresinden alınmıştır
- Deloitte . (2017). *Industry 4.0 and cybersecurity. Managing risk in an age of connected production* . Deloitte University Press .
- Deloitte. (2020). *Global Cyber Executive Briefing*. <https://www.deloitte.com/global/en/services/risk-advisory/research/Telecommunications.html> adresinden alınmıştır

- Dennis, L., Rajtmajer, S., & Grady, C. (2020). Analyzing cyber-physical threats to Pennsylvania dams through a lens of vulnerability . *IEEE International Symposium on Technology and Society (ISTAS)* , (s. 1-8). Tempe.
- Department of Defense Cyber Crime Center [DC3]. (tarih yok). *DC3 Mission Overview*. <https://www.dc3.mil/> adresinden alınmıştır
- Deutsche Bank. (2019). *Deutsche Bank acquires a 5 percent stake in fintech Deposit Solutions*. <https://www.db.com/news/detail/20190919-deutsche-bank-acquires-a-5-percent-stake-in-fintech-deposit-solutions> adresinden alınmıştır
- Deutsche Bank. (2020). *Deutsche Bank to invest in financing platform Traxpay*. https://www.db.com/news/detail/20200724-deutsche-bank-to-invest-in-financing-platform-traxpay?language_id=1 adresinden alınmıştır
- DFNC. (2021, 01 27). *A Cybersecurity Agreement Between Russia & Iran*. New Defense Order Strategy. <https://dfnc.ru/en/cyber/a-cybersecurity-agreement-between-russia-iran/> adresinden alınmıştır
- DHS. (tarih yok). *National Infrastructure Protection Plan Government Facilities Sector*. U.S. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/nipp_governmt.pdf adresinden alınmıştır
- DHS. (tarih yok(a)). *US-CERT Computer Emergency Readiness Team*. https://www.cisa.gov/uscert/sites/default/files/publications/infosheet_US-CERT_v2.pdf adresinden alınmıştır
- DHS. (tarih yok(b)). *National Cybersecurity and Communications Integration Center*. <https://www.hsdl.org/c/abstract/?docid=798888> adresinden alınmıştır
- DHS. (tarih yok(c)). *Cybersecurity*. <https://www.dhs.gov/topics/cybersecurity> adresinden alınmıştır
- DHS. (2014). *Sector Risk Snapshots*. U.S. Department of Homeland Security. The Office of Cyber and Infrastructure Analysis (OCIA).
- DHS. (2016). *Introduction to the Commercial Facilities Sector-Specific Agency*. U.S. Department of Homeland Security (DHS).
- Detica, J. G. (2012). *Organised Crime in the Digital Age*. BAE Systems. <https://www.baesystems.com/en/article/bae-systems-research-reveals-the-real-perpetrators-of-digital-crime> adresinden alındı
- Dickinson, B. (2021). *Cyber Threats Facing the Chemicals Industry*. <https://www.chemengonline.com/cyber-threats-facing-the-chemicals-industry/> adresinden alınmıştır

- Digital Watch. (2016). *India and Russia signed a cybersecurity agreement*. <https://dig.watch/updates/india-and-russia-signed-cybersecurity-agreement> adresinden alınmıştır
- Dimitrova, M. (2020). *Remove Snake Ransomware Virus – What You Should Know about It*. <https://sensorstechforum.com/remove-snake-ransomware/> adresinden alınmıştır
- Diners Club International. (tarih yok). *Diners Club History*. <https://www.dinersclub.com/about-us/history/> adresinden alınmıştır
- DNV GL. (2020). *New Directions, Complex Choices: The outlook for the oil and gas industry in 2020*. Hovik, Norway: Det Norske Veritas (Norway) and Germanischer Lloyd (Germany).
- DOJ. (tarih yok). *United States District Court Southern District of New York*. U.S. Department of Justice. <https://www.justice.gov/opa/file/834996/download> adresinden alınmıştır
- DOD. (2006). *National Military Strategy for Cyberspace Operations*. Washington, D.C.: NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS.
- DOD. (2008). *2008 National Defense Strategy*. https://history.defense.gov/Portals/70/Documents/nds/2008_NDS.pdf?ver=WEYyBjnf6UkNioPqfkSr3Q%3d%3d adresinden alınmıştır
- DOD. (2010). *Department of Defense Dictionary of Military and Associated Terms*. U.S. Department of Defence. Federation of American Scientist.
- DOD. (2010a). *U.S. Cyber Command Fact Sheet*. Department of Defense.
- DOD. (2015a). *The DOD Cyber Strategy*. Washington, DC: The Department of Defense.
- DOD. (2018). *Department of Defense Cyber Strategy*. Washington: Department of Defense.
- DOD. (2022). *Secretary of Defense Lloyd J. Austin III Opening Remarks at a U.S.-India 2+2 Joint Press Availability*. <https://www.defense.gov/News/Transcripts/Transcript/Article/2996798/secretary-of-defense-lloyd-j-austin-iii-opening-remarks-at-a-us-india-22-joint/> adresinden alınmıştır
- DOJ. (2003). *The Shadowcrew Criminal Organization / SSC/2003R01260*. District of New Jersey: United States District Court.

- DOJ. (2008). U.S. Department of Justice. <https://www.justice.gov/opa/press-release/file/1092091/download> adresinden alınmıştır
- DOJ. (2011). *The FBI's Ability to Address the National Security Cyber Intrusion Threat*. U.S. Department of Justice Office of the Inspector General Audit Division.
- DOJ. (2016). *ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison*. U.S. Department of Justice. <https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison> adresinden alındı
- DOJ. (2016a). *Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities*. <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated> adresinden alınmıştır
- DOJ. (2016b). *Conspiracy to Commit Computer Hacking-ITSEC TEAM*. <https://www.justice.gov/opa/file/834996/download> adresinden alınmıştır
- DOJ. (2018). *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. U.S. Department of Justice. <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and> adresinden alınmıştır
- DOJ. (2020). *Former employee of medical packaging company charged with sabotaging electronic shipping records leading to the delay of PPE to healthcare providers*. U.S. Attorney's Office Northern District of Georgia.
- DOJ. (2020a). *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research*. Washington. <https://www.justice.gov/opa/press-release/file/1295981/download>. <https://www.justice.gov/opa/press-release/file/1295981/download> adresinden alınmıştır
- DOJ. (2021). *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*.
- Dooley, B., & Ueno, H. (2020). *Honda Hackers May Have Used Tools Favored by Countries*. New York Times. <https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html> adresinden alınmıştır

- Dooley, B., & Ueno, H. (2022). *Toyota stops production in Japan after a cyberattack at a supplier*. <https://www.nytimes.com/2022/02/28/business/toyota-stoppage-cyberattack.html> adresinden alınmıştır
- Dominguez, G. (2022). *As Japan's neighbors ramp up offensive capabilities in cyberspace, SDF aims to bolster defense*. <https://www.japantimes.co.jp/news/2022/09/08/national/sdf-cyber-defense-boost/> adresinden alınmıştır
- Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 94(886), 533-578.
- Drozhzhin, A. (2015). *Black Hat USA 2015: The full story of how that Jeep was hacked*. <https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/> adresinden alınmıştır
- Duffy, C. (2021, 03 10). *Here's what we know so far about the massive Microsoft Exchange hack*. CNN: <https://edition.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html> adresinden alınmıştır
- Dziundziuk, V. (2011). *Stopping Cyberterror*. PerConcordiam, 17-21.
- DQ India. (2017). *India-CERT signs an MoU with US-CERT*. <https://www.dqindia.com/india-cert-signs-an-mou-with-us-cert/> adresinden alınmıştır
- EasyJet. (2020). *Notice of cyber security incident*. <http://otp.investis.com/clients/uk/easyjet1/rns/regulatory-story.aspx?cid=2&newsid=1391756> adresinden alınmıştır
- Edwards, L. (2006). Dawn of the Death of Distributed Denial of Service: How To Kill Zombies. *Cardozo Arts and Entertainment Law Journal*, 24(1), 23-62.
- Economy, E. C. (2018). *The great firewall of China: Xi Jinping's internet shutdown*. <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown> adresinden alınmıştır
- Elliott, K. (tarih yok). *Why the Chemical Sector is Critical to Modern Infrastructure*. <https://www.cybersaint.io/blog/why-the-chemical-sector-is-critical-to-modern-infrastructure> adresinden alınmıştır
- Emirates News Agency [WAM]. (2015). *ADNOC Grup CEO'su: "Petrol ve Gaz 4.0 Projesi Herşeyi Değiştirecek"*. Wakalat Anba'a al Emarat: <http://wam.ae/tr/details/1395302720854> adresinden alınmıştır

- Eni. (tarih yok). *Digitalization at Eni*. <https://www.eni.com/en-IT/digital-transformation/digitalisation.html> adresinden alınmıştır
- Enisa. (tarih yok). *Man-in-the-Middle*. <https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle> adresinden alınmıştır
- EPA. (2022). *Water Sector Cybersecurity Brief for States*. United States Environmental Protection Agency.
- Ermağan, İ. (2022). Dünya Ekonomisinin Evrim Sürecinde Almanya'nın Dördüncü Sanayi Devrimi. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, Sayı:71, 75-92.
- Esen, B. (2021). Teknoloji Rekabetinde Huawei Bir Tehdit Mi? *Maliye ve Finans Yazıları*, 116, 93-118.
- ESET. (2017). *Industroyer: Biggest malware threat to critical infrastructure since Stuxnet* . <https://www.eset.com/int/industroyer/> adresinden alınmıştır
- ESET. (tarih yok). *Fidye Yazılımı (Ransomware)*.
- Eseye. (2021). *Eseye 2021 State of IoT Adoption Report*. https://www.iotjournal.nl/wp-content/uploads/2021/10/Eseye_2021_State_of_IoT_Adoption_Report.pdf: Eseye Limited.
- Esfandiari, G. (2010). *Basij Members Trained To Conquer Virtual World*. https://www.rferl.org/a/Basij_Members_Trained_To_Conquer_Virtual_World/2134023.html adresinden alınmıştır
- Esfandiari, G. (2020). *Iran To Work With China To Create National Internet System* . <https://www.rferl.org/a/iran-china-national-internet-system-censorship/30820857.html> adresinden alınmıştır
- Etzioni, A. (2011). Cybersecurity in the Private Sector. *Issues in Science and Technology*, 28(1), 58-62.
- EU. (2019). *Council Decision*, 7299/19. Bussels: Council of the European Union.
- Euronews. (2023). *Ukrayna işgalinin yıl dönümü: AB'nin Rusya'dan enerji ithalatı nasıl değişti?* <https://tr.euronews.com/2023/02/24/ukrayna-isgalinin-yil-donumu-abnin-rusyadan-enerji-ithalati-nasil-degisti> adresinden alınmıştır
- EuroNews. (2023a). *Ukrayna işgalinin yıl dönümü: AB'nin Rusya'dan enerji ithalatı nasıl değişti?* <https://tr.euronews.com/2023/02/24/ukrayna-isgalinin-yil-donumu-abnin-rusyadan-enerji-ithalati-nasil-degisti> adresinden alınmıştır

- European Council. (2022). *European Council, 24-25 March 2022* .
<https://www.consilium.europa.eu/en/meetings/european-council/2022/03/24-25/> adresinden alınmıştır
- European Council for an Energy Efficient Economy [ECEEE]. (2020a). *EU to target 30 million electric cars by 2030*. [https://www.eceee.org/all-news/news/eu-to-target-30-million-electric-cars-by-2030/#:~:text=\(EurActiv%2C%207%20Dec%202020\),to%20a%20draft%20EU%20document](https://www.eceee.org/all-news/news/eu-to-target-30-million-electric-cars-by-2030/#:~:text=(EurActiv%2C%207%20Dec%202020),to%20a%20draft%20EU%20document). adresinden alınmıştır
- European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission .
- European Commission. (2022a). *EU Solar Energy Strategy*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0221&from=EN> adresinden alınmıştır
- European Commission. (2023). *European Green Deal: EU agrees stronger legislation to accelerate the rollout of renewable energy*. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2061 adresinden alınmıştır
- European External Action Service [EEAS]. (2022). *Cybersecurity: EU holds 8th dialogue with the United States*. https://www.eeas.europa.eu/eeas/cybersecurity-eu-holds-8th-dialogue-united-states_en adresinden alınmıştır
- European Union Agency for Cybersecurity [ENISA]. (2021). *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*. <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving> adresinden alınmıştır
- EUROSTAT. (tarih yok). *Shedding light on energy - 2023 edition* .
<https://ec.europa.eu/eurostat/web/interactive-publications/energy-2023> adresinden alınmıştır
- Evans, P. C., & Annunziata, M. (2012). *Industrial Internet: Pushing the Boundaries of Minds and Machines*. General Electric.
- Evans, S. (2022). *What can digitalisation do for the oil and gas supply chain?* <https://www.offshore-technology.com/features/oil-gas-digitalisation-supply-chain/> adresinden alınmıştır
- Eyidilli, S. (2020). *İslami bankacılık uygulaması Niyah, İngiltere'de faaliyete geçti*. <https://webrazzi.com/2020/01/22/islami-bankacilik-niyah/> adresinden alınmıştır

- Farmer, B. (2019). *Cyber crime warning as experts say hackers deliberately target hospitals*. <https://www.telegraph.co.uk/global-health/terror-and-security/cyber-crime-warning-experts-say-hackers-deliberately-target/> adresinden alınmıştır
- Farnsworth, T. (tarih yok). *Study Sees Cyber Risk for U.S. Arsenal*. Arms Control Association .
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Global Politics and Strategy*, 53(1), 23-40.
- FAS. (2009). *Cyberspace Policy Review*. <https://nsarchive.gwu.edu/sites/default/files/documents/2700108/Document-28.pdf> adresinden alınmıştır
- FAS. (2000). *National Plan for Information National Plan for Information Version 1.0*. Washington: The White House.
- FAS. (2000a). *James Adams* . https://irp.fas.org/congress/2000_hr/030200_adams.htm adresinden alınmıştır
- FBI. (tarih yok). *Law Enforcement Cyber Incident Reporting*. <https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view> adresinden alınmıştır
- FBI. (tarih yok(a)). *Mission & Priorities*. <https://www.fbi.gov/about/mission> adresinden alınmıştır
- FBI. (tarih yok(b)). *National Cyber Investigative Joint Task Force*. <https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force> adresinden alınmıştır
- FBI. (2011). *Law Enforcement at Risk for Harassment and Identity Theft through Cyber Intelligence Section : Federal Bureau of Investigation Intelligence Bulletin*. <https://publicintelligence.net/ufouo-fbi-threat-to-law-enforcement-from-doxing/> adresinden alınmıştır
- FBI. (2021). *Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks*. <https://www.documentcloud.org/documents/21053966-fbi-bc-cyber-criminal-actors-targeting-the-food-and-agriculture-sector-with-ransomware-attacks>: FBI Cyber Division.
- FBI. (2021a). *Russian FSB Center 16 Hackers*. <https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet> adresinden alınmıştır

- FBI. (2021b). FBI Statement on Compromise of Colonial Pipeline Networks. <https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks> adresinden alınmıştır
- Feakin, T. (2013). *Enter the Cyber Dragon: Understanding Chinese intelligence agencies' cyber capabilities*. Australian Strategic Policy Institute [ASPI].
- Federation of American Scientists [FAS]. (1998). *Presidential Decision Directive 63*. The White House. Washington.
- Federal Election Commission [FEC]. (2016). *2015-2016 Disbursements*. https://www.fec.gov/data/disbursements/?data_type=processed&committee_id=C00580100&recipient_name=cambridge+analytica&two_year_transaction_period=2016&min_date=01%2F01%2F2015&max_date=12%2F31%2F2016 adresinden alınmıştır
- Federal Trade Commission [FTC]. (2019, 07 24). *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> adresinden alınmıştır
- Federal Reserve . (1993). *Banking Act of 1933 (Glass-Steagall)*. <https://www.federalreservehistory.org/essays/glass-steagall-act> adresinden alınmıştır
- Federal Reserve. (tarih yok). *Federal Reserve History*. Stock Market Crash of 1929: <https://www.federalreservehistory.org/essays/stock-market-crash-of-1929> adresinden alınmıştır
- Financial Times. (2022). *Ukraine war is chip industry's kryptonite*. <https://www.ft.com/content/950072f0-8c22-4050-bc63-631fa4b481eb> adresinden alınmıştır
- Financial Times. (2022a). *US struggles to mobilise its East Asian 'Chip 4' alliance*. <https://www.ft.com/content/98f22615-ee7e-4431-ab98-fb6e3f9de032> adresinden alınmıştır
- Financial Times. (2022b). *China's Big Fund corruption probe casts shadow over chip sector*. <https://www.ft.com/content/8358e81b-f4e7-4bad-bc08-19a77035e1b4> adresinden alınmıştır
- Finkle, J. (2016). *J&J warns diabetic patients: Insulin pump vulnerable to hacking*. Reuters. <https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L> adresinden alınmıştır
- FitzGerald, M. C. (1996). *Russian Views on Electronic and Information Warfare*. Washington, DC: Hudson Institute.

http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf
adresinden alınmıştır

Fitzpatrick, T. (2017). *A brief history of the internet*. <https://sciencenode.org/feature/a-brief-history-of-the-internet-.php> adresinden alınmıştır

Fischer-Hübner, S. (1998). Privacy and security at risk in the global information society. *Information, Communication & Society*, 1(4), 420-441.

Fool. (2023). *The Largest Companies by Market Cap in 2023*. <https://www.fool.com/research/largest-companies-by-market-cap/> adresinden alınmıştır

Ford, C. A. (2020). U.S. National Security Export Controls and Huawei: The Strategic Context in Three Framings. *Arms Control and International Security Papers*, 1(8).

Foster, W., & Goodman, S. (2000). *The diffusion of the Internet in China*. Center for International Security and Cooperation (CISAC).

FoxNews. (2015). *It's an All-Out Cyber War as U.S. Hackers Fight Back at China*. <https://www.foxnews.com/story/its-an-all-out-cyber-war-as-u-s-hackers-fight-back-at-china> adresinden alınmıştır

Fox News. (2015). *Anonymous linked to hack of Albuquerque police amid shooting protests*. <https://www.foxnews.com/us/anonymous-linked-to-hack-of-albuquerque-police-amid-shooting-protests> adresinden alınmıştır

FRS, CSBS, FDIC. (2021). Community Banking in the 21st Century. *Ninth Annual Community Banking Research and Policy Conference*. Community Banking in the 21st Century 2021.

Fukuyama, M. (2018). Society 5.0: Aiming for a New Human-Centered Society. *Japan SPOTLIGHT*, 47-50.

G7. (2017). *G7 Declaration on Responsible States Behavior in Cyberspace*. Italia .

Gady, F.-S., & Austin, G. (2010). *Russia, The United States and Cyber Diplomacy*. New York: The EastWest Institute.

Gady, F.-S. (2015). *New Snowden Documents Reveal Chinese Behind F-35 Hack*. The Diplomat. <https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/> adresinden alınmıştır

Gallagher, S. (2013). *White House: NSA and Cyber Command to stay under one boss*. Ars Technica: White House. Washginton.

- Gallagher, J. C. (2019). *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*. Congressional Research Service.
- Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Journal for Control, Measurement, Electronics, Computing and Communications*, 58(3), 273-286 .
- Gargeyas, A. (2022). *The Chip 4 Alliance Might Work on Paper, But Problems Will Persist*. <https://thediplomat.com/2022/08/the-chip4-alliance-might-work-on-paper-but-problems-will-persist/> adresinden alınmıştır
- Gartzke, E. (2013). The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2), 41-73.
- Gatlan, S. (2021). *T-Mobile discloses data breach after SIM swapping attacks*. <https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/> adresinden alınmıştır
- Gatlan, S. (2022). *Microsoft releases Windows 10 22H2 preview for enterprise testing*. <https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/> adresinden alınmıştır
- Gatlan, S. (2022). *T-Mobile confirms Lapsus\$ hackers breached internal systems* . <https://www.bleepingcomputer.com/news/security/t-mobile-confirms-lapsus-hackers-breached-internal-systems/> adresinden alınmıştır
- Gasser, U., Gassmann, O., Hens, T., Leifer, L., Puschmann, T., & Zhao, L. (2017). *Digital Banking 2025*. Alexandria (University of St.Gallen).
- Geers, K. (2018). *Cyberspace and the Changing Nature of Warfare*. Tallinn: Cooperative Cyber Defence Centre of Excellence [CCDCOE].
- Gerasimov, V. (2016). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations . *Military Review*, 23-26.
- Ghazanchyan, S. (2022). *Armenia, Russia draft agreement on cooperation in cyber security* . Public Radio of Armenia: <https://en.armradio.am/2022/02/10/armenia-russia-draft-agreement-on-cooperation-in-cyber-security/> adresinden alınmıştır
- Gibbs, S. (2015). *Six bailed teenagers accused of cyber attacks using Lizard Squad tool*. *The Guardian*. <https://www.theguardian.com/technology/2015/aug/28/teenagers-arrested-cyber-attacks-lizard-squad-stresser#:~:text=The%20Lizard%20Stresser%20tool%20was,at%20targets%20of%20their%20choosing> adresinden alınmıştır

- Giles, M. (2019). *Triton is the world's most murderous malware, and it's spreading*. MIT Technology Review.
- Giordani, J. (2021). *Cyberattacks On Vehicles Pose A Threat To Drivers And Manufacturers*. Forbes Technology Council. <https://www.forbes.com/sites/forbestechcouncil/2021/12/10/cyberattacks-on-vehicles-pose-a-threat-to-drivers-and-manufacturers/?sh=63610e1e4620> adresinden alınmıştır
- Glaister, D. (2009). *China accused over global computer spy ring*. The Guardian: <https://www.theguardian.com/world/2009/mar/30/china-dalai-lama-spying-computers> adresinden alınmıştır
- Global Data. (2022). *Digitalization in Oil and Gas – Thematic Research*. Londra.
- Global Data. (2022a, 06 23). *TotalEnergies – Digital Transformation Strategies*.
- Global Times. (2021). *China, Indonesia sign MoU on internet security amid Washington pressure on Beijing's 5G technology*. <https://www.globaltimes.cn/page/202101/1212657.shtml> adresinden alınmıştır
- Global Times. (2022). *China's cyberspace whitepaper highlights cooperation, 'fundamentally different' from US' proposition*. <https://www.globaltimes.cn/page/202211/1278895.shtml> adresinden alınmıştır
- Goel, S., & Nussbaum, B. (2021). Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. *IEEE Open Journal of the Communications Society*, vol:2, 1082-1093. <https://ieeexplore.ieee.org/abstract/document/9411871> adresinden alınmıştır
- Goldthau, A., Westphal, K., Bazilian, M., & Bradshaw, M. (2019). How the energy transition will reshape geopolitics?. *Springer Nature*, 569(7754), 29-31.
- Goldman Sachs. (2019). *Goldman Sachs Partners with Apple on a Game-Changing Credit Card*. <https://www.goldmansachs.com/our-firm/history/moments/2019-apple-card.html#:~:text=In%20August%202019%2C%20Apple%20and,revolutionize%20the%20credit%20card%20experience>. adresinden alınmıştır
- Gong, X. (2021). *5G and China-US Relations: Competition and Intervention*. Halifax : Dalhousie University.
- Goosen, E., Nikitenko, S., Kagan, E., & Pakhomova, E. (2020). Toward industry 4.0 in energy sector. *IOP Conference Series: Materials Science and Engineering* .
- Goschenko, S. (2022). <https://news.bitcoin.com/samsung-is-investing-more-than-35-million-in-latam-focused-metaverse-initiatives/>. Bitcoin:

<https://news.bitcoin.com/samsung-is-investing-more-than-35-million-in-latam-focused-metaverse-initiatives/> adresinden alınmıştır

GOV.UK. (2022). *Russia's FSB malign activity: factsheet*. <https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet> adresinden alınmıştır

Government of the Islamic Republic of Iran. (2020). *Iran Thwarts over 412 Million Malware Attacks in One Year: ICT Ministry*. <https://irangov.ir/detail/352536> adresinden alınmıştır

Gönen, S., Yılmaz, E. N., Seda, Ş., Karacayılmaz, G., & Özbirinci, Ö. (2021). Endüstri 4.0'ın Gelişim Sürecinde Unutulan Bileşen: Siber Güvenlik . *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, Sayı:9, 1142-1158.

Goud, N. (tarih yok). *What is Telecom LightBasin Cyber Attack*. <https://www.cybersecurity-insiders.com/what-is-telecom-lightbasin-cyber-attack/> adresinden alınmıştır

Grace, R. (2020). *Shatter the web: Internet fragmentation in Iran* . <https://www.mei.edu/publications/shatter-web-internet-fragmentation-iran> adresinden alınmıştır

Graham, J., Howard, R., & Olson, R. (2011). *Cyber Security Essentials*. Boca Raton: Taylor and Francis Group.

Greenberg, A. (2020). *Russia's GRU Hackers Hit US Government and Energy Targets*. Wired. <https://www.wired.com/story/russia-fancy-bear-us-hacking-campaign-government-energy/> adresinden alınmıştır

Greenberg, A. (2021). *Russian Hackers Are Trying to Brute-Force Hundreds of Networks*. Wired. <https://www.wired.com/story/fancy-bear-russia-brute-force-hacking/> adresinden alınmıştır

Greenwald, G., & MacAskill, E. (2016). Obama orders US to draw up overseas target list for cyber-attacks. The Guardian. <https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas> adresinden alınmıştır

Greig, J. (2021). *Hackers used never-before-seen wiper in recent attack on Iranian train system* . <https://www.zdnet.com/article/hackers-used-never-before-seen-wiper-in-recent-attack-on-iranian-train-system-report/> adresinden alınmıştır

GreenArrow. (tarih yok). *WHAT IS METHBOT?*. <https://greenarrowmm.com/what-is-methbot/> adresinden alındı

- Gualtier, B. (2021). Treatment Plant Intrusion Press Conference. (P. Sheriff, Röportajı Yapan)
- Guerrero-Saade, J. A. (2021). *MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll*. Sentinel Labs: <https://www.sentinelone.com/labs/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll/> adresinden alınmıştır
- Guliev, I. A., Khubaeva, A. O., Chernysheva, E. A., & Kolesova, I. V. (2021). The influence of digitalization on Chinese banks: new financial technologies in a plan economy. *IV International Scientific and Practical Conference* (s. 319–326). Cham : Palgrave Macmillan.
- Gupta, A., & Xia, C. (2018). A Paradigm Shift in Banking: Unfolding Asia’s FinTech Adventures. *International Symposia in Economic Theory and Econometrics* (s. 215-254). Bingley: Emerald Publishing Limited .
- Güler, M. Ç., & Shakirova, A. (2021). Deciphering Russia's 2021 National Security Strategy Document. *SETA*, No:67, <https://setav.org/en/assets/uploads/2021/09/P67En.pdf>.
- Günen, E. (2019). *Amazon Go ABD Dışına Çıkıyor*. <https://fintechtime.com/tr/2019/02/amazon-go-abd-disina-cikiyor/> adresinden alınmıştır
- Güntay, V. (2019). 21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk. *Siyaset Bilimi ve Uluslararası İlişkiler Dergisi*, 1(2), 87-109.
- Haas, R. E., & Möller, D. P. (2017). Automotive Connectivity, Cyber Attack Scenarios and Automotive Cyber Security. *IEEE International Conference on Electro Information Technology (EIT)*, 635-639.
- Hakala, J., & Melnychuk, J. (2021). *Russia's Strategy in Cyberspace*. Riga: NATO Strategic Communications Centre of Excellence [CCDCOE].
- Hall, C., & Blas, J. (2012). *Qatar group falls victim to virus attack*. <https://www.ft.com/content/17b9b016-f2bf-11e1-8577-00144feabdc0> adresinden alınmıştır
- Hamann, F. (2021). *5 fintech and bank partnerships that are generating revenue*. <https://subaio.com/digital-banking/5-fintech-and-bank-partnerships-that-are-generating-revenue> adresinden alınmıştır
- Hanna, K. T. (2021). *Chernobyl virus* . <https://www.techtarget.com/searchsecurity/definition/Chernobyl-virus> adresinden alınmıştır

- Hanna, K. T., Lutkevich, B., & Rob, W. (2021). *Botnet*. <https://www.techtarget.com/searchsecurity/definition/botnet> adresinden alındı
- Hansman, T., Tan, K. T., Zhou, Y., & Loh, Y. W. (2022). *Harnessing volatility: Technology transformation in oil and gas*. McKinsey .
- Haour, G. (2016). *Why China's new cybersecurity law is a threat to international businesses and innovation*. <https://www.imd.org/research-knowledge/articles/why-chinas-new-cybersecurity-law-is-a-threat-to-international-businesses-and-innovation/> adresinden alınmıştır
- Harries, J., & Mayer, D. (2021). *LightBasin: A Roaming Threat to Telecommunications Companies*. <https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/> adresinden alınmıştır
- Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-885.
- Hawkins, B. (2016). Under The Ocean of the Internet - The Deep Web. *Global Information Assurance Certification Paper* (s. 2011). SANS Institute.
- Hayward, R. J. (2017). Evaluating The "Imminence" of A Cyber Attack for Purposes of Anticipatory Self-Defence. *Columbia Law Review*, Vol:117, No:2.
- Heickerö, R. (2010). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm : Swedish Defence Research Agency (FOI).
- Herr, T. (2014). PrEP: A Framework for Malware & Cyber Weapons. *Journal of Information Warfare*, 16(1), 87-106.
- Hoffman, S. (2018). *Cyber Attack Forces Internet Shut Down for Doe Lab*. <https://www.crn.com/news/security/231001261/cyber-attack-forces-internet-shut-down-for-doe-lab.htm?itc=refresh> adresinden alınmıştır
- Holm, L. (2017). *Cyber attacks & coercion in the digital era.: A qualitative case analysis of the North Korean cyber attack on Sony Pictures*. Uppsala : Publications from Uppsala University .
- Holmes, O. (2018). *Israel: Hamas created fake dating apps to hack soldiers' phones*. *The Guardian*. <https://www.theguardian.com/world/2018/jul/03/israel-hamas-created-fake-dating-apps-to-hack-soldiers-phones> adresinden alındı
- Holroyd, M. (2021). *Thousands of CityBee users have their personal data leaked online* . <https://www.euronews.com/2021/02/17/thousands-of-citybee-users-have-their-personal-data-leaked-online> adresinden alınmıştır

- Horsley, J. P. (2022, 08 08). *Behind the Facade of China's Cyber Super-Regulator* .
<https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/> adresinden alınmıştır
- Huawei. (2017). *Huawei Joins Hands with PCITC to Embrace Smart Factory 2.0*.
https://e.huawei.com/fr/publications/global/ict_insights/201708310903/manufacturing/201708311102 adresinden alınmıştır
- Huawei. (tarih yok). *Company Facts*. <https://www.huawei.com/en/media-center/company-facts> adresinden alınmıştır
- Huawei. (2020). *Digital Power 2030*. Shenzhen.
- Huawei. (2020a). *Green Development 2030*. Shenzhen.
- Huang, Y. (2020). *FinTech Development in the People's Republic of China and Its Macroeconomic Implications* . Asian Development Bank Institute .
- Hughes, P. L. (1999). *The Crash and Early Depression*. Austin Community College District.
- Iasiello, E. (2022). *Is Russia-India Cyber Cooperation on the Horizon?*
<https://infobrics.org/post/36044> adresinden alınmıştır
- IdeaPort. (2021). *Endüstri 4.0 ile Endüstriyel Üretim Dönüşürken İnsan-Makine Etkileşimi; Bugün ve Gelecekteki Teknoloji Trendleri*.
<https://www.ttgiv.org.tr/tur/images/publications/606ad2c302d2a.pdf> adresinden alınmıştır
- IFMAT. (tarih yok). *Cyber Police*. Iran, Iranian Regime - Frauds, Manipulations, Atrocities Threats: <https://www.ifmat.org/12/04/cyber-police/> adresinden alınmıştır
- Independent Commodity Intelligence Services [ICIS]. (2020). *ICIS Chemical Business*.
<https://edition.pagesuite-professional.co.uk/html5/reader/production/default.aspx?pubname=&edid=b360f3dc-4122-4444-a851-e27863e29061> adresinden alınmıştır
- ING. (2012). ING agrees to sell its stake in Capital One
- Interfax Ukraine. (2022). *Klitschko says his website attacked from Russia on Friday*.
<https://en.interfax.com.ua/news/general/791722.html> adresinden alınmıştır
- International Business Machines [IBM]. (2021). *X-Force Threat Intelligence Index 2022*. <https://www.ibm.com/downloads/cas/ADLMYLAZ> adresinden alınmıştır

- Jardine Motors Group. (tarih yok). *The History of Car Technology*. <https://news.jardinemotors.co.uk/lifestyle/the-history-of-car-technology> adresinden alınmıştır
- Java. (tarih yok). *Man-in-the-middle (MITM) Attacks*. <https://www.javatpoint.com/cyber-security-mitm-attacks> adresinden alınmıştır
- JBS Foods. (2021). *JBS USA Cyberattack Media Statement - June 9*. <https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9> adresinden alınmıştır
- Jindal, D. (2022). *Shifting Cyber Agenda in Shanghai Cooperation Organisation*. <https://moderndiplomacy.eu/2022/08/29/shifting-cyber-agenda-in-shanghai-cooperation-organisation/> adresinden alınmıştır
- Jingguang, F. (2011). *Policies and Practices on Network Security of MIIT*. Hangzhou: Asia-Pacific Economic Cooperation [APEC].
- Johnson, T. R. (1995). *American Cryptology during the Cold War, 1945-1989*. NSA.
- Joint Security Commission [JSC]. (1994). *Redefining Security*. Washington. (Joint Security Commission [JSC], 1994, s. 1). adresinden alınmıştır
- Jones, C. (2022). *What is hacktivism?*. <https://www.itpro.co.uk/hacking/30203/what-is-hacktivism> adresinden alındı
- Joshua, J. (2017). Information Bodies: Computational Anxiety in Neal Stephenson's Snow Crash. *Interdisciplinary Literary Studies*, 19(1), 17-47.
- Kadir, M. H. (2022). *Gelişmiş, Kalıcı ya da Devlet Destekli Siber Tehdit Aktörleri*. PUGAT. <https://www.pugat.org/siber-guvenlik/2022/01/01/gelismis-kalici-ya-da-devlet-destekli-siber-tehdit-aktorleri/> adresinden alındı
- Kalelioğlu, E. (2022). *Microsoft Hacklendi! Google rakibi Bing ve Siri Rakibi Cortana'nın Verileri Sızdırıldı*. <https://www.webtekno.com/microsoft-hacklendi-bing-cortana-verileri-sizdirildi-h121970.html> adresinden alınmıştır
- Kamasa, J. (2022). *Chip Shortages in the Light of Geopolitics and Climate Change*. Center for Strategic & International Studies [CSIS].
- Kapur, M. (2022). *The emerging role of cybersecurity in the automotive sector*. <https://timesofindia.indiatimes.com/blogs/voices/the-emerging-role-of-cybersecurity-in-the-automotive-sector/> adresinden alınmıştır
- Karataş, Z. (2015). Sosyal Bilimlerde Nitel Araştırma Yöntemleri. *Manevi Temelli Sosyal Hizmet Araştırmaları Dergisi*, 1(1), 62-80.

- Kaspersky. (2013). *The "Icefog" Apt : A Tale of Cloak and Three Daggers*. Kaspersky Lab Global Research and Analysis Team.
- Kaspersky. (2017). *Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies*. https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies adresinden alınmıştır
- Kaspersky. (2018). *Threat Intelligence Report for the Telecommunications Industry*. Kaspersky Lab .
- Kaspersky. (2022). *DDoS attacks hit a record high in Q4 2021*. https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021 adresinden alındı
- Kaspersky. (2022a). *Cyberwar in Ukraine leads to all-time-high levels of DDoS attacks*. https://www.kaspersky.com/about/press-releases/2022_cyberwar-in-ukraine-leads-to-all-time-high-levels-of-ddos-attacks adresinden alınmıştır
- Kaspersky. (2022b). *IP spoofing: How it works and how to prevent it*. <https://www.kaspersky.com/resource-center/threats/ip-spoofing> adresinden alınmıştır
- Kaspersky. (tarih yok). *Siyah şapkalı, beyaz şapkalı ve gri şapkalı korsanlar – Tanım ve Açıklama*. Kaspersky. <https://www.kaspersky.com.tr/resource-center/definitions/hacker-hat-types> adresinden alındı
- Kaspersky. (tarih yok(b)). *DDoS saldırısı nedir?* <https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks> adresinden alınmıştır
- Kaspersky. (tarih yok(c)). *What is a Botnet?*. <https://usa.kaspersky.com/resource-center/threats/botnet-attacks> adresinden alındı
- Kaspersky. (tarih yok(d)). *Fidye yazılımlarının tanınması – şifrelenmiş Truva atlarından farkı nedir?* <https://www.kaspersky.com.tr/resource-center/threats/ransomware-attacks-and-types> adresinden alınmıştır
- Kaspersky. (tarih yok(e)). *What is Keystroke Logging and Keyloggers?*. <https://www.kaspersky.com/resource-center/definitions/keylogger> adresinden alındı
- Kaspersky. (tarih yok(f)). *BlackEnergy APT Attacks in Ukraine*. <https://www.kaspersky.com/resource-center/threats/blackenergy> adresinden alınmıştır

- Katman, F. (2021). Routledge Companion to Global Cyber-Security Strategy. S. N. Romaniuk, & M. Manjikian içinde, *The Islamic Republic of Iran's Cyber Security Strategy* (s. 435-447). London: Taylor & Francis Group.
- Kaymak, O. (2019). *Dijital Bankacılık Kapsamında Türkiye'de Fintech İnovasyonu ve Uygulaması: Rusya Sektör Karşılaştırması*. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi .
- Katz, Y. (2011). *Iran embarks on \$1b. cyber-warfare program*. <https://www.jpost.com/defense/iran-embarks-on-1b-cyber-warfare-program> adresinden alınmıştır
- Keck, Z. (2014). *S. Korea Seeks Cyber Weapons to Target North Korea's Nukes*. <https://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/> adresinden alınmıştır
- Keen Security Lab of Tencent . (2016). *Car Hacking Research: Remote Attack Tesla Motors* . <https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/> adresinden alınmıştır
- Keivani, F. S., Jouzbarkand, M., Khodadadi, M., & Sourkouhi, Z. K. (tarih yok). A General View on the E-banking. 62-65.
- Keller-Lynn, C. (2022). *US and Israel to announce new cybersecurity collaboration framework Wednesday*. The Times of Israel: <https://www.timesofisrael.com/us-and-israel-to-announce-new-cybersecurity-collaboration-framework-wednesday/> adresinden alınmıştır
- Kelly, A. (2019). *Apple and Google named in US lawsuit over Congolese child cobalt mining deaths*. <https://www.theguardian.com/global-development/2019/dec/16/apple-and-google-named-in-us-lawsuit-over-congolese-child-cobalt-mining-deaths> adresinden alınmıştır
- Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights*, 10(1), 15-25.
- Kızılay, Ş. (2020). Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası. *International Journal of Economics Administrative and Social Sciences*, Cilt:3, Sayı:1, 33-44.
- Kim, Y., Park, Y.-J., Choi, J., & Yeon, J. (2015). An Empirical Study on the Adoption of “Fintech” Service: Focused on Mobile Payment Services. *Advanced Science and Technology Letters*, Vol:114, 136-140.

- Kitson, A., & Liew, K. (2019). *China Doubles Down on Its Digital Silk Road*. <https://reconasia.csis.org/china-doubles-down-its-digital-silk-road/> adresinden alınmıştır
- Kleinhans, J.-P., & Baisakova, N. (2020). *The Semiconductor Value Chain*. Berlin: Stiftung Neue Verantwortung.
- Klimburg, A., & Healey, J. (2012). Strategic Goals & Stakeholders. A. (. Klimburg içinde, *National Cyber Security Framework Manual* (s. 66-103). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE).
- Knibbs, K. (2014). *Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs* . <https://gizmodo.com/silk-road-3-is-already-up-but-its-not-the-future-of-da-1655512490> adresinden alınmıştır
- Kobor, E. (2007). Money Laundering Trends. *Money Laundering*, 55(5), 14-20.
- Kogosowski, M. (2022, 01 02). *2022 national defense budget cements additional US-Israel cyber cooperation*. <https://www.israeldefense.co.il/en/node/53190> adresinden alınmıştır
- Konheim, A. G. (2016). Automated teller machines: their history and authentication protocols. *Journal of Cryptographic Engineering*, Vol:6, 1-29.
- Korhan, S. (2017). Siber Uzayda Aktör - Güç İlişkisi. *Siberpolitik Dergisi*, 2(4), 75-104.
- Kotik, Y. Ö. (2015). *Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişen Stratejisi*. Adana: Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi .
- Kovacs, E. (2014). *ShadowCrew Cybercrime Forum Vendor Sentenced to Prison*. *Securityweek*. <https://www.securityweek.com/shadowcrew-cybercrime-forum-vendor-sentenced-prison> adresinden alındı
- Kramer, K. (2020). *US chemical plants risk disastrous cyberattacks relying on guidance a decade out of date*. <https://www.chemistryworld.com/news/us-chemical-plants-risk-disastrous-cyberattacks-relying-on-guidance-a-decade-out-of-date/4011915.article> adresinden alınmıştır
- Krauss, C., Chokshi, N., & San, D. E. (2021). *Gas Pipeline Hack Leads to Panic Buying in the Southeast*. <https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html> adresinden alınmıştır

- Krekel, B. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. McLean, VA: Northrop Grumman Corporation.
- KrebsOnSecurity. (2018). *Who and What Is Coinhive?*. <https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/> adresinden alındı
- KrebsOnSecurity. (2019). *Experts: Breach at IT Outsourcing Giant Wipro*. <https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/> adresinden alınmıştır
- Kremlin.ru. (2017). *Federal law on Security of Critical Information Infrastructure*. <http://www.kremlin.ru/acts/bank/42128> adresinden alınmıştır
- Kroutchinin, Y., & Baudrier, L.-A. (2019). *What are the impacts of mobile phones on society?* Sciences Po Paris .
- Kshetri, N. (2023). National Metaverse Strategies. *Computing's Economics* , 137-142.
- Kumar, D. K. (2020). *Oil prices jump after U.S. air strike kills top Iranian commander*. Reuters: <https://www.reuters.com/article/us-global-oil-idUSKBN1Z2030> adresinden alınmıştır
- Kurter, O., Temizkan, V., Yılmaz, K., & Yetgin, M. A. (2021). *İşletmelerde Dijital Dönüşüm* . Ankara : Detay Yayıncılık.
- Kurnaz, S., & Karatepe, S. (2019). Kritik Altyapıların Güvenliği Kapsamında Türkiye'deki Hava Alanlarının Siber Güvenliği. *ASSAM Uluslararası Hakemli Dergi*, 119-129.
- Lambert, J. (2021). Nation State Threats. *Microsoft Digital Defense Report* (s. 48-69). Microsoft.
- Laurence, E. (2023). *Is 5G Making You Sick? Here's What Experts Say*. <https://www.forbes.com/health/body/is-5g-safe/> adresinden alınmıştır
- Laux, J., & Honea, M. (2018). *Silent Cyber Scenario: Opening the Flood Gates*. <https://www.aon.com/reinsurance/gimo/20181025-gimo-cyber> adresinden alınmıştır
- Lee, R. M., Assante, J. M., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf: SANS, E-ISA .

- Lee, Y., Woo, S., Song, Y., Lee, J., & Lee, D. H. (2020). Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis. *IEEE Access*, Vol:8, 120009-120018.
- Lee, S. (2017). *The Cybersecurity Implications of Chinese Undersea Cable Investment*. <https://jsis.washington.edu/eacenter/2017/02/06/cybersecurity-implications-chinese-undersea-cable-investment/> adresinden alınmıştır
- Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. M. Lehto, & P. Neittaanmäki içinde, *Cyber Security Critical Infrastructure Protection* (s. 3-36). Switzerland : Springer Nature Switzerland AG.
- Lemos, R. (2002). *Cyberterrorism: The real risk*. Computer Crime Research Center (CCRC): <https://www.zdnet.com/article/what-are-the-real-risks-of-cyberterrorism/> adresinden alınmıştır
- Lenpravda. (2011). *Кто из ФСБ работает на форумах и в блогах*. <https://www.lenpravda.ru/digest/federal/275016.html> adresinden alınmıştır
- Levi, R. (2016). *What the Maroochy Incident taught us about Cyber Warfare* . <https://medium.com/curious-minds/what-the-maroochy-incident-taught-us-about-cyber-warfare-4a1abd6abcf6> adresinden alınmıştır
- Lewis, J. A. (2014). *Reference Note on Russian Communications Surveillance*. The Center for Strategic and International Studies (CSIS): <https://www.csis.org/analysis/reference-note-russian-communications-surveillance> adresinden alınmıştır
- Lewis, J. A. (2018). *How 5G Will Shape Innovation and Security*. Center for Strategic and International Studies.
- Lewis, J. A. (2019). *Iran and Cyber Power*. <https://www.csis.org/analysis/iran-and-cyber-power> adresinden alınmıştır
- Liaropoulos, A. (2011). War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory. J. Ryan içinde, *Leading Issues in Information Warfare and Security Research* (s. 121-134). Reading: Academic Publishing International Ltd.
- Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Pittsburgh: RAND Corporation.
- Li, H., & Zhang, J. (2022). Application of Existing Rules of International law in Cyberspace. *Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development* (s. 169-173). Atlantiss Press.

- Lindsey, N. (2019). *FBI Warning: Hackers Now Targeting US Automotive Industry*.
<https://www.cpomagazine.com/cyber-security/fbi-warning-hackers-now-targeting-us-automotive-industry/> adresinden alınmıştır
- Liu, Z. (2022, 10 13). *China Says No To Speculative All-Virtual Metaverse*.
<https://jingdaily.com/china-metaverse-real-economy-industrial-power/> adresinden alınmıştır
- Lopez-Diez, J. (2021). Metaverse: Year One. Mark Zuckerberg's video keynote on Meta. *Pensar public*, 15(2), 299-303.
- Lutkevich, B. (2021). *script kiddie*. 06 04, 2022 tarihinde Search Security:
<https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie> adresinden alındı
- Lyall, N. (2018). *China's Cyber Militias*. *The Diplomat*.
<https://thediplomat.com/2018/03/chinas-cyber-militias/> adresinden alındı
- Lyngaas, S. (2020). *Taiwan suggests China's Winnti group is behind ransomware attack on state oil company*. CyberScoop: <https://www.cyberscoop.com/cpc-ransomware-winnti-taiwan-china/> adresinden alındı
- Macheel, T. (201). *Citi Launches FinTech Unit to Lead Mobile-First 'Revolution'*.
<https://www.americanbanker.com/bank-technology/citi-launches-fintech-unit-to-lead-mobile-first-revolution-1077287-1.html> adresinden alınmıştır
- Mackie, K. (2017). *ISIS Laundered Money into US Using eBay: Investigators* .
OCCRP: <https://www.occrp.org/en/daily/6847-isis-laundered-money-into-us-using-ebay-investigators> adresinden alınmıştır
- Mahmud, A. H. (2021). *More cybersecurity cooperation between Singapore, US in public, defence and financial sectors*.
<https://www.channelnewsasia.com/singapore/singapore-us-mou-cybersecurity-cooperation-public-defence-finance-2130121> adresinden alınmıştır
- Mallon, S. (tarih yok). *Ransomware And The Defense Industrial Base*.
<https://www.smartdatacollective.com/ransomware-and-defense-industrial-base/> adresinden alınmıştır
- Mandiant. (2018). *TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers* .
<https://www.mandiant.com/resources/blog/triton-attribution-russian-government-owned-lab-most-likely-built-tools> adresinden alınmıştır
- Manufacturing USA. (2014). *History*.
<https://www.manufacturingusa.com/pages/history> adresinden alınmıştır

- Marco, G. (2010). *Regional and International Trends in Information Society Issues*. St. Lucia: HIPCAR – Working Group 1.
- Marr, B. (2015). *Big Data In Big Oil: How Shell Uses Analytics To Drive Business Success*. <https://www.forbes.com/sites/bernardmarr/2015/05/26/big-data-in-big-oil-how-shell-uses-analytics-to-drive-business-success/?sh=5102d7db229e> adresinden alınmıştır
- Masduki, A., Niu, P., Rochman, M. F., & Sulhan, M. (2021). The Digital Silk Road and Chiglobalization: A Post-Epidemic Information and Communication Technology Alternative Project. *Advances in Social Science, Education and Humanities Research*, vol: 596, 41-45.
- MASS. (2022). *Cybersecurity Advisory for Public Water Suppliers*. <https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers> adresinden alınmıştır
- Massie, G. (2022). *Russian EV charging stations hacked with 'Putin is a d***head' message*. <https://www.independent.co.uk/news/world/europe/putin-charging-station-hacked-ukraine-russia-b2026260.html> adresinden alınmıştır
- Masters, J., McBride, J., & Berman, N. (2023). *What Happens When Foreign Investment Becomes a Security Risk?* <https://www.cfr.org/background/foreign-investment-and-us-national-security> adresinden alınmıştır
- Mastercard. (2016). Mastercard makes fingerprint and 'selfie' payment technology a reality. <https://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/>.
- Mbanaso, U., & Dandaura, E. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 18(3), 17-24.
- McAfee. (tarih yok). *What is Malware?* <https://www.mcafee.com/en-us/antivirus/malware.html> adresinden alınmıştır
- McBride, J., & Chatzky, A. (2019). *Is 'Made in China 2025' a Threat to Global Trade?* <https://www.cfr.org/background/made-china-2025-threat-global-trade> adresinden alınmıştır
- McCurry, J. (2014). *South Korean nuclear operator hacked amid cyber-attack fears*. The Guardian. <https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack> adresinden alınmıştır
- McDonough, T. (2022). *Japan, Australia upgrade security pact against China threat*. <https://www.cnbc.com/2022/10/23/japan-australia-upgrade-security-pact-against-china-threat.html> adresinden alınmıştır

- McElroy, T. (2021). *Tech Safety In The Emergency Services Sector: Overcoming Obstacles In The Adoption Of New Mission-Critical Technology*. <https://www.forbes.com/sites/forbestechcouncil/2021/08/10/tech-safety-in-the-emergency-services-sector-overcoming-obstacles-in-the-adoption-of-new-mission-critical-technology/?sh=1f9ee79d6c3a> adresinden alınmıştır
- McKenzie, T. M. (2017). *Is Cyber Deterrence Possible?* Alabama: Air University Press.
- McKew, M. K. (2017, 09 05). *The Gerasimov Doctrine*. <https://www.politico.eu/article/new-battles-cyberwarfare-russia/> adresinden alınmıştır
- McKinsey. (2018). *Synergy and disruption: Ten trends shaping fintech*. McKinsey & Company.
- McMurtry, A. (2022). *Cyberattack on mobile operator in Portugal leaves millions disconnected*. <https://www.aa.com.tr/en/europe/cyberattack-on-mobile-operator-in-portugal-leaves-millions-disconnected/2497307> adresinden alınmıştır
- Medin, M., & Louie, G. (2019). *The 5G Ecosystem: Risks & Opportunities for DoD*. Defense Innovation Board.
- Meehan, S. (2018). *In Wake of Baltimore 911 Cyberattack, Officials Urge Layered Protections*. <https://www.govtech.com/security/in-wake-of-baltimore-911-cyberattack-officials-urge-layered-protections.html> adresinden alınmıştır
- Meer, S. v. (2015). *Foreign Policy Responses to International Cyber-attacks*. Netherlands: Netherlands Institute of International Relations .
- Mehr News Agency. (2019). *Iran, China agree to jointly counter cyber threats*. <https://en.mehrnews.com/news/147217/Iran-China-agree-to-jointly-counter-cyber-threats> adresinden alınmıştır
- Melzer, N. (2011). *Cyberwarfare and International Law*. United Nations Institute for Disarmament Research.
- Mendonca, J. (2019). *Wipro confirms attack on IT systems, hires forensic investigation firm*. <https://economictimes.indiatimes.com/corporate/wipro-it-systems-may-have-been-hacked-and-used-to-attack-its-clients-report/articleshow/68899479.cms> adresinden alınmıştır
- Merali, L., & Bavcic, E. (2022). *Cybersecurity and Human Rights in the Western Balkans: Mapping governance and actors*. DCAF – Geneva Centre for Security Sector Governance.

- Meredith, S. (2018). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. <https://www.cnn.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> adresinden alınmıştır
- Metzel, M. (2021). *Russia, Indonesia agree to cooperate on information security*. TASS: <https://tass.com/politics/1375155> adresinden alınmıştır
- Michaux, S. (2021). *How to keep automated electric vehicles safe*. <https://news.uga.edu/how-to-keep-automated-electric-vehicles-safe/> adresinden alınmıştır
- Microsoft. (tarih yok). *Xbox*. <https://www.microsoft.com/en-us/store/b/xbox?icid=CNavDevicesXbox> adresinden alınmıştır
- Microsoft. (tarih yok(a)). *Microsoft acquires GitHub*. <https://news.microsoft.com/announcement/microsoft-acquires-github/> adresinden alınmıştır
- Microsoft. (tarih yok(b)). *Microsoft buys LinkedIn*. <https://news.microsoft.com/announcement/microsoft-buys-linkedin/> adresinden alınmıştır
- Microsoft. (tarih yok(c)). *Microsoft purchases 'Minecraft'*. <https://news.microsoft.com/announcement/microsoft-purchases-minecraft/> adresinden alınmıştır
- Microsoft. (2009). *Trojan:Win32/PeskySpy.A*. <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/PeskySpy.A> adresinden alındı
- Microsoft. (2017). *Chevron fuels digital transformation with new Microsoft partnership*. <https://news.microsoft.com/transform/chevron-fuels-digital-transformation-with-new-microsoft-partnership/> adresinden alınmıştır
- Microsoft. (2021). *Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021*. Microsoft Threat Intelligence Center (MSTIC): <https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/> adresinden alındı
- Microsoft. (2021a). *New nation-state cyberattacks*. <https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/> adresinden alınmıştır
- Microsoft. (2022). *Microsoft to acquire Activision Blizzard to bring the joy and community of gaming to everyone, across every device*. <https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard/>

blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/ adresinden alınmıştır

Milosevic, N. (2014). *Case of the cyber war: Kosovo conflict*. <https://inspiratron.org/wp-content/uploads/kalins-pdf/singles/case-cyber-war-kosovo-conflict.pdf> adresinden alınmıştır

Ministry of Digital Development, Communications and Mass Media of the RF. (2017). *Россия и Иран подписали меморандум о сотрудничестве в области связи и ИТ*. https://digital.gov.ru/ru/events/36659/?utm_referrer=https%3a%2f%2fwww.c4isrnet.com%2f adresinden alınmıştır

Ministry of Digital Development, Telecommunications and Mass Media of the RF. (2016). *Министры связи России и Ирана обсудили сотрудничество в ИТ-сфере*. <https://digital.gov.ru/ru/events/35486/> adresinden alınmıştır

Ministry of Digital Development, Telecommunications and Mass Media of the RF. (2017). *В Минкомсвязи обсудили ИКТ-сотрудничество с Ираном*. <https://digital.gov.ru/ru/events/36389/> adresinden alınmıştır

Ministry of Economy, Trade and Industry (METI) Government of Japan. (2018). *Japan's New Robot Strategy*. <https://www.djw.de/ja/assets/media/Veranstaltungen/Symposium,%20MGV/duesseldorf-20180416/djw-symposium-duesseldorf-16.04.2018-kurihara-meti.pdf>.

Ministry of Foreign Affairs of Japan . (2022). *Japan-U.S. Security Consultative Committee (Japan-U.S. “2+2”)*. https://www.mofa.go.jp/na/st/page4e_001197.html adresinden alınmıştır

Ministry of Foreign Affairs of Japan. (2019). *Joint Statement of the Security Consultative Committee*. <https://www.mofa.go.jp/files/000470738.pdf> adresinden alınmıştır

Ministry of Foreign Affairs of the Russian Federation. (tarih yok). *Russian Federation Armed Forces' Information Space Activities Concept*. <https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle> adresinden alınmıştır

Miller, C. (2021). *Throwback Attack: BlackEnergy attacks the Ukrainian power grid*. <https://www.industrialcybersecuritypulse.com/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/> adresinden alınmıştır

Mission Secure. (tarih yok). *Critical Manufacturing Cybersecurity*. <https://www.missionsecure.com/manufacturing-cyber-security> adresinden alınmıştır

- Mitnick Security. (tarih yok). *Kevin Mitnick's Biography: Who is Kevin Mitnick?*. Mitnick Security. <https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security> adresinden alındı
- Moffitt, T. (2019,). *Post Coinhive, What's Next for Cryptojacking?*. <https://www.webroot.com/blog/2019/03/15/post-coinhive-whats-next-for-cryptojacking/> adresinden alındı
- Moon, H.-C., Chung, J.-E., & Choi, S.-B. (2018). Korea's Manufacturing Innovation 3.0 Initiative. *Journal of Information and Management*, 38(1), 26-34.
- Moynihan, H. (2020). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, 1-17.
- Moynihan, H., & Patel, C. (2021). *Restrictions on onlinefreedom of expression in China*. Chatham House.
- Muhn, J. (2023). *American Express Retires the Kabbage Brand with the Launch of Business Blueprint*. <https://finovate.com/american-express-retires-the-kabbage-brand-with-the-launch-of-business-blueprint/> adresinden alınmıştır
- Murray, W. (2013). *Edward Snowden's NSA surveillance revelations strain China-US relations* . <https://www.theguardian.com/world/2013/jun/13/snowden-revelations-nsa-china-relations> adresinden alınmıştır
- Murray, C. (2022). *The history of credit cards*. <https://www.bankrate.com/finance/credit-cards/the-evolution-of-credit-cards/> adresinden alınmıştır
- Nadimi, F. (2018). *Iran's Passive Defense Organization: Another Target for Sanctions*. <https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions> adresinden alınmıştır
- Nakashima, E. (2012). *Iran blamed for cyberattacks on U.S. banks and companies*. Washington Post. https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?utm_term=.6f75e1cfdd54 adresinden alınmıştır
- Nakashimave, E., & Timberg, C. (2020). *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce*. The Washington Post. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html adresinden alınmıştır

- Nakashidze, G. (2020). *Cyberattack against Georgia and International Response: emerging normative paradigm of 'responsible state behavior in cyberspace'?* <https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/> adresinden alınmıştır
- Nakashima, E., Harris, S., Hudson, J., & Lamothe, D. (2023). *Chinese balloon part of vast aerial surveillance program, U.S. says.* <https://www.washingtonpost.com/national-security/2023/02/07/china-spy-balloon-intelligence/> adresinden alınmıştır
- Napetvaridze, V., & Chochia, A. (2019). Cybersecurity in the Making – Policy and Law: a Case Study of Georgia. *International Conference on Learning Representations*, 19(2), 155-180.
- Naughton, K. (2021). *Driverless Cars' Need for Data Is Sparking a New Space Race.* Bloomberg. <https://www.bloomberg.com/news/articles/2021-09-17/carmakers-look-to-satellites-for-future-of-self-driving-vehicles?leadSource=uverify%20wall> adresinden alınmıştır
- Nasaw, D. (2009). *Hackers breach defences of joint strike fighter jet programme.* The Guardian. <https://www.theguardian.com/world/2009/apr/21/hackers-us-fighter-jet-strike> adresinden alınmıştır
- National Counterintelligence and Security Center [NCSC]. (2018). *Foreign Economic Espionage in Cyberspace.*
- National Institute of Standards and Technology [NIST]. (2018). *Risk Management Framework for Information Systems and Organizations 800-37 Rev 2.* U.S. Department of Commerce: National Institute of Standards and Technology.
- National Security Agency [NSA]. (2012). *60 Years of Defending Our Nation.*
- National Security Archive. (2013). *Basic Principles for States Policy of the RF in the Field of International Information Security to 2020.* <https://nsarchive.gwu.edu/sites/default/files/documents/5014250/Russian-Government-Basic-Principles-for-State.pdf> adresinden alınmıştır
- NATO. (2016). *Warsaw Summit Communique.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber adresinden alındı
- NATO. (2020). *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations .* NATO STANDARDIZATION OFFICE (NSO).

- NBC NEWS. (2017). *Target Settles 2013 Hacked Customer Data Breach For \$18.5 Million*. NBC News. <https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031> adresinden alınmıştır
- NBC News. (2018). *Baltimore's 911 emergency system hit by cyberattack*. NBC News. <https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876> adresinden alınmıştır
- NCSC. (2018). *Joint US - UK statement on malicious cyber activity carried out by Russian government*. UK National Cyber Security Centre. <https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government> adresinden alındı
- NCSC. (2018a). *UK and allies reveal global scale of Chinese cyber campaign*. UK National Cyber Security Centre. <https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign> adresinden alınmıştır
- NCSC. (2018b). *Reckless campaign of cyber attacks by Russian military intelligence service exposed*. UK National Cyber Security Centre: <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> adresinden alınmıştır
- NCSC. (2021). *UK and allies hold Chinese state responsible for a pervasive pattern of hacking*. UK National Cyber Security Centre. <https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking> adresinden alındı
- Negi, S. (2022). *Russia-Iran cybersecurity cooperation agreement poses threat to the U.S*. <https://asianatimes.com/russia-iran-cybersecurity-cooperation-agreement-poses-threat-to-the-u-s/> adresinden alınmıştır
- Neu, A. (2013). *The Iranian Cyber Threat*. <https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/> adresinden alınmıştır
- Neudert, L. M., & Marchal, N. (2019). *Polarisation and the use of technology in political campaigns and communication*. Brussels: Directorate-General for Parliamentary Research Services (EPRS) .
- Nieva, R. (2018). *Facebook says Cambridge Analytica had data on 87 million people*. <https://www.cnet.com/tech/tech-industry/facebook-says-cambridge-analytica-had-data-on-87m-people/> adresinden alınmıştır
- Nikolsky, A. (2019). *Putin approves National Strategy for AI until 2030*. TASS: <https://tass.com/economy/1082644> adresinden alınmıştır

- Nissenbaum, H. (1999). *The Meaning of Anonymity in an Information Age*. The Information Society: An International Journal, 15, (141-144).
- Nournews. (2020). *General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat*. <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat> adresinden alınmıştır
- NPR. (2021). *Revil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says*. <https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says> adresinden alınmıştır
- NTV. (2022). *Japonya'da 8 dev çip üretimi için bir araya geldi*. <https://www.ntv.com.tr/teknoloji/japonyada-8-dev-cip-uretimi-icin-bir-araya-geldi,wqWQQGKonkCQn0nXGeMehg> adresinden alınmıştır
- Nuroğlu, H. N. (2022). *Chip crisis, global dependency in context of China-Taiwan crisis*. Anadolu Ajansı. <https://www.aa.com.tr/en/analysis/analysis-chip-crisis-global-dependency-in-context-of-china-taiwan-crisis/2667865> adresinden alınmıştır
- O'Connell, M. E. (2012). *Cyber Security and International Law*. Chatham House.
- O'connell, B. (2020). *History of PayPal: Timeline and Facts*. <https://www.thestreet.com/technology/history-of-paypal-15062744> adresinden alınmıştır
- O'Connell, M. E. (2012). *Cyber Security and International Law*. Chatham House.
- OECD. (2022). *Competition in Energy Markets - OECD Competition Policy Roundtable Background Note*. Organisation for Economic Cooperation and Development.
- Official Journal of the European Union. (2008). *Official Journal of the European Union*. 07 2022 tarihinde COUNCIL DIRECTIVE 2008/114/EC: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF> adresinden alındı
- Office of the Director of National Intelligence [ODNI]. (2013). *U.S. National Intelligence: An Overview 2013*. Washington, DC: Office of the Director of National Intelligence.
- Office of the US Trade Representative [USTR]. (2018). *Section 301- China Technology Transfer*. Washington.

- O'Flaherty, K. (2019). *Breaking Down The Wipro Breach -- And What It Means For Supply Chain Security*. *Forbes*.
<https://www.forbes.com/sites/kateoflahertyuk/2019/04/16/breaking-down-the-wipro-breach-and-what-it-means-for-supply-chain-security/?sh=5e3e92bd5259> adresinden alınmıştır
- O'Neil, S. E., & Borgia, M. T. (2022, 08 22). *TSA Revises Cybersecurity Requirements for "Critical" Pipelines and LNG Facilities*.
<https://www.dwt.com/blogs/privacy--security-law-blog/2022/08/cybersecurity-tsa-pipelines-liquified-natural-gas> adresinden alınmıştır
- Organisation for Economic Cooperation and Development [OECD]. (2017). *DIGITAL AND OPEN INNOVATION IN THE AUTOMOTIVE INDUSTRY*. Paris.
- OSCE. (2016). *1092nd Plenary Meeting*. Organization for Security and Co-operation in Europe 10 March 2016 .
- Osawa, J. (2019). *Tencent-Backed WeBank Begins Trial Operation*.
<https://www.wsj.com/articles/BL-DGB-39958> adresinden alınmıştır
- Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare and Security*, 163-168.
- Ottis, R. (2020). *Proactive Defence Tactics Against On-Line Cyber Militia*. *The NATO Cooperative Cyber Defence Centre of Excellence*.
<https://ccdcoe.org/library/publications/proactive-defence-tactics-against-on-line-cyber-militia/> adresinden alınmıştır
- Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington: The National Academies Press.
- Ozsevim, I. (2023). *Saudi Aramco secures Accenture as its key digital consultant*.
<https://procurementmag.com/articles/saudi-aramco-secures-accenture-as-its-key-digital-consultant> adresinden alınmıştır
- Öğün, M. N., & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik. *Güvenlik Stratejileri Dergisi*, 9(18), 145-181.
- Özkan, S. (2021). Uluslararası Hukukun Siber Savaşta Rolü. *III. Uluslararası Kapadokya Sosyal Bilimler Öğrenci Kongresi* (s. 271-273). Kırşehir Ahi Evran Üniversitesi.
- Pace, J. (2016). Exchange relations on the dark web. *Critical Studies in Media Communication*, 34(1), 1-13.

- Panda, P. (2017). *Cyber Attacks in Connected Cars - What Tesla Did Differently to Win*. <https://www.appknox.com/blog/cyber-attacks-in-connected-cars> adresinden alınmıştır
- Panda Security Mediacenter. (2022). *What Is a Man-in-the-Middle (MITM) Attack? Definition and Prevention*. <https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/> adresinden alındı
- Pangrazzi, S. (2021). *Self-Defence Against Cyberattacks? ICT4Peace Foundation* .
- Paoli, G. P. (2018). *The Trade in Small Arms and Light Weapons on the Dark Web*. United Nations Office for Disarmament Affairs .
- Papez, M. G., & Veer, E. (2017). Don't feed the trolling: rethinking how online trolling is being defined and combated. *Journal of Marketing Management* 33(15-16), 1336-1354.
- Papuççuyan, A. (2018). *Şubesiz ve tamamen dijital bankacılık hizmeti İnsha, kullanıma sunuldu*. <https://webrazzi.com/2018/08/02/insha-acildi/> adresinden alınmıştır
- Pascucci, P. (2017). Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution. *Minnesota Journal of International Law*, 419-460.
- Paulo Filho. (2021). *On the National Security Strategy*. https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf adresinden alınmıştır
- Pawlicka, A., Choras, M., & Pawlicki, M. (2021). The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good. *Personal and Ubiquitous Computing*, 25, 843-852.
- Pawlicka, A., Choras, M., & Pawlicki, M. (2021a). Cyberspace threats: not only hackers and criminals. Raising the awareness of selected unusual cyberspace actors - cybersecurity researchers' perspective. *ARES 2020: The 15th International Conference on Availability, Reliability and Security* (s. 1-11). Ireland: Association for Computing Machinery.
- Payne, K. (2018). Artificial Intelligence: A Revolution in Strategic Affairs? *Survival: Global Politics and Strategy*, 60(5), 7-32.
- Payne, J. (2022). *Oil shipments in European oil hub delayed after cyber attacks*. <https://www.reuters.com/world/europe/oil-shipments-european-oil-hub-delayed-after-cyber-attacks-2022-02-04/> adresinden alınmıştır
- Perlroth, N., & Hardy, Q. (2013). *Bank Hacking Was the Work of Iranians, Officials Say*. New York Times.

[Thttps://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html](https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html) adresinden alınmıştır

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). *National Cyber Security Organisation: United States*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Petro-CyberWorks Information Technology Company [PCITC]. (tarih yok). *About PCITC*. http://www.pcitc.com/en/about_us/com_profile/ adresinden alınmıştır

Pike, J. (2000, 04 15). *Third Department*. https://irp.fas.org/world/china/pla/dept_3.htm adresinden alınmıştır

Plume, K., & Bing, C. (2021). *Iowa farm services firm: systems offline due to cybersecurity incident*. Reuters. <https://www.reuters.com/technology/iowa-farm-services-company-reports-cybersecurity-incident-2021-09-20/> adresinden alınmıştır

Phillips, A. (2012). *The Asymmetric Nature of Cyber Warfare*. <https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare> adresinden alındı

Pilette, C. (2021). *What is social engineering? A definition + techniques to watch for*. <https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html> adresinden alındı

Ponemon Institute . (2022). *2022 Ponemon Cost of Insider Threats Global Report*. Michigan.

Poulsen, K. (2018, 07 20). *Mueller Finally Solves Mysteries About Russia's 'Fancy Bear' Hackers*. <https://www.thedailybeast.com/mueller-finally-solves-mysteries-about-russias-fancy-bear-hackers?ref=scroll> adresinden alınmıştır

Prashad, V. (2019). *After Evo, the lithium question Looms Large in Bolivia*. <https://peoplesdispatch.org/2019/11/13/after-evo-the-lithium-question-looms-large-in-bolivia/> adresinden alınmıştır

President's Commission on Critical Infrastructure Protection [PCCIP]. (10). *The Report of the President's Commission on Critical Infrastructure Protection*. Washington.

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliamentary Research Service.

Pollitt, M. M. (1998). Cyberterrorism - Fact or Fancy? . *Computer Fraud & Security, Issue:2*, 8-10.

- Porter, J. (2019). *Popular 'cryptojacking' service Coinhive will shut down next week*. <https://www.theverge.com/2019/2/28/18244636/coinhive-cryptojacking-cryptocurrency-mining-shut-down-monero-date> adresinden alındı
- Radja, A. M. (2017). *Indonesia, Russia explore cooperation in cyber defense* . Antara News: <https://en.antaranews.com/news/110075/indonesia-russia-explore-cooperation-in-cyber-defense> adresinden alınmıştır
- Radkani, E. (2013). *International Telecommunication Union (ITU)*. Iran National CERT: https://www.itu.int/net/wsis/implementation/2013/forum/agenda/session_docs/Day4/113/Panelist3-Radkani.pdf adresinden alınmıştır
- Radware. (2015). *Anyone is a Targeted: DdoS Attack Case Analysis on Boston Children's Hospital* .
- Rafter, D. (2022). *What is the difference between black, white and gray hat hackers?*. <https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html> adresinden alındı
- Raud, M. (2016). *China and Cyber: Attitudes, Strategies, Organisation* . Tallinn : NATO Cooperative Cyber Defence Centre of Excellence [NATO CCD COE].
- Reed, J. (2022). *How Dangerous Is the Cyberattack Risk to Transportation?*. Security Intelligence. <https://securityintelligence.com/articles/how-dangerous-cyber-attack-risk-transportation/> adresinden alınmıştır
- Reed, T. (2018). *Man convicted of 'hactivist' attacks on Boston Children's Hospital*. Fierce Healthcare. <https://www.fiercehealthcare.com/tech/man-convicted-hactivist-attacks-boston-children-s-hospital> adresinden alınmıştır
- RedLock. (2018). *Lessons from the Cryptojacking Attack at Tesla*. <https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/> adresinden alındı
- Regjeringen.no. (2022). *Vi lar oss ikke skremme. Vi skal sta sammen*. <https://www.regjeringen.no/no/aktuelt/vi-lar-oss-ikke-skremme.-vi-skal-sta-sammen/id2937052/> adresinden alınmıştır
- Rehman, I. u. (2019). *Facebook-Cambridge Analytica data harvesting: What you need to know*. Lincoln: University of Nebraska.
- Rid, T. (2012). *Cyber War Will Not Take Place*. *Journal of Strategic Studies*, 35(1), 5-32.

- Reuters. (2012). *"Shamoon" virus most destructive yet for private sector, Panetta says*. Reuters. <https://www.reuters.com/article/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012> adresinden alınmıştır
- Reuters. (2015). *Tencent, Bank of Beijing launch \$1.6 bln online banking tie-up*. <https://www.reuters.com/article/ozabs-uk-tencent-banking-idAFKBN0NK0TH20150429> adresinden alınmıştır
- Reuters. (2015a). *Alibaba helps Sinopec with cloud computing, big data*. <https://www.reuters.com/article/alibaba-sinopec-corp-idUSL4N0XE1MX20150417> adresinden alınmıştır
- Reuters. (2016). *Austria's FACC, hit by cyber fraud, fires CEO*. Reuters. <https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF> adresinden alınmıştır
- Reuters. (2020). *China to import \$300 billion of chips for third straight year: industry group*. <https://www.reuters.com/article/us-china-semiconductors/china-to-import-300-billion-of-chips-for-third-straight-year-industry-group-idUSKBN25M1CX> adresinden alınmıştır
- Reuters. (2022). *Honda to cut production by 10% in two factories*. <https://www.reuters.com/business/autos-transportation/honda-cut-production-by-10-two-factories-2022-03-10/> adresinden alınmıştır
- Reuters. (2022a). *Tesla cut steering component from some cars to deal with chip shortage - CNBC*. <https://www.reuters.com/markets/europe/tesla-cut-steering-component-some-cars-deal-with-chip-shortage-cnbc-2022-02-08/> adresinden alınmıştır
- Reuters. (2022b). *Ford says European production hit by chip shortage, Ukraine conflict*. <https://www.reuters.com/business/autos-transportation/ford-says-european-production-hit-by-chip-shortage-ukraine-conflict-2022-03-21/> adresinden alınmıştır
- Reynard, M. (2021). *Chemical Industry a High value target for Cyber attacks*. <https://fundamentalsfirst.co.uk/2022/03/07/chemical-industry-a-high-value-target-for-cyber-attacks/> adresinden alınmıştır
- Ribeiro, A. (2022). *Growing need to shield food and agriculture sector from rising cybersecurity threats, amidst supply chain risks*. <https://industrialcyber.co/analysis/growing-need-to-shield-food-and-agriculture-sector-from-rising-cybersecurity-threats-amidst-supply-chain-risks/> adresinden alınmıştır

- Richer, A. D. (2019). *Man gets 10 years for cyberattack on Boston Children's Hospital*. <https://www.boston.com/news/local-news/2019/01/11/martin-gottesfeld-boston-childrens-hospital/> adresinden alınmıştır
- Russiaeu.ru. (2008). *The Foreign Policy Concept of the Russian Federation*. https://russiaeu.ru/userfiles/file/foreign_policy_concept_english.pdf adresinden alınmıştır
- Rodenhauser, T. (2021). *Cyber Warfare: does International Humanitarian Law apply?* International Committee of the Red Cross: <https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law> adresinden alınmıştır
- Rollins, J. W. (2015). *U.S.–China Cyber Agreement*. <https://sgp.fas.org/crs/row/IN10376.pdf> adresinden alınmıştır
- Romanova, I., & Kudinska, M. (2016). Banking and Fintech: A Challenge or Opportunity? . *Contemporary Studies in Economic and Financial Analysis*, Vol: 98, 21-35.
- Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
- Roskomnadzor. (tarih yok). *Powers of Roskomnadzor*. https://eng.rkn.gov.ru/about/powers_of_roskomnadzor/ adresinden alınmıştır
- Rosenthal, M. (2022). *Must-Know Phishing Statistics: Updated 2022*. <https://www.tessian.com/blog/phishing-statistics-2020/> adresinden alındı
- Rosenthal, M. (2022a). *Insider Threats Examples: 17 Real Examples of Insider Threats*. Tessian. <https://www.tessian.com/blog/insider-threats-types-and-real-world-examples/> adresinden alındı
- Rossetto, N., & Reif, V. (2021). *Digitalization of the electricity infrastructure: a key enabler for the decarbonization and decentralization of the power sector*. Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2021/47.
- Rossini, C., Green, N., & Knowledge, P. (2011). *Cybersecurity and Human Rights. Webinar Series Training Summaries*, 9-17.
- Roy, S. (2022). *In a first, Quad moves to act against cyberattacks coming from China-led axis*. <https://indianexpress.com/article/india/in-a-first-quad-moves-to-act-against-cyberattacks-coming-from-china-led-axis-8171039/> adresinden alınmıştır

- Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's Cybersecurity Law. *Computer Law & Security Review*, 34(6), 1-13.
- Quadri, L. A., & Rasaq, M. O. (2020). Cyber Theatre a Fifth Domain of International Politics: Africa and the rest of the world in the Cyberspace. *Akdeniz Havzası ve Afrika Medeniyetleri Dergisi*, 2(2), 98-11.
- Sacks, D. (2021). *China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond*. CFR: <https://www.cfr.org/blog/china-huawei-5g> adresinden alınmıştır
- Sajedi, F., & Ariani, M. G. (2014). Cyber-Crimes in Iran: Definition and Analysis. *The International Conference on Cyber-Crime Investigation and Cyber Security* (s. 7-10). Kuala Lumpur : Asia Pacific University of Technology and Innovation.
- Samsung News. (2021). *Samsung Electronics, Logic Chip İşletmelerindeki Yatırımı 2030'a Kadar 171 Trilyon KRW'ye Çıkaracak* . <https://news.samsung.com/global/samsung-electronics-to-boost-investment-in-logic-chip-businesses-to-krw-171-trillion-by-2030> adresinden alınmıştır
- Sanger, D. E. (2023). *Balloon Incident Reveals More Than Spying as Competition With China Intensifies*. <https://www.nytimes.com/2023/02/05/us/politics/balloon-china-spying-united-states.html> adresinden alınmıştır
- Samylovskaya, E., Makhovikov, A., Lutonin, A., Medvedev, D., & Kudryavtseva, R.-E. (2022). Digital Technologies in Arctic Oil and Gas Resources Extraction: Global Trends and Russian Experience . *MDPI*, 11(3).
- Saudi Press Agency [SPA]. (2022). *Saudi National Cybersecurity Authority and U.S. Department of Homeland Security Sign MoU to Promote Cybersecurity Cooperation*. <https://sp.spa.gov.sa/viewfullstory.php?lang=en&newsid=2370312> adresinden alınmıştır
- Scheer, S. (2012). *Israeli government websites under mass hacking attack*. <https://www.nbcnews.com/tech/tech-news/israeli-government-websites-under-mass-hacking-attack-flna1c7125572> adresinden alınmıştır
- Schmitt, M. (2018). *In Defense of Sovereignty in Cyberspace*. Just Security: <https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/> adresinden alınmıştır
- Schoolmeesters, R. (tarih yok). *Dam Incidents and Failures*. According to the Association of Dam Safety Officials (ASDSO). <https://damfailures.org/lessons-learned/site-security-is-critical/> adresinden alınmıştır

- Scholz, C., & Verfürden, M. (2022). "Black Cat"-Erpressersoftware: Staatsanwaltschaft ermittelt nach Angriff auf Tankstellen-Zulieferer. Handelsblatt. <https://www.handelsblatt.com/unternehmen/energie/benzinversorgung-black-cat-erpressersoftware-staatsanwaltschaft-ermittelt-nach-angriff-auf-tankstellen-zulieferer/28029264.html> adresinden alınmıştır
- Science and Technology Law Institute. (tarih yok). *Japan Industry 4.1J* . <https://stli.iii.org.tw/article-detail.aspx?tp=5&i=2&d=7288&no=57> adresinden alınmıştır
- Science Museum. (2018). *Boom and Bust : Telegraphy and the Wall Street Crash* . <https://www.sciencemuseum.org.uk/objects-and-stories/boom-and-bust-telegraphy-and-wall-street-crash> adresinden alınmıştır
- Security Council of Russia Federation [SCRF]. (2016). *Doctrine of Information Security of the Russian Federation* . http://www.scrf.gov.ru/security/information/DIB_engl/ adresinden alınmıştır
- Securelist. (2022). *DDoS attacks in Q1 2022*. <https://securelist.com/ddos-attacks-in-q1-2022/106358/>.
- Securelist. (2023). *Spam and phishing in 2022*. <https://securelist.com/spam-phishing-scam-report-2022/108692/> adresinden alınmıştır
- Securicon. (2019). *What's the Difference Between OT, ICS, SCADA and DCS?* [https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/#:~:text=Industrial%20Control%20System%20\(ICS\)%20is,belts%20in%20a%20mining%20operation](https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/#:~:text=Industrial%20Control%20System%20(ICS)%20is,belts%20in%20a%20mining%20operation) adresinden alınmıştır
- Segal, A. (2012). *China Moves Forward on Cybersecurity Policy*. CFR. <https://www.cfr.org/blog/china-moves-forward-cybersecurity-policy> adresinden alınmıştır
- Serger, S. S., & Bredt, M. (2007). China's Fifteen-Year Plan for Science and Technology: An Assessment. *Asia Policy*, No:4, 135-164.
- Shaohui, T. (2017). *International Strategy of Cooperation on Cyberspace*. http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm adresinden alınmıştır
- Sharma, S. (2022). *Google Blacklist – How to Remove Your Website from Google Blacklist (WordPress, Magento, PrestaShop, OpenCart, Drupal & PHP)*. <https://www.getastra.com/blog/911/google-blacklist/> adresinden alındı
- Sharifulin, V. (2021). *Russia, ASEAN discuss cooperation on cybersecurity — Foreign Ministry*. TASS: <https://tass.com/politics/1342009> adresinden alınmıştır

- Shcherbakova, T., & Kulikova, T. (2022). *Spam and phishing in 2021*. <https://securelist.com/spam-and-phishing-in-2021/105713/> adresinden alındı
- Shen, H. (2018). Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative. *International Journal of Communication*, Vol:12, 2683–2701.
- Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Negodenko, O. (2021). Information Security Risk Analysis SWOT. *Cybersecurity Providing in Information and Telecommunication Systems* (s. 309-3017). içinde Kyiv: CEUR Workshop Proceedings.
- Shepardson, D. (2021). *VW says data breach at vendor impacted 3.3 million people in North America* . <https://www.reuters.com/business/autos-transportation/vw-says-data-breach-vendor-impacted-33-million-people-north-america-2021-06-11/> adresinden alınmıştır
- Shepardson, D. (2022). *Nissan to trim production at U.S. plant over chips shortage*. Reuters: <https://www.reuters.com/business/autos-transportation/nissan-trim-production-us-plant-over-chips-shortage-2022-11-09/> adresinden alınmıştır
- Sherr, I. (2018). *Facebook, Cambridge Analytica and data mining: What you need to know*. <https://www.cnet.com/news/politics/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/> adresinden alınmıştır
- Shvartsman, D. (2023). *Apple Inc.: Our Modern-Day Symbol of Knowledge, Power, and Wealth*. <https://www.investing.com/academy/statistics/apple-facts/> adresinden alınmıştır
- Siboni, G., & Kronenfeld, S. (2014). *The Iranian Cyber Offensive during Operation Protective Edge*. Tel Aviv University. <https://www.inss.org.il/publication/the-iranian-cyber-offensive-during-operation-protective-edge/> adresinden alınmıştır
- Siboni, G., & Kronenfeld, S. (2014). Developments in Iranian Cyber Warfare, 2013-2014. *Military and Strategic Affairs*, 6(2), 83-104.
- Siboni, G., & Kronenfeld, S. (2012). Iran and Cyberspace Warfare. *Military and Strategic Affairs*, Volume:4, No:3, 77-99.
- Siddiqui, M. (tarih yok). *Why IOT in the Commercial Facilities Sector Opens As Many Opportunities As It Does Vulnerabilities*. <https://www.cybersaint.io/blog/why-iot-in-the-commercial-facilities-sector-opens-as-many-opportunities-as-it-does-vulnerabilities> adresinden alınmıştır
- Siegfried Group. (2021). *Siegfried overcomes cyber attack*. <https://www.siegfried.ch/siegfried+%25c3%25bcberwindet+folgen+der+cyberatactack+alt/news-en/11935> adresinden alınmıştır

- Siegfried Group. (2021). *Siegfried affected by attack on its IT systems*. <https://www.siegfried.ch/siegfried+von+angriff+auf+it-systeme+betroffen/news-en/11987> adresinden alınmıştır
- Silberg, G. (2022). *The impact of the Russia-Ukraine war on the auto industry*. KPMG .
- Sims, J. W. (2011). *Cybersecurity: The Next Threat to National Security* . Marine Corps Combat Development Command: Marine Corps University .
- Singer, P., & Friedman, A. (2014). *Siber Güvenlik ve Siber Savaş*. Oxford University Press.
- Sinopoli, A. F. (2012). *Cyberwar and International Law: An English School Perspective*. University of South Florida Scholar Commons.
- Sinopec. (2021). *Corporate Social Responsibility Report*. Beijing: China Petrochemical Corporation.
- Sluzhba Vneshney Razvedki [SVR]. (tarih yok). *Rusya Dış İstihbarat Teşkilatı'nın yetkileri*. <https://sgp.fas.org/crs/intel/R46616.pdf> adresinden alınmıştır
- Small Media. (2014). *Iranian Internet Infrastructure and Policy Report*. https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf.
- Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving Awareness of Social Engineering Attacks . *IFIP World Conference on Information Security Education*, 249–256.
- Social Welfare. (2011). *Social Welfare History Project*. Stock Market Crash of October 1929: <https://socialwelfare.library.vcu.edu/eras/great-depression/beginning-of-great-depression-stock-market-crash-of-october-1929/> adresinden alınmıştır
- Sohail, S. M., & Shanmugham, B. (2003). E-Banking and Customer Preferences in Malaysia: An Empirical Investigation. *Information Science Journal*. 150(3-4), 207-2017.
- Soldatov, A., & Borogan, I. (2016). *Putin brings China's Great Firewall to Russia in cybersecurity pact*. <https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact> adresinden alınmıştır
- Soldatov, A., & Borogan, I. (2022). *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*. <https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/> adresinden alınmıştır
- Solms, R. v., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

- Solon, O. (2016). *Team of hackers take remote control of Tesla Model S from 12 miles away.* The Guardian. <https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes> adresinden alınmıştır
- Son, H. (2019). *JP Morgan is rolling out the first US bank-backed cryptocurrency to transform payments business.* <https://www.cnbc.com/2019/02/13/jp-morgan-is-rolling-out-the-first-us-bank-backed-cryptocurrency-to-transform-payments-.html> adresinden alınmıştır
- Song, Y., Chen, B., & Wang, X.-Y. (2023). Cryptocurrency technology revolution: are Bitcoin prices and terrorist attacks related? *Financ Innov*, 9(1).
- Sophia, D., & Liaropoulos, A. (2010). Russia's National Security Strategy to 2020: A Great Power in the Making? *Caucasian Review of International Affairs*, Vol.4(1), 35-42.,
- Sophos. (2021). *The State of Ransomware in Manufacturing and Production 2021* . A Sophos Whitepaper.
- Sorbet, A. (2022). *History of mobile banking – how it all started?* <https://finanteq.com/history-of-mobile-banking-how-it-all-started/> adresinden alınmıştır
- Soylu, M. E. (tarih yok). *WordPress'te DDoS Saldırısı Nasıl Engellenir?* <https://www.mehmeteminsoylu.com/wordpress-te-ddos-saldirisi-nasil-engellenir/> adresinden alınmıştır
- Sönmez, E., & Codal, K. S. (2022). Terrorism in Cyberspace: A Critical Review of Dark Web Studies under the Terrorism Landscape. *Sakarya Üniversitesi Bilgisayar ve Bilişim Bilimleri Dergisi*, 5(1), 1-21.
- Sönmez, G., & Çelik, E. (2020). Anonimlik ile İlegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri. *Güvenlik Çalışmaları Dergisi*, 22(1), 66-88.
- Spadoni, G. (2019). *IRGC Cyber-Warfare Capabilities*. Institute for Counter-Terrorism (ICT) .
- Spafford, E. H. (1989). The Internet Worm Program: An Analysis. *ACM SIGCOMM Computer Communication Review*, 19(1), 1757.
- Spalevic, Z., & Ilic, M. (2017). The Use of Dark Web for the Purpose of Illegal Activity Spreading. *Ekonomika*, 63(1), 73-82.
- SPF. (tarih yok). *ARAMCO Control Center, Dhara, Saudi Arabia.* <https://spfconsoles.com/aramco-chooses-spf/> adresinden alınmıştır

- Springborg, M. (2018). *Made In China 2025 – Global Ramifications Of China Taking The Center Stage : White Paper* . C WorldWide Asset Management.
- Spitzner, L. (2022). *Nation State Threat Actors: From a Security Awareness Perspective*. SANS Institute. <https://www.sans.org/blog/nation-state-threat-actors-from-a-security-awareness-perspective/> adresinden alındı
- Stat Counter. (2023). *Mobile Vendor Market Share Worldwide*. <https://gs.statcounter.com/vendor-market-share/mobile> adresinden alınmıştır
- Statista. (2023). *Worldwide digital population 2023*. <https://www.statista.com/statistics/617136/digital-population-worldwide/> adresinden alınmıştır
- Statista. (2023a). *Distribution of cyber attacks across worldwide industries in 2022*. <https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/> adresinden alınmıştır
- Statista. (2023b). *Semiconductor foundries revenue share worldwide from 2020 to 2022, by country*. <https://www.statista.com/statistics/1230946/semiconductor-foundries-market-share-by-country-worldwide/> adresinden alınmıştır
- Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2014). *Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology (NIST).
- Stokes, M. A., Lin, J., & Hsiao, L. R. (2011). *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute.
- Subramanyam, K., Frank, C. E., & Galli, D. F. (2007). *Keyloggers: The Overlooked Threat to Computer Security*. <https://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html#.T6GcbOs9XmQ> adresinden alındı
- Suk-yeol, Y. (2022). *South Korea targets localizing 50% of chip materials by 2030* . <https://asia.nikkei.com/Business/Tech/Semiconductors/South-Korea-targets-localizing-50-of-chip-materials-by-2030> adresinden alınmıştır
- Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. *Journal of National Security Law & Policy*, 8(3), 437-468.
- Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. *Loyola of Los Angeles International and Comparative Law Review*, 32(2), 303-333.

- Swaine, J. (2008). *Georgia:Russia 'conducting cyber war'*. The Telegraph: <https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> adresinden alınmıştır
- Swearngin, L. W. (2019). *Terrorism in the 2020s: Examining the Global Threat Landscape*. Missouri State University.
- Sweeney, S. (2020). *After Bolivia, Elon Musk says capitalists can overthrow any government they want*. <https://www.peoplesworld.org/article/after-bolivia-elon-musk-says-capitalists-can-overthrow-any-government-they-want/> adresinden alınmıştır
- Sweigert, D. (2017). *Cyber Risk Assessment for the Emergency Services Sector - DHS*. <https://www.slideshare.net/dgsweigert/cyber-risk-assessment-for-the-emergency-services-sector-dhs> adresinden alınmıştır
- Swift. (tarih yok). *Swift history*. <https://www.swift.com/about-us/history> adresinden alınmıştır
- Sygnium Bank. (2021). *Sygnium Bank launches regulated digital asset options*. <https://www.insights.sygnium.com/post/sygnium-bank-launches-regulated-digital-asset-options> adresinden alınmıştır
- Synovitz, R. (2008). *Georgian Government Accuses Russia Of Waging 'Cyberwarfare'*. RFERL: https://www.rferl.org/a/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html adresinden alınmıştır
- Symantec. (tarih yok). *Windows Rootkit Overview*. White Paper: Symantec Security Response: <https://papers.vx-underground.org/archive/Symantec/windows-rootkit-overview-05-en.pdf> adresinden alındı
- Szymczak, P. D. (2022). *Gazprom Neft, ADNOC Step Up Efforts To Commercialize Digital Technology*. <https://jpt.spe.org/gazprom-neft-adnoc-step-up-efforts-to-commercialize-digital-technology> adresinden alınmıştır
- Şanlı, B., & Hobikoğlu, E. (2015). Development of Internet Banking as the Innovative Distribution Channel and Turkey Example. *Social and Behavioral Sciences*, Vol:195 , 343 – 352.
- Şevlin, R. (2019). *How Much Do Banks Spend On Technology? (Hint: It Would Weigh 670 Tons In \$100 Bills)*. Forbes : <https://www.forbes.com/sites/ronshevin/2019/04/01/how-much-do-banks-spend-on-technology-hint-chase-spends-more-than-all-credit-unions-combined/?sh=5e0dd7e5683a> adresinden alınmıştır

- Şenol, M. (2018). Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık. Ş. Sağiroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (s. 181-221). Ankara: Grafiker Yayınları.
- Tasnim News. (2015). *Iran, Russia Agree on Cyber-Defense Cooperation: Official*. Tasnim News Agency: <https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defense-cooperation-official> adresinden alınmıştır
- TASS. (2018). *Russia and India confirm readiness to cooperate in cyber security*. TASS Russian News Agency: <https://tass.com/world/990504> adresinden alınmıştır
- TASS. (2022). *Russia and Armenia to cooperate on cyber security — Security Council*. TASS Russian News Agency: <https://tass.com/politics/1439881> adresinden alınmıştır
- T.C. Ulaştırma ve Altyapı Bakanlığı [UAB]. (tarih yok). *CryptoLocker Virüsü Hakkında Bilgilendirme*. <https://www.uab.gov.tr/uploads/pages/cryptolocker-virusu-hakkinda-bilgilendirme/74bc0128f065b41.pdf> adresinden alındı
- Tecim, V. (tarih yok). *Endüstri 4.0*. <https://vahaptecim.com.tr/endustri-4-0/> adresinden alınmıştır
- Tekir, G. (2020). Huawei, 5G Networks, and Digital Geopolitics. *International Journal of Politics and Security*, 2(4), 113-135.
- Tesla. (2016). *A Tragic Loss*. <https://www.tesla.com/blog/tragic-loss> adresinden alınmıştır
- Thales . (2023). *2022-2023 : A year of Cyber Conflict in Ukraine*.
- Thaware, V. (2020). *COVID-19 Outbreak Prompts Opportunistic Wave of Malicious Email Campaigns*. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/covid-19-outbreak-prompts-opportunistic-wave-malicious-email-campaigns> adresinden alındı
- The Australia Institute. (2019). *Trolls and polls –the economic costs*. The Australia Institute.
- The Atlantic Council of the United Kingdom. (tarih yok). *Cyber Warfare: Evolving the Modern Battlefield*. <https://www.atlanticcounciluk.org/single-post/cyber-warfare-evolving-the-modern-battlefield> adresinden alınmıştır
- The Brainy Insights. (2021). *Fintech Market*. s. <https://www.thebrainyinsights.com/report/fintech-market-12704>.

- The Canadian Centre for Cyber Security. (2021). Cyber threat and cyber threat actors. *Canadian Centre for Cyber Security*. <https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors> adresinden alındı
- The Central News Agency [CNA]. (2022). 台積電先進製程占全球6成 專家：是台灣堅強砂盾 . <https://www.cna.com.tw/news/afe/202204270171.aspx> adresinden alınmıştır
- The China Project. (tarih yok). *State Grid Corporation of China (SGCC)*. <https://thechinaproject.com/company-profiles/state-grid-corporation-of-china-sgcc/> adresinden alınmıştır
- The Criminal Code Of The Russian Federation . (1996). *Chapter 28. Crimes in the Sphere of Computer Information*. <http://www.russian-criminal-code.com/PartII/SectionIX/Chapter28.html> adresinden alınmıştır
- The Geopost. (2022). *How the Ukrainians discovered ‘Center 16’, the Russian espionage system*. <https://thegeopost.com/en/news/how-the-ukrainians-discovered-center-16-the-russian-espionage-system/> adresinden alınmıştır
- The Guardian. (2020). *New Zealand stock exchange disrupted by fourth 'offshore' cyber attack*. <https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack> adresinden alınmıştır
- The Local. (2014). *300 oil companies hacked in Norway*. <https://www.thelocal.no/20140827/norwegian-oil-companies-hacked> adresinden alınmıştır
- The National Interest [TNI]. (2019). *How China Stole Top Secret Information on the F-22 and F-35*. <https://nationalinterest.org/blog/buzz/how-china-stole-top-secret-information-f-22-and-f-35-94201> adresinden alınmıştır
- The National Institute for Defense Studies [NIDS]. (2020). *NIDS China Security Report 2021 China’s Military Strategy in the New Era*. Tokyo.
- The National People's Congress PRC. (2010). *Report on the Outline of the Tenth Five-Year Plan for National Economic and Social Development (2001)*. http://www.npc.gov.cn/zgrdw/englishnpc/Special_11_5/2010-03/03/content_1690620.htm.
- The National People's Congress PRC. (2021). *Data Security Law of the People's Republic of China*. <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>.
- The Norwegian Police Security Service [PST]. (2023). *National threat assessment 2023* .

- The White House. (2015a, 09 25). *President Xi Jinping's State Visit to the United States*. <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> adresinden alınmıştır
- The White House. (2016). *Presidential Policy Directive / PPD-41*. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident> adresinden alınmıştır
- The White House. (2017). *2017 National Security Strategy*. Washington, DC: The White House.
- The White House. (2018). *National Cyber Security* . Washington, DC : The White House.
- The White House. (2021). *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*. The White House. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/> adresinden alındı
- The White House. (2021a). *Executive Order on Improving the Nation's Cybersecurity*. Washington: The White House.
- The White House. (2021b). *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*.
- The White House. (2021c). *FACT SHEET: President Biden Sets 2030 Greenhouse Gas Pollution Reduction Target Aimed at Creating Good-Paying Union Jobs and Securing U.S. Leadership on Clean Energy Technologies*.
- The White House. (2022). *2022 National Security Strategy*. <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> adresinden alınmıştır
- The White House. (2022a). *Indo-Pasific Strategy*. <https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf> adresinden alınmıştır
- The White House. (2022b). *U.S.-Singapore Joint Leaders' Statement*. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/29/u-s-singapore-joint-leaders-statement/> adresinden alınmıştır
- The World Bank. (tarih yok). *The World Bank Group and the International Monetary Fund (IMF)* . <https://www.worldbank.org/en/about/history/the-world-bank-group-and-the-imf> adresinden alınmıştır

- Thompson, M. (2016). *Iranian Cyber Attack on New York Dam Shows Future of War*. Time. <https://time.com/4270728/iran-cyber-attack-dam-fbi/> adresinden alınmıştır
- Thomson Reuters. (tarih yok). *Cyberspace Administration of China (CAC)* . [https://uk.practicallaw.thomsonreuters.com/8-618-2325?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/8-618-2325?transitionType=Default&contextData=(sc.Default)&firstPage=true) adresinden alınmıştır
- Tidy, J. (2020). *Honda's global operations hit by cyber-attack*. BBC. <https://www.bbc.com/news/technology-52982427> adresinden alınmıştır
- Tirrell, W. K. (2012). *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?* . Kansas : The George Washington University.
- Tirpak, J. A. (2012). Here Comes Adversary Stealth. *AIR FORCE Magazine*, 22-27.
- Tiwari, S. (2022). *Chinese 'Stealth' Espionage! How Beijing-Backed Hackers 'Acquired' Sensitive US Tech Used In Its F-35 Fighter Jet?*. Eurasian Times. <https://eurasianimes.com/chinese-stealth-espionage-us-tech-used-in-its-f-22-f-35-fighter/> adresinden alınmıştır
- Total Energies. (2019). *Total Opens a Digital Factory to Further its Ambition of Becoming the Responsible Energy Major*. <https://totalenergies.com/media/news/press-releases/total-opens-digital-factory-further-its-ambition-becoming-responsible-energy-major> adresinden alınmıştır
- Total Energies. (2021). *Total and Microsoft partner to drive digital innovation and Net Zero goals*. <https://totalenergies.com/media/news/press-releases/total-and-microsoft-partner-drive-digital-innovation-and-net-zero-goals> adresinden alınmıştır
- T-Mobile. (2023). *T-Mobile Informing Impacted Customers about Unauthorized Activity*. <https://www.t-mobile.com/news/business/customer-information> adresinden alınmıştır
- Traynor, I. (2007). *Russia Accused of Unleashing Cyberwar to disable Estonia* . The Guardian. <https://www.theguardian.com/world/2007/may/17/topstories3.russia> adresinden alınmıştır
- Troianovski, A., & Nakashima, E. (2018). *How Russia's military intelligence agency became the covert muscle in Putin's duels with the West*. https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html adresinden alınmıştır

- Tropeano, R. (2019). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. National Security Archive: <https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations> adresinden alınmıştır
- TRT World. (2022). *China, Iran begin implementation of 25-year strategic pact*. <https://www.trtworld.com/middle-east/china-iran-begin-implementation-of-25-year-strategic-pact-53678> adresinden alınmıştır
- TrendMicro. (2016). *BlackEnergy*. <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy> adresinden alınmıştır
- Turhost. (2021). *SQL Injection Nedir?*. <https://www.turhost.com/blog/sql-injection-nedir/#serp> adresinden alındı
- Turhost. (tarih yok). *Cryptojacking Nedir?*. <https://www.turhost.com/blog/cryptojacking-nedir/> adresinden alındı
- Turovets, J., Proskuryakova, L., Starodubtseva, A., & Bianco, V. (2021). Green Digitalization in the Electric Power Industry. *Journal of the National Research University Higher School of Economics*, 15(3), 35-51.
- TÜBİSAD. (2021). *Bilgi ve İletişim Teknolojileri Sektörü 2020 Pazar Verileri*. Deloitte.
- Türkiye Maden Profesyonelleri. (2020). *Akıllı Telefonlar İçerisinde Bulunan Madenler*. <https://www.madenprofesyonelleri.com/akilli-telefonlar-icerisinde-bulunan-madenler/> adresinden alınmıştır
- UAE Moments. (2022). *BAE, Ekonomik Başarıyı Ölçmek İçin Brüt Metaverse Ürünü (GMP) Kullanacak*. <https://www.uaemoments.com/uae-to-use-gross-metaverse-product-gmp-to-measure-economic-success-509680.html> adresinden alınmıştır
- UAE Moments. (2022a). *Ministry of Economy Announces Metaverse HQ*. <https://www.uaemoments.com/ministry-of-economy-announces-metaverse-hq-509904.html> adresinden alınmıştır
- U.K. Cabinet Office. (2011). *A Detica Report in Partnership With the Office of Cyber Security and Information*.
- Uma, M., & Ganapathi, P. (2013). A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security*, 15(5), 390-396.
- United Against Nuclear Iran [UANI]. (2022). *The Iranian Cyber Threat*.

- UN. (1948). *Universal Declaration of Human Rights*. New York : United Nations General Assembly.
- UN General Assembly. (2003). 57/239. *Creation of a global culture of cybersecurity*. United Nations .
- UN General Assembly. (2015). A/69/723, *International code of conduct for information security*. United Nations .
- United States Coast Guard [USCG]. (tarih yok). *Cyber Security*. <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/> adresinden alınmıştır
- United States Cyber Command [USCYBERCOM]. (tarih yok). *Our History*. <https://www.cybercom.mil/About/History/> adresinden alınmıştır
- United States General Accounting Office [GAO]. (2004). *CRITICAL INFRASTRUCTURE PROTECTION, Challenges and Efforts to Secure Control Systems*. GAO-04-354: United States General Accounting Office.
- United States Government Accountability Office [GAO]. (2011). *Defense Department Cyber Efforts*. <https://www.gao.gov/assets/gao-11-421.pdf> adresinden alınmıştır
- UNCCT. (tarih yok). *Cybersecurity and New Technologies*. UN Counter-Terrorism Centre: <https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity> adresinden alınmıştır
- UNODC. (2019). *E4J University Module Series: Cybercrime (Cyber organized crime: What is it?)*. United Nations Office on Drugs and Crime. https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html adresinden alınmıştır
- UNODC. (2010). *The Globalization of Crime A Transnational Organized Crime Threat Assessment*. Vienna: United Nations Office on Drugs and Crime.
- UNODC. (2019). *E4J University Module Series: Cybercrime (Cyber organized crime activities)*. United Nations Office on Drugs and Crime. <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html> adresinden alınmıştır
- UN Security Council. (2021). *UN Documents for DPRK (North Korea): Sanctions Committee Documents S/2021/211*.

- UN Security Council. (2023). *Democratic People's Republic of Korea's New Ballistic-Missile Launch Dangerously Raising Tensions, Senior Official Warns Security Council, Urging Unity, Dialogue*.
- Upchurch, T. (2018). *How China could beat the West in the deadly race for AI weapons*. <https://www.wired.co.uk/article/artificial-intelligence-weapons-warfare-project-maven-google-china> adresinden alındı
- Upstream Security. (2022). *Global Automotive Cybersecurity Report*.
- U.S. Attorney's Office. (2018). *Darknet international gun traffickers sentenced*. <https://www.justice.gov/usao-ndga/pr/darknet-international-gun-traffickers-sentenced> adresinden alınmıştır
- U.S. Army Cyber Command . (2022). *Cyber Mission Force*. <https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/2079661/cyber-mission-force/#:~:text=What%20is%20the%20Cyber%20National,aligned%20to%20support%20the%20CNMF>. adresinden alınmıştır
- U.S. Department of the Treasury . (2018). *Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators*. <https://home.treasury.gov/news/press-releases/sm0250> adresinden alınmıştır
- U.S. Department of the Treasury. (2018). *Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators*. <https://home.treasury.gov/news/press-releases/sm0250> adresinden alınmıştır
- U.S. Embassy and Consulate in Poland. (2019). *U.S., Poland Sign Cyberspace Defense Cooperation Agreement*. https://pl.usembassy.gov/cyberspace_agreement/ adresinden alınmıştır
- U.S. Energy Information Administration [EIA]. (tarih yok). *What is U.S. electricity generation by energy source?* <https://www.eia.gov/tools/faqs/faq.php?id=427&t=3> adresinden alınmıştır
- U.S. Government Publishing Office. (2016). *The Future of Iranian Terror and Its Threat to the U.S. Homeland*. Subcommittee on Counterterrorism and Intelligence: <https://docs.house.gov/meetings/HM/HM05/20160211/104455/HHRG-114-HM05-Wstate-BermanI-20160211.pdf> adresinden alınmıştır
- U.S. Government Accountability Office. (2023). *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management*

Agencies *Implement* *Statutory* *Responsibilities.*
<https://www.gao.gov/products/gao-23-105806> adresinden alınmıştır

- U.S. Immigration and Customs Enforcement [ICE]. (tarih yok). *HSI Cyber Crimes Center*. <https://www.ice.gov/partnerships-centers/cyber-crimes-center> adresinden alınmıştır
- U.S. Securities and Exchange Commission. (1993). *The Laws That Govern the Securities Industry*. <https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry> adresinden alınmıştır
- Ünay, S. (2019). *Bir şirketten daha fazlası: Huawei ve teknoloji savaşları*. <https://www.aa.com.tr/tr/analiz/bir-sirketten-daha-fazlasi-huawei-ve-teknoloji-savaslar/1492049> adresinden alınmıştır
- Ünver, M., & Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik . *EMO elektrik Mühendisliği Dergisi*, 438, 94-103.
- Ünver, M., Canbay, C., & Mirzaoglu, A. G. (2009). *Siber Güvenliğin Sağlanması : Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.
- Varma, J. R. (2019). Blockchain in Finance. *The Journal for Decision Makers*, 44(1), 1-11.
- Vatis, M. A. (2010). The Council of Europe Convention on Cybercrime. N. R. Council içinde, *Proceedings of a Workshop on Deterring Cyberattacks* (s. 207-223). Washington, DC : The National Academies Press .
- Verton, D. (1999). *Serbs launch cyberattack on NATO*. <https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/> adresinden alınmıştır
- Vincent, J. (2018). *1.5 million affected by hack targeting Singapore's health data*. <https://www.theverge.com/2018/7/20/17594578/singapore-health-data-hack-sing-health-prime-minister-lee-targeted> adresinden alınmıştır
- Volz, D., & Finkle, J. (2016). *U.S. helping Ukraine investigate power grid hack*. Reuters. <https://www.reuters.com/article/us-ukraine-cybersecurity-usa-idUSKCN0UQ24020160112> adresinden alınmıştır
- Volenik, A. (2022). *The 4 Best Digital-Only Banks In China*. <https://topmobilebanks.com/digital-banks-china/> adresinden alınmıştır
- Volenik, A. (2023). *Fintech Vs. Digital Banking (With Examples)*. <https://topmobilebanks.com/blog/fintech-vs-digital-banking/>.

- Xinhuanet. (2014, 02 27). 习近平: 把我国从网络大国建设成为网络强国. http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm adresinden alınmıştır
- Wakefield, J. (2020). *EasyJet admits data of nine million hacked*. BBC. <https://www.bbc.com/news/technology-52722626> adresinden alınmıştır
- Walker, S. (2016). *Russia blocks access to LinkedIn over foreign-held data*. <https://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data> adresinden alınmıştır
- Weber, V. (2020). *The Sinicization of Russia's Cyber Sovereignty Model*. <https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model> adresinden alınmıştır
- Weedon, J., Nuland, W., & Stamos, A. (2017). *Information Operations and Facebook*. Facebook Security.
- Wei, Y. (2016). *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*. <https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/> adresinden alınmıştır
- Weimann, G. (tarih yok). *Going Darker? The Challenge of Dark Net Terrorism*. Wilson Center .
- Whitehead, Y. G. (1999). *Information as a Weapon: Reality Versus Promises*. BiblioScholar.
- Warren, P., Kaivanto, K., & Prince, D. (2018). *Could a cyber attack cause a systemic impact in the financial sector?* Bank of England.
- Westby, J. R. (2020). *Russia Has Carried Out 20-Years Of Cyber Attacks That Call For International Response*. Forbes: <https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/?sh=1f6f532c6605> adresinden alınmıştır
- Western Union [WU]. (2019, 10 08). *6 fascinating things about Western Union's history*. <https://www.westernunion.com/blog/en/6-fascinating-things-about-western-unions-history/> adresinden alınmıştır
- Wolff, J. (2018). *Trump's Reckless Cybersecurity Strategy*. The New York Times: <https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html> adresinden alınmıştır

- Wong, E. (2019). *How China Uses LinkedIn to Recruit Spies Abroad*.
<https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html>
adresinden alınmıştır
- Wong, J. C. (2019). *The Cambridge Analytica scandal changed the world – but it didn't change Facebook*.
<https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook> adresinden alınmıştır
- Woolley, S. C., & Howard, P. N. (2016). Political Communication, Computational Propaganda, and Autonomous Agents. *International Journal of Communication*, 4882–4890 .
- World Trade Organization . (2013). *World Trade Report - Factors shaping the future of world trade*. WTO .
- World Economic Forum [WEF]. (2017). *Digital Transformation Initiative Oil and Gas Industry*. Geneva.
- World Economic Forum. (tarih yok). *Strengthening cybersecurity in the oil and gas industry*.
<https://www.weforum.org/impact/cyber-resilience-oil-and-gas/>
adresinden alınmıştır
- Yalman, Y. (2018). Siber Terör, Terörizm ve Mücadele. Ş. Sağiroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (s. 259-280). Ankara: Grafiker Yayınları.
- Yetgin, M. A. (2020). Covid-19'un Küresel İletişim ve Teknoloji Şirketleri Üzerindeki Etkilerine İlişkin Stratejik Bir Araştırma. 3. *International Economics, Business and Social Sciences Congress* (s. 105-115). Econdor .
- Yetgin, M. A. (2021). *Çin İstihbarat Örgütünün Stratejik Analizi*. Ankara: Gazi Kitabevi.
- Yetgin, M. A., & Özkan, S. (2021). Nükleer Silahsızlanmanın Hukuksal Boyutu: İran ve İsrail Örneği. *Ankara V. International Scientific Research Congress* (s. 112-122). Ankara: IKSAD.
- Yetgin, M. A., & Baştuğ, M. (2022). *Metaverse ve Şirketlerde Dijital Dönüşüm*. Ankara: Detay Yayıncılık.
- Yetgin, M. A., & Özkan, S. (2022). Metaverse, Küresel Şirketler, Ulus Devletler ve Yeni Bir Uluslararası Sistem. *5th International New York Academic Research Congress* , (s. 209-2015). New York .

- Yehoshua, M. (2019). *Takeaways From The Oldsmar Water Attack & What Security Leaders Can Do About It*. Scadafence. <https://blog.scadafence.com/takeaways-from-the-oldsmar-water-attack-what-security-leaders-can-do-about-it> adresinden alınmıştır
- Yıldız, A. (2018). Endüstri 4.0 ve Akıllı Fabrikalar . *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 22(2) , 546-556.
- Yılmaz, C. (2026). Siber Güvenlik ve İnsan Hakları . *Cyberpolitik Journal*, 1(2), 273-291.
- Yoo-chul, K. (2014). *NK behind nuclear plant hacking*. Korea Times. https://www.koreatimes.co.kr/www/news/tech/2014/12/133_170464.html adresinden alınmıştır
- YRIS. (2017). *Cyber-defense Strategies for Contending with Non-state Actors: A Review and Assessment of Existing Proposals*. *The Yale Review of International Studies*. <http://yris.yira.org/comments/2214> adresinden alındı
- Yu, E. (2021). *Singapore, US pledge deeper collaboration in cybersecurity*. <https://www.zdnet.com/article/singapore-us-pledge-deeper-collaboration-in-cybersecurity/> adresinden alınmıştır
- Zahra, I., Handayan, I., & Christiant, D. W. (2021). Cyber-Attack in Estonia: a New Challenge in The Applicability of International Humanitarian Law. *Yustisia Jurnal Hukum*, 10(1), 48-66.
- Zavershinskiy, V. İ. (2006). Генерал-полковник Владимир ЗАВЕРШИНСКИЙ "У президента с разведки спрос особый". (A. Bondarenko, Röportajı Yapan)
- Zeybek, H. (2018). Dijital Bankacılık . *Mali Çözüm*, 28(150), 79-107.
- Zeri, N. N., & Noordin, N. N. (2017). Framing Cyberterrorism: A Content Analysis of The New York Times. *Journal of Media and Information Warfare*, Vol:9, 179-200.
- Zhang, Z. (2022). *A Close Reading of China's New Cybersecurity Review Measures, in Effect Feb 15, 2022*. China Briefing: <https://www.china-briefing.com/news/a-close-reading-of-chinas-new-cybersecurity-review-measures-in-effect-february-15-2022/> adresinden alınmıştır
- Zhou, K., Liu, T., & Liang, L. (2016). From cyber-physical systems to Industry 4.0: make future manufacturing become possible. *International Journal of Manufacturing Research*, 11(2), 167-188.

Zoho Corporation. (tarih yok). *What is a brute force attack?* Manage Engine. <https://www.manageengine.com/log-management/cyber-security-attacks/what-is-brute-force-attack.html> adresinden alındı

Zhu, H., & Pasadilla, G. O. (2015). Manufacturing of Telecommunications Equipment. *Services in Global Value Chains: Manufacturing-Related Services* (s. 314-343). içinde APEC Secretariat.



TABLÖLAR LİSTESİ

Tablo 1: Farklı siber eylemlerin temel özellikleri.....	30
Tablo 2: Endüstri 4.0'da üretim değişiminin gelişimi.....	187



ŞEKİLLER LİSTESİ

Şekil 1: DDoS Saldırısı	39
Şekil 2: DDoS saldırılarının karşılaştırmalı sayısı 2022'nin 1. çeyreği, 2021 4. çeyreği, 2022'nin 1. çeyreği	41
Şekil 3: 2016-2021 yılları arasında fidye yazılım saldırıları ile alınan toplam kripto para değerleri.....	47
Şekil 4: Ortadaki Adam Saldırısında saldırganın gizli verileri ele geçirmek için kendisini istemci ve sunucu arasında konumlandırması	51
Şekil 5: Siber tehdit aktörünün güvenilir bir web sayfası gibi davranması.....	52
Şekil 6: 2022 Spam Kaynakları.....	56
Şekil 7: Kritik Altyapı Sektörleri	75
Şekil 8: Sektöre Yönelik Siber Saldırı İstatistikleri	76
Şekil 9: Kritik Altyapının Temel Bileşenleri	77
Şekil 10: Banka için siber güvenli riski ne kadar önemli? 2020 - 2021.....	83
Şekil 11: Acil Servis Alanları.....	89
Şekil 12: Endüstri 4.0'ın Evrimi	183
Şekil 13: Endüstri 4.0 Teknolojileri	185
Şekil 14: Dördüncü Sanayi Devrimi Hangi Ülkede Ne Zaman Başladı?.....	188
Şekil 15: 2020'den 2022'ye kadar dünya çapında yarı iletken gelir payı	198
Şekil 16: Haziran 2022 itibarıyla 5G patent sayısı.....	238
Şekil 17: Dünya çapında mobil satıcı pazar payı - Şubat 2023	239
Şekil 18: Huawei ekipmanlarını 5G ağlarında kullanmaya yönelik resmi yaklaşımlar	243
Şekil 19: Akıllı telefonlar içerisinde bulunan madenler.....	248
Şekil 20: İnternetin katmanları	262

Şekil 21: Piyasa değeri ile en büyük petrol şirketlerinde dijital inovasyon skoru 2021	272
Şekil 22: BP'nin Meksika Körfezi'nde işlettiği platformlar (Argos, Atlantis, Mad Dog, Na Kika, Thunder Horse).....	273
Şekil 23: 4IR Merkezi	276
Şekil 24: Ham petrol ürünleri için spot fiyatlar (2020-2022).....	280
Şekil 25: BloombergNEF raporuna göre petrol Endüstrisinin gelişmiş analitik ve bulut bilgi işlem harcamaları 2019'da 1,3 milyar dolardan 2030'da 12,5 milyar dolara katlanarak artacağı tahmin edilmektedir	281
Şekil 26: AB'nin doğalgaz ithalatı Rusya ve diğer, Ocak 2019 - Kasım 2022.....	282
Şekil 27: AB'nin doğal gaz ithalatı (Ocak-Kasım 2022).....	283
Şekil 28: Colonial Pipeline Boru Hattı Haritası	290
Şekil 29: Amsterdam-Rotterdam-Antwerp Rotası	292
Şekil 30: İnsan Hakları & Savaş Hukuku.....	301
Şekil 31: Araştırmanın Modeli	319
Şekil 32: Araştırmanın Genişletilmiş Modeli.....	323
Şekil 33: Devletler SWOT Analizi.....	325
Şekil 34: Şirketler SWOT Analizi.....	337

ÖZGEÇMİŞ

Sevcan ÖZKAN, 2019 yılında Çankırı Karatekin Üniversitesi'nden Uluslararası İlişkiler lisans bölümünden mezun oldu ve aynı yıl Erasmus Staj programıyla Romanya'da Estetick Pack şirketinde stajını tamamladı. 2021 yılında Karabük Üniversitesi Lisansüstü Eğitim Enstitüsü'nde Uluslararası İlişkiler Anabilim Dalı'nda Yüksek Lisans Programına başladı. Haziran 2021'de III. Uluslararası Kapadokya Öğrenci Kongresi'nde "Uluslararası Hukukun Siber Savaşta Rolü" isimli makale özetini, Ekim 2021'de Ankara V. Uluslararası Bilimsel Araştırma Kongresinde "Nükleer Silahsızlanmanın Hukuksal Boyutu: İran ve İsrail Örneği" isimli makaleyi, Nisan 2022'de V. Uluslararası New York Akademik Araştırma Kongresinde "Metaverse, Küresel Şirketler, Ulus Devletler ve Yeni Bir Uluslararası Sistem" isimli makaleyi sundu. Ocak 2022 yılında "Asya'da Güvenlik ve Çatışma Analizi Üzerine Stratejik Araştırmalar" isimli kitapta "Asya'da Uluslararası Örgütlerin Stratejik Etkileri" isimli başlıkta bölüm yazarı olarak yer aldı.