TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SOSYAL ÇEVRE BİLİMLERİ ANABİLİM DALI

ÇEVRE ETİĞİ BAĞLAMINDA SİBER GÜVENLİK

Doktora Tezi

Sema ALTINSOY

Tez Danışmanı
Prof. Dr. Nesrin ÇOBANOĞLU

Ankara, 2023

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SOSYAL ÇEVRE BİLİMLERİ ANABİLİM DALI

ÇEVRE ETİĞİ BAĞLAMINDA SİBER GÜVENLİK

Doktora Tezi

Sema ALTINSOY

Tez Danışmanı
Prof. Dr. Nesrin ÇOBANOĞLU

Ankara, 2023

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SOSYAL ÇEVRE BİLİMLERİ ANABİLİM DALI

ÇEVRE ETİĞİ BAĞLAMINDA SİBER GÜVENLİK

Doktora Tezi

Tez Danışmanı
Prof. Dr. Nesrin ÇOBANOĞLU

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı	İmzası
1. Prof. Dr. Nesrin ÇOBANOĞLU	
2. Prof. Dr. Türksel KAYA BENSGHİR	
3. Prof. Dr. Meryem BULUT	
4. Prof. Dr. Ayşe Nilsun DEMİR	
5. Doç. Dr. Serdar Hakan ÖZTANER	

Tez Savunması Tarihi
3 Şubat 2023

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE,

Prof. Dr. Nesrin ÇOBANOĞLU danışmanlığında hazırladığım "Çevre Etiği Bağlamında Siber Güvenlik (Ankara, 2023)" adlı doktora tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Tarih: 03/02/2023
Adı-Soyadı ve İmza
Sema ALTINSOY

TEŞEKKÜR

Tez çalışması süreci boyunca bilgi ve deneyimlerini paylaşarak beni destekleyen, cesaretlendiren değerli danışman hocam Prof. Dr. Nesrin ÇOBANOĞLU'na çok teşekkür ederim.

Tez çalışmamın olgunlaşmasına önemli katkıları olan değerli hocam Prof. Dr. Türksel BENSGHİR'e teşekkürü borç bilirim.

Sosyal Çevre Bilimleri Bölümünde değerli katkıları ile daha önce çok da farkında olmadığım çevre alanında, bana etik davranış sergileme sorumluluğu ile çevre bilinci kazandıran değerli hocalarım Prof. Dr. Ruşen KELEŞ, Prof.Dr. Berna ALPAGUT, Prof.Dr. Aykut Namık ÇOBAN, Prof.Dr. Ayşegül MENGİ, Prof.Dr. Hakan YİĞİTBAŞIOĞLU, Prof.Dr. Erol DEMİR ve Prof.Dr. Meryem BULUT'a şükranlarımı sunarım.

Doktora eğitimim ve tez yazma sürecim boyunca her alanda desteklerini benden esirgemeyen canım aileme de sonsuz teşekkürler…

Sema ALTINSOY

İÇİNDEKİLER

İÇİNDEKİLER i
KISALTMALAR iii
TABLOLAR viii
GİRİŞ 1

BİRİNCİ BÖLÜM
ÇEVRE ETİĞİ ve SİBER GÜVENLİK
KAVRAMSAL ÇERÇEVE

1.1 GÜVENLİK KAVRAMI 18
1.2 ÇEVRE ETİĞİNİN KAVRAMSAL TEMELLERİ 21
1.2.1 Çevre Kavramı 21
1.2.2 Uygulamalı Etik Kapsamında Çevre Etiği 25
1.3 SİBER GÜVENLİK KAVRAMLARI 44
1.3.1 Siber Uzay-Siber Ortam-Siber Alan-Siber Dünya 45
1.3.2 Siber Güvenlik Tanımı 48
1.3.3 Siber Güvenlik Olayları 52
1.3.4 Siber Güvenlik Açığı 54
1.3.5 Siber Tehditler 55
1.3.6 Siber Saldırılar 57
1.3.7 Siber Saldırganlar 65
1.3.8 Siber Terörizm ve Siber Savaş 69
1.4 ÇEVRE ETİĞİ ve SİBER GÜVENLİK İLİŞKİSİ 73

İKİNCİ BÖLÜM
KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİ

2.1 KRİTİK ALTYAPILAR VE ÇEVRESEL SORUNLAR OLUŞTURABİLECEK KRİTİK SEKTÖRLER 77
2.1.1 Kritik Altyapılar 78
2.1.2 Çevre Sorunları Oluşturabilecek Kritik Altyapı Sektörleri 81
2.1.3 Kritik Altyapılarda Kullanılmakta Olan Endüstriyel Kontrol Sistemleri 86
2.1.4 Kritik Altyapıların Birbirine Bağımlılığı 102
2.2 ENDÜSTRİYEL KONTROL SİSTEMLERİNİN SİBER GÜVENLİĞİ 106
2.2.1 Endüstriyel Kontrol Sistemlerindeki Siber Güvenlik Açıkları 110
2.2.2 Endüstriyel Kontrol Sistemlerinin Siber Güvenliğine Yönelik Tehditler 126
2.3 KRİTİK ALTYAPILARA YÖNELİK SİBER GÜVENLİK OLAYI ÖRNEKLERİ 133
2.3.1 Kritik Altyapılara Yönelik Gerçekleşen Bazı Siber Güvenlik Olayları 135
2.3.2. Kritik Altyapılara Yönelik Siber Güvenlik Olayı Örneklerinin Siber Güvenlik Açısından Değerlendirilmesi 150
2.3.3 Kritik Altyapılara Yönelik Siber Güvenlik Olaylarının Sürdürülebilirlik Açısından Değerlendirilmesi 154

ÜÇÜNCÜ BÖLÜM
KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK OPERASYONEL FAALİYETLER

3.1 OPERASYONEL SİBER GÜVENLİK YAKLAŞIMLARI 158

3.1.1 Önleyici-Koruyucu Yaklaşım ve Emniyetli-Sağlam Sistemler 159
3.1.2 Risk Yönetimi Yaklaşımı 165
3.2 BİREYSEL SİBER GÜVENLİK FAALİYETLERİ 171

3.2.1 Personel ile İlgili Siber Güvenlik Önlemleri 171
3.2.2 Siber Güvenliğin Sağlanmasında Bireysel Etik Davranış 182
3.3 KURUMSAL SİBER GÜVENLİK FAALİYETLERİ 187

3.4. KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK OPERASYONEL FAALİYETLERİN DEĞERLENDİRİLMESİ 207

DÖRDÜNCÜ BÖLÜM
KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK STRATEJİK FAALİYETLER

4.1. STRATEJİK SEVİYEDE SİBER GÜVENLİK YAKLAŞIMLARI 210

4.1.1. Caydırıcılık Yaklaşımı 211
4.1.2. Kamu Siber Güvenlik Yaklaşımı 213
4.2 DEVLETLERİN STRATEJİK SİBER GÜVENLİK FAALİYETLERİ 215

4.2.1 Devletlerde Siber Güvenlik Yönetişimi ve Siber Güvenlik Paydaşları 216
4.2.1.1. Siber Güvenlik Yönetişimi 216
4.2.2 Ulusal Siber Güvenlik Stratejisi 225
4.2.3 Kritik Altyapıların Siber Güvenliğine Yönelik Kriz Yönetimi 235
4.2.4 Türkiye'de Endüstriyel Kontrol Sistemlerinin Siber Güvenliğine Yönelik Politikalar 237
4.3 KÜRESEL SEVİYEDE KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK STRATEJİK FAALİYETLER 252

4.3.1 Küreselleşmeden Kaynaklanan Siber Güvenlik Sorunları 253
4.3.2 Küresel Yönetişim 256
4.3.3 Küresel Siber Güvenlik Yönetişimi 259
4.3.4 Küresel Siber Güvenlik Yönetişiminin Kurumsal Yapıları 260
4.3.5. Kritik Altyaspıların Siber Güvenliğine Yönelik Standartlar ve Kılavuzlar 270
4.3.6. Küresel Yönetişimin Sorunları ve Kozmopolitanizm 281
4.4 KRİTİK ALTYAILARIN SİBER GÜVENLİĞİNE YÖNELİK STRATEJİK FAALİYETLERİN DEĞERLENDİRİLMESİ 283

SONUÇ ve DEĞERLENDİRME 287

KAYNAKLAR 301

ÖZET 325

ABSTRACT 326

KISALTMALAR

ACM **:** Assocation for Computing Machinery- Bilişim Cihazları Derneği

AFAD : Afet ve Acil Durum Yönetimi

AGİT **:** Avrupa Güvenlik ve İşbirliği Teşkilatı

AMI **:** Advanced Metering Infrastructure Security- Gelişmiş Ölçüm Altyapısı

APT **:** Advanced Persistent Threat - Gelişmiş Sürekli Tehditler

BGYS : Bilgi Güvenliği Yönetim Sistemi

BM : Birleşmiş Milletler

BMKP : Birleşmiş Milletler Kalkınma Programı

BT : Bilişim Teknolojileri

BTC : Bakü- Tiflis-Ceyhan

CBDDO : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

CCDCOE :NATO Cooperative Cyber Defence Centre of Excellence
Siber Savunma Mükemmeliyet Merkezi

CEO : Chief Executive Officer
(Baş Yönetici)

CERT/ CSIRT/CIRT: Ulusal Siber Olay Müdahale Ekipleri

CIA : Central Intelligence Agency USA- ABD Merkezi İstihbarat Teşkilatı

CIS : İnternet Güvenlik Merkezi

CSIS : The Center for Strategic and International Studies-USA
(Stratejik ve Uluslararası Çalışmalar Merkezi-ABD)

DCS : Distributed Control Systems-Dağıtık Kontrol Sistemleri

DOE-USA : Department of Energy Unated States of America-ABD Enerji Bakanlığı

DOS : Denial of Service-Hizmet Reddi

DDOS : Distributed Denial of Service - Dağıtılmış Hizmet Reddi

DHS : Department of Homeland Security - İç Güvenlik Bakanlığı-ABD

DMZ : Demilitarized Zone - Güvenli bölge

EKS : Endüstriyel Kontrol Sistemleri

ENISA : Avrupa Ağ ve Bilgi Güvenliği Ajansı

ESCSWG : UK Emergency Services Collaboration Working Group
(İngiltere Acil Servisler İşbirliği Çalışma Grubu)

EU : Europe Union-Avrupa Birliği

FEMA : ABD Federal Acil Durum Yönetim Ajansı

FIRST : Uluslararası Siber Olay Müdahale ve Güvenlik Ekipleri Forumu

G/Ç : Giriş/Çıkış

GPS : Global Positioning System - Küresel Konumlama Sistemi

HMI : Human Machine Interface - Kullanıcı Arayüzü

ICANN : Internet Corporation for Assigned Names and Numbers
Internet Alan Adlari ve Numaralari Atama Şirketi

ICRC : Uluslararası Kızılhaç Komitesi

ICS-CERTS: Industrial Control Systems-Computer Emergency Teams

(Endüstriyel Kontrol Sistemleri Bilgisayar Acil Durum Ekipleri)

IDS : Intrution Detection Systems- Saldırı Tespit Sistemleri

IEC : Uluslararası Elektroteknik Komisyonu

IED : Intelligent Electronical Devices-Akıllı Elektronik Cihazlar

IGF : Internet Governance Forumu- İnternet Yönetişim Forumu

IMF : International Money Fund-Uluslararası Para Fonu

IIOT : Internet of Industrial Things- Endüstriyel Nesnelerin İnterneti

IOT : Internet of Things - Nesnelerin İnternet

IP : Internet Protocol

ISA : International Society of Automation -Uluslararası Otomasyon Topluluğu

ISAC : Information Securıty Access Control-Bilgi Güvenliği Erişim Kontrolu

ISAGCA : Global Cybersecurity Alliance -Küresel Siber Güvenlik Anlaşması

ISO : International Organization for Standardization -Uluslararası Standartlar Örgütü

ITU : International Telecomunication Unit - Uluslararası Telekomünikasyon Kuruluşu

IULA-EMME : Centre for Local Government Training and Development in the Eastern Mediterranean and the Middle East-Doğu Akdeniz ve Ortadoğu Yerel Yönetimler Eğitim ve Kalkınma Merkezi

LAN : Local Area Network-Yerel Alan Ağı

MIT : Massachusetts Teknoloji Enstitüsü

MSDE : Microsoft Data Engine

NATO : Kuzey Atlantik Paktı

NERC : North America Electric Reliability Concuil - Kuzey Amerika Elektrik Güvenilirlik Konseyi

NIST : National Institute Standarts and Technolgy - Ulusal Standartlar ve Teknoloji Enstitüsü-ABD

NIST SP : NIST - Special Publications- NIST Özel Yayınları

NSA : National Security Agency- ABD Ulusal Güvenlik Ajansı

OECD : Organisation for Economic Co-operation and Development - Ekonomik İşbirliği ve Kalkınma Örgütü

OT : Operasyonel Teknolojiler

PCCIP : President's Commission on Critical Infrastructure Protection - ABD Kritik Altyapıların Korunması için Başkanlık Komisyonu

PCS : Process Control Systems-Süreç Kontrol Sistemleri

PDD : Presidential Decision Directives- ABD Başkanlık Karar Yönergesi

PLC : Programmable Logic Controller- Programlanabilir Mantık Birimi

PPD : Presidential Political Directives -ABD Başkanlık Politika Direktifi

RTU : Remote Terminal Unit - Uzak Terminal Birimi

SCADA : Supervisory Control and Data Acquision-Merkezi Kontrol ve Veri Toplama

SGYS : Siber Güvenlik Yönetim Sistemi

SNMP : Simple Network Management Protocol-Basit Ağ Yönetim Protokolü

SOME : Siber Olaylara Müdahale Ekibi

SSL : Solid State Disk / Katı Hal Sürücüsü

STK : Sivil Toplum Kuruluşları

ŞİÖ : Şanghay İşbirliği Örgütü

T.C. : Türkiye Cumhuriyeti

T-CY : Avrupa Konseyi Siber Suç Sözleşmesi Konseyi

TCP : Transmission Control Protocol – Gönderi Kontrol Protokolü

TLS **:** Transport Layer Security / Taşıma Katmanı Güvenliği

UAB : Ulaştırma ve Altyapı Bakanlığı

UDHB : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

UDP : User DataGram Protocol- Kullanıcı Veri Bloğu Protokolü

UK : United Kingdom-İngiltere

UN : The United Nations- BM

USB : Universal Serial Bus - Evrensel Seri Veriyolu

WEF : Dünya Ekonomik Forumu

VPN : Virtual Private Network-Sanal Özel Ağ

WAN :Wide Area Network-Genş Alan Ağı

WCED : World Commission on Environment and Development-Dünya Çevre ve Kalkınma Komisyonu

TABLOLAR

Tablo 1 **:** Önemli çevre sorunlarına neden olabilecek kritik altyapı sektörleri…..…86

Tablo 2 **:** EKS'nin Gelişim Süreçleri……..90

Tablo 3 **:** EKS ve Geleneksel Bilişim Sistemlerinin Farkları……102

GİRİŞ

Günümüzden yaklaşık 10.000 yıl önce gerçekleştirilen Tarım Devrimi ile insan emeğinin yanısıra hayvan emeğinden de yararlanılmaya başlanmış; 18. yüzyılın ikinci yarısından itibaren ise Birinci Sanayi Devrimi ile kas kuvvetinden mekanik kuvvete geçiş sağlanmıştır. 1760 ve 1840 yılları arasını kapsayan bu dönemde demiryollarının inşası ve buhar makinesinin kullanıma girmesi ile mekanik üretim başlatılmıştır. On dokuzuncu yüzyıl sonları ile yirminci yüzyıl başlarında hızlanan İkinci Sanayi Devrimi ise elektriğin ve montaj hattının sağladığı destekle seri üretimin gerçekleştirildiği bir dönem olmuştur (Kumar, 1995:21). Bu dönem, 1913'te Henry Ford tarafından otomobiller için otomasyon montaj hatlarının başlamasıyla sembolize edilmektedir (Stückelberger,2018:29) Birinci Sanayi Devrimi buhar gücüne dayalı mekanik üretime geçişi; İkinci Sanayi Devrimi ise elektriğe dayalı montaj hatlarının kullanıldığı seri üretime geçişi anlatmak üzere kullanılmaktadır.

Amerikan ordusu için geliştirilen dünyanın ilk elektronik dijital bilgisayarının üretilmesini takiben yarı iletkenlerin, 1960'larda ana bilgisayarların, 1970'ler ve 1980'lerde kişisel bilgisayarların, 1990'larda ise İnternetin keşfi ile Bilişim Devrimi, Enformasyon Devrimi, Dijital Devrim olarak da adlandırılan dönem Üçüncü Sanayi Devrimi olarak anılmaktadır (Schwab, 2016, s:15-16). Üçüncü Sanayi Devrimi, geçmişte sadece insan beyni tarafından gerçekleştirilebilmekte olan bir takım faaliyetlerin, bilgisayarlar tarafından otomatik olarak yerine getirilebilir hale gelmesi ile gerçek anlamda başlamıştır (Kumar, 1995:21). Bilgisayar ve iletişim teknolojilerindeki gelişmeler, 1960'lardan itibaren bilgi ve iletişimin yaratılması, yönetilmesi ve kullanılması dünyayı derinlemesine, geri dönülemez biçimde çok hızlı bir şekilde değiştirmiş; hayatın her alanına girmiş, yaşam şekillerini değiştirmiş ve toplumsal alanda önemli dönüşümler yaratmaya başlamıştır.

Üçüncü Sanayi Devrimi ile birlikte sıklıkla kullanılır duruma gelen bilişim teknolojileri deyimi bir metafor, bir slogan olup topluluk ya da bireysel bilgi sistemleri gibi bilgilendirme durumlarının yanı sıra, yazılım uygulamaları ve donanımı da anlatmaktadır. Bilişim teknolojileri evlerde, eğitim kurumlarında, sağlık kurumlarında, kamusal alanlarda, yargıda, özel sektör kuruluşlarında hemen hemen her yerde güncel bilişim uygulamaları şeklinde kullanılmaktadır (Skovira, 2003:170). Üçüncü Sanayi Devrimi döneminde gerçekleştirilen teknolojik yeniliklerle birlikte, süreklilik arz eden değerler yerine modern elektronik ve bilişim sistemlerinde kullanılan ikili kod benzeri on/off durumunu gösteren sayısal (dijital) sistemler pekçok alanda kullanılmaya başlanmıştır (Cavelty, 2008:15). Günümüzde sayısal teknolojiler, bilgisayarlar dışında da hızlı bir şekilde gelişmektedir. Karmaşık elektronik devreler her geçen yıl daha da küçülürken verimlilikleri de hızla artmaktadır. Kullanmakta olduğumuz pek çok hizmet artık birbirlerine ağlarla bağlı bilgisayarlar ve sayısal teknolojiler olmadan verilemez hale gelmiştir. Kara, deniz, hava taşıtları, bankalar, mağazalar, hastaneler, elektrik üretim ve dağıtım sistemleri, petrol ve doğalgaz dağıtım hatları, nükleer santraller,barajlar, su ve kanalizasyon sistemleri, coğrafi bilgi sistemleri, ev eşyaları vb. pekçok alanda sayısal teknolojiler içeren mikroişlemciler kullanılmaktadır.

1970'li yıllarla birlikte başlayan bu dönemi; Harward'ın, IBM destekli Bilim ve Teknoloji Programı 1971'de Teknolojik Toplum; Peter Drucker Bilgi Toplumu; Brezinski Teknokratik Çağ; Bell ise Sanayi Sonrası Toplum diye adlandırmıştır. (Witheford, 2004:27-28). Bilgi toplumunda bilişim teknolojileri ve iletişim alanındaki teknolojik gelişmeler sayesinde üretimin temel bileşeni bilgi olmaya başlamıştır. Sanayi toplumu mal üretimine dayanırken bilgi toplumu da bilgiye dayanmaktadır. Bilişim teknolojileri ile insan müdahalesine gerek kalmadan bilginin otomatik olarak değiştirilmesi, dönüştürülmesi, iletilmesi, saklanması gibi işlemler çok kolaylıkla gerçekleştirilmeye başlanmıştır.

Bilişim teknolojilerinde baş döndürücü bir hızla devam etmekte olan gelişmeler bazı kesimler tarafından Üçüncü Sanayi Devrimi kapsamı içinde düşünülse de, Schwab tarafından içinde yaşadığımız bu dönem, birbiri ile bağlantılı, çok yönlü, yeni teknolojilerin önünü çok hızlı bir şekilde açması; ekonomide, iş dünyasında, toplumda ve bireylerde paradigma değişimlerine götürecek çok çeşitli teknolojileri bir araya getirecek genişlik ve

derinliğe sahip olması; ülkeler, şirketler ve sektörler arasında ve içinde sistemlerin bütünsel dönüşümünü içermesi gibi nedenler ile Dördüncü Sanayi Devriminin başlamış olduğu şeklinde yorumlanmaktadır (Schwab,2016:11). Bu dönemde, ev aletleri, bina ısı sistemleri gibi küçük ölçekli altyapılardan, enerji üretim, iletim, dağıtım şebekeleri, nükleer santraller, barajlar, su ve kanalizasyon sistemleri, kimya tesisleri gibi büyük ölçekli altyapılara kadar pekçok fiziki sistemin bilgi ve iletişim teknolojileri ile entegre edildiği siber fiziki sistemlerin kurulumu ve kullanımı hızlı bir şekilde yaygınlaşmaya başlamıştır. Fiziksel dünyadaki ısı, nem, duman, gaz, hareket, basınç gibi bir takım değerleri algılamak ve sayısal değerlere dönüştürmekte kullanılan sensörlerde ve fiziksel dünyadaki nesnelerin sanal ağlara bağlantısında kullanılan araçlarda yaşanmakta olan çok hızlı gelişmeler sonucu akıllı evler, akıllı şehirler, akıllı enerji iletim ve dağıtım şebekeleri tesis edilerek günlük hayatın vazgeçilmezleri arasına girmektedir.

Kizza, teknolojik yönden gelişmiş bir topluma katkıda bulunan faktörler arasında, yüksek oranda sayısallaşmış bilgi ve artan bant genişliğini, bilgi ve iletişim cihazlarının boyutlarının küçülmesini ve sayısal iletişimin, özellikle internetin potansiyel zararları hakkında daha fazla farkındalığı saymaktadır (Kizza, 2007:100). Bilgi toplumu, tüm dünya üzerinde kişisel bağlantıların olduğu kadar ticari ilişkilerin, devlet alanlarının küresel bağlantılarını açıklamak üzere de kullanılan bir terimdir. (Friedman, 2000:50) Bu dönemin en temel sözcükleri bilgi, siber ve sayısal sözcükleri olmuştur.

Geçmişte mekan ya da zamanla sınırlı olan toplum yapıları, bilgi ve iletişim teknolojilerinin bir arada kullanılması, özellikle internetin devreye girmesi ile önemli değişikliklere uğramaya başlamıştır. Bu teknolojilerin kullanılması ile herhangi bir yere gitmeye gerek kalmadan, ilke olarak dileyen herkese istediği yerde, istediği anda istediği bilgi sağlanabilmektedir. Bilişim teknolojileri iş yapma ve yönetme şekillerini ve işin gerçekleştirilme hızını da değiştirmiş; fiziki mekana bağlı olmaksızın dünyanın çok farklı bir bölgesinden bir iş istenilen zaman aralığında gerçekleştirilebilir hale gelmiştir. Üretimi artıran, ürünün yaşam döngüsünü kısaltan ve mesafelerin önemini azaltan bilişim teknolojileri pazarı ve ekonomiyi küreselleştirmiştir (Azari, 2003:vii).

1980'li yıllardan itibaren bilgi ve iletişim teknolojilerindeki hızlı gelişme sonucu küreselleşme hız kazanmış; devletler ve teknoloji çok hızlı bir şekilde bütünleşmeye

başlamıştır (Friedman,1999:30-33). Schultz, teknolojik gelişmenin kaçınılmaz, durdurulamaz olup büyük oranda faydalı olduğunu, teknolojik gelişmenin diğer etkenlerden daha öncelikli olması gerektiğini savunmuştur.(Schultz 2006, Ch.11:165). Küreselleşme ile birlikte dünya üzerindeki ekonomiler ve kültürler, bilgi teknolojileri ve ulaşım teknolojilerindeki gelişmeler sayesinde bütünleşmiştir. Bilgi ve iletişimin küreselleşmesi şimdiye kadar üzerinde düşünülmemiş yeni olanakları da gündeme getirmeye devam etmektedir (Kumar, 1995:195).

Bilişim teknolojilerinde önemli değişikliklerin yaşandığı, Üçüncü Sanayi Devrimi ya da Enformasyon Devrimi gibi adlarla anılan 1970'li yıllardan itibaren, insanların içinde yaşadıkları çevrenin önemi ve çevreye verilen zararlar da farkedilmeye başlanmıştır. İnsanın dünya sahnesine çıkmasından itibaren; özellikle Sanayi Devrimi döneminde doğanın tükenmez bir kaynak olarak görülmesi ile tüm dünya üzerinde geri döndürülemez şekilde çevre sorunları yaşanmaya başlanmış; doğanın kötü kullanılması neticesinde önemli çevre sorunları oluşmaya başlamış ve konu tüm dünya devletlerinin gündeminde yerini almaya başlamıştır. Bu dönemden itibaren çevre sorunlarının giderilmesine yönelik alınacak önlemleri belirleme kapsamında, insanların birbirlerine, diğer canlılara ve çevreye karşı davranışlarını, ahlaki sorumluluklarını konu edinen ve uygulamalı etiğin bir alt alanı olan Çevre Etiği kavramı kullanılmaya başlanmış; bu alanda yayınlar yapılmaya ve çözüm yolları aranmaya başlanmıştır.

Bilişim teknolojilerinin çok hızlı bir şekilde tüm dünyada her alanda kullanılıyor olması ile siyasi, ekonomik, hukuki boyutları olan bilgi toplumundan da sıklıkla bahsedilmeye başlanmıştır. Bilginin temel kabul edildiği Üçüncü Sanayi Devrimi ve sonrasında Dördüncü Sanayi Devrimi ile gelişmiş sensörlerin kullanıma sunulması sonucu fiziki dünya paralelinde oluşturulan ve her şeyin sayısallaştığı siber fiziki dünyanın hayatımızda önemli yer tuttuğu iyice belirginleşmiştir. Bilgi toplumu olarak adlandırılan ve insanların ve varlıkların küresel seviyede birbirlerine ağlarla bağlı bir şekilde hayatlarını sürdürdüğü günümüz dünyasında, bu teknolojilerin yararlı kullanımı yanında pekçok yüksek dereceli riskler de oluşmaya başlamıştır. Dünya üzerindeki varlıkların birbirlerine ağlarla bağlanması ile hızlı bir şekilde gelişen siber uzayın tüm canlılar için ve çevre için ne tür sorunlar oluşturabileceği henüz tam olarak bilinmemektedir. Ancak, insan eli ile

oluşturulan bir ortam olması dolayısı ile siber uzaydan kaynaklanabilecek sorunların insanın çevreye karşı sorumluluğu kapsamında ele alınması gerekmektedir.

Teknolojik yenilikler o kadar hızlı olmaktadır ki bu yeniliklerin toplumda yaratacağı etkileri tahmin etmek de gittikçe zorlaşmaktadır. İnsanların teknolojiye bağımlılıklarının her geçen gün artmasından dolayı teknolojinin kontrolden çıkması ve zafiyetlerden kaynaklanan tehditler sıklıkla kullanılan konular haline gelmiştir. Bilgi ve iletişim teknolojilerine hızlı bir şekilde artan bağımlılık sonucu insanların bu sistemleri anlama ve riskleri kontrol altına alma kapasiteleri yetersiz kalmaktadır (Cavelty, 2008:13)

Bilgi toplumu olarak adlandırılmakta olan günümüz dünyası, Ulrick Beck tarafından ise risk toplumu olarak adlandırılmaktadır. Teknolojik gelişmeler sonucu hayatımıza giren pek çok yeniliğin canlılar için ve çevre için ne tür sorunlar doğurabileceği, hemen anlaşılamamakta, çok uzun yıllar sonra ortaya çıkabilmektedir. Modern toplumlar, belirsizlikleri öngörebildikleri tehditlere yönelik önlemlerle kontrol altına alabilmektedir. Bu nedenle felaket öngörüsünü "risk" olarak tanımlamaktadır (Beck, 2011:357). Ona göre insanlığı tehdit eden tehlikeler, neyi bilmediğimizi bilmemekten doğmaktadır (Beck, 2011:355-356). Öngörülebilmekte olan felaketlerin önlenebilmesi ya da felaket sonrası oluşabileceği öngörülen sorunların en aza indirgenebilmesi için bazı faaliyetler gerçekleştirilmelidir. Küresel risk algılamalarının üç ayırdedici özelliği mahalsizleşme, hesaplanamazlık ve telafi edilemezliktir. Bir riskin sebepleri ve sonuçlarının tek bir coğrafi alan ya da mekanla sınırlı olmaması, prensipte her yerde etkili olması mahalsizleşme özelliğidir. Bu riskler ulus devlet sınırları ya da başka bir fiziki sınır tanımaz. Riskin sonuçlarının prensip olarak en temelde hipotez düzeyinde olması, bilmeme ve normatif görüş ayrılığına dayanması hesaplanamazlık özelliğidir. Riskin gecikme süresi uzun olduğu için zaman içindeki etkileri güvenilir bir şekilde belirlenemez ve sınırlanamaz. Riskin meydana gelmesi sonrasında telafi mantığı çöker ve yerini önleme yoluyla sakınma ilkesi alır. Varlığı kanıtlanamayan riskler öngörülüp önlenmeye çalışılmaktadır. Problemlerin karmaşıklığı ve etki zincirlerinin çok uzun olmasından dolayı, sebepler ve sonuçların güvenilir bir şekilde saptanması imkansızdır (Beck, 2011,:357-358). Bilişim teknolojilerine yönelik siber güvenlik olaylarında da riskin nedenleri ve sonuçları tek bir coğrafi alanla sınırlı olmayacaktır ve her yerde etkili olacağı için mahalsizdir. Ulus devlet sınırları ya da

başka bir fiziki sınır geçersizdir. Riskin sonuçları tam olarak hesaplanamaz ve zaman içinde oluşturacağı etkiler güvenilir bir şekilde belirlenemez ve sınırlanamaz. Beck'in tanımlamalarına uygun olarak siber güvenlik önlemleri için de risk yönetimi yöntemi uygulanmaya başlanmıştır.

Dördüncü Sanayi Devrimi ile, güvenlik tehditlerinin karakterinin değişmekte olduğu ve aynı zamanda coğrafi aktörlerden ve devletlerden devlet dışı aktörlere doğru güç kaymalarının yaşandığı ve devlet dışı silahlı aktörlerin arttığı gözlemlenmektedir.(Schwab, 2016:91). Yeni ölümcül teknolojilerin edinilmesi ve bu teknolojilerin kullanımı gittikçe daha kolaylaştığı için bireyler, başkalarına daha ciddi zarar verebilecek duruma gelebilmektedir (Schwab, 2016:94). Özellikle 2000'li yılların başlarından itibaren sayısal sistemlerin ve iletişim ağlarının enerji, ulaşım, iletişim gibi çok değişik sektörlerde aynı cihazlar üzerinden birlikte kullanılmaya başlanması ile güvenlik tehditleri tek fiziki alanla sınırlı kalmamaya başlamıştır. Artık saldırganlar sadece devletlerle sınırlı kalmadığı için güvenlik kavramı da değişikliğe uğramaya başlamıştır.

Geleneksel savaş alanları olan kara, deniz, hava ortamlarına ek olarak siber uzay da gündeme gelmiştir. Savaş ve barış zamanları iç içe geçmiştir. Askeri sistemlerin yanısıra sağlık ya da trafik kontrolleri, sivil enerji kaynakları, elektrik ve su şebekeleri gibi herhangi bir ağ ya da bağlantılı cihazlara yönelik siber saldırılar düzenlenebilecektir (Schwab, 2016:95). Teknolojik yeniliklerin olumlu kullanımının yanı sıra kötü niyetli kişilerin eline geçmeleri durumunda insanlar, toplumlar, diğer canlı ve cansız varlıkların oluşturduğu çevre için yıkıcı etkileri de göz ardı edilmemelidir. Teknoloji, sadece devletler ve çok ileri kuruluşlar tarafından değil tüm bireyler tarafından da kullanılabilecek şekilde yaygınlaştığından dolayı mevcut yasal ve ahlaki çerçeveler yetersiz kalmıştır.

2016 yılında Almanya'nın Hanover şehrinde gerçekleşen dünyanın en kapsamlı teknoloji fuarlarından CeBIT'in partner ülkesi olan Japonya'nın başbakanı Shinzo Abe, Fuarda *"Teknoloji toplumlar tarafından bir tehdit olarak değil, bir yardımcı olarak algılanmalı."* inancıyla temellendirilen **Toplum 5.0 (Society 5.0)** felsefesini tanıtmıştır. Japon Ekonomik Organizasyonlar Federasyonu Keidanren (Keidanren,2016), **Toplum 5.0** felsefesi ışığında gelişmesi beklenen ekonomi ve sosyoloji reformunu geniş kitlelere anlatmak üzere hazırlanan "Yeni Ekonomi ve Toplumun Gerçekleştirimi" başlıklı

dokümanda içinde bulunulan dönem, (Toplum 5.0) olarak tanımlanmış ve hedefleri arasında sanal dünya ile gerçek dünyanın beraber işler hale getirilmesi, Nesnelerin internetinden toplumun çıkarları gözetilerek faydalanılması, çevre kirliliği ve doğal afetler için çözüm yolları üretilmesini de saymıştır. Bilişim teknolojilerinin küresel seviyede kullanılması nedeni ile "Dünya çapında" toplumsal bir dönüşüm gerektiğini ve hukuk sistemindeki eksiklikler, nesnelerin dijitalleşmesindeki bilimsel boşluklar, nitelikli personel eksikliği, sosyo-politik önyargıları ve toplumsal direnci önemli eksiklikler arasında saymıştır. Keidanren, bu bariyerlerin yıkılması ve **Toplum 5.0**'ın yoluna devam edebilmesi için toplumların iş birliği içinde olması gerektiğini vurgulamaktadır. İçinde bulunduğumuz teknolojik çağın belirsizliklerle dolu olmasından dolayı; endüstri alanının dünyaya liderlik edebilmek için kendi inisiyatifi ile reformlar oluşturması gerektiği belirtilmektedir. Bu önerilerin ekonomi ve toplum reformu için başlangıç noktası olduğu kişisel konuları da kapsayacak şekilde daha fazla derinleştirilerek yaygınlaştırılması gerektiğinin altı çizilmektedir.

Yirminci yüzyılın son dönemlerinden itibaren üçüncü sanayi devrimi ve dördüncü sanayi devrimi ile daha önce görülmemiş bir hızla, çok kısa bir zaman dilimi içinde bilgi ve iletişim teknolojilerindeki gelişmeler sonucu toplumlar bilgi toplumuna dönüşmüş; yine görülmemiş bir hızla küreselleşme başlamış; teknolojiyi ileri seviyelerde uygulamakta olan Japonya gibi ülkeler artık bilgi toplumu dönemini de geride bırakmış ve Toplum 5.0'dan söz etmeye başlamıştır. Yazılım, donanım ve ağ bileşenlerinden oluşan bilişim teknolojileri, siber uzay üzerinden bireyleri, toplumları, devletleri de birbirlerine bağlı hale getirmişlerdir. Siber uzay üzerinde salt bilginin tutulduğu, işlendiği, iletildiği sistemler geleneksel bilişim sistemleri olarak adlandırılmaktadır. Fiziki dünya üzerinden algıladığı bir takım verileri ve kendi üzerinde yer alan verileri ve programları kullanarak belli faaliyetleri otomatikleştiren sistemler ise siber-fiziki sistemler ya da endüstriyel kontrol sistemleri olarak adlandırılmaktadır. Pek çok alanda hayatı kolaylaştıran ve vazgeçilmez duruma gelen bilişim teknolojileri, Ulrick Beck tarafından risk toplumu olarak adlandırılan günümüz dünyasında sonucunu kestiremediğimiz güvenlik olaylarına da neden olabilecek mahiyettedir.

Sivil, askeri, siyasi, ekonomik, hukuki her türlü işlemin gerçekleştirildiği siber uzayın sürdürülebilirliğinin sağlanması çok önemlidir. Ancak insanların ve diğer canlıların

varlıklarını sürdürebilmeleri için, birinci öncelikli husus içinde yaşadığımız ekosistemin güvenliğinin sağlanması, buna yönelik risklere karşı önlemlerin alınmasıdır.

Fiziki dünyada yer alan ulus devlet sınırlarının siber uzayda geçersiz kalması, siber saldırıların zaman ve mekan sınırlaması olmaksızın istenilen zamanda istenilen mesafeden gerçekleştirilebilir olması ve kim ya da hangi gruplar tarafından gerçekleştirildiğinin tam olarak tespit edilememesi gibi nedenlerle şimdiye kadar zihinlerde yer eden güvenlik önlemlerine yönelik algılarda da önemli değişiklikler oluşmaya başlamıştır. İnsanların ve diğer varlıkların dünya üzerindeki mevcudiyetini yok edebilecek ya da gelecek nesillerin de en az bugün sahip olunan kaynaklarla hayatını sürdürebilmesini engelleyecek nitelikteki siber güvenlik olaylarının engellenmesine yönelik çözüm arayışları tüm dünyanın gündeminde önemli yer tutmaktadır.

Tezin Konusu

Siber güvenliğin çevre etiği açısından incelenerek siber güvenlik olaylarının çevre etiği bağlamında ne tür sorunlara yol açabileceğinin araştırılması, çevresel sürdürülebilirliği engelleyecek nitelikteki siber güvenlik olaylarını önlemek ya da bu tür olayların meydana gelmesi durumunda hasarı azaltarak sistemlerin siber olay öncesi durumuna dönmesi için bireysel, kurumsal, ulusal ve küresel seviyede nasıl bir siber güvenlik yönetiminin gerçekleştirilmekte olduğunun araştırılmasını kapsamaktadır.

Tezin Amacı

Bilişim teknolojilerinin yoğun olarak kullanılmakta olduğu ve içinde yaşadığımız fiziki dünyaya paralel olarak geliştirilmiş siber uzayda meydana gelebilecek siber güvenlik olaylarının çevre etiği açısından incelenmesi ve dünya üzerindeki varlıkların sürdürülebilirliğini sağlamak için nasıl bir siber güvenlik yönetimi uygulanması gerektiği sorularına yanıt aramaktır.

Tezin Önemi

Hazırlık aşamasında yapılan literatür taramasında, siber güvenliğin etik açısından ele alındığı birtakım çalışmalar görülmüş ancak siber güvenliğin çevre etiği bağlamında ele alındığı çalışmaların çok az olduğu görülmüştür. Ülkemizde ise bu alanda yapılmış bir çalışmaya rastlanmamıştır. Siber güvenliğin sadece geleneksel bilişim sistemlerinin değil

operasyonel teknolojilerin ve bilişim teknolojilerinin bir arada kullanılmakta olduğu kritik altyapı sistemlerinin sürdürülebilirliğinin de ele alındığı bu çalışma farklı disiplinleri bir araya getirmesi açısından önem arz etmektedir. Siber güvenliğin çevre etiği bağlamında ele alındığı bu çalışmanın etik, siber güvenlik ve afet acil durum yönetimi, uluslararası ilişkiler gibi farklı alanlarda politika üretmeye çalışanlara, yeni bir bakış açısı kazandırabileceği değerlendirilmektedir.

Varsayımlar

- Canlı varlıkların yaşamının sürdürülebilmesi için içinde yaşadığımız ekosistemin yani fiziki dünyanın yaşamaya uygun bir şekilde varlığının devam ettirilmesi gerekmektedir.
- İçinde yaşamakta olduğumuz fiziki dünya üzerinde, insanlar tarafından geliştirilen, işletilen ve kullanılmakta olan paralel bir siber uzay bulunmaktadır.
- Siber uzay içinde bilişim teknolojilerini barındıran yazılım, donanım, ağ ürünlerinin yanı sıra, bu sistemleri geliştirenler, işletenler, bireysel kullanıcılar, kurumsal yapılar, devletler, uluslararası kuruluşlar, çok uluslu şirketler vb. yer almaktadır.
- Siber uzay üzerinde, devletlerin fiziki dünya üzerindeki sınırları gibi bir sınır yer almamaktadır ve küresel bir sistemdir.
- Teknolojinin gelişimine ve insanların yaratıcılığına bağlı olarak siber saldırı araçları ve siber aktörlerde sürekli yeni türler ortaya çıkmaktadır. Buna paralel olarak siber saldırılara karşı geliştirilmekte olan siber savunma araçları ve yöntemleri de sürekli gelişmektedir.
- Çevre etiğinin pragmatik yaklaşımlarından olan "sürdürülebilir kalkınma" kavramı günlük hayatta ekonomik, sosyal ve çevresel pekçok farklı alanda sıklıkla dile getirilmektedir. Bu çalışma kapsamında ise sadece çevresel sürdürülebilirliği ifade etmek üzere kullanılmıştır.

Araştırma Problemi, Yanıt Aranan Sorular ve Yöntemi

Günümüz küresel dünyasında bilişim teknolojileri çok farklı sektörlerde yaygın olarak kullanılmaya başlanmıştır. Bu teknolojiler ve siber uzay canlı-cansız tüm varlıkların sürdürülebilirliğini sağlamak üzere kullanılabildiği gibi kötü niyetli kişilerin ya da grupların

eline geçmesi durumunda, kasıt olmaksızın kaza eseri hatalı çalışması durumunda ya da deprem, yangın, sel, fırtına gibi doğal afetler nedeni ile canlı, cansız tüm varlıkların sürdürülebilirliğini engelleyebilecek siber güvenlik olaylarına da maruz kalınabilmektedir.

Tez çalışması kapsamında cevabı araştırılan temel soru, çevresel sürdürülebilirliği engelleyebilecek nitelikteki siber güvenlik olaylarına yönelik nasıl bir siber güvenlik yönetiminin uygulanması gerektiğidir.

Bu temel soru çerçevesinde yanıt aranan alt sorular ise aşağıda yer almaktadır:

- Güvenlik kavramında ne tür değişiklikler olmuştur, siber güvenliğin ve çevresel güvenliğin güvenlik kavramına eklemlenişi nasıl olmuştur?
- Çevre etiği bağlamında, hangi yaklaşımlar ve ideolojiler bulunmaktadır?
- Hangi tür siber güvenlik olayları, insanların ve diğer canlıların varlıklarını sürdürebilmeleri için gerekli olan ekosistemin sürdürülebilirliğine zarar verebilecek niteliktedir?
- Siber güvenlik olaylarının, çevresel sürdürülebilirliği önleme riski var mıdır?
- Yakın dönemde çevre merkezli çevre etiği bağlamında sürdürülebilirliği engelleyen ya da engelleme olasılığı yüksek siber güvenlik olayları gerçekleşmiş midir?
- Kritik altyapılara yönelik siber güvenlik tehditleri ve siber güvenlik açıkları nelerdir?
- Çevre etiği bağlamında siber güvenliği sağlamak üzere uygulanmakta olan operasyonel ve stratejik faaliyetler nelerdir?
- Sınır aşan çevresel sorunlara neden olabilecek siber güvenliğin küresel seviyede yönetilmesinde yönetişim mekanizmasını kullanılmakta mıdır?

Yöntem

Tez konusunun araştırılmasında felsefenin eleştirel düşünme ve tümevarım yöntemi kullanılmıştır.

Başlangıçta, kritik altyapıların siber güvenliğinin fiziki çevreye etkisi hususunda bireysel, kurumsal ve ulusal seviyedeki algıyı saptayabilmek için bir takım nicel araştırma yöntemlerinin uygulanması planlanmıştır. Ancak, tezin hazırlanması döneminde küresel

seviyede yaşadığımız Pandemi nedeni ile planlanan çalışma gerçekleştirilememiştir. Ağırlıklı olarak konunun felsefi yönü ön planda tutularak diğer tekniklerin uygulama imkansızlığı nedeniyle nitel araştırma doküman incelemesi yöntemi ile yapılmıştır. Bu kapsamda, güvenlik, bilişim teknolojileri, uluslararası ilişkiler, felsefenin alt alanlarından etik, uygulamalı etik türlerinden çevre etiği literatürü taranmış, ulusal ve uluslararası dokümanlar, raporlar, strateji ve politika belgeleri incelenmiştir. Belirtilen alanlar kapsamında yakın dönemde yayımlanmış kitaplar, makaleler, standartlar, kılavuzlar gibi dokümanlara erişilmiştir. Kaynak erişiminde yoğun olarak internetten faydalanılmıştır.

Sınırlılıklar

- Çalışma, çevre etiği ve siber güvenliğe ilişkin gelişmelerin başlangıcı olarak kabul edildiği için 1970'den günümüze kadar olan dönemi kapsamaktadır.
- Siber uzayda yer alan bilişim teknolojilerinin üretilmeleri ve kullanımları aşamasında ekosistem üzerinde oluşturdukları karbon ayak izleri kapsama alanı dışında bırakılmıştır.
- Bilişim teknolojilerinin hayatın her alanında kullanılır durumda olması nedeni ile siber güvenliğin siyasi, askeri, ekonomik, hukuki ve etik boyutları bulunmaktadır. Bu çalışmada, siber güvenliğe ilişkin genel bilgilere yer verilmekle birlikte, temel sorun siber güvenliğin fiziksel çevre üzerindeki olumsuz etkilerini araştırmak olduğu için, üzerinde sadece bilginin tutulduğu işletildiği iletildiği geleneksel bilişim sistemlerinin değil, bilişim teknolojileri ve operasyonel teknolojilerin birlikte kullanıldığı endüstriyel kontrol sistemlerinin yardımı ile faaliyetlerini sürdürmekte olan kritik altyapıların siber güvenliği, çevre etiği açışından ele alınmıştır.
- Geleneksel bilişim teknolojileri kullanılarak kritik bilgilerin tutulduğu, işlendiği, iletildiği bankacılık, finans, e-ticaret, sağlık sektörü gibi kritik sektörlerden çok, geleneksel bilişim sistemlerinin yanısıra endüstriyel kontrol sistemlerinin de kullanıldığı, bir siber olay sonrasında fiziki hasar görebilecek ve çevre sorunlarına yol açabilecek olan petrol ve doğal gaz tesisleri, nükleer enerji santralleri, barajlar, elektrik üretim ve dağıtım sistemleri, su ve kanalizasyon sistemleri, kimyasal tesisler gibi kritik altyapıların siber güvenliği temel alınmıştır.

- Siber güvenliğin pek çok alanında kişilerin etik davranışlar sergilemesini gerektiren ikilemli durumlar mevcuttur. Bu çalışmada sadece çevre etiği açısından oluşabilecek sorunlar ele alınmıştır.
- Çevre etiği açısından siber güvenlik ele alınırken küresel seviyede çıkarlar göz önünde bulundurulmuş; ulusal güvenliğe yönelik sorunlar ile son dönemde daha sıklıkla gündeme gelmeye başlayan bireysel seviyedeki mahremiyet konusu kapsam dışı bırakılmıştır.
- Etik alanında çok farklı yaklaşımlar var olmasına rağmen bu çalışmada siber güvenliğin çevre etiği açısından oluşturabileceği fiziki hasarlar incelenmiş; bireylerin davranışları erdem etiği, kurumların ve devletlerin tutumları da sonuçta en yüksek iyiyi elde etmek üzere ödevler etiğinin uygulanması çerçevesinde ele alınmıştır.
- Siber güvenlik, tüm dünya için çok önemli ve teknolojiye bağlı olarak hızlı değişen bir kavram olduğu için çalışmanın hazırlanması süreci içinde, siber saldırı türlerinde, siber saldırganların yöntem ve hedeflerinde değişikliklere, incelenen ülkelerin ve uluslararası kuruluşların siber güvenlik stratejilerinde, devletler tarafından ya da uluslararası kuruluşlar tarafından hazırlanan standartlarda ve kılavuzlarda; kimi durumlarda ise kavramların adlandırılmasında değişikliklere tanık olunmuştur.

Tezin Kapsamı ve Bölümleri

Tezde sunulan araştırma sorularına yanıt bulabilmek ve tezin amacına uygun olarak siber güvenlik olaylarının çevre etiği açısından incelenmesi ve dünya üzerindeki varlıkların sürdürülebilirliğini sağlamak için önerilecek yaklaşımı belirlemek üzere;

- Değişen güvenlik anlayışına, siber güvenliğe ve çevre etiğine yönelik genel bilgilere yer verilmiş,
- Hangi sistemlerin kritik altyapılar olarak kabul edildiği açıklanmış; çevre sorunları ile siber güvenliğin ilişkisi kritik altyapıların işlevlerini yerine getirmelerini sağlayan endüstriyel kontrol sistemleri üzerinden kurulmuş ve bu sistemlerin siber güvenliğine yönelik bireysel, kurumsal ve ulusal seviyede gerçekleştirilebilecek önlemler ele alınmış,
- Kritik altyapılara yönelik şimdiye kadar gerçekleştirilmiş siber saldırı örnekleri incelenmiş ve bu saldırılar çevre etiği açısından değerlendirilmiş,

- Çevre sorunlarının giderilmesi ve siber güvenliğin sağlanması faaliyetlerinin kesişim kümesinde yer alan kritik altyapıların siber güvenliğinin sağlanması konusunun bireysel, kurumsal, ulusal ve küresel seviyede nasıl ele alındığı araştırılmıştır.

Giriş Bölümünde, çevre etiği bağlamında siber güvenlik konusuna başlangıç yapmak üzere, antropojen çağında dünya üzerinde varlığının başlaması ile insanın sebep olduğu çevre sorunlarının farkına varılması ve devletlerin gündemine alınması; üçüncü ve dördüncü sanayi devrimleri sonrası günümüz modern toplumlarında yaşanmakta olan bilgi çağı; risk toplumu ve siber güvenlik konularına değinilmiştir.

Birinci Bölümde, çevre etiği bağlamında siber güvenlik konusundaki kavramsal çerçeve kurulmaya başlanmıştır. Günümüz dünyasında güvenlik alanındaki gelişmeler, güvenliğin kavramsallaştırılması ve çevresel güvenlik ile siber güvenliğin güvenlik alanına eklemlenmesine ilişkin genel bilgiler verilmiştir. Uygulamalı etik alanlarından biri olan çevre etiğinin insan merkezli, canlı merkezli ve çevre merkezli yaklaşımları ile ilgili kavramlar açıklanmış; bütüncül çevre etiği kapsamında yeryüzü etiği, derin ekoloji ve toplumsal ekoloji kavramları incelenmiş ve pragmatik yaklaşım olan sürdürülebilirlik kavramı üzerinde durulmuştur. 1980'li yıllardan itibaren hızlı bir şekilde gelişmeye başlayan ve hayatın her alanında kullanılmakta olan bilişim teknolojileri ile birlikte sürekli gündemde olan siber uzay, siber güvenlik, siber güvenlik olayları, siber güvenlik aktörleri gibi kavramlar açıklanmıştır. Bu bölümde siber güvenlik ile çevre etiğinin bağlantısı sürdürülebilirlik üzerinden kurulmuştur.

İkinci Bölümde, siber güvenlik olaylarının, çevresel sürdürülebilirliği önleme riski olup olmadığı sorusuna yanıt aramak amacı ile siber güvenliğin çevre üzerinde fiziki hasar yaratıp yaratmadığı ve bunu önlemek için ne gibi önlemler alınması gerektiği araştırılmıştır. Bir siber güvenlik olayına maruz kalması durumunda çevre üzerinde olumsuz etki oluşturabilecek ve sürdürülebilirliği engelleyebilecek sistemlerin belirli bazı kritik altyapılarda kullanılmakta olan bazı tür Endüstriyel Kontrol Sistemleri (EKS) olduğu görülmüştür. Öncelikle EKS kullanılarak görevlerini yerine getirmekte olan ve bir siber güvenlik olayı sonrası fiziki hasar yolu ile önemli çevre sorunlarına yol açabilecek kritik altyapı sektörleri tanımlanmıştır. Bu sektörlerde kullanılmakta olan ve bir siber güvenlik olayı sonrası görevini yerine getiremeyerek sürdürülebilirliğe engel olabilecek EKS türleri

açıklanmıştır. EKS'ne yönelik tehditler ve güvenlik açıkları ile siber saldırı türleri üzerinde durulmuş; şimdiye kadar gerçekleşmiş bazı siber güvenlik olayı örnekleri listelenerek fiziki çevre üzerinde oluşturdukları ya da oluşturma olasılığı bulunan hasarlara değinilmiştir.

Üçüncü Bölümde, siber güvenlik olaylarının çevresel sürdürülebilirliği engelleyecek boyutta çevre sorunları oluşturma riskini önlemek için nasıl bir siber güvenlik yönetimi uygulanması gerektiği araştırılmaya başlanmıştır. Öncelikle EKS'nin siber güvenliğini sağlamak üzere gerçekleştirilmekte olan faaliyetler, operasyonel ve stratejik faaliyetler şeklinde sınıflandırılmıştır. Operasyonel siber güvenlik faaliyetlerinde yoğun olarak kullanılmakta olan önleyici koruyucu yaklaşım ve risk yönetimi yaklaşımı hakkında genel bilgiler verilmiş; bu yaklaşımlar doğrultusunda gerçekleştirilmekte olan bireysel ve kurumsal seviye siber güvenlik önlemleri ve kontrolleri açıklanmıştır.

Dördüncü Bölümde, EKS'nin siber güvenliğini sağlamak üzere gerçekleştirilmekte olan operasyonel ve stratejik faaliyetler şeklindeki sınıflandırmaya uygun olarak stratejik faaliyetler ele alınmıştır. Bu kapsamda önleyici-koruyucu yaklaşım ve risk yönetimi yaklaşımının yanısıra kullanılabilecek caydırıcı yaklaşım ve kamu siber güvenlik yaklaşımı hakkında genel bilgilere yer verilmiştir. Devletler seviyesinde ve küresel seviyede stratejik siber güvenlik faaliyetleri incelenmiştir. Siber güvenlik faaliyetlerin gerçekleştirilmesinde, devletlerin fiziki sınırlarının geçersiz kaldığı, zaman ve mekandan bağımsız faaliyetlerin yürütülebildiğinden hareketle EKS'nin siber güvenliği için kullanılmakta olan yönetişim kavramı üzerinde durulmuştur. Bu bölümde, devletlerin siber güvenlik faaliyetleri kapsamında Türkiye'de Kritik Altyapıların Siber Güvenliğine Yönelik Politikalara da değinilmiştir.

Sonuç Bölümünde, kritik altyapılara yönelik siber güvenlik olaylarının önemli çevre sorunlarına yol açabileceği ve bu çevre sorunlarını önleyerek sürdürülebilirliği sağlamak üzere, bireysel, kurumsal, ulusal ve küresel seviyede gerçekleşirilmekte olan faaliyetlerin tümünün yapılması gerektiği, ancak bu faaliyetlerin küresel seviyede koordinasyon ve iş birliği gerektirdiği yani bir yönetişim çerçevesi içinde planlanması, uygulanması ve kontrol edilmesi gerektiği sonucuna ulaşılmıştır.

Başka Çalışmalarda Ele Alınabilecek Konular

Bu tez kapsamında ele alınamayan aşağıdaki konular, başka tezlerin, başka makalelerin konusu olarak ele alınmasında fayda vardır:

- Türkiye'de çevre etiği bağlamında siber güvenlik algısının incelenmesi,
- Kritik altyapıların siber güvenliğinin sağlanmasında ulusal çıkarların mı yoksa küresel çıkarların mı daha ön planda olması gerektiğinin araştırılması,
- Sektörel seviyede kritik altyapıların siber güvenliğinin sağlanması için hangi standartların kullanıldığının ve siber güvenlik konusunda gerekli faaliyetlerin gerçekleştirilmesindeki sürdürülebilirliğin incelenmesi,
- Çevre etiği bağlamında siber güvenliğin sağlanmasında Japon Hükümetinin ileri sürdüğü Toplum 5.0 felsefesinin ne şekilde kullanılabileceğinin araştırılması.

BİRİNCİ BÖLÜM

ÇEVRE ETİĞİ ve SİBER GÜVENLİK KAVRAMSAL ÇERÇEVE

Jeolojik dönemlerin sonuncusu olan Antroposen Çağın (insan çağı) en önemli özelliği, insanın yeryüzü sistemlerine hükmetmesi, müdahaleleri ile doğayı değiştirmesi olmuştur. İnsanın doğa üzerindeki faaliyetleri kendisinin de içinde yaşadığı tüm insanların ve diğer canlıların ortak varlığı olan doğaya zarar vermeye başlamış ve tüm canlıların yaşam ortamlarının kirlenmesine ve olumsuz etkilenmesine neden olmuştur. Bu olumsuz etki özellikle Endüstri Devrimi sonrası hızlanmış 1980'li yıllarda başlayan küreselleşme ile had safhaya ulaşmıştır.

1970'li yıllardan itibaren insanların içinde yaşadığı ekosistemde teknolojik gelişmeler ve doğanın kötü kullanılması neticesinde önemli çevre sorunları oluşmaya başlamış ve konu tüm dünya devletlerinin gündeminde yerini almaya başlamıştır. Çevre sorunlarının giderilmesine yönelik alınacak önlemleri belirleme kapsamında, insanların birbirlerine, diğer canlılara ve çevreye karşı davranışlarını konu edinen ve uygulamalı etiğin bir alt alanı olan Çevre Etiği kavramı kullanılmaya başlanmış ve bu alanda yayınlar yapılmaya ve çözüm yolları aranmaya başlanmıştır.

Bilişim teknolojilerinin hızlı bir şekilde gelişmeye başladığı 1970'li yıllardan itibaren bilgi ve iletişim sistemleri insan hayatının her alanında kullanılmaya başlanmış ve Dördüncü Sanayi Devrimi ya da Sanayi 4.0 olarak adlandırılan dönem ile birlikte içinde yaşadığımız fiziki dünya üzerinde insan eli ile geliştirilmiş yeni bir alan olan siber uzay oluşturulmuştur. Her geçen gün artan sayıda yazılım, donanım, ağ ürünü ile siber uzay genişlemeye başlamış ve daha çok insan tarafından kullanılır hale gelmiştir. İnsanların siyasi, ekonomik toplumsal açıdan çok fazla ilişki içinde olduğu küreselleşme olgusunun başlangıcı da bu dönemlere denk gelmektedir. Küreselleşmeyi teknolojik açıdan destekleyen bilişim teknolojilerinin yaygın kullanımı ve tüm dünyadaki sistemlerin birbirlerine ağlarla

bağlanmaya başlaması ile siber uzay daha da genişlemiş ve ulus devletler arasındaki sınırlar pek çok durumda geçersiz hale gelmiştir.

Pek çok önemli olayın başlangıcı sayılabilecek bu yıllar, soğuk savaş döneminin de bittiği yıllardır ve güvenlik kavramında da çok önemli değişimler yaşanmaya başlanmış; Kopenhag okulu tarafından askeri sektöre ek olarak siyasi, ekonomik, toplumsal ve çevresel güvenlik sektörleri de tanımlamıştır. Tezin temel problemi çevre etiği bağlamında siber güvenliğin ne tür etkilermeydana getirdiğini araştırmak olduğu için bu bölümde öncelikle önemli değişikliklere uğrayan güvelik kavramı ele alınacak, daha sonra, çevre etiği ve siber güvenlik kavramları üzerinde durulacaktır.

1.1 GÜVENLİK KAVRAMI

Bireylerin ihtiyaçlarını hiyerarşik bir sıra içinde tanımlayan Maslow, fizyolojik ihtiyaçların hemen sonrasında, sevme, ait olma saygı ve kendini gerçekleştirme gibi çok önemli ihtiyaçların bile öncesinde "güvenlik" ihtiyacına yer vermiştir (Ural, 2013:320).

Tarih öncesi dönemde güvenlik sözcüğü ile, sadece gıda arzı güvenliği ve diğer insanların ya da hayvanların saldırılarına karşı güvenliğin sağlanması ifade edilmekte idi. O dönemde doğal afetler ve hastalıklar güvenlik kavramı içinde sayılmıyordu. Uygarlığın gelişimi ile barınma güvenliği; özel mülkiyetin gelişmesi ile varlıkların güvenliği de güvenlik kavramı kapsamına alınmıştır. (Sadowsky,2003:18). Genel anlamda güvenlik, mülkiyetin yetkisiz erişiminin, kullanımının, değiştirilmesinin, çalınmasının ya da fiziki olarak zarar verilmesinin önlenmesidir (Kizza, 2007:101).

Geleneksel güvenlik anlayışında güvenliğin temel başvuru nesnesi devlettir ve devlete yönelik askeri tehditlere odaklanılmaktadır. Bu yaklaşımda devlet, dünya siyasetinde temel aktör ve güvenliğin sağlayıcısıdır; öncelikli olan ulusal güvenliktir. 1980'lerin sonlarında uluslararası güvenlik ortamındaki köklü değişim sonucunda geleneksel güvenlik anlayışı, devletlerin tek güvenlik aktörü ve askeri tehditlerin ise temel güvenlik sorunu olarak görülmesini eleştirilmeye başlanmış 1987'den itibaren Kopenhag Okulu, Bary Buzan ve Ole Waever'in çalışmalarını yayınlamaya başlamıştır. Kopenhag Okulunda yayımlanan çalışmalarda, nesneleri, insanları, kuruluşları, toplumu ve devleti korumak için önlem alma sürecini ve sonucunu ifade etmek üzere kullanılmakta olan güvenlik kavramı kapsamında

sadece askeri ve siyasi bağlamda değil ekonomik, toplumsal ve çevresel bağlamlarda da geçerli olabilecek koordineli eylemler yer almaya başlamıştır (Adams vd.,2019:119).

Kopenhag Okulu, güvenlik sektörlerini kavramsallaştırmış ve askeri sektöre ek olarak siyasi, ekonomik, toplumsal ve çevresel güvenlik sektörleri de tanımlamıştır (Buzan,vd.,1998:208). 1980'li yılların sonlarından itibaren güvenlik kavramı risk kavramı ile birlikte kullanılmaya başlanmıştır. Geleneksel güvenlik çalışmaları alanlarının çok ötesinde olan çevre, gıda güvenliği gibi olaylar gündeme gelmiştir. Çevre sorunlarındaki artış ve kaynakların azalmaya başlaması, Kopenhag Okulunun söylemlerine uygun olarak güvenlik gündemine dahil edilmiş ve medyada, akademik çevrelerde sıklıkla tartışılmaya başlanmış; devletler de bu sorunlarını gündemlerine almışlardır.

Çevre sorunları arasında sayılmakta olan kaynakların tükenmesi kapsamında enerji güvenliği konusu da yakın zamanlarda güvenlikleştirilen alanlar arasında dikkat çeken konulardan biridir. Enerji güvenliği, enerji arama, geliştirme, üretim, iletim, çevrim, dağıtım, pazarlama ve tüketim ağındaki tesislerin her türlü saldırıya karşı fiziki olarak korunması anlamına gelmektedir (Sevim,2009:93). Enerji, sanayi, ulaşım ve sağlık ile ilgili risk değerlendirme kavramı kritik altyapıların korunması başlığı altında ulusal güvenlik içine girmiştir (Waever, 2008:108).

Nükleer silahların ortaya çıkması ile güvenlik küreselleşmiştir. Günümüzde güvenlik, iki devlet arasındaki sorunlardan çok küresel seviyede ortak sorunlara ya da bölgesel seviyede çok taraflı sorunlara ilişkin olabilmektedir. Bu da temel amacı vatandaşının güvenliğini sağlamak olan modern devletleri tartışmalı hale getirmektedir. Clark, devlet ile güvenlik arasında köklü bir dönüşüm olduğunu, küreselleşmenin güvenlik sorunlarını dışarıdan etkilemenin yanı sıra devletin kendisini de denetlediğini savunmaktadır. O, güvenlik devletinin küreselleşmesini daha dikkate değer bulmaktadır (Clark,2014:219-226).

Kopenhag okulunun özünü oluşturan kavramlardan biri güvenlikleştirme kavramıdır. Kopenhag Okulunun temsilcilerinden Barry Buzan'a göre güvenlikleştirme sürecinde, hayati bir tehdit unsuru belirlenir, bu tehdidin ortadan kaldırılması acil bir durum olarak kabul edilir ve bu tehdidin ortadan kaldırılabilmesi için olağanüstü tedbirlerin alınması gerektiği kabul edilir. Güvenlikleştirilen bir tehdit, bir süre sonra güvenlik alanı dışına

çıkarılabilir yani güvensizleştirilebilir (Bingöl, 2016:21-23). Kopenhag okulunun güvenlik alanında getirdiği güvenlikleştirme kavramı kapsamında, son dönemlerde sadece askeri alanda değil sivil hayatın her alanında da kullanılmakta olan bilişim teknolojilerine yönelik siber güvenlik olgusu da kavramlaştırılmıştır. Siber uzayın yoğun kullanımı ile ülkelerin fiziki sınırları da önemini kaybetmeye başlamış; geleneksel güvenlik kavramı değişikliklere uğramıştır. Fiziki saldırılar, yerini siber uzay üzerinden gerçekleştirilecek siber saldırılara bırakma aşamasına gelmiştir. Dünyanın herhangi bir yerinden herhangi bir kişi tarafından saldırı yapılabilir hale gelmiştir.

Bilişim teknolojilerinin kullanımının yaygınlaşması ile güvenlik konusu farklı bir boyut kazanmaya başlamıştır. Bilgi güvenliği kavramı, yazının icat edildiği dönemden itibaren kullanılmakta olup verilerin ve bilgilerin bilgisayarların üzerinde tutulmaya başlanması ile bilgisayar güvenliği; ağlarla bilgisayarların birbirlerine bağlanmaları ile internet güvenliği, ağ güvenliği, siber güvenlik gibi kavramlar kullanılmaya başlanmıştır.

Bilgi ve iletişim teknolojilerinin kullanımının yaygınlaşması sürekli evrim geçiren siber uzayın toplumsal yapısını bilinmeyen bir yöne doğru dönüştürmektedir. Tüm aktörleri, organizasyonları ve toplumun tüm fonksiyonlarını kapsayan bu dönüşüm, mevcut sistemleri ve kurulu tüm toplumsal süreçleri etkileyecek niteliktedir. Toplumsal hizmetler ve fonksiyonların büyük çoğunluğu otomasyona geçirilmiş ve birbirlerine bağımlı hale getirilmiştir. Aktörler, fonksiyonları ve hizmetleri yürütmekte olan bilginin gizliliği, bütünlüğü ve erişilebilirliğine bağımlı hale gelmiştir. Siber dalandaki pek çok bilginin çeşitli güvenlik tehditlerine maruz kalabilme olasılığı yüksektir. Bu nedenle bilginin güvenlik özellikleri, bu bilgilerin üzerinde tutulmakta ve işlem görmekte olduğu teknolojik yapıların ve sistemlerin güvenliği kadar önemlidir. Sonsuz genişleme kapasitesine sahip siber uzay yeni ve ilk kez karşılaşılan aktörler, yapılar ve faaliyetler muhteşem fırsatlar sunmaktadır. Yüksek kapasiteli siber potansiyele sahip olmak, siber dünya aktörlüğünün de önemini artırmaktadır. Yüksek siber potansiyel ve karşılıklı bağımlılık siber dünyanın bazı yeni tür aktörleri ortaya çıkacak ve en azından bir süre için insanlara cazip gelecektir. Normlar ve değerlerinin yorumları gittikçe daha uyumsuz olmaya başlayacak ve yasal düzenlemelerin geliştirilmesi ihtiyacı çelişkili hale gelecektir. Siber dünyada toplumsal dönüşümün

niteliklerinin kapsamlı olarak anlaşılır olması toplumun güvenliğinin artırılması açısından çok önemlidir (Kuusisto, Kuusisto, 2015:32).

1.2 ÇEVRE ETİĞİNİN KAVRAMSAL TEMELLERİ

Bu bölümde, tezin temel konusu olan siber güvenlik kavramının çevre üzerindeki etkisini açıklayabilmek için öncelikle çevre kavramı üzerinde durulacak, insanlar tarafından üzerinde düşünülmesine ve harekete geçilmesine neden olan çevre sorunlarının nasıl başladığı; insanlar, diğer canlı ve cansız varlıklar üzerinde ne tür etkiler yarattığı ele alınacaktır. Daha sonra çevre etiği yaklaşımları üzerinde durulacak ve çevre sorunlarına çözüm aramak üzere geliştirilen "sürdürülebilirlik" kavramına da bu bölümde değinilecektir.

1.2.1 Çevre Kavramı

İnsanların, hayvanların ve bitkilerin içinde yaşadıkları, birbirleri ile ve hava, su, toprak, madenler, petrol gibi doğal kaynaklarla etkileşim halinde oldukları ortam, çevre olarak adlandırılmaktadır. Bir başka tanıma göre çevre, insanlık tarafından tarih boyunca geliştirilen uygarlığı da kapsayan ve tüm insanlığın ortak varlığı olarak kabul edilen evrensel değerler bütünüdür. Niteliği açısından fiziksel çevre ve toplumsal çevre; mekânsal boyutları açısından yerel, bölgesel, ulusal, uluslararası ya da küresel çevre şeklinde sınıflandırılabilmektedir (Keleş, Hamamcı,2002:27-36).

Çevre, sadece insanlar için yararlı olan varlıklardan oluşmaz, diğer canlıları da kapsar. Bu canlıların da çevre ile karmaşık ilişkileri vardır. Canlı ve cansız varlıklardan meydana gelen çevre ekosistem olarak adlandırılmaktadır. (Schultz,2010:209).

İnsanlar dünya üzerinde ilk var oldukları andan itibaren canlıların yaşaması için gerekli olan hava, su ve toprağın oluşturduğu yaşam ortamlarında bitkiler, hayvanlar ve mikroorganizmalardan oluşan canlı doğal kaynakları ve madenler, fosil yakıtlar gibi yeraltı zenginlikleri gibi doğal kaynakları kullanarak yaşamını sürdürmüştür. İnsan, başlangıçta çevredeki tüm varlıklardan yararlanmasına rağmen güçsüzlüğü nedeni ile doğa üzerinde bir hakimiyet sağlayamazken zaman içinde geliştirdiği teknolojiler sayesinde ve artan insan nüfusu ile doğada pek çok alanda hakimiyeti ele geçirmiştir.

Birbirinden tortul tabakaların özellikleri ile ayrılan jeolojik dönemlerin en sonuncusu, insanın gezegene hükmettiği ve tortul tabakaların benzeri izler bıraktığı Antroposen Çağ olarak adlandırılmaktadır. Bu izlerden bazıları, 20. Yüzyıldaki nükleer patlamalar sonucu yayılan radyoaktivite, okyanuslarda asitlenme ile biriken tortular, atmosferdeki yüksek karbon salımlarının buzul tabakalarında birikmesi, aşırı erozyon ve yeryüzündeki tortulanmalardır Bu çağın en önemli özelliği, insanın yeryüzü sistemlerine hükmetmesi, doğaya müdahale ederek canlı topluluklarının doğal özelliklerini değiştirmesi olmuştur (Ruddiman,W.F.(2013'den aktaran Brown&Schmidt,2014:87).İnsanın doğa üzerindeki faaliyetleri kendisinin de içinde yaşadığı tüm insanların ve diğer canlıların ortak varlığı olan doğaya zarar vermeye başlamış ve tüm canlıların yaşam ortamlarının kirlenmesine ve olumsuz etkilenmesine neden olmuştur. İnsanın doğa üzerindeki olumsuz etkisi özellikle Endüstri Devrimi sonrası hızlanmış ve devletlerin ekonomik sistemlerine uygun olarak büyüme politikaları da bu kirliliğin hızlı bir şekilde artması ve canlıları etkiler duruma gelmesine neden olmuştur. 1980'li yıllarda başlayan küreselleşme ile had safhaya ulaşmıştır.

İnsanların ve diğer canlıların yaşam ortamını olumsuz yönde etkileyen faaliyetler son dönemlerde önemli çevre sorunlarını gündeme getirmeye başlamıştır. Dünya üzerinde canlıların yaşamlarını sürdürebilmesi için gerekli olan sindirim, solunum, fotosentez gibi süreçler, hava sayesinde gerçekleştirebilmektedir. Nüfus artışı, sanayileşme, kentleşme gibi etkenler, atmosfer içindeki gazların dağılımında değişiklikler meydana getirerek doğal yapısını bozmakta ve zararlı maddelerin artması ile canlıların yaşam ortamında olumsuz etkilere neden olmaktadır.

Canlıların yaşaması için hayati önem taşıyan su kaynakları da uygarlığın gelişmesine paralel olarak insanlar tarafından sıklıkla müdahale edilen varlıklar arasındadır. Suyun katı, sıvı, gaz haline gelişine ve bir yerden başka bir yere taşınması ile doğal ortamda oluşturduğu olumsuz etkilerin yanı sıra tarımda, kentlerde ve sanayide ortaya çıkan atıkların ve atık suların da temiz su kaynaklarına karışması ile tüm canlı türlerini ve doğal ortamları tehdit eden önemli sorunlar oluşmaktadır.

İnsanın ve diğer canlı türlerinin büyük bölümünün yaşam ortamı olan toprak, canlıların besin kaynaklarının yetiştiği bir ortam, doğal bir kaynaktır. Toprak, yaşam için

temel olan doğal bir kaynak olmasının yanı sıra insanların yüzyıllar boyu oluşturdukları uygarlığa da ev sahipliği yapmaktadır. Toprak da insan müdahalesinden olumsuz yönde etkilenmekte, yanlış tarım teknikleri, yanlış ve bol miktarda gübre ve tarım ilacı kullanılması, zehirli ve tehlikeli atıkların toprağa bırakılması gibi nedenler ile yapısı bozulmaktadır. İnsanın toprağa doğrudan müdahalesine ek olarak hava ve suda oluşan kirliliğin toprağa ulaşması ile de toprakta geriye dönüşü olmayan etkiler meydana getirebilmektedir.

İnsanın içinde yaşadığı çevreyi oluşturan önemli ögeler arasında, bulunduğu bölgeye özgü bitki örtüsü olarak tanımlanan flora ve hayvan topluluğunun oluşturduğu fauna da sayılmaktadır. Bitki ve hayvan türlerinin biyolojik çeşitliliği de insan yaşamının sürdürülebilirliğini destekleyen unsurlar arasındadır. Bilinçli ya da bilinçsiz insan faaliyetleri sonrası yaşanılan ortamdaki flora ve faunalar da zarar görmektedir. Bu türlerin insan hayatına katkıları yanı sıra kendilerinin sahip olduğu içsel değer nedeni ile de korunması gerekmektedir.

İnsanın tarih boyunca oluşturduğu uygarlıklar tarafından üretilmiş kültürel varlıklar da çevreyi oluşturan ögeler arasında yerini almıştır. Kültürel varlıklar üretildikleri dönemler sonrasında insanların doğrudan kötü niyetli davranışları ile, ekonomik nedenlerle ya da dolaylı olarak havada suda ve toprakta oluşan zararlıların etkisi ile tahrip edilebilmekte ve yok edilebilmektedir.

İnsan hayatının sürdürülebilmesi için gerekli olan enerjinin özellikle Sanayi Devrimi sonrası kullanım alanlarının artması ile petrol, doğalgaz, kömür gibi fosil yakıtların yeraltından çıkarılması ve kullanılmaları sırasında atmosfere saldıkları zehirli gazlar önemli çevre kirliliği sorunlarına neden olmuştur. Yakın dönemlerde kullanımı artan güneş enerjisi, rüzgar enerjisi gibi yenilenebilir enerji kaynaklarının kullanımı da çevre kirliliklerine neden olmaktadır ancak bu kirlilik fosil yakıtların oluşturduğu kirliliğe oranla kıyaslanamayacak ölçüde azdır.

İnsanın çevre üzerinde oluşturduğu olumsuz etkiler arasında, oluşturulan çevre kirliliğinin yanı sıra yeraltında bulunan madenlerin yoğun kullanılması ve geri döndürülemez bir şekilde tüketilmesi de sayılmaktadır.

İnsan, hayvan ve bitkiler gibi canlı varlıklar ve hava, toprak, su, madenler gibi cansız varlıkların oluşturduğu ekosistemdeki bozulma tüm canlıların hayatını zorlaştırabilecek ve hatta imkânsız hale getirebilecek niteliktedir. Doğal kaynaklar, hava, su ve gıdaları kapsayan çevre desteği olmadan ekonomi olmaz. İnsanların sosyal iş birliği ve bireysel konuların var olabilmesi için öncelikle içinde yaşayabilecekleri uygun bir ekosisteme ihtiyaçları vardır (Schultz,2010:209).

Küreselleşme olarak adlandırılan 1980 sonrası yaşanan büyük değişim, ulaşım ve tüketimi artırmış, çevrenin tahribatı, kaynakların hızlı tüketimi sonuçlarını doğurmuştur. İnsan nüfusunun artması ve değişik uygarlıklar yaratması ile birlikte içinde yaşadığımız ekosisteme verilen zararlar artmış; insanların ve diğer canlıların yaşaması için gerekli doğal ortam da hızla yok olmaya başlamıştır. Kaynakların sınırlı olduğu dünyamızda artan nüfus ve artan kaynak tüketimi, dünya üzerinde uzun vadede yaşamın sürdürülebilirliğine yönelik tehditler oluşturmaya başlamıştır. Nüfus artışı ya da ekonomik gelişmeler ve tüketimdeki aşırı artış zaman içinde insan yaşamına yönelik olumsuz koşullar ortaya çıkarabileceği için kaynak kullanımının optimum seviyede tutulması ihtiyacı doğmuştur.

İnsanlar, içinde bulunduğumuz çevrenin, daha çok insan faaliyetlerinden kaynaklanan sorunlar nedeni ile canlılar üzerindeki olumsuz etkilerini 1980'li yıllardan itibaren daha yoğun olarak hissetmeye başlamıştır. Bu bölümün başında da değinildiği gibi, genel anlamda "mülkiyetin yetkisiz erişiminin, kullanımının, değiştirilmesinin, çalınmasının ya da fiziki olarak zarar verilmesinin önlenmesi" şeklinde tanımlanmakta olan (Kizza, 2007, s:101) ve temel başvuru nesnesi devlet olan geleneksel güvenlik anlayışında 1980'lerin sonlarında kapsamlı değişiklikler olmuştur. Bu değişikliklerin en önemlilerinden biri, Kopenhag Okulu tarafından, güvenlik sektörlerinin kavramsallaştırılması ve askeri sektör yanında siyasi, ekonomik, toplumsal ve çevresel güvenlik sektörlerinin de tanımlanmış olmasıdır. (Buzan,vd.,1998:208). 20. Yüzyılın son dönemlerinde, çevre sorunlarındaki artış ve kaynakların azalmaya başlaması, Kopenhag Okulunun söylemlerine uygun olarak güvenlik gündemine dahil edilmiş ve medyada, akademik çevrelerde sıklıkla tartışılmaya başlanmış; devletler de bu sorunu ciddiye almaya başlamış ve gündemlerine almışlardır.

Çevre sorunlarının sadece bilim ve teknolojiden kaynaklanmadığı ve sadece bilim ve teknoloji ile çözüme ulaştırılamayacağı anlaşılmıştır. Özellikle sanayileşmiş toplumlarda

hava, su, toprak, madenler gibi kaynakların kullanılmasında ve teknolojinin yönetimi ve denetiminde yapılacak yanlış bir hareket, temel dengelerin bozulmasına ve insan varlığının önlenemez sorunlarla karşı karşıya kalmasına yol açabilecektir (Keleş, Hamamcı, Çoban, 2009:266). Çevre sorunlarının çözüme kavuşturulabilmesi için, insanın neye değer verdiği, doğanın efendisi mi yoksa doğa içinde yaşamakta olan canlıların bir türü mü olduğu, nasıl bir çevrede yaşamak istediği ve bunun için neler yapılması gerektiği gibi soruların sorulmasının ve çevreye karşı yeni bir ahlaki sorumluluk geliştirmenin gerekliliğinin farkına varılmıştır (Des Jardins, 2006:35). Çevreci olmak insanın doğanın efendisi olmadığını, kendisinin de doğal bir nesne olduğunu ve dolayısıyla dünyanın evriminin içinde kendisinin evrim geçirdiği bir çerçevede olduğunu bilmesidir. Yeni insan, doğanın işleyişini en iyi biçimde öğrenerek eğitilmiş insandır (Hessel, 2011:43).

1.2.2 Uygulamalı Etik Kapsamında Çevre Etiği

Etik kavramı uzun yıllar boyunca bireyler arası ilişkileri anlatmak üzere kullanıldıktan sonra Apel'in deyimi ile uygarlıktaki gelişmeler paralelinde bu kavramın kapsamı da genişletilmiş; bireyin içinde yaşadığı toplum ve ülke içindeki ilişkilerini ilgilendiren davranışları da kapsama alanı içine almıştır. Evrensel bir yurttaşlık kavramının sıklıkla kullanıldığı günümüz dünyasında, insanların gezegen üzerinde yer alan tüm toplumlara ve onların değerlerine karşı birtakım sorumluluklar duyması, teknolojik gelişmelerin onlara zarar vermesinden kaçınması, sorumluluk alanını genişletmiştir (Keleş, Hamamcı, Çoban, 2009:268). Özellikle 20. yüzyıldan günümüze kadar çok daha gelişmiş sosyal bir topluluğa dönüşen insanoğlunun modern hayatın yarattığı karmaşık problemlere yönelik etiği kullanış ve hayata aktarış biçimi de değişimler göstermek zorunda kalarak, etik disiplininin altında yeni alt-disiplinlerin gelişimi izlenmiştir (Singer,1986:3).

Geleneksel ahlaklılık insanların refahı için kendi aralarındaki ilişkiler biçiminde tanımlandığı için çevre sorunlarının bu ahlaki sınırlar içinde tanımlanması zor olmuştur (Des Jarden,2006:260). Felsefi etik, insanın iyi yaşamasını ve gelişimini temel aldığı için, buna benzer durumlarda meydana gelen etik çıkmazların seçimlerin, standartların ve ahlak teorileri ile kavramlarının belirli bir konuya uygulanmasını inceleyen etik türü olarak Uygulamalı Etik kullanılmaya başlanmıştır (Fox ve De Marco 1990'dan aktaran David B.

Resnik,2004: 35). Uygulamalı etik alanları arasında tıbbi etik, biyoetik, sosyal etik, iktisat etiği, bilim etiği, meslek etiği, çevre etiği gibi alanlar bulunmaktadır (Pieper, 2012:85-128).

20. yüzyılın ortalarından sonra teknolojideki gelişmeler paralelinde yeni mesleklerin ve beyin gücü ile çalışanların artması ile birlikte meydana gelen problemleri tartışmak üzere 1970'li yıllardan itibaren, uygulamalı etik kullanılmaya başlanmıştır. Teknolojinin yaygın bir şekilde kullanılmaya başlanması ile günlük hayatın her alanında karşılaşılan sorunların ahlaki açıdan değerlendirilmesi, uygulama ve analizi bu alandaki konularda önemli artışlara neden olmuştur. Erdem etiği, ödev etiği, ahlaki yükümlülük etiği, yararcılık, gibi etik kuramlar kullanılarak edinilen birikimlerin değişik alanlara uygulanması yolu ile sorunlara çözüm bulunmasına çalışılmaktadır. Bir sorunun uygulamalı etik alanı içinde incelenebilmesi için bu sorunun tartışmalı bir durum oluşturması; bireylerin etik ödev ve yükümlülüklerinin neler olduğuna dair evrensel bir etik sorunun bulunması gerekmektedir. Etik sorunların çözülmesinde genellikle geleneksel ahlak kuralları ve teorik etikte edinilen bilgi birikimi kullanılmaktadır. Bu etik türünde, bireysel vakalar incelenirken bütüncül bir yaklaşım ile genel ilkeler somut durumlara uygulanmakta ve konu ile ilgili görüşler delillendirilmeye çalışılmaktadır (Cevizci, 2014:21-25).

Uygulamalı etik, gelecek kuşaklara karşı sorumluluklarımız temelinde, sürdürülebilirliğin sağlanmasına yönelik olarak, insanlığın ekosistem ile yeniden bütünleşmesini sağlayacak sürdürülebilir bir toplum oluşturmaya yönelik yönlendirici fikirler de sunabilmektedir. (Çobanoğlu, 2009:11).

1980'li yıllardan itibaren günlük hayatın hemen hemen her alanında kullanılmaya başlanan bilişim teknolojileri de sıklıkla savunan ve karşı koyan grupların olduğu tartışmalı durumlar yaratmakta olduğu, evrensel etik problemler oluşturduğu için uygulamalı etik kapsamında ele alınabilmektedir. Tezin temel sorunlarından biri, çevre etiği bağlamında siber güvenliğinin sağlanması olduğu için Çevre Etiği konusu incelenecektir.

1.2.2.1 Çevre Etiği

Bu çalışmada, siber güvenlik olaylarının çevre üzerinde oluşturabileceği olumsuz etkiler ve bu olumsuz etkileri önlemeye yönelik etik uygulamaların neler olması gerektiğini araştırmak hedeflendiği için uygulamalı etik türlerinden olan çevre etiği incelenmiştir.

İnsanlığın dünya üzerinde yayılması, değişik uygarlıklar yaratması ile birlikte içinde yaşadığımız çevreye verilen zararlar artmış insanların yaşaması için gerekli doğal ortam da hızla yok olmaya başlamıştır. İnsanların nasıl yaşaması, nasıl davranması, nasıl davranmaması, nasıl bir insan olması gerektiği ile ilgilenen etik, zamanla içinde yaşanılan çevreye de ilgi göstermeye başlamıştır (Des Jardens,2006:260). İnsanlar, içinde bulunduğumuz çevrenin canlılar üzerindeki olumsuz etkilerini 1970'li yıllardan itibaren daha yoğun olarak hissetmeye başlamış; çevre sorunları ve kaynak kısıtlılığının yaşanmaya başlandığı bu dönemde insanın-doğa ile ilişkisi daha önce hiç görülmemiş bir şekilde sorgulanır olmuş ve felsefe alanı içinde çevre etiği yeni bir araştırma alanı olarak yerini almaya başlamıştır (Cantzen,2015:228; Keleş, Hamamcı, 2002:232).

Antroposen çağında büyük ölçüde, insanın doğaya verdiği zararların neticesinde oluşan iklim krizi ile insanların, diğer canlıların ve varlıkların dünya üzerindeki sürdürülebilirliklerinin risk altına girmesine çözüm olarak insan ve yeryüzü sistemlerinin karşılıklı bağımlı olduğu görüşüne uygun normları devreye alarak siyasi ve çevresel düzenlemeleri yeniden düzenlemek için çevre etiği yaklaşımı benimsenmiştir (Lövbrand,2010:7-8). İnsanlar ile içinde yaşadıkları doğal çevreleri arasındaki ahlaki ilişkilerin bir sistem içinde incelenmesini hedefleyen uygulamalı etik türü çevre etiği olarak adlandırılmıştır (Des Jardens,2006:46).

İnsanlar, daha önce doğayı sadece kendi ihtiyaçlarını karşılayacakları tükenmez bir hammadde deposu olarak kullanmışlar ve oluşturdukları zararlı atıkları da yine bu ortama bırakarak doğayı sürekli sömürmüştür. Zamanla sadece insanın kendisine değil diğer tür canlılar için de türlerinin yok olmasına varan zararlı sonuçlar önemli boyutlara ulaşmış ve herkes tarafından fark edilir olmuştur (Pieper, 2012:91). Çevre etiği kapsamında çevreye karşı yeni bir ahlaki sorumluluk etiği geliştirmenin gerekliliğinin farkına varılmıştır.

Günümüzde çevre etiği kavramı, karar verenlere, sıradan insanlara, yetişkinlere ve çocuklara, şu anda yaşamakta olan insanların ve gelecek kuşakların varlığını sürdürebilmesi için nelerin yapılması, nelerin yapılmaması gerektiğinin söylenmesi amacı ile kullanılmaktadır. Kuçuradi, birbirinden farklı çevre sorunlarından kaynaklanan etik sorunlar tek tek incelendiğinde aslında bu sorunların insanların diğer alanlardaki uğraşılarında ve genel olarak yaşam boyu karşılaştıkları etik sorunları ile aynı türden

olduğunu belirtmektedir (Kuçuradi,2009:39). Çevre etiği, yaşayan insanlar, içinde yaşadıkları fiziki dünya ve henüz var olmayan gelecek nesiller gibi birçok şey arasındaki ilişkileri düzenlemeye çalışan bir uygulamalı etik türüdür.

1.2.2.2 Çevre Etiği Yaklaşımları

İnsanın geçmişte olup bitenlere karşı sorumluluğundan çok geleceğe dönük önlemlerin alınması isteğini anlatan sorumluluk kavramı, etik ile yakından ilişkilidir. Ahlaki değere sahip olması hasebi ile tek sorumluluk sahibi varlık insandır. (Keleş, Hamamcı, Çoban, 2009:270). Çevre etiği kapsamında felsefeciler tarafından doğanın, insan ihtiyaçlarının karşılanması dışında kendine içkin bir değeri olup olmadığı; insanın doğaya ve doğal varlıklara karşı sorumluluğunun bulunup bulunmadığı, insanın diğer canlılarla eşit öneme mi sahip olduğu yoksa diğer canlılar arasında üstün bir varlık mı olduğu gibi konular tarihsel süreç boyunca da hep tartışma konusu olmuştur. Zaman içinde; insanların sorumluluk alanları içinde yaşadıkları doğal ortamın bozulmasını önlemek, doğanın dengesini yeniden kurmak, insanların çıkarlarının yanı sıra diğer canlıların da yaşam hakkını gözetmek, cansız varlıkların varlığının sürdürülmesi gibi konuları kapsayacak şekilde genişletilmiştir.

Çevreye yönelik etik faaliyetler belirlenirken, çevrenin korunmasında insan merkezli anlayışla mı yoksa doğanın salt kendisinde mevcut olan bir değerden dolayı mı korunması gerektiği de sıklıkla tartışılır olmuştur (Cantzen, 2015:253). Çevre etiği alanında, insanların kimlere ve nelere karşı sorumlulukları bulunduğunu açıklamak için kullanılmakta olan farklı çevre etiği yaklaşımları bulunmaktadır. Kimileri insan merkezli ve çevre merkezli olmak üzere iki grupta toplamakta; kimileri insan merkezli, canlı merkezli ve çevre merkezli çevre etiğinden bahsetmektedir. Bu bölümde insan merkezli, canlı merkezli ve çevre merkezli etik yaklaşımlar incelenmiş; çevre merkezli bütüncül etik yaklaşımı açıklanmıştır. Bireysel hak ve ödevler konularının yanı sıra toplumsal sorunlara da yanıt aramakta olan çevre etiği kapsamında oluşan Derin Ekoloji, Toplumsal Ekoloji ile pragmatik yaklaşım örneği olan Sürdürülebilirlik gibi yeni alanlar da bu çalışma kapsamında incelenmiştir.

i. İnsan Merkezli Çevre Etiği

İnsan merkezli çevre etiği, canlı ve cansız varlıkların var oluş nedenlerini ve temel işlevlerini insana dayandıran, tüm varlıkların insanlara sağladıkları yarar oranında değerli olduklarını ileri süren insan odaklı bir yaklaşımdır (Ertan, 1998: 135). Bu yaklaşıma göre, ahlaki değere sahip olan tek varlık insandır. Bu etik yaklaşımı temellendiren Aristoteles'e göre bitkiler, hayvanlar için; hayvanlar, insanlar için vardır. Doğada var olan her şey insan içindir. Ahlaki özne olmak için gerekli ve yeterli niteliklere sahip tek varlık olan insan, çıkarları ve/veya hakları bağlamında ahlaki açıdan dikkate alınması gereken tek varlıktır (Erbil & İdemen, 2010:8). Keleş ve Ertan, doğada var olan tüm varlıkların insan için yaratıldığı şeklindeki görüşü, insan merkezli etik yaklaşımın en sıkı biçimi olarak tanımlamaktadır (Keleş ve Ertan,2002:188-189). Bu, çevrenin özsel bir değerden arındırılması ve insana en yüksek değerin atfedildiği bir yaklaşımdır (Ertürk,2009:89). Kimi görüşlere göre, çevre üzerinde olumsuz etkiler yarattığı değerlendirilse de bazı insan merkezli etik yaklaşımlar, insan çevre ilişkilerini düzenleme ve çevreyi koruma konusunda genişleme ve gelişme göstermektedir (Keleş & Ertan, 2002: 189). Çevrenin, insanlar için korunması gerektiği görüşünü savunan görüşler, insan merkezli çevre etiği yaklaşımları içinde anılmaktadır. Çevre sorunlarının çözümünde insana gözetmen ya da bakıcı rolü yükleyen John Passmore'un geliştirdiği "bekçilik (stewardship)" yaklaşımı ile insanın doğaya karşı sorumluluklarını yerine getirmesi gerektiğini savunan yaklaşım ve insanın doğada "en üstün değer" olduğunu savunan Rene Dubos'un ise, insanın doğayı kendi çıkarları için etkin bir biçimde koruması gerektiğini savunan ve "aydınlatılmış insan merkezlilik" olarak adlandırdığı yaklaşımı yer almaktadır. Doğadaki canlıların eşit gelişmişlik oranlarına sahip olmadıkları için eşit sayılamayacaklarından hareketle "Modern insan merkezli" etik yaklaşımını geliştiren Murdy ise, evrim sürecinin kendisinden kaynaklı bu sorun nedeni ile insanların haklarının, diğer türlerin haklarından üstün olduğunu savunmaktadır (Akkoç,2014:67).

Kuramcı Thomas Berry, insan merkezli yaklaşımı teknozoik zihniyet olarak adlandırmakta ve bu yaklaşımda insanı, biyosferi öğüten, litosferi kazıyan, atıklarını karaya

denize havaya dağıtan, en sonunda kendi bedenini de dağıtan varlık olarak tanımlamaktadır ((Berry,1999)'den aktaran Brown&Schmidt,2014:87).

İnsan merkezli çevre etiği yaklaşımları, ahlaki değere sahip olarak gördüğü insanın çevre sorunlarına neden olan davranışlarını göz ardı ederek, onun çevre sorunlarına çözüm bulabilen ve çevreyi koruyabilen niteliklerini ön plana çıkarmaktadır. Bu çevre etiği yaklaşımı, her şeyin en üstün değere sahip olan varlık olarak gördüğü insan için olduğunu; insanı mükemmelleştirmek için çevrenin korunması gerektiğini savunmaktadır. Doğal dünya ile ilgili sorumluluğun sadece insan hayatını en iyi şekilde sürdürebilmek ile sınırlı olduğunu; bunun dışında doğal dünyaya yani diğer canlı ve cansız varlıklara karşı insanın doğrudan bir sorumluluğu olmadığı düşüncelerine dayandırılmaktadır.

Bazı etikçiler, insan merkezli çevre etiği anlayışı kapsamında doğaya karşı koruyucu tavır gösterilmesini, yükümlülük oluşturma açısından yetersiz bulmaktadırlar. Asıl derdi insan varlığının sürdürülebilmesi olan insan merkezli yaklaşımın, ekolojik sorunların önemini ekonomik, toplumsal ve sosyal sorunlarla karşılaştırarak belirlediği eleştirisi getirilmektedir (Cantzen,2015:256).

Ahlaki açıdan sadece insanları ilgi alanına alan insan merkezli etik yaklaşım ile, insanların sorumluluk alanı henüz doğmamış insanları da kapsayacak biçimde genişletilmiş ve gelecek nesiller de ahlaki sorumluluğun konusu yapılmıştır (Des Jardins, 2006:47). İnsan merkezli çevre etiğinin alanları genişletilerek gelecek nesillerin de ahlaki sorumluluk kapsamına alınması ile sürdürülebilirlik kavramı ortaya atılmıştır.

ii. Canlı Merkezli Çevre Etiği

İnsan merkezli etik yaklaşımda, insan dışında kalan canlı ve cansız tüm doğal varlıkların tüketimi mübah sayılmıştır (Ürker,2014:190). Tarihsel süreçte insan merkezli çevre etiği yaklaşımını takiben; insanların yanı sıra bitki ve hayvan topluluklarının oluşturduğu canlı varlıkların yaşam hakları olduğundan hareketle canlı merkezli çevre etiği geliştirilmiştir. Canlı merkezli çevre etiği yaklaşımı, canlı varlıkların değeri, önemi ve bu bağlamda hakları bulunduğu görüşüne dayanmaktadır (Keleş & Ertan, 2002:193). Bu yaklaşıma göre, insan doğadan üstün değil, canlı topluluğunun bir parçasıdır.

İnsan dışındaki varlıklara da değer verilmesi; acı ve haz duyabilecek canlı varlıkları özne olarak tanımlayan bu yaklaşımda bazı çevresel unsurların göz önüne alınarak insanın ahlaki kaygılar ile doğadaki diğer canlılara sebepsizce acı çektirmesinin önlenmesi de hedefler arasındadır (Ertürk,209:89). Canlı merkezli etik yaklaşım, insanın ve hareket halinde olan canlıların yanı sıra daha az gelişmiş kabul edilen bitkilerin de içsel bir değere sahip olduğunu savunmaktadır. Bu etik yaklaşımda, canlıların acı çekip çekmediklerinden ve gelişmişlik derecelerinden bağımsız olarak sadece yaşadıkları için ahlaki bir değere sahip oldukları savunulmaktadır (Akkoç, 2014:68).

Aldo Leopold, insanın, evrim sürecinde diğer türlerle seyahat arkadaşı olduğu düşüncesine dayanan eşitlikçi bir ekosistem etiğini formüle etmiştir (Keleş & Ertan, 2002: 194). Her canlı türünün kendine özgü büyüme, gelişme, türünü sürdürme ve yayılma amacı vardır. Bu bakış açısı ile insan da diğer canlılarla eşit koşullarda aynı ortak amaca hizmet etme yolu ile, bağlı bulunduğu sistemin bir parçasıdır. İnsan türü, diğer türlerle eşit üstünlükte olduğu için doğadaki hiçbir canlıya hiçbir koşulda zarar verilmemelidir. Albert Schweitzer, yaşam biçimlerinden daha az değerli olan ile daha çok değerli olan arasında saygı gösterme açısından bir ayrım yapılamayacağı düşüncesinden hareketle yaşamı temel değer olarak kabul etmiş ve yaşama saygı etiğini formüle etmiştir. Böylelikle ahlaksal topluluğun sınırları hayvanları kapsayacak şekilde genişletilmiştir. (Ürker, 2014:192). Bu etik yaklaşımda ahlaki değerleri bulunmadığı gerekçesi ile cansız varlıklar, etik ilgi kapsamına alınmamaktadır.

iii. Çevre Merkezli Çevre Etiği

Doğanın insanla ilişkilendirilmeden de kendi başına bir değerinin ve var olma hakkının bulunup bulunmadığının ya da bu değer ve hakkın sadece insana yararlılığı açısından mı ele alınması gerektiği sorusu sıklıkla sorulmaya başlanmıştır (Cantzen,2015:228). İnsan merkezli çevre etiği kapsamında yer almayan tüm canlı ve cansız varlıkları içinde barındıran doğanın, ekolojik sistemin etiğin ilgi alanına girmesi, doğanın, ekolojik sistemin mevcudiyetinden dolayı kendi içinde, kendisi için bir değere sahip olduğunun savunulduğu çevre merkezli çevre etiği ile olmuştur. Çevre merkezli çevre etiği, doğa üzerindeki insan egemenliğinin yaratmış olduğu çevre sorunlarına dikkat çekmekte ve

doğada insanın yanı sıra başka canlı türleri ve cansız varlıkların da bulunduğunu, bu nedenle onların da hak sahibi olması gerektiği fikrini savunmaktadır (Mengi, 2012:70). Örs de, doğa üzerinde kendi çıkarları doğrultusunda hareket eden insan merkezli bencil yaklaşımdan vazgeçilmesini ve doğanın varlığını amaç olarak belirleyen bir yaklaşımla öz olarak doğa merkezli etik görüşün benimsenmesini önermektedir (Örs, 1997:370).

Doğal çevrenin korunmasına yönelik etik düşünceyi destekleyen Gaia varsayımı, İngiliz Bilim Adamı James Lovelock tarafından öne sürülmüştür. Bu varsayıma göre yeryüzü, canlı bir organizma olarak algılanmış; ekosistemlerin geri besleme ilişkileri ve denge kavramları kullanılarak sistemin bütününe, Yunancada yeryüzü tanrıçası anlamına gelen Gaia adı verilmiştir. Canlı bir organizma olduğu kabul edilen dünyanın bozulması ve kirletilmesine yönelik insan faaliyetlerini eleştirmede Gaia yaklaşımı sıklıkla kullanılmaktadır (Des Jardens, 2006:334-335). Ekolojik açıdan beslenme zincirinin en tepesinde olan insan, diğer canlılara ve içinde yaşadığı gezegenin doğasına hükmetmektedir. Biyologlar ve doğayı koruma görevi yapmakta olan ekolojistler, insan merkezci ekolojistler çevre sorunlarının insan kaynaklı olduğunu ancak bu sorunların yine insan tarafından çözümlenebileceğini savunmaktadırlar (Ertürk,2009:83)

1.2.2.3 Çevre Merkezli Çevre Etiği Kapsamındaki İdeolojiler

Çevre merkezli çevre etiği kavramı, başlangıçta Aldo Leopold tarafından Yeryüzü Etiği; daha sonra Naess tarafından Derin Ekoloji ve Bookchin tarafından ise Toplumsal Ekoloji ideolojileri öne sürülerek genişletilmiş ve daha bütüncül yaklaşım sergilenmiştir:

i. Yeryüzü Etiği

Çevre merkezli çevre etiğinin geliştirilmesi Aldo Leopold ile başlamıştır. Leopold, başlangıçta doğayı sadece insana sağladığı fayda açısından araçsal değeri ile ele alırken daha sonraki çalışmalarında doğal sistemlerin, bu araçsal değerlerinin yanı sıra kendi varoluşlarından kaynaklanan içsel bir değere de sahip oldukları fikrini savunmaya başlamıştır. Leopold, o döneme kadar sadece insanlar arası ilişkilerde ahlaki ehliyeti temel almakta olan etik yaklaşımın yetersiz kaldığını ve genişletilmesi gerektiğini belirtmiştir.

Yeryüzü etiği sayesinde çevre etiği, toprakları, suları, bitkileri ve hayvanları kapsayacak şekilde genişletilmiştir. (Des Jardens, 2006:352-357).

Leopold tarafından geliştirilen Yeryüzü Etiği, canlı ve cansız organizmalardan oluşan ekosistemi temel almaktadır. Leopold'un üç aşamalı etik anlayışının birinci aşamasında, bireyler arası ilişkilerin; ikinci aşamasında bireylerin toplumla olan ilişkilerinin düzenlenmesi yer almaktadır. Üçüncü aşamasında ise doğanın bir parçası olan insan türünün dünya üzerinde birlikte yaşadığı diğer türlerle toprağı, suyu, havasıyla bir bütün olarak yeryüzünü paylaşmak zorunda olduğu; insanın da bir parçası olduğu doğanın tüm bileşenleri ile birlikte ele alınması gerektiği vurgulanmaktadır. İnsanın etkileşimde bulunduğu topluluğun sınırları tüm doğayı kapsayacak şekilde genişletilerek doğa etiği tanımı yapılmaktadır. Bu üçüncü aşamada insanların, insan toplumlarının ve doğanın insan dışında kalan bileşenleri arasındaki ilişkileri düzenlemeyi hedefleyen etik kurallara ihtiyaç olduğu belirtilmektedir. Yeryüzündeki tüm türlerin varlığını sürdürebilmesi için, toprağı, suyu, havası, hayvanı ve bitkisi ile doğanın bir bütün olarak varlığını sürdürebilmesi şarttır (Özer, 2017:100-103). Leopold'un doğa etiği anlayışına göre insanlar kendilerini, doğanın efendisi olarak görmek yerine diğer varlıklar gibi doğanın sade bir üyesi olmayı kabul etmeli; doğanın sağlığını ve bütünlüğünü korumak için etkin ve uygulanabilir yöntemler geliştirmeye gayret etmeli; bilim insanlarının da araştırmalarını bu doğrultuda yürütmelerini talep etmelidir (Özer, 2017:105-106).

İnsan yaşamının yeryüzünde yoksullaşmadan sürmesi ve gelecek kuşakların da doğal zenginliklerden bizim kadar yararlanabilmesi için insanlar vicdanlarını insan dışında kalan doğayı da içerecek biçimde genişletebilmelidir (Leopold,1966:246). Ahlaki aktör olma yetisine sahip insanlar, diğer insanların sorumluluklarını üstlenebilmenin yanı sıra, bu yeteneklerini kullanarak kendilerinin de bir parçası oldukları doğanın diğer üyelerinin korunması hususunda da sorumluluk alıp bu sorumluluk bilinci ile hareket etmelidirler.

Leopold tarafından benimsenen bütüncül çevre etiği yaklaşımında, tek tek topluluğu oluşturan üyelerin değil, topluluğun kendisinin, bütünün iyiliğine yönelik eylemler doğru eylem olarak nitelendirilir. Ona göre, bir ekosistemin kendi içindeki bağlılıkları görmezden gelme, kötüye kullanımı ve tahribatı beraberinde getirir bu yanlışın önüne geçmek için ekosistemlerin sanki ahlaki ehliyetleri varmış gibi düşünülmesi gerekir. Yeryüzü canlı bir

ekosistem olarak kabul edilebiliyorsa ve sağlık, hastalık, büyüme ölüm gibi bazı özelliklere sahip olduğu kabul ediliyorsa ahlaki ehliyeti de vardır denilebilir. Leopold, canlı topluluğun bütünlüğünü, tutarlılığını ve güzelliğini korumaya yönelik faaliyetlerin doğru davranış türü olduğunu kabul eder (Des Jardens,2006:362-365). Moline'e göre Leopold'ün bütünlük ve tutarlılık ilkesi, tavırlar, istekler, düşünme ve arzu etme biçimlerini kapsayan insan karakteri için bir kural olarak görülmelidir Bütünlük ve tutarlılık ilkeleri, yapılması gereken özgül eylemleri değil insan karakterinin bir özelliğini, nasıl bir kişi olunması gerektiğini göstermektedir (Des Jardens,2006:373). Leopold'ün etiğine göre, doğru eylemin ya da kararın ne olduğu ayrıntıları ile bilinmeyebilir ancak kimin bir sorumluluk kapsamında hareket etmekte olduğu belirlenebilir. Seven ve saygılı bir davranış sergileyen kişi sorumluluk taşıyan bir karar vermiş olacaktır. Canlılar topluluğunu seven, sayan ve takdir eden kişilerin verdikleri kararlar etik açıdan sorumlu bir karar olarak kabul edilir. Leopold'ün yeryüzü etiği, Aristoteles'in erdem etiğinde olduğu gibi belli bir ahlaki kural ya da ilkenin tavsiye edilmesini değil, bir etik karakterin nasıl olması gerektiğini anlatmaktadır (Des Jardens, 2006:378-379).

Doğanın, insanlığın yaşamasını güvence altına almak için değil; kendi başına bir amaç ve erek taşımasından dolayı bir değere sahip olduğu için korunması gerektiğini savunan Amery ise insanı tehlikeli, kötü, saldırgan, tehdit edici olarak; doğayı iyi, uyumlu ve dost olarak tanımlamakta; insanın ve toplumun doğaya uyum sağlaması gerektiğini dile getirmektedir. Doğalcı düşünce olarak adlandırılan bu sistemde, insanın doğa ile karşılıklı ilişkiler içinde bulunduğu ve doğanın bir parçası olduğu anlayışı yerine insan ve doğa birbirine karşı kutuplar olarak tanımlanmakta ve insanın aktif müdahaleler ile doğayı değiştirmekten vazgeçmesi ve ona uyum sağlaması gerektiği savunulmaktadır (Cantzen,2015:254-255). Bu yaklaşıma göre, doğanın kendine içkin bir değeri bulunduğu için değiştirilmeme, zarar verilmeme hakkına sahiptir, insanın yeri ise doğadan üstün değildir.

ii. Derin Ekoloji

Çevre etiği içinde, bireysel ve toplumsal kurumlar ve uygulamalar düzeyinde ortaya çıkmakta olan etik sorunlar nedeni ile bireysel hak ve ödevler konularının yanı sıra

toplumsal adalet sorunlarına da yanıt arama aşamasında Derin Ekoloji, Toplumsal Ekoloji gibi yeni alanlar oluşmuştur. Çevresel adalet akımları da doğal dünya üzerinde baskı kurulmasını daha genel bir toplumsal baskı ve denetim olgusunun bir parçası olarak görmekte; çevre sorunları ile yeterli biçimde ilgilenmenin daha genel toplumsal adalet sorunlarına yönelmemizi gerektirdiği savunulmaktadır. (Des Jardins, 2006: 466-467). Thomas Berry, insanın doğayı yok edip en sonda kendini de yok ettiği yaklaşım olarak tanımladığı Teknozoik yaklaşımın karşıtı olarak Ekozoik yaklaşımı tanımlamıştır. Özenle ve saygıyla oluşturulmuş, insan-yeryüzü ilişkisinin hem doğayı hem de insanı karşılıklı olarak iyileştireceği ekozoik yaklaşım kullanılarak yeryüzü sistemlerinin yenilenip onarılabileceğini iddia etmektedir (Berry,1999). İnsan ve doğanın karşılıklı birbirine bağımlı olduğu fikrinin kabulü ile insanın sorumluluğu tekrardan gündeme getirilmektedir.

Çevre merkezli etiğin yeryüzü etiği yaklaşımından sonra önemli çevre sorunlarına neden olmuş birtakım değerlerin ve yaşam biçimlerinin sorgulandığı Derin Ekoloji ideolojisi felsefe ortamlarında tartışılır olmuştur. Ekosistemin kirletilmesi ve kaynakların tüketilmesine karşı savaş verilmesi gerektiğini savunanların sığ ekoloji akımı içinde tanımlanabileceklerini vurgulayan Naess, insanın merkezde olmadığı bütüncül yaklaşımı ise derin ekoloji olarak tanımlamıştır. İnsanın, yaşadığı doğal ortam içinde diğer varlıklardan ayrılamayacağını vurgulayarak derin ekoloji kavramının ilkeleri arasında, sadece insanın değil ekosistemde yer alan her şeyin değerli olduğunun kabul edilerek türlerin varlığının sürdürülmesi; insanların çevreyi yok etmeksizin ve ekosistemdeki dengeyi bozmaksızın yaşamaları için zorunlu ihtiyaçlarını karşılamaları; çevreye müdahalede bulunan insanların bundan rahatsızlık duymaları; endüstri toplumu koşulları gereği maddeci, faydacı ve rekabetçi hale gelen yaşam felsefesinin değiştirilmesi; ekonomik ve ideolojik kurumları etkileyecek değişikliklerin yapılması hususlarını saymaktadır (Naess,1994:9-16).

Derin ekoloji yaklaşımı, tüm evreni özne olarak kabul etmekte ve sadece insanları dikkate alan toplum sözleşmesi yerine bir doğa sözleşmesi oluşturulması gerektiğini savunmaktadır. Ekosfere insan türünden daha fazla bir içsel değer atfederek toplumsal yaşamı da içine alacak önermelerle toplumun adem-i merkezileştirilmesinin ve tabana dayalı demokrasi ile yönetilmesinin uygun olacağını belirtmektedir (Ertürk,2009:89).

Derin ekoloji, ekosistem içinde yer alan canlı, cansız tüm varlıkların herhangi bir şeyin öznesi olmaksızın sırf kendi var oluşlarından dolayı bir değere sahip olduklarını, insanın da bu kapsamda diğer varlıklardan hiçbir farkı olmadığını; çevre sorunlarının insan merkezci yaklaşımdan kaynaklandığını ve insanın doğaya müdahale etmemesi gerektiğini savunan; ekolojik sorunların birincil sorumlusu olarak insanı gören bir yaklaşımdır. Bu felsefi düşüncede insanın çevre sorunlarına yönelik yapıcı, onarıcı, geliştirici davranışlarına hiç değinilmemektedir.

iii. Toplumsal Ekoloji

Derin ekolojistler, insanın doğada yer alan diğer canlı ve cansız varlıklardan üstün bir tarafının bulunmadığı ve ekolojik sorunların tek sorumlusu olduğu görüşlerinden dolayı, Bookchin tarafından baskıcı ve insan karşıtı bir felsefenin savunucuları olarak suçlanmıştır. Bookchin, insan varlığının ussal yeteneklerinin küçümsenmesini ve diğer varlıklarla eşit özelliklere sahip olduğu fikrini reddetmektedir. İnsan, doğal evrim ile ekosistem içindeki diğer varlıklardan farklılaşmış; önemli özelliklere sahip olmuş ve evrim sürecinin yönünü belirleyebilme kapasitesine sahip olmuştur. İnsanın sahip olduğu akıl yürütme, alet yapma, teknoloji tasarlama, sembolik bir dil aracılığıyla iletisim kurma kapasitesinin biyosferin "iyiliği" için de kullanılabileceğini vurgulamaktadır (Bookchin,1994:44)'den aktaran (Ünal,2010:121).

Bookchin, insan dışındaki doğal fiziki ortamı anlatmak üzere biyolojik/birinci doğa; insanlık tarafından geliştirilen ussallık, kültür ve toplum özelliklerini anlatmak üzere de toplumsal/ikinci doğa terimlerini kullanmıştır. Bu iki doğanın birbirlerinden tamamen ayrı olmadığını; ikinci doğanın birinci doğa üzerinde gerçekleştirildiğini; toplumsal doğanın doğal evrimin bir sonucu olarak gerçekleştiğini belirtmektedir. Bookchin, geleneksel ideolojilerin, tahakkümü "doğa yasası" yakıştırmasıyla meşrulastırmakta olduklarını söylemektedir. Oysa toplumsal ekoloji bakış açısıyla yapılan incelemelere göre, hiyerarşi bir bütün olarak ikinci doğaya yani topluma ait toplumsal bir kavramdır. Hayvanlar arasındaki tahakküm iliskileri hiyerarşi ile açıklanamaz çünkü, hayvanlar arasındaki tahakküm, insan topluluğunda yer alan seçkinler topluluğunun baskı ve sömürüsünden farklıdır. Hayvanlar yönetmek amacıyla kurumsallasmamıştır, kurumsallasmıs şiddet biçimleri de

bulunmamaktadır. Bu nedenle hiyerarsi ve tahakküm zoolojik değil, toplumsal kavramlardır (Bookchin,1994:33). İnsanın "birinci doğanın" gelişimine yapabileceği olumlu ya da olumsuz katkının yine insan tarafından kurulmuş olan toplumun özellikleri ile ilgili olduğunu düşünmektedir. İnsanın gerçekleştirdiği tüm eylemleri ile, birinci doğa içinde yer alan bir varlık olduğunu ancak bunun, insanın gerçekleştirdiği tüm faaliyetlerinin zorunlu olarak ortaya çıktığı ve tahakkümün meşru olduğu anlamına gelmeyeceğini savunmaktadır (Bookchin, 2014:51).

Toplumsal hiyerarşi ve baskı kalıplarının doğayı baskı altına alma sonucunu doğurduğunu; yüksek derecede hiyerarşik yapıya sahip toplumların doğal çevrelerini kötüye kullanma ve ona zarar verme olasılıklarının yüksek olduğunu savunmaktadır (Des Jardens,2014:457). Bu yaklaşıma göre, toplumla doğayı karşı karşıya getiren sorunlar toplumsal gelişmeden kaynaklanmaktadır (Önder, 2002:70). Bookchin, ekolojik sorunların insanlığın doğayı sömürmesi ve hükmü altına alması gerektiği yolundaki kavrayıştan; bu kavrayışın ise, erkeğin ataerkil ailede kadını sömürmeye ve kendi hükmü altına almaya başlamasına kadar uzanan insanın insan üzerindeki tahakkümü ve sömürüsünden kaynaklanmakta olduğunu belirtmektedir. Toplumsal tahakkümle ortaya çıkan hiyerarşiler, sınıflar, mülkiyet biçimleri ve devlet kurumları gibi kavramlar, insan doğa ilişkisinde de kullanılmaya başlanmıştır. Zaman içinde doğa da acımasızca sömürülecek bir kaynak, bir hammadde olarak görülmeye başlanmıştır (Bookchin, 1996:45'den aktaran Ünal,2010:115). Doğanın sadece sömürülecek bir hammadde kaynağı olarak görülmesi, günümüzde yaşamakta olduğumuz önemli çevre sorunlarının başlıca nedenleri arasında sayılmaktadır.

Bookchin'e göre, insanın doğa üzerinde egemenlik kurması ahlaki değildir ve ekolojik dengenin çökmesine yol açmaktadır. Doğal çevrenin yıkımının önlenmesi için insanın doğa üzerindeki egemenliği kaldırılmalı ve ekolojik bir topluma en uygun yapısal temel oluşturulmalıdır (Bookchin, 1981:55'den aktaran Cantzen,2015:230). Bookchin, doğanın çok çeşitlilik içeren, ögelerinin birbirini tamamlama ilkesine göre kurulmuş adem-i merkeziyetçi bir yapısı olduğunu ve hiyerarşik bir kademelenme göstermediğini savunmaktadır. Buradan hareketle toplumun da çeşitlilikler içermesi, merkeziyetçi olmaması, ögelerinin hiyerarşik yapıda olmaması, bunun yerine birbirlerini tamamlayacak

şekilde düzenlenmeleri gerektiğini dile getirmektedir (Bookchin,1985:58'den aktaran Cantzen,2015:232).

Bookchin'in toplumsal ekoloji fikri ile, ekolojik sorunlara kısa vadede ve pragmatist yaklasan reformcu çevrecilikten tamamen farklı olarak köktenci bir bakıs açısı getirilmektedir (Ünal, 2010:115). Bookchin'in, yüksek derecede hiyerarşik yapıya sahip toplumların doğal çevreye zarar verme olasılığının yüksek olduğu düşüncesinin tam tersine Gruhl, doğal çevrenin korunabilmesi ve sınırlı doğa kaynaklarının verimli kullanılabilmesi için tüm iktidar ve güç kaynakları ile donatılmış ve zorunlu durumlarda insanların özgürlüklerini kendi istekleri ile kısıtlamalarını sağlayabilecek otoriter bir dünya hükümetinin iş başında olması gerektiğini belirtmektedir. Ekolojik zorunluluklardan ötürü merkeziyetçiliği, bireylerin hayatına diktatörce müdahaleyi ve temel hakların ilgili taraflarca kararlaştırılarak ortadan kaldırılabileceğini savunmaktadır (Gruhl, 1978:289-299'dan aktaran Cantzen, 2015:226).

Günümüzde iklim krizini doğuran insan ve çevre ilişkisindeki yanlış varsayımlar gözden geçirilmeli ve daha sonra ekozoik yola uygun olarak insan-yeryüzü ilişkisini karşılıklı olarak iyileştirmek üzere eskiden beri uygulanmakta olan kurallar yeniden keşfedilmeli ya da yeni kurallar konulmalıdır. Etik yaklaşımın benimsenmesi ile içinde yaşadığımız dünyanın yaşam destek sistemlerindeki bozulmaların onarılması için kurallar, kurumlar ve uygulamalar geliştirmek üzere gerekli adım atılmış olacaktır. Ekozoik bakış, gezegenimizde çok çeşitli ve farklı kademelerde özneler olduğunu; geleneksel toplulukların ekozoik inançla doğaya saygılı davrandıklarını kabul etmektedir. Çeşitliliğe, çokluğa ve farklı amaçlara ve sonuçlara dikkat çekerek basitleştirmeye karşı çıkıp demokratik normları desteklemektedir (Brown&Schmidt,2014:94).

1.2.2.4. Sürdürülebilirlik Kavramı

Çevre etiği yaklaşımları ve çevre merkezli çevre etiği kapsamındaki tartışmalardan da anlaşılacağı üzere pek çok durumda çevre sorunlarına kesin etik çözüm yaklaşımları getirmek oldukça zordur. Felsefi olarak gerçekleştirilmeye çalışılan bir ilke, bir grubun yararına iken başka bir grubun zararına olabileceği, ya da sonucun net olarak kestirilemeyeceği durumlar meydana gelebilmektedir. Bu tür durumlarda çevreci

pragmatizm olarak adlandırılan, ahlaki çoğulculuğa uygun olarak orta yolu benimseyen, uzlaşmacı yaklaşımlar benimsenebilmektedir.

Dünya üzerinde insan nüfusunun çok hızlı bir şekilde artması çevre üzerinde olumsuz etkiler yaratmıştır. Kimi çevreciler, nüfus artışındaki patlamanın çevre üzerinde yıkımlara neden olduğunu savunurken kimileri de asıl sorunun gelişmiş ülkelerin tüketime dayalı yaşam biçimlerinden kaynaklandığını öne sürmektedir. Özellikle küreselleşme olarak adlandırılan 1980 sonrası yaşanan büyük değişim, ulaşım ve tüketimi artırmış, çevrenin tahribatı, kaynakların hızlı tüketimi sonuçlarını doğurmuştur. Tüm canlı ve cansız varlıkların, mevcudiyetlerini sürdürebilmeleri için günümüz modern dünyasındaki yaşam şartlarının pek çoğundan vazgeçilmesini; doğal kaynakların girdi olarak kullanılıp bilimsel ve teknolojik yöntemler ile üretim yapılmasını ya da teknolojik gelişmelerin durdurulmasını gerektirebilmektedir. Mevcut yaşam şartlarından vazgeçmenin mümkün olmadığı göz önünde bulundurularak uzlaşmacı, pragmatik bir yaklaşım olarak sürdürülebilir kalkınma kavramı kullanılmaya başlanmıştır.

Tüm canlıların içinde yaşadıkları, birbirleri ile ve doğal kaynaklarla etkileşim içinde oldukları ortamın yani çevrenin bozulması tüm canlıların hayatını zorlaştırıp kimi durumlarda imkânsız hale getirecek niteliktedir. İnsan varlığının sürdürülebilmesi için, içinde diğer canlı ve cansız varlıklarla birlikte yaşamakta olduğu çevrenin uygun koşullarının bozulmaması gerekmektedir. İnsanlığın sürdürülebilirliği için insanların da bir parçası olduğu ekosistemin sürdürülebilirliği önceliklidir. Ekosistem olmaksızın ne insanların sosyal iş birliği olabilir ne de bireysel konular var olabilir (Schultz,2010:209). Sürdürülebilirlik kavramı, insan toplumunun çevresel güvenlikle ile ilgili temel kaygısı ve ihtiyacından ortaya çıkmıştır (Brown, 2008:142).

Çevre ile ilgili konular doğrudan ele alınmadığı için çevre sorunlarını gündeme getirecek bazı otoritelere ihtiyaç vardır. Çevre ne üreticidir ne de tüketicidir. Tüm insanlar yok edildiğinde çıkarlar anlamsız hale geleceği için çıkar elde etmenin bir anlamı ve değeri kalmayacaktır. Eğer firmalar çevreye öncelik vermezlerse ve uluslar üstü şirketler iş yaptıkları devletlerin kurallarına uymazlarsa bu şirketler ve devletlerin ortak bir anlaşmaya uygun olarak işlerini yürütmesine zorlayacak ve formüle edecek bazı uluslararası kuruluşlara ihtiyaç olacaktır. Bu kuruluş, çeşitli şirketlerin ve ekonomilerin eylemleri gezegen üzerinde

yaşayan tüm insanları etkilediği için, dünya üzerinde yaşayan her insandan sorumlu olacaktır (Schultz, 2010:215).

Canlı ve cansız varlıkların kendi aralarında etkileşimde bulunarak varlıklarını devam ettirebilmeleri için son dönemlerde sıklıkla kullanılır olan sürdürülebilirlik düşüncesi, 1960'lı yıllarda modern dünyada hüküm süren kalkınmacı ideolojinin yol açtığı sorunlar ve 1970'li yıllarda gelişmeye başlayan çevre hareketleri sayesinde olmuştur (Bozlağan,2010:1015). 1960'lı yıllar öncesinde kalkınma amaçlı her eylem meşru sayılıyor, çevrenin tahrip edilmesi sorgulanmıyordu. Çevre sorunlarına kalkınmanın doğal ve katlanılması gereken sonuçları olarak bakılıyordu (Özer,2017:78).

Modern teknoloji ve sanayi devrimi çevre ile tüm canlıların içinde yaşadığı ekosistem arasındaki çatışmayı hızlandırmıştır. İnsanların çevre üzerinde oluşturduğu tahribat ekosistemin varlığı için bir tehdit olmuştur. İnsanlarca kurulan sistemlerin boyutları büyüdükçe etkileri de küresel boyuta ulaşmıştır. Dünya üzerindeki mevcut ekosistemi bozma kapasitesine sahip ilk canlı türü insandır (Schultz,2010:211). Endüstri devrimi ile birlikte insanın yaşadığı çevredeki doğal kaynakları kullanmaya başlaması, özellikle küreselleşme olarak adlandırılan 1980 sonrası yaşanan büyük değişimle birlikte, tüketim toplumunun oluşması, çevrenin canlıların yaşamlarını sürdüremeyeceği bir duruma gelmesi ve doğal kaynakların tükenmesi sonuçlarını doğurmuştur. Hayatın sürdürülebilirliği için doğal ortamın korunması gerektiğine inananların büyük çoğunluğu şu an yaşamakta olan insanların ve gelecek kuşakların menfaatlerini korumak isteğindedir (Özer, 2017:78).

Kaynakların aşırı tüketiminden duyulan kaygı ve oluşan çevre kirliliği, bilinçli yöneticilerde ve bilim insanlarında endişeye oluşturmuştur (Uz, 2020:15). Massachusetts Teknoloji Enstitüsü'ne (MIT) yaptırılan ve 1972 yılında "Limits to Growth" (Türkçe'ye Ekonomik Büyümenin Sınırları biçimde çevrilmiştir.) adıyla yayımlanan çalışmada, ekonomik gelişme ile çevre arasında son derece önemli ve güçlü bir ilişkinin bulunduğu gündeme getirilerek, çevresel sorunlara dikkat çekilmiştir. Mevcut gelişme politikalarının varlığını devam ettirmesi halinde, yaşanacak hammadde kıtlığı ve çevre sorunları nedeniyle insanlığın yok olma tehdidi ile karşı karşıya kalacağı vurgulanmıştır (Meadows ve d., 1973).

1967'de insanlığın ortak mirası kavramı kullanılmaya başlanmıştır. 1980'ler ve 1990'larda kaynakların kötü kullanımı ve diğer çevre sorunları ile mücadele amacı ile

önemli sözleşmeler imzalanmıştır (Held-1,2014:205-207). 5-16 Haziran 1972 tarihinde İsveç'in başkenti Stockholm'de düzenlenen Birleşmiş Milletler İnsani Çevre Konferansında (Stockholm Konferansı) kabul edilen İnsani Çevre Bildirgesi'nde, "çevrenin taşıma kapasitesine dikkat çeken, kaynak kullanımında kuşaklararası hakkaniyeti gözeten, ekonomik ve sosyal gelişmenin çevre ile bağlantısını kuran ve kalkınma ile çevrenin birlikteliğini vurgulayan ilkeler", sürdürülebilirlik düşüncesinin temel dayanaklarını ortaya koymuştur (IULA-EMME, 1997:3). Şimdiki ve gelecek kuşaklar için insani çevrenin geliştirilmesi amacının gerçekleştirilmesi, bütün düzeylerdeki insanlar, topluluklar, girişimler ve kuruluşların sorumluluk yüklenmesini gerektirdiği; ulusal hükümetlerin ve yerel yönetimlerin kendi yetki alanları ve sınırları içinde kapsamlı bir çevre politikası ve eylemi konusunda büyük sorumluluğa sahip olduğu; gelişmekte olan ülkelere kendi yükümlülüklerini yerine getirebilmeleri için gerekli yardımların yapılması ve çevre sorunlarının aşılması için uluslararası iş birliğinin önemi vurgulanmıştır (UN, 1972).

1970'li yıllarda Birleşmiş Milletler tarafından çevreye dikkat çekmek üzere gerçekleştirilen çalışmalar 1980'li yıllarda da devam etmiştir. Birleşmiş Milletler, ekonomik gelişme, çevrenin korunması ve gelecek kuşaklar sorunlarına yönelik incelemeler yapmak üzere kurul başkanının soyadı ile anılan Brundtland Komisyonunu oluşturmuştur. Brundtland Komisyonu, ulusların dünya üzerindeki yaşamı sürdürerek, ekonomik gelişmelerini de sağlayabilecekleri uzun vadeli stratejiler üzerinde yoğunlaşmış ve 1987 yılında Brundtland Raporu, diğer adı ile Ortak Geleceğimiz adlı raporu yayımlamıştır (WCED,1987). Raporda, gezegen üzerinde pek çok türün yaşamını tehdit eden çölleşme, asit yağmurları, sera etkisi, kuraklık, ozon tabakasının delinmesi, besin zincirinin bozulması, suyun yetersiz hale gelmesi gibi sorunlar dile getirilmiştir. 1970'li yıllardan itibaren yaşanan hızlı ekonomik büyüme paralelinde hammadde kullanımının hızla arttığı; son dönem yaşanan teknolojik kazalar neticesinde ortaya çıkan zehirli gaz, nükleer sızıntı, akarsulara karışan kimyasallar, içme suyu ve gıda yetersizliği gibi olumsuz durumlardan bahsedilmiştir. Raporda insan faaliyetleri sonucu gezegenimizde yaşamı tehdit eden tehlikelerin meydana geldiği ve bu durumun farkına varılması ve yönetilmesi gerektiği; yaşayan canlı bir organizma olarak algılanabilecek dünyamızın, yine insanlar tarafından kurtarılabileceği vurgulanmıştır. İlk kez Ortak Geleceğimiz adlı bu raporda tanımlanan ve

sıklıkla kullanılan sürdürülebilir kalkınma, bugün yaşamakta olan kuşağın gereksinimlerini, gelecek nesillerin kendi ihtiyaçlarını karşılama yeteneğini ortadan kaldırmaksızın karşılamasına olanak tanıyan bir kalkınma türüdür (WCED,1987:16). İnsan eli ile meydana gelen çevre sorunlarının geçmişte yaşamış ve günümüzde yaşamakta olan insanların faaliyetleri sonucu oluştuğu akıldan çıkarılmamalıdır (Örs,1997:370).

1970'li yıllardan itibaren uluslararası toplantılarda ve sonuç raporlarında kalkınma çalışmaları ile meydana gelen çevre sorunlarını gündeme getirerek insanın ve diğer canlıların hayatlarına devam edebilmeleri açısından kullanılmaya başlanan sürdürülebilirlik kavramı daha sonraki dönemlerde daha çok sürdürülebilir kalkınma olarak kullanılmaya başlanmış ve ekonomik sistemlerin sürdürülebilirliği ön plana alınmaya başlanmış sürdürülebilir çevre kavramı daha geri planda kalmıştır.

"Sürdürülebilirlik" terimi insan ve içinde yaşamını sürdürdüğü ekosistemin dengeli duruma geldiği nihai hedef olarak görülmelidir; "sürdürülebilir kalkınma" terimi ise sürdürülebilirliğin son noktasına götürecek bütünsel yaklaşım ve zamansal süreçleri ifade etmektedir (Shaker,2015:305). İnsan neslinin ve dolayısı ile diğer tüm canlı cansız varlıklardan ve fiziki olaylardan meydana gelen çevrenin sürdürülebilirliği için temel prensip, bugünkü nesillerin ihtiyaçları için gerçekleştirilmekte olan gelişme çalışmalarının, gelecek nesillerin kendi ihtiyaçlarını karşılama yeteneğini ortadan kaldırmaksızın karşılamasına olanak tanıyacak şekilde gerçekleştirilmesi gereken sürdürülebilir kalkınmadır. Sürdürülebilir kalkınma, ekonomik büyümenin, çevrenin korunmasının ve sosyal adaletin sağlanmasını gerçekleştirebilecek bir kalkınma türü olarak açıklanmaktadır. Sürdürülebilir kalkınma güvenlikle çok yakından ilişkili olduğu için doğru koşullar göz önünde bulundurulduğunda toplum en sonunda sürdürülebilirliğe doğru bir ilerleme kaydedebilecektir (Brown, 2008:149).

Sürdürülebilir kalkınma kavramı, ilk ortaya atılışından itibaren farklı gruplar tarafından farklı şekillerde tanımlanmıştır. İktisatçılar tanımlamalarında daha çok yaşam standartlarının korunması gerektiğini ön plana çıkarırken çevrebilimciler doğal çevrenin korunmasını, sosyologlar ise toplumların sosyolojik bağlarının ve karşılıklı ilişkilerin korunmasını ön plana çıkaran tanımlamalar yapmışlardır. Bu çalışmanın konusu itibarı ile, ekonomik ve toplumsal sürdürülebilirlik yerine, canlı ve cansız varlıkların mevcudiyetinin

sürmesi için gerekli desteği sağlayan doğal çevrenin nitelik ve niceliğine odaklanan çevresel sürdürülebilirlik ön planda tutulmuştur. Sürdürülebilir kalkınma ve sürdürülebilirlik ifadeleri ile kastedilen, çevresel sürdürülebilirliktir.

Bugünkü nesillerle gelecek nesillerin arasındaki en büyük dayanışma gelecek nesillere miras bırakılacak sağlıklı ve dengeli bir çevreden oluşan yaşanılabilir sorunsuz yerleşim yerleri, doğayla, yaşamla dost teknoloji, etik ilkeler bağlamında yapılandırılmış sürdürülebilir siyasal, sosyal, kültürel, ekonomik sistemlerdir (Akkoç,2014:10). Sürdürülebilir kalkınma kavramı bizi gelecek kuşaklara karşı yükümlülük altına sokan bir etik içerik taşıdığından, bu yaklaşıma göre; gelecek kuşakların refahlarını azaltan ya da yok eden bir davranış, bugünkü kuşaklara fayda sağlıyor olsa bile etik açıdan iyi bir davranış olarak kabul edilmemektedir (Ergun, Çobanoğlu,2012). Sürdürülebilirlik anlayışı, bugünkü kuşakları, sadece gelecek nesiller için yükümlülük altına soktuğu ve doğayı yine kaynak olarak algıladığı dikkate alındığında, etik açıdan insan merkezli, yarattığı sonuçlar bakımından ise canlı ve çevre merkezli etik değerlere de hizmet ettiği söylenebilir (Ergun, Çobanoğlu,2012).

Günümüzde gerçekleştirilmekte olan toplumsal, ekonomik, siyasi faaliyetler içinde en öncelikli olanı bu faaliyetleri sürdürecek olan insanlığın ve dolayısı ile içinde yaşadığımız fiziki çevrenin uzun vadeli sürdürülebilirliğinin sağlanmasına yönelik eylemler ve politikaların belirlenmesi ve uygulanmasıdır.

2015 yılında BM'e üye tüm devletler tarafından 2030 Sürdürülebilir Kalkınma Gündemi kabul edilmiştir. Bu gündem içinde, yoksulluğu sona erdirmek, gezegeni korumak ve her yerde herkesin yaşamını ve beklentilerini iyileştirmek üzere evrensel eylem çağrısı olarak tanımlanan sürdürülebilir kalkınma hedefleri yer almaktadır. Sürdürülebilir kalkınma hedefleri, herkes için daha iyi ve daha sürdürülebilir bir gelecek elde etme planı olup yoksulluk, eşitsizlik, iklim değişikliği, çevresel bozulma, barış ve adalet dahil olmak üzere karşılaştığımız küresel zorlukları ele almaktadır. Ekonomik ve sosyal hedefleri de kapsayan 17 hedef arasında, herkesin temiz suya erişiminin sağlanması, güvenilir, sürdürülebilir ve modern enerjiye erişimin sağlanması, sürdürülebilir tüketim ve üretim kalıplarının sağlanması, iklim değişikliği ve etkileriyle mücadele için acil önlemlerin alınması, dayanıklı altyapı oluşturulması, okyanusların, denizlerin ve deniz kaynaklarının korunması ve

sürdürülebilir şekilde kullanılması, ormanların sürdürülebilir bir şekilde yönetilmesi, çölleşmeyle mücadele edilmesi, arazi bozulmasının durdurulması ve tersine çevrilmesi, biyolojik çeşitlilik kaybının durdurulması ve sürdürülebilir kalkınma için küresel ortaklığın canlandırılması gibi çevre merkezli çevre etiği bağlamında değerlendirilebilecek hedeflere de yer verilmiştir (UN,2015).

1.3 SİBER GÜVENLİK KAVRAMLARI

1970'li yıllardan itibaren yaşanmaya başlanan Üçüncü ve Dördüncü Sanayi Devrimleri ile bilişim teknolojileri ürünleri modern toplumların hayatının her alanında kullanılmaya başlanmış ve tüm dünya ağlarla birbirine bağlı hale gelmiştir. Bu dönemde bilişim sistemlerini ve ağlarını ilgilendiren kavramları adlandırmak üzere siber ön ekli sözcükler sıklıkla kullanılır hale gelmiştir. Ülkemizde de sadece teknoloji alanında değil, siyasi, hukuki, askeri, ekonomik, toplumsal tüm alanlarda siber uzay, siber dünya, siber ortam, siber güvenlik gibi terimler hemen hemen her kesim tarafından sıklıkla kullanılmaktadır. Türk Dil Kurumu Sözlüğünde Türkçe bir karşılığı bulunmayan' siber' sözcüğü karşılığı olarak kimi durumlarda 'sanal' sözcüğü kullanılmaktadır. 'Sanal 'sözcüğünün Türk Dil Kurumu Sözlüğündeki karşılığı "gerçekte yeri olmayıp zihinde tasarlanan, mevhum, farazi, tahminî" şeklindedir. Siber sözcüğü ile anlatılmak istenenin sadece zihinde tasarlanmakla kalmayan farazi, tahmini bir varlık olmadığı çoğu durumda elle tutulur gözle görülür varlıklar olduğu göz önünde bulundurularak uluslararası literatürde kullanıldığı şekli ile doğrudan siber sözcüğünün kullanımı tercih edilmiştir. Merriam-Webster çevrimiçi sözlükte siber sözcüğünü, "bilgisayarlara veya İnternet gibi bilgisayar ağlarına dahil olan, bunlarla ilgili olan" şeklinde tanımlanmakta ve önüne eklenen sözcüğe teknoloji ve bilgisayarla ilgili olan anlamını kazandırmaktadır (Merriam-Webster,2021).

Bu bölümde, çevre etiğinin önemli aşamalarından biri sayılan 2015 yılında BM üyesi tüm devletler tarafından kabul edilmiş olan 2030 Sürdürülebilir Kalkınma Gündemindeki 17 madde ile yakından ilişkili olan siber güvenlik kavramı ve bu kavramla alakalı olan diğer bazı terimlerle ilgili bilgilere yer verilmektedir.

1.3.1 Siber Uzay-Siber Ortam-Siber Alan-Siber Dünya

Siber uzay, siber ortam, siber alan ve siber dünya terimleri sıklıkla birbirinin yerine kullanılabilmektedir. Siber uzay görünmeyen bilgiden oluşan ortamı anlatan bir kavramdır. Siber uzay kavramını ilk kez William Gibson, Neuromancer adlı romanında, bilgi kaynakları ve tüketicileri olarak insanları, makineleri ve diğer objeleri birbirine bağlayan bilgisayar ağlarını kapsayan saf bilgi alanını anlatmak üzere kullanmıştır. Bu alan, yüksek hareket kapasitesi imkanına sahip olup kullanıcılara siber uzayda gezinmek ya da sörf yapmak imkanı tanır. Gibson'un bu kavramsallaştırmasına uygun olarak bilgisayarların küresel ağını anlatmak üzere İnternet sözcüğü de kullanılabilmektedir (Kizza, 2007:284). Ancak internet sözcüğü, siber uzayı tam olarak anlatmada yetersiz kalmaktadır.

Başlangıçta, insan faktörü dışarıda bırakılarak siber uzay tanımları yapılmıştır. Bunlardan bazıları:

- Siber uzay internet, diğer fiziki ağlar, dijital servisler ve sanal gerçekliğin birleşimi ile oluşmuş çok kullanıcılı sanal bir ortamdır (Lehto,2015:7);
- Sayısal teknoloji altyapısına sahip cihazların kullanıldığı dünya siber uzay olarak anılmakta olup birbirlerine bağlı ve birbirleri ile haberleşebilen tüm bilgisayarları ve sayısal teknolojiye sahip donanımları kapsamaktadır (Sadowsky, 2003:16).

Daha sonra siber uzayın sadece yazılım, donanım, ağ ürünlerinden oluşmadığı bu ürünlerin yanı sıra insanın da siber uzay içinde yer aldığını belirten tanımlamalar yapılmıştır. Witheford, siber uzayı, bilgisayar ağları içindeki elektronik veri akışının oluşturduğu kavramsal bir boyut olarak tanımlamakta ve farklı nitelikteki inisiyatiflerin yer aldığı bir çelişkiler alanı olduğuna dikkat çekmektedir. Sadece bilgisayar ve ağ sistemlerinin değil bu sistemleri yaratıp işleten bilişim uzmanları, yazılım mühendisleri, programcılar, teknisyenler, bu sistemleri kullanan montaj ve büro işçileri, çevrimiçi hizmetler ve bu sistemle iş yapan herkesin siber uzayda yer almakta olduğunu vurgulamaktadır (Witheford, 2004:183-185). ITU'nun tanımına göre de siber ortam, kullanıcılar, ağlar, donanımlar, tüm yazılımlar, süreçler, işletilen, iletilen ya da saklanan bilgiler ile ağlara doğrudan ya da dolaylı olarak bağlanabilen sistemler, servisler ve uygulamalardan oluşur (ITU-T,2008:2). Siber uzay birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim ve/ veya etkileşimde

bulundukları soyut veya somut mekânı tarif eden bir kavramdır. Siber uzay, fiziksel bir varlığı bulunmayan, internetin ortaya çıkışı ve gelişimiyle insanların, kurum ve kuruluşların farklı teknolojiler vasıtasıyla bu sanal dünyaya bağlanmasıyla ortaya çıkan karmaşık bir yapıdır (Vigano, Loi, Yaghmaei,2020:158).

Siber dünya, donanım, yazılım ve bilişim sistemlerinin yanı sıra insanları ve sosyal etkileşimleri de kapsamaktadır. Siber dünya bilgisayarlar, veri ve bilgi ağlarının yanı sıra bu ağlardaki tam ve kapsamlı insan varlığını da içermektedir (Kuusisto, Kuusisto, 2015, s:33-34). Gerçekten de siber uzayda, bireyler, kurumsal yapılar, devletler, bu sistemleri kullanarak faaliyetlerini yerine getirmekte olan özel sektör kuruluşları, yine siber uzayın teknolojik olarak çalışır vaziyette tutulması görevini yerine getirmekte olan özel sektör firmaları, ve siber uzayın güvenliğinin sağlanmasına yönelik faaliyetleri yerine getirmekte olan çoğunluğu özel sektörde görev yapmakta olan bilişim sektörü çalışanları da yer almaktadır.

Jordan, siber uzayın başlangıcını, kablolar ve telefon hatların bilgisayarları birbirine bağlamaya başladığı döneme dayandırmakta ve fiziki dünyaya paralel bir dünyanın oluşturulduğunu belirtmektedir. Gerçek fiziki dünyaya paralel olarak gelişmekte olan bu sanal ortamın dokunulabilir somut özellikleri olmayan ışık ve elektronikten meydana geldiğini ve hepimizi kapsamakta olduğunu vurgulamaktadır (Jordan,1999:1-2). Siber dünyada insanlar fiziki olarak bulunmamakla birlikte bir bilgisayar aracılığı ile bu ortama bağlanabilmekte ve dilediği faaliyetleri bu bilgisayar aracılığı ile gerçekleştirebilmektedir. Bir bilgisayar kullanılarak ağlarla bağlanılan siber dünyaya bağlanmış olan diğer insanlarla etkileşimde bulunulabilmekte, alışveriş, bilgiye erişim, iletişim gibi pek çok eylem gerçekleştirilebilmektedir.

Siber uzay, coğrafi anlamda sınırsız, fiziksel olmayan, zaman, mesafe ve konumdan bağımsız olarak insanların kendi aralarında, insanlarla bilgisayarlar arasında ve bilgisayarlarla bilgisayarlar arasındaki işlemlerin gerçekleştiği ortamdır. Bir faaliyetin nerede ve ne zaman gerçekleştiğini, nereden başlatıldığını tam olarak zaman ve yer olarak saptamak imkansızdır. Homojen olmayan siber uzayda çok farklı şekillerde dijital etkileşim ve iletişim sağlayan bir sanal alandır (Adams vd.,2019:119). Siber dünya ile gerçek dünyanın zaman dilimi, mesafe, konum, bağlantı ve yetki alanları birbirinden farklıdır. Siber dünya

akışkan, giriş ve ifade etme engellerini azaltabilecek, kimlikleri gizleyebilecek ve sorumlulukları önleyebilecek niteliktedir. Bu ortam henüz yüz yüze gelinmemiş ya da araştırılmamış pekçok farklılıkları ve zorlukları da beraberinde getirmektedir (Hutchinson, 2015: 103).

Siber ve fiziki dünya iç içe geçmiş durumdadır. Fiziki dünya yerküre ve üzerinde bulunan tüm canlılar ve onlarla ilişkili tüm varlıklardan meydana gelmektedir. Bu tanıma göre siber dünya, üzerinde bulunan tüm canlılardan ve bilgisayarlar ve bilgisayar ağları da dahil cansız varlıklardan meydana gelir.

İçinde yaşadığımız fiziki dünya doğal yollarla meydana gelen bir ortam olup insanlar olmaksızın da varlığını sürdürebilecek niteliktedir. Oysa siber uzay, en azından günümüz şartlarında insanlar tarafından oluşturulmuş bir ekosistemdir ve insan varlığı ve insan faaliyetleri olmaksızın mevcudiyetini devam ettiremiyecektir (Lehto, 2015:5).

Siber uzay, henüz çok yeni bir kavram olduğu için güvenlik, düzen ve adalet konularında ciddi endişelere neden olabilecek hızlı nüfuz etme, bağımlılık ve anonimlik özelliklerine sahiptir. Bilgi ve iletişim teknolojilerinin kullanımı ile anlık küresel iletişimin sağlanmasına ve az ya da çok filtrelenmiş bilginin hızlı ve evrensel olarak yayılmasına imkân sağlamaktadır. Tüm kullanıcılar için hızlı bir şekilde bağımlılık yaratan siber uzayın kalıcı ve yaygın özelliklerinden birisi de kullanıcıların anonim olmasıdır. Siber uzayda kullanıcıların belirlenmesi, niyetlerinin anlaşılması, sorumluluk yüklemek, cevap verme ve orantılılığı sağlamak; bu anonim aktörlere uygun karşılıkları verebilmek zordur. Siber uzayda neyin güvenli olduğunu ve hangi güvenlik açıklarının daha çok sorun yaratacağını ve ne tür zararlar vereceğini, tehditlerin kimden ve nelerden kaynaklanacağını ve ne tür sorunlar yaratacağını tespit etmek çok zordur (Cornish,2017:4).

Siber uzay, insan yaratıcılığının ürünü, insanlar tarafından geliştirilmiş olmasına rağmen kara, deniz, hava ve uzay alanlarından etkilenen bir alandır (Brantly&Puyvelde,2018:88). Milyarlarca cihazın ağ üzerinden birbirleri ile bağlanması ile oluşan siber uzayın ilk katmanı olan fiziksel katman, kara, deniz, hava ve uzaya en yakın olup bu ortamlardan etkilenebilen kısımdır. Fiziksel katmanda yer alan bilgisayarların, sunucuların modemlerin, yönlendirici vb.nin fiziki olarak çalışabilmesi için elektrik kullanılması şarttır (Brantly&Puyvelde,2018:95). Siber uzayın etki alanı, fiziksel ortama

bağlıdır, yasal olarak yerel, ulusal, uluslararası düzenlemelerle yasal bir çerçeve içinde yer alır. Siber uzayın sanal özellikleri yanı sıra temel altyapısı fizikseldir Brantly&Puyvelde,2018:96). Siber uzayın mantıksal katmanı, her türlü donanımın çalışmasını ve diğer cihazlarla etkileşimini sağlayan kural ve kod kümelerini, yazılımları, yazılı talimatları içerir. (Brantly&Puyvelde,2018:98). Kişisel katman, bilişim sistemleri üzerinden etkileşime giren ve bu ağları kullanan insanlardan, işletmelerden, şirketlerden, kimliğini gizli tutan insan gruplarından insan davranışlarını taklit eden bilgisayar programlarından oluşmaktadır (Brantly&Puyvelde,2018:110).

Siber uzay, bir iş birliği ve iş geliştirme yeri olmanın yanı sıra aynı zamanda bir çekişme, saldırı ve çatışma yeridir de (Cornish, 2017:7). Özellikle internetin kullanılmaya başlanması ile fiziki dünyada fiziki sınırlarla birbirinden ayrılmakta olan ulus devletler, siber dünya üzerinde böyle sınırlar olmaksızın birbirlerine bağlanmak durumunda oldukları için ve herkesin kolaylıkla bağlanabildiği bir ortam olduğu için, pek çok faydanın yanı sıra pek çok güvenlik riskini de beraberinde getirmektedir.

1.3.2 Siber Güvenlik Tanımı

Yazının icat edildiği M.Ö. 4000 yıl öncesinden beri kullanılmakta olan bilgi güvenliği kavramı, toplumsal hizmetler ve işlemlerin büyük çoğunluğunun otomasyona geçirildiği ve birbirlerine bağımlı hale getirildiği günümüz dünyasında daha da önem kazanmıştır. Verilerin ve bilgilerin bilgisayarların üzerinde tutulmaya başlanması ile bilgisayar güvenliği; ağlarla bilgisayarların birbirlerine bağlanmaları ile ağ güvenliği, internet güvenliği, siber güvenlik gibi kavramlar sıklıkla kullanılmaya başlanmıştır. Vigano vd. siber güvenliği bir üst çatı olarak almış ve bu çatının altında bilgi güvenliği, uygulama güvenliği, ağ güvenliği, internet güvenliği ve kritik bilgi altyapılarının güvenliği olmak üzere 5 farklı kavramı listelemiştir (Vigano, Loi, Yaghmaei,2020:158).

Bilişim sistemlerinin kullanılmaya başlandığı ilk dönemlerde siber güvenlik dendiğinde akla ilk gelen bilişim sistemleri üzerinde tutulan, işlem gören, iletilen verilerin ve bilgilerin güvenliğinin sağlanması idi. Bilgi güvenliğinin unsurları olarak gizlilik, bütünlük ve erişilebilirlik sayılırken son dönemlerde bu üç unsur, siber güvenliğin sağlanmasında yetersiz kalmaya başlamıştır. Siber uzayda programlanabilir nesnelerin

artması, bilişim teknolojilerideki gelişmelere bağlı kritik altyapıların temel bileşeni haline gelen endüstriyel kontrol sistemlerinin ve bu sistemler üzerindeki bilginin güvenliğinin sağlanmasının yanı sıra insanların ve onların içinde yaşadığı fiziki ortamların da güvenliğinin sağlanması ihtiyacı doğmuştur (Perkins ve Byrnes, 2015).

Siyasi, askeri, ekonomik, hukuki ve teknik açılardan artık insanların yaşam alanı haline gelmiş bulunan siber uzayın güvenliği, bu farklı kesimler tarafından da farklı algılanmakta ve farklı tanımlar kullanmaktadırlar. Üzerinde anlaşılmış tek bir tanım bulunmamakla birlikte, siber güvenlik aşağıdaki şekillerde tanımlanabilmektedir:

- Siyaset bilimciler, siber güvenliği siber terörizmin önlenmesi ve milli varlıkların korunmasına yönelik bilgisayar güvenliği şeklinde algılamaktadır. Bu kişiler ekonomik, sosyal ve politik güvenlik açıklarının siber küredeki güvenlik açıkları ile paralel bir şekilde ortaya çıktığını savunmakta; sosyal karışıklık, kritik altyapılara yönelik saldırı tehditleri ve bilgi sistemlerinin kendilerine yönelik saldırılar üzerinde durmaktadırlar (Manjikian, 2018, s:36).
- Bilişim teknolojileri çalışanları ise siber güvenliği, sahibinin kim olduğuna ve kimler tarafından kullanıldığına bakılmaksızın siber uzaydaki tüm sistemlerin ve verilerin korunması şeklinde tanımlamaktadır (Manjikian, 2018:36).
- Siber güvenlik alanındaki önemli meslek örgütlerinden biri olan ACM Siber güvenlik eğitim dokümanında siber güvenliği, güvenli çalışmanın sağlanabilmesi amacı ile teknolojiyi, kullanıcıları, bilgiyi ve süreçleri kapsayan; güvenli bilişim sistemlerinin oluşturulması, işletilmesi, analizinin yapılması ve test edilmesi aşamalarını kapsayan bilgi işlem tabanlı bir disiplin olarak tanımlamaktadır. Siber güvenliğin hukuki, siyasi, insan faktörü, etik ve risk yönetimi boyutları olan disiplinler arası bir faaliyet olduğu vurgulanmaktadır (Burley, 2017, s:683)
- Uluslararası Telekomünikasyon Birliği (ITU) ise "Bilgi varlıklarını korumak amacı ile kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü" şeklindeki tanımı ile bilişim sistemlerinin korunmasına ek olarak bu amaçla kullanılmakta olan politika, yöntem, yaklaşım, eğitim gibi faktörleri de siber güvenlik tanımı kapsamına dahil etmiştir (ITU-T, 2008: 2).

- Ülkemizin 2016-2019 Ulusal Siber Güvenlik Stratejisinde siber güvenlik, "siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" olarak kapsamlı bir şekilde tanımlanmıştır (UDHB,2016: 7). Ulusal Siber Güvenlik Stratejisi 2020-2023'te de aynı şekliyle korunan bu tanımda, sadece siber uzayda yer alan bilişim sistemlerinin korunmasına yönelik faaliyetler vurgulanmıştır (UAB,2020: 14).

- Sağıroğlu (2018: 24), yukarıdaki tanımları birleştirerek "veri, işlem, süreç politika, deneyim, kapasite, insan ve sistemlerin güvenliğinin siber ortamda sağlanmasıdır" şeklindeki tanımı ile içinde yaşadığımız fiziki ve siber sistemlerin bir arada olduğu ve siber fiziki dünya olarak da adlandırılmakta olan günümüz dünyası için uygun bir siber güvenlik tanımı yapmıştır.

Siber güvenlik, kendi içinde bir altyapı haline gelmiştir. Bilgisayarlar ve ağlardan oluşan bilişim sistemlerini ve bu sistemler kullanılarak üretilen, edinilen, işlenen, iletilen ve saklanan verileri korumak üzere hizmet vermekte olan siber güvenlik altyapısı da koruduğu bu sistemler gibi küresel ve birbirine bağlı sistemlerden oluşmaktadır. Bilişim teknolojilerindeki gelişmelere paralel olarak siber güvenlik altyapısı da her geçen gün büyümeye ve gelişmeye devam etmektedir (Denning, 2003:1).

Görüldüğü üzere, bilişim sistemlerinin kullanılmaya başlandığı dönemlerde siber güvenlik dendiğinde akla ilk gelen bilişim sistemleri üzerinde tutulan, işlem gören, iletilen verilerin ve bilgilerin güvenliğinin sağlanması idi. Bilgi güvenliğinin unsurları olarak gizlilik, bütünlük ve erişilebilirlik sayılırken son dönemlerde bu üç unsur, siber güvenliğin sağlanmasında yetersiz kalmaya başlamıştır. Siber uzayda programlanabilir nesnelerin artması, endüstriyel otomasyon ve kontrol sistemlerinin kullanılmaya başlanması ile bu sistemler üzerindeki bilginin güvenliğinin sağlanmasının yanı sıra insanların ve onların içinde yaşadığı fiziki ortamların da güvenliğinin sağlanması ihtiyacı doğmuştur (Perkins ve Byrnes, 2015). Bilişim teknolojilerinin endüstriyel otomasyon ve kontrol sistemlerinin birlikte kullanılmaya başlanması gerçek fiziki dünya ile dijital dünya arasındaki çizgiyi

bulanıklaştırmıştır. Enerji üretim ve dağıtım hatları, petrol rafinerileri, su arıtma tesisleri vb. kritik altyapılarda bilişim teknolojilerinin her geçen gün artan bir şekilde yaygın olarak kullanılması bu ihtiyacı daha da görünür hale getirmiştir. Siber güvenlikte çerçeve genişlemiş olup sadece soyut bilginin güvenliği değil, tüm fiziki çevrenin güvenliğinin de sağlanması gerekmektedir.

Siber güvenlik alanında emniyet ve güvenlik birbirinden farklılık göstermektedir. Aşağıdaki şekilde görüldüğü üzere zarar insanlardan ya da deprem, yangın, sel, enerji kaybı, sabit disklerin bozulmaları gibi doğal afetlerden kaynaklanabilmektedir. İnsanların neden olduğu siber olaylar, insan hataları sonucu yanlışlıkla yapılan ya da kötü niyetli eylemlerden kaynaklanabilmektedir. Doğal afetler nedeni ile ya da insanların istemeden yaptıkları hatalar emniyet problemi olarak algılanmaktadır. Siber fiziki sistemlerin emniyetli olmaları, sistem çalışması durduğunda ya da hatalı çalıştığında insanlara ve diğer canlılara doğal ortama zarar verebileceği için çok önemlidir. İnsanların bilerek zarar vermek üzere yaptıkları eylemler ise güvenlik kapsamında ele alınmaktadır (Herrmann ve Pridöhl,2020:15).

Siber güvenliğin sağlanması bilişim sistemlerinin kullanıldığı sektörlere göre farklılık gösterse de her alan için temel bileşenler insan, süreç ve teknolojidir (Leclair, Burns,2018,s:70). Bayuk, bu temel bileşenleri de dahil ettiği üçlüyü aşağıdaki gibi özetlemektedir (Bayuk vd.,2012: 2-3):

i. Önleme, tespit ve karşılık verme*,* hem fiziki güvenliğin hem de siber güvenliğin hedefleridir. Tüm saldırılar önlenemeyeceği için planlama ve hazırlık aşamasının, devam etmekte olan saldırıların bir hasara neden olmadan önce tespit edilmesini sağlayacak mekanizmaları da kapsaması gerekmektedir. Tespit süreçlerinin devrede olup olmadığına bakılmaksızın, siber güvenlik kapsamında bir sistemin tehdit altında olduğu anlaşılır anlaşılmaz bu tür olaylara müdahale yeteneğine sahip olunmalıdır. Siber güvenlik alanında karşılık verme, fiziki güvenlik önlemlerinden farklı olarak tüm sistemin yeniden yapılandırılması ve kritik görevlerin kesintiye uğramadan devam ettirilmesi için sistemin iyileştirilmesi ve saldırıdan önceki durumuna döndürülmesi anlamında kullanılmaktadır.

ii. İnsan, süreç ve teknoloji, teknoloji alanında ve siber güvenlik yönetimi alanında, kullanılmakta olan yöntemleri anlatmaktadır. Sistemlerin çalıştırılmasında görevli operatörler, görevlerini belli kurallar çerçevesinde yerine getirmektedirler. Siber güvenlik

sadece teknoloji kullanılarak sağlanamaz. Sistemin siber güvenliğinin sağlanmasında diğer insanların faaliyetleri ve kararları da önemli rol oynamaktadır. Bu kişilerin tümü bireysel olarak güvenliği sağlama konusunda istekli olsalar da daha önceden bir plan yoksa hep birlikte koruma, tespit ve saldırı öncesi duruma dönüş aşamasında nasıl davranmaları gerektiğini bilemeyecektir. Bu nedenle güvenlik alanında çalışanların, mevcut organizasyonel süreçler içinde siber güvenlik hedeflerini gerçekleştirmek üzere teknolojiyi stratejik olarak kullanmaları gerekmektedir.

iii. Gizlilik, bütünlük ve erişilebilirlik, bilgiye özgü güvenlik hedefleridir. Gizlilik, bilgi sistemlerinin belirlenen yetkiler dahilinde kullanıma sunulması demektir. Bütünlük, kaydedilen ya da iletilen bilginin gerçekliğinin, doğruluğunun ve gönderen kişiye ait olduğunu gösterir. Erişilebilirlik ise bilginin ya da üzerinde tutulduğu, işlendiği, iletildiği sistemin istenilen her zaman erişilebilir durumda olması demektir. Gizlilik, bütünlük ve erişilebilirlik, kullanılmakta olan sistemin özelliklerine göre farklı oranlarda olması kabul edilebilir. Bazı sektörler için bilginin sürekli erişilebilir nitelikte olması önemli iken bazılarında sadece yetkili kişiler tarafından erişilir olması daha önemlidir.

Sonuç olarak yukarıdaki tanımlarda da yer verildiği gibi, siber güvenlik siber uzayda bilginin ve bilginin üzerinde işletildiği, iletildiği, saklandığı bilişim sistemlerinin gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olarak; insan, süreç ve teknoloji kullanımı ile devre dışı kalmalarının, hatalı çalışmalarının önüne geçmek için ve siber saldırılardan korumak için gerekli önlemleri almak, saldırıları önceden tespit edebilmek ve bir saldırı sonrası sistemi tekrar çalışır vaziyete getirmek için geliştirilmiş genel yöntemler topluluğudur.

1.3.3 Siber Güvenlik Olayları

Siber güvenliğin ihlal edilmesine yönelik olaylar, siber güvenlik olayı olarak adlandırılmaktadır. Ulusal Siber Güvenlik Stratejisi 2020-2023'te siber olayı, "bilişim sistemleri ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliğinin, bütünlüğünün veya erişilebilirliğinin ihlal edilmesidir" şeklinde tanımlanmıştır (UAB,2020).

Güvenlik politikalarının; güvenlik yöntemlerinin; kabul edilebilir kullanım politikalarının ihlali sonucu, bilgi sisteminin ya da sistem süreçlerinin gerçekleştirilmesinde kullanılan, saklanan, iletilen bilginin gizliliğini, bütünlüğünü, erişilebilirliğini riske atarak siber güvenliğin ihlal edilmesine neden olan olaylar siber güvenlik olayı olarak adlandırılmaktadır (NIST SP 800-82r2, 2015:C.1).

Siyasi, askeri, ekonomik tüm işlemler hızlı bir şekilde siber uzayda yerlerini almaya başladıkları için, sivil-askeri alan ayırımı ve ulus devletlerin fiziki sınırları da önemini kaybetmeye başlamıştır. Fiziki hasar oluşturma potansiyeline de sahip olması nedeni ile siber silah olarak değerlendirilebilen bilişim teknolojileri kullanılarak birbirine ağlarla bağlı siber uzayda zaman ve mekandan bağımsız olarak siber güvenliğin ihlal edilmesine yönelik kasıtlı siber olaylar yani siber saldırılar gerçekleştirilebilmektedir.

Bilişim suçlarındaki artış sonucu bir yandan bilgi ve iletişim teknolojilerine olan güven ve bağımlılık artarken bir yandan da her geçen gün daha dayanıksız olmakta ve siber uzaydan gelebilecek kötülüklere ve güvensiz ortama maruz kalınmaktadır. Telekomünikasyon, elektrik dağıtım şebekeleri, petrol ve gaz depolama, su dağıtım şebekeleri, ulaşım gibi her biri bir şekilde siber uzaya bağlı kritik altyapılar her geçen gün daha da güvenliksiz ve korunmasız hale gelmektedir. Siber uzay altyapısı ve iletişim protokolleri başlangıçtan itibaren güvenlik açısından zayıf oldukları, siber uzay kullanıcılarının büyük çoğunluğu, konu ile ilgili sınırlı bilgiye sahip olduğu, toplumun büyük çoğunluğunun tam olarak anlayamadığı bir teknoloji ve altyapıya bağımlı hale geldiği, siber saldırganlara hâlâ hoşgörü ile bakıldığı, bu siber olayların yetkili mercilere haber verilmesi zorunlu olmadığı için siber olaylar her geçen gün daha da artmaktadır. (Kizza, 2007,s:13-14)

Ulusal Siber Güvenlik Stratejisi 2020-2023'te bilişim sistemleri ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliğinin, bütünlüğünün veya erişilebilirliğinin ihlal edilmesi siber olay olarak tanımlanmıştır.

Siber güvenlik olayları sadece insanlar tarafından gerçekleştirilen siber saldırılar şeklinde değildir. Bu saldırıların yanı sıra, sistemlerin kullanıcıları tarafından kaza eseri ya da deprem, yangın, sel gibi felaketler sonucu da meydana gelebilmektedir. 2014 yılında IBM, sistemin yanlış yapılandırılması, yama yönetiminin düzenli yapılmamış olması, ilk

değer olarak verilmiş kullanıcı adlarının ve sistem şifrelerinin değiştirilmemiş olması, kolay tahmin edilebilir parolalar verilmesi, telefon ya da bilgisayarların kaybedilmesi, yanlış e-posta adresine bilgi gönderme gibi insan hatalarının tüm bilgisayar güvenliği olaylarının yüzde 95'i üzerinde etkili olduğunu açıklamıştır. Bu hatalar içinde en büyük oranın ise e-postalardaki veya web sitelerindeki kötü amaçlı bağlantıların aktif hale getirilmesi olduğu belirtilmektedir (IBM,2014).

Siber olayların etkileri belli bir ülke ile sınırlı kalmayıp bölgesel hatta küresel ölçekte hissedilebilir duruma gelebilmektedir. Bilgi ve iletişim teknolojileri altyapıları ve endüstriyel sistemler de zarar görebilmektedir. BİT altyapılarının birbirleri ile olan sistemik bağımlılığı nedeni ile yerel olarak gerçekleşen bir siber güvenlik olayı küresel nitelik kazanabilmektedir (Irion,2013:85).

1.3.4 Siber Güvenlik Açığı

Siber ortamda yer alan bir varlığın kendisini ya da yerine getirmekte olduğu faaliyeti olumsuz yönde etkileyerek işlevini hiç yerine getiremez ya da yanlış çalışır hale getiren ya da o varlığın yetkisi olmayan kişilerin eline geçmesine neden olabilecek zayıflıklar güvenlik açığı olarak adlandırılmaktadır Sistemin olağan durumu içinde yapması beklenen davranışı bozan durumlardır (Tabansky, 2017:212), (NIST SP 800-82r2, 2015:C-2). Siber ortamda faaliyet göstermekte olan bir yazılımın, donanımın ya da ağ sisteminin mevcut zayıflıkları ya da bu sistemde hasar oluşturulmasına yönelik istismarlar o sistemin güvenlik açıklarıdır (Panguluri, vd., 2017:144). Bir sistemin güvenliğini tanımlamakta kullanılan gizlilik, bütünlük ve erişilebilirlik unsurları ile tanımlanmakta olan bir sistemin güvenliğini olumsuz yönde etkileyebilecek güvenlik açıkları bir ya da daha çok tehdit tarafından kullanılabilir.

Bir saldırganın bir bilgi sistemine yetkisiz erişebildiği ve bilgileri bu sistem dışına çıkarabildiği tüm farklı noktalar saldırı yüzeyi olarak adlandırılır (Tabansky, 2017:212). Bu noktaların her biri saldırı vektörü olarak anılır. Seri ya da usb bağlantıya fiziksel erişim; sisteme farklı ağ protokolleri üzerinden bağlı altyapılara mantıksal erişim bir saldırı vektörü örneğidir. Saldırı vektörü, sıklıkla bir güvenlik açığı kullanılarak oluşturulur. Bir güvenlik açığı, bir ya da daha fazla tehdit kaynağı tarafından tetiklenerek ya da istismar edilerek olumsuz sonuçlar elde edilebilir (Tabansky, 2017:212).

Lehto, güvenlik açığını sistemde bir siber güvenlik olayının meydana gelebilme olasılığını artıran veya sonuçlarını şiddetlendiren içsel bir zayıflık olarak tanımlamaktadır. Güvenlik açıkları, insan eylemlerinden, süreçlerden ya da kullanılmakta olan teknolojiden kaynaklanabilmektedir (Lehto,2015:17). Siber uzayda, gerekli önlemler alınmadığı takdirde, bilgi içeriğinin bozulması, silinmesi; bilgi hırsızlığı ve kişisel bilgilerin kaybı; bilgi bütünlüğünün, ağ bağlantısı ve diğer ağ bağlantı cihazlarının bozulması riskleri vardır. Aslında siber uzaydaki tüm eylemler, sistem fonksiyonları programlanabildiği için önceden belirlenmektedir. Bir bilgisayara saldırılabilmesi için ya sistemin saldırgana erişim izni vermesi ya da bellek aşımı istismarı meydana gelmiş olmalıdır (Cavelty, 2008: 18-19). Bir endüstriyel kontrol sistemi içinde tehdit kaynağı tarafından tetiklenebilecek ya da istismar edilebilecek uygulama, iç kontrol ya da sistem güvenlik yöntemleridir.

Bir sistemdeki güvenlik açığının, o sistemin üreticileri tarafından tespit edilmesi durumunda üretici firma en kısa sürede bu güvenlik açığını giderici önlemleri alarak çözümü bu sistemin kullanıcılarına yama şeklinde gönderebilir. Sistemin güvenlik açığının güvenlik denetçisi tarafından tespit edilmesi durumunda bu açık gizli tutulmalı ve denetimin yapıldığı sistemlerin sahipleri haberdar edilmelidir. Ürün satıcısı, güvenlik açığından haberdar olmadığı durumda soruna yönelik çözüm geliştiremeyecektir. Bildirilmediği için uzun süre düzeltilmeden kalan güvenlik açıkları ‘sıfır gün’ veya ‘0 gün’ hataları olarak adlandırılmaktadır. Kimi durumlarda bu güvenlik açıkları tespit edildikten sonra devletlerin gizli servislerine, suç örgütlerine, rakip şirketlere vb. maddi çıkar karşılığında satılabilmektedir (Herrmann ve Pridöhl,2020:34).

1.3.5 Siber Tehditler

Bilişim teknolojilerinin yoğun kullanıldığı günümüz dünyasında karşılaşılma olasılığı bulunan olumsuz durumlar siber tehdit olarak adlandırılmaktadır. Toplum için hayati önem taşıyan sistemlere yönelik tehditler arasında, fiziki tehditler ve ekonomik tehditlerin yanı sıra siber tehditler de sayılmaktadır (Lehto, 2015). Günümüzde diğer pek çok kritik hizmette olduğu gibi enerjinin evlere ve işyerlerine dağıtımı, sağlık sistemlerinin etkin hale getirilmesi gibi hizmetlerin yerine getirilmesi, bilgi ve iletişim sistemlerinin güvenilir hale gelmesine bağlıdır. Bu kritik bilgi altyapıları, kamu hizmetleri, acil hizmetler

ve ticari işlemler için temel gereklilik kabul edilen kesintisiz veri değişimini sağladıkları için kritik altyapıların omurgası olarak görülmektedir. Bilgiye bağımlılık, en azından teorik olarak bilgi ve iletişim sistemlerini zafiyeti yüksek hedefler haline getirmektedir (Cavelty, 2008: 138).

Siber tehditler hedeflenen varlığa, tehdit kaynaklarına, kaynağa erişim motivasyonuna vb. çok farklı özelliklerine göre sınıflandırılabilmektedir. Tehdidin kaynağına göre yapılan sınıflandırmada insanlardan gelen tehditler kötü niyetli ve gerekli teknik bilgiye sahip kurum çalışanlarından, müşterilerden, satıcılardan, eski çalışanlardan kaynaklanan tehditler sıralanmaktadır. İnsan dışı tehditler arasında bilişim sistemlerinin zarar görmesine yol açabilecek yangın, deprem, sel, iklim değişikliği, kötü hava koşulları, elektrik, su gibi ihtiyaç duyulan kaynakların kullanılabilir olmaması gibi durumlar sayılmaktadır.

Siber tehditlerin kaynağa erişim motivasyonuna göre yapılan sınıflandırmasında Cavelty'nin yapısal modeli de kullanılmaktadır (Cavelty,2010)dan aktaran (Lehto,2015). Bu modele göre ;

- **Birinci seviye siber vandallık, hackleme ve hactivizm.:** Tek bir şirket ya da tek bir kişinin gerçekleştirdiği saldırı türü.
- **İkinci seviye siber suç:** Bilişim sistemleri kullanılarak gerçekleştirilen suçlar.
- **Üçüncü seviye siber ispiyonaj:** Bilişim teknolojileri kullanılarak bireylerden, rakiplerden, gruplardan, devletlerden, düşmanlardan kendi haberleri olmaksızın, siyasi, askeri, ekonomik kazanç elde etmek üzere hassas, patentli ya da gizliliği olan bilgilerin temin edilmesi.
- **Dördüncü seviye siber terörizm:** Kritik bilgi ve iletişim sistemlerine, bilişim teknolojileri kullanılarak halkta korku, panik oluşturma yoluyla siyasi liderlere taleplerini kabul ettirmek üzere teröristler tarafından gerçekleştirilen saldırılar;
- **Beşinci seviye siber savaş:** Evrensel kabul görmüş bir tanımı bulunmamakla birlikte, stratejik siber savaş, taktik/operasyonel siber savaş ve düşük yoğunluklu çatışma olmak üzere 3 sınıfa ayrılmaktadır.

Cavelty, siber tehditlerin tam anlamı ile gerçek hale gelmediğini ancak karar vericilerin siber tehditleri gerçek saldırı olarak algıladıklarını ve bu algı paralelinde kararlar almakta olduklarını savunmaktadır. Gerçekleşme ihtimali düşük tehdidin gerçek hayatta sorunlara neden olabildiğini, bu nedenle karar vericilerin doğru ile gerçek arasında uygun davranışı saptayabilme ikilemi ile karşı karşıya kaldıklarını belirtmektedir (Cavelty, 2008: 143).

1.3.6 Siber Saldırılar

Ulusal Siber Güvenlik Stratejisi 2020-2023'te siber saldırı, "siber uzayda yer alan bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" şeklinde tanımlanmıştır (UAB, 2020). Casusluk, sabotaj, hırsızlık gibi tüm siber saldırılar, gizlilik, bütünlük ve erişilebilirlik özelliklerinden birine ya da birkaç tanesine odaklanılarak gerçekleştirilmektedir (Brantly&Puyvelde,2019:168).

Siber saldırı, hedef bilgisayar sistemlerinin, ağların, ya da bu sistemler ve ağlar üzerinde yer alan ya da iletilen bilgilerin ve programların değiştirilmesi, yok edilmesi, bozulması ya da ele geçirilmesi maksadı ile gerçekleştirilen siber operasyonlar anlamına gelmektedir. Bir siber saldırı, göreceli olarak önemsiz verilerin yok edilmesi ya da kısa bir süre için tali bilgisayar sistemlerine erişimi engelleyebileceği gibi çok gizli askeri planları değiştirebilir ya da hava trafik kontrol sistemi, enerji şebekeleri, gibi kritik sistemlerin işleyişini bozabilir (Lin, 2013:17-18).

Altyapılara yönelik olarak gerçekleştirilecek bir siber saldırı ile, kinetik bir saldırının gerçekleştirebileceği boyutta fiziksel hasarlar meydana getirilebilir ve ciddi boyutta zarara yol açabilir. Siber saldırıları gerçekleştirenler genellikle arkalarında iz bırakmadıkları ve konumlarını gizlemeye özen gösterdikleri için saldırganları belirlemek oldukça zordur. Çoğu durumda siber saldırganlar her yerde bulunabilecek bilişim teknolojileri ürünlerini kullanarak saldırılarını gerçekleştirmektedirler. Bilişim teknolojilerine erişiminin kolaylaşması ve bu teknolojilerinin hem kamu kurumlarının hem de özel kuruluşların

işletilmesindeki rolünün hızla artması güvenlik zaaflarını daha da arttırmaktadır (Bıçakçı vd., 2015:3).

T.C. İçişleri Bakanlığı tarafından hazırlanan Güvenlik Terimleri Sözlüğünde, "Teknolojik açıdan gelişmiş ülkeler, diğer ülkelerin eğitim, ulaşım, haberleşme, barajlar ve nükleer santraller gibi kurumsal altyapıları hedef alınarak önemli kayıplara neden olabilecek siber saldırılar gerçekleştirebilecek kapasiteye sahiptir." ifadesi yer almaktadır (T.C. İçişleri Bakanlığı, 2017:63). Ancak, sadece teknolojik açıdan gelişmiş ülkelerin değil, ücreti karşılığında bu teknolojiyi kullanan kişilerin, terörist grupların ya da diğer ülkelerin de hedefleri doğrultusunda kritik altyapılara saldırıları gerçekleştirebileceği değerlendirilmektedir.

Gerçek dünyadaki güvenlik ile siber uzaydaki güvenlik arasındaki temel farklar, siber uzaydaki güvenlik ihlallerinin çok hızlı gelişmesi; fiziki olarak çok uzak bir konumdan, bir siber uzayda güvenlik ihlali yaratılabilmesi; siber uzayda güvenlik sorumluluğunun birden çok aktöre bağlı olmasıdır (Sadowsky,2003: 23).

Siber uzayın kuralları henüz tam anlamı ile belirlenmediği için sahadaki unsurlar arasında etkin iletişim kanallarının kurulması ve bunların uyum içinde çalışması için zorlu bir mücadele gerekmektedir (Bıçakçı, 2016:109).

Siber uzay, ABD, Rusya, Çin, İngiltere, Fransa gibi gelişmiş ülkeler tarafından orduların güç kullanma açısından hedef ve araç olarak da kullanılmaktadır. Siber uzayda düşman tarafın bilgi sistemlerini ve ağlarını devre dışı bırakmaya ve kullanılamaz duruma getirmeye çalışılmaktadır.

Erik Gartzke ise, siber saldırı araçlarına ve oluşturacakları yıkım ve ölüme neden olma gibi sonuçlara çok fazla odaklanıldığını ancak harekete geçebilecek kişilerin güdülerine yeterince odaklanılmadığını belirtmekte ve rakiplerine siber ortamda zarar verme kapasitesine sahip aktörlerin çoğunun yeterli nedenlere sahip olmadıkça harekete geçmediğini savunmaktadır (Gartzke,2013:57). Siber saldırıların bir elektrik şebekesini kapatarak saldırıya uğrayan tarafa bir maliyet getirebildiğini ancak bu hasarın uzun süreli bir zarar olmadığını ve düzetilebilecek nitelikte olduğunu belirtmektedir (Gartzke,2013:57).

1.3.6.1 Siber Saldırı Yöntemleri

Siber uzay, fiziki katmanın yanı sıra mantıksal katman ve kişisel katmana da sahip olduğu için siber saldırgan hedefine yönelik olarak bu katmanları ayrı ayrı kullanabildiği gibi birlikte de kullanabilmektedir.

Siber saldırılar, gerçekleştirildikleri ortama göre ağ, veri, erişim ve bilgisayar bağlantılı saldırılar; yarattıkları sonuçlar açısından, çok az derecede hasar, sınırlı hasar, geniş kapsamlı hasar, felaket ile sonuçlanan saldırılar şeklinde gruplanabilmektedir.

Gerçekleştiriliş biçimleri, bilişim teknolojilerindeki gelişmelere ve saldırıda bulunan kişilerin, grupların, devletlerin yaratıcılığına göre hızlı bir şekilde değişmektedir. Her gün yenileri ortaya çıkmakta olan siber saldırıların en çok bilinen türleri şunlardır (Altınsoy,2008:21):

- Dağıtık Hizmet Engelleme (DDOS) Saldırıları,
- Hizmet Dışı Bırakma,
- Başkasının bilgisayarını ağ üzerinden yönetme,
- Yanıltma, trafiği başka yöne yönlendirme,
- Sahte saldırılar,
- Ağlarda geçici kesinti yaratma,
- Sabotaj,
- Engelleme,
- Veri trafiğinin izlenmesi,
- Hizmetlerin kötü niyetli kullanılması,
- Yetkisiz erişim,
- Casusluk,
- İstenmeyen e-posta iletisi,
- Sosyal mühendislik, oltalama.

1.3.6.2 Siber Saldırı Aracı Olarak Kullanılan Zararlı Yazılım ve Donanımlar

Günümüzde kullanılmakta olan zararlı yazılımların en önemli ortak özellikleri arasında, etkilerini artıracak yeni özelliklerin eklenmesini kolaylaştırmak üzere modüler

yapıda olmaları; çok güçlü ve yıkıcı etkileri olması; gelir kaynağı olarak kullanılmaları; talebe uygun arz yaratılması; bazı değişiklikler ve eklemelerle piyasaya yeniden sürülerek ve hızlı bir şekilde yayılmaları sağlanarak yaşam döngülerinin devam ettirilebilmesi; zararlı yazılım geliştiriciler arasında iş birliğinin yanı sıra rekabet ortamının da bulunması; saldırıda bulunulan hedefin sahibinin haberi olmaksızın gizlice gerçekleştirilmesi; İnternet ortamının, zararlı yazılımların yayılmasında ve etkinliğinin artmasında önemli bir ortam olması sayılmaktadır.

Siber saldırı amacı ile kullanılmakta olan basit yazılımlar, ortalama 125 satırlık koddan oluşmaktadır. Ulus devletler tarafından kullanılmakta olan daha karmaşık ve etkili kötü amaçlı yazılımlar ise 15.000 satır civarında olabilmektedir. Saldırı amaçlı kullanılan yazılımın ne olduğunu ve nasıl geliştirildiğini ve nasıl kullanıldığını araştırmak saldırganın niyetini anlamada ve bazı durumlarda saldırganın kim olduğunu anlamakta yardımcı olabilmektedir (Brantly ve Damien,2019:170).

Siber güvenliğe yönelik en etkili saldırı araçlarından bazıları aşağıda yer almaktadır:

- **Virüsler:** İçinde bulundukları program çalıştırıldığında, kendi kendilerini, çalıştırılabilir programlar içine, disklere, sürücülere, dokümanlara kopyalayarak çoğaltan program parçalarıdır. Temel özellikleri, bir dosyadan ötekine, bir bilgisayardan diğer bilgisayara, kullanıcısının bilgisi ve rızası olmadan kendi kendini kopyalayarak çoğaltmasıdır (Belous ve Saladukha, 2020:101).

- **Solucanlar:** Kendilerini ağ üzerinde bilgisayardan bilgisayara kopyalayarak çoğalan bağımsız bilgisayar programlarıdır. Ağların çökmesine, bağlantıların yok olmasına, sistemlerin çalışmaz hale gelmesine neden olabilecek bu yazılımlar ağ ortamında e-posta yolu ile yayılmaktadırlar (Esterle vd.,2005:24). Solucanlar tüm dünyada yayılabilen, sadece kişisel programları değil tüm sistemleri etkileyebilen virüslerdir. Son zamanlarda internetin küresel alanda yaygınlaşması ile aynı anda 40 milyon bilgisayara birden bulaşma olasılığı olduğu için, bu tür güvenlik ihlali en önemli tehditler arasında sayılmaktadır (Belous, Saladukha, 2020:101).

- **Truva Atları:** Yazılım içinde, yazılımın asıl gerçekleştirmesi gereken fonksiyon dışında başka fonksiyonları gerçekleştirmek üzere eklenmiş program parçalarıdır. Özellikle ağ güvenliği ile ilgili programlar içine yerleştirilerek sistemin güvenlik açısından

zayıf noktalarının tespit edilmesini sağlamak üzere kullanılabildikleri gibi virüslerin ve solucanların gizlenmesi amacı ile mantık bombaları olarak da kullanılabilmektedirler Gelbstein, Kamal, 2002:147).

- **Tuzak Kapılar:** Arka kapı olarak da adlandırılan bu oluşumlar, üretici firma tarafından varlığı tespit edilemeyecek şekilde sistemlere eklenebilecek ilave donanım ya da yazılımla gerçekleştirilebilecek mekanizmalardır. Üreticinin sistem üzerindeki mevcut yetkilendirmeyi devre dışı bırakarak sisteme nüfuz etmesini ve kendi isteği doğrultusunda kullanmasına imkan vermektedir. Üretici firmanın, müşterinin isteği doğrultusunda uzaktan erişimle sorunları gidermek için kullanabileceği bu uygulamalar, kötü niyetli kişilerce kullanıldığında önemli bir siber silaha dönüşebilecek niteliktedir. Saldırgan, bu tuzak kapıları kullanarak eriştiği bilişim sistemleri üzerinde verileri kopyalama, silme yok etme, uygulamayı durdurma gibi zararlı işlemleri rahatlıkla gerçekleştirebilir. Yine bu uygulama kullanılarak, eriştiği bilgisayar sistemine DDOS saldırıları gerçekleştirilebilir. Bir programın gizli bir bölümü olabileceği gibi başlı başına farklı bir program halinde hazırlanmış bir rootkit kullanılarak ya da sisteme istenen fonksiyonları gerçekleştirmek üzere sistem çökertilebilir (Panguluri vd., 2017:148)

- **Paket Koklayıcılar:** Bir ağda yer alan bilgileri tarayan, seçilen IP adreslerinden gönderilen ya da bu adreslere gelen verilerin hareketini ya da ağdaki mevcut veri trafiğini kontrol etmek üzere ayarlanabilecekleri gibi belirli sözcüklerle karşılaştıklarında aktif hale gelebilen programlardır. İstenen arama kriterlerine uygun gönderilen ve alınan tüm e-posta iletilerini ele geçirebilirler. Kullanıcı şifrelerini ele geçirmede ve mesajlara erişmede kullanılabilirler (Esterle vd.,2005:20-21).

- **İstismar (exploid) Yazılımı:** Genellikle etkilenen bilgisayara yetkisiz erişime izin veren bir yazılım hatasından kaynaklanan güvenlik açıklarıdır (Brantly ve Puyvelde,2018:173)

- **Casus Yazılımlar:** Genellikle zararsız gibi görünen ve internetten ücretsiz indirilen bazı uygulamalar aracılığı ile bulaşan program parçacıkları olup temel hedef, yerleştikleri bilgisayardan giriş yapan kullanıcıların hangi sitelere, ne kadar süre ile bağlandığı bilgilerinden hareketle ilgili kullanıcının eğilimleri hakkında bilgi

edinebilmektir. Bu yazılımlar da üzerinde çalıştırıldıkları bilgisayarlardan diğer bilişim sistemlerine erişim ve saldırı başlatmak için de kullanılabilmektedir.

- **Fuzzing:** Bir yazılım içindeki güvenlik açıklarını bulmak üzere kullanılan tekniktir. Hedef yazılıma kasten kusurlu giriş yapılarak hatanın bulunması prensibine dayanır. Kusurlu veri girişi ile oluşacak durumlar test edilir; test verileri hedef yazılıma uygulanır ve yazılımdaki başarısız durumlar tespit edilir. Çok çeşitli veriler kullanılarak güvenlik açıklarının otomatik olarak bulunması sağlanır (Panguluri vd. 2017:147).

- **nMap (Network Mapper):** Açık kaynak kodlu çok işlevli bir ağ tarama aracı olup temel olarak ağların keşfi ve güvenlik denetimi için IP bağlantı noktalarının hangi adreslerle eşleştiğini belirlemekte kullanılır. Bu yazılım ile ağda yer alan her cihazın açık bağlantı noktaları belirlenir. Her bağlantı noktası üzerinde çalışan servisler belirlenir; SCADA sistem üzerindeki güvenlik açıklarına yönelik testlere nereden başlayacağının belirlenmesinde; bilinmeyen bağlantı noktalarının belirlenmesinde kullanılır. nMapin bir üretim cihazının çalışmakta olduğu durumda, anormal bir sonuç yaratmaması için dikkatli kullanılması gerekmektedir (Panguluri vd., 2017:147).

- **Nessus:** Hedef sistemin uzaktan güvenlik taramalarının yapıldığı, güvenlik açığı içeren servisleri bulan ve her olası güvenlik açığı için uyarı seviyesini belirleyen açık kaynak kodlu bir yazılımdır. Bu yazılımın ürettiği rapor, sistemin test edilmesi ve istenen amaç doğrultusunda kullanılması için başlangıç noktası bilgilerini verir. Sistemin ele geçirilmesinde kullanılabilecek olası güvenlik açıklarını belirler. Nessus tüm güvenlik açıklarını belirleyemez ya da Nessus tarafından raporlanan tüm güvenlik açıkları da sistem için risk yaratacak boyutta olmayablir (Panguluri vd., 2017:148).

- **Rootkits:** Bulaştığı sistem her açıldığında aktif hale gelen zararlı bir yazılım türüdür. Sistemin hafızasına, işletim sisteminin kurulmasından önceki aşamada yüklendiği ve aktif hale getirildikleri için tespit edilmeleri zordur. Bir Rootkit kullanılarak gizli dosyalar, süreçler, gizli kullanıcı hesapları sisteme yüklenebilir. Terminalden ağ bağlantısından ve klavyeden veri girişini ve erişimi kesmek üzere kullanılabilmektedir (Panguluri vd., 2017:148).

- **Sosyal Mühendislik:** Siber güvenlik bağlamında yetkisiz faaliyetlerin gerçekleştirilmesi ya da gizli bilgiyi ifşa ederek insanların psikolojik olarak etkilenmesi sağlanır. Daha karmaşık bir dolandırıcılığın adımlarından biridir. (Panguluri vd.,2017:148).
- **Cross Domain Çapraz Etki Alanı:** İki ya da daha fazla sayıda farklı güvenlik alanı ve ağı arasında bilginin transferi ya da erişimini mümkün kılan yazılım ve donanımdan oluşan bütünleşik sistemlerdir.
- **Tersine mühendislik:** Elektronik sistemlerin kötü niyetli kullanımı için tasarım bilgilerinin edinilmesi sürecidir. Elektronik bir bileşenin ya da bilgisayar programının parçalara ayrılması ve her parçanın incelenerek işlevinin belirlenmesidir. Daha çok erişim sınırlandırmalarını aşmak amacı ile kullanılmaktadır (Panguluri vd., 2017:149).
- **Sql İnjection:** SQl, ilişkisel veri tabanı yönetim sistemi içindeki verileri yönetmek üzere tasarlanmış bir sistem yazılımıdır. SQL injection ise veri tabanı uygulamalarına saldırmak için kullanılan kod enjekte etme yöntemidir. EKS'lerinin pek çoğunda uygulama verilerinin saklandığı veri tabanı sistemleri bulunmaktadır. Bir SQL İnjection saldırısında zararlı SQL deyimleri gönderilir. Bu teknik, bir uygulamadaki güvenlik açıklarını kullanarak sisteme sızmak için kullanılır (Panguluri vd., 2017:149-150).
- **Man in the Middle Saldırısı:** İki grup arasındaki elektronik iletişim gizlice dinlendiğinde, iletişim geciktirildiğinde ya da bilgiler değiştirildiğinde bu saldırı türü gerçekleştirilmiş olur. Bu saldırıyı başarılı bir şekilde gerçekleştirmek için saldırgan kurban olarak belirlediği iki grup arasındaki mesajları kesebilmeli, içeriği değiştirebilmeli ya da yeni bir içeriği devreye sokabilmelidir (Panguluri vd., 2017:150).
- **BOTNETler**: Genellikle bilgisayar kullanıcısının ya da yöneticisinin isteği dışında faaliyetlerde bulunmak üzere bilgisayar sistemlerini kullanan yazılımlardır (Brantly ve Puyvelde,2018:172). Botnetler, sistem arka kapılarını kullanarak uzaktan kumandalı cihazlara veya diğer virüslü bilgisayarlara ve sunuculara yeniden bağlanmak için tasarlanmış kötücül yazılım parçalarının tasarlanması ve yayılmasıyla başlar. Bilinen güvenlik açıklarından yararlanan bu kötücül yazılım parçaları, internette veya hedeflenen ağda yayınlanır. Botnetler bir kez bir makineye bulaştıktan sonra etkisi üstel biçimde artacak bozulmalar oluşturabilecek niteliktedir. Güvenliği ihlal edilmiş cihazlar ve ağlar, topluca

harekete geçerek bu siber olayı başlatanların amaçlarına yönelik bir bilgisayar ordusu şeklinde işlevlerini yerine getirebilmektedir (Adams vd.,2019:121).

Başlıcaları yukarıda açıklanan bu siber saldırı araçları, ilk dönemlerde tek başlarına kullanılırken günümüzde daha etkili hale getirmek üzere birlikte kullanılarak gelişmiş sürekli tehditler oluşturulabilmektedir.

- **Gelişmiş Sürekli Tehditler (APT)**

Her geçen gün birbirine daha fazla bağlanan günümüz dünyasında siber saldırılar, fiziki olarak çok farklı bir yerden başlatılabilir ve içerden ya da dışarıdan herhangi biri tarafından gerçekleştirilebilir. Günümüzde en tehlikeli saldırı türlerinin başında Gelişmiş Sürekli Tehditler gelmektedir. Genellikle son derece kararlı rakip ulus devletler, ya da teröristler kritik altyapıları hedef alan saldırıları gerçekleştirmek üzere gerekli kaynaklara sahiptirler. Siber güvenlik olaylarının büyük çoğunluğu APT'leri içermektedir. APT'lerin tehdit aktörleri, kendi amaçlarına uygun özel hedefleri seçerler. Amaçları veri sızdırma, sabotaj ve/veya sürmekte olan bir işlemi sonlandırmak olabilir. Hedeflenen bir saldırıyı gerçekleştirebilmek için kontrol sisteminin ve /veya sürecin ayrıntılı tasarım bilgisine, tesise elektronik ya da fiziki erişimin nasıl gerçekleştirilebileceğine, sistemlerin ve süreçlerin işleyişinin bilinmesine, gerekli erişimi sağlamak üzere istismar edilebilecek güvenlik açıkları ve zafiyet bilgisinin edinilmesine ihtiyaç vardır (Panguluri vd., 2017:144).

APT, yani Gelişmiş Sürekli Tehdit, çok iyi finanse edilmiş saldırganın sistemlere sızmak için elindeki tüm olanakları ve gelişmiş araçları kullandığı; birden fazla sızma yöntemini birleştirerek saldırma işlemini gerçekleştirdiği; yavaş ve durum gözleme yöntemi kullanarak fark edilmeden sızma yöntemini kullandığı; bilinen ve otomatize edilmiş saldırı araçları kullanmak yerine insan faktörünü devreye sokarak saldırıyı gerçekleştirdiği bir yöntemdir.

APT'ler, hedef sistemler ne kadar iyi korunuyor olursa olsun birçok siber saldırı aracını ve güvenlik açıklarını bir arada kullanarak sistemi ele geçirebilirler. APT'ler sistemlere sızmak için İnternet üzerinden zararlı yazılım bulaştırma, fiziksel yol ile zararlı yazılım bulaştırma ve dış çevreden sisteme sızma yöntemlerini kullanırlar. İyi finanse edilen

saldırgan, sistemi koruyan diğer araçları aşmak yerine, iç tehdit unsurlarını ve güvenli bağlantıları kullanarak bunları kendine avantaj olarak kullanır ve sızma işlemini gerçekleştirir. APT'lerin amacı sistemlere yavaş bir şekilde sızıp orada olabildiğince fazla kalmaktır. Bir sistemden diğer sistemlere atlayarak yayılmak aynı zamanda bunu fark edilmeden yapabilmek APT'lerin genel özelliklerindendir. Uzaktan kontrol mekanizması saldırgan için hayati önem taşımaktadır. Uygun bir uzaktan yönetim teknolojisi olması durumunda saldırı gerçekleşebilecektir (https://lostar.com.tr/2014/11/advanced-persistent-threat-apt.html,2018). Saldırganlar, kayda değer hasar/yıkım ve hizmet verememe, uzun süreli hizmet alamama durumunda halkın paniğe kapılması gibi ikincil hasarlar yaratmak için SCADA/EKS'lerin nasıl etkileneceği ile ilgili bilgiye ihtiyaç duyarlar (Panguluri vd., 2017:145).

APT'ler, tüm dünyada her geçen gün artan ölçüde risk oluşturmaya devam etmektedir. Büyüyen ve gelişen tehditler, toplumun tüm kesimlerini etkileme potansiyeline sahiptir (Clark ve Hakim, 2017:4).

1.3.7 Siber Saldırganlar

Bir coğrafi alandaki olayların etkileri çok uzak mesafede olsa da farklı coğrafi alanlarda derin etkiler yaratabilecek niteliktedir. Bir yerde insanlar tarafından gerçekleştirilen küçük olaylar katalizör etki yaratarak başka yerlerde devasa sonuçlara neden olabileceği için bu olaydan ekonomik, toplumsal ve askeri faydalar sağlamak isteyen insanlar öngörülemez şekilde davranabilecektir. (Keohane ve Nye Jr.,2014:102). Geleneksel çatışma aktörlerinden farklı olarak, kötü amaçlı yazılımları oluşturma ve kullanma yeteneğine sahip siber saldırganlar, sadece devletlerin güvenlik güçleri ile sınırlı değildir. Yetenek seviyeleri farklılık göstermekle birlikte bireysel bilgisayar korsanları, suçlular, teröristler gibi çeşitli aktörler de siber saldırı araçlarını yazabilir, yeniden kullanabilir ya da satın alabilir (Brantly ve Puyvelde,2019:174). Siber uzayda en güçlü saldırganlar olarak devletler kabul edilmekle birlikte en yaygın tehdit grubunun devlet dışı aktörler olduğu iddia edilmektedir. Bireysel saldırganlar, organize suç örgütleri, ajanlar, siber teröristler gibi devlet dışı siber saldırganların kendi fiziksel güvenlikleri için çok az riskin bulunduğu siber

uzayda kendilerini geliştirmeleri için gerekli her türlü bilgi mevcuttur. Siber uzay, her türlü bilgiye erişilebilen, düşük maliyetlerle potansiyel üyelere ulaşılarak iletişim ve organizasyonların gerçekleştirilebildiği bir ortamdır. Devletler de siber uzayda düşük maliyetle güçlerini artırabilme olanağına sahiptir. (Brantly ve Puyvelde,2018:308).

1.3.7.1 Bireysel Saldırganlar

Bireysel saldırganlar, teknolojik bilgi seviyelerine ve saldırı amaçlarına göre üç grup halinde ele alınmıştır:

i. Hazır Yazılım Kullanan Çocuklar

Pek çok durumda saldırganlar, henüz ahlaki ya da sorumluluk gelişimleri tamamlanmamış çocuklar ya da gençlerdir. Bunlar İnternetten indirdikleri kullanıma hazır programlar kullanırlar. Kendi kendilerine saldırı programları yazamazlar. Çoğunluğu yakalandığında yaşları yasal olarak sorumluluk taşıma yaşından küçüktür. Çocuklar ve ergenler, eylemlerinin sonucunu değerlendirme kapasitesine sahip olmadıkları için bu tür saldırıları daha kolaylıkla gerçekleştirebilmektedir. Kullandıkları saldırı programlarını ve Truva Atlarını yazacak teknik bilgileri olmamakla birlikte bu saldırı araçlarını kullanma cesaretleri ve becerileri vardır. Yaptıkları saldırı sonrasında verecekleri zararın da çok farkında değildirler. Siber saldırıları para kazanma ideali olmaksızın zevk için ya da felsefi amaçlarla gerçekleştirenler siber hacktivisler olarak anılmaktadır (Clark ve Hakim,2017:4). Bu çocuklar büyüdükleri zaman bazıları bilgisayarlara karşı ilgisini kaybederken bazıları da sistem operatörü, ağ yöneticisi, kimileri de bilgisayar güvenliği konularında çalışmıştır. Fakat bazıları yaşları ilerleyince de suç işlemeye devam etmiştir. (Sadowsky, 2003: 198).

ii. Kötü Niyetli Çalışanlar

İşverenine karşı, intikam, kasıt, kötü duygu besleyen, taktik açıdan yetenekli çalışanlar da tehdit yaratmaktadır. Bilişim sistemlerine erişim yetkisine sahip kurum personeli ya da bu erişime yetkili olan yüklenici firma çalışanları tarafından siber saldırılar gerçekleştirilebilmektedir (Han ve Çelikpala,2016:78) Bazı durumlarda işine son verilen çalışanlar, daha sonraki dönemlerde işverenlerine ait bilgisayarlara Truva Atları ya da mantık bombaları yönlendirmektedir.

iii. Endüstriyel Casuslar

Bilgisayardan bilgi çalınması gün geçtikçe büyüyen bir pazardır. Bazıları, fidye karşılığında ya da tehditle bilgiyi asıl sahibinden almaya çalışır. Bazı saldırganlar da para kazanma amacı ile yasa dışı siber saldırılar ile firmaların ticari sırlarını ele geçirip rakip firmalara satmaya çalışmaktadır.

1.3.7.2 Organize Suç Örgütleri:

Çok büyük miktarda değerli veriler ve finansal bilgiler İnternet üzerinden iletilmektedir. Bu ortamda dolandırıcılık, korsanlık, kara para aklama gibi organize suçlar da mevcuttur. İnternet üzerinden iletişim, cinsel suçlar, pornografi, kumar, yasa dışı esrar-eroin trafiği, silah ticaretine de ortam yaratmaktadır. Yasal siteler de suçlular tarafından kendileri hakkında neler bilindiğini öğrenmek ya da yaptıkları suçların tanıklarını öğrenmek üzere hedef haline gelebilmektedir. Ağlar sayesinde küreselleşen dünyada İnternet her geçen gün daha da büyük oranda suç ortamı haline gelmektedir. (Sadowsky, 2003: 199)

1.3.7.3 İdeolojik ve Milli Ajanlar, Siber Teröristler ve Siber Savaşçılar

1993 yılında Rand Corporation'dan Arquilla ve Ronfeldt, komuta kontrol sistemlere sahip, uyumlu tek bir büyük ağa sahip ulus devletler arası gerçekleşen siber savaştan farklı olarak düşmanlar arasında, uluslararası teröristler, suçlular, radikal eylemciler gibi organize devlet dışı hacker toplulukların da bulunduğu, her biri kendi içinde istiklarlı ortak çıkarı ve bağlılıkları olan organize edilmiş çok sayıda küçük birimlerden oluşan yıkıcı grubu tanımlamıştır (Soesanto ve Smeets,2020:388).

Ulusal sorunlar, dini ya da ideolojik nedenlerle, haksızlığa uğradığını düşünerek intikam almak, bir hedefe ulaşmak, seslerini duyurmak ya da politik bir söylem geliştirmek çalışma karşıtlığı gibi nedenlerle protesto gibi amaçlara yönelik olarak siber uzay üzerinden saldırılar düzenleyen bireyler ya da gruplar siber terörist olarak adlandırılmaktadır.

Casuslar, hırsızlar ve sabotajcılar gibi siber teröristler, bilgisayar donanımlarına, enerji santralleri gibi kritik altyapıların kontrol sistemlerine erişmekte kullanılan bilişim ağlarına ve bilginin kendisine yönelik kanunsuz saldırılar ve tehditler

gerçekleştirebilmektedirler. Siber terörizm, bilgisayarların bilgiyi çalmak, bozmak ya da değiştirmek için kullanılmasını da kapsamaktadır. Saldırının siber terörizm olarak adlandırılması için insanlara, varlıklara karşı şiddet oluşturması ya da en azından genel bir korku yaratması gerekmektedir. Siber teröristler, saldırılarını sınırlı kaynaklarla küçük gruplar halinde uzak konumlardan gerçekleştirilebilmektedir. Siber terörist atakları arasında, bilişim sistemleri ağlarında zayıflıkları ve güvenlik açıklarını kullanan bilgisayar virüsleri, çalınan şifreler, iç itilaflar, tespit edilemeden sızma amaçlı arka kapı içeren yazılımlar ve bilgisayar sistemlerini kullanılamaz hale getiren elektromanyetik dalga trafiği de sayılmaktadır. Bilişim sistemlerinin fiziki bileşenlerine patlayıcı ya da elektromanyetik silici ile doğrudan saldırı da kullanılabilmektedir (Bennett, 2007:45-46).

Siber teröristler yeni teknolojileri ve ağları kullanarak hemen hemen hiçbir fiziki risk oluşturmadan saldırılarını gerçekleştirebilirler. Kimileri, siber terörizmi, teröristler tarafından yürütülen bilgi savaşı olarak tanımlarken kimileri de daha farklı bir olay olarak tanımlamaktadır. Siber terörizm, siber uzayda doğrudan ya da diğer saldırı türlerini kullanarak gerçekleştirilebilmektedir. Siber terörizm BT sistemlerine, personele ya da ekipmanına yönelik bilişim teknolojilerini kullanarak fiziki zarar meydana getirmeye odaklanır. Çeşitli kötü niyetli yazılımlar ya da donanımlardan oluşan siber silahlar hedefe yönelik çevrimiçi olarak kullanılabilir. Teröristler, saldırı amaçlı kullandıkları bilişim teknolojileri doğrudan siber silah olarak üretilmedikleri için, ağ içinde gerçekleştirmeyi hedefledikleri fiziki ya da teknik hasarın ölçüsünü iyi hesaplamaları gereklidir. BT ağları da bilgisayar ağlarından ayrı olarak hedef haline gelebilir. Zarar ve hasar yaratmak üzere tasarlanan siber saldırılar muhtemelen fiziki zarar yaratmayı amaçlayan operasyonları desteklemek üzere kullanılır. Birisinin kontrolü altındaki ağı ele geçirme bir başka siber operasyonu desteklemek üzere ya da başka bağımsız amacı gerçekleştirmek için yapılabilir.

Lehto, siber terörist tanımını saldırganların motivasyonuna göre farklılaştırmakta, temel motivasyonu maddi kazanç olanları siber suçlu; temel motivasyonu askeri hedefler olanları siber savaşçı; kendi saldırı gündemini belirleyenleri siber terörist olarak açıklamaktadır (Lehto, 2015:12-13). Hacker olarak kendi deneyimlerini test etmek isteyen, iyi organize olmuş, motivasyonları yüksek siber teröristler, SCADA teknolojilerine sahip firmaları hedef almaktadır (Alcaraz vd.,2015:6).

Siber saldırıları bir savaş türü olarak kabul eden devlet destekli ya da devlet dışı aktörler siber teröristler olarak anılmaktadır. Devletler ya da özel kuruluşlar tarafından gizlilik dereceli ya da tescilli bilgileri rekabette stratejik üstünlük sağlamak; güvenlik, finans ya da politika alanlarında avantaj elde etmek amacı ile çalanlar ya da çalma girişiminde bulunanlar da siber casus olarak adlandırılmaktadır (Clark ve Hakim,2017:4). Terörist gruplar, korku salmak ya da kendi amaçlarına dikkat çekmek üzere siber saldırılar düzenleyebilmektedir. Ulus devletler, terörist grupları, suçluları ya da bireyleri tolere edebilmekte, diğer devletlere karşı onları destekleyebilmektedir (Lin, 2013:18).

Dipert, bilişim teknolojilerindeki gelişmeler sonrası saldırı aracı olarak kullanılabilecek bilgisayar sistemlerine dikkati çekerek, bilgisayarları potansiyel silah; bilişim sistemleri ile ilgili ileri seviye bilgiye sahip kişileri ise potansiyel siber savaşçı olarak tanımlamıştır (Dipert, 2000:385).

Zamanla siber savaşlar internetin yaygınlaşmasıyla ivme kazanmıştır. İlk defa, Sun Tzu'nun "Düşmanı savaşmadan ele geçirmek" kavramının, şu anki çağdaş dünyasında sınırsız olan, bu güçlü yeni silahı kullanarak, güç elde edilir hale gelmiştir. Sınırların, gözle görülür kısıtlama veya yasaların olmadığı bu ortamda zaman içinde bilgi savaşı kavramı olgunlaşmıştır. Bilgi savaşının veya siber savaşın stratejik tarafının belirleyici bir taktiksel güce indirgenmesine neden olmuştur. Bu kuvvet, siber savaşın güçlendirici yönü, geleneksel savaşın önemli ve belirleyici bir bileşeni olsa da, geleneksel bilgeliğe karşı bu son olmamaktadır. Sadece siber savaşın stratejik yönünün başlangıcıdır (Sharma, 2010: 63).

1.3.8 Siber Terörizm ve Siber Savaş

Diğer siber güvenlik kavramlarında olduğu gibi siber terörizm ve siber savaşın da herkes tarafından kabul görmüş tek bir tanımları bulunmamaktadır. Bazı durumlarda birbirlerinden ayrıştırılmakta bazı durumlarda ise siber terörizm, siber savaş ile eş anlamlı kullanılabilmektedir.

Cavelty'nin yapısal modelinde, birinci seviyede tek bir şirket ya da tek bir kişinin gerçekleştirdiği saldırı türü olan vandallık, hackleme ve hacktivizmi; ikinci seviyede bilişim sistemleri kullanılarak gerçekleştirilen siber suçları; üçüncü seviyede bilişim teknolojileri kullanılarak bireylerden, gruplardan, devletlerden, düşmanlardan siyasi, askeri, ekonomik

kazanç elde etmek üzere hassas, patentli ya da gizliliği olan bilgilerin temin edilmesi yolu ile gerçekleştirilen siber ispiyonajı sayarken, siber terörizmi dördüncü seviyede; siber savaşı ise beşinci seviyede göstermiştir. Cavelty'nin tanımına göre dördüncü seviyede bulunan siber terörizm, kritik bilgi ve iletişim sistemlerine, bilişim teknolojileri kullanılarak halkta korku, panik oluşturma yoluyla siyasi liderlere taleplerini kabul ettirmek üzere teröristler tarafından gerçekleştirilen saldırılardır. Beşinci seviyede yer verdiği siber savaşı ise evrensel kabul görmüş bir tanımı bulunmadığını vurgulayarak, stratejik siber savaş, taktik/operasyonel siber savaş ve düşük yoğunluklu çatışma olmak üzere 3 gruba ayırmıştır (Cavelty,2010) dan aktaran (Lehto,2015).

Siber terörizm, terörist faaliyetlerin siber uzay üzerinden gerçekleştirilmesi ya da terör örgütlerinin siber uzayı kullanarak faaliyetlerini gerçekleştirmeleri olarak tanımlanmaktadır (Krasavin, Serge'den aktaran Yayla, M.,2014:195). ABD Federal Soruşturma Bürosu FBI siber terörizmi bilgisayarlara ve ağlarına çatışma, belirsizlik ve / veya sayısal hizmetlere zarar vermekle sonuçlanan bir suç olarak tanımlamaktadır. Siber terörizm ile politik, sosyal ve ideolojik amaçlarla geleneksel terör saldırılarında olduğu gibi sivil halk arasında kaos ve belirsizlik yaratma yolu ile bir devlet ya da vatandaşının gözünü korkutulabilmektedir. Siber teröristler hedef olarak sadece bilgi ve iletişim ve altyapılarını hedef alıp bunlara saldırıda bulunarak korku ve terör estirebilirler ya da diğer saldırı araçlarının etkisini artırmak üzere kullanabilirler (Lehto, 2015:12). Siber terör saldırıları, devlet kurumlarına ait internet sayfalarının ele geçirilmesinden, kritik bilgi altyapılarının çalışmaz hale getirilmesine ve bu yolla ekonomik ve maddî hasar oluşturulmasına kadar geniş bir yelpazede gerçekleşebilir Siber terörizm, bilişim teknolojilerinin politik olarak motive olmuş ulus-altı gruplar veya gizli ajanlar tarafından şiddet, bir toplumu etkilemek veya bir hükümetin politikalarını değiştirtmek maksatlı olarak şiddet oluşturmak üzere silah veya hedef olarak kullanılması şeklinde de tanımlanmaktadır. Siber terörizmi icra eden ulus-altı gruplar iken siber savaşı icra eden kişi grup veya organizasyonlar bir devlet tarafından yönlendirilmektedir (Yayla,2014:195).

Dünya devletleri, daha önce kara, deniz ve havada birbirine karşı mücadele verirken, 1950'li yıllardan itibaren uzay; 21. yüzyıldan itibaren ise siber uzay bu mücadele alanlarına eklenmiş ve bu ortamda da çatışmalar yaşanmaya başlanmıştır. Ulutaş, siber uzayda

meydana gelen ve değişik türde tarafları barındıran bu çatışmalar arasında bir ayırım yapmaksızın tümünü siber savaş olarak isimlendirmiştir (Ulutaş, 2018: 89).

1993 yılında Rand Corporation'dan Arquilla ve Ronfeldt siber savaşı, bilgi dengesini kendi lehine çevirmek amacı ile düşman bilgi ve iletişim sistemlerinin yok edilmese bile bozulmasına odaklanarak geleneksel karşıt komuta kontrol sistemler arası çatışma olarak tanımlamıştır (Soesanto ve Smeets,2020:388). Komuta kontrol sistemlerine sahip, uyumlu tek bir büyük ağa sahip ulus devletler arası gerçekleşen siber savaştan farklı olarak düşmanlar arasında, uluslararası teröristler, suçlular, radikal eylemciler gibi organize devlet dışı hacker toplulukların da bulunduğu, her biri kendi içinde istikrarlı ortak çıkarı ve bağlılıkları olan organize edilmiş çok sayıda küçük birimlerden oluşan yıkıcı grubun siber uzaydaki faaliyetlerini de netware olarak tanımlamışlardır (Soesanto ve Smeets,2020:388). Martin C. Libicki, siber savaşları amaçlarına göre, hedeflerine göre, kapsam ve uygulama düzeylerine göre sınıflandırmıştır. Libicki'ye göre siber savaşlar ya Stratejik Siber Savaştır ya da Operasyonel Siber Savaş'tır. Buna göre; bir ulusun ya da topluluğun, başka bir ulusun ya da topluluğun karar ve davranışlarını değiştirmek ve etkilemek adına başlattığı siber savaşlara Stratejik Siber Savaş denir. Arquilla ve Ronfeld'in aksine Libicki, saldırıyı gerçekleştiren devlet haricinde bir başka oluşum ya da kişi olsa da bunu siber savaş olarak tanımlamaktadır. Operasyonel Siber Savaş durumunda ise; savaş sırasında askeri düzeydeki veya askeri düzeye bağlı olan sivil hedeflere karşı doğru bir şekilde ve dikkatle kullanıldığında kuvvetli bir çarpan niteliği oluşturabilmektedir (Libicki, 2009: 117).

ABD'de siber güvenlik danışmanlığı yapan Richard A. Clarke ve eski Ulusal Güvenlik Konseyi çalışanı Robert Knake, "Cyber War" adlı eserlerinde, yıkıcı siber saldırılar ile elektrik üretim dağıtım tesisleri, hava trafik kontrol sistemleri, ulaşım ve taşıma sistemleri, petrol ve doğalgaz rafinerileri gibi kritik altyapılara yönelik siber saldırılar ile binlerce can kaybına yol açabilecek ve sıklıkla elektronik Pearl Harbour olarak adlandırılan bir senaryoya yer verilmektedir. Clark'a göre siber savaş; bir devletin, başka bir devletin bilişim sistemlerine veya ağlarına zarar vermek, sistemleri bozmak ya da yok etmek maksadıyla gerçekleştirdiği eylemleridir (Clarke ve Knake, 2010: 11). Siber savaş, ulus-devlet sınırları boyunca, saldırı ve savunma operasyonlarında, bilgisayarları kullanarak diğer bilgisayarlara veya ağlara elektronik araçlarla saldırmak için düzenlenen birimleri

içermektedir. Yazılım geliştirme ve bilgisayar ağlarının karmaşıklıklarını kullanma konusunda eğitim almış bilgisayar korsanları ve diğer kişiler bu saldırıların başlıca uygulayıcılarıdır. Bu kişiler genellikle ulus devlet aktörlerinin desteği altında faaliyet göstermektedirler (Billo ve Chang, 2004:3). Ulus Devletler, diğer ulus devletlerin özellikle ulusal kritik altyapılarına internet üzerinden zarar verme hedefi doğrultusunda faaliyetlerde bulunabilmektedir (Demiröz,2018:349).

Siyaset bilimci Thomas Rid, siyasi amaçlı tüm siber saldırıların savaş olarak kabul edilemeyeceğini, sabotaj, casusluk ve yıkımın farklı şekilleri olduğunu belirtmektedir. Ona göre, bir savaş eylemi, araçsal olmalı, siyasi olmalı ve ölümcül olma potansiyeline sahip olmalıdır. Siber saldırılar doğrudan ölümcül değildir ve saldırının başarılı sayılması için ölümcül olması gerekli değildir uygulamada hiçbir siber suç kimseyi yaralamamıştır. Rid, siber gücün kullanımının çok asgari düzeyde araçsal olduğunu ve bir siber saldırının düşmanları davranışlarını değiştirmeye zorlamada çok da yeterli olmadığını savunmaktadır. Rid son olarak da bir siber saldırının siyasi olarak atıf yapılmadığı durumda saldırının depolitize edildiğini söyleyerek bu tarz saldırıların siber savaş sayılamayacağını ifade etmektedir (Brantly ve Puyvelde,2018:275-276).

Öztürk, siber savaş ve siber saldırının anlam olarak benzerlik göstermelerine rağmen saldırı kavramı tek taraflılığı içerirken, savaşın iki ya da daha çok taraflılığı içerdiğini belirtmekte ve saldırıda mağdurların pasif ve savunma halinde olduğunu oysa savaşın her iki tarafın yönettiği, birden çok siber saldırıyı kapsadığını vurgulamaktadır (Öztürk, 2014: 24).

Küresel seviyede çok sayıda siber tehdidin mevcudiyetine rağmen büyük ölçekli siber savaşlar henüz yaşanmamıştır. Devletler, siber savaşı düşmanı yaralamak, zayıflatmak ve moralini bozmak için sabotaj ve casusluğun kullanıldığı asimetrik savaş biçimi olarak değerlendirmektedir (Mansbach ve Taylor,2018:493). Siber uzayın yetenekleri sayesinde ordularda birtakım dönüşümler yaşanmıştır. Askeri kurumlar beşinci boyut kabul edilen siber uzayı hesaba katarak askeri kurumlar ve doktrinler oluşturulmalı ya da uyarlanmalıdır. Batı toplumları için en belirgin tehdidin siber savaş değil siber suçlar olduğuna inanılmaktadır (Brantly ve Puyvelde,2018:296-297).

1.4 ÇEVRE ETİĞİ ve SİBER GÜVENLİK İLİŞKİSİ

Bu bölümde öncelikle güvenlik kavramı incelenmiş, 1990'ların öncesinde güvenliğin sadece ulus devletler arası bir kavram olduğu oysa günümüzde neoliberal politikaların uygulanması ve küreselleşme sonrası daha da belirgin olarak çevresel güvenlik, siber güvenlik gibi alanların da güvenlik kavramına eklemlendiği görülmüştür.

20. Yüzyılın başlarından itibaren üzerinde çalışılmaya başlanan uygulamalı etik kapsamında çevre etiğine ilişkin yapılan araştırma ile felsefeciler tarafından doğadaki canlı, cansız varlıkların ve işlevlerin tümünün, ahlaki değere sahip tek varlık olan insan için olduğunu savunan insan merkezli çevre etiği; insan dışındaki canlı varlıkların sırf doğada var oldukları için ahla1aki değere sahip olduğunu savunan canlı merkezli çevre etiği ile doğanın, ekolojik sistemin mevcudiyetinden dolayı kendi içinde, kendisi için bir değere sahip olduğunu savunan çevre merkezli çevre etiğinin geliştirildiği bilgisi edinilmiştir.

Ekosistemin kirletilmesi ve kaynakların tüketilmesine karşı savaş verilmesi gerektiğini savunanlar, sığ ekoloji akımı içinde tanımlanmış; insanın merkezde olmadığı bütüncül yaklaşım ise derin ekoloji olarak tanımlanmıştır. Derin ekoloji yaklaşımı, ekosistemde yer alan her şeyin değerli olduğunun kabul edilerek türlerin varlığının sürdürülmesi; insanların çevreyi yok etmeksizin ve ekosistemdeki dengeyi bozmaksızın yaşamaları için zorunlu ihtiyaçlarını karşılamaları; çevreye müdahalede bulunan insanların bundan rahatsızlık duymaları; endüstri toplumu koşulları gereği maddeci, faydacı ve rekabetçi hale gelen yaşam felsefesinin değiştirilmesi; ekonomik ve ideolojik kurumları etkileyecek değişikliklerin yapılması hususlarını kapsamaktadır. İnsan merkezli yaklaşımın doğadaki her şey insan içindir yaklaşımının da insanın doğadaki diğer varlıklardan hiçbir farkı bulunmadığı ve çevre sorunlarının tek sorumlusu olduğu derin ekoloji yaklaşımının da çok abartılı olduğu değerlendirilmektedir. Doğada var olan tüm canlı ve cansız varlıkların mevcudiyetlerinden dolayı bir değerleri olduğu ve varlıklarının sürdürülmesi gerektiği temel varsayımından hareketle, bütüncül çevre etiği yaklaşımı benimsenmiştir. Değer bakımından mevcudiyeti ile doğada yer alan diğer canlı ve cansız varlıklarla bir farkı olmadığı düşünülen insanın ahlaki ehliyeti olduğu ve yaptıklarından sorumlu tutulması gerektiği de kabul edilmektedir.

Bookchin'in de vurguladığı gibi insan, ekosistemdeki diğer varlıklardan farklılaşmış ve evrim sürecinin yönünü belirleyebilir duruma gelmiştir. Onun tanımına göre, insan dışındaki doğal fiziki ortam olan biyolojik/birinci doğa ve insanlık tarafından geliştirilen ussallık, kültür ve toplum özelliklerini kapsayan toplumsal/ikinci doğa vardır. Genel anlamda insan davranışlarının tamamı doğaya zarar verecek şekilde değildir; insan geliştirdiği teknoloji ile kendi ihtiyaçları doğrultusunda doğa üzerinde değişiklikler de yapmaktadır. Yazılım, donanım, ağ bileşenlerinden oluşan bilişim sistemleri ile bu sistemleri üreten, yöneten, kullanan, bu sistemlerden etkilenen insanlar ve kurumsal yapılardan oluşan siber uzay bu tanıma göre toplumsal/ikinci doğa üzerinde insan eli ile gerçekleştirilmiş bir katman olarak yer almaktadır. Siber uzayda, dünya üzerindeki ulus devletlerin fiziki sınırlarının bir önemi yoktur. Faaliyetler, zaman ve mekân kavramlarından bağımsız olup istenilen zaman aralığı ayarlanarak çok uzak mesafelerden başlatılabilmekte, sürdürülebilmekte ve sonlandırılabilmektedir. İnsan davranışlarının tamamı doğaya zarar verebilecek nitelikte olmadığı gibi siber alanda da insanlık ve canlı cansız diğer varlıklar yararına pekçok faaliyet gerçekleştirilmektedir.

Bookchin, toplumsal/ikinci doğada yer alan toplumsal hiyerarşi ve baskı kalıplarının doğayı baskı altına alma sonucunu doğurduğunu; yüksek derecede hiyerarşik yapıya sahip toplumların doğal çevrelerini kötüye kullanma ve ona zarar verme olasılıklarının yüksek olduğunu savunmaktadır (Des Jardins,2014:457). Bu yaklaşıma göre, toplumla doğayı karşı karşıya getiren sorunlar toplumsal gelişmeden kaynaklanmaktadır (Önder, 2002:70). Bookchin, ekolojik sorunların insanlığın doğayı sömürmesi ve hükmü altına alması gerektiği yolundaki kavrayıştan; bu kavrayışın ise, erkeğin ataerkil ailede kadını sömürmeye ve kendi hükmü altına almaya başlamasına kadar uzanan insanın insan üzerindeki tahakkümü ve sömürüsünden kaynaklanmakta olduğunu belirtmektedir. Toplumsal tahakkümle ortaya çıkan hiyerarşiler, sınıflar, mülkiyet biçimleri ve devlet kurumları gibi kavramlar, insan - doğa ilişkisinde de kullanılmaya başlanmıştır. Zaman içinde doğa da acımasızca sömürülecek bir kaynak, bir hammadde olarak görülmeye başlanmıştır (Bookchin, 1996:45'den aktaran Ünal,2010:115).

Çalışmanın alt araştırma sorularından biri olan "Siber güvenlik olaylarının, çevresel sürdürülebilirliği önleme riski var mıdır?" sorusuna yanıt bulmak amacı ile yapılan

araştırmalarda, doğal çevrenin fiziki hasar görmesine neden olabilecek siber güvenlik olaylarının, kritik altyapılara yönelik siber güvenlik olayları olacağı ön fikri ile ikinci bölümde bu sistemler araştırılacaktır.

Ancak kritik altyapı sistemleri ayrıntısına girilmedan önce de siber güvenliğin çevre etiği ile bağlantısının kurulmasında siber uzayın ağlarla birbirine bağlı sistemlerden oluşan doğası göz önünde bulundurulmalıdır. Siber uzay, Bookchin'in birinci doğa olarak adlandırdığı fiziki çevre üzerinde insan eli ile inşa edilmiş ağ temelli bir sistemdir. Toplumsal ekolojinin, insanın insan üzerindeki ve doğa üzerindeki tahakkümünün önüne geçilebilmesi için çözüm olarak sunduğu adem-i merkeziyetçi yapıların siber uzay üzerinden de oluşturulması ve merkezi hiyerarşik yapının devre dışı bırakılması gerekmektedir. Siber uzayda merkezsizleştirilmenin sağlanması için geliştirilmesine başlanan blok zincir teknolojileri bulunmakla birlikte henüz tam olarak uygulamaya giremediği için en azından günümüz dünyasında sistemlerin birbirlerinden ayrı olarak faaliyetlerini sürdürmeleri mümkün değildir. Temelinde ağ yapılanması olan siber uzayın yönetiminde bir hiyerarşik yapı yer almaktadır. Bu durumda toplumsal ekoloji yaklaşımının siber uzay için tam olarak geçerli olamayacağı, onun yerine pragmatik yaklaşım ile çevresel sürdürülebilirliğin benimsenmesinin daha uygun olacağı değerlendirilmektedir.

Çevresel sürdürülebilirlik yaklaşımı kapsamında, gelecek nesillerin kullanımını kısıtlamadan bugünkü kaynakların verimli kullanımı ile siber uzayda yer alan bilişim teknolojileri faaliyetlerinin devam ettirilmesi gerektiği düşünülmektedir. 2015 yılında BM'e üye tüm devletler tarafından kabul edilen 2030 Sürdürülebilir Kalkınma Gündeminde yer alan 17 maddenin tümü için bilişim teknolojilerinin kullanımının doğrudan ya da dolaylı olarak önemli fayda ve verimlilik sağlayacağı değerlendirilmektedir. Tezin sınırlılıkları içinde sadece çevre etiği bağlamında, herkesin temiz suya erişiminin sağlanması; güvenilir, sürdürülebilir ve modern enerjiye erişimin sağlanması; dayanıklı altyapı oluşturulması; sürdürülebilir sanayileşmenin ve inovasyonun teşvik edilmesi; şehirlerin güvenli, dayanıklı ve sürdürülebilir kılınması; sürdürülebilir üretim kalıplarının sağlanması; iklim değişikliği ve etkileriyle mücadele için acil önlemlerin alınması; okyanusların, denizlerin ve deniz kaynaklarının korunması ve sürdürülebilir şekilde kullanılması; ormanların sürdürülebilir bir şekilde yönetilmesi, çölleşmeyle mücadele edilmesi, arazi bozulmasının durdurulması ve

tersine çevrilmesi, biyolojik çeşitlilik kaybının durdurulması; şeklinde tanımlanan faaliyetlerin önemli bir kısmının, bilişim teknolojileri kullanılarak gerçekleştirildiği görülmektedir.

İkinci bölümde, bir siber güvenlik olayına maruz kalması durumunda fiziki çevre üzerinde hasar yaratabilecek ve çevresel sürdürülebilirliği önleyebilecek kritik altyapılar ve kritik altyapı sektörleri yakından incelenecek ve çevresel sürdürülebilirliği sağlamak üzere bu sistemlerin siber güvenliği üzerinde durulacaktır. Kritik altyapı sistemlerine yönelik siber güvenlik açıkları ve tehditler ele alınacak ve örnek olaylar eşliğinde siber güvenlik olaylarının sürdürülebilirliği engelleyecek durumlar oluşturup oluşturmayacağı araştırılacaktır.

İKİNCİ BÖLÜM

KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİ

İçinde yaşadığımız dönemde, bilişim teknolojilerindeki ve siber güvenlik alanındaki gelişmeler paralelinde, kamu ve özel sektör kuruluşları tarafından işletilmekte olan ve işlevlerini yerine getiremediklerinde ya da yanlış sonuçlar ürettiklerinde toplumsal kaos, can ve mal kaybına neden olabilecek kritik altyapı sistemleri de siber alana dahil olmaya başlamış ve siber güvenlik olaylarından etkilenebilir duruma gelmişlerdir.

Tezin araştırma soruları arasında, siber güvenlik olaylarının, çevresel sürdürülebilirliği önleme riskinin mevcudiyetini araştırmak bulunduğu için bu bölümde öncelikle bir siber güvenlik olayına maruz kalması durumunda fiziki çevre üzerinde hasar yaratabilecek ve çevresel sürdürülebilirliği önleyebilecek kritik altyapı sektörleri ve kritik altyapılar ile kritik altyapıların temel bileşeni haline gelen endüstriyel kontrol sistemleri (EKS) hakkında genel bilgiler verilecektir. Daha sonra çevresel sürdürülebilirliği sağlamak üzere bu sistemlerin siber güvenliği üzerinde durulacak ve kritik altyapı sistemlerine yönelik siber güvenlik açıkları ve tehditler ele alınacaktır. Bu bağlamda 1980'li yıllardan itibaren kritik altyapıların maruz kaldığı siber güvenlik olayı örneklerine yer verilecek ve meydana gelen ya da meydana gelmesi muhtemel sorunlar çevre etiği açısından irdelenecektir.

2.1 KRİTİK ALTYAPILAR VE ÇEVRESEL SORUNLAR OLUŞTURABİLECEK KRİTİK SEKTÖRLER

Bu bölümde, BM'e üye devletler tarafından 2015 yılında kabul edilen sürdürülebilir kalkınmanın 17 maddesi kapsamında, çevre etiğinin siber güvenlik ile bağlantısını kurabilmek amacı ile kendilerine yönelik bir siber saldırı sonucu fiziki çevre üzerinde olumsuz etki meydana getirebilecek olan siber fiziki sistemleri, bir başka deyişle endüstriyel kontrol sistemlerini kullanarak faaliyetlerini yerine getirmekte olan kritik altyapıların tanımlaması yapılacak ve bu çalışma kapsamındaki kritik sektörler ele alınacaktır.

2.1.1 Kritik Altyapılar

Kritik altyapı terimi, kamu ya da özel sektör tarafından işletilmekte olan iletişim, enerji, bankacılık, ulaşım, su sistemleri, acil durum hizmetleri gibi sektörlerin işlevlerini yerine getirmesi için gerekli olan fiziki veya bilgisayar tabanlı sistemleri ifade etmektedir (Radvanovsky, 2018: 58).

Kritik altyapı terimi ilk kez ABD'nde 1996 yılında Başkan Clinton döneminde yayınlanan, EO-13010 sayılı Başkanlık Emri ile kurulan Kritik Altyapıların Korunması için Başkanlık Komisyonu (PCCIP) tarafından yayınlanan ve komisyon başkanı Robert Marsh'ın adı ile anılan Marsh Raporu'nda kullanılmıştır (Lewis, 2015:7). Bu raporda kritik altyapılar arasında enerji bankacılık, finans, ulaşım, sağlık ve iletişim sektörleri sayılmıştır.

Marsh Raporu çalışması sonrasında 1998 yılında Başkanlık Karar Yönergesi (PDD-63) yayınlanmıştır (The White House, 1998). Bu yönergede, bankacılık ve finans, acil kolluk hizmetleri, acil durum hizmetleri, enerji, bilgi ve iletişim, halk sağlığı hizmetleri, ulaşım ve su sağlama hizmetleri olmak üzere 8 temel kritik altyapı sektörü tanımlanmıştır. Fiziki ve siber tabanlı olan bu kritik altyapıların devlet işleri ve ekonominin yürütülmesi için gerekli olduğu; bilişim teknolojilerindeki gelişmelerden ve verimliliğin artırılmasının gerekliliğinden dolayı bu altyapı sistemlerinin birbirleri ile bağlantılı ve otomatik çalışır duruma geldiği belirtilmiştir. Bu gelişmelerin donanım hatası, insan hatası, doğal felaketler, fiziki ve siber saldırılar gibi yeni güvenlik açıkları doğurabileceği; güvenlik açıklarının tanımlanmasının hem kamu hem de özel sektör tarafından uygulanabilecek esnek evrimsel yaklaşımlar gerektirdiği vurgulanmıştır.

Kritik altyapılar, 2001 yılında yürürlüğe giren USA Patriot Yasasında, ABD için yetersizlikleri veya yok edilmeleri durumunda güvenlik, ulusal ekonomik güvenlik, ulusal halk sağlığı veya bunların herhangi bir kombinasyonu üzerinde zayıflatıcı etki oluşturabilecek hayati öneme sahip fiziki ya da sanal sistemler ve varlıklar olarak tanımlanmıştır .

Şubat 2003'te ABD'nde Kritik Altyapılar ve Temel Varlıkların Fiziksel Korunması için Ulusal Strateji belgesi yayınlanmıştır. Bu belgede, kritik altyapı sektörünün, milli güvenlik, yönetişim, ekonomik canlılık ve yaşam biçimi için temel oluşturduğu; nükleer

santraller ve barajlar gibi temel varlıkların sadece ulusal seviyede değil küresel seviyede önem taşıdığı belirtilmiştir. Kritik altyapılar, yetersizlikleri ya da yok edilmeleri durumunda güvenlik, ulusal ekonomik güvenlik, ulusal halk sağlığı ve güvenliği konularında zayıflatıcı etki yaratabilen fiziki ya da sanal sistemler ve varlıklar olarak tanımlanmıştır (The White House, 2003:6). Kritik altyapı sektörleri olarak tarım, gıda, su, halk sağlığı, acil durumlar, kamu, savunma sanayi, bilgi ve iletişim, enerji, ulaşım, bankacılık ve finans, kimya sanayi ve tehlikeli malzemeler, posta ve nakliye sektörleri sayılmıştır. Korunması gereken kritik altyapılar ve temel varlıkların listeleri sektör bazında çıkarılmıştır. (The White House, 2003:9). 12 Şubat 2013 tarihli Kritik Altyapı Güvenliği ve Dayanıklılığı Başkanlık Politika Direktifi (PPD-21)'nde Kimya, Ticari Faaliyetler, İletişim, Kritik Üretim, Barajlar, Savunma Sanayi, Acil Hizmetler, Enerji, Finans, Gıda ve Tarım, Kamu Kuruluşları, Sağlık, Bilişim Teknolojileri, Nükleer Reaktörler, Materyaller ve Atıklar, Ulaşim Sistemleri, Su ve Atık Su Sistemleri şeklinde 16 Farkli Kritik Altyapı Sektörü Belirlenmiştir (The White House, 2013).

Ülkemizde ise T.C. İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) tarafından hazırlanan Açıklamalı Afet Terimleri Sözlüğünde, "işlevlerini kısmen veya tamamen yerine getiremediğinde toplumsal düzenin sürdürülebilirliğinin veya kamu hizmetlerinin sunumunun olumsuz etkileneceği, ulaşım, haberleşme, enerji, su, finans gibi sektörleri kapsayan ağ, varlık, sistem ve yapılar bütünü." şeklinde tanımlanmıştır (AFAD, 2014). 2013 yılında Siber Güvenlik Kurulu tarafından yayımlanan ve Bakanlar Kurulu Kararı ile yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında Kritik Altyapılar, işlevlerini yerine getirmekte kullandıkları bilişim teknolojileri göz önünde bulundurularak "İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" olarak tanımlanmıştır (UDHB, 2013: 3). 11 Kasım 2013 Tarihli ve 28818 Sayılı resmi gazetede yayımlanarak yürülüğe giren Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğde Kritik Altyapılar tanımı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planındaki tanıma "endüstriyel kontrol sistemlerini barındıran altyapılar"ın eklenmesi ile genişletilmiştir. Kritik altyapıları barındıran sektörler kritik

sektörler olarak tanımlanmıştır. Bu tebliğ kapsamında hazırlanan Kurumsal Siber Olaylara Müdahale Ekibi (SOME) Rehberinde kritik altyapı sektörleri enerji, elektronik haberleşme, finans, su yönetimi ve ulaştırma olarak belirlenmiştir. 2016 ve 2020 yıllarında yayımlanan Ulusal Siber Güvenlik Stratejilerinin her ikisinde de kritik altyapının tanımı değişmemiş, Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğdeki tanımın aynısı kullanılmıştır. Yayımlanan her üç strateji belgesinde de kritik altyapı sektörleri en başta 20 Haziran 2013 tarihli ve 2 sayılı Siber Güvenlik Kurulu kararı uyarınca belirlenen kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" sektörleri aynen korunmuştur (UDHB, 2016:7; UDHB,2020: 13).

NATO tarafından hazırlatılan Tallinn Manuelinde ise kritik altyapı, bir devletin sınırları içinde yer alan ve zarar görmesi ya da yok olması durumunda o devletin güvenliğini, ekonomisini, halk sağlığını ya da çevre güvenliğini olumsuz yönde etkileyecek fiziki ya da sanal sistemler ve varlıklar şeklinde tanımlanmıştır (Schmitt, 2013: 258).

Kritik altyapı terimini ilk kez kullanan ABD, kritik altyapıları güvenlik, ulusal ekonomik güvenlik, ulusal halk sağlığı veya bunların herhangi bir kombinasyonu üzerinde zarar oluşturabilecek sistemler olarak tanımlamıştır. Ülkemizde, AFAD tarafından hazırlanan sözlükte ve Ulusal Siber Güvenlik Stratejilerinde kritik altyapı tanımı 2013'ten bu yana değişmemiş ve hepsinde can kaybına, ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek sistemler olarak tanımlanmış; çevreye ve diğer varlıklara verilebilecek zararlar dikkate alınmamıştır. Ilk kez Tallinn Manuelinde çevreye verilebilecek zarar da gündeme getirilmiştir.

Çok sayıda kullanıcısı olan ve yoğun bir şekilde kullanılmakta olan siber uzayda haberleşme güvenliğinin yanı sıra elektrik, su, kamu hizmeti gibi kritik altyapıların güvenliğinin sağlanması önem kazanmıştır (Karadağ, 2019:74).

Kritik altyapılar, zarar görmesi veya yok olması halinde, vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya kamu hizmetlerinin etkin ve verimli işleyişine ciddi boyutta olumsuz etki edebilecek fiziksel ve teknolojik tesisler, şebekeler, hizmetler ve varlıklardır (EU,2018). Kritik altyapılar, günlük hayatta kullanılan fiziki ya da siber sistemlerdir. Çok temel ve hayati önem taşıdıklrından dolayıbu sistemler, ayrıcalıklı

sistemler olarak değerlendirilmektedir. 2000'li yılların öncesinde batı toplumları için kaliteli su, güvenli gıda, sağlam köprüler, çalışan telefonlar, ambulans, polis hizmetleri, mal ve hizmetlerin alım satımının yapılabilmesi, gaz sistemini çalıştıran elektrik, buzdolaplarının çalışır vaziyette tutulması gibi bölgesel konular, kritik sistemler arasında sayılıyordu. Son dönemde kasırga, fırtına gibi doğal felaketler, enerji kıtlığı, sınır kapatma olayları, bankaların sistem hataları nedeni ile çalışamaz duruma gelmesi, tüm dünyada küresel boyutta tüm insanları etkilemeye başlamıştır.

Kritik altyapı terimi, ekonominin ve devletlerin operasyonlarını gerçekleştirebilmeleri için gerekli olan fiziksel ve bilgisayar tabanlı sistemleri ifade eder. Bu sistemler, kamu ya da özel sektör tarafından işletilmekte olan iletişim, enerji, bankacılık, ulaşım, su sistemleri, acil durum hizmetleri gibi sektörleri kapsamaktadır (Radvanovsky, 2018:58).

Vigano ve diğerlerinin insan vücudundaki kafatası ve kemiklerine, kan damarlarına, sinir sistemine, kısacası, insan vücudunun verimli ve acısız bir şekilde gerçekleştirebileceği her hareketi için gerekli hayati önemdeki organlarına benzettiği (Vigano vd.,2020:164); geniş kesimler tarafından ekonominin ve toplumun omurgası olarak kabul edilmekte olan kritik altyapıların güvenliğine yönelik bilimsel araştırma çalışmaları uzun süre ihmal edilmiştir. Ancak ABD'nde gerçekleşen 11 Eylül olayları sonrası, özellikle modern batı toplumlarında kritik altyapı sistemleri ve hizmetlerinin kritikliği hakkında bir farkındalık oluşmuş ve güvenlik açığı hakkındaki fikirler önemli ölçüde değişmiştir (Lukszo vd., 2010: 1-2).

2.1.2 Çevre Sorunları Oluşturabilecek Kritik Altyapı Sektörleri

Devletlerin ulusal güvenlik önlemleri kapsamında dikkate aldıkları ve kritik sistem olarak tanımladıkları kritik altyapı listeleri birbirinden farklı olabilmektedir. Bunlar arasında Kimya, Ticari Faaliyetler, İletişim, Kritik Üretim, Barajlar, Savunma Sanayi, Acil Hizmetler, Enerji, Finans, Gıda ve Tarım, Kamu Kuruluşları, Sağlık, Bilişim Teknolojileri, Nükleer Reaktörler, Materyaller ve Atıklar, Ulaşım Sistemleri, Su ve Atık Su Sistemleri, Trafik Sistemleri, Akıllı Şehirler vb. sayılabilmektedir.

Bu çalışmada, geleneksel bilişim teknolojileri kullanılarak kritik bilgilerin tutulduğu, işlendiği, iletildiği kritik altyapılardan çok, geleneksel bilişim sistemlerinin yanı sıra

endüstriyel kontrol sistemlerinin de kullanıldığı, bir siber olay sonrasında fiziki hasar görebilecek ve çevresel sorunlara yol açabilecek olan enerji sektörü, baraj, su ve kanalizasyon sektörü, kimya sektörü ile iletişim sektöründe yer alan kritik altyapıların siber güvenliği temel alınmıştır.

2.1.2.1 Enerji Sektörü

Enerji sektörü, son teknolojik gelişmeler paralelinde bilişim teknolojilerinin yoğun olarak kullanılmaya başlandığı ve beklenmeyen bir siber olayın gerçekleşmesi durumunda çok önemli çevresel etkiler yaratabilecek kritik altyapı sektörlerinin başında gelmektedir. Bu sektör içinde petrol ve doğalgaz üretim tesisleri, nükleer enerji santralleri, enerji dağıtım sistemleri sayılmaktadır.

i. Petrol ve Doğal Gaz Üretim ve Dağıtım Tesisleri

Petrol ve doğal gaz sanayisi birbiri ile iç içe geçmiş durumdadır. Petrol altyapısı, petrol üretimi, ham petrol taşımacılığı, arıtma, ürün nakliyesi ve dağıtımı, kontrol ve diğer dış destek sistemlerini kapsamaktadır. Petrol ve doğalgaz üretiminin alt işlemleri arasında arama, çıkarma, depolama işlemleri yer almaktadır. Günümüzde pek çok alanda kullanılan enerjinin temel hammaddesi petroldür. Küreselleşmenin en önemli unsurlarından biri olan ulaşım sektörü de petrole bağımlıdır. Petrol rafinerileri 7 gün 24 saat çalışır vaziyette olup kısa süre için bile üretimin durdurulması önemli sorunlara neden olabilmektedir. Ham petrolün temininde ve arıtılmış petrolün dağıtımında kolaylık sağlamak için rafinerilerin pek çoğu deniz kenarında limanlara yakın bölgelerde tesis edilmiştir. Çoğu durumda liman fonksiyonları ve güvenliği doğrudan ya da dolaylı olarak kontrol sistemlerinin düzgün çalışmasına bağlıdır (Krutz, 2006:26). Petrol rafinerilerinin, yapılan işlemlerin her aşamasında sıkı bir şekilde korunmaması durumunda insan hayatına, çevreye önemli zararları olabilir.

ii. Nükleer Enerji Santralleri

Nükleer enerji santralleri, endüstriyel kontrol sistemlerinin kullanıldığı kritik altyapılar arasındadır. Dünyanın pek çok yerinde elektrik üretimi için nükleer santraller kullanılmaktadır. Bir nükleer santrale yönelik saldırının başarılı olması durumunda radyoaktif maddelerin çevreye saçılması, canlılar için ölümcül sonuçlar doğurabilecektir.

Nükleer santral yakıtı bir ya da iki yıl kullanılmak üzere yüklenir. Santralin zincirleme reaksiyon oranı kontrol altında tutulmalı ve yeniden yakıt yüklemesi yapılmalıdır. Nükleer tesis dursa bile radyoaktif etki devam eder ve ısı açığa çıkar. Bu ısı yok edilmezse reaktör çekirdeği erir. 28 Mart 1979'da Pensilvanya yakınlarında gerçekleşen nükleer santral kazasında da aynı durum oluşmuştu. Reaktör çekirdeğinin kısmi erimesinin operatör hatası ve bozuk donanımdan kaynaklanan bu kazada az miktarda radyasyon yayılmış ve bilinen bir zarar saptanmamıştır. Uygun soğutma sistemi uygulanmazsa çekirdeğin erimesinden dolayı radyoaktif maddeler çevreye yayılabilir.

iii. Elektrik Dağıtım Sistemleri

Günümüzde her türlü üretim faaliyeti için elektriğe ihtiyaç duyulmaktadır. Petrol arıtma, tesisleri, nükleer enerji santralleri gibi diğer enerji üretim faaliyetleri için de elektrik enerjisi kullanılmaktadır. Elektrik enerjisinde yaşanacak yaygın ve uzun süreli bir kesinti, küresel olarak algılanabilecek önemli sorunlar doğurabilecek nitelikte olduğu için kritik altyapılar arasında sayılmaktadır. Pek çok ülkede elektrik sistemleri birbiri ile bağlantılı bir şekilde dağıtım yapmaktadır. Elektrik, petrol ve doğalgaz santralleri, hidroelektrik santralleri ve nükleer enerji santrallerinde üretilmektedir.

Günümüz toplumunun bağımlı olduğu kritik altyapı sistemlerinden biri de elektrik dağıtım şebekeleridir. Her gün milyonlarca wattlık elektrik enerjisi, üreticilerden tüketicilere taşınmaktadır. Elektrik sistemleri, ulaşım sistemleri, su arıtma sistemleri, iletişim sistemleri gibi pek çok kritik altyapı işleminin gerçekleştirilmesinde temel etmenlerden biridir. Son dönemde yaşanan deprem, sel, kasırga gibi felaketler, enerji dağıtım altyapılarının çalışmaması durumunda temel hizmetlerin sağlanması ciddi bir biçimde aksadığı için enerji dağıtım sistemleri de pek çok devlet tarafından da kritik altyapı olarak tanımlanmıştır (Henrie, 2012:201-202).

2.1.2.2 Baraj, Su ve Kanalizasyon Sektörü

Su ve elektrik ihtiyacını karşılamak için kullanılan barajlar da kritik altyapılar arasında sayılmaktadır. Baraj kapaklarının kontrolsüz olarak açılması; açılması gereken durumlarda doldurulmasına devam edilmesi fiziki tüm canlılara ve çevreye zararlı doğal

felaketlere yol açabilecektir. Barajların uzaktan takibi ve yönetiminde endüstriyel kontrol sistemleri kullanılmaktadır.

Halk Sağlığı, çevre ve ekonomik açıdan su ve kanalizasyon sistemleri de kritik sistemlerdir. Bu alanda içilebilir ve kullanılabilir su kaynakları ile atık suların depolanması ve arıtılması işlemlerini de kapsayan kanalizasyon sistemlerinin uygun şekilde çalışıyor olması önem arz etmektedir. Sektöre yönelik altyapılar çok çeşitli, karmaşık ve bazı durumlarda birkaç kişiye bazı durumlarda ise milyonlarca kişiye hizmet verebilen dağıtık sistemlerdir.

Suyun kullanıma sunulduğu tarafta su depoları, barajlar, kuyular, yeraltı su kaynakları, su arıtma tesisleri, pompalama istasyonları, su kemerleri ve dağıtım boruları kritik tesislerdir. Atık su hizmeti, evsel, ticari ve endüstriyel kaynaklardan toplanan atık suların işlenip iyileştirilerek farklı alanlarda yeniden kullanıma sunulması işlemlerini kapsamaktadır.

Çevre etiği kapsamında da değinildiği gibi küresel ısınma ve iklim değişikliği olaylarının hız kazandığı günümüz dünyasında tüm devletler için suyun depolanması, arıtılması ve dağıtılmasına yönelik işlemler hayati derecede önemlidir ve bu işlemlerin gerçekleştiği tüm tesisler kritik altyapılar arasında yer almaktadır.

2.1.2.3 Kimya Sektörü

Çevreye zarar verebilme potansiyeli yüksek olan bu tesisler genellikle, yerleşim alanlarına yakın konumlarda yer almaktadır. Bir kaza ya da sabotaj sonucu kimyasal gazların çevreye yayılması atmosferde, tarım alanlarında, sularda bozulmaya, ekolojik olaylarda dengesizliklere, insanlar ve diğer canlılarda yaralanma, ölüm gibi çok önemli sorunlara neden olabilecektir. Kritik altyapılar arasında yer alan kimyasal tesislerin zarar görmesi ya da hatalı çalışmasına neden olabilecek güvenlik olayları tüm canlıları ve fiziki çevreyi olumsuz etkileyebilecek niteliktedir.

2.1.2.4 İletişim Sektörü

Kamu refahı, ekonomik istikrar, sağlık, eğitim, kamu güvenliğini sağlamak üzere kolluk hizmetleri ve savunma operasyonları için bilgi ve iletişim sistemlerinin kendilerinin güvenliğinin sağlanması da çok önemlidir. Toplumlar her geçen gün daha da çok BİT

ağlarına ve hizmetlerine bağımlı hale gelmektedir. Siber uzayın güvenliği ve dayanıklılığı, siber uzaydaki güvenlik açıkları, kritik altyapıları bozabileceği ve yok edebileceği için BİT ağlarına ve hizmetlerine büyük ölçüde bağımlı olan altyapılar ulusal bir güvenlik meselesidir (Vigano vd.,2020:158). Teknolojik gelişmeler, iş ve rekabet ortamının yarattığı baskılar gibi nedenlerle iletişim sektörü sürekli olarak değişikliklere ve gelişmelere maruz kalmaktadır. İletişim sektörü, karmaşık ve çeşitli ağ altyapılarını, interneti kullanarak kamu ve özel sektöre ses, görüntü ve veri aktarım hizmetleri sunmaktadır. İletişim altyapısı dahilinde, switchler, santraller gibi fiziki donanımlar, kablolu iletişim için fiber ve bakır kablolar, mobil iletişim için hücresel, mikrodalga ve uydu teknolojileri kullanılmaktadır. Bu sistemler, ödeme, muhasebe, konfigürasyon ve güvenlik yönetimini sağlamak üzere kurulum, operasyon, yönetim ve bakım hizmetleri ile desteklenmektedir.

Veri ağlarındaki gelişmeler ve veri hizmetlerine yönelik artan talep sonucu internet altyapısı her geçen gün tüm dünya üzerinde hızlı bir şekilde yaygınlaşmaktadır. İnternet, ortak iletişim protokollerinin kullanıldığı küresel bir ağdır. İnternet servis sağlayıcılar, son kullanıcılara internete erişim olanağı sağlamaktadırlar. İnternet servis sağlayıcılar, diğer internet bağlantı noktalarına ya da ağ erişim noktalarına bağlantı yolu ile kendi yüksek kapasiteli ağlarını yönetmek için ağ işlem merkezlerini kullanmaktadırlar.

Günümüz toplumunda, çalışmaması durumunda önemli aksaklıklara neden olabilecek, insanların ve diğer canlıların, çevrenin zarar görmesine neden olabilecek kritik altyapılarda endüstriyel otomasyon kontrol sistemleri, scada sistemler, gömülü sistemler, programlanabilir mantık birimleri uzak terminal birimleri gibi bilişim sistemleri donanım, yazılım ve ağ ürünleri kullanılmaktadır. Süreç kontrol iletişim yöntemleri, kimileri BT sistemleri için de kullanılmakta olan kimileri ise sadece bu alan tarafından kullanılmakta olan havalı tüpler ve hidrolik sistemlerden kiralık telefon hatlarına, çevirmeli ağlara, ethernete, 3g, 4g, uydu, noktadan noktaya mikrodalgalar dahil çok çeşitli teknolojileri kullanmaktadır (Macaulay ve Singer, 2011:42-43).

Yukarıda en çok bilinen birkaç tanesi sayılan kritik altyapılar, doğrudan kamu, özel sektör bazen de kamu teşebbüsü firmalar tarafından işletilmektedir.

Kritik altyapıların işlevlerini yerine getirmelerinde kullanılmakta olan endüstriyel kontrol sistemleri de birbirlerine ağlarla bağlı olduğu için bu sistemlerin çalışır halde

tutulmasında da iletişim sistemleri hayati öneme sahiptir. Genellikle kapalı bir fabrika ya da tesis merkezli daha küçük alanlarda faaliyetlerini sürdürmekte olan imalat sanayi alanlarında hızlı ve güvenilir olan Yerel Alan Ağı (LAN) teknolojileri; dağıtım sanayinde ise çok uzak mesafeler arası iletişimi sağlamak üzere geniş alan ağları (WAN) ve kablosuz/RF teknolojileri kullanılmaktadır. Dağıtım sanayiinde kullanılmakta olan EKS'nin iletişim ortamında veri transfer gecikmesi ve veri kaybı gibi uzun mesafeli iletişimden kaynaklanan sorunları giderecek şekilde tasarımlar yapılmaktadır (NIST SP 800-82r2,2015:2.2).

Ana Sektör	**Alt sektör**
Enerji Sektörü	Petrol ve Doğal Gaz Üretim ve Dağıtım Tesisleri
	Nükleer Enerji Santralleri
	Elektrik Dağıtım Sistemleri
Baraj-Su-Kanalizasyon Sistemleri	Barajlar
	Su Arıtma Tesisleri
	Su Dağıtım Sistemleri
	Sulama Sistemleri
	Kanalizasyon sistemleri
Kimya Sektörü	Kimyasal fabrikalar vb.
İletişim Sektörü	Bilgi ve İltişim altyapısı
	İnternet Altyapısı

Tablo 1: Önemli çevre sorunlarına neden olabilecek kritik altyapı sektörleri

2.1.3 Kritik Altyapılarda Kullanılmakta Olan Endüstriyel Kontrol Sistemleri

Kritik altyapıların temel faaliyetlerini yerine getirmesinde 1960'lı yıllardan itibaren çok farklı işlevleri yerine getirebilecek şekilde geliştirilen, özellikle 1980'li yıllar sonrasında önemli gelişmelerin yaşandığı bilişim teknolojilerini barındıran Endüstriyel Kontrol Sistemleri (EKS) kullanılmaktadır.

Güvenlik standartları konusunda çalışmalar yapan International Society of Automation (ISA), bu sistemleri Endüstriyel Otomasyon ve Kontrol Sistemleri olarak adlandırmıştır. IP yapısını kullanan ve BT sistemleri ile uyumlu çalışan ve SCADA sistemleri de kapsayan Endüstriyel Otomasyon ve Kontrol Sistemleri terimi, daha kapsamlı ve geniş bir anlatım için kullanılmış; 2006 yılında DHS tarafından Kontrol Sistemleri şeklinde kullanılmış; 2008 yılında NIST, Endüstriyel Kontrol Sistemleri olarak kullanmıştır (Macaulay ve Singer, 2011:25). Aralarında biçimsel farklar olmakla birlikte sanayide ve

kritik altyapılarda kullanılmakta olan SCADA sistemler, Dağıtık Kontrol Sistemleri (DCS) ve Programlanabilir Mantık Birimleri (PLC) gibi çeşitli kontrol ve koordinasyon sistemleri için ortak terim olarak EKS kullanılmaktadır (NIST SP 800-82r2, 2015:2.1; Macaulay ve Singer, 2011:42).

Bu sistemlerin, yerine getirdikleri işlevlere bağlı olarak farklı tanımlamaları yapılabilmektedir. Bunlardan bazıları:

- EKS, üretim, kimyasal tesis, elektrik üretim ve dağıtım, enerji nakil gibi pek çok endüstri alanında ekipmanların otomatik veya yarı otomatik kontrolünün, bilgisayarlar, elektrikli ve mekanik cihazlar aracılığı ile yürüten çeşitli sistemlerdir (Kott vd., 2016:1).
- EKS, kritik altyapı tesislerinin temel işlevlerinin yerine getirilmesini sağlamak üzere kontrol, takip ve koordinasyon fonksiyonlarını yerine getirmek için kullanılmakta olan Süreç Kontrol Sistemleri (PCS), Dağıtık Kontrol Sistemleri (DCS) ve SCADA Sistemleridir (Macaulay ve Singer, 2011: 42).
- Geniş kapsamlı tanımlamalardan biri, merkezi bir tesisten, uzaktaki endüstriyel süreçlerin sistem durumu, alarmlar ve diğer verilerin takibi ve kumandası için kullanılan yazılım tabanlı sistem ve sistemler şeklinde yapılanıdır (Henrie, 2012: 204).
- Her geçen gün daha da çok birbirine bağlanmakta olan ağlarla bağlı günümüz dünyasında, kritik altyapı tesislerinin kontrolü, izlenmesi ve yönetimini sağlamak üzere kontrol ve koordinasyon fonksiyonlarını yerine getirmek için kullanılmakta olan ve bir takım biçimsel farklılıkları olan Süreç Kontrol Sistemleri, Dağıtık Kontrol Sistemleri ve SCADA Sistemleri ve gömülü sistemler Endüstriyel Kontrol Sistemleri olarak anılmaktadır. (Macaulay ve Singer, 2011:42).

EKS, enerji santrali, petrol rafinerisi, kimyasal tesis gibi üretim alanında; coğrafi olarak dağıtık birbirlerinden binlerce kilometre uzakta yer alan varlıkları kapsayan su dağıtım, su arıtma, kanalizasyon, tarımsal sulama, petrol ve doğal gaz dağıtım elektrik şebekesi gibi dağıtım alanında hizmet veren pek çok kritik altyapıda kullanılmaktadır. Bu sistemler, elektrik enerjisi, su, petrol/doğal gaz dağıtım boru hatları, kimyasallar, madenler, ilaç sanayii, ulaşım ve üretim gibi dünya çapında çok geniş alanlara yayılmış endüstriyel altyapıları çalıştırır; fiziki süreçleri ölçer, sensör değerlerini görüntüler ve süreçleri yönetir.

Üretimin sürekliliğinin gerekli olduğu bir enerji santralinde, yakıt ve buhar akışını; petrol rafinerisinde petrol akışının, kimyasal tesiste damıtma işleminin sürekliliğini sağlamak üzere; üretimin farklı aşamalarında kontrol amacı ile fabrika, daha küçük alanlarda genellikle üretim sistemlerini kontrol, takip ve yönetim amacı ile kullanılırlar. Petrol rafinerilerinde kritik arıtma süreçlerinin gerçekleştirilmesinde; insansız petrol üretim platformlarının uzaktan kontrol ve takibi ile acil durumlarda petrol kuyularının görüntülenmesinde; elektrik üretim ve dağıtımında gerçek zamanlı uzaktan görüntüleme ve takip işleminde; su arıtma işleminde su arıtma sürecini, pompalama sistemini, boru hattı basıncını görüntüleme ve kontrol etmede; nükleer santrallerin soğutma ve diğer normal ve acil durumların kontrolünde EKS kullanılmaktadır (Krutz, 2006:26-36).

Bir EKS, üretim, ulaşım, enerji gibi bir endüstriyel amacı gerçekleştirmek üzere elektronik, mekanik, hidrolik, pnömatik kontrol bileşenlerinin birlikte kullanıldığı kombinasyonları içerir. Sistemin asıl gerçekleştirmekte olduğu amaca uygun olarak yaptığı iş, süreç; sürecin sağlıklı işlemesine yönelik yapılan işler ise kontrol olarak anılmaktadır (NIST SP 800-82r2, 2015:2.1). Kontrol süreci tamamen otomatik olarak kurulan sistemler tarafından gerçekleştirilebilir, sistemin çalışmasından elde edilen veriler kullanılarak çalışması sürdürülebilir ya da sistem tamamen insan kontrollü olarak gerçekleştirilir.

Endüstriyel kontrol sistemleri, tamamen ya da kısmen otomatik üretim süreçlerinin mevcut durumları hakkındaki verileri uç nokta birimlerinden toplar; tipik BT sistemi olan tarihçe kayıt sistemleri, üretim sürecine ilişkin bilgileri tarih ve saatine göre kaydeder. Süreç kontrol sistemi, dağıtık kontrol sistemi, SCADA gibi EKS'leri ise değerleri okur; otomatik mantık alarmlarını harekete geçirir; operatör müdahalesine imkan tanır ya da otomatik sistem durum değişimlerini raporlar. Bazı EKS'ler, sadece uç birimlerden gelen bilgiyi toplama, görüntüleme ve arşivleme işlevini yerine getirirken bazıları ise nükleer güç santrali ya da içme suyu sistemleri gibi kritik altyapı tesislerinde, otomatik, yarı otomatik ya da operatör kontrolü altında bir takım kontrol işlemlerini gerçekleştirirler (Macaulay ve Singer, 2011:25-27). Ulaşım ağları, elektrik üretim dağıtım şebekeleri, karmaşık iletişim sistemleri, su ve gaz dağıtım şebekeleri gibi sahada yer alan fiziksel sistemler, işlevlerini gerçekleştirmek üzere internet ve ağ bağlantıları ile bilişim teknolojilerini kullandıkları için siber fiziki sistemler olarak anılmaktadır. Siber fiziki sistemlerin iki bileşeni, bilişim

teknolojilerinin kullanıldığı siber yapılar ve fiziksel süreçlerdir. Fiziksel süreç, algılama, bilgi işleme ve iletişim özelliklerine sahip birkaç küçük aygıttan oluşan ağ sistemi şeklinde tanımlanabilecek olan siber sistem tarafından takip edilir ya da kontrol edilir. Fiziksel bileşen doğal ortam, insan yapımı ya da ikisinin birleşimi olabilir. Bu bileşenler fiziksel süreçleri takip etmek ve faaliyetlerinin etkinliğini ve verimliliğini artırmak üzere iyileştirici eylemleri başlatmak için birlikte çalışırlar (Jiow, 2017:222).

Endüstriyel Kontrol Sistemleri, fiziki ortamlardan veri topladığı, topladığı bu verileri kullanarak bir kontrol işlemi gerçekleştirdiği ve tam otomatik ya da yarı otomatik bir şekilde sahada gerçekleştirilmekte olan üretim ya da dağıtım işlemine müdahalede bulunduğu için siber-fiziki sistemler olarak da adlandırılmaktadırlar. Fiziki sistemleri kontrol etmek üzere kullanılan EKS, bilişim teknolojileri (BT) ile kontrol ve ölçüm amaçlı özel cihazlardan yani operasyonel teknolojilerden (OT) oluşmaktadır. BT, bilginin işlenmesi ve saklanması amacı ile kullanılan geleneksel bilişim sistemlerini anlatmak üzere kullanılmakta olup bilgisayarları, yazılımı, ağları ve insan-makine ara yüzlerini kapsamaktadır.

2.1.3.1 Endüstriyel Kontrol Sistemlerinin Gelişim Evreleri

Endüstriyel kontrol sistemleri, 1960'lı yıllarda veri toplama ve gerçek zamanlı iş süreçlerini kontrol etmek için kullanılan yazılım ve donanımların gelişmiş halidir (Krutz, 2006:74). 1960'ların sonlarına kadar endüstriyel sistemlerinin kontrolü mekanik veya elektromekanik röle tabanlı sistemlerle gerçekleştirilmiştir (Flaus,2019:7). 1971 yılında mikroişleyicilerin icadı ve giriş çıkış bileşenlerinin entegrasyonu ile mikrokontrol birimlerinin de gelişmesi sonrasında, daha önce analog bileşenler kullanılmakta olan karmaşık endüstriyel kontrol sistemlerinde bu mikroişleyiciler kullanılmaya başlanmıştır. Mikrokontrol cihazları, fiziki dünyada belli bir görevi yerine getirmek üzere tasarlanmış uygulamaların üzerinde çalıştığı bilişim sistemleri içinde gömülü vaziyette bulunmaktadır. Büyük sanayi tesisleri, nükleer güç santralleri gibi büyük pek çok endüstriyel kontrol sisteminin görevlerini yerine getirebilmesi, genellikle daha küçük gömülü sistemlerin oluşturduğu bileşenlere bağlıdır (Farooq-i-Azam ve Ayyaz, 2012:180).

Endüstriyel kontrol sistemleri, okuduğu verileri iletmek ve bahse konu altyapılara ait temel komutları gönderebilmek için hava basıncı, buhar basıncı gibi havalı sistemleri ve su basıncı, sıvı basıncı ile çalışan hidrolik sistemleri kullanmaktadır. Havalı kontrol

sistemlerinin sadece kurulumu değil bakımı ve taşınmasının da maliyeti yüksektir. Elektronik dalgaların kablolar ile iletilmesinin mümkün hale gelmesi ile modern süreç kontrol sistemleri doğmuş ve altyapı sahipleri bu sistemleri hızla kendi sistemlerine uyarlamışlardır. Ancak dayanıklı ve uzun ömürlü oldukları için geçmişte kurulmuş ve halen kullanımına devam edilen hava ve su basıncı ile çalışan analog sistemler de mevcuttur. Bu sistemler hem çok pahalı hem de yeşil alan uygulamaları için uygulanamaz sistemlerdir (Macaulay ve Singer, 2011:47). Hidrolik sistemlerde hidrolik sıvısı kaçağı olabileceği için çevreye zararlı etkileri olabilmektedir.

Günümüzde kullanılmakta olan EKS'lerinin çoğu, mevcut fiziksel sistemlere BT yeteneklerini kapsayan fiziksel kontrol mekanizmaları eklenerek geliştirilmiş; mekanik sistemler ise sayısal sistemlere dönüştürülmüştür. Bir yandan EKS'nin uzun ömürlü kullanımlarına devam edilirken öte yandan bu sistemlere yeni yetenekler kazandırılmasına yönelik mühendislik çalışmalarına da devam edilmektedir (NIST SP 800-82r2, 2015:2.1).

	İşlemci	**Verilerin İletilmesi**	**Özellikler**
1960'lı yıllar	Veri toplama ve gerçek zamanlı iş süreçlerinin gerçekleştirilmesi için mekanik veya elektromekanik röle tabanlı analog bileşenler	Veri iletimi ve temel komutları göndermek için havalı sistemlerin ve hidrolik sistemlerin kullanılması(Analog) Patentli müstakil ağlar	Pahalı, Çevreye zararlı, Siber güvenlik açısından daha az risk
1971 sonrası	Mikroişleyicilerin icadı ve giriş/çıkış bileşenlerinin entegrasyonu ile mikrokontrol birimlerinin gelişmesi Tam otomatik sistemler	Elektronik dalgaların kablolar ile iletiminin mümkün hale gelmesi (Sayısal ağlar)	Siber güvenlik riskleri yüksek
1990'lar sonrası	Ortak işletim sistemlerinin kullanılabilmesi Açık protokoller ve standart donanımların kullanılması	IP tabanlı standart iletişim protokollerinin kullanımı, BT ve EKS iletişim protokollerinin uygun hale gelmesi yerel ağlarla, geleneksel bilişim sistemleri ağları ve internetle bağlantı sağlanması	Etkili Daha hesaplı Çevreye zararı daha az Siber güvenlik riskleri ve saldırı vektörü daha geniş

Tablo 2: EKS'nin Gelişim Süreçleri

Süreç kontrol ağları önce analogdan dijitale daha sonra ise dijitalden IP sistemlere dönüşmüştür. IP ağ cihazları her yerde bulunabilir olup kurulumu ve desteği kolaydır. (Macaulay ve Singer, 2011:51). Eskiden pompalar, ısı ölçüm cihazları, basınç ölçüm aletleri gibi otomasyon cihazlarının uzaktan takibini ve kontrolünü sağlayan endüstriyel kontrol sistemleri için patentli ve tek başına çalışan kapalı ağlar kullanılırken 1990'ların sonlarından itibaren bu sistemler IP tabanlı ağları kullanmaya başlamışlardır. Yine enerji, su, gaz gibi tüketim ürünlerinin son kullanıcılar tarafından tüketim miktarını ölçmek ve takip etmek için de IP tabanlı sistemler kullanılmaya başlanmıştır (Macaulay ve Singer, 2011:59-60). Endüstriyel Kontrol Sistemleri, başlangıçta kendi içinde izole olarak başka ağlara bağlı olmadan çalışmakta idi. Ancak internet ağlarının tüm dünya üzerinde yaygınlaşmasını müteakip eski ya da yeni teknoloji ürünü tüm EKS' de bu ağlara bağlanmaya başlanmıştır. (Alcaraz vd., 2015:6). IP sayesinde ses ve veriler aynı ortam üzerinden iletilebildiği ve IP ağ cihazları her yerde bulunabilen kurulumu ve desteği kolay sistemler oldukları için EKS'nin üreticileri ve sahipleri, ağ sistemlerinde IP'ye geçişi tercih etmektedir (Macaulay ve Singer, 2011:51).

SCADA Sistemler, dağıtık kontrol sistemleri, operasyonel teknolojiler gibi değişik şekillerde adlandırılan endüstriyel kontrol sistemleri, son dönemlerde bilişim teknolojilerinin farklı bir türü olarak değerlendirilmektedir. Geçmişte, BT iletişim protokolleri ile endüstriyel kontrol sistemlerinin protokolleri uyumlu olmadığı için bu endüstriyel ortamlar birbirleri ile bağlantısı olmayan kapalı sistemlerdi. Günümüzde bu protokoller birbiri ile konuşmaya başladığı için BT ve endüstriyel kontrol sistemleri birbirleri ile bağlanabilmektedir. SCADA sistemleri, yönetime üretim süreçleri ile ilgili gerçek zaman verilerini temin eder; daha etkili kontrol imkanları sağlar; tesis ve ürün güvenliğini artırır; işlem maliyetlerini düşürür. Bu faydalar, SCADA sistemlerde İnterneti de kapsayan iyileştirilmiş iletişim protokolleri ile birleştirilmiş standart yazılım ve donanım ürünlerinin kullanılması ile mümkün hale gelmiştir. Belirtilen faydaların yanı sıra dış ortama bağlantı sağlanması, çok çeşitli iç ve dış etkenlerden kaynaklanan saldırı ve hata durumlarını da mümkün hale getirebilmektedir (Krutz, 2006:1).

Günümüzde, pek çok EKS, uzaktan erişim ve uzaktan operasyona imkan sağlayan internet sistemi üzerinden işlevlerini yerine getirmektedir (Warren ve Leitch, 2015:226).Yeni nesil SCADA sistemler sayesinde otomatik çalışma kapasitesi artırıldığı için uzak istasyonlarda insanların çalıştırılmasına gerek kalmamaktadır. Bu otomasyon adımı sayesinde önemli gelişmeler devam edecektir. İlk zamanlarda, uzak alanda çalışan cihazlar, sistem durumunda meydana gelen değişiklikleri merkeze bildirebilmekte idi. Uzak alanda, sistemin çalışıp çalışmadığını ya da vana pozisyonunun açık mı kapalı mı olduğunu belirlemek üzere konuşlanmış röleler buna örnek olarak gösterilebilir. Uzak alandaki bilgileri edinme avantajını kullanmak üzere uzak aptal terminaller kullanılmaktadır. Bu terminaller çoklu alan durumu ve alarm bilgisini tek bir cihaz üzerinden alarak fiziksel bağlantı sağlayan temel uzak alan veri toplayıcılar olarak kullanılmakta idi. Çeşitli uzak alan cihazlarının durum bilgisi tek bir akılsız terminal üzerinden toplanarak merkeze iletilmekte idi. Uzak alandan yoğunlaştırılmış bilgiye erişim olanağı, merkezi ana bilgisayar sistemlerinin gelişmesini de kapsamaktadır. Merkezi bilgisayar sistemi uzak veriyi, kontrol odasında görevli operatöre yanıt iletişim düzeni içinde almakta ve sunmakta idi. Bu ilkel sistemler boru hattı sahipleri ve işleticilerini de kapsayan çok farklı firmalar tarafından tasarlanıp geliştirilmekte idi. Bu sistemler patentli süreçler ve iletişim yöntemleri temel alınarak geliştirilmişti ve iç ya da dış hiçbir ağ bağlantısı olmayan, tek başına çalışan sistemlerdi. Uzak alan sistemleri, zaman içinde yarı otomatik ve sonunda tam otomatik sistemler haline gelmiştir. Bu gelişim, programlanabilir mantık birimleri (PLC) ve dağıtık kontrol sistemlerinin kullanılmaya başlanması ile gerçekleşmiştir. Programlanabilir mantık birimleri, SCADA sistem mühendislerine, yerel alan seviyesinde merkezi alana farklı tür verilerin iletilmesinin yanı sıra farklı işlerin gerçekleştirilebilmesi olanağı sağlayan adanmış bilgisayar sistemleridir. Yerel istihbarat ve gelişmiş iletişim sayesinde merkezi alanda daha kapsamlı ve derinlikli işler yapma olanağı doğmuştur. Bu yeni sistem yeteneklerinin desteklenmesi ve verdiği katkılar ile merkezi bilişim sistemleri ve grafik arayüzü birimleri yeteneklerinde gelişmelere olanak tanımıştır (Henrie, 2012:204-205).

Bu gelişmeler sonrasında ağ tabanlı SCADA sistemler kullanılmaya başlanmıştır. Ağ tabanlı sistemlerin kullanıma girmesi ile ortak işletim sistemlerinin, standart iletişim protokollerinin kullanımı ve yerel ağlarla, ofis işlerinin yürütülmesinde kullanılan ağlarla ve

internetle bağlantı olağan hale gelmiştir. Artık SCADA sistemler tek başına hiçbir yere bağlantısı olmadan çalışan, güvenlik seviyesi bilinmeyen sistemler olmaktan çıkmaya başlamıştır. Günümüzde SCADA sistemler, ağ tabanlı, çeşitli standartlara dayalı ya da ortak kullanımda olan yazılım donanım ürünlerinin kullanıldığı sistemlerdir.

Son zamanlarda kullanıma sunulan EKS'nin çoğunluğu, mevcut fiziki sistemlere, bu sistemlerin fiziki kontrol mekanizmalarının BT ürünleri kullanılarak yenilenmesi ya da desteklenmesi yöntemi ile geliştirilmiştir. Fiziki kontrol mekanizmalarının bilişim sistemleri kullanılarak performanslarının geliştirilmesi sonrasında bu sistemler, akıllı elektrik şebekesi, akıllı binalar, akıllı üretim gibi adlarla anılmaya başlanmıştır. Akıllı sistemlerin birbirleri ve diğer bilişim sistemleri ile bağlantılarının artması, bu sistemlerin uyumluluğu, dayanıklılığı, emniyeti ve güvenliği daha da önemli hale gelmiştir (NIST SP 800-82r2, 2015:2.1).

Geçmişte, EKS, özel yazılım ve kontrol protokolleri ile çalışan izole sistemler olduğu için geleneksel bilişim sistemleri ile çok az benzerlik göstermekte iken zamanla bu sistemlerin her geçen gün artan bir şekilde bağlanabilirlik, verimlilik, uzaktan erişim olanağı gibi açılardan ana akım kurumsal bilişim sistemleri ile bütünleşmeye başlaması ile EKS, geleneksel bilişim sistemlerine daha çok benzemeye başlamıştır. EKS, artan bir şekilde kurumların geleneksel bilişim sistemleri ile aynı donanım ve yazılım bileşenlerini kullanmaya başlamıştır. EKS mimarisindeki değişim yeni bilişim sistemi yeteneklerini desteklerken aynı zamanda bu sistemlerin dış dünyadan soyutlanmasını da azaltmıştır (Perdikaris, 2014:107). Geleneksel bilişim sistemlerinde bulunan güvenlik açıkları EKS için de geçerlidir.

Endüstriyel kontrol sistemleri, 1960'lı yıllarda sadece endüstriyel süreçlerin uzaktan kontrol ve takibi için kullanılırken transistor ve modern elektroniğin icadı ile günümüzdeki yaygın ve her alana nüfuz eden işlevlerine kavuşmuşlardır. Günümüzde sadece uzaktan kontrol ve takip için değil sürecin gerçekleştirimi aşamasında meydana gelebilecek tehlikeli durumları araştırıp önleyebilecek yetenekler kazanmıştır.

Geçmişte BT güvenliği endişeleri tek bir cihaz ya da hizmetle sınırlı iken sensörler ve aktuatorlerden meydana gelen internet nesneleri (IOT) olarak adlandırılmakta olan cihazların EKS içinde yaygın olarak kullanılmaya başlanması ile saldırı vektörleri artmış ve siber güvenlik daha da karmaşıklaşmıştır.

Teknolojik gelişmeler paralelinde son dönemde EKS'nin işletiminde açık protokoller ve standart olarak satılan donanımlar kullanmaya ve internete bağlanmaya başlanmıştır. Bunun nedenleri arasında;

- Donanım üreticilerinin artık analog sistem üretimini bırakmış olmaları ve yeni yazılımlara dayalı teknolojilerin kullanılmaya başlamasıyla sağlanan süreç optimizasyonu etkisinin sonucunda, EKS'lerin kendi aralarında ve birbirleriyle, internet bağlantıları üzerinden daha fazla iletişim içinde olmaları,
- EKS'nin modernleşmesiyle, işletim ve güvenlikle ilgili unsurlarının büyük bir çoğunluğunun, bilgisayarla çalışan dijital sistemlere dönüşerek bilişim altyapısına bağımlı hale gelmesi sonucu yeni teknolojilerin siber saldırı ihtimalini ve zafiyetini arttıran biçimde sürece dâhil olması,
- Kritik altyapının fiziki güvenlik önlemlerinin ötesine geçilerek korunması ihtiyacının ortaya çıkmış olması ve bu ihtiyaca cevap vermek amacıyla, çeşitli yazılım temelli sistemlerin geliştirilerek kullanılmaya başlanması sayılmaktadır (Han ve Çelikpala,2016:85).

Günümüzde EKS, fiziki süreçleri takip etmek üzere yönetimsel, idari ve düzenleyici sorumlulukları da kapsayan çok farklı bileşenlere sahip karmaşık sistemler haline gelmiştir. EKS, çeşitli bilgi işleme sistemlerini bünyesinde barındırmakla birlikte, fiziki sistemler üzerinde de işlemler gerçekleştirdikleri için Operasyonel Teknolojiler (OT) olarak değerlendirilmektedir (Flaus, 2019:4). Altyapıları yönetmek ve birbirine bağlamak için kullanılmakta olan kontrol sistemleri, iş sistemleri için kullanılmakta olan geleneksel bilişim teknolojilerinden farklı olup operasyonel teknolojiler olarak da adlandırılmaktadır (Perdikaris, 2014:107). Operasyonel Teknolojiler (OT), bir fiziksel sistem ile etkileşim halindeki BT sistemlerini anlatmak üzere kullanılmaktadır. Bir fiziki sistemden sensörler aracılığı ile bilginin alınması ve aktüatörler aracılığı ile bu fiziki sistem üzerinde bir takım işlemlerin gerçekleştirilmesini sağlayan donanım ve yazılımlardan oluşur (Flaus, 2019:2). OT, fiziki ortamların doğrudan takip ve kontrolünü sağlayabilen, kuruluştaki fiziksel cihazların, süreçlerin ve olayların doğrudan izlenmesi ve/veya kontrolü yoluyla bir değişikliğe neden olan veya algılayan donanım ve yazılımdır (Gartner, 2015). BT ise

verilerin işlenmesi ve dağıtılması için bilgisayar sistemlerinin, yazılımların ve ağların geliştirilmesini, bakımını ve kullanımını içeren teknolojidir (Merriam-Webster 2015).

2.1.3.2. Endüstriyel Kontrol Sistemlerinin Türleri

2016-2019 Ulusal Siber Güvenlik Stratejisinde, endüstriyel kontrol sistemleri, "Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan sistemler" olarak tanımlanmış; Süreç Kontrol Sistemleri, SCADA (Supervisory Control and Data Acquisition) ve Dağıtık Kontrol Sistemleri şeklinde gruplandırılmıştır. Aşağıda açıklamaları yer alan bu sistemler aynı tür hizmetleri yerine getirebildikleri için bazı durumlarda birbirlerinin yerine de kullanılabilmektedir.

i. Süreç Kontrol Sistemleri (PCS)

Gıda işlemede; silah üretiminde; petrolün arıtılmasında, depolanmasında ve dağıtımında; elektriğin kullanıldığı tüm sektörlerde, sağlık sektöründe, önemli dini, tarihi, politik alanlardaki tarihi eserlerin korunmasında; su arıtma ve dağıtım sistemlerinde; kimya sektöründe; barajlarda; nükleer tesislerin çalıştırılmasının her aşamasında; kargo dağıtım işlerinde; ulaşım ve taşımacılığın her alanında otomasyon sürecini kontrol etmek üzere kullanılmakta olan temel sistemlerdir (Macaulay ve Singer, 2011:31-34).

Bir ürünün aynı nitelikte üretilebilmesini sağlamak üzere üretim sürecinin kesintiye uğramadan sürekliliğinin sağlanması; farklı başlangıç ve bitiş adımları ve işlem sırasında ara adımların gerçekleştirebilmesi; kimi durumlarda da bir dizi makinenin tek bir adımda bir dizi işlemi gerçekleştirebilmesi için süreç kontrol sistemleri (PCS) kullanılmaktadır.

ii. Dağıtık Kontrol Sistemleri

Dağıtık kontrol sistemleri, aynı fiziki alanda hizmet veren petrol rafinerileri, su ve su arıtma, elektrik üretim tesisleri, kimyasal üretim tesisleri gibi kritik altyapı tesislerinin ve ilaç üretim tesisleri gibi sanayi alanlarında hizmet vermekte olan üretim sistemlerinin kontrolü için kullanılmaktadır. Kapalı bir fabrika ya da tesis merkezli daha küçük alanlarda; üretim sürecinin kesintiye uğramadan aynı nitelikte ürünün imalatını sağlamak işlevini yerine getirmektedirler.

Yerel olarak gerçekleştirilen üretim işleminin ayrıntılı kontrolünü sağlayan çoklu ve bütünleştirilmiş sistemlerdir. Bir DKS, üretim sürecinin tamamının yerine getirilmesi görevlerini paylaşan yerel olarak çalışan kontrol birimlerine aracılık eden merkezi denetim ve kontrol döngüsünü kullanmaktadır (NIST SP 800-82r2, 2015:2.5). DKS, belirli bir aşamada ihtiyaç duyulan faaliyetlerde ve süreçte beklenen bir aşama ile karşılaştırma işleminin yapılabileceği ortamı sağlar. Bu sistemde yer alan yazılımlar, genellikle olay tetiklemeli değil sırayla ve kronolojik olarak çalışır (Macaulay ve Singer, 2011:44-45). Sahadan veri toplamakta kullanılan sensör ve actuator gibi çok sayıda fiziksel birimin gerçek zamanlı kontrolünü sağlayan ve takip eden bilgisayar tabanlı kontrol sistemleridir (Demiröz,2017:342).

iii. SCADA Sistemleri

SCADA Sistemler, genellikle ulusal elektrik dağıtım şebekesi, enerji nakil hatları, petrol ve doğalgaz boru hatları gibi geniş alanlara yayılmış farklı konumlarda kurulu elektronik ortamları takip ederek buralardan veri toplayan ve süreci kontrol eden bütünleşik sistemlerdir. Bazı kurumlar için SCADA terimi sadece ana kumanda birimini ifade ederken bazı kurumlar için ise ana kumanda merkezinden uç kontrol birimine kadar tüm kontrol döngüsünü ifade edebilmektedir (Bayuk vd. 2012:59). Birden çok Dağıtık Kontrol Sistemi ve Programlanabilir Mantık Birimini kapsayan fiziki olarak birbirinden uzak alanlarda tesis edilmiş; merkezi veri toplamanın da kontrol kadar önemli olduğu, birbirlerine geniş alan ağları ile bağlanmış dağıtık sistemlerde kullanılmakta olan karmaşık yapılardır. Bu sistemler, su dağıtımı, kanalizasyon sistemleri, petrol ve doğal gaz boru hatları, elektrik iletim ve dağıtım sistemleri gibi kritik altyapılarda kullanılmaktadır.

SCADA sistemler, çok sayıda girdi ve çıktısı olan merkezi kontrol ve takip sistemleri oluşturmak üzere veri toplama sistemleri ile iletim sistemlerini ve kullanıcı arayüzü yazılımını bir araya getiren sistemlerdir. SCADA sistemler, saha bilgisini toplamak, bu bilgiyi merkezi bir bilgisayar sistemine aktarmak ve işlem sorumlusu operatöre bu bilgileri temin etmek yolu ile operatörün merkezi bir konumdan gerçek zamanlı olarak takip ve kontrol görevini yapmasını sağlayan sistemlerdir (NIST SP 800-82r2, 2015:2.5). Kimileri SCADA sistemlerin, kritik altyapıların kontrolü işleminden çok bu altyapıların koordinasyonunu sağladığını düşünmektedir. Oysa bu sistemler sadece koordinasyon

sağlamakla kalmaz, takip ettiği olayın gerçekleşme durumuna göre de gerekli işlemleri yerine getirmektedir. Yakın dönemde sadece bir görev için bir kez programlanan gömülü sistemlerden, içinde standart işletim sistemi barındıran bir çeşit bilgisayar sayılabilecek sistemlere geçilmeye başlanmıştır.

Bu çalışmada, SCADA sistemler, Endüstriyel Kontrol Sistemleri, Kontrol Sistemleri, siber fiziki sistemler ve operasyonel teknolojiler, aynı anlamı karşılamak üzere kullanılmıştır.

1.1.3.3 EKS'nin İnternet Tabanlı Geleneksel Bilişim Sistemlerinden Farkları

Kritik altyapıların temel bileşenlerinden olan modern Endüstriyel Kontrol Sistemleri, fiziksel süreçleri izlemek ve kontrol etmek üzere bu görevle ilgili birçok yönetimsel, idari ve düzenleyici sorumlulukla birlikte çok sayıda farklı bileşene ve teknolojiye bağlı olan karmaşık sistemlerdir. EKS'lerinin en temel bileşeni, kritik süreçlerin kullanılabilirliğini ve emniyetini destekleyen operasyonel teknolojidir. Günümüz EKS'lerinde, operasyonel teknolojiler, sistemin gerçekleştirmesi istenen işlevlere uygun bilişim teknolojisi ürünleri ile birleştirilmiştir (Hahn, 2016:51). Siber fiziki sistemler olarak da adlandırılan bu sistemler ile geleneksel bilişim sistemlerinin birtakım farklılıkları bulunmaktadır (Flaus, 2019:64):

- Bir EKS, daha önceden tanımlanmış iş akışları ve sensorler aracılığı ile fiziksel ortamdan gerçek zaman verilerini alıp, bu verileri parametre olarak kullanarak belirli işlemleri gerçekleştirmek ve bu verileri saklamak yolu ile fiziksel bir sistemi izlemek, harekete geçirmek ve yönetmek için kullanılırken geleneksel bilişim sistemi, sadece dijital ortamdaki verileri işlemek saklamak ve iletmek üzere kullanılmaktadır.
- EKS'nin görevleri arasında fiziksel sistemin güvenliğini etkileyebilecek sapmaları tespit edip önlemek ya da sistemin ve çevrenin güvenliğini sağlamak üzere birtakım eylemleri gerçekleştirmek de yer almaktadır. Bu işlem, örneğin, sıcaklık veya basınç eşiklerinin veya tehlikeli konumların tespiti ve bir valf açılması, soğutma işleminin tetiklenmesi veya bir işlemin engellenmesi şeklinde olabilmektedir (Flaus, 2019:65).
- EKS'nin kullanılabilir ve erişilebilir olması ve bir işin verilen süre içinde gerçekleştiriliyor olması özellikle emniyet açısından zorunludur. Gecikmeye, dalgalanmalara ve veri kaybına tahammül yoktur. Geleneksel bilişim sistemlerinde örneğin

bir maaş hesaplama işleminin belirlenen süreden daha geç tamamlanmasında hiçbir sakınca bulunmazken bir aracı çalıştıran EKS'nde saatte 60 km gitmesi gerekirken 16m.lik bir sapma oluşuyorsa bu çok önemli sorunlara yol açabilecektir. Sahadan toplanan veri sistemin çalışması açısından önem arz ettiği için bu verideki bozulma tüm sistemin doğru çalışmasını engelleyebilecek ve hasarla, ölümle sonuçlanabilecek önemli güvenlik sorunlarına neden olabilecektir.

- Fiziksel sistemlere bağlı PLC'ler ve gömülü sistemler gibi saha ekipmanları gerçek zamanlı olarak işlevlerini yerine getirirler ve merkezi yönetim ve güvenlik için çok kısıtlı imkanlar sunarlar. Çoğu sürekli olarak gerçek zamanlı çalışmak durumunda olan EKS süreçlerinin ve bu süreçleri kontrol eden sistemlerin beklenmedik bir şekilde devre dışı kalması önemli sorunlara yol açabilecek nitelikte olduğu için durdurulup yeniden başlatılmaları imkân dahilinde değildir. Bu sistemler kullanılarak gerçekleştirilen fiziki ortamlara yönelik üretim ve yönetim süreçleri ile kullanılmakta olan cihazlar, aktarılacak veriden daha önemli olabilmektedir. Geleneksel sistemlerde alışılagelmiş bir yöntem olan sistemlerin kapatılıp yeniden başlatılması gerçek zamanlı çalışmak durumunda olan EKS'nde çözüm olarak kullanılamamaktadır Antivirüs programları, kripto işlemleri gibi güvenlik çözümlerinin uygulanması ve bu güvenlik çözümlerinin güncellenmesi, sistemin çalışmasını yavaşlatabileceği ya da durdurabileceği için önemli derecede hasar, ölüm gibi sonuçlara neden olabilecektir (Flaus,2019:65).

- Geleneksel bilişim sistemleri, 3-5 yılda bir yenilenebilen, aktarımı kolaylıkla gerçekleştirilebilen son teknoloji ürünü sunucuları, kullanıcı bilgisayarlarını ve ağ bağlantı cihazlarını kullanmaktadır. Oysa EKS, değiştirilmesi, aktarımı, durdurulması ve yeniden başlatılması çok daha zor olan ve 15-20 yıllık sürelerle kullanılabilen standart modüllerden ya da çok daha eski model değişik cihazlardan oluşmaktadır ve sınırlı kaynağa sahiptir. Mevcut güvenlik olanaklarını iyileştirici uygun programlar bulunmayabilir (Macaulay ve Singer, 2011:85-92). Bir EKS, kuruluş aşamasında tasarlanır ve ne kadar süre hizmet vereceği de bu aşamada belirlenmiş olur. (NIST SP 800-82r2, 2015)'den aktaran Flaus, 2019:66). Bu hizmet süresi içinde sistemin değişen tehditlere yanıt verecek ve güncel güvenlik önlemlerini içerecek şekilde geliştirilmesi geleneksel bilişim sistemlerine göre oldukça zor kimi durumlarda ise imkansızdır.

- Geleneksel bilişim sistemlerinde, geniş çaplı kullanıcısı olan büyük yazılım firmaları güvenlik yamalarını hızlı bir şekilde gerçekleştirebilmektedir (Macaulay ve Singer, 2011:85-92). EKS ile birlikte kullanılmakta olan geleneksel bilişim sistemleri için saptanan güvenlik açıklarını önlemek üzere üretici firma tarafından hazırlanan yamaların geçilmemesi durumunda siber saldırganların saldırılarının başarılı olma olasılığı artmış olacaktır. Ancak EKS genellikle 7 gün 24 saat çalışmak zorunda olduğu ve çok az sayıda tesisin test ortamı bulunmakta olduğu için güvenlik sistemlerinin güncellenmesi ve yama dağıtımın yapılması zordur. Yama geçilmemiş sistemlerde önemli güvenlik açıkları bulunabilir. Yazılım güncellemeleri, bu güncellemelerin endüstriyel kontrol uygulaması ve uygulamanın son kullanıcısı tarafından en ince ayrıntılarına kadar test edilmesi gerektiği ve EKS kesintileri planlı şekilde yapılmak zorunda olduğundan belirli zaman aralıklarında sürekli olarak gerçekleştirilememektedir. EKS güncelleme sürecinin bir parçası olarak yeniden doğrulama ihtiyacı duyabilir. EKS'nin pek çoğunun işletim sistemleri eski sürüm olup üreticileri tarafından desteklenmemektedir. Mevcut yamalar uygulanabilir durumda değildir.

Kimi durumlarda da EKS'nin kullanılmakta olduğu kritik altyapılarda bazı sistem yazılımlarının özel sürümleri kullanılmaktadır. Örneğin Duke Enerji gibi bir enerji şirketi Windows 10 işletim sistemi yerine Duke Enerji için özelleştirilmiş Duke Enerji Windows 10 işletim sistemi kurulu olabilir. Bu tarz özelleştirilmiş yazılım ortamlarına yüklenecek yama, mevcut yazılım ve donanım bileşenlerine uyumsuzluklara ve dolayısı ile önemli hasarlara neden olabilecektir. Yamanın üretilmesi ve ilgili sitemlerde kurulumunun yapılması çok hızlı bir şekilde gerçekleştirilirken özelleştirilmiş yazılımlar için yamanın özelleştirilmesi daha uzun zaman alabilmektedir. Bu süreç içinde yama geçilmemiş sistemler, genel olarak bilinen bir güvenlik açığına karşı savunmasız kalabilmektedir (Puyvelde ve Brantly,2019:367-368).

- Genellikle EKS, elektrik şebekeleri, petrol boru hatları, su arıtma sistemleri ve barajlarda olduğu gibi birbirinden uzakta ve izole durumda olan ekipmanlarla çalışmakta olup erişim için harici fiziki bir bağlantı kullanılmaktadır. Fiziki olarak uzak mesafelerde farklı coğrafi alanlarda çalıştırılan sistemler veri iletişimi aşamasında verilerin şifrelerin ya da kripto anahtarlarının çalınması gibi sorunlara karşı savunmasız kalabilmektedir.

- Her biri farklı işlevlere sahip çeşitli ağ bileşenlerine bağlı ayrı teknolojilere sahip çok sayıda cihazın (OT) oluşturduğu ortam saldırı vektörlerini artırmakta ve siber güvenliği geleneksel bilişim sistemlerinin güvenliğinden çok daha zor duruma getirmektedir (Tanczer vd.,2019:39).

- EKS, karmaşık bir sistemdir ve genellikle ekipman ve güvenlik açığı yönetimi için kullanılmakta olan güvenlik politikaları farklı satıcılardan temin edilebilmektedir. Bir EKS'nin kurulmasında, bu sistem hakkında detaylı teknik bilgiye sahip olmayan görevli genellikle sistemin yapılandırılmasında programlanmasında entegratörün desteğini alır. Operasyonel modda EKS'nin yönetimi için farklı alanlarda becerileri olması gereklidir. BT cihazlarını yöneten personel, OT sistemini yöneten üretim ve bakım personelinden farklıdır. EKS'nin BT bölümü, OT bölümünden bağımsız olarak BT bölümü tarafından yönetilir (Flaus,2019:66). Bunlara ek olarak, EKS'nin sahipleri ve işletmecileri, kamu, özel sektör, kamu işletmesi olabileceği için net bir risk etki alanı ve en iyi uygulama örneği bulunmaması da riskler arasında sayılabilir (Henrie, 2012:202).

- EKS işletim sistemleri ve uygulamaları çok karmaşık olduğu için EKS'nin güvenliğine yönelik sorunların giderilmesi için kontrol mühendisleri, kontrol sistem operatörleri ve BT güvenlik profesyonelleri kurulum, işletim ve bakım işlemlerinde birlikte çalışmalıdır. EKS alanında çalışan BT profesyonelleri, bilgi güvenliği teknolojilerini uygulamaya koymadan önce bu sistemlerin güvenilirliğinden emin olmalıdır. EKS üzerinde çalışan bazı işletim sistemleri ve uygulama yazılımları, EKS'nin özelleştirilmiş çevre mimarisi nedeni ile BT güvenliği için kullanılmakta olan ticari yazılımlarla uyumlu çalışamayabilmektedir. (NIST SP 800-82r2, 2015:2.17).

- Endüstriyel tesislerin, çalışanlar, çevre ve insanlar açısından riskli durumlar yaratma olasılıkları geleneksel bilişim sistemlerine göre çok daha fazladır. Üretim ekipmanlarının arızalanması durumunda da sonuçta üretilen ürünün kalitesi önemli risklere neden olabilmektedir. Bu tür risklerin yönetilebilmesi için güvenlik yönetim sistemleri kullanılabilmektedir. BT bölümünün sorumluluğunda gerçekleştirilmekte olan Bilgi Güvenliği Yönetim Sistemi, OT sistemlerinin güvenliğini yönetmede tek başına yeterli olamamakta ancak BGYS kontrollerinden yararlanılabilmektedir. BT'nin OT için oluşturabileceği riskleri tam olarak algılanamamaktadır. Örneğin erişim yetkilerinin

yönetilmesinde geleneksel bilişim sistemlerinde kullanıcılar ve yöneticiler arasında ayrıcalıklar belirlenir. Bir EKS'nde ise kişi bazlı yetki tanımlaması yerine görev bazlı yetkilendirmeler yapılır. 8 saatlik vardiyalı sisteme göre sürekli çalışmakta olan SCADA operatörleri genellikle aynı kimliği kullanarak görevlerini yerine getirmektedir. Bilgisayar işletim sisteminin yönetilmesine ek olarak PLC parametrelerinin ve programlarının da güncellenmesi gerekmektedir. Genellikle uzaktan müdahale ile sistemin kullanıma sokulması için geliştirme görevi bir dış firmaya yaptırılmaktadır. Bu erişimler güvenlik açısından çok da iyi kontrol edilememektedir (Flaus,2019:67-68).

- Mevcut durumda, endüstriyel nesnelerin interneti (IIOT) olarak da anılmakta olan saha cihazları, temel güvenlik özelliklerine sahip olmadıkları için siber güvenlik açısından önemli zayıflık noktalarıdır. Siber saldırganlar, varsayılan parolaları deneyerek kolaylıkla bu sistemlere erişebilmektedir. Büyüyen cihaz ekosistemi, bilgisayar korsanlarının bu cihazlara erişmek üzere botnet geliştirme iştahlarını artırmaktadır. Sensörler aracılığı ile çok büyük miktarda yeni veri türleri toplanmasını sağlayacak milyarlarca sensörden oluşan birbirine bağlı sistem muazzam bilgi kaynağı sağlayabilmektedir. (Puyvelde ve Brantly,2019:443).

- EKS'nin geleneksel BT sistemlerinden operasyonel açıdan ve oluşturacakları riskler açısından farklılıkları nedeni ile, siber güvenliğinin sağlanması daha karmaşık yöntemler gerektirmektedir. Bu sistemlerin faaliyetlerinin yerine getirilmesinde olduğu gibi siber güvenliklerinin sağlanmasına yönelik kontrol sistemi çalışmasıyla bağlantılı olarak güvenlik çözümlerinin kurulumu, çalıştırılması ve bakımının olası etkilerini anlamak için de kontrol mühendisleri, kontrol sistemi operatörleri ve BT güvenlik uzmanlarının bir ekip olarak çalışmaları gerekir (NIST SP 800-82r2, 2015:2-17).

- EKS şemsiyesi altında toplanan Programlanabilir Mantık Denetleyicileri (PLC), Akıllı elektronik cihazlar (IED), Uzak Terminal Birimleri (RTU) ve bu sistemleri yönetmekte kullanılan G/Ç cihazları gibi yerel ya da dağıtık sistemlere yeterince hakimiyet bulunmamaktadır. Büyük ölçekli coğrafi olarak dağıtılmış, eski ve tescilli sistem bileşenlerini birleştiren bu ortam Güvenlik Operasyon Merkezleri ve Siber Acil Müdahale Ekipleri için önemli zorluklar yaratmaktadır. Geçmişte EKS, kamu iletişim altyapılarına bağlı olmayan ayrı ağlar olarak çalıştırılmıştır ancak zaman içinde işletmeler İnternet üzerine

sağlanan hizmetlerden ve verilerden yararlanmaya yöneldikçe bu sistemlerin güvenlik sorunları da artmaya başlamıştır. Gerçek zamanlı izleme, noktadan noktaya iletişim, çoklu oturumlar, bakım ve yedeklilik ile sağlanan faydalar sayesinde bu sistemlerin sunduğu hizmetlerde de iyileştirmeler sağlanmıştır. Bu karşılıklı bağlantılılık akıllı şebekelerin yaygınlaşması ve endüstriyel nesnelerin internetinin yaygınlaşması ile daha da artacaktır. Kuruluşlar sorunların tespitinde araçlara değil personele güvenmektedir (Maglaras vd.,2018:43). Sistemler birbirleri ile bütünleştiği için bir geleneksel bilişim sisteminin nerede başladığını ve nerede bittiğini, EKS'nin nerede başlayıp nerede bittiğini, net olarak gösteren bir ayıraç bulunmamaktadır. (Perdikaris, 2014, s:108).

EKS (Operasyonel Teknolojiler)	**Geleneksel Bilişim Sistemi (Bilişim Teknolojileri)**
Fiziksel ortam ve dijital ortam verileri	Sadece dijital ortam verileri
Fiziksel ortamın güvenliğinin sağlanması gerekmektedir	Sadece dijital ortamın güvenliği
Kullanılabilirlik ve erişilebilirlik	Gizlilik bütünlük erişilebilirlik
Gerçek zamanlı faaliyet. Sistemler istenen zamanda durdurulup yeniden başlatılamaz.	İstenilen zamanda çalıştırılabilir ya da durdurulabilir
Gerçek ortam verisi hassasiyeti vardır.	Veri hassasiyeti hayati önemde değildir.
Merkezi yönetim ve güvenlik imkanları kısıtlı. Güvenliğe yönelik yama uygulamasının eklenmesi ve güvenlik yazılımlarının devreye alınması çok daha zor.	Merkezi yönetimleri kolay yama uygulaması ya da güvenlik yazılımlarının kurulması, güvenlik uygulamalarının kullanımı daha kolay .
Yazılım ve donanımın uygulamaya konulması öncesinde test ortamı oluşturulması çok zor kimi durumlarda olanaksız.	Yazılım ve donanımın uygulamaya konulması öncesinde teste tabi tutulması çok daha kolay.
15-20 yıllık sürelerle kullanılabilir. Standart modüller ya da eski cihazlar.	3-5 yılda bir yenilenebilir, veri aktarımı kolay.
Fiziksel olarak uzak mesafelerde konuşlanmış olabilmektedirler	Yerel Alan Şebekeleri birbirine geniş allan ağları ile bağlanmaktadır.
Fiziki çevreye yönelik güvenlik sorunları oluşturma riskleri daha yüksek.	Fiziki çevreye yönelik güvelik sorunları oluşturma olasılığı daha düşük
Özel işletim sistemi yazılımları kıullanılabilmekte ve bu yazılımların güncellenmesi daha zor.	Standart ve herkes tarafından kullanılmakta olan işletim sistemi yazılımları kullanılmakta ve kolayca güncellenmektedir.

Tablo 3: EKS ve Geleneksel Bilişim Sistemlerinin farkları

2.1.4 Kritik Altyapıların Birbirine Bağımlılığı

Başlangıçta geleneksel bir şekilde, birbirleri ile etkileşimi ve bağımlılıkları bulunmaksızın fiziksel olarak birbirinden bağımsız sistemler olarak tesis edilen kritik

altyapılar, zamanla teknolojik gelişmelere uygun olarak, temel işlevlerinin yerine getirilmesinde endüstriyel kontrol sistemlerinin kullanılmaya başlanması ile farklı fiziki alanlarda tesis edilmeye ve birbirine ağlarla bağlı hale gelmeye başlamıştır (Radvanovsky, 2018:58). 1900'lü yılların başlarında, gezegenlerin hareketleri ile ilgilenmekte olan matematikçilerden Poincare, kullandıkları denklemlerde, girdiler üzerindeki yuvarlama hataları olarak düşünülebilecek çok küçük etkilerin, önemli ölçüde farklı bazı durumlarda tamamen hatalı sonuçlara neden olabildiğini fark etmiş ve doğrusal olmayan Kaos Teorisini öne sürmüştür. Ünlü kelebek etkisi de buradan gelmektedir. Kaos teorisine göre Brezilya'da kanat çırpan bir kelebek, 2 yıl sonra Teksas'da fırtınaya neden olabilir. Başlangıçta meydana gelebilecek çok küçük bir sapma dramatik sonuçlara neden olabilecektir. Sürprizlerin, doğrusal olmayan ve öngörülemeyenlerin bilimi olarak tanımlanan Kaos Teorisi, önceden tahmin edilemeyen ve kontrol etmenin imkânsız olduğu doğrusal olmayan olaylarla ilgilenmektedir (Macaulay, 2009:6). Kritik altyapıların birbirine bağımlılığının artması ile de doğrusal olmayan kaotik dünyanın herhangi bir yerinde meydana gelen bir sorun dünyanın diğer yerlerinde de etkisini gösterebilir duruma gelmiştir. Birbiri ile bağlantılı bu sistemler, doğrusal olmayan kaotik sistemlerin özelliklerini taşıdıkları için güvenliklerinin sağlanması daha da zorlaşmaktadır.

Farklı kritik altyapı sektörleri arasındaki bağımlılığın çok olması, çok miktarda güvenlik açığı olması nedeni ile savunmasız halde bulunması, alternatifi olmaması gibi durumlar, o kritik altyapının kritiklik seviyesini arttıran etkenler arasındadır (Bennet, 2018:44-45). Kritik altyapılar, değişik sanayi sektörleri ve iş ortakları ile olan karşılıklı bağımlılıkları nedeni ile sistemler sistemi olarak tanımlanmaktadır. Bu sistemler fiziki olarak ve bilişim teknolojilerinin kullanıldığı alanlar olarak yüksek seviyede entegre olup karmaşık bir biçimde karşılıklı bağımlılıkları vardır. Elektrik iletim ve dağıtım şebekeleri elektriği, binlerce kamu ya da özel sektör kuruluşunu kapsayan yüksek seviyede birbirine bağlı ve dinamik sistemleri işleterek son kullanıcılara ulaştırmak için, coğrafi olarak dağıtık yapıda konuşlandırılmış EKS teknolojilerini kullanmaktadır. EKS'nin coğrafi olarak uzak alanlarda kurulan kontrol istasyonlarından gelen verileri toplayarak faaliyeti görüntüleme ve kontrol edebilme özelliklerine sahip türü olan SCADA sistemler su, petrol, doğal gaz iletimi ve kanalizasyon sistemleri için kullanılmaktadır.

EKS, kimya sektörü, kritik üretim sektörü, barajlar, ulaşım, enerji, gıda ve tarım, su ve atık su sistemleri, nükleer reaktörler gibi kritik altyapı tesislerinin en temel bileşenleri arasındadır (Hahn,2016 ,s:54). Bir kritik sistemde oluşan sorunun diğer kritik sistemi de etkileyebilmesine neden olan karşılıklı bağımlılıklar söz konusudur (Macaulay, 2009:1-2). Kritik altyapılar hem fiziksel olarak hem de bilgi ve iletişim teknolojileri aracılığı ile birbirlerine bağlıdır ve karşılıklı bağımlılıkları vardır. Bu nedenle EKS'deki bir olay doğrudan veya dolaylı olarak bağımlı altyapıları zincirleme olarak etkileme kapasitesine sahiptir. Örneğin petrol arıtma tesislerinin çalışması için nükleer santrallerde enerji üretilmesine, üretilen bu enerjilerin enerji nakil hatları ile dağıtımının yapılmasına ihtiyaç vardır.

Enerji iletim ve dağıtım şebekeleri, son kullanıcılara elektrik temin etmek üzere kamu ya da özel sektör firmaları tarafından işletilmekte olan çok sayıda firmadan oluşan birbirleri ile bağlantılı dinamik sistemler, coğrafi olarak dağıtılmış SCADA kontrol teknolojilerini kullanmaktadır. Enerji üretim, iletim ve dağıtımı süreçlerinde SCADA ve Dağıtık Kontrol Sistemleri birlikte kullanılabilmektedir. Elektriğin, birbirine bağımlı kritik altyapılardaki en yaygın bozulma nedeni olduğu düşünülmektedir. Enerji nakil işleminde kullanılmakta olan SCADA sistemin iletişim ağındaki bir arıza, zincirleme sorunlara neden olabilecek durumdadır. Takip ve kontrol işleminin yapılamıyor olması, büyük bir enerji üretim biriminin devre dışı kalmasına, bu da zincirleme olarak bir iletim alt istasyonunda güç kaybına neden olacaktır. Bu güç kaybı, dağıtım şebekesinde kademeli bir arızanın tetiklenmesi yolu ile petrol ve doğal gaz üretimini, rafineri faaliyetlerini, su arıtma sistemlerini, atık su toplama sistemlerini, elektrikle çalışan boru hattı taşıma sistemleri gibi kritik tesislerin faaliyetlerinde kesintilere yol açabilecektir (NIST SP 800-82r2, 2015:2.3).

Bir bileşendeki bir bozulma, diğerleri üzerinde de zincirleme olarak olumsuz durumlar yaratabilecektir. Bilişim teknolojileri kullanılarak işlevini yerine getirmekte olan bir enerji üretim ve dağıtım sisteminde meydana gelebilecek bir sorun, bu sistemin ürettiği ve dağıtımını sağladığı elektriğin iletilememesi sonrasında, sadece yerel bir bölgede değil çok geniş alanlarda elektrik kesintisine neden olabilecek ve pek çok sistem devre dışı kalabilecektir. Bulut bilişim teknolojisi kullanılarak üzerinde verilerin tutulduğu ve servislerin çalıştırıldığı bir veri merkezinde oluşabilecek bir arıza, bu veri merkezinden

hizmet almakta olan diğer pek çok sistemi zincirleme olarak çalışamaz duruma getirebilecektir. Böyle bir veri merkezinin hizmetinde kesinti meydana gelmesi durumunda, iletişim, ulaşım üretim gibi kritik sektörlerde kesintiler yaşanabilecektir.

Son dönemde yaygın bir şekilde birbirlerine ağlarla bağlı kritik altyapı tesislerinin faaliyetlerini yerine getirebilmesi için, bu sistemleri birbirine bağlayarak aralarında veri aktarımını sağlayan iletişim altyapısına da bağımlılıkları vardır. İnternet altyapısında ya da bu sistemlerin kullandığı özel iletişim altyapısında bir kesinti olması, bu altyapılara kapasiteleri üstünde veri yüklenerek çalışamaz hale getirilmeleri durumunda bağlı oldukları sisteme veriler aktarılamayacağı için faaliyetler yerine getirilemeyecektir.

Macaulay, fiziki dünya paralelinde oluşturulan ve birbirlerine ağlarla bağlı bilişim teknolojisi ürünlerinin yer aldığı siber uzayı, tüm sektörleri birbirine bağlayan sinir sistemi olarak nitelendirmektedir (Macaulay, 2009:263). Farklı işlevleri yerine getirmek üzere hizmet vermekte olan kritik altyapı tesisleri, 1980'li yıllardan itibaren uygulanmakta olan neoliberal politikalar bağlamında, sadsece devletler tarafından değil daha çok özel sektör firmaları tarafından işletilmektedir. Çoğu zaman bu özel sektör firmaları, farklı devletlerin egemenliğinde olan büyük çok uluslu firmalardır. Bir kritik altyapı tesisinin yerine getirmekte olduğu faaliyet sadece o devletle sınırlı kalmamakta ve başka devlet sınırları içinde de işlemine devam edebilmektedir. Örneğin bir petrol boru hattı, bir ülkeden başlayıp diğer ülkelerin fiziki sınırları içinde devam etmekte ve çok farklı nihai ülkelere petrol taşıma işlevini yerine getirebilmektedir. Bu petrol boru hattında, uzaktan yönetim ve görüntüleme sistemi olarak kullanılmakta olan SCADA sistemin işletilmesi ve yönetimi de farklı bir ülkeden gerçekleştirilebilmektedir. Çoğu kez uluslar üstü büyük firmalar bu işlevi gerçekleştirmektedir. Bu gibi durumlarda, ulus devlet sınırlarının bir anlamı kalmamakta ve zincirleme bir bağımlılık da ortaya çıkmaktadır. Fiziki sınırlar kullanılarak birbirinden ayırt edilemeyecek bu sistemlerin bir siber olay sonrası işlevlerini yerine getirememeleri halinde olumsuz etkileri belli bir ülke ile sınırlı kalmayıp bölgesel hatta küresel ölçekte hissedilebilir duruma gelebilmektedir. BİT altyapılarının birbirleri ile olan sistemik bağımlılığı nedeni ile yerel olarak gerçekleşen bir siber güvenlik olayı bölgesel hatta küresel nitelik kazanabilmektedir. (Irion, 2013:85)

Günümüzde uygulanmakta olan teknolojik bağımlılık da değinilmesi gereken bağımlılıklar arasında sayılabilmektedir. Gelişmiş ülkeler tarafından üretilmekte olan yazılım, donanım ve ağ ürünlerinden oluşmakta olan EKS çok sayıda devletin kritik altyapılarının faaliyetlerinin yerine getirilmesinde kullanılmakta; bu da gelişmekte olan devletlerin, zorunlu hizmetlerin yerine getirilmesinde, teknolojik açıdan gelişmiş devletlere bağımlı hale gelmesine neden olmaktadır. Buna bir örnek de Çin'in kendi teknolojilerinin ve standartlarının kullanımını yaygınlaştırma yolu ile diğer devletlerin kendisine bağımlı hale gelmesini sağlamak üzere Baltık, Akdeniz ve Arktik denizlerinde fiber optik denizaltı kablo ağları üzerindeki etkisini hem satın alarak hem de inşa ederek genişletmek istemesi gösterilebilir (Arcesati, 2020).

Enerji tedarik sektöründe sanal sistemler ve fiziksel altyapı arasındaki karşılıklı bağımlılıklar da önemli riskler yaratabilecek niteliktedir. Akıllı şebeke cihazları arasındaki iletişimde meydana gelebilecek siber olaylar enerji kaybı; aşırı enerji yüklenmesi; şebeke boyunca cihazların zarar görmesi ve çalışmaz hale gelmesi ile sonuçlanabilmektedir. Birden fazla ülkede elektrik şebekesinin kendisini çökertebilir. Sistemin çalışmasına verilecek zarar, tehlikeli aşırı güç sağlanmasına veya elektrik kesintilerine neden olarak enerji santrallerini farklı şekillerde etkileyebilir. İletişimin ve ağın kontrolünün kaybına neden olarak enerji üretiminin durmasına neden olabilir. Hizmet reddi (DoS) saldırıları ve dağıtılmış DoS (DDoS) saldırıları, akıllı şebekede enerji veya bilgi alışverişinin olmamasına neden olan bilgileri geciktirebilir, engelleyebilir veya bozabilir. Siber saldırılar, enerji iletimini etkileyebilir ve hizmetlerin bağlantısını uzaktan kesebilir (Tessari ve Muti.2021:21).

2.2 ENDÜSTRİYEL KONTROL SİSTEMLERİNİN SİBER GÜVENLİĞİ

Bilişim sistemlerinin kullanılmaya başlandığı dönemlerde siber güvenlik dendiğinde akla ilk gelen bilişim sistemleri üzerinde tutulan, işlem gören, iletilen verilerin ve bilgilerin güvenliğinin sağlanması idi. Bilgi güvenliğinin unsurları olarak gizlilik, bütünlük ve kullanılabilirlik sayılırken son dönemlerde bu üç unsur, siber güvenliğin sağlanmasında yetersiz kalmaya başlamıştır. Siber uzayda programlanabilir nesnelerin artması, endüstriyel otomasyon ve kontrol sistemlerinin kullanılmaya başlanması ile bu sistemler üzerindeki

bilginin güvenliğinin sağlanmasının yanı sıra insanların ve onların içinde yaşadığı fiziki ortamların da güvenliğinin sağlanması ihtiyacı doğmuştur (Perkins ve Byrnes, 2015). Endüstriyel otomasyon ve kontrol sistemlerinin geleneksel bilişim teknolojileri ile birlikte kullanılmaya başlanması gerçek fiziki dünya ile dijital dünya arasındaki çizgiyi bulanıklaştırmıştır. Enerji üretim ve dağıtım hatları, petrol rafinerileri, su artma tesisleri vb. kritik altyapılarda bilişim teknolojilerinin her geçen gün artan bir şekilde yaygın olarak kullanılması bu ihtiyacı daha da görünür hale getirmiştir. Siber güvenlikte çerçeve genişlemiş olup sadece soyut bilginin güvenliği değil, tüm bilginin ve uygulamaların üzerinde işlendiği iletildiği, saklandığı siber uzayın ve fiziki çevrenin güvenliğinin de sağlanması ihtiyacı doğmuştur. Endüstriyel kontrol sistemlerinde ve bilişim teknolojisi sistemlerinde, bilgisayar kaynaklarının, ağların ve ilgili ekipmanların eylemlerini gerçekleştirirken güvenilir, verimli ve emniyetli bir şekilde çalışması önemlidir (Krutz,2017:34). EKS için birincil güvenlik odağı, veri koruma ve gizlilikten ziyade sistemlerde operasyonel bütünlük sağlamaya yöneliktir. Bu nedenle, bir kuruluşun OT sistemleriyle ilişkili riskini ele almak için bir güvenlik programı geliştirirken kullanılabilirlik birincil endişe kaynağıdır (CIS-1:3).

Kritik altyapıların görevlerinin otomasyonunu sağlamak üzere 1960'lı yıllarda kullanılmaya başlanan siber fiziki sistemler ya da EKS, o dönemlerde internet olmadığı için diğer sistemlere bağlı olmadan tek başlarına çalışan cihazlardı. Genelde, dışarıdan gelecek zararlı yazılım ve saldırılara karşı korumalı durumda ancak içerden oluşabilecek tehditlere karşı korumasız durumdaydılar. İnternetin yaygınlaşması ile siber güvenliğe yönelik ortaya çıkan tehditler, sistemlerini BT sistemleri olarak görmeyen EKS kullanıcıları tarafından kendi sistemlerine yönelik tehditler olarak algılanmamıştır. Bu grup dış saldırganların EKS'ni yeterince bilmediği için kendi sistemlerine ilgi duymayacağını ve saldırıda bulunmayacağını düşünmektedir. O dönemde güvenlik sorunları daha çok kazara ya da memnuniyetsiz çalışanlar marifeti ile meydana gelmekte idi (Krutz, 2006:74). İlk dönemlerde endüstriyel otomasyon ve kontrol sistemleri, özel donanımlar ve ağlar üzerinden çalıştıkları için ve bütünleşik bilişim sistemlerinin baş belası olan ağ saldırılarına karşı dirençli oldukları düşünüldüğü için bu sistemler güvenli kabul edilmekte idi. Ancak son dönemlerde bu sistemlerin de geleneksel bilişim sistemleri ile entegrasyonları arttığı için

siber saldırılara maruz kalma potansiyelleri artmış ve bu güven ortamı ortadan kalkmıştır. (Susanto vd., 2014:88).

Siber fiziki sistemler olarak da anılmakta olan EKS günlük hayatın her alanına girdiği için kötü niyetli kişiler ve suçlular, bu sistemlerin güvenlik açıklarını avantaj olarak kullanmaya çalışmaktadırlar. Özellikle endüstriyel ve nükleer tesisler, yaptıkları işin önemine binaen saldırı hedefi olabilmektedir. Bu tür saldırıların hedefi olan kurumsal yapılar, sistemlerinin güvenlik sorunları olduğunu ifşa etmemek, diğer varlıklarının güvenliği hakkında şüphe uyandırmamak, ya da isimlerinin güvenilirliğini zedelememek gibi çok değişik nedenlerle saldırıya uğradıklarını saklı tutmaktadır.

Enerji sanayi sistemlerine yönelik tehditler, geçmişin tipik fiziki saldırılarının yanı sıra başka tehditler de artmaya başlamıştır. Bu fiziki saldırılar, kontrol sistemlerine yönelik siber saldırılar ile birleştiğinde çok daha büyük zararlar meydana getirebilecek kapasitededir. Hackerlardan örgütlü siber suçlulara ve kurum çalışanlarına kadar bir dizi siber saldırgan da siber araçlar kullanmak yolu ile fiziki etki yaratabilmektedir. (Susanto vd.,2014:88)

EKS'nin saha cihazları olarak adlandırılan, sensörler ve aktuatörlerden meydana gelen ve her biri farklı işlevlere sahip çeşitli ağ bileşenlerine bağlı ayrı teknolojilere sahip çok sayıda cihazın (IIOT) oluşturduğu ortam, saldırı vektörlerini artırmakta ve siber güvenliği geleneksel bilişim sistemlerinin güvenliğinden çok daha zor duruma getirmektedir (Tanczer vd.,2019:39). EKS'nin izole durumdan ağ tabanlı sistemlere dönüşmeleri ile siber güvenlik riskleri ve güvenlik açıklarında da yeni gelişmeler olmaya başlamıştır. Bu sistemlerde de pek çok kişi tarafından kullanılmakta olan ve bilinen yazılım donanım ürünlerinin kullanılmaya başlanması ile endüstriyel kontrol sistemlerine yönelik siber saldırı gerçekleştirebilecek, risk oluşturabilecek kişilerin sayısı da artmıştır (Henrie, 2012:204-205). Özel endüstriyel protokoller saldırılara açıktır ve esneklik ya da güvenlik sağlamazlar. Süreç kontrol ağları önce analogdan sayısala daha sonra ise sayısaldan IP sistemlere dönüşmüştür. Hem EKS birimlerinin üreticileri için hem de altyapı sahipleri için, kolayca temin edilebilen, kurulumu ve desteği kolay olan IP'ye geçiş hızlı bir şekilde gerçekleşmiştir (Macaulay ve Singer, 2011:51) Bu sistemlerin çalıştırıldığı ortamlarda bilinen güvenlik açıklarına sahip açık standart teknolojilerinin kullanılması; bu sistemlerin geleneksel bilişim ağlarının da bağlı olduğu diğer ağlarla bağlanması ve güvenliği sağlanmamış uzak

bağlantıların yapılmasının yanı sıra, kontrol sistemlerine ait teknik bilgilerin geniş kitlelerce erişilebilir olması da bu sistemlerin siber güvenliği açısından risk oluşturan durumlar arasında sayılmaktadır (Susanto vd., 2014:89).

Günümüzde, EKS de gelişmiş iletişim yeteneklerini kullanmakta ve süreçlerin etkinliğini, verimliliğini, mevzuata uyumluluğunu ve güvenliğini artırmak üzere birbirlerine ağlarla bağlanmaktadır. Bu bağlantı, özel bir tesisle ya da farklı kıtalarda bulunan tesislerle sağlanabilmektedir. Bir EKS'nin düzgün çalışmaması büyük felaketlere neden olabileceği için bu sistemlerin işlevlerini yerine getirmesini önleyecek elektronik etkilerin meydana gelmemesi çok önemlidir. (Bayuk vd., 2012:57).

Son dönemlerde bir endüstriyel kontrol sisteminin ekonomik ömrünün 15 ila 30 yıl arasında olduğu görülmektedir. Daha 15-20 yıl öncesine kadar, bilişim teknolojileri ve endüstriyel kontrol sistemleri teknolojik olarak birbirlerine bağlanamadığı için yazılım ve ağ güvenliği, kontrol sistemleri açısından hiç önemli değildi. Kontrol sistemleri bilişim ağlarına bağlı olmayan kendi başına çalışan sistemlerdi. Kontrol sistemlerinin, daha çok iş dünyasında kullanılmakta olan bilişim sistemleri ile aynı Internet Protokolunu (IP) ve işletim sistemlerini kullanmaya başlamaları ile bu sistemlere yönelik riskler artmıştır. Bu sistemlerin güvenlik açıkları konusundaki farkındalık her geçen gün artmaktadır. Endüstri kuruluşları, bilgi güvenliği profesyonelleri, kontrol mühendisleri, yöneticiler, kamu ve özel sektör çalışanları, bu sistemleri korumanın önemini her geçen gün daha iyi algılamaktadır. EKS'nin güvenlik sorunu olmadığı fikrinden bu sistemlerin güvenliğine yönelik güvenlik standartlarının geliştirilmesi, eğitime önem verilmesi, güvenlik önlemleri konusundaki en iyi uygulamalara odaklanılması aşamasına geçilmiştir (Krutz, 2006:87). Her geçen gün birbirine ağ ile bağlanmış cihazlar artmakta olduğu için BT tabanlı tehditler de mevcut BT kontrolleri ve güvenlik önlemlerine rağmen artmaktadır. SCADA ağ mimarisinin kendi zayıflıkları da bir başka problemdir. BT ağındaki bir sorun, en güçlü güvenlik duvarı ve saldırı tespit sistemi yazılımı kullanılsa da sistemin tümünde önemli güvenlik sorunları oluşturabilecektir.

SCADA ağları, uzak konumlardan verilerin toplanmasını, analiz edilmesini, pompa, vana gibi ekipmanların yönetilmesinde kullanılmaları önemli ölçüde verimlilik sağlamasından dolayı yaygın olarak kullanılmaktadır. Elektrik, doğalgaz üretim ve dağıtım;

su ve atık su arıtma, ulaşım gibi temel hizmetlerin sağlanmasında temel işlevleri yerine getiren ve kritik altyapılar arasında sayılmakta olan bu sistemlerin, siber uzayda var olan çeşitli tehditlere karşı korunması gerekmektedir (DOE-USA,2007:2).

Sanayide kullanılan cihazların sahipleri süreçlerin geleneksel olarak bu süreçleri destekleyen mekanik ve elektrik mühendisliği uygulamalarından kaynaklanan fiziksel problemlerini çözmeye alışmışlardır, gerçekleşmekte olan süreç içinde kontrol sistemlerine yönelik kasıtlı tehditlere alışkın değildirler. Fiziki süreçlerin siber güvenlik tehditlerinden bağımsız olduğu yönünde yanlış algılar mevcuttur (Macaulay ve Singer, 2011:82-83). SCADA sistemler, İnternetin icadından önce üretildiği için bu sistemlerin hala, kendi içinde izole olarak başka ağlara bağlı olmadan çalıştığını düşünenler vardır. Oysaki pekçok sistem mühendisi İnternet bileşenlerini, ağın nasıl genişlediği ya da internet bağlantısının sistemin güvenliğini nasıl etkileyeceğini dert etmeden SCADA sistem içine entegre edebilmektedir. SCADA sistem uzmanlarından pek çoğu, SCADA sistemler arası bağlantıların ve bütünleşik ağların güvenli olduğuna inanmaktadır. Eski teknoloji ürünü SCADA sistemlerin modern iletişim ağları kullanılarak birbirine bağlanması, uyumluluk sorununu gündeme getirmektedir. Bu durumda dış ağlardan yetkisiz erişimi önlemek üzere geliştirilen erişim kontrolleri yetersiz kalmaktadır (Alcaraz vd., 2015:6). EKS'nin internet sistemi üzerinden uzaktan erişim ve uzaktan operasyona imkân veriyor olması da zararlı yazılımların bulaşması gibi pek çok yeni tehditi ve zafiyeti beraberinde getirmektedir.

SCADA sistemlerin gerçekleştirmekte oldukları süreçlere siber uzay üzerinden yöneltilen saldırılarla maddi kayıplara, sağlık sorunlarına, can kayıplarına neden olabilir ve çevreye zarar verilebilir. Başarılı bir siber saldırının genel olarak ekonomik, toplumsal, çevresel ve psikolojik sonuçları, saldırının hedef aldığı sistemlere, bu sistemlerin yer aldığı konumuna ve sonuçta meydana gelen hasara bağlı olarak değişiklik gösterir. Bireysel saldırıların maliyetlerini belirlemek oldukça zordur. Yaratılan hasar bazı açılardan çok az gibi görülürken bazı açılardan ise yıkıcı sonuçlar doğurabilecektir (Panguluri vd., 2017, s:153).

2.2.1 Endüstriyel Kontrol Sistemlerindeki Siber Güvenlik Açıkları

Bir sistemin olağan durumu içinde yapması beklenen davranışı bozan durumlar güvenlik açığı olarak tanımlanmaktadır (Tabansky, 2017:212). EKS'nin güvenlik açıkları, bu sistemlerin üretilmeleri

aşamasındaki eksiklikler ya da bu sistemlerde hasar oluşturulmasına yönelik istismarlardır (Panguluri vd., 2017:144). EKS'nde yer alan bilgi sistemlerinin, sistem yordamlarının, kontrollerin ya da uygulamaların bir tehdit kaynağı aracılığı ile istismar edilmesi sonucu bu sistemin gerçekleştirmesi gereken işlevlerini yerine getirilememesine sebep olabilecek zayıflıklar güvenlik açığı olarak adlandırılmaktadır. NIST tarafından hazırlanan rehber dokumanda ise güvenlik açığı, "Bir tehdit kaynağı tarafından tetiklenebilecek ya da istismar edilebilecek uygulamalar, kontroller ya da sistem güvenlik yöntemleridir." şeklinde tanımlanmıştır (NIST SP 800-82r2, 2015:C-2). Gizlilik, bütünlük ve kullanılabilirlik unsurları ile tanımlanmakta olan bir sistemin güvenliğini olumsuz yönde etkileyebilecek güvenlik açıkları bir ya da daha çok tehdit tarafından kullanılabilir. Güvenlik açıkları bilinen sistemlere, saldırganlar tarafından bu güvenlik açıkları ve çeşitli saldırı teknikleri kullanılarak siber saldırı gerçekleştirilebilmektedir. Siber saldırılar, verinin ve sistemin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyecek siber etki oluşturma potansiyeline sahiptir. Saldırgan dokümanları ve verileri çalabilir, değiştirebilir ya da sisteme erişimi engelleyebilir. Siber saldırılar, süreçleri de sistemin tasarım özelliklerine bağlı olarak etkileyebilir. Bir saldırgan gerçek zamanlı verileri barındıran bir veri tabanının içeriğini değiştirerek sistem bütünlüğünün bozulmasına ve bu veri tabanının içerdiği verileri parametre olarak kullanan mekanizmanın normalden hızlı ya da yavaş çalışmasını sağlayabilir. Örneğin bir su sistemi için bu değişiklik su tankının belirlenen zaman diliminde gereğinde çok dolmasına; gereğinden çok su aldığında taşmasına neden olabilir. Ancak bunun gibi anormal durum gerçekleştiğinde örneğin gelen suyun kesilmesi gibi bir işlem tasarlanmışsa taşma işlemi gerçekleşmeden gerekli önlem alınmış olur. Bu sistemi iyi bilen saldırgan, sonraki aşamalardaki parametreleri de değiştirerek saldırısının başarılı olmasını sağlayabilir.

Günümüzde Endüstriyel Kontrol Sistemleri ve alt sistemleri, operasyonel teknolojiler ve bilişim teknolojilerinin birleşiminden meydana gelmektedir. Çakışan faaliyetleri tekilleştirme, yazılım, donanım, ağ ve bakım araçlarını standartlaştırarak maliyeti azaltmak, firmanın mali bilgileri ve müşteri verilerini SCADA sistemlerini kullanarak birleştirmek, kritik karar aşamasında kullanılmak üzere ayrıntılı veri sağlamak gibi amaçlarla daha bütünleşik işlemleri gerçekleştirmek üzere SCADA sistemler, geleneksel BT sistemlerine bağlanmaktadır (Krutz, 2006:37). Bu entegrasyonlar gerçekleştirilirken güvenlik ön planda tutulmadığı için önemli güvenlik açıkları meydana gelebilmektedir (Panguluri vd., 2017:150). SCADA sistemlerinin internet ağlarına bağlı olması,

geleneksel bilişim sistemlerinde bulunan güvenlik açıkları benzeri açıkların oluşmasına yol açabilecek niteliktedir.

Geçmişte iş ortamında geleneksel olarak kullanılmakta olan bilişim sistemleri ve SCADA sistemler, farklı teknolojiler kullandıkları için farklı ağlar üzerinden haberleşmekte idiler. SCADA sistemlerin iletişimi geleneksel bilişim sistemlerinin kullandığı IP bağlantısını desteklememekte ve seri bağlantı üzerinden çok düşük radyo frekans iletişim yöntemini kullanmakta idi. Bu sistemlerin farklı ağlar üzerinden haberleşiyor olması, SCADA sistemlerin internet ağına bağlanamadığı için saldırıya uğrayamayacağı düşüncesini doğurmuştur (Panguluri vd., 2017:150).

Yaygın bir kanıya göre EKS'lere saldırıda bulunabilmek için bu sistemler hakkında kapsamlı bilgi sahibi olunması gerektiği düşünülmektedir. SCADA sistemlerin, sıradan bilgisayarlarda bulunmayan özel güvenlik önlemlerine sahip olduğu gibi abartı düşünceler bulunmaktadır. Aslında orta seviyede bilgisayar programlama bilgisi olan bir kişi, SCADA sistemine ağ ile bağlanabilen bir bilgisayara sahipse SCADA sistemin çalışmasını durdurabilir. SCADA sistemlerin ilkel yapısından dolayı ortalama bir SCADA sistem modern bir bilgisayara göre daha fazla güvenlik açıklarına sahiptir. SCADA teknolojilerine sahip firmalar, iyi organize olmuş, motivasyonları yüksek, hacker olarak kendi niteliklerini test etmek isteyen siber teröristlerin hedefidir. (Alcaraz vd., 2015:6).

Enerji dağıtım hatları, petrol ve doğal gaz boru hatları gibi kritik altyapıların güvenli, verimli ve etkin olarak kullanılabilmesi için görüntülenmesi ve kritik durumların, alarm ve süreç bilgilerinin merkeze bildirilmesini kapsayan kontrol işlemi genel adlandırma ile EKS olarak adlandırılan modern SCADA sistemler kullanılarak gerçekleştirilmektedir. Böylesine zorlu bir işi başarabilmek için SCADA sistemleri saha cihazlarına ve kontrol odasındaki operatörün kullandığı kullanıcı arayüzüne bağlanmak için iletişim sistemleri, uzak terminal birimleri, bilgisayarlar, sunucular, yönlendiriciler gibi cihazlara bağımlıdır. Uzaktan kontrolü sağlamak üzere kullanılan çok sayıda fiziki bağlantı ve her geçen gün artan sayıda diğer sistemlere yapılan bağlantılar, SCADA sistemlerde siber güvenlik açıklarını da beraberinde getirmektedir. Bu bağlantıların artması ile dünyanın herhangi bir yerinden de bu uzak terminal birimine bağlanma olasılığı da artmaktadır. Çok sayıda kullanıcısı olan Windows gibi ortak işletim sistemlerinin kullanılıyor olması da güvenlik açıklarına sebep olmaktadır. Bu sistemleri kullanmayı bilen çok sayıda kişi bulunduğu için çok sayıda potansiyel siber sistem saldırganları olabilmektedir (Henrie, 2012:202-205).

Endüstriyel kontrol sistemleri, faaliyetlerini yerine getirirken, uygulama yazılımında belirlenmiş olan sınır değerleri arasında çalışmalıdır aksi durumda sistem görevini yerine getiremez duruma gelmiş olacaktır. Sınır değerleri büyük ölçüde içinde bulunulan duruma bağlıdır ve sonuç olarak sistemin mühendislik tasarımı ve analizi, kontrol sistemlerinin sınır değerlerinin doğru tanımlanması ile yakından ilişkilidir. Bu sınır değerler ve katlanılabilecek oranlar ile bunları aşan durumlarda yapılması gerekenler sisteme kodlanır. En ciddi arızalar, belirlenen sınır değerlerin aşılması ya da ayarların katlanılabilecek değerleri aşması ya da ayarlara sınır değerlerini veren kontrollerin mevcut durumda yetersiz kalması halinde meydana gelir. Örneğin bir su vanasının çok fazla miktarda açılıyor olması, boruları korumak açısından kontrol altında tutulmalıdır. Eğer bu vanayı kontrol eden programda hatalı değerler verilirse ya da verilen değerler değiştirilirse ya da kontrol, tasarlandığı gibi çalışmazsa uygulanan kontrol görevini yerine getirmez, çok miktarda su pompalanması sonucu sınır değerler aşılır ve borular patlar. Tüm sistemin uygun sınır değerleri içinde çalışmasını sağlamak için sensörler gerçek ve güncel verileri yansıtmalıdır. Boru patlaması örneğinde, hatalı sensör verisi, kontrol birimini aslında hızlı olan dönüş oranını çok yavaşmış gibi yönlendirirse kontrol biriminin, dönüş hızını boruların patlaması ile sonuçlanacak şekilde yükseltmesine neden olabilir.

Perdikaris'e göre, EKS'nin güvenlik açıklarından en önemli olan ilk 10'u aşağıdadır (Perdikaris, 2014:108);

- Operatör istasyonunun, operatörün kullanmadığı zamanlarda da açık olması ve bu yolla kimlik doğrulama işlemi yapılmaksızın yetkisiz kişilerin sisteme erişiyor olması;
- EKS cihazlarına fiziksel erişimin kolay olması,
- Korunmasız EKS ağlarına DSL ve/veya dial-up modem hatları ile uzaktan kimlik doğrulaması olmaksızın yetkisiz erişim,
- Ağdaki kablosuz erişim noktalarının güvenlik önlemlerinin alınmamış olması,
- EKS'nin doğrudan ya da dolaylı olarak yeterli güvenlik önlemlerinin bulunmadığı İnternet ortamına bağlı olması,
- EKS iletişim ağı üzerinde güvenlik duvarı bulunmaması ya da uygun ayarların yapılmamış olması,
- Sistem erişim kayıtlarının tutulmuyor olması,
- Saldırı tespit sistemlerinin kullanılmaması,
- İşletim sistemi ve EKS sistem yazılımlarının yamalarının güncel olarak geçilmemiş olması,
- Ağ ve/veya yönlendirici konfigürasyonunun güvenliksiz olması,
- Üretici tarafından sağlanmış olan fabrika ayarlarındaki şifrelerin değiştirilmemiş olması.

Amerika Birleşik Devletlerinin, bilgi güvenliği standartları ve rehber dokümanları hazırlamakla sorumlu kuruluşu olan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlattırılan, 2015 yılında yayımlanan ve 2021'de güncellenen Endüstriyel Kontrol Sistemlerinin Güvenliği Rehberinde (NIST SP 800-82r2, 2015) bu sistemlerde yer alabilecek güvenlik açıkları ayrıntılı olarak ele alınmış ve Yönetimsel Güvenlik Açıkları, Operasyonel Güvenlik Açıkları, Teknik Güvenlik Açıkları başlıkları altında toplanmıştır. Bu kısımda yönetimsel, operasyonel ve teknik güvenlik açıkları ve bunlara ek olarak Fiziksel güvenlik açıkları ve bu güvenlik açıklarının hepsinin meydana gelmesinde önemli bir faktör olan personelden kaynaklanan siber güvenlik açıklarına değinilecektir.

2.2.1.1 Yönetimsel Güvenlik Açıkları

- EKS güvenliğine ilişkin resmi politika, doktrin ya da yaptırım olmaması

Devletler ve toplumlar açısından hayati öneme sahip kritik altyapıların görevlerini yerine getirmesinde kullanılmakta olan EKS'nin güvenliğine ilişkin en üst seviye resmi politikalar ve bu politikaların yerine getirilmemesi durumunda uygulanacak yaptırımlar, bu sistemlerin siber güvenliğinin tüm kesimlerce dikkate alınması ve uygulanmasında etkili olacaktır.

- Üst seviye kurumsal hedeflerle bağlantısı sağlanmış, yazılı, yasalara uygun, üst yönetimin desteğini almış, personeli ve paydaşları kurum yararına doğru işleri yapmada zorlayıcı etkiye sahip, eğitici ve öğretici rolü olan bir kurumsal risk yönetimi politikasının bulunmaması ya da hatalı politikaların uygulanıyor olması önemli yönetimsel açıklar arasında sayılmaktadır (NIST SP 800-82r2, 2015:C-3). Üst yönetim tarafından desteklenen ve doğru uygulanan politikalar, paydaşlar ve çalışanlar tarafından daha ciddi bir şekilde dikkate alınacaktır.

- Ayrıntılı savunma stratejileri, yönetim ve erişim kontrol ihtiyaçları, kriptoloji kullanımı gibi üst seviye kavramlara ilişkin rehberlik hizmetinin de verilmiyor olması, yönetim, uyum sorunları ve standartların yazıldığı Kurumsal Risk Yönetimi raporu gibi ayrıntılı bir rehberin de hazırlanmıyor olması (Macaulay ve Singer, 2011:175-176). Uyulması gereken kuralların yazılı dokuman haline getirilmiş olması çalışanlar için eğitici nitelik de taşıyacaktır.

- EKS'nin güvenliğinden sorumlu kişiler için yetki ve sorumlulukları belirleyen ve sorumlulukların ortada kalmasını önleyecek nitelikte iyi tanımlanmış politikaların bulunmaması.
- EKS güvenliği için bir defalık değil süreklilik arz eden net bir güvenlik bütçesinin tanımlanmamış olması.
- Kurum personelinin mevcut ve güncellenmiş güvenlik politikaları, mevcut ve yeni oluşan güvenlik açıkları, tehditler, sanayiye yönelik siber güvenlik standartları gibi konularda güncel bilgileri edinmesini sağlamak üzere dokümantasyonu yapılmış, eğitim programlarının eksikliği ve ilgili personelin sistem güvenliğinden sorumlu tutulamaması (NIST SP 800-82r2, 2015:C-4).
- Güvenlik programının ve bileşenlerinin düzgün uygulanıp uygulanmadığının takibini sağlayan yöntemler ve çizelgelerden oluşan EKS Güvenlik Kontrollerinin yetersizliği.
- Yazılım, donanım ya da ağ sorunu gibi beklenmedik bir durum olduğunda işlemin nasıl yürütüleceğini açıklayan, test edilmiş, uygulamaya hazır beklenmedik durum planı bulunmaması.
- Sistemlerin birbirleri ile bağlantılarını, birbirlerini etkileme durumunu da içeren yazılı, ayrıntılı bir EKS konfigürasyon değişikliği yönetimi politikasının bulunmaması.
- Görevli personelin rolleri, sorumlulukları ve yetkileri, kurumun yerine getirmek zorunda olduğu işlevlere uygun olarak tanımlanmış ve belgelenmiş uygun erişim kontrol politikasının bulunmaması (NIST SP 800-82r2, 2015:C-5).
- Şifre, akıllı kart gibi yetki mekanizmalarının ne zaman kullanılacağı, ne kadar güçlü olacağı, güncellemelerinin nasıl yapılacağı gibi konuların yer aldığı yetkilendirme politikasının bulunmayışı (NIST SP 800-82r2, 2015:C-5).
- Siber olayı hızlıca tespit etmek, veri kaybı ve bozulmayı minimum seviyeye indirmek, daha sonra maruz kalınabilecek siber saldırıları, zararlı yazılımları tanıyabilmek, istismar edilebilecek güvenlik açıklarını en aza indirgemek ve EKS'ni siber olay öncesi mevcut durumuna geri döndürebilmek için siber olay tanıma ve karşılık verme planları, yöntemleri ve prosedürlerinin iyi tanımlanmamış ve belgelenmemiş olması, anormal

durumların sürekli izlenmemesi, olayların ele alınışının önceliklendirilmemesi, siber olaya ilişkin verilerin toplanmıyor olması, analiz edilmiyor olması ve rapor oluşturulması için verimli yöntemlerin kullanılmaması (NIST SP 800-82r2, 2015:C-5).

- Kritik Bileşenler için yedekliliğin bulunmaması: EKS'nin kritik bileşenlerinin yedekli olmaması, en ufak bir arıza durumunda sistemin devre dışı kalması.

2.2.1.2 Operasyonel Güvenlik Açıkları

- EKS trafiğinin geleneksel BT verileri trafiğinden ayrılmamış olması.

EKS ağının BT ağından ayrı yapılandırılması gerekir ancak bu tam anlamı ile sorunu çözmez. Gerçekleştirilen işin doğası gereği ve kolaylık sağladığı için ağlar her geçen gün daha fazla oranda birbirine bağlanmaktadır. Bütünleşik bir ağa giren saldırgan için, kolaylıkla hedeflediği SCADA sisteme ve cihaza tünel yaparak erişmek hiç de zor değildir. Pek çok SCADA sistem, güvenlik önlemi alınmadan İnternete bağlandığı için bu sistemler, internet kaynaklı virüsler ve solucanlar gibi güvenlik açıklarına maruz kalabilmektedir (Slay ve Miller, 2008:76).

- Yönetim hesapları ve rolleri için görevlerin ayrılmamış olması,
- Saldırı tespit, cevap ve raporlama yöntemlerinin kullanılmıyor olması,
- EKS ağında yer alan tüm BT ve EKS varlıklarının değişim yönetiminin, EKS Uzmanları ve BT Uzmanları tarafından, cihazın üreticileri ile de iş birliği yaparak kontrol altında tutulmuyor olması,
- EKS ağında yer alan tüm BT ve EKS varlıklarının kabul testlerinin ve zafiyet test yöntemlerinin belirlenmemiş olması.

2.2.1.3 Teknik Güvenlik Açıkları

Teknik sistem güvenlik açıkları, EKS'nin kurulması aşamasında donanım, aygıt yazılımı ya da uygulama yazılımlarından kaynaklanabilir. Bunlar arasında, tasarım hatası, hatalı konfigürasyon, bakım yetersizliği, yönetim yetersizliği, diğer sistemlerle ve ağlarla bağlantı sayılabilir.

EKS güvenliği konusunda rehber niteliğinde NIST tarafından hazırlanan (NIST SP 800-82r2, 2015:C-7-9) dökümanda teknik güvenlik açıkları, Tasarım ve Mimari; Konfigürasyon ve Bakım; Fiziki Güvenlik Açıkları başlıkları altında ele alınmıştır:

i. Tasarım ve Mimariden Kaynaklanan Güvenlik Açıkları

EKS'ne yönelik güvenlik tehditleri, standart bir işletim sistemi ya da yazılım uygulamasına yönelik tehditler kadar hızlı yayılmazlar. Geçmişte üretilmiş olan bazı EKS'nin elektronik parçası olarak açıklanabilecek gömülü (embedded) sistemlerin teknik özellikleri kendilerine özgü tek olduğu için ve güvenlik tehdidinin bir cihazdan diğerine bulaşması hemen hemen imkânsız idi. Bir gömülü sisteme yönelik güvenlik tehdidi cihaz üretilmeden önce tasarım aşamasında başlatılmakta idi (Farooq-i-Azam ve Ayyaz, 2012:180).

EKS'nin tasarımı aşamasında bütünleşik güvenlik tasarımının ihmal edilmiş olması; EKS'nin kullanımda olduğu süreç içinde yapılacak bazı değişikliklerin güvenlik sorunlarına neden olması; EKS'nde bir güvenlik kontrol kapsamının net olarak tanımlanmamış olması; kontrol trafiğinin ve işlem trafiğinin aynı ağ üzerinden iletilmesi; EKS için gerekli olan güvenilirlik ve erişilebilirlik ilkelerinin, bu sistemlerle birlikte kullanılmakta olan geleneksel bilişim sistemleri için de uygulanıyor olmaması; sistemin işleyişi ile ilgili yeterli log kayıtlarının toplanmıyor olması; düzenli olarak güvenlik takibinin yapılmıyor olması.

ii. Konfigürasyon ve Bakımdan Kaynaklanan Güvenlik Açıkları

Yazılım, donanım, aygıt yazılımı (firmware) gibi tüm varlıkların nerede kullanıldıklarını, yama durumlarını, çalışmadıklarında ya da yeterli savunma işlemi yapılamadığında ne tür sonuçlarla karşılaşılacağı bilgilerini kapsayacak şekilde bir yapılandırma yönetiminin bulunmaması; işletim sistemi ve üretici yamalarının geliştirilmemiş olması; EKS'leri testlerinin gerçekleştirilmemiş olması; güncellenmiş yazılımın alt birimlere dağıtımı için geçen sürede yeni güvenlik açıklarının oluşması; geçerlilik süresi dolan işletim sistemleri ve uygulama yazılımlarında yeni keşfedilmiş güvenlik açıklarının bulunması; güvenlik yamaları ile bakımın nasıl yapılacağını açıklayan yöntemlerin belirlenmemiş ve belgelenmemiş olması; kullanım desteği verilme süresi bitmiş işletim sistemlerinin bulunduğu EKS için güvenlik yamalarının geliştirilmediği durumlarda

oluşabilecek güvenlik açıklarını en aza indirgeyecek yöntemlerin belirlenmemiş olması; donanım, aygıt yazılımı ve diğer yazılımların test işlemine tabi tutulmaksızın güncellenmesi; güvenlik değişikliklerinde yetersiz test, uzaktan erişim kontrollerinin yetersiz oluşu; kötü konfigürasyonların kullanılıyor olması kritik konfigürasyonların yedeklenmemiş olması; taşınabilir cihazlar üzerindeki verilerin korunmuyor olması; güvenlik politikasına uygun olmayan parola oluşturma, kullanma ve koruma yöntemleri; uygulanmakta olan erişim kontrollerinin yetersizliği; uygun olmayan veri bağlantısı; kötü amaçlı yazılımlardan korunma amaçlı yazılımların kurulmamış olması ya da güncellenmemiş olması; yeterli teste tabi tutulmadan uygulanan kötü amaçlı yazılımlardan korunma; sistemim üzerinden hizmetin engellenmesi atakları; saldırı tespit ve önleme yazılımlarının kurulu olmaması; günlük erişim log kayıtlarının tutulmuyor olması. Test aşaması, sistem satıcıları ve entegratörler ile koordine ederek gerçekleştirilmelidir. EKS'ne, satıcı ve entegratörlerin sistem bakım fonksiyonlarını gerçekleştirebilmeleri için, uzak mesafede yer alan sistem bileşenlerine erişimi için uzaktan erişim imkânı sağlanmalıdır. Uzaktan erişim yetenekleri, yetkisiz kişilerin sisteme erişimini engelleyecek şekilde kontrol altında bulundurulmalıdır.

Gereksiz portların ve protokollerin kapatılmadığı sistemlerde tüm sisteme yönelik riskleri artıran durumlar ortaya çıkabilir.

iii. Yazılım Geliştirmeden Kaynaklanan Güvenlik Açıkları

- Uygunsuz veri doğrulama; sistemde yüklü olduğu halde varsayılan olarak etkinleştirilmemiş güvenlik önlemleri; yazılım içinde kimlik doğrulama, yetkilendirme ve erişim kontrolünün tanımlanmamış olması.
- Yama geçilmemiş sistemlerde önemli güvenlik açıkları bulunabilir. Yazılım güncellemeleri, bu güncellemelerin endüstriyel kontrol uygulaması ve uygulamanın son kullanıcısı tarafından en ince ayrıntılarına kadar test edilmesi gerektiği ve EKS kesintileri planlı şekilde yapılmak zorunda olduğundan her zaman belirli dönemlerde gerçekleştirilememektedir. EKS güncelleme sürecinin bir parçası olarak yeniden doğrulama ihtiyacı duyabilir. EKS'nin pek çoğunun işletim sistemleri eski sürüm olup üreticileri tarafından desteklenmemektedir. Mevcut yamalar uygulanabilir durumda değildir.

iv. İletişim ve Ağ Yapılandırılmasından Kaynaklanan Güvenlik Açıkları

Veri akış kontrollerinin kullanılmıyor olması; güvenlik duvarlarının bulunmaması ya da yanlış yapılandırılmış olması; güvenlik duvarları ya da aktif ağ cihazlarının log kayıtlarının yetersiz oluşu; saldırganlar tarafından da kullanımı çok iyi bilinen FTP, http, NFS gibi iyi dokümante edilmiş standart iletişim protokollerinin kullanılıyor olması; güvenli olmayan EKS protokollerinin kullanılıyor olması; iletişimde gönderilen verinin alınan veri ile aynı olduğunun kontrolü olan bütünlük kontrolünün eksikliği; kablosuz cihazlardan erişim noktası cihazlarına erişimde yeterli kimlik doğrulama ve veri koruması işlemlerinin yapılmıyor olması.

2008 yılında hazırlanan NIST 800-82r2 dokümanına göre (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77);

- EKS'nin çalıştırılması, bakımı ve güvenliği konusundaki sorumluluk gereği emniyet ve güvenlik arasındaki bağlantının anlaşılması önemlidir. EKS, sürecin sonunu kontrol etmekten doğrudan sorumlu oldukları için dikkatli bir şekilde korunmalıdır. Saha kontrol sistemlerini etkilediği için merkezi sunucunun doğru çalışıyor olması da önemlidir.

EKS fiziksel süreçlerle karmaşık etkileşim halindedir. EKS içine entegre edilmiş tüm güvenlik fonksiyonları normal işlevi değiştirmediklerini kanıtlamak üzere test edilmelidir. Günümüzde kullanılmakta olan EKS'nde fiziki ve mantıksal kontroller birlikte kullanılabilmektedir (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77); Bazı EKS için, otomatik yanıt süresi ya da insan müdahalesi için sistem yanıtı çok kritiktir. Bilgi akışı kesintiye uğramamalı ya da yetkisiz kişilerin eline geçmemelidir. Bu sistemlere erişim titizlikle yapılacak fiziki kontroller ile engellenmelidir (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77). Kontrol ağına yönelik sızma testleri rutin olarak değil, mevcut kontrol sistemlerinin çalışmasına zarar vermeden çok dikkatli bir şekilde yapılmalıdır. Bilgi güvenliği denetimleri rutin olarak yapılmamaktadır (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77);

- EKS güvenliği konusundaki farkındalık ve eğitim seviyesi düşüktür.
- Kontrol mesajları ve veriler kriptolanmadan gönderilmektedir.

SCADA sistemlerin kendilerine özgü mimarileri, protokolleri ve güvenlik önlemleri bulunduğu için BT güvenlik teknikleri ve araçlarının doğrudan SCADA güvenliği için kullanılması önerilmemektedir. Bunun yerine özellikle SCADA sistemlere yönelik hazırlanmış güvenlik çözümlerinin tasarlanması gerekmektedir. SCADA protokollerini anlayabilen ve endüstriyel ortamlarda çalışabilen araçlar şüpheli trafiği daha verimli bir şekilde tanıyıp etkisiz hale getirebilecektir (Slay ve Miller, 2008:80).

Geleneksel bilişim sistemleri güvenliği ve EKS güvenliği birbiri ile ilişkili fakat farklı uygulamalardır. Ancak güvenlik uzmanları bu iki sistemin birleşme noktalarında ya da ortak kullandıkları ağ ortamlarında dengeli olarak önlemleri almalıdır. Endüstriyel kontrol sistemlerinin verileri, mantıksal olarak farklı VLAN'lar, anahtarlar ve diğer teknikler kullanılarak mantıksal olarak bilişim sistemleri üzerinde tutulan verilerden ayrılmış olsa bile, geleneksel bilişim sistemleri verileri ile belli ortamlarda karışmış hale gelebilmektedir (Macaulay ve Singer, 2011:93). EKS'ni de içeren ağların güvenliğini sağlamak üzere geleneksel BT güvenliğinin sağlanmasında da en iyi uygulamalar arasında yer alan güvenlik duvarı, güvenli bölge (DMZ), VPN gibi uygulamalar kullanılabilmektedir.

İhtiyaca yönelik olarak bilgi sistemleri güvenliğine daha fazla önem verilmekte; standardizasyon kuruluşları konu ile ilgili yeni standartlar ve rehber dokümanlar oluşturmaktadır. En etkili güvenlik önlemlerini alabilmek için test ortamları yaratılmaktadır. Teknolojinin yaratıcısı olan gelişmiş ülkelerde bu tür önlemler alınmaya çalışılmakta ancak bu sistemler dünya üzerinde pek çok yerde kullanılmakta olup her kullanıcı aynı hassasiyete sahip değildir.

2.2.1.4 Fiziksel Güvenlik Açıkları

Bu tür güvenlik açıkları arasında yetkisiz personelin EKS cihazlarına fiziksel olarak erişebilir durumda olması; radyo frekansı, elektromanyetik darbe, statik deşarj, kesintiler ve voltaj yükselmeleri; enerji yedekliğinin sağlanmamış olması; çevresel kontrolün kaybedilmiş olması; fiziksel bağlantı noktalarının güvenli olmayışı sayılmaktadır.

Bunlara ek olarak deprem, yangın, sel, fırtına gibi tabiat olaylarının EKS cihazlarına ve iletişim hatlarına zarar verebileceği durumlar da fiziksel güvenlik açıkları arasında sayılmaktadır.

2.2.1.5 Personelden Kaynaklanabilecek Güvenlik Açıkları

Kritik altyapıların faaliyetlerini normal olarak yerine getirmesine engel olabilecek yönetimsel, operasyonel, teknik güvenlik açıklarında ve fiziksel güvenlik açıklarında bu sistemleri tasarlayan, gerçekleştiren, kullanan bilişim profesyonellerinin, kullanıcıların ve siber güvenlik uzmanlarının önemli etkileri olduğu görülmektedir. Bu kısımda, operasyonel teknolojilerde ve bu teknolojilerle bütünleşmiş hale gelen geleneksel bilişim sistemlerinde, personelden kaynaklanabilecek ve siber güvenlik açıklarına neden olabilecek durumlara yer verilmektedir:

i. Taşeron Çalıştırma

Fiziksel olarak birbirinden uzak mekanlarda konuşlandırılmış olan kritik altyapı sistemlerinin işletilmesinde iş yapma ve yaptırma şekilleri değişmiş, faaliyetlerin bir kısmı taşeron firma çalışanlarına devredilmiştir. Geçici personel tarafından gerçekleştirilmekte olan faaliyetlerin başarılı olabilmesi için kolayca anlaşılan veya kullanıcı kılavuzlarıyla desteklenen işletim sistemleri kullanılmaya başlanmıştır. Kimi durumlarda uzak mekanlarda yer alan bu sistemlere yetkisiz kişilerin müdahale etmesi gerekebilmekte, bunun için de sık aralıklarla değiştirilmeyen standart parolaların kullanılması veya parolaların yetkisiz kişilerle paylaşımı gündeme gelebilmektedir. Taşeron firma adına çalışan geçici personel, kritik altyapı tesisinin kendi personeli kadar yeterince tanınamayacağı, etkin bir şekilde izlenemeyeceği ve denetlenemeyeceği için niyetlerinin ve siber güvenliğe yönelik zararlı faaliyetlerinin anlaşılması çok daha zor olacaktır (Bridges,2013:84).

ii. Hazır yazılım ve Donanımların Kullanılması

Kritik altyapı tesislerinde, küresel seviyede standartlaşmış sistemlerin kullanılması yeni zafiyetleri de beraberinde getirmektedir. Özel yapım kontrol süreçleri yerine, hazır EKS kullanılması nedeni ile, çok sayıda kişi bu sistemlerin nasıl çalıştığı konusunda bilgi sahibi olabilmektedir. Hazır sistemler, kullanıma girecekleri ortamlardan çok uzakta farklı bir ülkede ve farklı bir şirkette tasarlanmış ve üretilmiş olması nedeni ile kuruluşlar, bu sistemlerden kaynaklanan tehditler hakkında erken uyarı bilgisi

alamayabilecektir. Aynı hazır sistemi kullanmakta olan kuruluşların, EKS dokümantasyonu ve kullanıcı kılavuzlarında yer alan bilgileri başkaları ile paylaşmaları durumunda güvenlik zafiyetleri oluşabilecektir.

iii. Personelin Eksik ya da Hatalı Bilgiye Sahip Olması

Aslında kolayca yönetilebilecek siber güvenlik olayları, bu sistemlerin kullanıcılarının eksik ya da hatalı bilgileri doğrultusunda asıl sorunu fark edememeleri ya da uygun olmayan güvenlik önlemleri nedeni ile hızla tırmanabilecek ve daha hayati önemde sorunlara yol açabilecektir. Kritik altyapılarda kullanılmakta olan endüstriyel kontrol sistemlerinin karmaşık veya eski olduğu için siber saldırılara maruz kalmayacağı düşüncesinin, bu sistemlerin kurulmasına veya bakımına yardımcı olan kişiler ya da zarar verme motivasyonu yüksek bir organizasyon tarafından saldırıya uğraması durumunda, geçersiz olduğu görülmüştür.

iv. Personelin Kendinden Beklenmeyen Davranışları

İnsanın karmaşık yapısı ve sistemin diğer öğeleriyle etkileşimi önemli siber güvenlik açıklarına neden olabilmektedir. Sistemler genellikle kurallara ve mantığa dayanır. Belirli bir girdi, belirli bir şekilde işlenecek ve kurallara göre belirli bir sonuçla son bulacaktır. Oysa insan davranışı bir dereceye kadar öngörülebilirdir. Çalışan personel, konu ile ilgili eğitimleri almış olmasına rağmen kimi durumlarda kendisinden beklenen davranışları sergilemeyebilecektir. İnsanlar, kurum içinde kutsal sayılan davranış yerine kendi istekleri doğrultusunda davranabilmektedir.

EKS'nin siber güvenliğinin sağlanmasına yönelik güvenlik sistemleri oluşturulurken, bu sistemlerin kullanıcılarının bazı güvenlik açıklarını fark ederek kullanma yeteneklerinin bulunduğu ve çalışan personelin görevlerini yerine getirmenin en basit yolunu arayacağı göz önünde bulundurulmalıdır. Sistemler sağlam teknoloji kullanılarak geliştirilmiş olmasına rağmen, kullanıcılar, mantık gerektirmeksizin bir bağlantıya tıklayabilmekte, basit şifreler seçebilmekte veya şifreyi bir parça kağıda yazabilmektedirler. Kullanıcılar, kendi motivasyonları ve eğilimleri nedeni ile sistem tasarımının gerektirdiği gibi davranmayabilmektedirler. Destek personeli, farklı sunuculara erişmek için aynı

parolayı kullandığı için saldırganlar ortak yerel yönetici parolalarından yararlanabilmektedir.

v. Personelin Siber Güvenlik Alanına Odaklanmaması

Kimi durumlarda, endüstriyel kontrol sistemlerinin siber güvenliğinin sağlanmasına yönelik çok çeşitli güvenlik teknolojileri kullanıldığı için sadece bu sistemlere ve güvenlik personeline güvenen çalışanlar kendi yaptıkları işe odaklanmakta; ekipmanlarının ve verilerinin güvenliğini dikkate almayabilmektedir. Bu duruma verilebilecek örneklerden birisi, kişiye özel yetkiler çerçevesinde kullanılması gereken farklı kullanıcı adı ve parolaların, sisteme erişimi ve gerçekleştirilecek faaliyeti kolaylaştırmak niyetiyle çok sayıda çalışan tarafından ortak bir kullanıcı adının kullanılması ve kolay anımsanacak basit bir parolanın çok sayıda kişi tarafından bilinmesi sistemde önemli güvenlik açıklarına neden olabilecektir. Sisteme, verilere ve kontrollere erişiminde yaşanabilecek sorunları azaltacak olan ortak kullanıcı adı ve basit parola kullanımı, güvenlik profesyonelleri tarafından sistem kullanıcılarının zeka seviyesinin yetersiz olduğu şeklinde değerlendirilmesine rağmen asıl hedefi kendi işlerini en kolay biçimde yürütmek olan kullanıcı açısından oldukça mantıklı bir davranış şeklidir. Kullanıcı personelin hassasiyeti ve işin nitelikleri çok fazla dikkate alınmaksızın tasarlanan ve gerçekleştirilen güvenlik sistemleri, kullanıcılar tarafından oluşturulacak güvenlik açıklarına sahne olabilecektir.

Çalışanlar, güvenlik sistemi içinde zayıflıklar oluşturan davranışsal bir sorundan dolayı, kimi durumlarda ise çoğu insanın uyum sağlayamayacağı güvenlik sistemi tasarımı nedeni ile parolayı kolay erişilebilir ortamlarda muhafaza edebilmektedir. Çalışan personelin görevleri basitleştirme ihtiyacı doğrultusunda kolay erişim sağlamak üzere, bilgileri gerekli özen göstermeksizin çoğaltarak yedeklemelerinin bir sonucu olarak yetkisiz kişilerin de bu bilgiye erişim riski artacaktır.

vi. Personel Temininde Güvenlik Özelliklerinin Göz Ardı Edilmesi

Kuruluşlar eleman alırken, güvenlik kurallarını uygulayıp uygulamayacağını çok fazla dikkate almaksızın örneğin kurallara bağlı kalmayı sevmeyen, prosedür ve düzenlemeleri anlamaya çalışmak için zaman harcamamayı tercih eden, güvenlik

gereksinimlerini göz ardı eden veya hatta bunlarla çatışan güvenlik sisteminin gerektirdiği şekilde davranmayacakları belli olan personeli işe alabilmektedir.

Kritik altyapı tesisleri çalışanlarının büyük çoğunluğu teknik veya mesleki alanda eğitime sahip olup temel görevleri güvenlik olmadığı için bu alana odaklanmamıştır. Bu personel, asıl işe odaklanma ihtiyacı veya gerçek bir güvenlik riskinin bulunmadığı gibi bahaneler ile güvenlik süreçlerine uymayabilmektedirler. Güvenlik kurallarına ve prosedürlerine uymayan personel, güvenlik kurallarının gereksiz ve bürokratik olduğu veya işi anlamayan kişiler tarafından konulduğu fikri ile kendilerini ikna ederek oluşabilecek riskleri dikkate almayabilmektedirler (Bridges,2013:94). Bu tür bireysel inançları değiştirmek üzere kurumsal seviyede faaliyetler gerçekleştirilmeli; verimli güvenlik uygulamaları kullanılmalı ve takibi sağlanmalıdır.

vii. Personelde Güvenlik Kültürünün Oluşmaması

Personelin sağlam bir güvenlik kültürünün bulunmaması, genellikle kuruluşların güvenliğinde zayıf bir halka olarak algılanmaktadır. Asıl görevini ne pahasına olursa olsun gerçekleştirmek isteyen ve güvenlik kavramı hakkında ayrıntılı bilgiye sahip olmayan ve bunun önemi üzerinde gerekli farkındalığa sahip olmayan personel, güvenlik süreçlerine ve kurallarına uymayabilecektir. Güvenliği sadece güvenlik bölümünün görevi olarak algılaması, meydana gelmekte olan siber güvenlik olaylarından ve zararlı sonuçlarından haberdar edilmemesi, bu personelin tehdit algısını ve güvenliğin gerekliliğini anlamamasına neden olabilecektir. Güvenlik sorunlarının sıklıkla yaşandığı ve bu sorunların bilmesi gereken seviyesinde personelle paylaşılarak siber saldırılara karşı kurumsal bir farkındalık oluştuulabilecektir (Bridges,2013).

viii. Kötü Niyetli Personel

Bazı çalışanların çeşitli nedenlerle sistemleri bozmaya veya hassas verileri elde etmeye eğilimleri olabilmektedir. Personel, görev süresi boyunca erişim yetkisi bulunduğu için edindiği, kullandığı verileri görevinin bitmesini müteakip de kullanmasının kendi hakkı olduğunu düşünebilmektedir. Kimi durumlarda da kendilerine gereken değerin verilmediği, haksız davranışlara maruz bırakıldığı hissine kapılmaları durumunda sadakat ve iş motivasyonları azalabilmekte, erişim yetkileri bulunan sistemler üzerinden hassas bilgileri

ele geçirip, kuruluş dışı suç örgütleri, diğer devletler ya da kişilerle paylaşarak ya da sonraki dönemlerde bizzat kendisi bu verileri kullanarak siber saldırılar gerçekleştirebilmektedir.

Kritik altyapı tesislerine siber saldırıların gerçekleştirilmesinde kullanılmakta olan IP adreslerinin genellikle teknik araçların kullanılması yerine o kuruluş içindeki memnuniyetsiz çalışanlardan edinildiği görülmüştür.

EKS'nin siber güvenliğini sağlamak amacı ile kullanılmakta olan güvenlik sistemlerinin, personelin asıl yapması gereken birincil görevlerini ne ölçüde desteklediği ve ne ölçüde ek yükler veya engeller oluşturduğu bilinmelidir. Kimi durumlarda, sistem kullanıcılarından kaynaklanan sorunlar ya da güvenlik sistemindeki süreçlerin veya prosedürlerin kötü niyetli kullanımı kritik altyapı sistemlerinin doğru bir şekilde görevini yerine getirmesini engelleyebilmektedir.

ix. Şeffaflığın Bulunmaması

Pek çok kuruluş, müşterilerinin veya paydaşlarının kendilerine olan güvenini kaybedeceği endişesiyle yaşadıkları güvenlik sorunlarını gündeme getirmekten kaçınmaktadır. Bu kuruluşta görev yapmakta olan personel, bir güvenlik ihlaline kişisel olarak dahil olmadıkça, siber güvenlik olaylardan haberdar olmayacaktır. Personelin, güvenlik yöneticileri tarafından sürekli olarak güvenlik süreçlerini takip etmeleri hususunda bilgilendirilmesi, ancak çalışanların güvenliğin bir sorun olduğunu düşündüren bir olayla asla karşılaşmamaları sonucu bu kavram gerçekçi bir sorun olarak algılanmayacaktır. Emniyet alanında potansiyel riskler, etkilenebilecek ilgili personele hızla iletilmelidir. Ancak karşılaşılan siber güvenlik olaylarının tüm personelle paylaşılması, personelin güvenliğin sadece güvenlik biriminde görev yapmakta olan personelin işi olmadığını görmesi ve güvenliğin önemi konusunda farkındalık yaratacaktır. Siber güvenlik farkındalığı, personelin kendi işyerlerindeki ani siber güvenlik olaylarına karşı hazırlıklı olmalarına yardımcı olacaktır. (Bridges,2013:92).

x. Evden Çalışma

Kurumsal siber güvenliğin sağlanmasında güvenlik yöneticileri, BT personeli ve diğer mesai arkadaşları, personelin bir siber güvenlik olayında olumsuz rol almasına engel olabilmektedir. Ancak son dönemdeki teknolojik gelişmeler ve zorunluluklar nedeni

ile kritik altyapı personelinin görevlerini uzak mesafe bağlantı ile evlerinden yerine getirmekte olduğu durumda kendilerine engel olabilecek ya da danışabilecekleri mesai arkadaşları bulunmayacağı için hatalı davranışlarda bulunabileceklerdir. Siber saldırılar, kurumsal siber güvenlik önlemlerinin bulunmadığı ev ortamından başlatılabileceği için, uzaktan çalışan bu personelin uyması gereken siber güvenlik önlemleri konusunda rehberlik hizmetleri verilmelidir (Bridges,2013:96).

xii. Sosyal Mühendislik

Gizli bilgileri elde etmek, erişim sağlamak veya bir kişiyi kandırarak veya manipüle ederek bir eylemde bulunmasını sağlamak 'sosyal mühendislik' olarak bilinmektedir. Personel, kimi durumlarda, sahip olduğu bilgilerin değerinin farkında olamayabilmektedir. Oysa görünüşte çok önemli olmayan bu kurumsal bilgiler, sosyal mühendislik saldırılarında kullanılabilmektedir. Sosyal mühendislik uygulamaları kapsamında, yabancılara ve kendileri hakkında endişeli görünen kişilere karşı kibar olma eğilimleri, zeki ve bilgili görünmekten hoşlanmaları gibi temel insan davranışları ve duyguları manipüle edilerek kişisel ve kurumsal bilgiler elde edilebilmektedir.

2.2.2 Endüstriyel Kontrol Sistemlerinin Siber Güvenliğine Yönelik Tehditler

Tehdit, kurumsal faaliyetleri, varlıkları, bireyleri, diğer kurumsal yapıları veya devletleri bir bilgi sistemi aracılığıyla yetkisiz erişim, imha, ifşa, bilgi değişikliği ve/veya hizmet reddi yoluyla olumsuz etkileme potansiyeli olan herhangi bir durum veya olaydır (NIST SP 800-39). Bir sistemin gizliliğini, bütünlüğünü ve kullanılabilirliğini bozmaya yönelik olumsuz etki oluşturma potansiyeli olan faaliyetler siber güvenlik tehditleri olarak anılmaktadır.

Bilişim teknolojilerinin kullanıldığı siber uzayda karşılaşılma olasılığı bulunan olumsuz durumlar siber tehdit olarak adlandırılmaktadır. Endüstriyel kontrol sistemleri de kritik altyapıların işlevlerini yerine getirmek üzere kullanılmakta olan siber fiziki sistemler olarak siber uzayda yer aldıkları için bu sistemlerin çalışmasının durdurulması ya da istenmeyen şekilde anormal çalıştırılmasının meydana gelmesi olasılığı EKS'nin siber güvenliğine yönelik siber tehdit olarak tanımlanabilir. EKS'nin faaliyetinin durdurulması ya da istenmeyen şekilde çalıştırılması, kritik altyapıların görevini, işlevlerini, imajını, örgütsel

varlıklarını, bu altyapılarla ilişkili diğer kurumları, devletleri, toplumları, bireyleri, diğer canlıları ve hatta ekolojik ortamı olumsuz etkileyecektir. Ulusal güvenliği tehdit, ağır hasar oluşturmak, ekonomiyi zayıflatmak, devlete olan güveni zedelemek, günlük faaliyetlerde aksaklıklar oluşturmak gibi nedenlerle kritik altyapıların temel bileşeni olan EKS'ne saldırılar düzenlenmektedir (Bennet, 2018:44-45).

Kasıtlı ya da kasıt olmaksızın güvenlik açığı yaratabilecek yöntemler tehdit kaynağı; istenmeyen etki ve sonuç yaratma potansiyeline sahip olaylar ya da durumlar ise tehdit olayıdır.

Geleneksel bilişim teknolojileri veri ile uğraşırken EKS'nin çalışma mantığında da veriler önemli rol oynamasına rağmen, bu sistemler daha çok fiziki dünyanın kontrolü için kullanılmaktadır. EKS'nin, geleneksel bilişim sistemlerinden farklı olarak güvenilirlik ve performans ihtiyacı bulunmaktadır. Geleneksel bilişim sistemlerinde siber güvenlik tehditleri, bu sistemler üzerinde tutulmakta, işenmekte, iletilmekte olan bilginin gizliliği, bütünlüğü ve erişilebilirliğine yönelik olup çoğu durumda bilginin gizliliği ve bütünlüğü ön planda tutulurken, EKS için siber güvenlik tehdidi ağırlıklı olarak bu sistemlerin çalışır durumda bir diğer deyişle kullanılabilir olmasına yöneliktir. EKS ağları geleneksel bilişim sistemleri ile aynı ağları kullanmaya başladıkları için BT sistemlerine yönelik siber tehditler de bu sistemlerin güvenliği açısından önemlidir. (Bayuk vd., 2012:58)

EKS varlıkları EKS ağına bağlı ve bu sistemi destekleyen yönetim konsolu, üzerinde koştuğu standart işletim sistemi, servis bilgisayarları, dosya yöneticileri gibi sistemler üzerinden doğrudan hedef gösterilebilir. Ya da veri alışverişi yapılan birbirine bağlı geleneksel bilişim sistemleri üzerinden dolaylı olarak hedef haline gelebilirler. EKS ağına uzaktan erişim çok zor olabilir ancak iç kullanıcıların erişimi daha kolaydır. EKS ağları hedeflendiğinde katmanlı saldırı teknolojileri daha kolaylıkla kullanılabilir. Tehditler doğrudan hedef PLC'lere, uzak terminal birimlerine, SCADA sistemlere olmak zorunda değildir; EKS'nin bulunduğu ağ içinde yer alan ve güvenlik açıkları bulunan işletim sistemleri ve uygulamalar aracılığı ile de etkili hale gelebilirler. Mevcut zararlı yazılımlar, kendilerini değiştirerek tanınmalarını ve yok edilmelerini önleyebilmektedirler. (Macaulay ve Singer, 2011:111).

Kritik altyapılarda, geleneksel BT sistemleri ve EKS birlikte kullanılmaya başlandığı için her iki sisteme yönelik siber tehditlerden etkilenebilmektedir. Bir EKS'ne yönelik siber saldırı, tek bir hedefe yönelik saldırıdan daha büyük etkiler yaratabilmekte ve fiziki bir saldırı ile bir arada da gerçekleştirilebilmektedir. (Bayuk vd., 2012:58) Bu sistemlerin çoğunluğu, geçmişte kendilerine özgü yazılımların kullanıldığı, analog, üretici destekli, doğrudan seri kablo bağlantılı ve/veya kablosuz erişimli ve IP bağlantı özelliği olmayan sistemler olarak üretilmiş olup halen kullanımdadır. Uzak terminal bağlantı birimleri, programlanabilir mantık birimleri (PLC), fiziksel erişim kontrolü, saldırı tespit sistemleri, CCTV, yangın alarm sistemleri ve yardımcı sistemler uzun yaşam döngüsüne sahip sistemler olup tipik olarak operasyonel teknoloji ürünleri olarak üretilmiş cihazlardır. Bu sistemler ve bileşenleri dijital ve IP uyumlu olmaya başladığı için kurumsal ağlara ve geleneksel bilişim sistemlerine bağlanabilmekte; bu da bu sistemleri işletmekte olan kurumları istismara ve önemli güvenlik açıklarına maruz bırakabilmektedir. Son dönemlerde, sistemler birbirleri ile bütünleştiği için bir geleneksel bilişim sisteminin nerede başladığını ve nerede bittiğini, EKS'nin nerede başlayıp nerede bittiğini, net olarak gösteren bir ayıraç bulunmamaktadır. (Perdikaris, 2014:108).

Bilişim sistemlerindeki tehditleri gidermek için geleneksel olarak sisteme güvenliğe yönelik donanım ve yazılım ürünleri eklenebilmektedir ancak EKS için bu teknik olarak olanaksızdır. Özellikle üretim esnasında güvenli çalışması istenen EKS cihazlarının tasarım bilgileri başkaları ile paylaşılmamaktadır. Pek çok süreç kontrol sistemi, ısı ve nem gibi fiziksel ölçütler dikkate alınarak ve normal işletim şartları altında yüksek güvenirlikli olarak tasarlanmışlardır. Kullanım aşamasında ek güvenlik süreçlerini oluşturmak için çoğunun yeterli kapasitesi bulunmamaktadır ve güvenlik amacı ile kurulan ara sisteme düzgün cevap veremeyebilirler. Sisteme eklenen cihazlar, zaman kritik işlerde gecikmeye sebep olabilirler. EKS cihazları ve ağları özel tasarım olabilir ve özgün olmayan güvenlik elementleri, üretici garantisini geçersiz kılabilir. EKS'nin kendisi yeni güvenlik önlemlerini tolere edemeyecek kadar eski olabilir. Tipik bir fabrika ortamı, süreç tamamen devre dışı bırakılmadan ya da tamamen güncellenmeden önce 12, 15 hatta 30 yıl aktif olarak çalışmak üzere tasarlanmış bileşenlerden oluşan gerçek bir müze görünümündedir (Macaulay ve Singer, 2011:101).

EKS'nde dijital teknolojilerin kullanımının artması, bu sistemlerin bulut bağlantılarının ve kurumsal ağ bağlantılarının sürekli olarak artmasına yol açmaktadır. Siber uzayın fiziki alan ile etkileşimini sağlamak üzere sahada kullanılmakta olan çok çeşitli özel cihazlar ve robotlardan oluşan ve IIOT olarak adlandırılan; sayıları ve nitelikleri her geçen gün artmakta olan çok sayıda cihaz da EKS'ne yönelik siber tehditlerde niteliksel ve niceliksel artışlara neden olmaktadır.

Son teknolojik gelişmeler bağlamında EKS ağları ile IP ağlarının izole edilmesi de artık mümkün görünmemektedir.

2.2.2.1 Siber Tehditlerin Hedef Aldığı Kritik Altyapılar

Çiftci, "Siber güvenliğe yönelik saldırılar sonucunda, rafinerilerde ve nükleer tesislerde yangın çıkıp patlama olabilir; elektrikler kesilebilir ve elektrikle çalışan sistemler kullanılamaz hale gelebilir; petrol ve doğalgaz boru hatlarında patlamalar meydana gelebilir; uydu sistemleri ele geçirilip meteoroloji, seyrüsefer, iletişim uyduları ve diğer uydular düşürülebilir veya yörüngesinden çıkarılıp rotalarından saptırılabilir" ifadesi ile siber saldırıların çevre üzerinde oluşturabileceği olumsuz durumlara dikkat çekmektedir (Çifci, 2012:14-15).

EKS'nin çalıştırıldığı rafineriler tehdit ve saldırılara açık iletişim protokolleri kullanarak geniş alan ağlarına bağlandıkları için kritik arıtma süreçleri de risk altındadır. Başarılı saldırılar, ısı ve basınç sınırlarının aşılması, süreç akışının kesintiye uğratılması, zararlı sıvı ve gaz kaçışı, katalizör kirlenmesine neden olabilir. Bu durumlar, yangın, patlama, arıtma işinin yapılamaması, ölüm, yaralanma, çevre kirliliği gibi olaylara neden olabilir (Krutz, 2006:26).

Nükleer santrallerin soğutma ve diğer acil ve normal durumların kontrolü için SCADA sistemleri kullanılmaktadır. SCADA sistemlerin çalışmasında karışıklığa neden oabilecek bir siber tehdit dramatik ve tehlikeli sonuçlar doğurabilir (Krutz, 2006:29-30).

Su arıtma işlemini gerçekleştirmede kullanılan bir EKS, su arıtma sürecini, pompalama sistemini, boru hattı basıncını görüntüler ve kontrol eder. Kimi durumlarda, uzak mesafelerden dolayı merkezi kontrol istasyonu ile uzak lokasyon arasındaki iletişim için radyo modemleri kullanılmaktadır. Su arıtma ve dağıtım sisteminde su arıtma sürecinde, dağıtım işlemini bozmak için yanlış basınç uygulama ve veri pompalama; su deposu

bilgisinin değiştirilmesi gibi saldırı senaryoları bu sisteme yönelik tehdit oluşturabilecek durumdadır (Krutz, 2006:36).

Kritik altyapıların siber güvenliğinin sağlanması kapsamında, bilişim teknolojilerine yönelik tehditlerin yanı sıra bu sistemlere yönelik fiziki tehditler de dikkate alınmalıdır.

Bir tehditin gerçekleşmesi için kritik altyapının faaliyetlerini gerçekleştirme görevini yerine getirmekte olan EKS'nin mevcut güvenlik açıkları kullanılarak potansiyel bir zarara maruz kalması gerekmektedir. Güvenlik politikalarının; güvenlik yöntemlerinin; kabul edilebilir kullanım politikalarının ihlali sonucu, bilgi sisteminin ya da sistem süreçlerinin gerçekleştirilmesinde kullanılan, saklanan, iletilen bilginin gizliliğini, bütünlüğünü, kullanılabilirliğini riske atan bir tehdit olayı gerçekleştiğinde siber güvenlik olayı meydana gelmiş olur (NIST SP 800-82r2, 2015:C.1).

2.2.2.2 Tehdit Aktörleri

Tehdit aktörlerinin teknik yeteneklerinin her geçen gün gelişmekte olduğunu ve şaşırtıcı bir şekilde fiziksel hasara neden olma isteğine sahip olduklarını; siber güvenliğe yönelik olayların fiziksel dünyaya önemli ölçüde zarar verme potansiyeli olduğunu göstermektedir. İyi finanse edilen bir tehdit aktörünün istediği herhangi bir siber sisteme saldırabilme yeteneği, kritik altyapıların sahipleri ve operatörleri için endişe kaynağıdır. Kritik altyapıların siber saldırganların saldırılarından korunması mümkün olmadığı için siber saldırıların tespit edilmesi ve kurtarılması ile ilgili yeteneklerin geliştirilmesi çok önemlidir. Basit tekniklerin yanısıra gelişmiş teknikler de siber saldırıların gerçekleştirilmesinde kullanılabilmektedir.

Ulus devletler de aktif olarak kritik altyapılara saldırıda bulunmak üzere yeteneklerini geliştirmektedirler. Ulus devletlerin yanısıra bireysel olarak saldırganlar da kötü amaçlı, yıkıcı saldırılar yapmaya isteklidir.

Kritik altyapıları ve onları kontrol eden sistemleri hedef alan saldırıların sıklığının hızlı artışına paralel olarak gelişmiş tehdit aktörlerinin beceri seviyeleri de artmaktadır. EKS'lerini hedef alan tehdit aktörleri, ileri seviyede bilgi ve beceriye sahip olduğu için; bu kaynakları korumakla ve savunmakla görevli bilişim profesyonellerinin de en az bu seviyede gelişmiş bilgi ve beceriye sahip olmalısı gerekmektedir.

2.2.2.3 En Bilinen Tehditler

Kritik işlemleri yerine getiren EKS'nin büyük çoğunluğu, görüntüleme, takip ve otomasyon amaçlı çok sayıda bilişim sistemi bileşenlerinden oluşmaktadır. Kritik sistemler, yoğun olarak bilişim sistemlerine bağımlı hale gelmiş; TCP/IP bağlantılarının ve açık kaynak kodlu yazılımların kullanımı ile sistemlerin güvenlik açıkları, hatalar, zayıflıklar daha çok gündeme gelmeye başlamıştır. Bilişim sistemlerine yönelik tehditler, aynı zamanda EKS için de geçerli tehditlerdir. EKS'na yönelik tehditler, bireyler tarafından gerçekleştirilen saldırı, kaza, teknik hata gibi nedenlerden kaynaklanabilir ve önemli çevre sorunlarına neden olacak şekilde sonuçlanabilir.

Kritik altyapılarda faaliyet gösteren EKS'ne yönelik tehditlerden en çok bilinenleri arasında;

- Deprem, sel, fırtına, yangın, kasırga gibi doğal afetler,
- İstemsiz insan hatası sonucu sistemlerin hatalı çalıştırılması ve kazaların meydana gelmesi, Virüsler, Truva Atları, Solucanlar, DDOS Atakları gibi zararlı yazılımlar,
- Teröristler,
- Enerji hatlarındaki kirlilik, elektromanyetik parazit ve radyo frekans parazitleri,
- Cihazların arızalanması,
- Tesisin bakım için kapatılıp açılması (Pek çok zararlı durum tesisin kapatılıp açılması esnasında oluşur) (Krutz, 2006: 82),
- Yazılım yamalarının doğru geçilmemesi,
- Diğer ağlarla ve destek elementleri ile karşılıklı bağımlılık sayılabilir.

2.2.2.4 İletişim Altyapısından Kaynaklanan Tehditler

EKS'nin birbirleri ile bağlantısını sağlayan iletişim sistemlerinden kaynaklanabilecek tehditlerden bazıları ise (Krutz, 2006:82-83);

- İnternet bağlantıları, kurumsal ağ bağlantıları,
- Güvenlik açığı olan diğer ağlara bağlantı, güvenlik açığı olan sanal kişisel ağlar (VPN), arka kapı bağlantıları,
- Güvensiz kablosuz bağlantılar,
- Paket başlık bilgisi içerikte yer alan paket verisi ile çakışan kusurlu IP paketleri, IP fragmentasyon saldırıları,
- SNMP güvenlik açıkları,

- UDP, TCP portları gibi korunmasız ve gereksiz yere açık bırakılmış bilgisayar portları,
- EKS bileşenleri ve protokollerde zayıf kimlik doğrulama sistemlerinin kullanılması,
- EKS'nin geliştirme, test ve bakm aşamalarında güvenlik önlemlerini aşmak üzere kullanılan bakım kancaları, tuzak kapılar,
- EKS ağı üzerinden e-posta iletimi,
- EKS sunucuları üzerinden buffer overflow saldırıları,
- Telefon hatları.

2.2.2.5 Tehditin Gerçekleşmesi Durumu

EKS cihazları, ağları ve hizmetlerindeki teknolojik değişiklikler paralelinde bu sistemlere özgü sorunların ölçeği ve kapsamı da değişmekte ve yukarıda sayılan tehditlere her geçen gün yenileri de eklenmektedir. Son dönemlerde kullanılmakta olan zararlı yazılımlar antivirüs ve IDS gibi eski tür güvenlik denetimlerini atlatabilmektedir. Bu zararlı yazılımların EKS'ni etkileme olasılıkları yüksektir. Eski ve yama işlemi yapılmamış işletim sistemlerinin de yakın zamanda geliştirilmiş zararlı yazılımlardan etkilenme olasılığı yüksektir (Macaulay ve Singer, 2011:140). Eğer bir saldırgan EKS'ne erişmekte başarılı olursa bir sonraki adım sistem bileşenlerinin kontrolünü ele geçirmek olacaktır. Bir saldırgan tarafından EKS'ne yapılacak kötü amaçlı saldırı ile gerçekleştirilebilecek istismar örnekleri (Krutz, 2006: 83);

- EKS'ne erişimi sağlamak,
- EKS ana kontrol sistemine erişimi sağlamak,
- Uzak terminal bağlantısı ya da yerel PLC'leri tehlikeye atmak,
- EKS ana kontrol sistemini tehlikeye atmak,
- EKS'nin sistem şifresini ana kontrol istasyonunu kullanarak ele geçirmek,
- Uzak terminal birimi ya da yerel programlanabilir mantık birimlerine erişimi ele geçirmek,
- Uzak terminal birimini yanıltma ve ana kontrol birimine yanlış veri gönderme,

- Ana kontrol birimini yanıltma ve uzak terminal birimine hatalı veri gönderme,
- Ana kontrol birimini kapatma,
- Yerel uzak terminal birimini kapatma,
- EKS ana kontrol birimi ile uzak kontrol birimi arasındaki iletişimi bozmak,
- Uzak terminal birimi kontrol programını değiştirmek.

EKS'ne yönelik tehditlerde dizüstü ve masaüstü bilgisayarlar gibi kurumsal varlıkların kişisel kullanımı ortak sorundur. Dış kullanıma kapalı olmaları durumunda bile personelin kendi kullanımı için dosya indirmesi ya da geçici süreler için internete bağlanması sonucu zararlı yazılım bulaşabilmektedir. Zararlı yazılım bir kez yüklendikten sonra çok güçlü araçlarla bile kolaylıkla temizlenemez. Bedava yazılım ve müzik indirme sitelerinden zararlı yazılımlar bulaşabilmektedir. Zararlı yazılımların dağıtılmasında en etkili yöntemlerden biri de sosyal mühendislik uygulamalarıdır. Günümüzde sosyal mühendislik, facebook, myspace, instagram, twitter gibi sosyal ağlar ve iletişim uygulamaları kullanılarak gerçekleştirilmektedir.

1.3 KRİTİK ALTYAPILARA YÖNELİK SİBER GÜVENLİK OLAYI ÖRNEKLERİ

Başlangıçta diğer sistemlere bağlı olmadan müstakil bir şekilde çalışmakta olan ve kendilerine özgü iletişim protokollerinin kullanıldığı endüstriyel kontrol sistemleri, 1990'lı yıllardan itibaren standart ağ protokolleri kullanmaya ve bütünleşik ağlara ve böylelikle internete bağlandıkları için siber saldırılara ve siber güvenlik olaylarına maruz kalmaya başlamıştır. Kritik altyapılara yönelik gelecekte olabilecek siber güvenlik olaylarını anlayabilmek ve bunlara yönelik önlemleri alabilmek için günümüze kadar yaşanan siber güvenlik olayı örneklerinin incelenmesi daha da önemli hale gelmiştir.

Siber fiziki sistemler olarak da anılmakta olan EKS günlük hayatın her alanına girdiği için kötü niyetli kişiler ve suçlular, bu sistemlerin güvenlik açıklarını avantaj olarak kullanmaya çalışmaktadırlar. Özellikle endüstriyel ve nükleer tesisler, yaptıkları işin önemine binaen saldırı hedefi olabilmektedir. Bu tür saldırıların hedefi olan kurumsal yapılar, sistemlerinin güvenlik sorunları olduğunu ifşa etmemek, diğer varlıklarının

güvenliği hakkında şüphe uyandırmamak, ya da isimlerinin güvenilirliğini zedelememek gibi çok değişik nedenlerle saldırıya uğradıklarını saklı tutmaktadır (Farooq-i-Azam ve Ayyaz, 2012:180). Kritik altyapı tesislerine ve kritik sektörlere yönelik siber olaylar, bu sistemlerin güvenlikleri ulus devletler tarafından bir ulusal güvenlik sorunu olduğu için gerçek anlamı ile bildirilmemekle birlikte kısıtlı da olsa bir kısmına ait bilgilere açık kaynaklardan erişilebilmektedir.

1980'li yıllardan itibaren bilgi ve iletişim teknolojilerindeki gelişmeler küreselleşmeyi tetiklemiş; neoliberal politikaların uygulanması ile ulus devletlerin yanı sıra Birleşmiş Milletler, Dünya Ticaret Örgütü, OECD gibi uluslararası kuruluşların ve Microsoft, IBM, Siemens gibi çok uluslu şirketlerin de etkinlikleri gözle görülür seviyede artmıştır. Birinci bölümde anlatıldığı gibi, dünya üzerinde fiziki alana paralel olarak siber uzay hayatımıza girmiştir. Siber uzay bilgi ve iletişim teknolojileri ürünleri olan yazılım, donanım ürünleri ve bu ürünleri birbirine bağlayan iletişim ağlarından, bu sistemleri tasarlayan, üreten ve kullananlardan oluşmaktadır. Siber uzayda ulus devletlerin fiziki sınırlarının hiçbir önemi kalmamış durumdadır. Bir devletin sınırları içinde yer alan ve zarar görmesi ya da yok olması durumunda o devletin güvenliğini, ekonomisini, halk sağlığını ya da çevre güvenliğini olumsuz yönde etkileyecek fiziki ya da sanal sistemler ve varlıklar olan kritik altyapılarda meydana gelebilecek bir siber güvenlik olayı tüm dünyayı olumsuz yönde etkileyebilecek durumdadır.

Ulusal güvenliği tehdit, ağır hasar oluşturmak, ekonomiyi zayıflatmak, devlete olan güveni zedelemek, günlük faaliyetlerde aksaklıklar oluşturmak gibi nedenlerle kritik altyapılara saldırılar düzenlenebilmektedir (Bennet, 2018:44-45). Yerine getirdiği görevlerin otomasyonu için EKS'nin kullanıldığı bir kritik altyapıya yönelik siber saldırı ulusal güvenlik, ekonomi, günlük hayat ve vatandaşların emniyeti açısından önemli etkiler doğurabilecek seviyededir. Her gecen gün bilgisayara ve internete daha da bağımlı hale geldiği için kritik altyapıların iletişim sistemlerine ve ağlarına yönelik siber saldırılar giderek artmakta ve karmaşıklaşmaktadır. Çeşitli örnekler, kritik altyapılara yönelik siber saldırıların etkilerinin uluslararası güvenlik için de önemli olduğunu göstermektedir (Clark ve Hakim, 2017:1).

Bu çalışma kapsamında, EKS yardımı ile faaliyetlerini yerine getirmekte olan kritik altyapılara yönelik siber güvenlik olaylarının önemli çevre sorunlarına yol açarak sürdürülebilirliği engelleyip engelemeyeceği araştırıldığı için 1982 yılından bu yana gerçekleşmiş bazı siber güvenlik olayları incelenecektir. Öncelikle açık kaynaklardan edinilen bilgiler ışığında siber güvenlik olayları örneklerine yer verilecek, daha sonra da bu siber güvenlik olaylarından çıkarılan dersler gündeme getirilecek ve bu olayların çevre etiği açısından değerlendirilmesi yapılacaktır.

2.3.1 Kritik Altyapılara Yönelik Gerçekleşen Bazı Siber Güvenlik Olayları

Kiminin etkisi hâlâ saptanamamış, kimisi de ifşa edilmemiş olmakla birlikte, mikroişleyicileri barındıran EKS'ne yönelik gerçekleşmiş ve açık kaynaklardan edinilmiş bilgiler ışığı altında siber saldırı örneklerinden bazıları aşağıdadır:

1982-Sibirya Boru Hattı Saldırısı

Sibirya Boru Hattını yöneten SCADA sisteme, verileri ve bilgileri değiştiren bir Truva Atı saldırısı yapılmıştır. Boru hattını yöneten SCADA Sisteme Truva Atı yöntemi ile gerçekleştirilmiştir (Miller ve Rowe,2012:51-56). SCADA Sistemler, belli durumlarda ortamdan sensörler aracılığı ile aldıkları verilere göre işlem yaptıkları için değiştirilmiş verilerle yapılacak işlem, sadece verilerin değiştirildiği basit bir işlevsel sonuç doğurmakla kalmayacak; boru hattında petrolün dışarıya akması yolu ile patlamalara, yangınlara, gaz kaçaklarına neden olabilecek çevre kirliliği, enerjinin boşa harcanması gibi çevre sorunlarını gündeme gelirebilecek nitelikte fiziksel ya da fiziksel ve siber sonuç oluşturabilecek bir saldırıdır.

1992-Chevron Alarm Sistemine Saldırı

Yangına karşı kurulan Chevron Alarm Sistemi, uzaktan bilgisayarların ele geçirilmesi ile devre dışı bırakılmıştır. BT kaynaklarına yetkisiz erişim, sunucu üzerindeki dosyalara daha fazla yetkisiz erişimi sağlayabilmek amacı ile sitenin sıçrama tahtası olarak kullanılması, failin ana sistem üzerinde yer alan kullanıcı önceliklerini ele geçirerek yetkisiz erişim imkanı elde etmesi yolu ile gerçekleştirilmiştir (Miller ve Rowe,2012:51-56).

Saldırı aracı olarak sadece siber sistem kullanılmıştır. Alarm sisteminin düzgün çalışmasını önlemeye yönelik yetkisiz erişimler sonrası yangının söndürülememesi, can ve

mal kaybına dolayısı ile önemli çevre sorunlarına yol açabilecek nitelikte fiziksel ve işlevsel sonuçları olabilecek bir saldırıdır.

1994-Salt River Projesine Saldırı

Bir saldırgan, ABD Phoneix bölgesindeki kullanıcılara su dağıtımı yapan Salt River Projesinin bilgisayar ağına çevirmeli ağ özelliğine sahip modem kullanarak erişmiş; kendisine daha sonra erişim olanağı sağlayacak bir arka kapı oluşturmuştur (Miller ve Rowe,2012:51-56). Olayın faili ana sistemde yetkisiz yönetici haklarına sahip olmuş, kullanıcı adı ve şifrelerin bulunduğu dosyayı, sistemin günlük erişim kayıtlarını ele geçirmiş, Truva atı saldırısı yapmış, yetkisiz erişim gerçekleştirmiştir (Krutz,2006:75 ve Turk, 2005:45).

Su dağıtım sistemine yönelik bir siber saldırı ile tesisin hatalı çalışması ya da devre dışı bırakılması sel baskınları ya da sulanması gereken bölgeye su verilmemesi sonucu kuraklığa neden olabilecek fiziksel ve işlevsel sorunlar oluşturma olasılığı olan bir saldırıdır.

1999-Gazprom'a Saldırı

Rusya'da bulunan Gazprom doğal gaz şirketinin bilgisayar sistemlerine, öfkeli çalışanlar tarafından içeriden saldırı gerçekleştirilmiştir (Miller ve Rowe,2012:51-56). Siber saldırganlar, boru hatlarından gaz akışını kontrol eden merkezi santralin yönetimini Truva Atı yöntemini kullanarak ele geçirmişlerdir. Kurum çalışanları tarafından içeriden gerçekleştirilen bu saldırı siber fiziksel sistemler kullanılarak gerçekleştirilmiştir. İlk bakışta sadece işlevsel sonuçları olabilecek bir saldırı gibi gözükse de boru hattının gaz akışı kontrolünün devre dışı bırakılması ya da hatalı çalıştırılması, gaz sızıntısı veya gaz kesintisine neden olabilecek işlevsel bir sonuç oluşturacak gibi durmaktadır ancak gaz sızıntısının patlamalar yolu ile fiziki hasar yaratacağı ya da gaz kesintisinin gerçekleşmesi gereken hayati önemde faaliyetlerin durmasına neden olacağı göz önünde bulundurulduğunda fiziksel ve işvevsel sonuç doğurma olasılığı olan bir saldırıdır.

1999-Bellingham Boru Hattında Arıza

Bellingham, Washington'da, Gaz Boru Hattı'ndan çok fazla miktarda benzin sızıntısı olmuştur. 1.5 saat süren gaz sızıntısı ve yangın sonucu 3 ölüm 8 yaralanma meydana gelmiştir(Miller ve Rowe,2012:51-56). Olaya kontrol ve görüntüleme sistemlerinin görevini

yerine getirmemesi neden olmuştur. Teknik bir saldırı değil, kaza sonucu meydana gelmiş bir olaydır. Görüntüleme ve kontrol sisteminin normal çalışmasını önleyen siber fiziksel bir olay gerçekleşmiş ve sonucunda işlevsel hasar oluşarak görüntüleme ve takip sistemleri devre dışı kalmıştır. Ancak bu sistemlerin görevlerini yerine getirememesi, işlevsel hasarın devamında fiziksel ve işlevsel hasara neden olmuş ve gerekli önlemlerin alınamamasından dolayı can kaybı ve yaralanmalar ile sonuçlanmıştır.

2000-Maroochy Kanalizasyon Sistemi Saldırısı

Avustralya'da Maroochy SCADA sistemi 142 kanalizasyon pompalama istasyonunun işlemlerini kontrol etmek üzere 2 görüntüleme merkezi ve 3 radyo frekans merkezinden oluşmakta idi. Su Hizmetleri Birimine bağlı kanalizasyon kontrol sisteminin radyo frekansları ile sağlanan iletişimin kesildiği, pompaların düzgün çalışmadığı, sorun olduğunu belirten alarm sisteminin görevini yerine getirmediği anlaşılmıştır. Başlangıçta, sorunun kurulan sistemin kendisinden kaynaklandığı düşünülmüş ancak bir süre sonra, sistem üzerinden geçen tüm sinyalleri izleyen bir mühendis, sistemin hacklendiğini ve kasıtlı olarak problem yarattığını fark etmiştir. Daha sonra yapılan incelemede açıklanamayan pompa istasyonu alarmları, iletişim hatalarına neden olan radyo frekanslarındaki artış, pompa istasyonu yazılımının konfigürasyon setlerinde değişiklikler, pompaların beklenmeyen biçimde sürekli çalışması, pompa istasyonlarının kilitlenmesi ve hiç alarm vermeden kapanması, bilgisayar iletişiminin kilitlenmesi ve alarm izlemenin kesilmesi olaylarının gerçekleştiği görülmüştür. Başlangıçta sorunun sistem kurulum hatalarından kaynaklandığı düşünülmüş, tüm yazılımların yeniden kurulması ve sistemin kontrolü sonucunda pompa istasyonu ayarlarının kontrol dışı olarak değiştiği görülmüştür. Bu aşamada sistemin dışarıdan gerçekleştirilen bir saldırı olabileceği düşünülmeye başlanmış; gelişmiş görüntüleme araçları yardımı ile bir hackerin SCADA sisteme kablosuz erişim cihazları ile eriştiği belirlenmiştir (Slay ve Miller, 2008:79). Bir solucan bulaşmış dizüstü bilgisayar dağıtık kontrol sistemini durdurmuş, akabinde bir IP adresi değişikliği kimyasal tesisin çalışmasını durdurmuştur. (Susanto vd.,2014:89) Soruna neden olan işlemin bu kuruma iş başvurusu kabul edilmeyen küskün bir kişi tarafından gerçekleştirildiği anlaşılmıştır. Saldırganın 150 kanalizasyon pompa istasyonunun kontrolünü bir dizüstü bilgisayar ve radyo vericisi kullanarak ele geçirdiği ve gerçekleştirilen bir dizi siber saldırı

sonucu, 4 aylık süre içerisinde 1 milyon galon lağım suyu, içme sularına karışmıştır (Slay ve Miller, 2008:74-75).

Öfkeli eski çalışanın gerçekleştirdiği siber saldırı sonucu kanalizasyon sularının akarsulara, parklara ve yakınlardaki bir otelin zeminine yayılmış; çevreye zarar verilmiş ve toplumsal maliyeti yüksek olmuştur. Buradaki problemlerin büyük çoğunluğu ekipman hatasından değil insan müdahalesinden kaynaklanmıştır. Saldırı ile ilgili sorunlar, saldırıdan sorumlu kişinin yakalanması ile son bulmuştur (Panguluri vd., 2017:153).

İnsan eli ile gerçekleştirilen bir siber fiziksel saldırı sonrası fiziksel ve işlevsel saldırı sonrası işlevsel hasarı fiziksel hasar takip etmiş ve önemli miktarda kanalizasyon suyu içme sularına karışmış; çok önemli bir çevre felaketi yaşanmıştır.

2001-Kaliforniya Elektrik Şebekesine Saldırı

Saldırganlar, Kaliforniya ana elektrik dağıtım şebekesinin bilgisayar sistemlerini ele geçirmiş ve 17 gün sonra fark edilebilmiştir (Miller ve Rowe,2012:51-56). Yetkisiz erişim yöntemi ile düzenlenen siber saldırı sonucu elektrik şebekesince oluşturulabilecek bir arıza ile işlevsel hasar olarak elektrik dağıtımının engellenmesi riski oluşmuştur.

2001-Houston Limanına Saldırı

Houston limanının web tabanlı sistemine, dağıtılmış hizmet reddi (DDOS) saldırısı yapılmıştır. Saldırının yapıldığı bilgisayarın sahibi, bilgisayarının sıçrama sitesi olarak kullanıldığını ve kendisinin bu olaydan haberdar olmadığını söyleyerek savunma yapmıştır (Krutz, 2006:75). Houston Limanının, gemi hareketini, kenetlenmeyi, demir atmayı, yükleme boşaltma işlemlerini gerçekleştiren kontrol sistemleri durdurulmuştur. Bu sistemler hedef olmadıkları halde, organize suç örgütleri tarafından geleneksel bilgisayar ağlarına yönelik botnet saldırısı sonucu istenmeden devre dışı bırakılmıştır (Susanto vd., 2014:88). Sadece siber saldırı ile fiziksel ve işlevsel hasar meydana gelmiştir.

Kullanılmakta olan siber saldırı araçları ile geleneksel bilgisayar ağına yönelik bir siber saldırı bağlı bulunduğu EKS'nin de görevini yerine getirmesini engelleyebilmektedir.

2003-Ohaio Davis-Besse Nükleer Santraline Saldırı

Ohio'da Davis-Besse nükleer santralinde Slammer solucanından kaynaklanan tıkanıklık sonucu önce ağda bir yavaşlama yaşanmış; daha sonra emniyet sistemleri etkilenmiş; tesisin Güvenlik Parametreleri Görüntüleme Sistemi ve Süreç Kontrol Bilgisayarları en az 5 saat devre dışı kalmıştır (Krutz,2006:75;Miller ve Rowe,2012:51-56). Konunun uzmanları, soğutma sistemleri, çekirdek ısı sensörleri ve harici radyasyon sensörleri gibi en önemli güvenlik göstergeleri olan bu sistemlerin çoğunluğunun tesis kapalı durumda iken bile izlenmesi gereken sistemler olduğunu belirtmiştir (Poulsen,2003). Microsoft SQL sunucuları ve Microsoft Data Engine (MSDE) 2000 ile çalışan bilgisayarlara yönelik yazılan Slammer Solucanı, ağın yükünü artırarak "buffer overflow" hatasına yol açarak SQL sunucularını erişilmez hale getirmiştir. Solucanın Nükleer Santrala First Energy Nuclear isimli bir yüklenicinin ağından ulaştığı; Nükleer Santralin güvenlik duvarının aslında Slammer solucanının kullandığı portu bloke etme özelliği bulunduğu ancak nükleer santralin iş ağı üzerinde bulunan farklı geçişlerin bunu geçersiz kıldığı anlaşılmıştır. Microsoft'un Slammer solucanının nükleer tesiste etkili hale gelmesinden altı ay kadar önce bu solucana yönelik yamayı yayınladığı ancak tesisin bilgisayar mühendislerinin bu yamayı sisteme yüklemeyi ihmal ettiği düşünülmektedir (Bıçakçı, 2016:110-111).

Nükleer santrale dışarıdan gerçekleştirilen siber saldırı, sadece işlevsel hasara neden olmuştur. Ancak santralin güvenlik göstergelerinin devre dışı bırakılması, santralin çalışmasında meydana gelebilecek sorunların zamanında anlaşılamamasına ve gerekli önleyici tedbirlerin alınamamasına neden olabilecek ve önemli çevre sorunlarını gündeme getirebilecek niteliktedir.

2003-ABD Elektrik Santrali Arızası

Bu elektrik kesintisi ABD ve Kanada'da tahminen 50 milyon kişiyi etkilemiştir. Abonelerin büyük çoğunluğuna elektrik birkaç saat içinde geri gelirken, Amerika Birleşik Devletleri'ndeki bazı bölgelerde iki gün süren bir elektrik kesintisi yaşanmış; Ontario'nun bazı kısımlarında ise iki haftayı bulan elektrik kesintileri yaşanmıştır (Krutz, 2006:75);

Kuzey Amerika elektrik şebekesi kesintisi olayının başlangıcında, bir işlemcinin durması nedeni ile kontrol odası operatörleri, EKS içindeki önemli bir unsurla ilgili bir sorunun sesli ve görsel göstergelerini sağlayan alarm işlevini kaybetmiştir. Yazılım mantığı

gereği alarm verilemeyince bir sonraki komuta geçilmiş ve alarm işlemcinin tampon alanı dolmuş ve normal sınırların dışına çıkmıştır. Belli bir süre zarfı içinde kontrol bilgisayar ekranları daha fazla alarm alamamış ve herhangi bir alarm oluşturulamamıştır. Bir alarmın oluşturulamaması, sistemin durumunun yanlış anlaşılmasına katkıda bulunmuş ve durum daha da kötüleşmiştir. Sistem daha sonra başka hatalara nrden olmuştur. Raporlara göre, "bilgisayarın ve beklenen tüm işlemlerin çalıştığını doğruladı. Buna göre, bilgisayar destek personeli, düğümü ve barındırdığı tüm süreçleri başarıyla yeniden başlattıklarına inanıyordu. Ancak sunucu ve uygulamaları tekrar çalışır durumda olmasına rağmen alarm sistemi donmuş ve işlevsiz kalmıştır (Bridges,2013:84)..

Fiziksel bir siber olay olarak elektrik santralinin kazara arızalanması sadece işlevsel hasara sebep olarak elektriklerin kesilmesine neden olmuştur. Kritik altyapıların çalışabilmeleri için kullanmakta oldukları elektriklerin devre dışı kalması zincirleme olarak diğer kritik altyapıların çalışmamasına ya da yanlış çalışmasına neden olabilecek, bu da fiziksel ve işlevsel hasara yol açarak çevre güvenliği açısndan sorunlar yaratabilecektir.

2004-ABD Hatch Nükleer Enerji Santralinde Hatalı İşlem

ABD'nde Hatch nükleer enerji santralinin, yazılım güncellenmesinin ardından 48 saatliğine acil bir biçimde zorunlu olarak kapatılması gerekmiştir. Nükleer tesisin 2 numaralı ünitesi, tesisin idari ağında kullanılan bir yazılımın güncellenmesi öncesinde düzgün bir şekilde çalışırken güncelleme sonrasında idari bilgisayarın yeniden başlatılması ile birlikte süreç kontrol ağından sistem kontrol bilgisi toplanmaya başlanmıştır. Bu olay, kontrol sisteminin eşleme programının kurulmasını ve sistemin, reaktörün rezervuarındaki su miktarında ani azalma olarak algılanmış ve otomatik kapatma sistemi başlatılmıştır. İlgili firma sözcüsü, devreye giren acil durum sistemlerinin, nükleer enerji santralinin emniyetinin sağlanması için tasarlandığını; güncellemeyi yapan mühendisin bu özelliği bilmediği için sistemi yeniden başlattığını, bu durumda sistemin kendisini tekrar kurduğunu ve diğer ağları da buna zorladığını söyleyerek konuya açıklık getirmiştir (Bıçakçı, 2016:112-113).

Nükleer Enerji Santralinde yanlışlıkla yapılan bir siber fiziksel işlem, oluşan işlevsel hasar aşamasında santralin hatalı çalışmasına neden olmuştur. Bir fiziksel sorun oluşmadan normale döndürülen bu nükleer santralde, işlevsel olarak hatalı çalışma önemli çevre

sorunlarına neden olabilecek fiziksel ve işlevsel bozukluk olarak devam edebilecek niteliktedir.

2006-ABD Brown Ferry Nükleer Enerji Santralinin Devre Dışı Kalması

Alabama yakınlarında bulunan dünyanın en büyük nükleer enerji santrallerinden Brown Ferry Nükleer Enerji Santrali'nin ağında yaşanan yüksek veri trafiği nedeni ile su devirdaim pompasının faaliyeti durmuş; santralin iki reaktöründen biri manuel olarak kapatılmak zorunda kalınmıştır. Reaktöre pompalanan suyun akışını kontrol eden ve kaynar sulu reaktörlerin enerji çıktısını yöneten devirdaim pompaları kritik öneme sahip cihazlardır. Sorunun, kontrolörün tesisin devirdaim pompasında yanlış ağ kodları kullanmasından şüphelenildiği, aşırı trafik yaratarak sistemin çökmesine neden olan kodun bilinen bir yazılım hatası olduğu iddia edilmektedir. Öte yandan ağdaki aşırı yüklenmenin sebebi açıklanamadığı sürece bunun dışarıdan kaynaklanan bir hizmet dışı bırakma saldırısı olup olmayacağının anlaşılamayacağı, logların ve ilgili verilerin bağımsız denetçilerce incelenmesi gerektiği de gündeme getirilmektedir (Bıçakçı, 2016: 111-112).

Nükleer santraldeki bir yazılım hatası ya da santral dışından gerçekleştirilen bir hizmet dışı bırakma saldırısı siber fiziksel bir saldırı olup sadece işlevsel hasar ile sonuçlanmıştır ancak bu sistemin işlevsel olarak hatalı çalışması, patlama, yangın, nükleer sızıntı gibi çevre felaketleri işlevsel ve fiziksel hasara da neden olabilecek niteliktedir.

2007-TCAA EKS'ne Yetkisiz Erişim

Tehama Colusa Canal Authority (TCCA) firmasında 17 yıldır çalışmakta olan eski bir yönetici, görevden uzaklaştırıldığı gün firmanın endüstriyel kontrol sistemi üzerinde yetkisi olmadan bir yazılım yüklediğini itiraf etmiştir (Miller ve Rowe,2012:51-56). İntikam alma nedeni ile yine bir insan tarafından yetkisiz erişim mekanizmaları kullanılarak siber fiziksel saldırı olarak nitelendirilebilecek bu siber olay da sonuçta o sisteme, dolayısı ile fiziki çevreye önemli ölçüde zarar verebilecek faaliyetlerin gerçekleştirilebileceği görülmektedir.

2008- Bakü- Tiflis-Ceyhan (BTC) Petrol Boru Hattında Patlama

Patlamaya bir siber saldırının neden olduğu iddia edilmektedir (Robertson ve Riley,2014). Dünyanın en güvenli hatlarından biri olarak her mili sensörlerle

görüntülenecek, basınç, petrol akışı ve diğer önemli göstergeleri kablosuz erişim sistemi ve uzak mesafeler için uydu sistemi kullanılarak, merkezi kontrol sistemine aktarılabilecek şekilde inşa edilen petrol boru hattına yapılan saldırıdan, elektronik kontrol sistemleri tarafından üretilen uyarılar yerine alevleri gören güvenlik görevlisi sayesinde haberdar olunduğu belirtilmektedir. Konu ile ilgili uzmanlar, hackerların kameraların iletişim yazılımındaki bir güvenlik açığını kullanarak iç ağa sızdıkları, iç ağda alarm yönetim sisteminin Windows işletim sistemi üzerinde çalıştığını gördükleri ve sistem üzerine bir arka kapı yazılımı yükledikleri ve bu yazılımı kullanarak her istediklerinde gizlice bu sisteme giriş yaptıkları tahmininde bulunmaktadır. Saldırıyı gerçekleştirmek için, alarmları devre dışı bıraktıkları, ana kontrol sistemine ulaşmaksızın vana istasyonlarındaki küçük sanayi tipi bilgisayarlara erişerek borular içinde yer alan petrolün basıncının artırılmış olabileceği söylenmektedir. Bir başka iddia ise yeterli veri olmadan bu patlamanın siber araçlardan kaynaklandığının net bir şekilde ifade edilemeyeceği, fiziki bir saldırı olarak değerlendirilebileceği yönündedir (Hemsley ve Fisher, 2018:5).

Bu olayda da siber fiziksel saldırı aracı kullanılmış ve sonuçta çok önemli çevre sorunlarına yol açan fiziksel ve işlevsel hasar meydana gelmiştir.

2009-2010-İran Nükleer Tesislerine Stuxnet Solucanı ile Saldırı

2010 Haziran ayında meydana gelen ve etkileri açısından en önemli siber saldırı olarak görülen bu siber güvenlik olayında İran'ın nükleer tesislerine Stuxnet solucanı sızıp nükleer çalışmaları sekteye uğratmıştır. Bu solucanın, özellikle Siemens üretim kumanda sistemlerini kullandığı ve İran'ın Buşehr veya Natanz nükleer tesislerinde etkili olduğu belirtilmektedir. Stuxnet solucanı işletim sisteminin güvenlik açıklarını topluca kullanma ve bilgisayarlar arasında dolaşma yeteneğine sahiptir. Kendini gizlemek için kullandığı işletim sistemi çekirdek sürücülerini yüklemek için güvenilir firmaların kök sertifikalarını kullanmıştır. İran'ın internete bağlı olmayan nükleer santral sistemine USB bellek kullanılarak bulaştırıldığı düşünülen Stuxnet solucanı, bulaştığı sistemlerin konfigürasyon bilgilerini kaydetmiştir. Bu solucanı yazanlar, pek çok endüstriyel sistemin kritik verilerine de sahip olmuştur (Çifci, 2013s: 173-176). Bu saldırı ile santrifüjların dönen motorlarının 1064 Hz olan hızının 15 dakikalığına çok çabuk bir biçimde 1410 Hz'e çıkarılması ile başlamış, takip eden 27 gün boyunca sessiz kalmış, daha sonra 50 dakikalığına hız 2 Hz'e

düşürülmüştür (Chien, 2012). Solucanın Çernobil benzeri bir nükleer faciaya neden olabileceği iddia edilmektedir. Stuxnet solucanı, özel endüstriyel süreçleri kontrol ve takip amaçlı kullanılan SCADA sistemleri hedef alan bir kötücül yazılımdır (NIST SP 800-82r2, 2015:C-12). Bu yazılım, sadece bilgisayarların kendilerinde değil endüstriyel kontrol sistemlerinde ve dış dünyaya kapalı sistemlerde de etkili olması nedeni ile çok önemlidir. Stuxnet'ten öğrenilen önemli bir ders, iyi finanse edilen bir karmaşık tehdit oyuncusu muhtemelen istediği herhangi bir sisteme saldırabilir. Pekçok teknik özellik barındıran siber sistemlerin tamamının farklı nitliklere sahip saldırganlardan korumak mümkün olmadığı için bir siber saldırı tespit ve kurtarma uygulaması kullanmak faydalı olacaktır (Hemsley ve Fisher, 2018:6).

2011- Night Dragon Saldırısı

McAfee, 5 küresel enerji ve petrol şirketinin, sosyal mühendislik, Truva atı ve Windows tabanlı güvenlik açıklarının birlikte kullanıldığı "Night Dragon" kod adı ile bilinen saldırıya iki yıl boyunca maruz kaldığını; saldırının Çin menşeli olduğu rapor etmiştir. SCADA sistemlerin kendileri doğrudan olmasa da SCADA altyapılarının işletildiği ortak ağlar saldırıya maruz kalmış; operasyonel planlar gibi bazı veriler bu sistem üzerinden alınmıştır (Nicholson, 2012:432).

ICS-CERT, Night Dragon'da uyarmak için Şubat 2011'de bir uyarı yayınlamıştır. Night Dragon saldırıları becerikli ve ısrarcı bir düşman tarafından uygulanan basit tekniklerin enerji sektörü şirketlerine girmek için yeterli olduğunu göstermesi açısından önemlidir. Siber saldırı amaçlı kullanılan uzak masaüstü benzeri yetenekler aracılığıyla güvenliği ihlal edilmiş sistemlerin tam kontrolününün ele geçirilebileceği görülmüştür (Hemsley ve Fisher,2018:7). Bu araçlar kullanılarak EKS'nin kullanıcı arayüzünün kontrolünün de ele geçirilebileceği ve saldırganların kritik sistemlerin uzaktan kontrolünü sağlayabileceklerini göstermesi açısından önemlidir.

2012-Suudi Ulusal Petrol Şirketi Aramco ve Katar Şirketi RasGas'a saldırı

2011'in sonları ve 2012'nin başlarında ABD ve İsraile atfedilen tersine mühendislik uygulanarak silme işlemi gerçekleştiren Shamoon olarak adlandırılan kötücül yazılım tespit edilmiştir. ABD hükümeti ve buna bağlı olarak Küresel Siber Güvenlik

Topluluğu bir dikkat çekme faaliyeti olarak tanımlamıştır anack çok daha güçlü etkiye sahip bir kötücül yazılımdır (Shires,2019:21). Shamoon, yıkıcı bir modül de içeren, bilgi çalan, verilerin olduğu bölümlerin üzerine yazarak ve sistemlere virüs bulaştırarak kullanılamaz hale getiren kötücül bir yazılımdır.

Symantec firmasının ve ABD DHS ICS-CERT kuruluşunun, kötü amaçlı yazılımı açıklamaları ve bu yazılım hakkında bir rapor yayınlamalarını müteakip Shamoon kötü amaçlı yazılımı ikinci hedefini, dünyanın en büyük sıvılaştırılmış doğal gaz şirketlerinden biri olan Katar doğal gaz şirketi RasGas'ı vurmuştur. Shamoon'un ne Saudi Aramco ne de RasGas'ta EKS üzerinde doğrudan bir etkisi olduğuna dair hiçbir kanıt bulunmamaktadır ancak Saudi Aramco ve RasGas, kötü niyetli tehdit aktörlerinin yıkıcı saldırılar gerçekleştirebileceklerini tecrübe etmiştir (Hemsley ve Fisher,2018:11).

2012-ABD Nükleer Santrala Virüs Bulaşması

ABD'ne bir teknisyenin, adı ve konumu saklı tutulan bir nükleer enerji santralinin ekipmanının planlı bakımı için, santralın çalışmasının durdurulduğu sırada sorunlu bir USB'yi sisteme bağlaması nedeni ile santral üç hafta boyunca kapalı kalmıştır. Yüklenici firmada çalışan teknisyenin bilmeden Mariposa virüsünün değişik bir türü olan kötücül yazılımı bu sisteme bulaştırdığı, bu kötücül yazılımın, bulaştırıldığı bilgisayardan veri sızıntısı yapabildiği, dağıtık hizmet dışı bırakma saldırılarının düzenlenmesinde de kullanılabildiği bilgisine yer verilmektedir (Bıçakçı, 2016:113).

2012- Diablo Canyon Nükleer Enerji Santralinin Bilgisayar Ağına Yetkisiz Erişim

Sistemlerin güvenlik önlemlerinin nasıl devre dışı bırakılabileceğini anlayabilmek amacı ile bir grup hacker, Kuzey Amerika'daki çeşitli doğal gaz üreticilerinin sistemlerine saldırılar düzenlemiştir. Bir nükleer tesisin yönetiminde bulunanların e-posta adreslerine bir casus yazılım gönderilmiş ve bu yöntemle Diablo Canyon nükleer enerji santralinin bilgisayar ağına zorla girme teşebbüsü başarı ile sonlanmıştır (Bıçakçı, 2016:113).

2012-Amerika Nükleer Tesis Yöneticisinin Bilgisayarına Yetkisiz Erişim

Ağustos 2012'de Çinli askeri hackerlar, ABD nükleer tesisinin kıdemli yöneticisinin bilgisayarının kontrolünü ele geçirmiş nükleer tesisin bilişim sistemlerine

sızmıştır. Olay inceleme ekibi burada amacın bir Amerikan nükleer reaktörünün güvenlik ve işletim zafiyetlerini tanımlamak olduğu tahmininde bulunmuştur (Bıçakçı, 2016:113).

2012-ABD Enerji Santrali Güvenlik Testlerinde Başarılı Yetkisiz Erişim Denemesi

Güvenlik uzmanı Paul Blomgren ve ekibi tarafından 4 milyon abonesi olan büyük bir enerji santralinin güvenlik testleri yapılırken tesisin dışında park etmiş bir araç içinden bir dizüstü bilgisayar kullanılarak kablosuz ağ ile enerji santralinin operasyonel kontrol ağına ve bilgisayar sistemine müdahale edilebilmiştir.

2013-New York Barajına İran Saldırısı

ABD Adalet Bakanlığı'na göre, New York yakınlarında küçük bir baraja İranlı bilgisayar korsanları tarafından erişilmiştir. Bowman Barajı adı ile bilinen bu küçük barajın tesisleri, fırtına dalgalarını kontrol etmek için kullanılmakta olan ve bir hücresel modem aracılığıyla internete bağlanmış şekilde faaliyetlerini yerine getirmekte olan SCADA sistemi bakımda iken saldırıya uğramıştır. Bakımda iken güvenlik kontrollerinin tam olarak yapılamadığı ve İnternet bağlantısı savunmasız olduğu için bu saldırının gerçekleştirilebildiği söylenmektedir. Bu saldırının teknik ayrıntıları ABD ulusal güvenlik sorunu olarak kabul edildiği için açıklanmamış ancak saldırganların İran devlet destekli bir bilgisayar güvenliği şirketi olduğu belirtilmiştir (Hemsley ve Fisher,2018:13).

Bu siber saldırı, EKS'nin doğrudan İnternet'e bağlı olduğunda saldırganların hedefi haline gelebileceğini, ulus devlet destekli saldırganların coğrafi olarak çok uzak dünyanın herhangi bir yerinden saldırı yapabilecek teknik bilgiye sahip olabileceğini gösteren bir örnektir.

2013-İsrail Su Kaynaklarına Siber Saldırı

İran basını Suriye Silahlı Kuvvetlerinin İsrailin Haifa kentinde bulunan su kaynaklarına bir siber saldırı düzenlediğini duyurmuştur. Başbakan Benjamin Netanyahunun siber güvenlik danışmanı bu haberi yalanlamış fakat kritik altyapılara yönelik siber saldırıların İsrail için gerçek ve var olan bir tehdit olduğunu da belirtmiştir (Geers,2015:80).

2014: Alman Çelik Fabrikası EKS'ne Kurumsal Ağ Üzerinden Saldırı

2014 Aralık ayında, bir Alman Çelik fabrikasının EKS'ne kurumsal ağ üzerinden kimlik avı ve sosyal mühendislik yöntemlerinin kullanıldığı bir saldırı yapılmıştır (Demiröz,2018,s:350). Fabrikanın kontrol sistemleri devre dışı kalmış ve fiziki tahribat oluşmuştur. Sadece ileri bilişim teknolojileri konusunda değil, EKS ve çelik üretim süreci hakkında da ileri seviyede bilgi sahibi oldukları anlaşılan saldırganlar, çelik fabrikasının geleneksel bilişim ağına girmişler, buradan üretim ağına sızmışlar ve çoklu kontrol sistemi arızalarına yol açarak tesisde büyük fiziki hasara neden olmuşlardır (Hemsley ve Fisher, 2018:17).

EKS'ne yönelik siber saldırı ile önemli hasarlar ve çevre sorunları meydana getirilmiştr.

2015-Ukrayna Enerji Şebekesine Saldırı

2015 Noel arifesinde Ukrayna enerji şirketi, bir hizmet dışı kalma olayını rapor etmiştir. Yapılan bir soruşturma, bir BlackEnergy zararlı yazılımının, şirketin çalışan sistemlerinde enerji kesintisine yol açan bir parazit oluşturduğunu açığa çıkarmıştır. ESET firmasının yetkilileri, BlackEnergy zararlı yazılımının zararlı makrolar içeren MS Ofis dökümanlarını kullandığını belirtmişlerdir (Bisson,2016). CIA, NSA ve DHS uzmanları, 600.000 evin elektriğinin kesilmesine neden olan siber güvenlik olayının siber saldırganlar tarafından gerçekleştirilip gerçekleştirilmediği ve saldırı kaynağın Rusya olup olmadığı araştırılmıştır. Konu ile ilgili araştırmalar yapan küresel güvenlik şirketi, bölgenin üçüncü enerji firmasını etkileyen ve yıkıcı sonuçlar yaratan zararlı yazılım kanıtlarına ulaşıldığını ve NATO, Ukrayna, Polonya ve Avrupa sanayisini hedefleyen Sandworm Çetesi tarafından gerçekleştirildiğini iddia etmiştir (Clark ve Hakim,2017:7). Saldırganlar hedeflerine ulaşmak için basit teknikler kullanmışlardır ancak bu saldırı, enerji ağlarına yönelik bilinen ilk başarılı siber saldırı olması açısından önemlidir (Hemsley ve Fisher,2018:19). Merlo, bu siber saldırıyı uluslararası ilişkiler açısından değerlendirmiş ve Rusya'nın 2014 yılında Kremlin Destekli Devlet Başkanının devrilmesi ile sonuçlanan Ukrayna Devrimi sonrası Ukrayna'ya karşı gerçekleştirdiği operasyonları Ukrayna toplumunun çeşitli sektörlerinini hedef alarak siber uzayda da sürdürdüğünü belirtmiştir. Rusya bu saldırılar ile kendi siber

savaş yaklaşımını mükemmelleştirmiş ve Batının kararlılığını test etme imkanı elde etmiştir (Merlo,2017).

2015-Ukrayna Bilgi Teknolojileri Altyapısına Saldırı

23 Aralık 2015'de yerel saatle 15:35-16:30 saatleri arasında Ukrayna'nın Kyivoblenergo kurumu, bilgi teknolojileri altyapısına üçüncü şahıslar tarafından yetkisiz erişim gerçekleştirildi. Bu ihlal sırasında 30 adet trafo merkezinin bağlantıları kesilmiş; bu da yaklaşık 80.000 farklı müşteri kategorisi için 3 saatlik bir elektrik kesintisine neden olmuştur. Müşterilerin, elektrik kesintisi esnasında kurumun çalışanlarıyla iletişim kurmasını engelleyen bir başka teknik arıza da yaşanmış ve mağdur müşterilerin sayısı 225 bin olarak belirtilmiştir. Ukrayna'daki kesinti, sivil nüfusu doğrudan etkileyen kritik altyapı operatörlerine yapılan siber saldırının ilk örneğidir. Araştırmacılar ve analistlerin hazırladığı raporlar, saldırının arkasında kimin olduğuna ilişkin farklı görüşler sunmaktadır. Ukrayna güvenlik servisi ve iSIGHT Partners'ın analistleri hızlıca Rusya'yı işaret etti. Saldırıya uğrayan kamu kurumlarının bilişim sistemlerinde Moskova merkezli Sandworm grubunun desteklediği BlackEnergy zararlı yazılımına rastlanmıştır. Ray Parks'ın vardığı sonuç, bazı özel uygulamalardan edinilen bilgiler doğrultusunda saldırının büyük ihtimalle bir ulus devletle bağlantısı olan saldırgan grup tarafından yürütüldüğü ancak kişisel güdülerinden dolayı kendi başlarına hareket ettikleridir. SANS EKS tarafından oluşturulan olayın senaryosu ve saldırganların izlediği adımlar şöyledir: 1. Saldırganlar, ilgili kamu kurumunun BT ağlarına, kuruluş çalışanlarına gönderilen e-posta eklerinde saklı kötü amaçlı yazılım aracılığıyla sızmışlardır 2. Saldırganlar olaydan 6 ay önce bir kötücül yazılım aracılığı ile EKS ağlarına erişmek için gerekli giriş kimlik bilgilerini toplamışlardır. 3. Toplanan giriş kimlik bilgilerini ve BT'yi EKS ağlarına bağlayan VPN tünellerini kullanan saldırganlar, EKS ağlarına erişim sağlamış ve siber saldırı araçlarını silah olarak kullanmaya başlamışlardır. Hedefledikleri kamu kurumlarının en az birinde kesintisiz güç kaynağına bağlı bir ağ keşfetmişler; tüm elektriği kesecek ve tetiklenen kesintiyi takiben kamu kurumlarının binalarında ve veri merkezlerinde de kesinti olacak şekilde yeniden yapılandırmışlardır. Daha sonra, trafo merkezleriyle uzaktan iletişim için mağdurların SCADA sistemi tarafından kullanılmakta olan seriden ethernete çevirici cihazlar için kötü amaçlı yazılım geliştirmişler ve dağıtmışlardır. Sonunda, faaliyetlerinin kanıtlarını silmek

ve bazı sistemlerin (örn. HMI'lar) kullanılamamasını sağlamak için ortama kötü amaçlı yazılımlar yerleştirmişlerdir. 4. Bu hazırlıklar bittiğinde, saldırganlar operatörlerin iş istasyonlarının denetimini ele geçirmiş ve çeşitli trafo merkezlerinin devre kesicilerinin açılması için bir komut yayınlamışlar ve kesintiyi sağlamışlardır. Saldırganların faaliyetlerini değerlendirip müdahale etmelerini engelleyecek bir şekilde, iş istasyonlarının klavyelerini ve farelerini bile kullanılamaz hale getiren kötü amaçlı yazılım bileşenleri tarafından operatörlerin gözleri ve elleri bağlanmıştır. Son olarak, saldırganlar, kamu kurumunun çağrı merkezlerine yapılan aramalarda servis dışı bırakma atağı başlattmış; böylece hedeflerin, eylemlerin sonuçlarını fark etme kabiliyetlerini sınırlamış ve kesintiyi bildirmeye çalışan müşteriler engellenmiştir. Koşullar göz önüne alındığında, saldırının mağdurlarının, müşterilerine elektriği tekrar sağlamada son derece hızlı ve etkili davrandığı söylenebilir. Aslında SCADA sistemlerinin zarara uğraması sonucu sürecin uzaktan ve otomatik olarak kontrol edilememesi nedeniyle açık olan devre kesicileri elle yeniden kapatmak ve sistemi çalışır durumuna getirmek için, etkilenen tüm trafo merkezlerinde saha görevlilerini görevlendirmek zorunda kalmışlardır. SCADA sistemi hala kullanılamadığından dolayı, tüm dağıtım süreci olaydan sonra bir süre daha bir tür "acil durum modu"nda çalıştırılmıştır (Trivellato ve Murphy,2018). İlki bir yıl önce gerçekleştirilen bu siber saldırıda, enerji şebekesini sabote etmek için özel olarak tasarlanmış kötü amaçlı bir yazılım kullanılmıştır. Siber güvenlik analistleri, bulunan ipuçları ve olası nedenleri bu saldırıların Rusya tarafından gerçekleştirildiği izlenimini edinmiştir (Puyvelde ve Brantly,2019:285).

2017 ABD, Türkiye ve İsviçre'ye Dragonfly 2.0 Saldırısı

Symantec firması, 2017 Ekim ayında, özellikle ABD, Türkiye ve İsviçre'deki enerji sektörünün gelişmiş bir saldırı grubu tarafından hedef alındığını iddia eden bir rapor yayınlamıştır. Raporda, bu saldırı grubunun gelişmiş kaynaklara sahip olduğu, emrinde bir dizi kötü amaçlı yazılım aracı bulunduğu ve saldırı başlatma yeteneğine sahip olduğu belirilmektedir. Symantec tarafından "Dragonfly 2.0" olarak adlandırılan bu saldırı aracı, operasyonel sistemlere erişim sağlayabilecek ve gelecekte daha yıkıcı amaçlar için kullanılabilecek nitelikte olduğu ve EKS'ni sabote etme veya kontrolünü ele geçirme yeteneğine sahip olduğu vurgulanmaktadır (Symantec,2017).

2020-İsrail Su Arıtma Tesisine Siber Saldırı

Nisan 2020'de İsrail yetkilileri, ülkenin su arıtma sistemlerine yönelik bölgesel su yollarını bozmaya çalışan bir siber operasyon gerçekleştiğini bildirmiştir (Kastelic,2021:3).

2021-Florida Su Arıtma Tesisine Siber Saldırı

8 Şubat 2021'de Florida-Oldsmar'da 15.000 nüfuslu küçük bir kasabanın su kaynağını zehirleme girişiminde bulunulmuştur. Arıtma tesisinde, sistemi uzaktan izlemekte kullanılan bilgisayarlar üzerinde Microsoft Windows işletim sisteminin eski sürümü yüklü olduğu için ve uzaktan yönetim yazılımlarının da eski sürümleri kullanıldığı için güvenlik açıklarından yararlanarak yetkili kullanıcı kimlik bilgilerini kolayca ele geçiren saldırgan, su arıtma sisteminin kullanıcı arayüzüne (HMI) popüler bir uzaktan erişim yazılımı kullanarak uzaktan erişmiş; sudaki asitliği kontrol etmek için kullanılan sodyum hidroksiti normal seviyenin 100 katına çıkarmıştır. Değişiklikler fiziki olarak gerçekleştirilemeden, bir süpervizör saldırı sonucu oluşan hatalı sodyum hidroksit seviyesini tespit etmiş, doğru formülü geri yüklemiş ve saldırıda kullanılan uzaktan erişim sistemini devre dışı bırakmıştır (Izuakor,2021).

Çevre açısından önemli olumsuz sonuçlara neden olamamasına rağmen bu saldırı, yeterli güvenlik önlemleri alınmaksızın sisteme uzaktan erişimi kullanmanın risklerini gündeme getiren bir örnektir.

2021-Colonial Akaryakıt Boru Hattına Saldırı

ABD'deki rafine petrol ürünleri için en büyük boru hattı sistemi olan Georgia merkezli Colonial Pipeline, Mayıs 2021'de saldırıya uğramış ve şirketin yakıt dağıtımı için Amerika'nın ana arterlerinden birini kapatmasına neden olmuştur. Colonial Şirketi ve FBI, bilgisayar korsanlarının Doğu Avrupa dışında faaliyet gösteren organize bir suç grubu olduğunu bildirmiştir. Saldırganlar, firmanın kurumsal BT sistemlerinin kontrolünü ele geçirdikleri olayda saldırının sadece şirketin kurumsal BT sistemleriyle sınırlı olmasına rağmen şirket, operasyonel altyapıyı saldırıdan kaynaklanabilecek olası hasarlardan korumak için proaktif olarak operasyonlarını durdurma kararı almıştır. Günde 3 milyon varil yakıt taşıma kapasitesine sahip Colonial Pipeline'ın dağıtım ağı, Texas'tan New York'a 5500

milden fazla uzanan iki devasa tüpten oluşmaktadır. Saldırı tespit edildikten sonra şirket, BT ve OT (Operasyonel Teknoloji) altyapısını kapatmıştır. Petrol dağıtımı bir hafta süre ile gerçekleştirilememiştir. Petrol dağıtımının gerçekleştirilememiş olması zincirleme olarak diğer faaliyetleriin yerine getirilmesinde aksaklıklara neden olmuştur (Izuakor, 2021)

Fidye yazılımı Ransomware kullanılarak gerçekleştirilen bu siber saldırıda firmanın kurumsal BT sistemleri ele geçirildiği gibi, proaktif önlem olarak petrol dağıtım faaliyetini yerine getirmekte olan operasyonel teknoloji altyapısı kapatılmamış olsaydı bu sistemlerin kontrolü de saldırganların eline geçebilirdi; dağıtımı yapılan petrolün kontrolden çıkması ile yangınlar, patlamalar, atmosferde, tarım alanlarında, sularda kirlilik yaratarak önemli çevre sorunlarına neden olabilirdi.

2.3.2. Kritik Altyapılara Yönelik Siber Güvenlik Olayı Örneklerinin Siber Güvenlik Açısından Değerlendirilmesi

EKS yardımı ile faaliyetlerini yerine getirmekte olan kritik altyapılara yönelik siber güvenlik olaylarının önemli çevre sorunlarına yol açarak sürdürülebilirliği engelleyip engelemeyeceği araştırıldığı için açık kaynaklardan edinilen bilgiler ışığında 1982 yılından bu yana gerçekleşmiş bazı siber güvenlik olayları incelenmiştir.

Her geçen gün niteliği, hedefi, oluşturduğu riskleri farklı olan çok sayıda yeni tehditler piyasaya sürülmekte ve farklı sonuçlara neden olmaktadırlar. Bu çalışmada özellikle enerji üretim, dağıtım, su, kimya, nükleer sanayi, bilişim ve iletişim sektörlerinde hizmet vermekte olan kritik altyapıların siber güvenliği ele alındığı için siber güvenlik olayı örnekleri de sadece bu kritik sektörlere yönelik altyapılar arasından seçilmiştir. Farklı sektörlere yönelik siber güvenlik olaylarının farklı etkiler doğurabileceği bu örneklerden de anlaşılmaktadır. Bir nükleer enerji üretim santraline yönelik bir siber güvenlik olayı, su arıtma tesisine yönelik siber güvenlik olayından daha farklı bir etki yaratacaktır. Bu tip siber güvenlik olaylarının birlikte kullanılması, yıkımı daha da kolaylaştırabilecektir. Bir siber güvenlik olayının en kötü etkisi EKS'ni sadece devre dışı bırakmak değil bu EKS'ni kontrol eden sürecin bozulması da olabilmektedir (Bayuk vd., 2012:60).

Siber olayların yangın, sel, deprem gibi doğal felaketler sonrası oluşabileceği; öfkeli kurum çalışanları ya da görevden alınan eski çalışanların bilinçli faaliyetleri; kurum

çalışanlarının yeterli bilgi sahibi olmamaları ya da dikkatsizlikleri sonucu meydana gelebileceği; ilgili kurumu siyasi, ekonomik, askeri vb. nedenlerle hedef olarak belirleyen bireysel siber saldırganlar, siber teröristler ya da ulus devletlerin kendi siber savaşçıları ya da destekledikleri organize suç örgütleri tarafından gerçekleştirilen siber saldırılar sonucu oluşabileceği anlaşılmaktadır.

Kamu hizmeti görmekte olan pekçok şirket, kritik altyapı sistemlerinin fiziki olarak uzak mesafeden yönetimini sağlamak üzere, EKS'ne uzaktan erişime izin vermektedir. Ancak bu durumda çok faktörlü kimlik doğrulama, güçlü şifreler vb. gibi gerekli güvenlik önlemleri alınmaksızın bu erişimler sağlanabilmektedir. Siber saldırılar konusunda gelişmiş teknolojik araçları ve yöntemleri kullanabilen rakipler tarafından yapılan benzer bir saldırı, potansiyel olarak kamuya yönelik kritik hizmetlerin yerine getirilmesini önleyebilecek ve ciddi zararlar verebilecek niteliktedir.

Kritik altyapıların faaliyetlerini yerine getirmesinde kullanılmakta olan endüstriyel kontrol sistemlerinin bilişim sistemleri ile bütünleşmeye başlamasının saldırı yüzeyinin hızlı bir şekilde genişlemesine yol açtığı anlaşılmaktadır.

Ulus devletlerin, diğer devletlerde yer alan kritik altyapılara saldırmak için aktif olarak siber yeteneklerini geliştirmekte oldukları ve siber saldırıların kritik altyapılara zarar vermenin gerçekten mümkün olduğunu gösteren örnek olaylar geçekleşmiştir.

Bireylerden kaynaklanan küçük hataların hizmet, üretkenlik kaybı kimi durumlarda ise ölüm ve yaralanmalarla önemli çevre felaketlerine yol açabileceği görülmüştür.

Bir saldırının veya arızanın erken aşamalarında doğru kararları vermekten sorumlu kişilerin, karşı karşıya oldukları sorunu tam olarak anlamaları ve buna uygun faaliyetler yürütmeleri oldukça zordur. Sistemi işletmekten sorumlu operatörlerin belirsizlikle başa çıkmaları da çok zordur.

Siber saldırılar kurum çalışanları tarafından yapılabildiği gibi, kurumun anlaşmalı olduğu taşeron firma çalışanları tarafından da gerçekleştirilebilmektedir. Kimi durumlarda, kurumun siber güvenliğini geliştirmek amacı ile güvenlik açıklarını belirlemek üzere sızma testi yapan ve beyaz şapkalı hacker olarak adlandırılan siber güvenlik profesyonelleri de daha sonraki aşamalarda siber saldırılar gerçekleştirebilmektedir.

EKS'nin eski teknoloji ürünü olduğu, geleneksel bilişim sistemleri ve yeni nesil iletişim sistemleri ile bütünleştirilmediği için saldırıya maruz kalmasının zor olduğu inanışının da bu sistemlerin kurulması ve bakımı görevlerinde bulunan kişiler tarafından saldırıya maruz kalabilecekleri için geçersiz olduğu anlaşılmıştır.

Kritik altyapıları etkileyen kötü niyetli siber faaliyetlerin önemli bir kısmı saldırıya uğrayan kuruluşlar ve devletler tarafından fark edilemeyebilmekte ya da fark edilmesine rağmen kamuya açıklanmayabildiği için bu tarz kayıtlı siber olayların sayısı, mevcut istatistiklerden ve raporlarda belirtilenlerden daha yüksek olabileceği değerlendirilmektedir.

Kritik altyapıları etkileyen siber olayların çoğunun, altyapı operatörlerinin talepleri doğrultusunda ya da bu altyapıları kendi sınırları içinde barındırmakta olan devletlerin mevzuatları gereği kamuya açıklanmasının engellendiği görülmektedir. Bazı teknoloji firmaları da mevcut durumda meydana gelen siber güvenlik olaylarının, kamuya duyurulan siber güvenlik olayları sayısından çok daha fazla olduğunu iddia etmektedir (Kastelic,2021:2). Bu bölümde incelenen örneklerde de görüldüğü gibi pek çoğu ilgili devletler ve ilgili kurumsal yapılar tarafından ulusal güvenlik kaygıları, prestij kaybı gibi nedenlerle kamuya açıklanmamakla birlikte modern devletlerde şimdiye kadar gerçekleşen siber güvenlik olaylarından, siber tehdit aktörlerinin yeteneklerinin teknolojik gelişmeler paralelinde önemli ölçüde geliştiğini ve fiziksel hasar verme istekleri olduğu, saldırganların kötü niyetli, yıkıcı saldırılar yapmaya istekli ve yetenekli oldukları anlaşılmaktadır.

Fiziksel dünyanın siber güvenlik olaylarından önemli ölçüde etkilenebileceğinin en önemli göstergelerinden biri, karmaşık bir tehdit aktörünün istediği her sisteme saldırabilecek durumda olmasıdır (Hemsley ve Fisher,2018:23). Belirli bir EKS'ni hedef alan gelişmiş kötü amaçlı yazılımlar aracılığıyla gerçekleştirilen son derece karmaşık siber saldırı örnekleri yaşanmaktadır.

Çıkarılması gereken en önemli sonuçlardan birisi, tüm sistemleri saldırganların tümünden korumak mümkün olmadığı için, kritik altyapılarda bir siber saldırıyı algılama ve kurtarma becerisinin geliştirilmesi gerektiğidir. Night Dragon gibi saldırılardan, yetenekli ve ısrarcı bir düşman tarafından uygulanan basit tekniklerin, enerji sektöründeki şirketler de dahil olmak üzere kritik altyapıya girmek için yeterli olduğu görülmekedir. Kritik altyapılara

yönelik siber saldırıların ilk aşamasında Duqu, Flame ve Gauss gibi kötücül yazılımlar kullanılarak ihtiyaç duyulan istihbaratın toplandığı anlaşılmaktadır.

Hükümetler ve işletmeler, güvenlik konusunda daha dikkatli ve zorlu savunucular olmak zorundadır. Teknolojik gelişmeler paralelinde siber saldırıların karmaşıklığı gittikçe arttığı için saldırı yüzeyini azaltarak olası hasarları kontrol altına alabilmek ve sistemi siber güvenlik olayı gerçekleşmeden önceki durumuna döndürebilmek için daha iyi savunma yöntemleri ve kontrollerin uygulanması gerekmektedir. Kuruluşların, devam etmekte olan tehditleri ve saldırıları tespit etmek üzere daha gelişmiş teknikleri kullanmaları ve hasarı en aza indirmek için saldırı yaşam döngüsünün en başından itibaren saldırıyı anlamaları ve buna uygun önlemleri uygulamaları gerekmektedir. Bu önlemler arasında, akıllı izleme gibi daha gelişmiş teknolojik ürünlerin, güvenlik odaklı süreçlerin ve güvenlik hijyeninin farkında olan bir iş gücünün bulunması sayılabilir. Bu saldırıların geniş kapsamlı ve endişe verici sonuçlarının iyi takip edilmesi, çözümlerin önceliklendirilmesinde yardımcı olabilecektir.

Bu örnekler, bilişim sistemlerinin kullanıldığı kritik altyapıların kötücül yazılımlar, güvenlik açıkları gibi siber güvenlik olaylarına karşı korumasız olduğunu ve riskin her geçen gün artacağını, bilişim sistemlerinin endüstriyel kontrol sistemleri ile gereken önlemler alınmadan bağlandığında ve ilgili personele yeterli eğitim verilmediğinde, ayrıntılı iş bölümünü de kapsayan koruyucu ve önleyici müdahale yöntemleri belirlenmediğinde, ciddi sonuçlar doğuracağını göstermektedir. Kritik tesislerin siber saldırılardan korunmasını sağlamak üzere siber saldırılar konusunda deneyimli, eğitimli, özel yazılım ve donanımları kullanabilen olay inceleme ekiplerinin görevlendirilmesi de çok önemlidir. EKS her geçen gün daha fazla oranda internete bağlandığı ve bilişim sistemlerine bağımlı hale geldiği için bu liste her geçen gün daha da uzayıp çeşitlenecektir.

Cavelty, 2008 yılında, siber güvenlik olaylarının çevresel sürdürülebilirliğe etkisi ile ilgili olarak bilgisayar ağlarından kaynaklanan zafiyetlerin artan bir biçimde ciddi problemlere neden olmakta olduğunu belirtmiştir. Ancak bu zafiyetlerin nasıl bir çevre sorunu oluşturabileceği konusunun da abartılmaması gerektiğini vurgulamıştır (Cavelty, 2008: 144). Puyvelde ve Brantly de medyanın, siber güvenlik şirketlerinin CEO'larının, okuyucularının ve müşterilerin dikkatini çekmek üzere 'Siber Pearl Harbour' ve 'cybergeddon' gibi terimleri sıklıkla kullanmışlar ancak şüpheci yaklaşıma sahip

gözlemcilerin bu senaryoların gerçekleşmediğini sıklıkla dile getirmiş olmalarına dikkat çekmişlerdir (Puyvelde ve Brantly,2019:274). Kritik altyapılara yönelik siber güvenlik olayları sonrası çok büyük çaplı çevre sorunları yaşanmamıştır. Çok büyük ölçüde can kaybına ve çevre felaketlerine, fiziki hasara neden olduğunu gösteren örnekler bulunmasa da bu alandaki hızlı teknolojik gelişmeler ve örnek olaylar göz önünde bulundurulduğunda, bu tarz fiziki hasarlı siber güvenlik olaylarının gerçekleşme ve hasar yaratma olasılığının hiç de düşük olmadığı değerlendirilmektedir.

2.3.3 Kritik Altyapılara Yönelik Siber Güvenlik Olaylarının Sürdürülebilirlik Açısından Değerlendirilmesi

Bu çalışma kapsamında, siber güvenliğin, tüm canlıların, varlıkların ve doğa olaylarının mevcudiyetinin devam ettirilmesi; günümüzdeki nesillerin ihtiyaçlarının gelecek nesillerin kullanımını etkilemeksizin sürdürebilmesi olarak açıklanabilecek olan çevre etiği yaklaşımı açısından ele alınması nedeni ile çevre üzerinde fiziki etki oluşturabilecek siber güvenlik olayı örnekleri incelenmiştir. Ulus devletlerin ya da işletmelerin ulusal güvenlik ve prestij kaygısı gibi nedenlerle şeffaf davranmadığı, tüm olayları açıklamadığı günümüz dünyasında kısıtlı sayıda örnek olay bilgisi edinilebilmiştir. Bu kısıtlı sayıdaki örnek olayda bile, petrol boru hatlarına, nükleer santrallere, elektrik üretim ve dağıtım hatlarına, sulama, kanalizasyon, su arıtma tesislerine, kimyasal tesislere vb.ne yönelik siber güvenlik olaylarının çevreye önemli ölçüde zarar verdiği durumların yaşandığı ya da çevre üzerinde önemli olumsuz etkiler oluşturma kapasitesinin yüksek olduğu görülmüştür.

Dünya üzerinde temel enerji kaynaklarından olan petrol üretim ve aktarım tesislerinde bu sistemleri izlemek ve uzaktan yönetimini gerçekleştirmekte yararlanılan SCADA sistemlere yönelik kasıtlı ya da kasıtsız siber saldırılar sonucu ham petrolün, doğal gazın çevreye yayılması, canlıların yaşamını olumsuz yönde etkileyebilecek patlamalara, yangınlara neden olmuş; toprağın verimsizleşmesi, havanın kirlenmesi, bitki örtüsünün bozulması ile insan, hayvan diğer canlıların ve varlıkların sürdürülebilirliğinin tehlike altına girdiği durumlar yaşanmıştır.

Nükleer santrallere yönelik siber güvenlik olayları bu santrallerde kullanılmakta olan EKS'nin işlevlerini yerine getirememesi ya da yanlış çalışması durumlarını ortaya çıkarmıştır. Henüz bilinen büyük boyutlu çevre sorunları yaşanmamış olsa da bir nükleer

santral sisteminin istenen şekilde çalışmaması ve kontrolden çıkması tüm dünya için radyoaktif sızıntı, patlamalar, yangınlar yolu ile ekosistemi bozacak, geri dönülemez çevre felaketlerine yol açabilecek potansiyele sahiptir.

Barajlarda, içme suyu ve kanalizasyon sistemlerinde yoğun olarak kullanılmakta olan EKS'nin dışarıdan br müdahale ile işlevini yerine getirecek şekilde çalışmaması ya da belirlenen şekilde faaliyetini yerine getirmesinin önlenmesi durumunda can kaybına, çevre kirliliğine neden olan siber güvenlik olayları yaşanmıştır. Bu sistemlere yönelik daha büyük boyutlu siber güvenlik olaylarının yaşanması seller, su taşkınları, içme sularına zehirli kimyasal karıştırılması, bitki örtüsünün ve besin zincirinde yer alan diğer canlıların yaşamlarını sürdüremiyeceği, varlıkların önemli hasar göreceği önemli çevre felaketlerine yol açabilecektir.

Elektrik üretim ve dağıtım sistemleri de hızlı bir şekilde sayısallaştığı ve birbirine bağlandığı için bu sistemlerde kullanılmakta olan bir EKS'nde meydana gelen siber güvenlik olayının geniş alanlarda uzun süreli elektrik kesintilerine yol açtığı ve kalabalık nüfusların elektriksiz kaldığı örneklerde görülmüştür. Elektrik kesintilerinin ölüm oranlarında artışa neden olduğu kanıtlanmıştır (Anderson ve Bell,2012). Bu sistemlerde oluşan siber güvenlik olayları sadece elektrik kesintisi ile sınırlı değildir yangınlar, patlamalar yolu ile önemli çevre felaketlerine yol açabilecek kapasitededir.

Daha önce de değinildiği gibi, yukarıda bahsi geçen kritik altyapılar birbirlerine ağlarla bağlı olduğu için oluşan hasar sadece küçük bir fiziki alanla sınırlı değildir, birbirlerini tetikleyebilecek çok önemli çevre felaketlerinin yaşanmasına neden olabilecektir. Günümüz modern dünyasında hemen hemen tüm faaliyetler için enerji ihtiyacı olması nedeni ile ve enerji nakil hatları da birbirleri ile bağlantılı olduğu için bir elektrik kesintisi olması durumunda bu tek bir ülke ile sınırlı kalmamakta, bölgesel olarak etkili olabilmektedir. Elektrik kesintisi, hayati öneme sahip pekçok faaliyetin yapılamaz hale gelmesine neden olmaktadır. Yine günümüz modern dünyasında pekçok işlem ağlarla birbirine bağlı bilişim sistemleri üzerinden gerçekleştirildiği için bu sistemlerde oluşacak bir siber güvenlik olayı diğer sektörlerdeki faaliyetlerin de yerine getirilememesine, önemli aksamalara neden olabilecektir.

Bu kısımda, çalışmanın temel sorunu olan siber güvenlik olaylarının çevre etiği açısından önemli sonuçlar meydana getirip getiremeyeceği sorusuna yanıt aranmıştır. İşlevlerini yerine getiremedikleri durumda önemli çevresel sorunlara yol açabilecek enerji üretim, dağıtım, su ve kanalizasyon, nükleer tesisler ve kimyasal tesisler gibi kritik altyapılarda son dönemlerde endüstriyel kontrol sistemlerinin yoğun olarak kullanılmaya başlandığı, endüstriyel kontrol sistemlerinin de bilgi ve iletişim teknolojilerindeki gelişmeler sonrası her geçen gün daha da artan bir şekilde dijitalleştiği ve siber fiziki sistemler olarak adlandırıldığı görülmüştür. Bu sistemlere yönelik kasıtlı insan faaliyetleri ile gerçekleştirilen siber saldırı olayları, sistemlerin korunmasına yönelik işlemlerin düzgün bir şekilde gerçekleştirilmediği durumlarda ya da deprem, yangın, sel gibi doğal felaketler sonucu oluşan siber güvenlik olaylarının fiziki çevre üzerinde canlı ve cansız varlıkların sürdürülebilirliğini olumsuz yönde etkileyebileceği sonucuna varılmıştır.

Ele alınan olaylardan mevcut durumda iki devletin karşılıklı olarak siber saldırılar ile gerçekleşen bir siber savaş durumunun henüz yaşanmadığı ancak hibrid savaş yöntemi olarak diğer fiziki saldırıları desteklemek üzere Estonya örneğinde de görüldüğü gibi siber saldırılara maruz kalınabildiği görülmüştür.

İncelenen örnekler ile, BM'e üye devletler tarafından 2015 yılında kabul edilen sürdürülebilir kalkınma hedeflerinin, kritik sektörler ve kritik altyapıların doğru çalışması ve siber saldırılardan, siber güvenlik olaylarından korunması ile yakından ilgili olduğu anlaşılmıştır.

ÜÇÜNCÜ BÖLÜM

KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK OPERASYONEL FAALİYETLER

Hayati öneme sahip hizmetleri yerine getirmek üzere kullanılmakta olan ve yok olması, zarar görmesi ya da hatalı çalışması durumunda önemli çevresel güvenlik sorunlarına yol açabilecek kritik altyapı sistemlerinin faaliyetlerini yerine getirmek üzere siber fiziki sistemler olarak da adlandırılmakta olan endüstriyel kontrol sistemleri (EKS) kullanılmaktadır. Dijital dönüşüm ve endüstriyel nesnelerin interneti (IIOT) sayesinde edinilecek verimlilik ve yeni iş modelleri Bilişim Teknolojileri (BT) ve Operasyonel Teknolojilerin (OT) bütünleştirilerek hizmete sunulmasını hızlandırmıştır. Bu durum daha büyük riskleri de beraberinde getirmekte olduğu için EKS'nin siber güvenliğinin sağlanması her geçen gün daha da zorlaşmaktadır.

İkinci Bölümde, endüstriyel kontrol sistemlerinin kullanılmakta olduğu kritik altyapılara yönelik siber güvenlik açıkları ve tehditlere yer verilmiş; teknolojideki hızlı gelişmeler paralelinde bu tehditlere ve siber güvenlik açıklarına her gün yenilerinin eklenmekte olduğu görülmüştür. Açık kaynaklardan edinilen bilgiler ışığında derlenen kritik altyapılara yönelik siber güvenlik olayları örneklerinden, doğal felaketler, siber saldırılar ya da istemsiz insan faaliyetleri sonucu gerçekleşen bir siber güvenlik olayının önemli çevre felaketlerine yol açabileceği ve sürdürülebilirliği engelleyebileceği anlaşılmıştır.

Bu sistemlerin zarar görmeksizin planlandıkları gibi faaliyetlerine devam etmeleri, çevre etiği açısından sürdürülebilirliğin sağlanması yani bugün yaşamakta olan kuşağın gereksinimlerinin, gelecek nesillerin kendi ihtiyaçlarını karşılama yeteneğini ortadan kaldırmaksızın karşılanmasının sağlanabilmesi için gerekli güvenlik önlemleri alınmalıdır.

Siber güvenlik uzun bir süredir bilişim teknolojileri alanında çalışmakta olan mühendisler, bilgisayar bilimciler gibi teknik personelin ilgi alanı içinde iken son yirmi yılda, sosyal bilimler alanında da tartışılmaya başlanmıştır. Siber güvenliğin sadece teknolojik boyutu değil, bireysel, kurumsal, ulusal ve uluslararası boyutları da gündeme

getirilmeye başlanmıştır (Puyvelde ve Brantly,2019:456). Bu çalışmada Endüstriyel kontrol sistemlerinin dolayısı ile kritik altyapıların siber güvenliğinin sağlanmasına yönelik faaliyetler operasyonel faaliyetler ve stratejik faaliyetler olarak 2 grupta toplanmıştır. Bu sistemlerin tasarımı, geliştirilmesi, üretilmesi, kullanımda olması ve kullanım dışı kalması aşamalarını kapsayan tüm yaşam döngüleri boyunca doğrudan ilişkili bireyler ve kuruluşlar tarafından gerçekleştirilen faaliyetler, operasyonel faaliyetler olarak adlandırılmıştır. Sistemlerin siber güvenliğinin sağlanmasına yönelik politika ve stratejilerin geliştirilmesi faaliyetleri ise stratejik faaliyetler olarak adlandırılmıştır.

Bu bölümde kritik altyapıların siber güvenliğinin sağlanmasında birinci dereceden sorumluluğu olan bireyler ve kurumsal yapılar tarafından gerçekleştirilmesi gereken siber güvenlik faaliyetlerine yer verilecek ve bu faaliyetlerin yeterli olup olmadığı irdelenecektir. Bu kapsamda öncelikle operasyonel seviyede bireyler ve kurumlar tarafından uygulanabilecek olan önleyici koruyucu yaklaşım ve risk yönetimi yaklaşımları açıklanacak; daha sonra bireysel ve kurumsal seviyede operasyonel siber güvenlik faaliyetleri üzerinde durulacaktır.

3.1 OPERASYONEL SİBER GÜVENLİK YAKLAŞIMLARI

Bilişim sistemlerinin yetenekleri, kullanıldıkları alanlar, kullanım şekilleri ve kullanıcı kitlesi geliştikçe siber teröristlerin, siber savaşçıların ya da siber suçluların gerçekleştirdikleri siber saldırılar, doğal olaylar sonucu ya da çalışanların kazara gerçekleştirdikleri siber olayların önlenmesine yönelik siber güvenliğin sağlanması yaklaşımlarında da değişiklikler olmaktadır. Bir önceki bölümde yer verilen örnek olaylardan da anlaşılacağı üzere hayatın her alanında yoğun olarak kullanılmakta olan bu teknolojilere yönelik siber olaylar sürdürülebilirliği olumsuz yönde etkileyebilecek, çok önemli olumsuz çevresel sonuçlara neden olabilecek niteliktedir.

Geleneksel bilişim teknolojilerinin güvenliğinin sağlanmasında genellikle birbirlerine ağlarla bağlı bilgisayar sistemlerinin yazılımsal ve donanımsal olarak korunmalarına odaklanılmaktadır. EKS'nin güvenliğinin sağlanması için ise geleneksel bilgi ve iletişim sistemleri güvenliği ve kontrol mühendisliğinin birlikte uygulanması gerekmektedir. Ancak son zamanlarda IP tabanlı iletişim altyapısının kullanılmaya

başlanması ile geleneksel BT güvenliği, iletişim güvenliği ve kontrol sistemlerinin güvenliğinin sınırları belirsiz hale gelmiş ve birbirlerinin içine girmiştir (Luallen,2014:3). Kritik altyapı sistemlerinde son yıllarda gerçekleşen en önemli teknolojik değişiklik olarak kabul edilen, bilgisayarlaşmanın artması ve büyük ölçekli endüstriyel faaliyetlerin kaçınılmaz sistemleri olan EKS'lerin birbirleri ile bağlantılı hale gelmesi, yeni fırsatların yanı sıra yeni güvenlik risklerini de beraberinde getirmektedir (Tabansky,2017:212) (Misbahuddin ve Al-Holou, 2012:176). Her gün, dünyanın herhangi bir yerindeki şirketlerin ya da devlet kurumlarının yaşadığı siber güvenlik olayları gündeme gelmektedir. Şiddetli etkiler oluşturarak fiziki yıkıma neden olan siber saldırı örnekleri çok fazla değildir ancak bu tarz saldırılar kamuoyunda daha fazla dikkat çekmektedir.

EKS'nin siber güvenliğin sağlanmasında teknoloji tek başına belirleyici değildir ve farklı yaklaşımların kullanılması gerekmektedir. Mulligan ve Schneider, önleyici/koruyucu yaklaşım, risk yönetimi yaklaşımı, caydırıcılık yaklaşımı ve kamu siber güvenlik yaklaşımı olmak üzere 4 farklı siber güvenlik yaklaşımından bahsetmektedir (Mulligan ve Schneider,2011:72-78). Bu siber güvenlik yaklaşımları çoğu kez birbirlerini tamamlayıcı şekilde birlikte kullanılmaktadır. Ancak bireysel ve kurumsal seviyede daha sıklıkla kulanılmakta olan önleyici- koruyucu siber güvenlik yaklaşımı ile risk yönetimi yaklaşımı bu kısımda açıklanacaktır.

3.1.1 Önleyici-Koruyucu Yaklaşım ve Emniyetli-Sağlam Sistemler

Güvenli olduğu kabul edilen bir sistem, zaman içinde güvenlik özelliklerini kaybedebileceği için, sistemin içinde bulunduğu ortam belirli aralıklarla gözden geçirilmeli ve gerekiyorsa değişiklikler yapılmalıdır. Bu yaklaşım, bir siber olayın gerçekleşmesi öncesi proaktif önlemlerin alınmasını ve alınan tüm önlemlere rağmen bir siber olayın gerçekleşmesi durumunda da vereceği hasarı en aza indirgemek üzere gerekli faaliyetlerin gerçekleştirilmesini kapsamaktadır. Geleneksel bilişim sistemleri ilk kullanılmaya başlandığı, daha basit ve yalın oldukları dönemlerde, bu sistemlerin tüm güvenlik açıklarının kapatılması halinde saldırıların risk olmaktan çıkacağı kabul edilmiş ve yazılım, donanım ve ağ teknolojileri kullanılarak sistemlerin tüm güvenlik açıklarının kapatılması yolu ile saldırıların risk olmaktan çıkarılması ve güvenli sistemlerin kullanıma sunulması hedeflenmiştir. Zaman içinde bilişim teknolojilerindeki hızlı ve kapsamlı gelişmeler sonucu

bu sistemler her alanda kullanılmaya başlanmıştır. Günümüz dünyasında hem eski sistemler hem de son teknoloji ürünü kritik sistemlerin kullanılmasına devam edilmekte olup bu teknolojileri tasarlayan, üreten, kurulumunu yapan, kullanan çok çeşitli insan profilinin yer aldığı siber uzayda mutlak bir siber güvenliğin sağlanması çok daha zor bir duruma gelmiştir.

Kritik altyapıların faaliyetlerini yerine getirmesi için kullanılmakta olan ve siber fiziki sistemler, operasyonel teknolojiler olarak da adlandırılmakta olan endüstriyel kontrol sistemleri 1960'lı yıllarda veri toplama ve gerçek zamanlı iş süreçlerini kontrol etmek üzere kullanımına başlanan EKS'nin kontrolü mekanik veya elektromekanik röle tabanlı sistemlerle gerçekleştirilmiştir (Flaus,2019:7). Bu dönemde EKS için siber güvenlik riski bulunmamakta idi. 1971 yılında mikroişleyicilerin icadı ve giriş çıkış bileşenlerinin entegrasyonu ile mikrokontrol birimlerinin de gelişmesi sonrasında EKS'nin analog bileşenlerinin yerini mikroişleyiciler almaya başlamıştır. Bu dönemde de siber güvenlik EKS için risk olarak değerlendirilmemiştir. EKS için ilk dönemlerde patentli ve tek başına çalışan kapalı ağlar kullanılırken 1990'ların sonlarından itibaren bu sistemler IP tabanlı ağları kullanmaya başlamışlardır. İnternet ağlarının tüm dünya üzerinde yaygınlaşması ile eski ya da yeni teknoloji ürünü tüm EKS de bu ağlara bağlanmaya başlanmıştır. (Alcaraz vd., 2015:6).

Siber uzayda bilgisayarları, ağları veya kullanıcılarını alınacak önlemlerle tam olarak koruma yolu bulunmamaktadır (Puyvelde ve Brantly,2019:389). Bu durum, EKS'ler için de artık koruyucu/önleyici güvenlik önlemlerinin alınmasını zorlaştırmaktadır. Son yıllarda önleyici/koruyucu güvenlik yaklaşımı kapsamında, bu sistemlerin emniyeti ve dayanıklılık özellikleri gündeme getirilmektedir.

Kritik altyapıların işlevlerini yerine getirmelerinde kullanılmakta olan EKS'nin temel bileşeni operasyonel teknolojiler iken son dönemdeki teknolojik gelişmeler paralelinde operasyonel teknolojiler ile bilişim teknolojileri bütünleştirilmeye ve birlikte kullanılmaya başlanmıştır. Fiziki süreçlerin yönetimi işlevini yerine getirme görevi bulunan OT'ler için sistemin emniyeti de önem kazanmaktadır. Bir sistemin emniyetli olması, deprem, yangın, sel gibi doğal felaketler, kasıtlı ya da kasıtsız siber olaylar esnasında ve sonrasında normal olmayan koşullar altında faaliyetlerini sürdürebilmesi için, kendi işleyişini ayarlama yeteneğidir (Johnsen vd., 2009:114). Hollnagel, Woods ve Leveson'a göre dayanıklılık, "bir sistemin, büyük bir aksaklıktan sonra veya sürekli stresin varlığında

bile operasyonları sürdürebilmesi için, değişiklikler ve bozulmalardan önce veya sonra işleyişini ayarlamaya yönelik içsel yeteneği" olarak tanımlanmaktadır (2006). Dayanıklılığın sağlanması sistemin kritik bileşenlerinin sürekliliğini desteklemek için kilit bir strateji durumundadır (Johnsen,2013:288). Genellikle bir EKS'nin normal çalışmaması personelden ya da dış ortamın yani çevrenin, bu sistemin güvenliğini olumsuz yönde etkilemesinden kaynaklanmaktadır. Güvenlik endişeleri, patlamalar, çarpmalar gibi kinetik kuvvetlerden, elektrik çarpmasından, radyasyondan veya toksik kimyasal madde salımlarından kaynaklanabilmektedir. Bu nedenle, emniyet genellikle EKS operatörleri için en yüksek önceliktir. EKS'nde, genellikle emniyet parametrelerini izlemek için özel olarak tahsis edilmiş sistemler bulunmalıdır (Hahn,2016:52).

EKS'nin çalıştırılması, bakımı ve güvenliği konusundaki sorumluluk gereği emniyet ve güvenlik arasındaki yakın ilişki vardır (Krutz, 2006:76-77). EKS içindeki prosedürlerin ve politikaların çoğu önce emniyet ilkesine dayalıdır. Bir EKS'nin hatalı çalışması nedeniyle ölüm olayları ve canlı cansız varlıkların sürdürülebilirliği için zorunlu olan fiziki çevre hasarı yaşanması gibi çevre üzerinde olumsuz etkiler meydana getirebilecek nitelikte tehditler ve güvenlik açıkları bulunmaktadır.

Sistemlerin dayanıklılığı, belirli koşullar altında, mümkün olduğunca az işlevsellik kaybıyla beklenmeyen durumlara dayanabilen, kurtarma süresini en aza indirerek yeni koşullara uyum sağlayıp olası hizmet kesintisinin süresini azaltarak ve sistemlerin işlevselliğini geliştirerek beklenmeyen durumlara dayanma yeteneğini kapsamaktadır (OECD, 2019:309).

Kritik altyapıların karşı karşıya olduğu yangın, deprem, sel gibi doğal afetler ve bu afetlerin iklim krizi sonrası etkilerinin katlanarak arttığı; istemsiz kaza eseri insan faaliyetleri ve bilişim teknolojilerindeki çok hızlı gelişmelerin kullanılması ile gerçekleştirilebilecek hedefli saldırılar sonucu meydana gelen siber olaylar ya da hibrit siber olayların tamamını engellemek mümkün değildir. Kritik altyapılara yönelik risk ve tehdit çeşitliliği bu sistemlerin dayanıklılığı yaklaşımının uygulanmasını gerektirmektedir (OECD,2019:35). Siber güvenliğin temel hedefi sistemlerin ve altyapıların değişen koşullara uyum sağlayabilmesi yolu ile tüm siber olaylara karşı dayanıklı olmasını temin etmektir. Sistem, saldırıların ilk aşamasında önlenebilmesini sağlayacak nitelikte, saldırılara karşı güçlü

olmalı; saldırıdan sonra da en kısa zamanda normal çalışma durumuna döndürülebilmelidir (Rajamaki, 2017:237).

Barami, kritik altyapıların dayanıklılığı sistemik yaklaşımın, karmaşıklığı, karşılıklı bağımlılıkları ve karşılıklı bağlantıları daha iyi bütünleştirilebilmesinde tamamlayıcı bakış açısı sunduğunu savunmaktadır. Günümüz dünyasında kritik altyapıların doğal afetlerden, hatalı teknolojik üretimden veya insanlar tarafından gerçekleştirilen terör olaylarından kaynaklı olarak faaliyetlerini sürdürememesi olasılığı vardır. Kritik altyapıların hizmetlerinde kesinti olmasına yönelik en dikkat çeken riskler arasında, iklim krizi ve birbirine ağlarla bağlı günümüz dünyasında karşılıklı bağlantılar ve bağımlılıklar nedeni ile yeni güvenlik açıkları bulunması; bu sistemleri birbirine bağlayan siber fiziksel altyapılar aracılığı ile birbirini tetikleyecek yeni risklerin oluşması sayılabilir. Bu tür risklerin gerçekleşmesi insanlığı her geçen gün daha da savunmasız hale getirmektedir. Bu riskleri sistem seviyesinde ele almak için dayanıklılık yaklaşımı kullanılmaktadır. Dayanıklılık yaklaşımı ile günümüzün karmaşık altyapıları arasındaki bağlantıları ele almak için risk tabanlı ve katmanlı bir yaklaşım benimsenmekte; altyapıların tasarımı, üretimi ve işletilmesine yönelik bir yaşam döngüsü modeli kullanılmaktadır (Barami,2013:1).

Esnek bir kritik altyapı sisteminin temeli katmanlı savunma ilkeleri ile birleştirilmiş sistematik risk değerlendirmesidir. Risk analizi modeli olumsuz olayların risklerini tehdit ya da tehlikelerin gerçekleşme olasılığı ile sonuçların ciddiyetini tahmin etmek üzere kullanılmaktadır. Bir tehdidin gerçekleşmesi için altyapı alt sistemlerinin mevcut güvenlik açıkları kullanılarak potansiyel bir zarara maruz kalması gerekmektedir. Altyapıların korunmasına yönelik dayanıklılık yaklaşımı; yapısal güvenlik açıklarını ve yüksek etkili sistem sorunlarına maruz kalmayı azaltan sağlam ve hataya dayanıklı tasarım ve üretim ile destelenen koruyucu önlemler; önleme, tespit ve ilişkilendirme yetenekleri; olumsuz olayların sonuçlarını hafifletmek ve normal faaliyetleri hızlı bir şekilde eski haline getirebilmek için karşı önlemlerle desteklenen müdahale ve kurtarma operasyonları şeklinde özetlenebilir.

ABD İç Güvenlik Bakanlığı (DHS) Strateji Politikası ve Planlarından Sorumlu Müsteşarı Robert Silvers, Siber güvenlik yöneticileri ve ekiplerinin, iş operasyonlarının ne kadar hızlı geri yüklendiği ve başarılı bir siber saldırının ardından olay müdahale sürecinin

ne kadar sorunsuz ve zamanında olduğu ile giderek daha fazla değerlendirileceğini vurgulamakta ve "şirketler bir siber saldırıya uğrayıp uğramadıklarına göre değil, verdikleri yanıtın karakterine göre değerlendirilir." demektedir (Silvers,2021)

Siber uzayda tam güvenliğe ulaşmak imkânsız olduğu için hedef, kötü amaçlı ya da istem dışı kesintileri öngörme ve bunlardan hızlı bir şekilde kurtulma yeteneği olarak tanımlanabilecek siber dayanıklılığı en üst düzeye çıkarmaya çalışmak olmalıdır (Herrmann ve Pridöhl,2020). Hizmetlerini EKS kullanarak yerine getirmekte olan kritik altyapılarda beklenmeyen bir siber güvenlik olayı sonrasında meydana gelebilecek ve önemli çevre felaketlerine neden olabilecek hasarın kapsamını sınırlamak ve bu siber olayın neden olabileceği hizmet kesintisinin süresini olabildiğince azaltmak ve beklenmeyen siber olayın meydana gelmesinden önceki duruma tam olarak dönülemese de yeni duruma uyum sağlamak ve zaman içinde sistemlerin faaliyetlerinde iyileştirme sağlayabilmek için yani bu sistemlerin dayanıklılığını artırmak üzere aşağıdaki temel faaliyetlerin gerçekleştirilmesi gerekmektedir :

- EKS ağı ve sistemleri için güvenlik ön planda tutularak, aktif bir savunma zihniyeti ve canlı süreçlerde ayarlanabilen esnek bir kontrol sistemi mimarisi kullanılmalıdır (Luallen,2014:26). Bu sistemler, öngörülebilir bir olay boyunca ayakta kalabilecek şekilde tasarlanmalıdır. Gerçekleşme olasılığı düşük ancak çok önemli hasarlar oluşturabilecek durumlara dayanabilmeleri için bu sistemlere tüm yaşam döngüleri boyunca bakım yapılmasını da kapsayacak şekilde gerekli yatırım yapılmalıdır (OECD,2019:79-81). Bir sistem geliştirilirken güvenlik özelliklerinin en son aşamada eklenmesi, bu sistemlerin verimliliğini ve dayanıklılığını olumsuz yönde etkileyen sonuçlara neden olabilecektir. Etkin güvenliğin sağlanması için sistemlerin tasarım aşamasından itibaren kullanışı kolay ve güvenlik özelliklerine sahip olmaları ön planda tutulmalıdır (Smetters, 2014:46-50). Emniyet için teknik sistemlerde, organizasyonda ve işgücünde dayanıklı tasarım kullanılmalıdır (Johnsen vd.,2009:114).

- Meydana gelen bir siber olayı iyi yönetebilmek için bu olay esnasında, sistem yöneticilerinin ve operatörlerin, devam etmekte olan bir saldırıyı engelleyebilmek üzere gerçek zamanlı olarak şüpheli ağ trafiği hakkında saldırı tespit sistemleri, güvenlik duvarları gibi uygulamaların verdikleri gerçek zamanlı uyarılara, bildirimlere veya belgelere

odaklanarak algılama kontrollerini gerçekleştirmeleri gerekmektedir. Sistemlerin topladığı günlük log kayıtları, ağ trafiğini, kullanıcı faaliyetlerini, çalışan programları, değiştirilmiş dosyaları ve işlemi gerçekleştirenleri ele verecek diğer bilgileri içerebilmektedir. Siber olay sonrası gerçekleştirilecek bu kayıtların analizi ile saldırının kapsamı hakkında, yani hangi sistemlerin güvenliğinin ihlal edildiğine dair bilgiler edinilebilecektir (Herrmann ve Pridöhl,2020). Hareket tarzlarının belirlenmesini, hasarın kontrol altına alınmasını ve etkilerini azaltmaya yönelik yapılması gerekenlere öncelik verilmesini ve bu kararların bunları uygulayacak kişilere iletilmesi faaliyetlerini içerir. Bu nitelik teknolojiye değil insana bağlıdır. Hızlı kurtarma, bir felaketten sonra işleri olabildiğince çabuk normale döndürme kapasitesidir. Acil durum ve iş sürekliliği planları, verimli acil durum hizmetleri ve doğru insanları ve kaynakları doğru yerlere ulaştırma araçları çok önemlidir (OECD,2019:79-81). Siber olay esnasında, kuruluş ağının farklı bölümlerinde bulunan cihazların birbirleri ile iletişim kurmasını engelleyen ağ yapılandırması, gerçekleşmiş bir siber olayın etkisini azaltabilecektir (Herrmann ve Pridöhl,2020).

- Bir siber olayın etkilerini en hızlı şekilde devre dışı bırakacak ve sistemin normal çalışma düzenine geçmesini sağlayacak kurtarma faaliyetler gerçekleştirilmelidir. Bu faaliyetlere örnek olarak, sistem yedeklerinin düzenli bir şekilde alınması ve saldırılardan etkilenmeyecek konumlarda tutulması, acil durum planlarının hazırlanmış ve tatbikatlarla test edilmiş olması verilebilir (Herrmann ve Pridöhl,2020). Siber olay sonrası bir daha bu durumla karşılaşmamak için çıkarılabilecek dersler sonrası planların gözden geçirilmesi, prosedürlerin değiştirilmesi ve bir sonraki siber olaydan önce sağlamlığı, beceriyi, kurtarma yeteneklerini geliştirmek için ihtiyaç duyulan yeni araç ve teknolojileri belirlemeyi kapsamaktadır (OECD,2019:79-81). Dayanıklılığı artıracak bir uygulama, olayın etkisini devre dışı bırakacak ve faaliyetine devam edebilecek sağlamlıkta; ortaya çıkacak kriz durumunu ustaca yönetmek üzere yeterli kaynaklara sahip; hizmetleri normal durumuna döndürebilmek için hızlı kurtarma özelliğine sahip ve geçmişte yaşanmış aynı tür olaylardan öğrenilenlerin uyarlanabileceği nitelikte olmalıdır (Bennett, 2018:45).

Sistemlerin emniyeti ve dayanıklılığı da göz önünde bulundurulduğunda, önleyici/koruyucu güvenlik yaklaşımının, bu sistemlerin tasarlanması aşamasından itibaren üretimi, kullanılması ve kullanım dışı kalması aşamalarını kapsayan tüm yaşam döngüsü

boyunca uygulanılması kaçınılmazdır. Bu yaklaşım, operasyonel faaliyetlerin gerçekleştirildiği bireysel ve kurumsal seviyede ele alınması ve uygulanması temel faaliyetleri kapsamaktadır. Bu tarz operasyonel faaliyetlerin gerçekleştirilebilmesi için, gerekli politikaların kurumsal, ulusal ve çoğu durumda da küresel seviyede belirlenmiş ve kabul edilmiş olması ve desteklenmesi şarttır.

3.1.2 Risk Yönetimi Yaklaşımı

Günümüzde çok farklı amaçları gerçekleştirmek üzere kullanılmakta olan bilişim sistemlerinin yazılımları biçimsel mantıklar kullanılarak doğrulanamayacak kadar büyük ve karmaşıktır. Sistemlerin güvenlik açıklarının bulunmadığını belirlemek üzere kullanılmakta olan güvenlik testleri, güvenlik açıkları varsa bu açıkları ortaya çıkarabilirler ancak bu, -hiç güvenlik açığı yoktur anlamına da gelmemektedir. Güvenlik açıklarının bulunmadığını göstermek, kapsamlı testler gerektirmekte olup; sistemin ne yapması gerektiği ve çalışacağı ortamlar hakkında bazı beklentilere göre farklı penetrasyon testleri uygulanmaktadır. Bu durumda koruyucu/önleyici yöntem, belirli varsayımlar çerçevesinde sistemlerin güvenlik açıklarının bulunup bulunmadığını belirleyebilmektedir (Mulligan ve Schneider, 2011:72). Henüz bilinmeyen bir güvenlik açığı o sistemde yer alıyorsa bunun koruyucu önleyici güvenlik yaklaşımı kapsamında ele alınması olasılığı düşüktür. Sistemlerin siber güvenliğinin sağlanabilmesi için farklı yaklaşımlara ihtiyaç vardır.

Kritik altyapılarda kullanılmakta olan EKS'nin BT ve OT'in bir arada kullanılmaya başlanması ve bu sistemlerde yaşanmakta olan başdöndürücü gelişmeler sonucu sistemlerin gittikçe karmaşıklaşması, bağlantıların ve kullanıcıların artması, buna paralel olarak bilgili siber saldırganların sayısının artması gibi nedenlerle bu sistemler için önleyici/koruyucu güvenlik önlemleri yetersiz kalmakta ve mutlak bir siber güvenliğin sağlanması mümkün olamamaktadır.

Sistemlerin tüm güvenlik açıklarının kapatılamayacağı; güvenliğe yapılacak yüksek miktardaki yatırımların sonuçta önlenecek saldırıdan kaynaklanan zarara değmeyeceği; karşılaşılabilecek risklerin oluşturacağı hasarın kurumsal yapıya, verilen hizmetin niteliğine ve hizmetin verildiği hedef kitleye göre de değişebileceği göz önünde bulundurularak risklerin belirlendiği, değerlendirildiği, önemine binaen gerekli önlemlerin alındığı risk yönetimi yaklaşımı kullanılmaya başlanmıştır. Günümüz dünyasında, siber saldırıların

anonimlik ve inkâr edilebilirlik özellikleri bulunmasından, risk ve tehditlerin asimetrik nitelikli olmalarından dolayı da siber güvenliğin sağlanmasındaki muğlaklıklar göz önünde bulundurularak mutlak bir güvenliğin sağlanamayacağından hareketle siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulması hedefine yönelik risk yönetimi yaklaşımı kullanılmaktadır (UDHB,2016: 5).

Günümüz dünyasında pek çok alanda uygulanmakta olan risk yönetimi yaklaşımını daha iyi anlayabilmek için öncelikle riskin tanımına bakmak yerinde olacaktır. Riskin çok farklı tanımlarından birisi, "insanların sahip oldukları değerlerin, insan faaliyetleri veya olayların sonuçları nedeniyle zarar görmesi olasılığı" şeklindedir (Klinke ve Renn, 2002:1071). Bilişim teknolojisinde kullanılan risk kavramı ise, 'henüz tehdide dönüşmemiş ve yönetilmediğinde tehdide dönüşecek bir olgudur (Küçükşahin vd., 2009:15). Bir sisteme, bu sistemde yer alan güvenlik açıklarının kullanılarak zarar verilmesine neden olabilecek tehditlerin bulunması olasılığı da risk olarak tanımlanmaktadır. Risk felaket değil felaket öngörüsü anlamına gelmektedir. Felaketler öngörülüyorsa bu konuda harekete geçme zorunluluğu doğacaktır (Beck, 2011: 357). Riskin 'tam ve net olarak bilinememesi, zamanla değişkenlik göstermesi, olumsuz sonuçlar doğurma olasılığına sahip olması ve yönetilebilir olması' gibi özellikleri bulunmaktadır. (Babuşçu, 2005). Riskler üzerinde algılanabilecek bir aciliyet duygusu yaratmak üzere tehdit terimi kullanılmıştır (Radu,2014:17). Risk, bir tehdidin, bir varlık ya da varlık kümesinde mevcut güvenlik açıklarının istismar etmesi ve bu yolla kritik altyapı sistemlerine zarar vermesi anlamına gelmektedir. NIST dokümanında ise risk, "potansiyel bir durum veya olay tarafından tehdit edilme ölçüsü olup bu durumun meydana gelme olasılığı ve bu durum meydana geldiğinde ortaya çıkacak olumsuz etkilerdir" şeklinde tanımlanmaktadır (NIST SP 800-39).

Risklerin çeşitli denetimlerle azaltılamaması durumunda kritik süreçlerin saldırı yüzeyleri hızla büyümeye devam edeceği için risk yönetimi yapılmalıdır. Risk yönetimi, etkili sonuçlar meydana getirebilecek riskleri kontrol etmede kullanılacak faaliyetlerin ve yöntemlerin ele alınmasıdır (Tabansky, 2017:212). Bir risk yönetim süreci, riskleri belirlemede örgüt seviyesi, görev/iş süreçleri seviyesi ve bilişim sistemleri seviyesi olmak üzere üç seviyede gerçekleştirilebilir. Risk yönetim sürecinin, kapsamın belirlenmesi, değerlendirme, çözüm bulma ve takip etme olmak üzere süreklilik arz eden aşamaları vardır.

Bu aşamalar bilgi güvenliğinden, fiziki güvenlikten, emniyet ve finanstan kaynaklandığına bakılmaksızın tüm riskler için uygulanmalıdır (NIST SP 800-82r2, 2015:3.2).

Risk yönetim süreci, ISO 27001 Standardında ise yine birbirini takip eden ve sürekli uygulanması gereken "Planla, Uygula Kontrol Et, Önlem Al" aşamalarından oluşmaktadır.

Risk yönetimi yaklaşımına göre, kritik altyapıların güvenlik açıklarının analiz edilmesi ve uygun güvenlik önlemlerinin uygulanması ile siber güvenlik olayı meydana gelme riski azaltılabilecektir. Başarılı bir risk yönetimi için, saldırı tehdidinin ciddiyetinin farkında olmak ve saldırganların yüksek motivasyonlu, konu ile ilgili yeterli donanıma sahip oldukları ve saldırıda bulundukları kritik altyapılara zarar verebilecek nitelikte oldukları kabul edilmelidir. Bu sürecin bir parçası olarak tehditlerin belirlenmesi ve risk değerlendirmesi faaliyetleri uygulanmalıdır. Bu adımlar bir kez tamamlandığında, risk azaltma metodolojilerine uygun güvenlik önlemleri geliştirilmiş ve uygulanmış olmaktadır. Etkili olduklarından emin olmak için, kritik altyapı varlıklarının tanımlanması, bu varlıkların kurum açısından değerlerinin belirlenmesi, bu varlıklara yönelik tehditlerin ve güvenlik açıklarının belirlenmesi, risk analizinin yapılması, güvenlik açıklarından kaynaklanabilecek risk olasılıklarını azaltmak amacı ile uygulanabilecek önlemlerin işleme konulması ve riskin yeniden değerlendirilmesi aşamalarından oluşan risk yönetimi döngüsü belirli aralıklarla yinelenmelidir.

Riskin üç temel bileşeni, kritik bir varlığa yönelik tehdit bulunması, bu tehdide karşı kritik altyapının savunmasız olması, yani güvenlik açıklarının bulunması ve bu tehditin kritik varlık üzerinde olumsuz bir etki meydana getirebilme olasılığının bulunmasıdır. Bu bileşenlerden hareketle risk aşağıdaki şekilde formüle edilmiştir (Bennett-2018: 204):

Risk = Güvenlik açığı * (Tehdit * Sonuç)

Bu formülde, "Tehdit" bir siber güvenlik olayının gerçekleşme olasılığını; "Sonuç", siber güvenlik olayının gerçekleşmesi durumunda kritik varlığın uğradığı hasarın derecesini göstermektedir. "Güvenlik açığı", saptanmış olan güvenlik açığının önlenmesine yönelik alınmış güvenlik önleminin etkisini gösterecek şekilde belirlenmektedir. Güvenlik açığını gidermek üzere alınan önlemin etkisi yüksek ise, güvenlik açığı da buna bağlı olarak düşük olacaktır. Siber güvenlik olayının meydana gelme olasılığı ve siber güvenlik olayının meydana gelmesi durumunda kritik sistemde oluşturabileceği hasarla birleştirilerek genel

risk derecesi hesaplanmaktadır. Risk, EKS'ne, bu sistemde yer alan güvenlik açıklarının kullanılarak sistemin gizliliği, bütünlüğü ve kullanılabilirliğini bozmaya yönelik olumsuz etki yaratma potansiyeline sahip tehditlerin gerçekleşme olasılığıdır.

EKS'nin siber güvenliğinin sağlanmasına yönelik risk yönetimi faaliyetleri, EKS'nin yaşam döngüsünün tasarım, geliştirme, işletim ve bakım da dâhil olmak üzere her aşamasında gerçekleştirilmelidir. Bir risk yönetim süreci, riskleri belirlemede kurumsal seviye, görev/iş süreçleri seviyesi ve bilişim sistemleri seviyesi olmak üzere üç seviyede gerçekleştirilebilir. Kritik altyapıların siber güvenliğinin sağlanması için uygulanmakta olan risk yönetimi sürecinin kapsam belirleme, risk değerlendirme, çözüm bulma ve takipten oluşan bileşenleri, bu altyapıya yönelik bilgi güvenliği, fiziki güvenlik, emniyet ve finans gibi tüm risk alanları için uygulanmalıdır (NIST SP 800-82r2, 2015:3.2).

Siber güvenlik çalışmaları için en baştan başlanması ve tekerleğin yeniden icat edilmesi yerine var olan kaynaklardan ve deneyimlerden yararlanmak daha anlamlı olacaktır. Geleneksel bilişim sistemlerinin siber güvenliğinin sağlanmasına yönelik uzun yıllardır kullanılmakta olan ve iyi bilinen risk yönetimi yöntemleri, kritik altyapıların güvenlik açıkları ve istismara neden olabilecek tehditlerin olumsuz etkisini azaltmak için kullanılabilmektedir. Bu amaçla geleneksel bilişim sistemlerinin siber güvenliğinin sağlanmasına yönelik ISO 27000 serisinin yanı sıra ISA-62443-2-1 (99.02.01)-2009 Siber Güvenlik Yönetim Sistemi Standardı ile NIST SP 800-39 Bütünleşik Kurumsal Risk Yönetimi Standardı gibi standartlardan da sıklıkla yararlanılmaktadır.

3.1.2.1 Risk Analizi

Kritik altyapıların korunması sürecinda kasıtlı siber saldırılar, doğal afetler ve kazalar gibi istenmeyen olaylardan kaynaklanabilecek siber güvenlik olaylarının meydana getirebilecekleri hasarı en aza indirgemek üzere gerçekleştirilen adımlardan biri **risk analizidir**. Kritik altyapı sistemlerinin emniyeti ve güvenliğini sağlamada risk etkilerini azaltmak üzere risk analizi teknikleri yaygın olarak kullanılmaktadır (Radulescu,2020:24). Risk analizi ile kritik altyapılara yönelik siber güvenlik olaylarının meydana gelmesine neden olabilecek güvenlik açıklarının belirlenmesi ve meydana gelebilecek siber güvenlik olaylarının etkisinin tahmin edilmesi hedeflenmektedir. Bu süreçte, öncelikle olası tehdit stratejileri, güvenilir senaryolar kullanılarak tanımlanmalı; kritik altyapılarla ilgili tüm

varlıkların mevcut riskleri değerlendirilmeli ve güvenlik açıkları ve dolayısıyla riskler azaltılarak bu sistemleri korumak için mevcut güvenlik önlemleri gözden geçirilerek güvenlik önlemleri alınmalıdır. Kritik altyapılarda mevcut güvenlik önlemlerinin istenmeyen olayları önleme kabiliyeti bir siber olayın başlamadan önce örneğin bir siber saldırının aktif hale gelmesi öncesinde tespit edilme yeteneği sistemin etkinliği açısından değerlendirilmelidir.

3.1.2.2 Risk Minimizasyonu

Kritik altyapılara yönelik olası tüm tehditlere karşı her zaman tam koruma sağlayan mutlak güvenlik diye bir şey yoktur. Kimi durumlarda güvenlik önlemi, karşılanamayacak seviyede çok yüksek maliyet gerektirebilir ya da alınacak güvenlik önlemi, hizmetin yerine getirebilmesine engel olabilir. Risk yönetimi sürecinin amacı, tüm riskleri ortadan kaldırmak değil, bir siber güvenlik olayına neden olabilecek riski kabul edilebilir bir seviyede, kabul edilebilir bir maliyetle, kabul edilebilir sınırlar içinde yönetmektir. Bu teknik, risk minimizasyonu olarak bilinir. Alınan risk karşılığında elde edilebilir olarak algılanan avantaj daha fazla ise bu kabul edilebilir risktir. Ancak kimi durumlarda bireyler ve toplumlar için kabul edilemeyecek ölçüde ciddi risk oluşturma olasılıkları yüksek olan tehditler vardır. Eğer kritik sisteme yönelik siber güvenlik olayı sonucunda meydana gelecek zarar insanlar ve diğer varlıklar açısından olumsuz sonuçlar doğurabilecek nitelikte ise bu risk önlenmesi gereken bir risk olarak kabul edilmelidir (Bennett,2018:206). Bu riskler, kabul edilemez risk olarak adlandırılmaktadır. Kabul edilemez riskler, risk seviyesi kabul edilebilir hale gelene kadar ek risk azaltma önlemleri uygulanarak tehdidin oluşturduğu olumsuz etkilerin azaltılmasına çalışılmalıdır.

3.1.2.3 Risk Değerlendirmesi

Risk değerlendirmesi, bilgi sistemi kullanılmasından kaynaklanan kurumsal operasyonlara, misyon, işlevler, imaj, itibar gibi kurumsal varlıklara, bireylere ve/veya kuruluşlara yönelik risklerin belirlenmesi anlamına gelmektedir (NIST,2012). Daha geniş anlamı ile, sistem kaynaklarına yönelik potansiyel güvenlik açıklarını ve bu kaynaklara yönelik tehditleri tanımlayan, kayıp maruziyetlerini ve bunların meydana gelme olasılığına göre sonuçlarını ölçen ve (isteğe bağlı olarak) toplam maruziyeti en aza indirmek için kaynakların karşı önlemlere nasıl tahsis edileceğini öneren süreçtir (ISA-62443-1-1,2007).

Sisteminin işleyişinden kaynaklanan, kurumsal işlemlere (misyon, işlevler, imaj ve itibar dahil), kurumsal varlıklara, bireylere, diğer kuruluşlara ve ulusa yönelik risklerin belirlenmesi sürecidir (NIST SP 800-39). Bu süreç ile güvenlik açıklarının belirlenmesi ve bu açıkların istismar edilmesi olasılığının hesaplanması için gerekli kaynakların en etkin biçimde dağılımı ile faaliyetlerin belirlenmesinde yardımcı olur. Risk değerlendirmesi yapılırken tehditlerin ve güvenlik açıklarının gözden geçirilmesi, kritik altyapı sektörlerinin temel bileşeni haline gelmiş olan EKS'ne yönelik olarak gerçekleşebilecek siber güvenlik olaylarını engellemek ya da meydana gelebilecek hasarı minimuma indirmek için gereken önlemlerin alınmasında yardımcı olabilecektir.

Bir risk değerlendirmesi, bir siber olayın olasılıklarını belirlemeye ve bir olayın olasılığını ve sonuçlarını azaltmak için hafifletici eylemlerin belirlenmesine yardımcı olmalıdır. Böylece bir risk değerlendirmesi maliyetlere ve faydalara dayalı olarak azaltıcı eylemlerin önceliklendirilmesi için önemli bir araçtır. "Black Swan" gibi büyük bir siber güvenlik olayını önleyebildiği ya da en azından olumsuz etkisinin azaltılabildiği durumda, SCADA sistemlerinin risk değerlendirmesini gerçekleştirmek için harcanan çabanın belirgin bir karşılığı vardır (Johnsen,2013:288). Bu güvenlik açıkları ve SCADA sistemlerinin kritikliği, hem bilinen güvenlik açıklarını azaltmak hem de sistemin kabul edilebilir davranış sınırları dışındaki sapmaları işleme yeteneğini geliştirmek için kapsamlı bir risk değerlendirmesine dahil edilmelidir. Ayrıca, sektördeki düzenleyiciler ve yetkililer arasındaki temel zorluklara ilişkin farkındalığı ve bilgiyi geliştirmek için tüm olaylar raporlanmalı ve paylaşılmalıdır (Johnsen,2013:288).

Siber güvenlik olayları örneklerinde de görüldüğü gibi, SCADA sistemlerin kontrol ve takip işlevlerini yerine getirememesi nedeniyle olumsuz sonuçlar yaşanmıştır. Siber olayın izlenmesi ve SCADA sisteminin dayanıklı olması ve beklenmeyen durumlarda bile çalışmaya devam edebilmesi risk yönetimine dahil edilmelidir (Johnsen,2013:289).

Kritik altyapıların siber güvenliğini sağlamakta çoğu kez önleyici/koruyucu güvenlik yaklaşımı ile birlikte kullanılmakta olan risk yönetimi yaklaşımı, bireysel ve kurumsal seviyede operasyonel faaliyetler gerçekleştirilirken uygulanmakta, ulusal seviyede ise bu yaklaşıma yönelik politikalar oluşturulmakta ve kullanımları desteklenmektedir.

3.2 BİREYSEL SİBER GÜVENLİK FAALİYETLERİ

Kritik altyapıların siber güvenliğinin bu sistemlerin doğrudan tasarlandığı, üretildiği, kullanıldığı ve kullanım dışı bırakıldığı operasyonel seviyede sağlanmasında bireylerin rolü çok önemlidir. Bu kısımda, öncelikle kurumsal bir yapı içinde personelin sistemin güvenliğini sahiplenmesi ve gereken faaliyetleri yerine getirmesi için alınabilecek önlemlere değinilecek daha sonra da bireysel etik davranışın önemi üzerinde durulacaktır.

3.2.1 Personel ile İlgili Siber Güvenlik Önlemleri

İşlevlerini yerine getiremedikleri ya da yanlış sonuçlar ürettikleri durumlarda toplumsal kaos, can ve mal kaybına neden olabilecek kritik altyapı sistemleri siber uzaya dahil olmaya başladıkları için siber güvenlik olaylarından etkilenebilir duruma gelmiştir. Bu sistemlerin çalıştırılması ve siber güvenliğinin sağlanması görevlerini yerine getirmekte olan personelden kaynaklanabilecek güvenlik açıklarını en aza indirgeyebilmek için personele yönelik birtakım güvenlik önlemlerinin alınmasının yerinde olacağı değerlendirilmektedir. Her geçen gün yenileri ortaya çıkmakta olan siber güvenlik riskleri ve güvenlik açıkları paralelinde alınacak önlemlerin de sıklıkla değiştiği ve geliştiği günümüz dünyasında güvenlik alanında çalışan personel tarafından uygulanabilecek önlemlerden başlıcaları aşağıda yer almaktadır:

3.2.1.1 İşe Alım Sürecinde ve İşin Yaptırılması Sürecinde Güvenliğin Dikkate Alınması

Personelin işe alınması sürecinde güvenlik alanındaki becerileri ve nitelikleri de dikkate alınmalıdır. Kurallara uymayan ve işi ne pahasına olursa olsun yapmak isteyen personelin güvenlik süreçlerine bağlı kalmama olasılığı vardır. Bireylerin sadece yerine getirmesi gereken görevi bilmesi yeterli değildir. Bu görevi yapmaya istekli ve yetenekli olmalıdırlar (Bridges,2013:82). Sistemi işletmek, sürdürmek veya yönetmek için uygun niteliklere sahip bireyler seçilmeli ve bu bireylerin gerekli becerilerini geliştirmek ve sürdürmek için gereken eğitimler yeterli seviyede sağlanmalıdır.

Personel seçiminde çalışanın işyerine sadakati de göz önünde bulundurulmalıdır. Güvenlik birimi, kuruma karşı aidiyet duygusunu ve motivasyonunu kaybetmiş personelin tespitine yönelik çalışmalar yapmalı; risk değerlendirme ve eylem planlarında bu durumu

göz önünde bulundurmalıdır. Kritik altyapı tesislerinde çalışacak personelin diğer becerilerinin yanı sıra güvenlikle ilgili niteliklerinin de yapacağı iş açısından kritik öneme sahip olduğu unutulmamalıdır. Bu personel özellikle siber güvenlik uzmanı olarak çalışacaksa teknik becerileri uygulamaya ek olarak bir ekip içinde iyi çalışma, etkili kararlar alma, bilgileri uygun şekilde kullanma ve ortaya çıkan sorunlara hızla yanıt verme becerilerine de sahip olmalıdır.

Kuruluş içinden gelen siber güvenlik tehditlerinde insan müdahalesi önemlidir (Bridges,2013:91). Güvenlik uygulamaları kullanılarak verilerin izlenmesi yolu ile çalışanların potansiyel şüpheli davranışları algılanabilmektedir ancak bu bilgilerin insan kaynakları ve iş arkadaşları tarafından dile getirilen endişeler ile birlikte yorumlanması gerekmektedir. Kimi durumlarda sadece veri izleme yapılması yanlış alarmlara yol açabilecektir. Bu nedenle, davranışı veri izleme yazılımından bir alarm tetikleyen herhangi bir kişiyle etkileşime geçmek için insan müdahalesine ihtiyaç vardır. Bu müdahale, personele kendi işverenleri tarafından güvenilmediklerini hissettirmeyecek, gereken incelikle durumu yönetebilecek bir görevli tarafından gerçekleştirilmelidir.

3.2.1.2 Sistem Tasarımı

Kritik altyapıların faaliyetlerini gerçekleştirmesinde kullanılan EKS'nin tasarlanması aşamasından itibaren her geçen gün yenileri ortaya çıkmakta olan siber güvenlik riskleri değerlendirilmeli ve gerekçelendirilmelidir. Sistemin nasıl istismar edilebileceği ayrıntılı olarak incelenmelidir. Güvenlik tasarımı, uygulamanın sadece uygun ortamda işi bilen kullanıcılar için değil her türlü hatalı kullanımı ve kötü niyetli kullanımı olasılıkları da göz önünde bulundurularak yapılmalıdır. Sömürüldüğünde önemli zararlara neden olabilecek ağa bağlı programlar ve kablosuz cihazlar için, son kullanıcı eğitimi ve güvenli ve güvenli çalışma talimatı dahil olmak üzere ek / yükseltilmiş güvenlik önlemleri alınmalıdır. Bu sistemlerin güvenliği konusunda çalışmakta olan profesyoneller, görevleri ile ilgili riskleri anlayabilecek etik kaygılara sahip olmalıdır (Vallor&Rewak,2018:19).

Sistemler tasarlanırken sağlam ve kullanılabilir olmasına önem verilmelidir. Bu tarz sistemler için sağlamlık birincil husus olmalıdır. Sistemin amacına uygun çalışmasını sağlamak için gerekli özen gösterilmeli ve kaynakları kazara ve kasıtlı kötüye kullanım, değişiklik ve hizmet reddine karşı güvence altına almak için uygun eylem

gerçekleştirilmelidir. Sistemin amacına uygun çalışmasını sağlamak için güvenlik özellikleri mümkün olduğunca sezgisel ve kullanımı kolay olacak şekilde tasarlanmalıdır. Bilişim personeli, çok kafa karıştırıcı, duruma göre uygunsuz veya başka bir şekilde meşru kullanımı engelleyen güvenlik önlemlerinin olumsuz etkileri konusunda gerekli bilgilendirmeyi yapmalıdır. Kullanıma girdikten sonra ortaya çıkabilecek tehditleri de dikkate almak üzere izleme, yama uygulama ve güvenlik açığı raporlama gibi teknikler ve ilkeler de sisteme entegre edilmelidir (ACM,2018).

Hassas verilerin güvenli bir şekilde saklanması ve iletilmesine yönelik tasarımlar yapılmalı ve uygulanmalıdır. Veri sahiplerine ve bu verilerin kullanıcılarına şifreleme, anahtar yönetimi ve veri depolama uygulamaları hakkında açık ve doğru bilgi verilmelidir. Üçüncü taraflarla (şifreleme araçları, güvenlik denetimleri, bulut hizmetleri veya fiziksel sunucular, vb.) sözleşme yaparken, bu sistemlerin kullanıldığı her ortam için güvenilirlik hususunda gerekli özen gösterilmelidir. Kullanılabilecek şifreleme tekniklerinin güçlü yönleri, riskler ve faydaları göz önünde bulundurulmalıdır. Şifreleme uygulamalarının endüstri standartlarına uyup uymadığı, bu standartların yeterli olup olmadığı gözden geçirilmelidir. Şifreleme uygulamalarını zayıflatmak veya belirli cihazların şifresini çözmek için kolluk veya istihbarat kurumlarından gelen taleplere nasıl cevap verileceği ile ilgili politikalar belirlenmiş olmalı ve bu politikalar, tüm paydaşlar tarafından bilinmelidir. Saklanmakta olan verilerin tüm yaşam döngüsü için uçtan uca bir güvenlik planı hazırlanmalı ve bu plan belirli aralıklarla güncellenmelidir.

Gizlilik ve güvenlik hedeflerinin teşviki için sistem tasarımı, yazılım, donanım ve ağları içeren teknik tasarımın yanı sıra gruplar, politikalar, prosedürler, teşvikler, kaynak tahsisleri, yöntemler gibi alanlarda uygulanacak sosyal ve organizasyonel tasarımı da kapsamalıdır. Belirli bir görevde, verimli çalışılabilecek sürenin yanı sıra genel mesai ve vardiya uzunluklarının belirlenmesi yolu ile operatörün tetikte kalma, hızlı yanıt verme ve etkili kararlar alma becerisi geliştirilmelidir (Bridges,2013:82-84). Sistem tasarımının nasıl yapılması gerektiği, bağlama göre farklılıklar gösterebilmektedir. Burada asıl sorun, gizlilik ve güvenlik değerlerinin proje tasarımı, planlama, yürütme ve gözetimin diğer proje hedefleriyle birlikte ön sıralarda yer alması ve sıradan bir uygulama muamelesi görmemesidir (Vallor, Rewak,2018:52).

Sistemlerdeki arayüz değişiklikleri, bazı özelliklerin kaldırılması ve hatta yazılım güncellemeleri, kullanıcıların üretkenliği ve çalışmalarının kalitesi üzerinde bir etkiye sahiptir. Çalışanların ya da kullanıcıların hâlâ kullanmakta olduğu sistem özellikleri için desteğin sonlandırılması ya da değiştirilmesi işlemi dikkatli bir şekilde yapılmalıdır. Eski bir sistemin desteğini sonlandırmak gerekiyorsa uygun alternatifleri kapsamlı bir şekilde araştırmalıdır. Uygulamayı geliştiren bilişim uzmanları, kabul edilemez ölçüde riskli veya pratik olmayan alternatiflere geçişte paydaşların isteklerini ve ihtiyaçlarını göz önünde bulundurmalıdır. Kullanıcılar, destek sona ermeden çok önce desteklenmeyen sistemin sürekli kullanımının riskleri konusunda bilgilendirilmelidir (ACM).

3.2.1.3 Gereksinimlerin Belirlenmesi ve Uygun Kaynak Tahsisi

Kritik altyapıların amaçlarına uygun çalışmasını sağlamak üzere etkili bir güvenlik sistemi oluşturmak için hangi seviyede güvenliğin gerekli olduğu açıkça tanımlamalıdır. Sisteme dahil olan kişilerin, sistemi uygun şekilde kullanabilmeleri, süreçlere bağlı kalmaya istekli olmaları ve onlardan ne beklendiğini bilmeleri gerekir. Yönetim tarafından kabul edilen bu güvenlik hedefleri, sistemlerin çalışanlarına ve kullanıcılarına açık bir şekilde iletilmelidir. Sistemler sürekli takip edilerek hatalı tasarım ve süreçler belirlenmelidir. Güvenlik sistemini oluşturan teknolojilerin ve süreçlerin insan üzerindeki etkisi tam olarak hesaba katılmalıdır. Sistem tasarımı kullanıcılara uygun yapılmış olmalı, çalışanlar da sistemin çalışması için nelerin gerekli olduğunu bilmelidir.

Sistemlerin siber güvenliğine yönelik ihtiyaçların belirlenmesi ve risk yönetimi aşamalarında, farklı bakış açılarını gündeme getirebilecek çeşitli temsilciler de çalışmaya dahil edilmelidir. Bir siber güvenlik uygulamasının farklı kesimler tarafından nasıl algılanacağı veya nasıl etkilenebileceği iyi tahmin edilemezse, ihtiyaçlar sağlıklı bir şekilde belirlenemeyecek, siber güvenlik uygulamalarının çoğu başarılı bir şekilde gerçekleştirilemeyecektir. Siber güvenlik alanında görev yapmakta olan farklı niteliklere sahip güvenlik kuruluşları ve ekiplerinin yanı sıra, uygulamadan etkilenebilecek kesimlerin de temsil edilmesi gereksinimlerin doğru belirlenmesi yolu ile uygulamanın başarı oranını artırabilecek ve daha verimli sonuçlara ulaşılmasına imkân sağlayacaktır.

Güvenliği artırmak üzere tüm sistemi kapsayacak güvenlik önlemleri almak yerine, gerçek anlamda güvenlik ihtiyacı olan alt sistemlerin belirlenmesi ve sadece onlara özgü

güvenlik kontrolleri oluşturulması kritik altyapı sistemlerinin bir bütün olarak erişilebilir olmasına engel olmayacaktır.

Siber güvenlik çalışmalarında zaman, para ve uzmanlık gibi önemli bireysel ve kurumsal kaynaklara ihtiyaç vardır. Siber güvenliğe yönelik önlem alma çalışmaları kimi durumlarda sistemin kullanılabilirliğini ve güvenilirliğini olumsuz yönde etkileyebilmektedir. Gereğinden fazla güvenlik önlemi alınan sistemlerin kullanımı ve asıl görevlerini yerine getirmeleri zorlaşabilmektedir. Siber güvenliği sağlamak üzere belirlenmiş kısıtlamalar, iş süreçlerini kabul edilebilir seviyede engelliyor olmalıdır. Etkili bir güvenlik sistemi, kuruluşun asıl faaliyetlerini yerine getirmesine engel olmamalıdır. Kimi durumlarda da güvenlik önlemleri için haddinden fazla harcama yapılabilmektedir. Bu da son dönemlerde önemli tartışma konularından biri haline gelmiştir. Kaynakların siber güvenlik için tahsisi kararı verilirken, zararlar, faydalar, haklar ve değerler üzerine dikkatlice düşünülmelidir.

3.2.1.4 Personelin Eğitime Tabi Tutulması-Tatbikatlara Katılımının Sağlanması

Siber güvenlik stratejileri ve gelişim planları bu sistemlerin kullanıcılarının teknik bilgilerinin sürekli iyileştirilmesini ve yenilenmesini öngörmektedir. Kurum çalışanlarının davranış şekillerini geliştirmelerinin ve iyileştirmenin ön koşulu geçmiş deneyimlerini kullanarak sürekli öğrenme modunda olmalarıdır (Rajamaki, 2017:248). Çalışanların tehdidi tehdit olmayan durumlardan ayırt edebilmeleri için eğitilmeleri gereklidir. Personelin belirli aralıklarla bu tarz tehditlere maruz bırakılması farkındalığı artıracak ve performans ölçümleri yapılabilecektir.

Bir kuruluşun sistemine bir Truva atı virüsü yerleştirmek için e-postaların kullanılması gibi saldırı durumlarında, personelinin tehdit algılama performansı ölçülmeli ve değerlendirmelidir. Bazı kötü amaçlı yazılımlar otomatik algoritmalar tarafından algılanabilse de daha karmaşık saldırıları tespit etmek için yine de insan kontrolüne ihtiyaç vardır. Genelde kuruluşlar, çalışan personeline yeterli eğitimi vermediği ve teste tabi tutmadığı için bireyler de tehdit e-postalarını belirleme yeteneğine sahip olmayabilmektedir.

Çalışanların siber saldırılara karşı hazırlıklı olması, tatbikatlarla bu hazır olma durumunun pekiştirilmiş olması gerekmektedir. Daha önce provası yapılmamış bir siber

saldırı durumunda kuruluşta kimin hangi görevi yapacağı iyice belirsiz duruma gelecek, panik ve kargaşa yaşanabilecek, önemli kayıplar ve hasar meydana gelebilecek sistemlerin siber olay öncesi duruma getirilmesi çok uzun zaman alabilecektir. Sistemin güvenliğinden sorumlu birim, kuruluşu önemli bir saldırıdan korumaya çalışırken yardım isteyenlerin telefon ve mesajları ayrı bir yoğunluk yaşanmasına neden olabilecektir.

Kuruluşların bir siber tehdit alarmını oluşturmak için kullanılacak sisteme, personelin nasıl yanıt vermesi gerektiği de net bir şekilde tanımlanmış olmalı ve personel bu konuda eğitilmiş olmalıdır. EKS'nin normal faaliyetini sürdürebilmesi için operatöre yüklenen sorumluluk iyi anlatılmış olmalıdır. Yine de personel umulan şekilde davranmayabilir. Siber olay esnasındaki kafa karışıklığı, belirsizlik hesaba katılmalıdır. Siber güvenlik olayının dışarıdan bir saldırı mı olduğu, kurum içinden mi başlatıldığı, gibi cevabı net olmayan sorular belirsizlik ve güvensizlik oluşturabileceği için durumun yönetilmesinde liderlik önemlidir (Bridges,2013:91).

Kuruluşlar bir siber saldırı için nadiren düzenli testler veya provalar yaparlar. Çalışanların davranışlarının düzenli olarak test edilmesini sağlayacak sistemler mevcut değildir. Personel, programları e-posta eklerine veya bağlantılarına yerleştirmek gibi saldırganların kullanabileceği çeşitli yaklaşımların farkında olmalıdır. Bazı saldırı e-postaları otomatik algılama programları tarafından alınabilirken, daha karmaşık saldırılar, bir insanın normal ticari faaliyetlerle bağlantılı tehdit oluşturmayan e-postaları tehdit oluşturanlarla tanımlamasını gerektirir. Bireyler şüpheli işaretleri aramak için eğitilebilir. Bu görevde etkili olabilmek için, bireylere tehdidin nasıl görünebileceği konusunda düzenli olarak hatırlatılması ve onu doğru bir şekilde tespit etmede performans hakkında geri bildirim alması gerekir. Personel kurslara, eğitimini aldıkları becerileri uygulayabileceklerinden emin oluncaya kadar devam etmeleri durumunda, işyerinde kabul edilebilir standartlarda performans gösterebilecektir.

Güvenlik politikaları, statik bir süreç değildir; farklı tutum ve davranışlara sahip yeni personelin göreve başlaması, iş gereksinimlerindeki değişiklikler ve yeni tehditlerin ortaya çıkması gibi durumlarda, kullanımda olan güvenlik teknolojileri ve güvenlik süreçleri de geliştirilmeli, dinamik bir yaklaşım benimsenmelidir.

3.2.1.5 Personelde Güvenlik Kültürünün Oluşturulması

Bir sistemi korumak için gereken güvenlik düzeyi, personelin önemli ölçüde ek çaba göstermesini gerektiriyorsa, bu sürecin öneminin tüm personele iyi anlatılmış olması, kurum içinde güvenlik kültürünün oluşturulması gerekmektedir. Kritik altyapı kuruluşlarının yöneticileri güvenlik hedeflerini belirlemiş olmalı ve belirli aralıklarla gözden geçirmelidir. Güvenlik hedefleri açık politika ve prosedürlerle desteklenmelidir. Üst düzey yöneticiler, temel iş ölçütleri olarak belirli güvenlik performansı ölçütlerine sahip olarak ve astlarına güvenlik hakkında sorular sorarak bunları pekiştirmeli, güvenlik süreçlerini kendileri takip etmeli; kişisel cihazlar, hassas belgeleri şifrelemeden taşınmamalıdır (Bridges,2013:92-93).

Kuruluşun uluslararası standartlara uygun güvenlik kültürünün oluşturulmasına önem verilmelidir. Periyodik güvenlik kontrolleri yapılarak üst yönetime raporlanmalıdır. Siber güvenlik olaylarının olası sonuçlarına dikkat çekilerek, yönetimin siber güvenlik önlemlerini geliştirmesi teşvik edilmelidir. Kritik altyapı tesislerinde faaliyet göstermekte olan en üst seviyedeki yöneticilerden, uygulamayı tasarlayan, geliştiren ve kullanmakta olan çalışanlara kadar tüm personel güvenlik için gerekli davranışların nasıl olması gerektiği konusunda bilinçlendirilmelidir. Bu kapsamda yöneticiler, personelin görevlerini güvenlik kurallarına uygun olarak yerine getirmek üzere motive edilmesi ve gerekli şekilde eğitilmesini sağlamalıdır. Yöneticilerin güvenliğe önem vermesi durumunda, personelin de asıl görevini yerine getirirken güvenliğin sağlanmasına yönelik çabalarını artıracağı değerlendirilmektedir (Bridges,2013:99)

Personel, kuruluşun siber güvenliğinin sağlanmasında kendi rolünün gerçek anlamda farkında olmalı, yöneticilerin siber güvenliğe önem vermelerinin nedenini gerçek anlamda algılamış olmalıdır. Gerekli gördüğü durumda yetkilileri potansiyel sorunlara karşı açık ya da gizlice uyarabilmelidir. Personel, siber güvenlik konusunda endişeleri olduğunda kiminle konuşması gerektiğini biliyor olmalıdır. Etkili bir güvenlik kültürü oluşturmak, bir BT güvenlik politikası, kontrollü erişim veya bir güvenlik duvarı gibi güvenlikle ilgili süreçleri veya yapay öğeleri devreye sokmak gibi faaliyetlere ek olarak personelin siber güvenliği destekleyici varsayımlara, değerlere ve tutumlara, sahip olmasını gerektirir.

Siber güvenlik testleri yapmakta olan personel, daha önce bilinmeyen güvenlik teknikleri, araçları veya güvenlik açıkları hakkında yayınladıkları bilgilerin kötü niyetli

kullanımını önleyebilmek amacı ile gerekli önlemleri alabilmeli, etik davranış ilkelerini benimsemiş olmalıdır. Güvenlik araştırma ve testlerinde görevli personeli etik davranışlar sergilemeye teşvik edici uygulamalar geliştirilmelidir.

3.2.1.6 Siber Olaylara Müdahale Planlarının Yapılması ve Bu Planlara Uyum

Karşılaşılabilecek her tehdit veya siber güvenlik olayı için uygun bir olay müdahale planı hazırlanmış olmalıdır. Bu müdahale planları, bir siber güvenlik ihlalini ya da siber saldırıyı önlemeye yönelik önlemlerin yetersiz kalması durumunda, diğerlerine yönelik zararları sınırlamak veya sorunu gidermek için azaltma stratejileri de dahil olmak üzere en kötü senaryolar için somut eylem planlarını içeriyor olmalıdır. Siber Olay müdahale planlarının başarıyla uygulanabilmesi için gerekli ve yeterli kaynağın ve sistemin mevcudiyetini sağlayacak çalışmalar yapılmış olmalıdır. Müdahale planları, gerçekte yapılabilecek ve yapmaya hazır olunan müdahaleleri kapsamalıdır; bir tehdit veya güvenlik ihlaline yanıt olarak ne yapılmak istendiğini tam olarak yansıtabilmelidir. Gerçekçi müdahale planı ile yapılması arzu edilen müdahale planı arasındaki boşluk etik olarak kabul edilebilir seviyede olmalıdır. Siber olay müdahale uygulamasında, karşılaşılan etik gri alanlar iyi belirlenmelidir. Saldırıları bertaraf etmek ve caydırmak konusunda nelerin yapılabileceği iyi değerlendirilmiş olmalıdır. Müdahale ve karşılık vermede etik çizgi iyi belirlenmeli; masum taraflara "teminat hasarı" veya kendimize ve kuruluşumuza itibar zararı riskleri göz önünde bulundurulmalıdır.

Sistem kullanıcılarının ve diğer paydaşların ihlaller ve güvenlik açıkları da dahil olmak üzere ne zaman ve nasıl bilgilendirileceği konusunda etik olarak sağlam bir plana sahip olunmalıdır. Bir bildirim gecikmesini veya seçici olan ve herkese açık olmayan bir bildirim hakkında ilgililer bilgilendirilmiş olmalıdır. Doğru, zamanında ve yardımcı raporlama ihtiyacının karşılanıp karşılanmadığı dikkate alınmalıdır. Bir siber güvenlik olayına etkili bir müdahalenin hızlı bir şekilde gerçekleştirilebilmesini sağlamak üzere etkin bir sistemin varlığı veya müdahalenin gerçekte ne olduğu ve ne yapılması gerektiği konusunda araştırma ve planlamada iç karışıklık, düzensizlik ve anlaşmazlık nedeniyle yavaşlama söz konusu olmamalıdır. Etkilenen paydaşlara nasıl daha fazla bilgi ve yardım alabileceklerini veya kendilerini daha fazla zarar riskinden korumak için ne gibi önlemler almaları gerektiğini bildirmek için gerekli protokoller yapılmış olmalıdır. Müdahalede

sadece siber güvenlik ekibinin bakış açısı değil, diğer paydaşların muhtemel bakış açısını da dikkate alınmış olmalıdır. Etik açıdan tutarlı risk değerlendirmesi yapılmış olduğu düşünülse bile, paydaşların verilmekte olan hizmetlere, ürünlere veya kuruluş değerlerine güvenini sarsabilecek bir ihlal veya güvenlik açığına ilişkin gecikme veya anormal durum olup olmayacağı gözden geçirilmelidir.

Önemli görevleri bulunan endüstriyel kontrol sistemlerinin yazılım, donanım, ağ bileşenleri ve bu sistemler üzerinde tutulmakta, işletilmekte iletilmekte olan veriler, bu sistemlerin tüm yaşam döngüleri boyunca olduğu gibi kullanım dışı kaldıklarında da ne olacakları hususu düşünülmelidir. Bir ürün kullanıma sunulmadan önce kapsamlı güvenlik testleri ve denetimi yapılmış olsa da her zaman yeni tehditler, ortaya çıkabilecek yeni güvenlik açıkları ve ürünün yeni güvenlik sorunları yaratabilecek yeni uygulamaları vardır. Bu nedenle ürün kullanıma girdikten sonra da her zaman güvenlik riskleri göz önünde bulundurmalı ve bu aşamalarda sistemi veya ürünü güvende tutacak konumda olan kişilerle iletişim halinde olunmalıdır. Ürünün tasarım ve yapılandırma aşamalarında güvenlik özelliklerinin dikkate alınmamış olması ya da bazı çalışanların güvenlik uygulamalarını görmezden gelmesi veya geçersiz kılması durumlarında nelerin yapılabileceği belirlenmiş olmalıdır.

3.2.1.7 Siber Güvenlik Konusunda Hesap Verebilirlik

Bir siber güvenlik ekibinde, siber güvenlik uygulamasının sorumluları belirlenmiş olmalıdır. Risklerden veya zararlardan sorumlu olacak ve hesap verebilecek belirli eylemlerle görevlendirilmiş sorumlu personel belirlenmiş olmalıdır. Planlı güvenlik denetimleri, olay raporları, erişim politikalarının gözden geçirilmesi, ayrıcalık düzeyleri, şifre yönetimi ve denetimler gibi kuruluş / ekip politikaları ve kuralları oluşturmalı ve uygulanmalıdır. Siber güvenliğe yönelik çalışmaların düzeltilmesi, onarımı ve yinelemeli iyileştirilmesine yönelik siber olay planlaması gibi süreçler tanımlanmış olmalıdır. Prosedürler, kurallar, teşvikler ve organizasyon / ekip kültürü bu güvenlik açıklarının göz ardı edilmesini engellemelidir. Siber güvenliğe yönelik çalışmalar, uygun eğitim, öğretim ve rehberlik seviyelerine sahip, uygun vasıflı ve sorumlu personel tarafından yürütülmelidir. Yeterli bir güvenlik uygulaması için sorumluluk verilen personelin, yapılması gerekenler

konusunda iyi bilgilendirilmiş, eğitilmiş, motive edilmiş, donanımlı olmasına dikkat edilmelidir.

Kurumsal yapılarda, iş bölümünün bulunmaması, sorumluluk ve hesap verebilirlik açısından önemli bir sorundur. Bir takımdaki hiç kimsenin etkili ve etik siber güvenlik uygulamasını sağlamak için gerekli adımları atma yetkisi olmadığını veya zorlanamayacağı bir sorumluluk yayılımından kaçınmak için, net sorumluluk zincirlerinin oluşturulması ve çalışmaya katılan herkese açık hale getirilmesi önemlidir. Bir projenin mümkün olan en erken aşamalarından itibaren güvenlik yönetiminin ve zararın önlenmesinde hangi zaman aralığında, kimin neden sorumlu olduğu açık ve net bir şekilde tanımlanmış olmalı ve kayıt altına alınmış olmalıdır. Sorumluluk ve hesap verebilirlik zincirlerinin temel işlevi, bireylerin siber güvenlik çalışmasının ve etik öneminin açıkça sahiplenmesini sağlamaktır.

3.2.1.8 Mevcut Güvenlik Sistemlerinin Kullanımının Sağlanması

Kritik altyapıların faaliyetlerinin otomasyonunu sağlayan endüstriyel kontrol sistemleri, bu sistemleri kullanmakta olan operatörlerin bilgileri yorumlamasına ve karar vermesine yardımcı olacak ara yüz yazılımlarına sahiptir. Sistemler normal çalışma aralıkların dışına çıktığında alarmları devreye sokan otomatik izlemenin kullanılması, insan operatörlerin izleme için harcadıkları sürenin azalmasına ve daha büyük ağları kontrol etmelerine izin vermiştir. Bu sistemleri yanı sıra çoğu kuruluşta, fiziksel erişimi kaydeden ve yazılım izleme sağlayan güvenlik sistemleri de mevcuttur, ancak bunlar etkin bir şekilde izlenmemektedir. Sistem, davranıştaki değişiklikleri, yeni tehditleri ve yeni sistem güvenlik açıklarını belirlemek için sistemlerin ve faaliyetlerin sürekli izlenmesini içermelidir. Kullanıcıların arzuları, hangi nedenle olursa olsun, uyumluluğun zayıf olduğu sistemin parçalarını vurgulayacaktır. Sistemin neyi koruduğuna bağlı olarak (değerli veriler, kritik kontrol sistemlerine erişim) bu bilgiyi almak veya kontrolü ele geçirmek isteyenler, kuruluşun çalışanlarına zarar veren teknikleri kullanmaya hazır olabilirler. Bu, kişisel mali zorluklardan yararlanmayı veya çalışanları, onları baskıya karşı savunmasız hale getiren ilişkilere katılmaya teşvik etmeyi içerebilir. Güvenlikte benzer bir yaklaşım bir dereceye kadar benimsenebilirken, güvenlik insanlar için insanlardan kaynaklanan bir tehdittir. Bu nedenle, sistemi tehlikeye atmaya çalışanlar güvensizlik, utanç ve güvenlik açığından yararlanacaktır. Bu nedenle kuruluşun, çalışanların kendilerini nasıl koruyabilecekleri

konusunda rehberlik sağlamak da dahil olmak üzere, çalışanları desteklemek ve savunmak konusunda çok daha proaktif olması gerekir.

Önceki saldırılar, sistemlere erişilebileceğini ve hasara neden olabileceğini ve kazalar, nispeten küçük hataların çok daha önemli olaylara yol açabileceğini göstermiştir. Bu nedenle saldırı kayıtları tutulmalı belirli aralıklarla incelenerek yönetime raporlar sunulmalıdır. Mevcut güvenlik sistemlerinin verimli kullanılabilmesi için bu sistemler ile etkileşimde bulunan personelin yalnızca uygun güvenlik süreçleri ve prosedürlerinin ne olduğunu bilmeleri değil, aynı zamanda bunlara uymaya istekli ve yetenekli olmaları da gerekmektedir.

3.2.1.9 Şeffaflık ve Bilgilendirme

Kritik altyapı sistemlerinin güvenliklerinin sağlanması için yürütülmekte olan faaliyetlerin, sistemin asıl işlevini yerine getirmesine engel olmayacak şekilde gerçekleştirilmesi için tüm paydaşlarla dürüst görüşmeler yapılmalı, sahte güvenlik hissi verilmemeli, yerine getirilemeyecek güvenlik ya da sistem işlevselliği vaat edilmemelidir. Paydaşlara, sisteme yönelik önemli zararlara neden olabilecek güvenlik ihlalleri hakkında doğru bilgi verilmelidir. Eylemleri değer taahhütlerindeki tutarlılık, samimiyeti ve şeffaflığı yansıtıyor olmalı; keyfi, tutarsız, samimiyetsiz veya aldatıcı olmamalıdır.

ACM kurallarında bilgisayar uzmanlarının bilişim sistemleri, sistemlerin sınırlılıkları, güvenlik açıkları ve sundukları fırsatlar gibi teknik bilgileri kamu ile paylaşması, kamuda bilişim bilincini geliştirmesi ve bilgisayar anlayışını teşvik etmesi; bilgisayarla ilgili yanlış veya yanıltıcı bilgileri ele alması gerektiği vurgulanmaktadır. Yine bilişim uzmanlarının veri ihlallerinden etkilenen tarafların zamanında ve net bir şekilde bilgilendirilmeleri ve uygun rehberlik ve iyileştirme sağlamaları için gerekli adımları atmaları önerilmektedir (ACM,2018:8).

Ancak kimi durumlarda güvenlik açıklarının duyurulması sistemler için riskli durumlar oluşturabilmektedir. Güvenlik uygulaması geliştiren kuruluş kendi ürününde kritik bir güvenlik açığı bulursa, bu ürünü kullanmakta olan müşterilerini bu sonradan keşfedilen güvenlik açığını gidermek üzere, zamanında bir yama (varsa) kurulumunu yapmaları veya diğer savunma önlemleri temin etmeleri konusunda bilgilendirmek üzere gerekli anlaşmaları yapmış olmalıdır. Bu anlaşmanın uygulanması aşamasında çoğu durumda, açıklamanın

uygun şekli ve kapsamı ve 'zamanında' bildirim olarak kabul edilenler önemli tartışmaları beraberinde getirmektedir. Örneğin, bir güvenlik açığının üçüncü bir tarafça keşfedilmesi ve kullanılmasının çok zor olacağı bir durumda, henüz güvenlik ekibi tarafından yamalanamaz. Güvenlik açığını giderecek bir yamanın çalışır hale getirilmesi öncesinde açığın yayınlanması potansiyel olarak saldırı olasılığını artıracak ve başkalarına zarar verme riski de ortaya çıkacaktır. Bu nedenle güvenlik açıklarının kimlere, ne zaman ve hangi yolla duyurulacağı üzerinde durulmalıdır.

3.2.2 Siber Güvenliğin Sağlanmasında Bireysel Etik Davranış

Toplumsal düzenin sağlanmasında önemli rolleri olan kanunlar ve hukuki düzenlemeler, günümüzdeki teknolojik gelişmelerin hızı, ölçeği ve karmaşıklığı ve bunların öngörülmesi zor sosyal etkileriyle baş edememektedir. Bilişim teknolojileri çok farklı alanlarda kullanılmaya başlandığı için kanun yapıcılar, etkili politikalar geliştirme hususunda yetersiz kalmaktadır. Bu nedenle, teknik uzmanlar giderek artan şekilde bu sosyal etkileri tahmin etmeye ve teknik seçimlerinin insan yaşamlarını nasıl etkileyebileceği konusunda proaktif bir şekilde düşünmek zorunda kalmaktadır (Vallor ve Rewak:3-4).

Siber güvenliğin sağlanmasında sistemi tasarlayan, geliştiren, kullanan tüm personele önemli görevler düşmektedir. Küresel, ulusal, kurumsal seviyede alınabilecek güvenlik önlemlerinin uygulanması aşamasında bireysel seviyede karar alınması durumları ortaya çıkacaktır. Kişinin kendi başına bir karar alacağı durumda etik karar alma ve uygulama kavramı gündeme gelmektedir. Tezin temel sorunu çevre etiği bağlamında siber güvenliğin nasıl sağlanacağı olduğu için bireyin kamu yararını dikkate alması gerekmektedir. ACM Etik ve Mesleki Davranış Kuralları da "Bilgisayar profesyonellerinin eylemleri dünyayı değiştirir" ifadesiyle başlamaktadır. Küresel seviyede bilişim profesyonellerin ACM Etik Kuralları'nın geliştirilmesine katılımı, küresel bilişim topluluğunun kamu yararına olan sorumluluğu ciddiye aldığı görülmektedir (ACM,2018:1).

Etik kararların büyük çoğunluğu kişinin gelişme döneminde öğrendiği etik karar becerilerini uygulaması sonucu verilmektedir. Ancak bilişim teknolojilerinin karmaşıklığı nedeni ile sadece teknik gereksinimlere dar bir odaklanma ve potansiyel olarak bazı gereksinimlerin ıskalanması durumu gündeme gelebilmektedir (ACM,2018). Bilişim

teknolojilerinin küresel seviyede önemli çevre sorunlarına yol açabileceği göz önünde bulundurularak karar alma aşamasında uygulanabilecek etik kuralları netleştirmek üzere etik standartlar gözden geçirilmelidir.

Siber güvenlik uzmanlarının kamuya karşı yükümlülüklerinin nitelikleri ve detayları belirsiz olabilmektedir (Vallor ve Rewak,2018:30). Bu durumda, siber güvenlik çalışanlarının birey olarak yaptıkları faaliyetler nedeni ile toplumdan saygı görmek ve desteklenmek için hayati öneme sahip kamu yararı sağladıklarının bilincinde olarak görevlerini yerine getirmeleri gerekmektedir.

Siber güvenlik olayları, küresel seviyede önemli çevre etiği sorunlarına yol açabileceği için gerekli önlemlerin alınması da önemli ölçüde risk ve maliyet gerektirebilmektedir. Bu durumda başkaları tarafından daha önce gerçekleştirilmiş en iyi uygulamaların gözden geçirilmesi yararlı olabilecektir. Siber güvenlik uygulayıcıları etik zorlukları akıllıca ve iyi bir şekilde yönetmek için siber güvenlik alanındaki en iyi uygulamalara odaklanmanın yanı sıra yaşamlarını sürdürebilmek ve etik davranışlar sergilemek için uygulama kümesinden yaratıcı şekillerde yararlanabilmelidirler.

Her alanda herkes için geçerli tek, ayrıntılı bir siber güvenlik etiği kuralı olmadığı için kuruluşlar ve meslekler, siber güvenlik etiği için kendi faaliyetlerine ve zorluklarına özel olarak uyarlanmış açık iç politikalar, prosedürler, yönergeler ve en iyi uygulamalar geliştirmeye teşvik edilmelidir. Bununla birlikte, bazı genel etik kurallar, siber güvenlik uygulamaları için özelleştirilebilir niteliktedir:

Kritik altyapı tesislerinin faaliyetlerini yerine getirmede kullanılmakta olan EKS'nin teknik personeli, üzerinde çalıştıkları sistemlerin insan hayatına olumsuz etkisini dikkate almayabilmektedir. Ancak meydana gelebilecek bir siber güvenlik olayının oluşturabileceği olumsuz sonuçlar bireysel seviyede her zaman akılda tutulmalı ve buna uygun davranışlar geliştirilmelidir.

Siber güvenlik çalışmalarında, teknik olmayan aktörlerin farkında olmadan yapabilecekleri hatalar göz önünde bulundurulmalı ve empati yapılmalıdır.

Siber güvenliğe yönelik tehditlerin doğası ve kapsamı sürekli olarak değiştiğinden, siber güvenlik etiği, güvenlik uygulamalarının etik sonuçlarının sürekli olarak gözlemlendiği, hatalardan ders çıkarıldığı, daha fazla bilginin toplandığı, daha fazla etik ve

teknik uzmanlığın edinildiği ve güvenlik uygulamalarının buna göre güncellenip geliştirildiği sürekli bir öğrenme döngüsü olarak ele alınmalıdır.

İhlallere ve siber güvenlik olaylarına aşırı tepki ile yetersiz tepki arasındaki etik olarak uygun dengenin belirlenmesine çalışılmalıdır. Siber güvenlik ekibi, olası bir ihlalin belirtilerini dikkate almalı, gerçek riski azaltmama yönünde çaba sarf etmelidir. Kritik bir güvenlik açığı ortaya çıktığında, buna uygun önlemler alınmalıdır. Başka amaçları gerçekleştirmek için siber güvenlik riskleri, çok da abartılmamalıdır.

Siber güvenlik uygulamalarını mükemmelleştirmek için diğer mükemmel kişiler ve profesyonellerle iş birliği yapılması herkes tarafından kullanılacak standartların iyileştirilmesine katkıda bulunacaktır. Teknolojik ve etik açıdan üstün siber güvenlik normlarının, standartlarının ve uygulamalarının bireysel seviyede savunulmasının, küresel seviyede herkes için siber güvenliğin sağlanması seviyesini yükselteceği değerlendirilmektedir.

Günlük yaşam içinde bireysel etik davranış alışkanlıkları siber uzayda da kendini gösterdiğinde çevre etiği açısından olumlu yansımaları olacak ve siber güvenliğin sağlanmasında önemli adımlar atılmış olacaktır. Bunun için kişinin bugün olduğu kişi ile olmak istediği kişi hakkında sürekli olarak düşünmesi; değiştirmek veya geliştirmek istediği karakter özelliklerini ve alışkanlıklarını belirlemesi; kendi seçimlerini ve karakterini hayran olduğu ve en çok saygı duyduğu kişilerin bakış açıları ile yargılaması, onların davranışlarını örnek alması gerekmektedir. Gerçekleştirilen bir faaliyetin sadece yakınlar üzerinde değil çok uzak mekanlarda tanınmayan kişiler üzerinde ne tür etkileri olabileceğini düşünmek önemlidir. (Vallor ve Rewak,2018:59). İkinci Bölümde ele alınan Maroochy örneğinde olduğu gibi saldırgan, anlık öfkesi ile su arıtma tesisine saldırı düzenlemiş, bu saldırı sonrası önemli ölçüde can ve mal kaybı, çevre felaketine neden olmuştur. Yaptığı davranışın sonuçlarının bu boyutta gerçekleşebileceğinin farkında olsa idi büyük olasılıkla bu saldırıyı gerçekleştirmeyecekti. Eylemlerin diğer paydaşlar üzerindeki muhtemel etkisini öngörme yeteneği geliştirilmelidir.

Kişinin cesur, merhametli ve dürüst davranışlar sergilemesi, özel hayatında ve meslek hayatında kendisine saygı duyulmasını ve güvenilmesini sağlayacak, bu da onu mutlu edecektir. Yaptığı davranışın sadece kendi iyiliği için değil başkaları için de yani

çoğunluğun iyiliği için de geçerli olması uzun vadede bu kişiye saygınlık kazandıracak ve onu mutlu edecektir.

Günümüz dünyasında eylemleri ile küresel seviyede etkiler yaratabilecek olan bilişim uzmanları (ACM,2018: Birinci Bölüm);

- Etik karar verme aşamasında, farklı ilkeleri bir arada dikkate almalı,
- Hesap verebilirliği ve şeffaflığı teşvik etmek üzere etik konular hakkında açık tartışmalar yapmalı,
- Sürekli olarak kamu yararını destekleyerek çalışmalarının daha geniş etkileri üzerinde düşünmeli,
- Dürüst ve güvenilir olmalı,
- Şeffaf davranmalı ve ilgili taraflara tüm sistem yeteneklerini, sınırlamaları ve olası sorunları tam olarak açıklayabilmeli,
- Kasten yanlış veya yanıltıcı iddialarda bulunmamalı, verileri uydurma, tahrif etme, rüşvet teklif etme veya kabul etme gibi dürüst olmayan davranışlardan kaçınmalı,
- Kendi nitelikleri ve bir görevi tamamlama yeterliliğindeki sınırlamalar konusunda dürüst ve açık sözlü olmalı, taahhütlerini yerine getirilmeli,
- Kuruluşun politikalarını veya prosedürlerini yanlış tanıtmamalı ve yetkilendirilmedikçe bir kuruluş adına konuşmamalı,
- Eşitlik, hoşgörü, başkalarına saygı ve adalet değerlerini ön planda tutarak adil olmalı ve ayrımcılık yapmamalı, yeterince temsil edilmeyen gruplar da dahil olmak üzere tüm insanların adil katılımını teşvik etmeli,
- Bilişim sistemleri ve etkileri hakkında kapsamlı değerlendirmeler yapmalı,
- Sadece kendi yetkinlik alanlarında fikir beyan etmeli,
- Mesleklerinin karmaşıklığı, aşırı basitleştirilmiş yaklaşımların tehlikelerinin, olası her çalışma koşulunu tahmin etmenin imkansızlığının, yazılım hatalarının kaçınılmazlığının, sistemlerin ve bunların bağlamlarının etkileşimlerinin ve sistemle ilgili diğer sorunların tamamen farkında olmalıdır.

Enerji üretim ve dağıtım tesisleri, su ve kanalizasyon sistemleri, petrol üretme ve arıtma tesisleri, nükleer enerji tesisleri gibi kritik altyapıların kurulması, işletilmesi,

kullanılması aşamalarında, zayıf teknik seçimlerden kaynaklanabilecek etik açıdan önemli zararları görülebilmektedir. Bu nedenle çok bilinen ve uygulanan en iyi teknik uygulamaları takip etmek, etik açıdan önemli faydalar sağlayabilecektir. Kritik altyapıların kurulması, işletilmesi, kullanılması aşamalarında meydana gelebilecek bir siber güvenlik olayı, insanlar ve diğer canlılar için sürdürülebilirliği engelleyebilecek önemli sorunlar oluşturma kapasitesine sahiptir. Bireysel seviyede ihmal veya sorumsuz hareket önemli çevre sorunlarına yol açabilecek niteliktedir (Vallor, ve Rewak:7-8).

Siber uzaydaki çok hızlı teknolojik gelişmeler siber güvenlik alanında önemli belirsizlikler yaratmaya devam etmektedir ancak bu alanda insanların rolü de oldukça önemlidir (Puyvelde ve Brantly,2019:452-455). 268 katılımcı kuruluşla yapılan bir ankette, kuruluşların çoğunun kritik EKS varlıklarını bildirmediğini ve sorunları tespit etmek için araçlara değil, personele güvendiğini belirtmiştir (Luallen,2014:3).

Siber güvenlik profesyonellerinin, uygulamalarının insanların yaşam kalitesini önemli ölçüde etkileyebileceği birçok yol konusunda dikkatli olmaları ve etkili bir şekilde ele alınabilmeleri için potansiyel zararlarını ve faydalarını daha iyi tahmin etmeyi öğrenmeleri gerekir (Vallor ve Rewak, 2018:12).

Siber güvenliğin sağlanmasına yönelik uygulamaların doğru bir şekilde kullanılması da çevrenin korunması ve sürdürülebilir kalkınmanın sağlanması açısından önemlidir. Siber güvenliğin sağlanamaması, insan özgürlüğüne, ekonomisine, itibarına zarar verebilmesinin yanı sıra, insanın ve tabii ki diğer canlı varlıkların ve hatta tüm dünyanın zarar görmesine neden olacak boyutlara ulaşabilecek nitelikte sonuçlar doğurabilir.

Petrol ve doğal gaz gibi enerji üretim, dağıtım sistemleri, barajlar, su arıtma ve kanalizasyon tesisleri, kimyasal tesisler gibi kritik altyapı sistemlerine uzaktan erişim sağlanarak izlenmesi ve faaliyetlerinin yerine getirilmesi verimliliği artırmış ve önemli ölçüde tasarruf sağlamıştır. Endüstriyel kontrol sistemleri, diğer kurumsal sistemlerle ve geleneksel bilişim sistemleri ile entegre edilmeye başlanmıştır. Ancak bu entegrasyon, önemli faydaların yanı sıra önemli güvenlik açıklarına da yol açmaktadır. EKS'nin diğer kurumsal BİT sistemleriyle entegrasyonu ile EKS, geleneksel bilişim sistemlerine yönelik risklerle de karşı karşıya gelmeye başlamıştır.

Endüstriyel kontrol sistemlerinin geniş alanlara yayılmış kapsamlı kurumsal ağlara ve İnternet'e bağlantısı arttıkça, yetkisiz erişim tehdidi de artmaya başlamıştır. Bu sistemlerin saldırılara karşı korunmasında, teknolojik çözümlerin kullanılması yeterli olmamaktadır. Buna ek olarak geniş alanlara yayılmış olan bu sistemleri tasarlayan, geliştiren, kullanan insanların da dikkate alınması gerekmektedir.

Siber güvenliğin sağlanmasında kullanıcıların sorumluluğunu azaltmak ve kabul edilebilir bir güvenlik derecesini sağlamak üzere güvenlik sistemleri geliştirilmeye başlanmıştır. Siber güvenliğin sağlanmasına yönelik sürdürülmekte olan faaliyetler, güvenlik personelinin istihdamı ve güvenliğe yönelik yazılım-donanım ürünlerinin kullanılması şeklindedir. Teknoloji ile insanın karmaşık etkileşimine sahne olan bu sürecin teknoloji bölümünde uzaktan erişim yöntemi ile kritik altyapı tesislerinde üretim, aktarım, yönetim faaliyetlerini gerçekleştirmek üzere karmaşık yazılım, donanım, ağ bileşenlerinden oluşan EKS yer alırken insan bölümünde, bu sistemleri tasarlayan, üreten, bakımını yapan, yöneten, kullanan tasarımcılar, operatörler, bakım personeli, yöneticiler ve herhangi bir nedenle sisteme erişmek isteyen herkes yer almaktadır (Bridges,2013:82-83). Siber güveliğin sağlanmasında, bireylerin her alanda etkin davranışlar sergilemesi, işyerlerinin, topluluklarının ve ülkelerinin yönetimine katılmaya kendilerini adaması önemli yer tutmaktadır (Renner ve Prugh,2014:25).

3.3 KURUMSAL SİBER GÜVENLİK FAALİYETLERİ

Faaliyetlerini yerine getirememesi durumunda canlı ve cansız varlıkların mevcudiyetlerini sürdürebilmeleri için gerekli fiziki çevrenin, kimi durumlarda ekosistemin önemli ölçüde zarar görmesine neden olabilecek kritik altyapı siber güvenliğinin sağlanmasında insan faktörünün önemi ve yapması gerekenler bir önceki kısımda ele alınmıştır. Bu sistemlerin tasarımı, üretimi, faaliyete geçirilmesi, güvenliklerinin sağlanması tek başına bireylerin yapamayacağı görevler olup bu sistemleri tasarlayan, geliştiren, işleten kurumsal yapılara ihtiyaç vardır.

Kritik altyapıların siber güvenliğinin sağlanması için risk yönetimi yaklaşımı kapsamında BT risklerini ele alarak bu risklerin azaltılması için tanımlanmış özel faaliyetler olan siber güvenlik kontrolleri gerçekleştirilmelidir (Tabansky,2017:212). Şahsi kontroller,

belirli siber güvenlik tehditlerinin meydana gelmesi ya da olumsuz etki yaratması olasılığını azaltabilir, buna ek olarak bir siber güvenlik olayının etkisini ve tekrarlanması olasılığını azaltmak üzere çoklu kontroller gerçekleştirilmelidir (Alexander ve Panguliri,2017:36). Kontroller kullanılarak etkili sonuçlar meydana getirebilecek riskleri denetim altında tutmak üzere kullanılacak faaliyetler ve yöntemler gözden geçirilebilmektedir. Risklerin kontrollerle azaltılamaması durumunda endüstriyel süreçlerin saldırı yüzeyleri hızla büyümeye devam edebilecektir (Tabansky, 2017:212). Siber güvenlik faaliyetleri, siber olayların gerçekleşmesini önlemeye yönelik faaliyetlerin yanı sıra bir siber olayın gerçekleşmesi anı ve sonrasındaki faaliyetleri de kapsamaktadır.

3.3.1 Yönetimsel Kontroller

Yaptıkları işlerin farklılığı nedeni ile tüm kurumsal yapılar için tek bir rol belirlemek mümkün değildir. Şirketler, her durumda sistemlerini en iyi uygulamalara göre güvenceye almalı ve maliyetleri düşürmek amacı ile güvenli olmayan sistemleri, uygulamaları ve prosedürleri kullanmaktan kaçınmalıdırlar (Inversini, 2020:274).

Standartlara ve düzenlemelere uygunluk, hizmet seviyeleri, sözleşmeler, iş stratejileri gibi yönetimsel konularla ilgilenmek üzere kullanılmakta olan yönetimsel kontrol, en üst seviye yönetim ihtiyaçlarını karşılamak üzere uygun operasyonel ve teknik kontrollerin uygulanmasını sağlayacak kurumsal politika şeklinde açıklanabilir (Macaulay ve Singer, 2011:165-166).

3.3.1.1 Güvenlik Politikalarının Geliştirilmesi

Yönetim amacını ifade eden, güvenlik misyonunu ele alan, rolleri ve sorumlulukları tanımlayan ve hesaplama kaynaklarının kullanımını ele alan politikalar geliştirilmelidir (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013;AMI,2008). Siber güvenlik gereksinimleri net olarak tanımlanmalıdır. Kurumların ve firmaların, beklentileri karşılamak için zorunlu ihtiyaçları karşılayacak ve çalışanlara gerekli sorumlulukları verecek şekilde yapılandırılmış güvenlik programlarına ihtiyaçları bulunmaktadır. Kurumun tamamını kapsayacak şekilde, kişilerin inisiyatiflerine bağlı olmaksızın siber güvenliği sağlamak için tutarlı, standart tabanlı bir yaklaşım kurmak için resmi bir program gereklidir. Politikalar ve

süreçler ise çalışanları siber güvenlik konusundaki sorumlulukları ve bu sorumlulukları yerine getirmede başarısız olunması durumundaki sonuçları hakkında bilgilendirmelidir. Bu dokumanlar, bir siber güvenlik kazası durumunda alınacak önlemlere ilişkin yönlendirici bilgileri ve kriz döneminde alınacak etkili önlemleri de geliştirecek bilgileri sağlamalıdır. Siber güvenlik ihtiyaçlarını tanımlamanın bir bölümü olarak kullanıcılara imzalatılan sözleşmeleri, duyuruları, uyarı afişlerini de kapsamalıdır. Kötü niyetli kullanıcılardan gelecek tehditleri en aza indirgemek üzere bilmesi gereken prensibine göre ağ erişimini sınırlamayı ve arka plan kontrollerini gerçekleştirmeyi kapsayan ihtiyaçlar listesi hazırlanmalıdır (DOE-USA,2002).

3.3.1.2 Program Yönetim Planı

Kuruluş içinde güvenlik programı yönetim kontrollerinden ve kıdemli bir bilgi güvenliği görevlisinin atanmasından sorumlu kişileri belirten Program Yönetim Planı oluşturulmalıdır. Bu plan, tüm sermaye planlaması ve yatırım taleplerinin bilgi güvenliği programını uygulamak için gereken kaynakları içermesini sağlamalıdır. Kurumsal mimari, sistem güvenliği göz önünde bulundurularak geliştirilmelidir. Tüm sermaye planlaması ve yatırım taleplerinin bilgi güvenliği programını uygulamak için gereken kaynakları içermesini sağlamalı ve bilgi güvenliğini göz önünde bulundurarak bir kurumsal mimari geliştirilmelidir. Bilgi güvenliğini ve bunun sonucunda kurum, personel ve kritik altyapı için ortaya çıkan riski dikkate alarak görev/iş süreçleri tanımlanmalıdır (NIST SP 800-53r4,2013;AMI,2008). Siber güvenlik performansı konusunda istenenleri gerçekleştirmek ve bireyleri kendi performanslarından sorumlu tutmak üzere üst kurumsal liderlik önemli yarar sağlayacaktır. Etkili siber güvenlik uygulaması için kurumun üst düzey yöneticilerinin desteği gereklidir. Üst düzey yönetimin güçlü bir siber güvenlik beklentisi oluşturması ve bu beklentiyi kurum genelindeki tüm alt yöneticilere iletmeleri esastır. Üst düzey yöneticilerin siber güvenlik programlarının uygulanmasına yönelik yapının kurulmasına liderlik etmeleri de önemlidir. Siber güvenlik programının sürekli ve tutarlı bir şekilde uygulanmasını teşvik edecek olan bu yapı, siber güvenlik konusunda çalışan yöneticiler, sistem yöneticileri, teknisyenler, son kullanıcılar ve operatörler gibi bireylerin yaptıkları işten sorumlu tutulmaları açısından da önemlidir. (DOE-USA,2002)

3.3.1.3 Güvenlik Planlarının Geliştirilmesi

Güvenlik kontrolleri tanımlanmalı ve uygulanmalı, siber personel tarama politika ve prosedürleri geliştirilmelidir (NIST SP 800-82r2,2015; ISA-62443-2-1-2009; NIST SP 800-53r4,2013; AMI,2008).

Güvenlik şirketleri tarafından ortaklaşa geliştirilen ve uyulan etik davranışlarla ilgili yönergeler hazırlanmalı ve kullanıma sunulmalıdır. Bu yönergelerdeki kuralların ihlali durumundaki yaptırımlar da belirlenmiş olmalı ve gerektiğinde uygulanmalıdır (Inversini, 2020:274).

Kritik altyapı tesislerinin kurulu olduğu fiziki çevrenin yerel yönetim birimleri ile koordineli bir şekilde yönetilecek kurumsal bir doğal afet planına da ihtiyaç vardır. Kritik tesislerin kurulacağı yerin seçimi ve doğal afet planlaması yapılırken bu ortamdaki tehdit düzeyleri BM Afet Riskini Azaltma Ofisi (United Nations Office for Disaster Risk Reduction ve ABD İç Güvenlik Bakanlığı Federal Acil Durum Yönetim Ajansı (FEMA) yayınlarından yararlanılabilecektir (Stallings,2019:793).

3.3.1.4 Personel Politika ve Prosedürlerinin Geliştirilmesi

Görevli personelle ilgili olarak personelin geçmişi, istihdam koşulları, sorumlulukları, işe alım, transfer ve iş akdinin sonlandırılması gibi konularda uygulanmak üzere ilgili politika ve prosedürleri belirlenmiş olmalıdır (NIST SP 800-82r2,2015; ISA-62443-2-1-2009; NIST SP 800-53r4,2013; AMI,2008). EKS'ne yönelik güvenlik ihlallerindeki artış ve sistemlerin güvenlik açıkları nedeni ile EKS'ni çalıştıran operatörler ve sistem satıcıları, üreticileri arasında daha fazla ve daha yakın bir koordinasyona ihtiyaç vardır (Luallen,2014:27).

Güvenlik riskleri, siber suçlar ve diğer yetkisiz erişimlerle çok hızlı bir şekilde artmaya devam ettiği için, aynı hızla BT güvenliği yönetimi ve güvenlik çözümlerinin uygulanması ve yeni yaklaşımların geliştirilmesine ihtiyaç vardır. BGYS'nin başarılı kullanımı için personel eğitilmeli ve farkındalığı geliştirilmelidir. Siber tehditlerin engel olarak görüldüğü mevcut durum bir fırsat olarak değerlendirilmelidir. Siber güvenliğin artırılması için en verimli yöntem, teknik bilginin geliştirilmesidir. Bilgi ve iletişim teknolojilerini kullanarak bilginin işlenmesi sürecinde görev alan tüm kullanıcıların, değişen rolleri ve sorumlulukları ile ilgili alanlarda desteklemek üzere farkındalık oluşturma ve

eğitim verme süreçleri gereklidir (Rajamaki,2017:248). Güvenlik bilinci, siber güvenliği her çalışanın görevleriyle ilişkilendirmeli ve güvenliğin yalnızca BT veya güvenlik personelinin sorumluluğunda olduğunu varsaymamalıdır. Bir kuruluşun en iyi izinsiz giriş tespit yeteneği, uyanık personeldir (Luallen,2014:8).

3.3.1.5 Satın Alma Politikalarının Geliştirilmesi

Sistemin yaşam döngüsü boyunca risk değerlendirmesine dayalı satın alma politikaları uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). EKS hızlı bir şekilde birbirleri ile bağlantılı hale gelmeye başlamakta ve kontrol edilen fiziksel varlıkların sayısı da her geçen gün çoğalmaktadır. Aktif tehdit aktörleri artarken, siber güvenlik için kurumsal bütçeler değil tehditleri, sistem açıklarıyla başa çıkmak için bile yeterli değildir. Tedarik sürecinde siber güvenlik bütçeleri artırılmalı ve güvenlik ihtiyaçları tanımlanmalıdır (Luallen,2014:26-27).

Güvenliğin sağlanması ve artırılması için donanım ve uygulama satıcıları ile iş ortakları olarak anlaşmalar yapılmalıdır. İş ilişkilerinin sürekliliğini sağlamada temel ihtiyaç olan güvenli sistemler için sürekli iletişim halinde olunmalıdır (Harp ve Gregory-Brown, 2015:19).

Yazılım geliştiricilerinin geleneksel işletim sistemleri güvenlik kontrollerinin yanı sıra güvenli yazılımlar oluşturmak için eğitim alıp almadıkları hususunda satıcılardan bilgi alınmalıdır (Luallen,2014:26).

3.3.1.6 Bakım Yönetimi Politikası

Sistem bakımının tüm bölümlerini ele almak için politikalar ve prosedürler geliştirilmeli ve uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). Kurum tesislerinde kullanılan yazılım, donanım ve ağ olmak üzere her türlü bilişim teknolojisi ürününün hizmetten çıkarılması veya yeniden konuşlandırılması için eskime prosedürleri oluşturulmalıdır (Luallen,2014:26).

3.3.1.7 Yama Politikasının Geliştirilmesi ve Uygulanması

İşletim sistemlerini, donanımlara ait sürücü yazılımlarını, uygulama yazılımlarını vb.ni geliştiren yazılım firmaları uygulamanın geliştirilmesi aşamasında dikkatten kaçan güvenlik açıklarını düzelten ve yazılımın işlevselliğini artıran ve yama olarak adlandırılan

yazılım güncellemelerini yayımlamaktadır. Üretici firma, sistemlerin kullanılması aşamasında çalışanlar tarafından ya da kötü niyetli siber saldırganlar tarafından keşfedilen güvenlik açıklarını önlemeye yönelik çözümleri hızlı bir şekilde bulmaya ve geliştirilen bu çözümleri yama adı altında son kullanıcıya iletmektedir. Sistemin mevcut siber güvenlik açıklarının herhangi bir siber güvenlik olayına neden olmaması için, son kullanıcılar, düzenli olarak bu yamaları takip etmeli ve kurulumunu yapmalıdır. İlgili firma tarafından yayımlanan yamanın, son kullanıcı tarafından yüklenmemesi durumunda kötü niyetli kişiler de bu güvenlik açığından haberdar olmuş olacakları için güvenlik açığı riski daha da artacaktır (Puyvelde ve Brantly,2019:367).

EKS'ne yama uygulanması, geleneksel bilişim sistemlerindeki kadar kolay bir işlem değildir. Yama yapma veya yama yapmama seçimi, kontrol sistemi varlıklarının tipine, ortak bir kesinti penceresine sahip olup olmadıklarına veya yeterli sayıda mevcut olup olmadığına bağlıdır.

Yama geçilmemiş sistemlerde önemli güvenlik açıkları bulunabilir. Yazılım güncellemeleri, bu güncellemelerin endüstriyel kontrol uygulaması ve uygulamanın son kullanıcısı tarafından en ince ayrıntılarına kadar test edilmesi gerektiği ve EKS kesintileri planlı şekilde yapılmak zorunda olduğundan her zaman periyodik dönemlerde gerçekleştirilememektedir. EKS güncelleme sürecinin bir parçası olarak yeniden doğrulama ihtiyacı duyabilir. EKS'nin pek çoğunun işletim sistemleri eski sürüm olup üreticileri tarafından desteklenmemektedir. Mevcut yamalar uygulanabilir durumda değildir. Donanım için uygulanacak değişim yönetimi süreci, güvenlik ve BT uzmanları ile birlikte EKS uzmanları tarafından, cihazın üreticileri ile de iş birliği yaparak gerçekleştirilmelidir. (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77; NIST SP 800-82r2,2015; ISA-TR62443-2-3-2015; NIST SP 800-53r4,2013).

Varlık sahipleri, çalışma süresini ve kapalı kalma süresini kontrol etmek için güncellemelerin ne zaman gerçekleştirileceğini belirlemelidir. Her EKS farklıdır ve kesintiye tahammülleri özellikle topluca yapılması gereken işler ve sürekli yapılması gereken işlerde farklıdır. Sistemlerin ne kadar kesintiye tahammülleri olduğu herkese açık ortamlarda yayınlanmışsa bu, saldırganlar için avantaj yaratacak bir durumdur. Örneğin

planlı bakım çizelgelerinin internette yayımlandığı durumlarda, saldırgan sistemin son kesinti döneminde hangi yamaların yüklendiğini tam olarak tahmin edebilir .

SCADA sistemlerin sahipleri, satıcılara güvenlik özelliklerini uygulamak üzere ürün yamaları ve yeni sürümleri üretmeleri hususunda ısrarcı olmalıdır (DOE-USA,2002).

3.3.1.8 Etkili Parola Politikasının Geliştirilmesi ve Uygulanması

Uzunluk, karakter türleri, denetim sıklığı ve değişiklik dönemleri gibi özelliklere sahip güçlü parolalar oluşturulmalıdır. Parola politikası, kullanılan parola korumalı erişim mekanizmaları türleri ile bir otomasyon sistemi operatörünün acil bir durumda stres altındaki sistem bileşenlerine hızla erişme ihtiyacı arasındaki dengeyi hesaba katmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008).

3.3.1.9 İş Sürekliliği ve Felaket Kurtarma Planları

Felaket kurtarma ve iş sürekliliği planları geliştirilmeli, test edilmeli ve uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; CIS-1:12,21; AMI,2008). Bir siber güvenlik olayı sonrasında güvenli duruma dönebilmek için yapılması gereken süreçler iyi tanımlanmış olmalıdır. Saldırı bir kez tespit edildiğinde tüm sistemler tehlikeye maruz kalır (Harp ve Gregory-Brown, 2015:19). “En kötü durum” senaryolarının tartışılmasına dayalı olarak hazırlanacak sistem yedekleme felaket/kurtarma planları “arızaya dayanıklı” sistemlerin arızalarını da içermelidir (Johnsen,2013:289).

Siber saldırılar da dahil bir acil durum sonrasında hızlıca mevcut duruma dönmeyi sağlayacak olan bir felaket kurtarma planı hazırlanmalıdır. Sistem yedekleri felaket kurtarma planının temel bölümü olup ağın hızlı bir şekilde yeniden çalışır hale gelmesini sağlayacaktır. Felaket kurtarma planlarının doğru çalıştığından emin olmak ve personelin bu planların uygulanmasını daha iyi öğrenebilmesi için düzenli olarak tatbikatlar yapılmalı; bu tatbikatlardan öğrenilen sonuçlara yönelik güncellemeler felaket kurtarma planlarına da uygulanmalıdır (DOE-USA,2002). Bir felaket durumunda ya da kritik sistemlerde başka bir arıza olması durumunda sistemin sürekliliğini sağlamak üzere sistem donanımını, yazılımını ve verilerini yedeklemek için gerekli düzenlemeler yapılmalıdır (NIST SP 800-82r2,2015; T.C.CBDDO,2020:179; AMI,2008).

3.3.1.10 Sertifikasyon ve Akreditasyon

Uluslararası geçerliliği olan sertifikalar alınmalı akredite olunmalı ve artık riskler kabul edilmelidir (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI). EKS standartları ile uyumlu bir güvenlik politikası geliştirilmeli ve uygulanmalıdır (Harp ve Gregory-Brown, 2015:19). IEEE, NERC gibi standart örgütleri ile birlikte çalışılmalıdır (Misbahuddin ve Al-Holou, 2012:176). Yetki verme, veri akışı, segmentlere ayrılmış ağ yapısı ve farklı işlerin sadece o işler için ayrılmış sunucular üzerinden yürütülmesi gibi güvenlik önlemleri NERC rehberlerine uygun olarak yürütülmelidir (Misbahuddin, Al-Holou, 2012:176).

EKS güvenlik açıklarının belirlenmesinde bağımsız test birimleri tarafından laboratuvar ortamında yapılacak güvenilir testlere itibar edilmelidir (NIST SP 800-82r2, 2015:E-1-E-4).

EKS siber güvenlik standartlarının geliştirilmesine devam edilmektedir. Ulus devletler de kendi özel yönergelerini oluşturmaya devam etmektedir. Bu nedenle özellikle uluslar üstü EKS firmalarının çok sayıda değişik standart ve düzenlemeye uyması gerekeceği değerlendirilmektedir (Luallen,2014:27).

3.3.2 Teknik Kontroller

Bu başlık altındaki kontroller, yazılım, donanım tabanlı güvenlik önlemleri ile ilgilenir. Bu uygulamalar ve cihazlar, en üst düzey yönetim kontrollerine uygun şekilde tasarlanmış operasyonel kontroller kullanılarak yönetilecektir. Teknik kontrol, güvenlik duvarı, bir ağda saldırı tespit uygulaması, sunucu üzerinde antivirüs yazılımı ya da başka bir uygulama olabilir. Teknik kontroller, zararlı ya da şüpheli durumu belirleyip durdurmalı, uyarı yayınlamalı ancak işlemsel verinin işlenmesini ya da uygulama sürecini durdurmamalıdır (Macaulay ve Singer, 2011, s:165-166).

3.3.2.1 Güvenlik Açıklarının Kontrolü ve Sistem Sıkılaştırma

Kritik yazılımların güvenlik açıklarını tespit etmek üzere testler uygulanmalıdır (NIST SP 800-82r2,2015; AMI,2008). Geleneksel BT sistemlerinin güvenlik açıklarının tespit edilmesinde kullanılmakta olan pek çok araç bulunmaktadır. Ancak bu araçlar mevcut güvenlik açıklarının tespiti ve sızma testi aşamasında, EKS üzerindeki sınırlı kaynakların

tüketilmesine ve önemli arızalara yol açabildikleri için pasif, daha az müdahalede bulunan otomatik güvenlik açığı ve sızma testi araçlarının kullanılması daha yerinde olacaktır.

EKS üzerinde güvenlik açıklarını belirlemek üzere kullanılmakta olan bu tür yazılımların hiç durmadan çalışması gereken EKS üzerinde uygulanmasından kaynaklanabilecek riskler göz önünde bulundurulmalı ve bağımsız test birimleri tarafından laboratuvar ortamında yapılacak güvenilir testlere itibar edilmelidir (NIST SP 800-82r2, 2015:E-1-E-4).

İyi bilinen teknikler kullanılarak periyodik olarak güvenlik açığı değerlendirme ve sızma testleri yaptırılmalıdır (Misbahuddin ve Al-Holou, 2012:176). SCADA ağının tüm bağlantıları için, sızma testleri ve zafiyet analizi yaptırılmalıdır (DOE-USA,2002). Kontrol ağına yönelik sızma testleri rutin olarak değil, mevcut kontrol sistemlerinin çalışmasına zarar vermeden çok dikkatli bir şekilde yapılmalıdır. Bilgi güvenliği denetimleri rutin olarak yapılamamaktadır (NIST 800-82 dokümanından aktaran (Macaulay, Singer, 2011:85-92), (Krutz, 2006:76-77).

Sistemin normal çalışmasını etkilemeyecek şekilde gerçek zamanlı ve sistem gereksinimleriyle uyumlu bir şekilde, güvenlik açığı değerlendirmeleri yapılmalıdır. (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). Donanım ve ağ elemanlarının saldırı yüzeyini azaltmak için gerekli sıkılaştırma kontrolleri uygulanmalıdır (T.C.CBDDO,2020:182).

SCADA ağının tüm bağlantıları için, sızma testleri ve zafiyet analizi yaptırılmalıdır (DOE-USA,2002). Bu bilgi SCADA ağlarının korunmasında sağlam bir güvenlik stratejisi geliştirmek için risk yönetim süreçleri ile birlikte kullanılmalıdır. SCADA ağları, en zayıf bağlantı noktasının güvenliği kadar güvenli oldukları için güvenlik duvarı, saldırı tespit sistemi ve diğer uygun güvenlik önlemleri her noktada alınmış olmalıdır. Güvenlik duvarları kuralları SCADA ağına erişimi yasaklayacak ve onaylanmış bağlantılara izin verildiğinde olabildiğince özelleştirilecek kurallar olmalıdır (DOE-USA,2002)

Günümüzde faaliyette olan EKS'nde fiziki ve mantıksal kontroller birlikte gerçekleştirilebilmekte olduğu göz önünde bulundurularak fiziksel süreçlerle etkileşim halinde olan EKS, içine entegre edilmiş tüm güvenlik fonksiyonları normal işlevi

değiştirmediklerini kanıtlamak üzere test edilmelidir (NIST 800-82, 2008'den aktaran (Macaulay ve Singer, 2011:85-92; Krutz, 2006, s:76-77).

Sistem sıkılaştırma olarak adlandırılan ve EKS'nin güvenlik özelliklerini artırmak üzere kullanılmakta olan ve her geçen gün yenileri geliştirilmekte olan güvenlik ürünlerinin bazıları aşağıdadır:

- **Güvenlik Duvarı:** EKS'ni korumak; İnternet ve kurumsal uygulamaların birbirinden ve diğer ağlardan izole etmek için güvenlik duvarları kullanılmaktadır. EKS için özel olarak geliştirilmiş güvenlik duvarları da bulunmaktadır (NIST SP 800-82r2, 2015:E-1-E-4). Kritik verileri korumak prosedürlerle birleştirilmiş çift yönlü ve tek yönlü güvenlik duvarları kullanılması önerilmektedir (NIST SP 800-82r2,2015), (NIST SP 800-53r4,2013), (AMI,2008). Güvenlik duvarına ek olarak, yönlendirici ve diğer saldırı tespit sistemleri, VPN gibi yazılım, donanım ve ağ ürünleri kullanılmalıdır (Misbahuddin ve Al-Holou, 2012:176).

- **Saldırı Tespit ve Önleme Sistemleri (IDS):** EKS ağlarına ve bileşenlerine yönelik bilinen siber saldırıları tespit etmek üzere kullanılmaktadırlar. Ağlar için geliştirilmiş IDS ürünleri, ağ üzerindeki trafiği takip eder ve trafik bilgilerini, bilinen saldırı türlerine ait imzalar ile karşılaştırmak gibi çeşitli algılama yöntemleri kullanarak saldırıları tanımaya ve tespit etmeye çalışır. Ana bilgisayar sistemindeki saldırıların tespiti için de bu sisteme yüklenmiş bir IDS yazılımı ile olası istismarlara karşı sistem üzerindeki verileri ve devam etmekte olan olayları inceleyerek yine bilinen saldırı türlerinin imzaları ile karşılaştırarak istismarı tespit eder ve bu istismarın oluşmasını sağlayan zararlı yazılımı durdurabilecektir (NIST SP 800-82r2, 2015:E-1-E-4).

- **Veri Diyotu (Data Diode):** Dışarıdan gelebilecek saldırılara karşı EKS'nin korunmasını sağlamak üzere verilerin yalnızca tek yönlü hareketine imkân tanıyan ağ cihazlarıdır. Bu cihazlar, kritik sistemlerin güvenilmeyen ağlara bağlanması durumunda kullanılmaktadır (NIST SP 800-82r2, 2015:E-1-E-4).

- **Şifreleme (Encryption):** Veriler, sadece yetkili alıcılar tarafından çözülebilecek şekilde özel olarak tasarlanmış ve ticari olarak temin edilebilecek şifreleme ürünleri ile şifrelenerek gönderilir (NIST SP 800-82r2, 2015:E-1-E-4).

- **Antivirüs Yazılımları:** Yanıt süresi ve bellek kapasitesi üzerindeki etkisi de dahil olmak üzere otomasyon sistemlerinin sınırlamaları ve gereksinimleri dikkate alınarak virüsten koruma uygulamaları kullanılmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). Geleneksel bilişim sistemlerinde kullanılmakta olan bazı antivirüs programları, EKS üzerine kurulmaları yapılandırılmaları ve çalıştırılmaları, performans kaybı gibi birtakım zorluklar oluştursa da, virüsleri etkisiz hale getirmek üzere bu sistemler üzerinde kullanılmaktadır (NIST SP 800-82r2, 2015:E-1-E-4).

- **Kullanıcı Dostu Siber Güvenlik Teknolojilerinin Kullanılması:** Kullanışlı olmayan güvenlik önlemleri, güvenlik özellikleri olmayan bir sistemin başlangıçta güvenlik özelliği olmayan bir sisteme sonradan güvenlik özellikleri eklendiğinde daha güvenliksiz hale getirilmesi gibidir. İnsan faktörü, güvenliğin kritik bileşenlerinden biri olduğu için sistemlerin kullanışlı ve güvenlikli olması çok önemlidir (Smetters, 2014:41).

3.3.2.2 Sistem Mimari Şemasının Güncel Tutulması

Kullanımda olan PLC, IIOT RTU, sensör, aktivatör gibi otomasyon sistemi cihazlarının, bu cihazların çalışmasını sağlayan yazılımların, koruma mekanizmalarının konumlarını içeren diyagram hazırlanmalı ve güncel tutulmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). Ağ mimarisi dokümante edilmeli ve kritik hizmet veren ya da ek koruma seviyesine ihtiyaç duyulan hassas veri içeren sistemler belirlenmelidir. Etkili bir koruma stratejisi kurabilmek için sürecin bir parçası olarak güçlü bir bilgi güvenliği mimarisi geliştirilmeli ve dokümante edilmelidir. Kurumlar, ağlarını güvenliği akılda tutarak tasarlamalı ve tüm yaşam döngüsü boyunca ağ mimarilerine gereken önemi vermelidir. Risklerin uygun bir şekilde değerlendirilmesi ve yeterli koruma stratejilerinin geliştirilebilmesi için, sistemin gerçekleştirdiği işlevlerin ve saklanan verinin hassasiyetinin ayrıntılı olarak anlaşılması çok önemlidir. Tüm sistemin durmasına neden olabilecek genel hataları tanımlayabilmek ve genel koruma stratejisinin anlaşılabilmesi için bilgi güvenliği mimarisinin ve bileşenlerinin dokümante edilmesi kritik öneme sahiptir (DOE-USA,2002).

Siber uzayda kullanılmakta olan siber varlıklar ve ağ hakkında gerekli bilgiye sahibi olmak, saldırgan karşısında sahip olunan en önemli avantajlardan biridir. Güvenlik odaklı kuruluşların, kendi endüstriyel ağları üzerinde hangi siber varlıkların bulunduğu, hangi

görevi yerine getirdikleri, kimin hangi varlıkla nasıl bir etkileşimi olduğunu belgelemeleri durumunda saldırıların tespiti ve saldırı öncesi duruma dönüş çok daha kolay olacaktır (Luallen,2014:9). Cihazları, fiziksel ara bağlantılarını, mantıksal veri kanallarını ve cihazlar arasında uygulanan okuma bobinleri, yazma kayıtları, taramalar ve zaman damgaları gibi EKS protokolü davranışları bilinmeli ve eşlenmelidir (Luallen,2014:26).

3.3.2.3 Erişim Kontrolü ve Güçlü Kimlik Doğrulama

EKS'nde otomatik yanıt süresi ya da insan müdahalesi için sistem yanıtı çok kritik olduğu için bu sistemlerde bilgi akışı kesintiye uğramamalı ve yetkisiz kişilerin eline geçmemelidir. Bu sistemlere yönelik yetkisiz erişim titizlikle yapılacak fiziki kontroller ile engellenmelidir. NIST 800-82,2008 dokümanına göre (Macaulay ve Singer, 2011:85-92), (Krutz, 2006:76-77). Kritik sistem bilgilerine erişim taleplerinin yetki düzenlemeleri yapılmış olmalıdır. (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). İşletim sistemlerinin güvenliği, kısıtlayıcı kurulum ayarları ve yetkisiz müdahaleyi zorlaştırıcı sistemler kullanılarak maksimum seviyeye çıkarılmalıdır (Harp ve Gregory-Brown, 2015:19). Bu sistemlere İnternet ve diğer genel ağlar üzerinden erişimde kullanılmakta olan arayüz uygulamalarında güçlü kimlik doğrulama mekanizmaları kullanılmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008).

3.3.2.4 Sistem Veri Bütünlüğünün Korunması

Verilerin bütünlüğünü sağlamak için politikalar ve prosedürler uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). EKS için iletişim görüntüleme işlemi ve mümkün olan ortamlarda, asıl işlemde bir kesintiye sebep olmaksızın ayrıntılı paket denetimi yapılmalıdır (Harp ve Gregory-Brown, 2015:19).

3.3.2.5 Derinlemesine Savunma Yönteminin Kullanılması

Güvenlik önlemleri, fiziki çevrenin savunulmasından başlanarak ve EKS'ni tanıyan güvenlik duvarları ve izinsiz giriş algılama ve önleme sistemleri kullanılarak katmanlar halinde uygulanmalıdır (NIST SP 800-82r2,2015; ISA-62443; NIST SP 800-53r4,2013; CIS-1:11).

Bir önceki güvenlik katmanının ihlal edilmesi durumunda sonraki katmanın koruma sağlayacağı çok sayıda koruma katmanı oluşturma eylemi, derinlemesine savunmadır.

ANSI/ISA-62443-1-1(99.01.01)-20075, derinlemesine savunmayı "Bir saldırıyı engellemese de geciktirme niyetiyle, özellikle katmanlarda çoklu güvenlik koruması sağlanması." şeklinde açıklamaktadır. Bu yöntem ile saldırganların, tespit edilmeden her katmanı aşması veya atlaması durumu; bir katmandaki güvenlik açığının, diğer katmanlardaki yeteneklerle hafifletilebilmesi ve sistem güvenliğinin, genel ağ güvenliği içinde bir dizi katman haline gelmesi amaçlanmaktadır (Krutz,2017:36). Güvenlik kontrollerinin katmanlaştırılması ile derinlemesine savunma sağlanabilecektir. EKS konfigürasyon ve yönetim verilerine çoklu kontroller uygulanarak, bir tehdit aktörünün aşması gereken başka engeller devreye alınmış olacaktır. Derinlemesine savunma, katmanlı bir yaklaşımda farklı engeller (kontroller) sağlayarak tehditlerin varlıklara tek bir başarısızlık noktası üzerinden ulaşmasını engelleyecektir (Woods vd., 2017:18). Bilgi varlığına birden çok kontrol uygulanarak tehdit aktörünün üstesinden gelmesi gereken başka engeller devreye girecektir. Bu engeller, daha yetkin tehdit aktörlerinin faaliyetlerini yavaşlatacaktır. Bazı kontrolleri geçmek için gereken süre içinde, sistem takibi yapılabilecek ve saldırı konusunda uyarı oluşturacaktır. Bu sayede tehdidin devre dışı bırakılması gibi daha ileri seviye önlemler alınabilecektir. Derinlemesine savunma, katmanlı bir yaklaşım ile farklı engeller (kontroller) sağlayarak varlıklara yönelik tehditlerin tek bir noktadan giriş sağlayarak başarılı olmasını engelleyebilecektir (Maglaras vd.,2018:44).

DOE-USA'de de temelinde derinliğine savunma ilkesi yer alan bir ağ koruma stratejisinin kurulması gerektiği vurgulanmaktadır. Herhangi bir ağ koruma stratejisinin parçası olması gereken temel ilke, derinliğine savunma ilkesidir. Derinliğine savunma ilkesi geliştirme sürecinin tasarım aşamasında göz önünde bulundurulmalı ve bir ağla ilgili tüm teknik kararların alınmasında bütünleşik bir değerlendirme olmalıdır. Ağın tüm katmanlarında olabildiğince büyük ölçüde tanımlanan risklerin oluşturacağı tehditleri azaltmak için teknik ve yönetim kontrolleri kullanılmalıdır. Tüm sistemin durmasına neden olabilecek hatalardan kaçınılmalı ve herhangi bir güvenlik kazasının etkisini kapsaması ve sınırlandırması için siber güvenlik savunması katmanlı olarak uygulanmalıdır. Her katman, aynı katmandaki diğer sistemlere karşı korunmalıdır. Örneğin, içerden gelen tehditlere karşı koruma sağlamak için erişimi sadece işlerini yapmak için bu kaynaklara ihtiyacı olan kullanıcılara sınırlı erişim hakkı verilmelidir (DOE-USA,2002).

NIST SP 800-82r3 dokümanında derinlemesine savunma mimarisi, Güvenlik Yönetimi, Fiziksel Güvenlik, Ağ Güvenliği, Donanım Güvenliği, Yazılım Güvenliği olmak üzere 5 katman halinde tasarlanmıştır (NIST SP 800-82r3 ipd, 2015:66).

Luallen de, saldırganlara pivot noktalar sağlayabilecek olan savunmasız süreç kontrol sistemlerinin ve veri tabanı sunucularının derinlemesine savunma mantığı içinde korunmasını önermektedir (Luallen,2014:26).

3.3.2.6. İletişim Altyapısının Korunması

Sistem aktarım elemanlarının korunmasına yönelik yöntemler uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; CIS-1:14; AMI,2008). SCADA ağının gereksiz bağlantıları kaldırılmalıdır. SCADA sistemlerin en yüksek seviye güvenliğini sağlamak için SCADA ağı diğer ağ bağlantılarından olabildiğince izole edilmelidir. Bir başka ağa herhangi bir bağlantı özellikle İnternet bağlantısı güvenlik riskleri doğurabilecektir. Diğer ağlara doğrudan bağlantı önemli bilgilerin verimli ve uygun bir şekilde iletilmesini sağlayabilecektir. Ancak bu tarz güvensiz bağlantılar, sistemlerin güvenliği açısından önemli riskleri de beraberinde getirecektir. Gereken korumayı sağlamak için SCADA ağının izolasyonu temel hedef olmalıdır. DMZ ve veri ambarı kullanımı gibi stratejiler verinin SCADA ağlarından işlem göreceği ağlara güvenli taşınması için kullanılabilir. Stratejiler, uygun olmayan konfigürasyonlar ile ek riskler yaratmayacak şekilde tasarlanmalı ve uygulanmalıdır (DOE-USA,2002).

İnternet bağlantısı gerektiren tüm EKS ağları, çift ana bilgisayara bağlanmamış olan ve çok güvenilir olmasa da dahili bir ağda yapılandırılmış olan Proxy üzerinden bağlantı sağlanmalıdır. Bu proxy cihazı, EKS ağlarına uygulanamayan alt kontrolleri içerebilen EKS dışı güvenlik kontrollerine tabi tutulmalıdır (CIS-1:14).

EKS protokolleri (örneğin, Modbus/TCP, kimlik doğrulaması olmayan DNP3, Ethernet/IP, ProfNet, BACnet, ISO-TSAP, S7, ICCP ve benzeri sertifikalar) tasarım, yapılandırma veya satıcı uygulaması nedeniyle doğası gereği savunmasız oldukları için, iç iletişim ağına ulaşan saldırganlardan korunmalıdırlar (Luallen,2014:26). Operasyonel faaliyetlerin kritikliğine uygun olarak EKS ağı belirlenen kritiklik derecesine göre segmentlere ayrılmalı; oluşturulan ağlar birbirlerinden izole edilmeli ve erişim güvenliğine yönelik kısıtlayıcı önlemler alınmalıdır. (T.C.CBDDO,2020:179)

Dış tehditler birincil saldırı vektörü olduğu için SCADA ve EKS çalışanları, devam eden güvenlik çabalarının bir parçası olarak harici bağlantı güvenliği dikkate almalıdır (Luallen,2014:12). Gerekli durumlarda ortak ağları ve dış ağ bağlantıları en aza indirilmeli ve güvenli hale getirilmelidir (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008).

3.3.2.7 Uzaktan Erişim Yönetimi

VPN'ler gibi güçlü kimlik doğrulama ve şifreli bağlantılar kullanılarak uzaktan erişim kontrol edilmeli ve yönetilmelidir. Kablosuz cihazlara ve masaüstü modemlere özel güvenlik önlemleri uygulanmaladır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; CIS-1:17; AMI,2008).

3.3.2.8 Yalnızca Gerekli Servislerin Açık Olması

Gereksiz sistem servisleri ve kullanılmayan açık bağlantı noktaları devre dışı bırakılmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013). SCADA ağlarını gereksiz servisleri silerek ya da kullanım dışı bırakarak güçlendirilmelidir. SCADA kontrol sunucularının kurulumunda kullanılan ticari ya da açık kaynak kodlu işletim sistemleri varsayılan ağ servisleri kullanılarak saldırılara maruz kalabilir. Doğrudan saldırı riskini azaltmak için gereksiz servisler ve ağ araçları silinmeli ya da kullanım dışı bırakılmalıdır. (DOE-USA,2002)

SCADA ağı içinde arka kapı olarak kullanılan her araç için güçlü kontroller oluşturulmalıdır. SCADA sistemlerde arka kapı ya da üretici bağlantıları olduğu zaman güvenli iletişim için güçlü kimlik doğrulama sistemleri kurulmalıdır. İletişim ve bakımda kullanılan modemler, kablolu ya da kablosuz ağlar SCADA ağları ve uzak siteler için önemli güvenlik açıklarına neden olur. Başarılı saldırılar bir saldırgana diğer kontrolleri devre dışı bırakarak SCADA ağı ve kaynaklarına doğrudan erişme olanağı sağlayabilir. Bu tür saldırıların yarattığı riski en aza indirgemek için dışarıdan gelen erişimler engellenmeli ve geri arama sistemleri geliştirilmelidir (DOE-USA,2002).

3.3.2.9 Öngörülebilir Arızaların Önlenmesi

Belirli çalışma ortamlarında kritik bileşenler için ortalama arıza süresini dikkate alarak bilgi sistemini zarardan koruyan kontroller uygulanmalıdır (NIST SP 800-53r4,2013;

AMI,2008). Olası saldırı senaryolarını tanımlamak ve değerlendirmek için Acil Ekipler kurulmalıdır. Potansiyel saldırı senaryolarını tanımlamak ve potansiyel sistem güvenlik açıklarını değerlendirmek için, projelerin, çözüm önerilerinin, yaklaşımların bağımsız değerlendirmesini yapan uzmanlar grubundan oluşan bir ekip kurulmalıdır. Bu ekip, tüm ağın, SCADA sistemlerin, fiziki sistemlerin ve güvenlik kontrollerinin güvenlik açıklarına ışık tutmasını sağlayacak farklı nitelikteki kişilerden oluşmalıdır. Kurum için en büyük risklerden biri olarak gösterilen kötü niyetli çalışanlardan kaynaklanan riskler de değerlendirilmelidir. Risk yönetimi sürecinde bilgilerin değerlendirilmesi ve uygun koruma stratejilerinin kurulmasında bu ekibin değerlendirmeleri kullanılmalıdır (DOE-USA,2002).

EKS'nde kontrol sistemleri, sürecin sonunu kontrol etmekten doğrudan sorumlu oldukları için dikkatli bir şekilde korunmalıdır. Kontrol sistemlerini etkilediği için merkezi sunucunun doğru çalışıyor olması da önemlidir. NIST 800-82 dokümanına göre (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77). EKS'nin öngörülebilir donanım arızaları dikkate alınmalı ve gerekli bakım, yedekleme işlemleri ihmal edilmemelidir.

3.3.3 Operasyonel Kontroller

Görevlerini, politikalar ve standartlara uygun bir şekilde yerine getirmek zorunda olan operatörlerin, teknisyenlerin ve diğer personelin iş yapma yöntemleri için operasyonel kontroller kullanılmaktadır. Bu kontroller, kalite ve zaman çizelgelerine uyum; değişiklikleri, hataları, kusurları ve ihmalleri azaltmak üzere genelleştirilmiş rehberleri kapsamalıdır. Çok özel ölçümleri ve ayrıntılı iş adımlarını içerebilen operasyonel kontroller, yönetim kontrolleri aşamasında oluşturulmuş politikaları uygulamalıdır (Macaulay ve Singer, 2011:165-166).

3.3.3.1. Risk Yönetimi

Potansiyel etkiler, olasılıklar ve azaltma seçenekleri dahil olmak üzere sistemlere yönelik riskler belirlenmelidir. (NIST SP 800-53r4,2013; AMI). Risk yönetimi yaklaşımı kapsamında, EKS'nin tüm bağlantıları tanımlanmalıdır. EKS ağının her bağlantısının gerekliliğini ve risklerini değerlendirmek için ayrıntılı bir risk analizi yapılmalıdır. Tüm bağlantıların nasıl daha iyi korunacağı konusunda kapsamlı bir anlayış geliştirilmelidir. Her türlü bağlantının, yerel alan ağı mı yoksa geniş alan ağı mı olduğu belirtilmeli; İnternet

bağlantısı, uydu uplinkleri dahil kablosuz ağ cihazları, modem ya da çevirmeli ağ bağlantıları tanımlanmalı; iş ortaklarına, üreticilere ya da düzenleyici kuruluşlara olan bağlantılar açıklanmalıdır (DOE-USA,2002).

Titiz ve süreklilik arz eden bir risk yönetim süreci kurulmalıdır. Etkili bir siber güvenlik programı için DDOS saldırıları ve hassas verilerin güvenlik açıklarından bazı riskli durumların kabul edilmesine bilişim sistemlerinin risklerinin iyice anlaşılması şarttır. Ağ güvenliğinin korunmasına yönelik strateji geliştirebilmek için öncelikle mevcut tehditlere yönelik bir risk analizi yapılmalıdır. Teknolojinin hızla değişiyor olmasına ve her gün yeni tehditlerin gündeme gelmesine rağmen koruma stratejisinin etkisini sürdürmek için rutin değişiklikler yapılmalı ve sürekli bir risk değerlendirme süreci gerçekleştirilmelidir (DOE-USA,2002).

Kurumsal yapıların, mevcut güvenlik düzenlemelerine uygunluklarını hazır kontroller aracılığı ile gözden geçirmenin yanı sıra uygulamaya çalıştıkları güvenlik önlemlerini iyileştirerek riski azaltmaya yönelik çalışmalara da önem vermeleri gerekmektedir (Luallen,2014:27).

EKS'nin emniyeti ve güvenliği için yönetim politikaları oluşturmak, mevcut en son bilgilere dayalı bir risk değerlendirmesi oluşturmak, olayların açık raporlanmasını sağlamak, risk farkındalığını sağlamak, sistemleri izlemek, esnekliği sağlamak ve hem olasılığı azaltmak hem de olayların sonuçlarını azaltmak önemlidir (Johnsen,2013:289).

3.3.3.2 Fiziksel Güvenliğin Sağlanması

EKS cihazları mümkün olduğunca, yetkisiz erişimi önleyen yerlerde kurulmalı, yedek enerji, yangın algılama ve önleme, fiziksel erişim kontrolleri, kameralar, rozetler ve belirteçler dahil olmak üzere fiziksel güvenlik kontrolleri uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008) Güvenlik değerlendirmesi için EKS ağına bağlı tüm uzak alanlar belirlenmeli ve fiziki güvenlik araştırmaları yapılmalıdır. EKS ağına bağlı herhangi bir konum, özellikle insansız ve korunmasız olan uzak alanlar saldırganlar için hedeftir. Bu sistem ile bağlantısı olan tesisteki erişim noktalarının envanteri oluşturulmalı ve fiziki güvenlik araştırmaları yapılmalıdır. Telefon, bilgisayar ağları, fiber optik gibi dağıtılabilen kablolu bağlantıları, saldırıya açık radyo ve mikro dalga bağlantıları, erişilebilen uçlar ve kablosuz yerel alan ağları erişim noktalarını kapsayan tüm bilgi

kaynakları tanımlanmalı ve değerlendirilmelidir. Tüm sistemin durmasına neden olabilecek durumlar tanımlanmalı ve devre dışı bırakılmalıdır. Site, yetkisiz erişimi saptamak ve önlemek için yeterli güvenliğe sahip olmalıdır. Sadece kolaylık sağlamak için yeterli güvenlik önlemleri alınmayan uzaktaki sitelere ağ erişim izni verilmemelidir. (DOE-USA,2002). Kuruluşun sahip olduğu sistemleri ve bu sistemler arasında nasıl iletişim kurulduğunu belirlemek için tüm sistemlerin envanteri çıkarılmalı, izlenmeli ve bu sistemlere erişim, yetki bazında kısıtlanmalıdır. Bu konuda gerekli altyapıya sahip kuruluşlar, olağan dışı faaliyetleri rahatlıkla izleyebilecek ve konu ile ilgili yeterli eğitime sahip personel, önceden tanımlanmış olay müdahale prosedürlerini yürüterek siber olayların sonlandırılmasını ve olay öncesi normal duruma dönüşü sağlayabilecektir (Luallen,2014:22).

3.3.3.3 Güvenlik Farkındalık Eğitimleri

EKS güvenliği konusundaki farkındalık ve eğitim seviyesi düşüktür (Macaulay ve Singer, 2011:85-92; Krutz, 2006:76-77) Bu nedenle, kurum çalışanlarında farkındalık oluşturmak üzere sosyal mühendislik ve kimlik avı gibi konularda güvenlik eğitimleri verilmelidir. Ayrıca, bir siber olayın meydana gelip gelmediğinin nasıl belirleneceği, meydana gelmesi durumunda kime bildirileceği ve bu olayda yapılması gerekenler konusunda da bilgilendirilmelidirler (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008) SCADA sistemlerin tasarım, işlem ve güvenlik kontrollerine ilişkin hassas bilgilerin kurum çalışanları tarafından farkında olmadan ifşa edilmesi olasılığını en aza indirgemek üzere politikalar ve davranış eğitimleri oluşturulmalıdır. SCADA ağlarına ilişkin veriler, sadece bilmesi gereken prensibine göre sadece bu bilgileri almaya yetkili kişilere açıktır. Bir bilgisayar ya da bilgisayar ağındaki bilgilerin genellikle sorular sorularak edinilmesi olarak açıklanabilecek olan sosyal mühendislik yöntemleri kullanılarak edinilmesi bilgisayar ağına yapılan kötü niyetli saldırının ilk adımıdır. Bir bilgisayar ya da bilgisayar ağı ile ilgili ne kadar bilgi ortaya çıkarsa o bilgisayar ya da bilgisayar ağı daha çok güvenlik açığına sahne olur. Sistem operatörlerinin ve yöneticilerin isim ve iletişim bilgileri SCADA ağlarına ilişkin veriler, bilgisayar işletim sistemleri ve bilgisayarların fiziki ve mantıksal konumları, telefonla ya da elemanlara açıklanmamalıdır. Tanınmayan kişiler tarafından talep edilen bilgiler merkezi bir ağ güvenlik konumuna doğrulama amaçlı olarak

gönderilmelidir. Personelin hassas ağ verilerinin özellikle kendi şifrelerinin korumasını sağlamak için eğitimler düzenlenmeli ve farkındalık oluşturulmalıdır. (DOE-USA,2002). Çalışanlara, güvenlik süreçlerini doğru uygulayabilmeleri için konu ile ilgili eğitimler verilmelidir (Harp ve Gregory-Brown, 2015:19; Luallen,2014:26).

3.3.3.4 Varsayılan Hesapların Kullanım Dışı Bırakılması

Otomasyon sistemi üreticileri tarafından, bakım veya sistem erişimi için üretim aşamasında oluşturulan varsayılan hesaplar, sistemin kullanıma girmesini müteakip silinmeli ve varsayılan şifreler değiştirilmeli veya ortadan kaldırılmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008).

3.3.3.5 Denetim Prosedürlerinin Uygulanması

Kullanılmakta olan güvenlik kontrollerinin yeterliliğinden ve uyumluluğundan emin olmak için denetim kayıtları, bağımsız kuruluşlar tarafından değerlendirilmelidir (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). Kendi kendini değerlendirme yordamı çalıştırılmalıdır. Kurumlara siber güvenlik politikaları ve teknik uygulamaların etkisi ile ilgili geribildirim sağlanması için güçlü performans değerlendirme süreçleri gereklidir. Gelişmiş bir kurum olmanın işaretlerinden biri, kendi işlemlerini tanımlayabilmek, temel neden analizlerini gerçekleştirmek ve etkili düzeltici eylemlerin uygulanmasını sağlamaktır. Etkili bir siber güvenlik programının bölümlerinden olan kendi kendini değerlendirme süreçleri, güvenlik açıkları için sürekli tarama, ağın otomatik olarak takibi ve örgütsel ve bireysel performansın kendi kendini değerlendirmesini kapsamaktadır. (DOE-USA,2002). Yazılım ve donanımlar için yaptırılacak tarafsız üçüncü taraf güvenlik değerlendirmeleri sonrası güvenlik açıklarının bulunması halinde bu açıkların siber güvenlik olaylarına neden olmasını önlemek için iyileştirme planları ve ilerleme raporları hazırlanmalıdır (Harp ve Gregory-Brown, 2015, s:19).

3.3.3.6 Kritik Verilerin ve Kritik Ortamın Korunması

Korunması ve felaket kurtarma planlamasına dahil edilmesi gereken kritik sistem öğeleri tanımlanmış olmalıdır. Bu ögeler, kullanım, depolama, iletim ve imha dahil yaşam döngülerinin tüm aşamalarında korunmalıdır. Kritik verilerin şifreleme işlemi, güvenlik ilkelerine göre uygulanmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; CIS-

1:15; AMI,2008). Veri manipülasyonunu önlemek üzere EKS ağı izlenmeli ve gerekli önlemler alınmalıdır (T.C.CBDDO,2020:179).

3.3.3.7 Sistem Günlüğünün Uygulanması

Acil bir durumda kritik sistemlerin performansını belgelemek için analiz edilmek üzere, günlük log kayıtları aktif duruma getirilmeli ve çalışma sahasından uzakta saklanmalıdır. (Johnsen,2013:289). Endüstriyel kontrol sistemlerinin çalışma prensiplerine uygun olarak kritik sistem parametreleri kayıt altına alınmalı ve belirli zaman aralıklarında gözden geçirilmelidir (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; CIS-1:9; AMI,2008). Eylem gerçekleştikten sonra denetim kayıtları ve takip yöntemleri BT sistemleri için yararlı yöntemler olup EKS için de benzer faydaları sağlayabilecektir. Sistemin yerine getirmesi gereken temel faaliyete dayalı olarak cihaz günlüğü, sıkı değişiklik yönetimi ve günlük analizi otomasyonu etkinleştirilmelidir (Laullen, 2014:26). Ancak daha eski yıllarda üretildikleri için ve karmaşık tasarımlarından dolayı EKS'nin çoğunun bu özelliği bulunmamaktadır. Güvenlik açıklarını azaltmak için tüm yük seviyelerinin log kayıtları oluşturulmalı, sistemin esnekliği geliştirilmeli ve ağdaki istenmeyen yük, penetrasyon ve diğer dış etkenleri azaltmak için bariyerler oluşturulmalıdır.

3.3.3.8 Konfigürasyon Yönetimi

Herhangi bir sistem donanımı ve yazılım değişikliğini belgeleyen konfigürasyon yönetimi uygulamaları kullanılmalıdır (NIST SP 800-82r2,2015; NIST SP 800-53r4,2013; AMI,2008). Etkili bir yapılandırma yönetimi süreci kurulmalıdır. Güvenli bir ağın bakımını yapabilmek için gerekli temel yönetim süreci, konfigürasyon yönetimidir. Konfigürasyon yönetimi yazılım ve donanım konfigürasyonlarını kapsamaktadır. Yazılım ya da donanımdaki değişiklikler ağ güvenliğini tehlikeye atacak güvenlik açıklarına sebep olabilir. Ağın güvenlikli kalmasını sağlamak için herhangi bir değişikliğin kontrolüne ve değerlendirmesine ihtiyaç vardır. Konfigürasyon yönetimi, farklı sistemler için iyi test edilmiş ve dokümantasyonu sağlanmış güvenlik tabanları ile başlar. (DOE-USA,2002; CIS-1:13).

3.3.3.9 Yedekleme İşlemi

Yedeklilik, bir siber olay sonrasında sistemin bozulması ya da faaliyetin durması halinde devreye alınabilecek yedek sistem veya sistemler aracılığıyla çalışmaya devam etme yeteneğidir. Kritik altyapıların siber güvenliğine yönelik yönetimsel, operasyonel ve teknik güvenlik açıkları arasında sayılan yedekliliğin bulunmaması durumunun giderilmesi gerekmektedir. EKS'nin önemli bileşenleri periyodik olarak yedeklenmeli ve yeniden başlatılmalıdır (Misbahuddin ve Al-Holou, 2012:176). Sistemlerin değişiklik ve yıkımdan korunması için yedeklemeler yapılmalı, tüm yapılandırmaları ve cihaz donanım yazılımını doğrulamak için gerekli prosedürler oluşturulmalı ve bu prosedürlere uygun yedeklemeler yapılmalıdır (Luallen,2014:26). EKS'nin çalışması için gerekli olan enerji ve diğer kritik yazılım, donanım ve ağ bileşenleri yedeklenerek sistemler değişiklik veya yıkımdan korunabilecektir. Yedeklemeler yapılarak, sistemlerin değişiklik veya yıkımdan korunması; tüm yapılandırmaları ve cihaz donanım yazılımını doğrulamak için prosedürler oluşturulması gerekmektedir.

3.4. KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK OPERASYONEL FAALİYETLERİN DEĞERLENDİRİLMESİ

Bu çalışma kapsamında kritik altyapıların siber güvenliği operasyonel seviyede ve stratejik seviyede ele alınmıştır. Operasyonel seviyede siber güvenlik faaliyetleri bu sistemlerle doğrudan teması olan bireyler ve kurumsal yapılar tarafından yürütülen faaliyetlerdir. Çoğu kez birlikte ve birbirlerini tamamlayıcı mahiyette kullanılması gereken siber güvenlik yaklaşımlarından önleyici koruyucu güvenlik yaklaşımı ve risk yönetimi yaklaşımlarının bu faaliyetlerde yoğun olarak kullanıldığı anlaşılmaktadır.

Hizmetlerini EKS kullanarak yerine getirmekte olan kritik altyapılarda beklenmeyen bir siber güvenlik olayı sonrasında meydana gelebilecek ve önemli çevre felaketlerine neden olabilecek hasarın kapsamını sınırlamak; bu siber olayın neden olabileceği hizmet kesintisinin süresini olabildiğince azaltmak; beklenmeyen siber olayın meydana gelmesinden önceki duruma tam olarak dönülemese de yeni duruma uyum sağlamak ve zaman içinde sistemlerin faaliyetlerinde iyileştirme sağlayabilmek için önleyici/koruyucu güvenlik yaklaşımının, bu sistemlerin tüm yaşam döngüsü boyunca uygulanılması

kaçınılmazdır. Önleyici-koruyucu güvenlik yaklaşımı, operasyonel faaliyetlerin gerçekleştirildiği bireysel ve kurumsal seviyede ele alınması ve uygulanması gereken temel faaliyetleri kapsamaktadır. Bu tarz operasyonel faaliyetlerin gerçekleştirilebilmesi için, gerekli politikaların kurumsal, ulusal ve çoğu durumda da küresel seviyede belirlenmiş ve kabul edilmiş politikalar olması ve desteklenmesi şarttır.

Kritik altyapılarda kullanılmakta olan EKS'nin BT ve OT'in bir arada kullanılmaya başlanması ve bu sistemlerde yaşanmakta olan başdöndürücü gelişmeler sonucu sistemlerin gittikçe karmaşıklaşması, bağlantıların ve kullanıcıların artması, buna paralel olarak bilgili siber saldırganların sayısının artması gibi nedenlerle bu sistemler için önleyici/koruyucu güvenlik önlemleri yetersiz kalmakta ve mutlak bir siber güvenliğin sağlanması mümkün olamamaktadır.

Sistemlerin tüm güvenlik açıklarının kapatılamayacağı; güvenliğe yapılacak yüksek miktardaki yatırımların sonuçta önlenecek saldırıdan kaynaklanan zarara değmeyeceği; karşılaşılabilecek risklerin oluşturacağı hasarın kurumsal yapıya, verilen hizmetin niteliğine ve hizmetin verildiği hedef kitleye göre de değişebileceği göz önünde bulundurularak risklerin belirlendiği, değerlendirildiği, önemine binaen gerekli önlemlerin alındığı risk yönetimi yaklaşımı kullanılmaya başlanmıştır. Risklerin çeşitli kontrollerle azaltılamaması durumunda kritik süreçlerin saldırı yüzeyleri hızla büyümeye devam edeceği için bireysel ve kurumsal seviyede risk yönetimi döngüsü belirli aralıklarla uygulanmalıdır.

Kritik altyapıların siber güvenliğini sağlamakta çoğu kez önleyici/koruyucu güvenlik yaklaşımı ile birlikte kullanılmakta olan risk yönetimi yaklaşımı, bireysel ve kurumsal seviyede operasyonel faaliyetler gerçekleştirilirken uygulanmakta, ulusal ve küresel seviyede ise bu yaklaşıma yönelik politikalar oluşturulmakta ve kullanımları desteklenmektedir.

Dördüncü Bölümde, kritik altyapıların siber güvenliğinin sağlanmasına yönelik politika ve stratejilerin belirlendiği ve uygulamanın desteklendiği stratejik siber güvenlik faaliyetlerinin nasıl olması gerektiği araştırılacaktır.

DÖRDÜNCÜ BÖLÜM

KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK STRATEJİK FAALİYETLER

Günümüzde, işlevlerini yerine getiremedikleri ya da yanlış sonuçlar ürettikleri durumlarda toplumsal kaos, can ve mal kaybına neden olabilecek kritik altyapı sistemleri çok hızlı bir şekilde siber uzaya dahil olmaya başlamış ve siber güvenlik olaylarından etkilenebilir duruma gelmişlerdir. Bu sistemlerin bir siber güvenlik olayına maruz kalması durumunda önemli çevre sorunlarının oluşabileceği, gelecek nesillerin de en az günümüzdeki doğal kaynaklar ve çevre koşullarına sahip olarak varlıklarını sürdürebilmeleri anlamına gelen sürdürülebilirliği engelleyebilecektir.

Tezin temel araştırma sorularının ikincisi olan "Sürdürülebilirliğin sağlanması için siber güvenlik alanında ne tür faaliyetler gerçekleştirilmelidir?" sorusuna yanıt aramak üzere Üçüncü Bölümde, sürdürülebilirlik açısından hayati önem taşıyan kritik altyapıların siber güvenliğinin sağlanmasına yönelik bireysel ve kurumsal seviyedeki siber güvenlik faaliyetleri operasyonel faaliyetler olarak tanımlanmıştır. Operasyonel faaliyetler bireysel ve kurumsal seviyede incelenmiş; bu faaliyetlerin önleyici koruyucu yaklaşım ve risk yönetimi yaklaşımları kullanılarak gerçekleştirilmekte olduğu görülmüş; bireysel etik davranışın önemi üzerinde durulmuş ve kurumlar tarafından gerçekleştirilmekte olan siber güvenlik denetimleri ele alınmıştır.

Bireyler ve kurumlar tarafından gerçekleştirilmesi gereken operasyonel siber güvenlik faaliyetlerinin uluslararası kuruluşlar ve çok uluslu şirketler tarafından geliştirilmiş belirli standartlara ve rehber dokümanlara uygun olarak yürütmekte oldukları görülmüştür. Kritik altyapıların siber güvenliğine yönelik politika ve stratejilerin, standartların nasıl hazırlandığı, neleri kapsadığı konularına bu bölümde yer verilmiştir. Bu amaçla öncelikle devletler seviyesinde ve küresel seviyede, sistemlerin emniyeti ve sağlamlığını da kapsayan önleyici-koruyucu yaklaşımın ve risk yönetimi yaklaşımının operasyonel seviyede kullanılmasının desteklenmesine ek olarak doğrudan devletler ve uluslararası kuruluşlar

tarafından uygulanabilecek olan caydırıcılık yaklaşımı ve kamu siber güvenlik yaklaşımı açıklanacak; daha sonra devletler seviyesinde siber güvenlik stratejilerinin hazırlanması ve yönetişim mekanizmasının uygulanması faaliyetleri incelenecek; devletler seviyesinde gerçekleştirilmekte olan stratejik siber güvenlik faaliyetleri kapsamında Türkiye'deki siber güvenlik dokümanları yeterlilikleri ve çevresel sürdürülebilirliği ele alıp almadıkları açısından incelenecektir. En son aşamada ise küresel seviyede uygulanacak siber güvenlik yönetişimi üzerinde durulacaktır.

4.1 STRATEJİK SEVİYEDE SİBER GÜVENLİK YAKLAŞIMLARI

Kritik altyapıların siber güvenliğinin operasyonel seviyede sağlanması için bireyler ve kurumlar tarafından gerçekleştirilmekte olan faaliyetlerin neler olacağının belirlendiği politikalar ve stratejiler, devletler ve küresel seviyede uluslararası kuruluşlar vb. tarafından belirlenmektedir. Üçüncü bölümde, operasyonel seviyede daha yoğun olarak kullanılmakta olan önleyici koruyucu yaklaşım ve risk yönetimi yaklaşımı açıklanmıştır. Stratejik seviyede, devletlerin faaliyetlerinde ve küresel faaliyetlerde de önleyici koruyucu yaklaşım ve risk yönetimi yaklaşımı desteklenmekte ve kullanımı önerilmektedir Kritik altyapı sistemlerinin faaliyetlerinin otomasyonu için kullanılmakta olan endüstriyel kontrol sistemlerinin faydalarını en üst seviyeye çıkarabilmek; güvenlik sorunlarını en aza indirgeyebilmek ve bu sistemlerin emniyetini ve dayanıklılığını sağlamak üzere etkili bir şekilde yönetilmeleri gereklidir (Tanczer,2019:38). Bu etkili yönetim, kritik altyapıların, sınırları içinde konuşlandığı devletlerin güvenliği açısından da büyük önem taşımaktadır. Devletler seviyesinde siber güvenliğin sağlanmasına yönelik politikaların, stratejilerin belirlendiği ve yayımlandığı ulusal siber güvenlik stratejilerinde, devletlerin koruyucu önleyici güvenlik yaklaşımı kapsamında, ilgili paydaşları kritik altyapı sistemlerinin emniyeti ve sağlamlığını sağlamaya ve derinlemesine savunma yöntemlerini kullanmaya teşvik etmesi önem arz etmektedir.

Stratejik seviyede, bu yaklaşımlara ek olarak aşağıda açıklamalarına yer verilen caydırıcı siber güvenlik yaklaşımı ve kamu siber güvenlik yaklaşımı da kullanılmaktadır.

4.1.1 Caydırıcılık Yaklaşımı

Genel anlamda caydırıcılık, askeri güç kullanılarak misilleme yapılacağı tehdidi ile bir rakibin istenmeyen hareketinin önlenmesi ve istenilen şekilde davranmaya ikna edilmesi amacı ile kullanılmakta olan siyasi ve askeri kontrol ve güç unsurlarını kapsayan bir strateji türüdür (Taddeo,2017:343). Düşman faaliyetlerini engellemeyi amaçlayan caydırıcılık, nükleer çağ olarak adlandırılan soğuk savaş döneminin temel stratejisi olmuştur. Tehditlere dayanan caydırıcılık, savunmaya göre daha ucuz bir yöntemdir. Aktörlerin bir eylemin olası maliyetlerini ve getireceği faydaları tartacak nitelikte akılcı hareketlerde bulunduğunu varsayan caydırıcılık stratejisinde, düşmanı, saldırganlığının maliyetinin ulaşılacak sonuçtan daha yüksek olacağına ikna etmek temel faaliyettir (Mansbach ve Taylor,2018:471). Caydırıcılık ABD ve SSCB arasında soğuk savaş döneminde nükleer caydırıcılık olarak yoğun bir şekilde kullanılmıştır.

Siber caydırıcılık, siber ortamda siber saldırganların saldırı ve tehdit oluşturma yeteneğine sahip olunarak saldırı yeteneklerinin geliştirilmesi ile onların saldırganlıklarının önüne geçilmesi ve engellenmesidir (Meral, 2015:24).

Siber uzayda düşmanca bir siber saldırıya yönelik caydırıcılığın mümkün olup olmadığı konusu bilim insanları tarafından farklı değerlendirilmektedir. Birinci grup, siber uzayın pek çok özelliğinin geleneksel alanlarla ortak nitelikler taşıdığını ve siber caydırıcılığın da geleneksel caydırıcılıkta olduğu gibi normlar ve uluslararası anlaşmalar, daha iyi siber güvenlik ve cezalandırma mantığı ile başarılabileceği ve kimi zaman da başarısız olunabileceğini belirtmektedir. İkinci grup, siber uzayın doğası gereği geleneksel alanlardan farklı olduğu için siber caydırıcılığın da benzersiz konuları kapsadığını düşünmektedir. Siber caydırıcılığın uygulanabileceğini düşünmekte olan her iki grup da,

- Siber güvenlik önlemlerinin artırılması ile kötü niyetli saldırganın maliyet fayda analizi yapmasını sağlayarak ağ etkisini azaltması yolu ile saldırıdan cayma ya da saldırganı durdurmaya zorlayabileceğini;
- Ceza yoluyla, saldırganın eylemlerinin sonucunda ortaya çıkacak maliyeti fark etmesi ve cesaretinin kırılması ile eylemi yapmaktan vazgeçirilebileceğini;
- Devletler arası karşılıklı bağımlılığın devletler arası çatışmayı azaltabileceğini;

- Siber uzayda devletlerin davranışlarını düzenleyecek ve zamanla kötü davranışı genel bir kısıtlama ilkesine dönüşecek norm ve kuralların oluşturulmasına odaklanan gayrı meşrulaştırma yoluyla caydırıcılığın işlev kazanacağını düşünmektedirler.

Üçüncü grup ise, siber uzayın benzersiz özelliklerinden dolayı siber caydırıcılığın mümkün olmadığına inanmakta ve caydırıcılık yerine farklı bir yöntem ve stratejinin uygulanması gerektiğini savunmaktadır (Soesanto ve Smeets,2020:391-394).

Günümüz dünyasında caydırıcılık, devletlerin karşı karşıya olduğu bazı tehditlerle başa çıkmak için pek uygun değildir. Tehditler daha yaygın hale geldiği için hangi tarafın caydırılması gerektiği her zaman net olmamaktadır. Caydırıcılık, maliyet ve fayda değerlendirilmesini dikkatli bir şekilde yapabilen rasyonel, siyasi-askeri bir strateji ve aynı zamanda psikolojik bir stratejidir. Bu kararı verebilecek devletlerin rasyonel davranmama, kendi halklarını tehlikeye atma olasılıkları da bulunmaktadır. Son zamanlarda ulus devletler arası çatışmalar yerine devlet içindeki ayrılıkçı gruplar ya da ulus ötesi aktörlerin oluşturduğu, rasyonel davranmayan terörist gruplarla çatışmalar yaşandığı için caydırıcı nitelikte misilleme yapma olanağı bulunmamaktadır. Saldırganların tespit edilmesi bile oldukça zor bir duruma gelmiştir. Günümüzdeki tarafların gücünün ve kullandıkları silahların asimetrik olduğu düzensiz savaş olarak adlandırılan ölümcül çatışmaların çoğunluğu caydırıcılık için uygun değildir (Mansbach ve Taylor,2018:475).

Siber caydırıcılık yaklaşımı uygulanırken, daha az sayıda insan ile daha etkili siber tehditler oluşturulabileceği, esas olanın bilgi olduğu; kullanılacak olan cihazların ve donanımın ucuz olduğu ve asıl ihtiyacın caydırıcılık uygulanacak tarafların zekası olduğu; günlük hayatın her alanında ileri teknolojileri kullanan modern toplumların siber güvenlik ihtiyaçlarının daha çok olacağı; siber saldırıların birbirini takip eden modüler saldırılar şeklinde yapılabileceği; siber saldırganların kendi kimliklerini gizleyebilecekleri ya da konu ile ilgisi olmayanları asıl saldırganmış gibi gösterebilecekleri akıldan çıkarılmamalıdır (Gaycken ve Martellini,2013:3-4).

Siber saldırıları azaltmakta kullanılabilecek caydırıcılığın bir türü de bir siber olay gerçekleştiğinde, bu olaya neden olan saldırıların suç niteliğinde kabul edilerek faillerin tespit edilmesi ve cezalandırılmalarına yönelik önlemlerin alınmasıdır. Kritik bilgi ve iletişim sistemlerine, bilişim teknolojileri kullanılarak halkta korku, panik oluşturma yoluyla

siyasi liderlere taleplerini kabul ettirmek gibi amaçlarla gerçekleştirilen ve siber terörizm olarak adlandırılan saldırıların aynı devlet ya da birlik içinde yer alan kişiler ve gruplar tarafından gerçekleştirildiğinin tespit edilmesi ve bu saldırılara yönelik hukuki kuralların bulunduğu durumlarda ceza verme yöntemi ile siber caydırıcılık gerçekleştirilebilecektir. Ancak bu saldırganların ülke sınırları dışından olduğu ya da devletler arasındaki siber savaşın gerçekleştiği durumlarda caydırıcılık için daha çok uluslararası kuralların kullanılması gerekecektir. Siber saldırıların, ulusal hukuk kurallarının geçerli olmadığı ulusal sınırlar dışından gerçekleştirilmesi, saldırganın kim olduğunun mevcut olanaklarla net bir şekilde anlaşılamaması caydırıcılığın uygulanmasını zorlamaktadır.

Devletler, siber uzayda çok taraflı kurumlar ve ikili anlaşmalar yoluyla düşmanları daha fazla siber saldırı düzenlemekten caydırmaya çalışmaktadır ancak birkaç istisna dışında siber uzaydaki caydırıcılık çok başarılı bir yöntem olamamıştır (Brantly ve Puyvelde,2018:390).

Siber caydırıcılıkta kullanılan maliyet-fayda analizi, ham girdilerin kavramsallaştırılmasında kullanılabilmektedir ancak siber saldırıların yarattığı psikolojik etki yanında bu analizin hiçbir önemi yoktur. İran'ın Natanz bölgesindeki nükleer tesislere yapılan Stuxnet saldırısında kullanılan istismarlar, İran'ın siber uzayının güvenliğini sağlamak için üstlendiği savunma maliyetlerinden ve bir kez hasar oluştuğunda bu tesislerin onarılması için gerekli maliyetten çok daha fazladır. (Brantly ve Puyvelde,2018:388-390).

Yukarıdaki açıklamalardan da anlaşılacağı üzere, caydırıcılık yaklaşımı daha çok devletler seviyesinde kullanılabilecek bir yaklaşımdır.

4.1.2 Kamu Siber Güvenlik Yaklaşımı

Mulligan ve Schneider, tüm zafiyetlerden arındırılmış tam güvenlikli bir sistemin olamayacağı; güvenlik açıkları, riskler ve ortaya çıkabilecek iç ve dış tehditler hakkındaki eksik bilgiden dolayı risk hesaplamanın zorluğu; saldırganın tespit edilmesindeki zorluklar gibi etkenleri göz önünde bulundurarak dördüncü yaklaşım olan Kamu Siber Güvenliği yaklaşımını önermektedirler: Siber güvenliğin, çoğunluğun ortak faydası için gerçekleştirileceğinden hareketle kamu yararı niteliği taşıdığı ve önemli bir ihtiyaç olduğu vurgulanmaktadır (Mulligan ve Schneder, 2011:74). Kamu siber güvenlik yaklaşımı,

bireysel, kurumsal ve ulusal seviyede ve daha da ileri gidilerek küresel seviyede kullanılabilecek siber güvenliğin sağlanmasına yönelik bir düşünce tarzıdır.

Cavelty de siber güvenlik sorununa çözüm için uygun teknik koruma mekanizmaları yerine ekonomik ve pazar açısına odaklanıldığını gündeme getirmekte ve bu açıdan ele alındığında İnternetin güvensizliğinin çevre kirliliği ile karşılaştırılabilir olduğunu ve siber güvenliğin aslında kamu yararı için sağlanması gereken bir olgu olduğunu savunmaktadır (Cavelty, 2008: 141).

Kritik altyapıların faaliyetlerini yerine getirmesini sağlayan endüstriyel kontrol sistemlerine yönelik siber güvenlik olaylarının önemli çevre sorunlarına, toplumsal felaketlere neden olduğu ve olabileceği anlaşılmaktadır. Kamu siber güvenlik yaklaşımında bu toplumsal felaketleri önlemek düşüncesi ile hareket edilmesi öngörülmektedir. Burada bahsedilen kamu ya da toplum kimlerden oluşmaktadır diye bakıldığında, Vallor ve Revak bu soruyu basit bir şekilde 'kamu herkestir' şeklinde açıklamaktadır. Kamu diğer deyişle toplum, dünyanın her yerinde yaşamakta olan aileler, dostlar, mesai arkadaşları, işverenler, komşular, hemşehriler, vatandaşlar, kadınlar gibi farklı biçimde tanımlanabilecek insanlardan oluşmaktadır. Herkese yönelik güvenlik önlemleri alınması, bu alanda görevli siber güvenlik elemanlarının çocuklarını, ailelerini, dostlarını, vatandaşlarını da kapsadığı düşünüldüğünde daha anlamlı hale gelmektedir (Vallor ve Rewak,2018:30). Gelecek nesillerin de en az bugünkü olanaklara sahip olarak yaşamlarını devam ettirebilmeleri için sürdürülebilirlik kavramına uygun olarak siber güvenlik faaliyetlerinin sürdürülmesi, bu alanın her seviyesinde görev yapmakta olan bireyler için işin anlamlı hale gelmesine yardımcı olacaktır.

Kamu siber güvenlik yaklaşımına uygun olarak çoğunluğun ortak faydası için kamu yararı niteliği göz önünde bulundurulsa da teknik olarak yine ilk üç yaklaşımın devre dışı bırakılması mümkün değildir. Günümüzde kullanılmakta olan bilişim sistemlerinin teknolojik karmaşıklığı, kullanım amaçlarının ve ürettikleri hizmetlerin çeşitliliği; kullanıcıların farklı seviyelerdeki teknik bilgi ve becerisi, hassasiyeti; siber saldırganların teknik bilgilerindeki ve motivasyonlarındaki farklılıklar; saldırılardaki çeşitlilikler gibi nedenlerle günümüz siber dünyasında siber güvenliğin bu yaklaşımlardan sadece biri kullanılarak sağlanması mümkün görünmemektedir.

Tek başına çok anlamlı olmayan bu yaklaşım, bireysel ve kurumsal seviyede motive edici, ulusal ve küresel seviyede ise politikaların oluşturulmasında yararlanılabilecek bir düşünce tarzıdır.

4.2 DEVLETLERİN STRATEJİK SİBER GÜVENLİK FAALİYETLERİ

Geleneksel güvenlik anlayışına göre devletler, kendi fiziki sınırları içinde yer alan tüm varlıklarını koruyabilecekleri emniyetli ve güvenilir bir ortamı, kendi hukuki düzenlemelerini kullanarak tesis etmeyi hedeflemektedir. Ancak teknolojideki hızlı gelişme ve aynı hızla günlük hayata dahil olması nedeni ile bu teknolojilere yönelik mevzuat henüz tam olarak geliştirilememiştir. Özellikle nesnelerin interneti olarak adlandırılan cihazların oluşturduğu siber-fiziksel sorunlar için uygulanabilecek düzenlemeler mevcut değildir. Tanczer bu alandaki mevzuatın hızlı bir şekilde tamamlanacağını öngörmektedir (Tanczer,2019:38). Ancak tüm devletlerin aynı gelişmişlik seviyesinde olmadığı göz önünde bulundurulduğunda, yasal düzenlemelerin hızlı bir şekilde devletlerde uygulamaya konulamayacağı değerlendirilmektedir. Bu sistemlerde yaşanmakta olan çok hızlı teknolojik gelişmelerden kaynaklı belirsizlikler ve öngörülemezliklerden dolayı mevcut politikaların bu tehditlerle etkili bir şekilde başa çıkamayacağı da göz önünde bulundurulmalıdır (Tanczer,2019:39). Devletlerin bu tür belirsizlikleri dikkate alarak duruma uyarlanabilir politikalar geliştirmeleri gerekmektedir.

Kritik altyapıların korunması hemen hemen tüm toplumlar tarafından paylaşılan bir kaygı ve sorumluluk konusudur. Kritik altyapıların önemli bir kısmı özel sektöre aittir ve özel sektör tarafından işletilmektedir. Devletler ise kritik altyapılara yönelik düzenleyici kuralları belirlemekte ve bu sistemlerden hizmet almaktadır (Rajamaki, 2017:233).

İkinci bölümde ele alınan siber güvenlik olayı örneklerinde de görüldüğü gibi, devletlerin desteği ile geliştirilmiş karmaşık tehditler, kamu- özel sektör bilişim sistemlerini etkilemeye başlamış ve pek çok devlet siber saldırı kurbanı ülkeler arasına girmiştir. Siber uzayın saldırıya uğraması ve siber tehditler küresel seviyede olmaya başlamıştır. Siber güvenlik küresel bir yaklaşım gerektiren küresel bir sorundur. Ancak siber uzayın fiziksel katmanının büyük bir kısmı ve tehditlerin yönetimi ulus devletler düzeyinde gerçekleşmekte

olduğu ve siber uzayda en gelişmiş saldırı ve savunma yeteneklerine sahip birimlerin devletler olduğu görülmektedir (Puyvelde ve Brantly,2019:69

Modern toplumlar, çok sayıda güvenlik açıklarına sahip kritik altyapılara güvenmek zorundadır. Bu sistemlerin toplumlara yönelik olumsuz yan etkilerini en aza indirgemek üzere siber güvenlik olayının meydana gelmesini müteakip, sorunun nereden kaynaklandığının belirlenmesi, yaşananlardan ders alınarak gerekli önlemlerin alınması ve hizmetin sürdürülebilirliği sağlanmalıdır (Rajamaki, 2017:247).

4.2.1 Devletlerde Siber Güvenlik Yönetişimi ve Siber Güvenlik Paydaşları

Birinci bölümde kapsamlı olarak anlatıldığı gibi siber uzay, teknik altyapısı, işlevleri ve aktörlerinin çeşitliliği nedeni ile yönetiminde yönetişim uygulanması gereken bir alandır. Siber uzayda, farklı çıkarları olan çok çeşitli kurumsal yapılar ve aktörler yer almaktadır. Ağ karmaşıklığının artarak tüm dünya üzerinde kullanım alanlarının yaygınlaşması ile sistemin yönetilmesi de gittikçe karmaşıklaşmış, daha önce hiç gündemde olmayan siyasi, ekonomik, hukuki sorunların yanı sıra güvenlik sorunları da gündemde ilk sıralarda yerini almaya başlamıştır.

Günümüz küresel dünyasında, hâlâ otoriter ve yasal güç olmalarına rağmen modern devletlerin önemli güçleri gittikçe azalmaktadır (Rosenau,2014:272). Siber güvenliğin sağlanmasında sadece kamu kurumlarının yürüttüğü faaliyetler yeterli olmamaktadır. Bu çalışmaların siber uzayın doğası gereği yönetişim mekanizması kapsamında kamu kurumları, üniversiteler ile, özel sektör tarafından işletilmekte olan teknoloji firmaları ile birlikte farklı bağlamlarda farklı aktörlerle koordinasyon ve iş birliği içinde yürütülmesi önemli faydalar sağlayacaktır.

4.2.1.1 Siber Güvenlik Yönetişimi

Bir toplumsal-politik sistemdeki tüm ilgili aktörlerin ortak çabaları ile elde edilen sonuçların oluşturduğu yapı ya da düzen yönetişim olarak adlandırılmaktadır. Yönetişimin amacı, toplumsal sorunlarla başa çıkabilmek ve karmaşıklığı, dinamikliği ve çeşitliliği yaratan olgularla baş edebilmektir. Kimi durumlarda ulus devletin içsel egemenliğinin azalmasına yol açabilmekte olsa da toplumsal çıkarları dengeleme, olanakları ve sınırlılıkları ortaya çıkarma özelliği de bulunmaktadır (Ergun, 2008:274). Yönetişim sadece yönetim

değildir, belli bir şekilde sınırlar çizen ve bireylerin, kuruluşların ve şirketlerin hareketlerini teşvik eden kurallar, kurumlar ve planlı eylemler bütünlüğü anlamını da taşımaktadır (BMKP-1999,2014:505).

Geleneksel ulus devlet sistemlerinde güç kullanma yetkisi devlete aittir. Devletler, devletin nasıl yönetileceğini ve hangi konuların kamu yararına olduğunu da belirleme yetkisine sahiptir. Ancak günümüz modern toplumlarında kamu-özel sektör ilişkilerinde değişen dinamikler gereği devlet dışı aktörler de politika belirlemede her geçen gün daha aktif olmaya ve devletin rolünü değiştirmeye başlamıştır. Merkezi olmayan, ağ yapılanmasına sahip yönetişim mekanizması, kamu politikasını geleneksel hiyerarşik devlet merkezli güç yapısından uzaklaştırmaktadır (Adams vd.,2019:125). Küreselleşme sonrası kamu, özel sektör, sivil toplum kuruluşları, sanayi, üniversite, vatandaş olmak üzere toplumun tüm kesimlerinin, tüm paydaşların yönetimde söz sahibi olduğu bir sistem olarak tanımlanan yönetişim, resmi ve özel kuruluşlarda idari, ekonomik ve siyasi otoritenin ortak kullanımını belirten bir kavram olup belli bir alandaki faaliyetlerin idare edilmesini, koordinasyonunu ve regülasyonunu kapsamaktadır (Tangör,2007:29-35). Devletlerin, kritik altyapıların siber güvenliğinin sağlanmasında ve vatandaşlarının emniyetinin, güvenliğinin sağlanmasında sorumlulukları bulunmaktadır. Devletler, kritik altyapıların dayanıklılığını artırmak için bütüncül bir yönetişim altyapısını benimsemelidir. Bu tür bir yönetişim, çok sayıda kritik sektörde altyapı teslimini ve düzenlemesini denetleyen sektörel bakanlıklar ve kurumların yanı sıra tüm tehlikelere ve tehditlere karşı dayanıklılıktan sorumlu olan diğer aktörleri içerecektir. (OECD,2019:106).

Devletler, bir siber saldırıya maruz kalınması durumunda yönetişim mekanizması gereği, özel sektör, sivil toplum kuruluşları, üniversiteler ve şahıslar gibi aktörlerden destek alabilmektedir. Buna ek olarak siber güvenlik politikalarının, stratejilerin, standartların hazırlanmasında da bu aktörlerle birlikte hareket etmektedir. Günümüzün siber güvenlik yönetişimi, devletlerin hiyerarşik düzenlemelerini özel sektörün idari kararlarını ve özel kuruluşlar arasındaki sözleşmeleri de içermektedir (Eggenschwiler,2019:87-88).

Siber güvenlik yönetişimi, siber çatışmaların önlenmesi, kritik bilgi altyapılarının korunması, siber suçların ve siber terörizmin önlenmesine yönelik düzenlemeleri kapsamaktadır. Siber güvenlik yönetişimi, siyasi, ekonomik ve sosyal sonuçları olan çok

boyutlu bir yapıdır. Siber uzayın çok farklı aktörleri arasında teknik uzmanlar, devlet kurumları, düzenleyici kuruluşlar ve kullanıcılar sayılmaktadır. Bu nedenle siber güvenlik yönetişimi, çok farklı aktörleri ve yönlendirme mekanizmalarını bir araya getiren bir yönetişim türüdür (Eggenschwiler,2019:87-91). Siber güvenlik yönetişiminde devletler tarafından yürütülmekte olan hiyerarşik yönetişim; özel sektör tarafından yürütülmekte olan pazar odaklı piyasa yönetişimi ve kamu kurumları ile devlet dışı paydaşların birlikte faaliyette bulunduğu çok paydaşlı yönetişim yöntemleri tanımlanmaktadır. Bu yöntemler birbirinden tamamen yalıtılmış olmasa da her biri farklı alanlarda kullanılmaktadır (Eggenschwiler,2019:87-91).

Devletler de özel sektör kuruluşları da siber güvenliği kendi başlarına sağlayamayacaktır. Endüstri liderleri, devam eden tehditleri belirlemek ve bunlara yanıt vermek için devletle birlikte çalışmalıdır. Özel sektör ayrıca kriz anlarında olduğu gibi ihtiyaç olan diğer durumlarda da hükümet ortaklarına güvenebilmelidir. Sanayi ve hükümet, amacına uygun ve firmaların siber savunmalarına istemeden de olsa zarar vermeyen siber politikalar geliştirmek ve uygulamak için iş birliği yapmalıdır. Benzer şekilde, endüstri, özellikle sistemik riskle ilgili olarak, sektörün karşı karşıya olduğu stratejik siber tehditler hakkında bilgi sağlamak için hükümet ortaklıklarına giderek daha fazla güvenmelidir (San Juan ve Martin,2019:346). Siber güvenlik yönetişimi, ulus devlet yönetişimi ya da uluslararası anlaşmalar, özel sektör ve diğer paydaşların yerine getirdiği farklı görevlerin karmaşık bir ağını içermektedir.

Bilişim teknolojilerinin kullanımının daha çeşitli ve karmaşık hale gelmesi ile devletlerin, kurumların ve daha geniş anlamda toplumun çevrimiçi güvenliğinin sürdürülebilirliği konusunda endişeler oluşmaktadır. Teknolojik değişimin hızlı temposu, yasaları ve politikaları geride bırakmaktadır. Çok karmaşık ve merkezsiz siber ortamda tutarlı siber güvenlik uygulamaları geliştirebilmek ve düzenlemeler yapabilmek için, devletler, özel sektör kuruluşları gibi aktörler arasında ortak çabalar gerekmektedir. Çok paydaşlılık kavramının bile yeterli olmayacağı bu durumda, siber güvenlik yönetimini daha iyi anlamak, açıklamak ve karar vericilerin ortak düzenlemeler geliştirmesine ve uygulamasına yardımcı olmak üzere yeni kavramlara ve teorilere ihtiyaç vardır. Güçlü devletler, şirketler ve ortaklıklar siber uzaya hakimiyetlerini artırırken bireysel kullanıcılar,

gelişmekte olan devletler, vb. siber güvenlik olaylarına maruz kalabilecektir (Puyvelde ve Brantly,2019:454).

4.2.1.2 Siber Güvenlik Paydaşları

Bilişim teknolojileri alanında mevcut kurumları yeniden görevlendirmekte olan ya da yeni kurumsal yapılar tesis etmekte olan devletler siber uzay üzerinde kendi otoritelerini kurmaya devam ederken devlet dışı aktörler de bu otoriteye meydan okumaktadır (Nye, 2011'den aktaran Radu, 2014:5). Kritik altyapıların siber güvenliğine yönelik faaliyetlerin devletler seviyesinde yönetişim mekanizmasına uygun olarak iş birliği içinde yürütülmesinde rolü olan başlıca paydaşlar aşağıda yer almaktadır.

i. Devletler

Devletler, ulusal seviyede kamuya ait şirketler aracılığı ile EKS'ni kapsayan kritik altyapıların sahipleri ve işleticileridirler (OECD,2019:106). Kritik altyapıların siber güvenliğinin devlet sınırları içinde sağlanmasına yönelik devlet kurumları kendi içlerinde birtakım çalışmalar geçekleştirmek durumundadır. Bu kurumlar, ulusal hükümet, kamu ve yarı kamu kurumları, bağımsız düzenleyici kurumlar, silahlı kuvvetler, yerel yönetim birimleri ve belediyeler gibi kurumsal yapılardan oluşmaktadır. Son dönemlerde kritik altyapıların tesisinde ekonomik gerekçelerle daha az maliyetle daha yüksek verimlilik sağlamak üzere küresel dağıtım kanalları aracılığı ile heterojen bir küresel endüstri tarafından üretilmiş, testleri tam olarak yapılmamış donanım ve yazılım ürünleri kullanılabilmektedir. Bu kritik altyapıların sahipleri ve işletmecileri çevresel güvenliği dikkate almaksızın ekonomik getiriyi ön planda tutabilmektedirler. Kritik altyapı sistemlerinin önemli bir bileşeni olan EKS'nde kullanılmakta olan yazılım ve donanımın büyük çoğunluğunun araştırma, tasarım, geliştirme ve üretimi özel sektör firmaları tarafından gerçekleştirilmektedir. Bu firmalar, kaynakları planlayan, yöneten, güvenilir bağlantıyı sağlayan; trafik ve hizmetlerin dağıtımını gerçekleştiren hizmet sağlayıcı konumundadır. Ancak siber uzayın yönetimi sadece özel sektöre bırakılamayacak kadar önemli bir sorumluluk alanıdır (Tanczer,2019:38) Kritik altyapıların faaliyetlerini gerçekleştirmesinde kullanılmakta olan siber fiziki sistemleri tasarlayan, üreten, çalıştıran çok uluslu büyük teknoloji firmalarının, artık devletler ve uluslar ile karşılaştırılabilir veya

bazı durumlarda daha büyük küresel siyasi nüfuz düzeylerine sahip oldukları ve sadece kâra odaklanabilecekleri göz önünde bulundurulduğunda toplumsal çıkarların korunmasında devletlere önemli görevler düşmektedir (Vallor ve Rewak,2012:3-4).

Kritik altyapı sistemlerine yönelik riskleri yönetmek amacıyla en uygun ve etkili güvenlik önlemlerinin alınabilmesi için devletler, gerekli politikaları belirlemeli ve uygulamalıdır. Bu politikaların, kritik altyapı sistemlerinin amaçlarına uygun olarak hizmetlerini yerine getirmesine engel olmaksızın siber güvenlik önlemlerinin alınmasını da sağlaması gerekmektedir (Hathaway ve Klimburg, 2012:37).

Devletler, kritik kamu hizmetlerinin yerine getirilmesi işlevine sahip kritik altyapıların siber güvenliğinin sağlanması hususunda özel sektöre yardım etmelidir. Bu yardım kimi durumlarda, devletlerin teknoloji dağıtımı, iç güvenlik kontrolleri ve acil durum kurtarma ve iş sürekliliği planları için belirli standartlar uygulayarak özel sektör firmalarına düzenleyici kurallar getirmesi yolu ile olmaktadır. Kimi durumlarda ise özel sektöre uygulanan vergi teşvikleri, teşvik hibeleri, düşük maliyetli ya da karşılıksız krediler, düşük sübvansiyonlar, sigorta gibi yöntemlerle sağlanmaya çalışılmaktadır.

Devletler, esneklik ve sağlamlık çabalarına öncelik verebilmek için kritik altyapı sistemleri arasındaki karşılıklı bağımlılık ve güvenlik açıklarının iyi anlaşılmasını sağlamak üzere diğer altyapı, hizmet ve etki kapsamı ile bağımlılıklar ve karşılıklı bağımlılıklar ve minimum hizmeti sürdürmek için gereken kriterleri belirlemelidir (OECD,2019:107).

Eggenschwiler'in hiyerarşik yönetişim olarak adlandırdığı, kanunlar, kurallar ve politikaların rehberliğinde yukarıdan aşağıya bir düzenleme tarzı olan yönetişim türü daha çok devletlerin kullandığı bir yöntemdir. Krizler ve önemli belirsizliklerin olduğu durumlarda, otoriter merkezi komuta kontrol sistemleri ile birlikte iç ve dış hesap verebilirlik süreçleri de kullanılmaktadır. İlgili aktörler, devlet çalışanları tarafından yönetilirler. Devletler tarafından siber güvenlik olaylarını takiben Avrupa Konseyi Siber Suçlar Sözleşmesi gibi uluslararası yasal belgelere uygun olarak yürütülen soruşturmalar örnek olarak verilebilir. Kuvvet kullanılarak çözülebilecek krizler, afet durumları gibi sorunların çözümünde kullanılabilecek bir yaklaşımdır. Kanunlar, düzenlemeler, kontroller, prosedürler oluşturulur. Başarısız yönü ve sınırlı kaldığı durum bürokrasi ve etkisizliktir (Eggenschwiler,2019:87-91).

Kritik altyapı sistemleri son yıllarda özellikle siber uzay üzerinden birbirlerine bağlanırken ülke genelinde kimi durumlarda küresel seviyede ortak iletişim hatlarını kullanmaktadır. Siber uzayın bütünleştirici doğası gereği aynı iletişim ağları kullanıldığı için bir kamu kurumunun faaliyet alanı diğerlerinden ayrıştırılamadığı durumlar mevcuttur. Her bakanlığın sadece kendi ağlarından sorumlu olması mümkün değildir. Kritik altyapılarda internet bağlantısı ile kendi özel faaliyetleri dışında geleneksel bilişim sistemleri kullanılarak da birtakım faaliyetler gerçekleştirilmektedir. Bu nedenle farklı kamu kurumları arasında koordinasyonu sağlayacak kurumsal bir yapıya ihtiyaç vardır.

Kritik altyapıların siber güvenliğinin sağlanmasında devlet kurumlarının, bütçe, ekipman ve eğitimli personel açısından avantajlı olduğu durumlar vardır ancak siber saldırının ilgili kurum sınırlarını aştığı durumlarda farklı yetki alanları ve devlet kurumlarının ulus devletin sınırları dışında hızlı hareket edememesi önemli dezavantajlar arasında yer almaktadır. Bu saldırıların çoğu, özel sektör ağlarını ve sistemlerini etkilediği için devlet kurumları doğrudan müdahale edememekte, savunmada bu kurumlara güvenmek zorunda kalmaktadır.

ii. Özel Sektör Firmaları

Neoliberal politikaların yaygın olarak uygulandığı günümüz modern toplumlarında kritik altyapı sektörlerinde hizmet vermekte olan enerji üretim dağıtım şirketleri, su ve kanalizasyon şirketleri, kimya tesisleri gibi büyük sektörel kuruluşların sahipleri ya da işletenleri özel sektör firmalarıdır. Kritik altyapıların faaliyetlerini yerine getirmelerinde önemli rolü olan İnternet Servis Sağlayıcılar, bulut bilişim hizmeti vermekte olan firmalar da önemli siber güvenlik paydaşları arasındadır. Ulus devlet sınırları içinde kurulmuş olan ulusal yazılım ve donanım şirketleri ve sistem entegratörleri, EKS ve bilişim sistemlerini oluşturan yazılım, donanım, ağ bileşenlerinin tasarlanmasında, üretiminde, kurulmasında ve teknik destek verilmesinde görev almaktadır.

Eggenschwiler, pazar odaklı piyasa yönetişimi ile, rekabet ve verimliliği ön planda tutan, hizmet odaklı aşağıdan yukarıya bir düzenleme tipini anlatmaktadır. Ademi merkezilik ve bağımsız, otonom birimlerin oluşturulması için piyasa yönetişimine önem veren bu yöntemde sistem ve ağ ihlallerini önlemek üzere özel sektör firmaları tarafından geliştirilmekte olan uç nokta koruma önlemleri, yama uygulamaları, tehdit algılayıcı ve

güvenlik ürünleri sağlayan özel sektör firmaları kastedilmektedir. Hassas olmayan rutin olaylarda söz edilen bu yönetişim türünde, hizmet sunumu, ürünler, sözleşmeler kullanılır. Başarılı yönü uzlaşma, anlaşmalar, sosyal değişim, ittifaklar iken başarısız yönü verimsizlik ve piyasa başarısızlığı olarak belirtilmektedir (Eggenschwiler,2019:87-91).

Özel sektör firmaları, ulus devlet sınırları içinde kurulmuş yerli firmalar olabileceği gibi sistemi barındıran devletin sınırları dışında, çok uluslu şirketlerin kontrolünde de olabilmektedir. Kritik altyapıların siber güvenliğinin sağlanmasında, çok uluslu büyük özel sektör firmalarının faaliyetleri hayati öneme sahiptir. Siber güvenliğin sağlanması, yalnızca büyük yazılım şirketlerinin (Microsoft gibi), güvenlik şirketlerinin (McAfee gibi) veya telekom firmalarının iş birliğiyle gerçekleşebilmektedir.

Internet Servis Sağlayıcılar (ISS) ve iletişim şirketlerinin de siber uzayın yönetiminde önemli görevleri vardır. Bu kuruluşlar, internetin dağıtım altyapısının sağlıklı çalışmasını sağlar ve sürdürür. 2012'de ABD, siber uzayda önemli endişe duyulan botnetler, alan adı sahtekarlığı ve internet hedef alan korsanlığı alanlarında gerekli önlemleri alma sorumluluğunu internet servis sağlayıcılara (ISS) vermiştir. ISS'ların ve iletişim şirketlerinin siber güvenlik sorunları ile mücadele yetenekleri ülkelere göre değişmekle birlikte internetin koruyucusu ve hizmet sağlayıcısı olarak bu aktörlerin güvenlik yönetişiminde önemli görevleri bulunmaktadır (Puyvelde ve Brantly,2019:150).

Önemli kaynaklara sahip olan Microsoft, McAffe, Hp, Siemens gibi büyük BT şirketlerinin, devletten daha çevik olmalarına rağmen yine de siber güvenlik önlemleri alabilmek için yeni prosedürler geliştirilmesinde devlet yardımına ihtiyaçları vardır. Ancak bazı çok uluslu şirketlerin güçlü siber güvenlik altyapısı bulunmamaktadır. Bu firmalar hem kendileri için hem de faaliyetlerini yürüttükleri fiziki alanın ait olduğu devletler için tehdit oluşturabilmektedir. Bu nedenle, kritik altyapıların faaliyetlerini gerçekleştirmesini sağlayan siber fiziki sistemleri tasarlayan, üreten, çalıştıran özel sektör kuruluşları ile bu sistemlerin siber güvenliğine yönelik ürünleri tasarlayan, üreten, çalıştıran özel sektör kuruluşları da siber güvenliğin paydaşları arasındadır. Özel sektör, siber saldırılar için kullanılan neredeyse tüm yazılım, donanım ve hizmetlerden sorumludur, bu saldırıların gerçekleştirildiği ağ altyapısının çoğunu korur ve çoğu zaman bu saldırılara maruz kalan kritik altyapıya sahiptir.

Siber uzayın ve bilişim teknolojilerinin çift yönlü(dualite) kullanılabilmelerinden dolayı, kritik altyapıların siber güvenliğini sağlama görevi bulunan özel sektör firmalarının yanı sıra paralı asker grubu gibi görev yapan, çatışma alanlarına dijital silah ihraç eden, siber saldırı yapma niyeti bulunan ulus devletler tarafından desteklenen özel sektör firmaları da bulunmaktadır (Inversini, 2020:274).

iii. Devlet Dışı Sivil Toplum Kuruluşları-Küçük Gruplar

Bu gruplar, devletlerin sahip olduğu maddi kaynaklara sahip olmasalar da gerekli teknik bilgi ve çevikliğe sahip olabilmektedirler. Beyaz şapkalılar olarak anılan ve çoğu gönüllülerden oluşan bu gruplar ya da bireyler, siber saldırılara pek çok devletten daha hızlı yanıt verebilmektedir. Ancak, faaliyetleri, devlet olanakları olmaksızın sürdürülebilir değildir (Klimburg ve Healey, 2012:70-71).

Çok uluslu profesyonel kurumlardan destek alarak devletleri küresel konuların ulusal çıkarlarla paralel olduğuna ikna etmek amacıyla ulus devlet bakış açısı ile hareket eden uzmanlar da devlet dışı küçük gruplar arasında sayılabilir (Mann,2014:172:174).

Siber güvelik alanında araştırmalar yapan kamuyu bilgilendiren ve siber uzayda geçerli bazı protokolleri tanımlamak gibi faaliyetleri yürütmekte olan yerel sivil toplum kuruluşları da siber uzayda etkili gruplardan biridir.

iv. Üniversiteler

Kritik altyapı sistemlerinin ve bu sistemlerin siber güvenliğine yönelik ürünlerin araştırılması, geliştirilmesi, politikaların belirlenmesi gibi alanlarda üniversiteler de önemli paydaşlar arasında sayılmaktadır. Son zamanlarda pek çok üniversitede bilişim ağları, bilişim sistemleri, matematik, veri madenciliği gibi alanlarda eğitim ve araştırmalar güvenlik konusu ile birleştirilerek yürütülmektedir. Sadece güvenlik alanında uzmanların yetiştirilmesi yerine diğer araştırma alanları ile güvenlik alanının birleştirilerek kapsamlı araştırmalar yapılmaya başlanmıştır (Rajamaki, 2017:248).

v. Bireyler

Siber uzayda yer alan her kullanıcının diğer kullanıcılara karşı özel bir sorumluluğu vardır. Bireyler, kullanmakta oldukları sistemin veya uygulamanın düzgün bir şekilde güvenliğini sağlamazsa önemli hasara yol açacak eylemler için ilk saldırı vektörü

olarak kötüye kullanılabilecektir (Inversini,2020:275). Etkili bir yönetişimde, diğer özelliklerin yanında uyanık, ekolojik okuryazarlığı olan düşünceli ve empatik vatandaşlar da önemlidir (Orr,2014:xxiii).

vi. Uluslararası Paydaşlar

Kritik altyapılara yönelik siber güvenlik olayları devletlerin kendi sınırları içinde önemli çevre felaketlerine neden olabileceği gibi bu çevre felaketleri bölgesel ve hatta küresel seviyede etkili boyutlara ulaşabilecektir. Bu nedenle ulus devletlerin sadece kendi ulusal sınırları içinde aldıkları önlemler yetersiz kalacaktır.

Çok geniş bir kullanıcı kitlesi tarafından yoğun bir şekilde kullanılmakta olan siber uzayda, devletler saldırıya açık hale gelmiş ve kendilerini ulusal çapta savunmaları yetersiz kalmıştır. Bu alanda uluslararası birliktelik ve iş birliği önemli bir hale gelmiştir (Karadağ,2019:74).

Siber güvenliğin karmaşık uluslararası boyutu her zaman tam olarak anlaşılamamıştır. İlk dönemlerde hazırlanan ulusal siber güvenlik strateji belgelerinin çoğunda siber uzayın ulus devlet sınırları dışındaki alanları da kapsadığı durumlara gerçek anlamda değinilmemiştir. Son yıllarda siber güvenliğin uluslararası boyutu devletler tarafından daha iyi anlaşılmaya başlanmıştır ancak siber güvenliğe bütüncül yaklaşım genellikle devletlerin dışişleri bakanlıklarının faaliyetleri ile sınırlı olabilmektedir (Klimburg ve Healey,2012:99-100). Siber güvenlik olaylarına hazırlıklı olmak, bu olayları önlemek, azaltmak ve siber saldırıya cevap verebilmek için siber uzayda faaliyet göstermekte olan uluslararası paydaşlarla operasyonel iş birliğini güçlendirmek gereklidir. Siber uzayın dayanıklılığını ve güvenliğini sağlamada uluslararası operasyonel ilişkiler çok önemlidir. Küresel siber saldırılara yanıt verme ve üstesinden gelme yeteneği, koordinasyon ve yakın iş birliği ile geliştirilebilecektir. Siber uzayda yer alan devletlerde konu ile ilgili farkındalık oluşturmak, bilgi paylaşımını artırmak, siber güvenlik risklerini azaltmak ve uluslararası müdahalenin koordinesi için de uluslararası paydaşlarla iş birliğine ihtiyaç vardır.

Ulusal siber güvenliğin sağlanmasında devlet kurumları dışındaki devlet dışı ve uluslararası paydaşların da önemli görevleri bulunmaktadır. Bu uluslararası paydaşlar arasında BM, ITU, Avrupa Birliği, OECD, Dünya Bankası, İnterpol gibi uluslararası kuruluşlar; İnternet Governance Forum (IGF), Internet Corporation for Assigned Names

and Numbers (ICANN) gibi çok paydaşlı enstitüler; FIRST ve ISO gibi uluslararası standart kuruluşları, IETF = Internet Engineering Task Force ve IEEE gibi gayrı resmi uluslararası düzenleme kuruluşları, önemli küresel altyapı sağlayıcılar ile küresel boyutta yazılım ve donanım üreticisi olan firmalar sayılabilmektedir.

Kritik altyapıların siber güvenliğinin küresel seviyede sağlanması için uygulanacak yönetişim mekanizması ve birlikte çalışması gereken bölgesel ve küresel kuruluşlar, bir sonraki kısımda ayrıntılı olarak ele alınacaktır.

4.2.2 Ulusal Siber Güvenlik Stratejisi

Devletlerin siber güvenlik yaklaşımları, sahip oldukları teknolojik gelişme düzeyine, ekonomik durumlarına, gelişmişlik seviyelerine göre farklılık göstermektedir ancak her geçen gün artan siber tehdit olasılıkları ile karşı karşıya kaldıkları için tüm devletlerin bu sorunu tanımlamaları, sorunun çözümüne yönelik hedefler ve stratejiler belirlemeleri gerekmektedir. Yirminci Yüzyıl ortalarında değişen güvenlik kavramı kapsamında, devletler, ulusal güvenlik stratejileri içinde siber güvenliğe yönelik tehditlere ve çevresel güvenlik sorunlarına yer vermeye başlamışlardır.

Bu kısımda, devletlerin etkili siber güvenlik politikaları yürütebilmek amacı ile hazırlamakta oldukları siber güvenlik stratejilerinin taşıması gereken temel özelliklere değinilecektir. Bu kapsamda stratejinin sürekliliğinin anlatıldığı yaşam döngüsü, paydaşlar arasında sağlanması gereken koordinasyon, bilgi paylaşımı ve iş birliği; araştırma-geliştirme ve eğitim faaliyetlerinin önemine değinilecek ve stratejide yer alması gereken diğer hususlar ele alınacaktır.

4.2.2.1 Temel Özellikler

Devletler, ulusal güvenlik stratejilerinin yanı sıra siber güvenlik konusundaki vizyonlarını, üst düzey hedeflerini, ilkelerini ve önceliklerini ifade etmek; siber güvenliği geliştirmekle görevli paydaşları ve bu paydaşların siber güvenliğin sağlanmasındaki rol ve sorumluluklarını genel olarak açıklamak; ulusal siber altyapıyı korumak; güvenliği ve direnci artırmak için atılacak adımları, programları ve girişimleri tanımlamak üzere Ulusal Siber Güvenlik Stratejilerini yayınlamaktadır. Kimi ülkeler için ulusal siber güvenlik stratejilerinin birincil önceliği kritik altyapılar iken kimi ülkeler için ise fikri mülkiyeti

korumak, çevrimiçi ortamda güveni teşvik etmek veya bu sorunların bir kombinasyonu olabilmektedir (ITU,2021:13).

Kritik altyapıların siber savunma sistemleri yeterli olmadığı için özellikle bu alana odaklanılmalıdır. Kritik hizmetler veren ve hizmetin kesilmesi durumunda ülke çapında önemli zararlara neden olacağı ve siber ve endüstriyel kontrol sistemlerinin güvenliğini sağlamak üzere daha akıllı politikaların yaratılması için ulus devletler, kendi sınırları içinde hizmet vermekte olan kritik altyapıların ulusal ve uluslararası faaliyetlerini de kapsayan tanımlamaları net bir şekilde yapmalı, ürünleri veya hizmetleri kritik altyapı olarak nitelendirilen sektörleri belirlemeli ve kritik varlıkların bir listesini tutmalıdır. Bu tanımlar ve tanımlamalar, güven artırıcı bir önlem olarak uluslararası toplumla paylaşılmalıdır (Kastelic,2021:1). (Bayuk vd., 2012:152). Kritik altyapıların siber güvenliğinin devletler seviyesinde sağlanmasında, saldırgan tarafı caydırmak ve devletlerin kendi siber sistemlerinin dayanıklılığını artırmak yöntemleri kullanılabilmektedir. Kamu kurumlarına stratejik rehberlik sağlamak üzere hazırlanan strateji belgelerindeki ayrıntıya girmeyen anlatım, potansiyel düşmanlar için caydırıcı da olabilmelidir (Lindstrom ve Luiijf, 2012:46-47). Ulusal siber güvenlik stratejileri, potansiyel düşmanlara karşı devletlerin kırmızı çizgisinin nerede başladığını ve bu konuda hangi yeteneklere ve nasıl bir teknolojiye sahip olduğunu göstermesi açısından önemli bir işleve sahiptir. Sadece konunun uzmanları tarafından anlaşılabilecek teknolojik yeteneklerin siber güvenlik stratejilerinde bulunması caydırıcı etki yaratabilmektedir. (Lindstrom ve Luiijf, 2012:59).

4.2.2.2 Stratejinin Yaşam Döngüsü

Siber uzayın ve siber güvenlik konularının sürekli gelişmesi ve evrimi nedeni ile kritik altyapıların siber güvenliğine yönelik politikaların tanımlandığı Ulusal Siber Güvenlik Stratejisi yaşayan bir belge olmalıdır ve strateji çerçevesinde geliştirilen eylem planları sürekli takip edilmeli, yeniden değerlendirilmeli ve belirli aralıklarla güncellenmelidir.

Siber Güvenlik Stratejisi hazırlanmaya başlandığında ilk aşamada koordinatör birim ve stratejinin geliştirilmesinde yer alacak paydaşlar görevlendirilerek planlama yapılması; siber uzayda yer alan kritik sektörlerin ve kritik altyapıların belirlenerek siber risklerin değerlendirilmesi; stratejinin hazırlanması; siber güvenliğe yönelik faaliyetleri, bu faaliyetler için gerekli insan kaynakları ve bütçeyi, faaliyetlerin zaman planını kapsayan eylem planının

uygulanması; stratejinin uygulanmasının takip edilerek sonucun değerlendirilmesi aşamalarından oluşan yaşam döngüsünün belli periyotlarda devam etmesi gerekmektedir (ITU,2021:15,26).

Kritik altyapı operatörleri için bir hesap verebilirlik çerçevesi tanımlanmalı; hükümetler bu uygulamayı ve hedeflere ulaşma seviyelerini takip edilmelidir. Altyapıların güçlendirilmesi için ilk adım kapsamlı bir politika hazırlanmasıdır. Hesap verebilirlik mekanizması, operatörlerin kritiklik ve güvenlik açığı değerlendirmeleri, iş sürekliliği planları, yedek işletim sistemleri, tatbikatlar ve stres testleri, karşılıklı yardım anlaşmaları, varlıkların güçlendirilmesi veya risk finansman mekanizmalarını kurmuş olmalarına bağlıdır. Uygulamanın takibi, düzenli raporlama, teftişler ve performans değerlendirmeleri gibi çeşitli biçimlerde olmalıdır (OECD,2019:112).

4.2.2.3 Koordinasyon

Ulusal siber güvenlik faaliyetlerinin başarıya ulaşabilmesi için genel koordinasyon sağlanarak politik seviyede kararlar alınmalıdır. Alınan kararların uygulanabilmesi için ve uygulamada aynı işlemlerin tekrar yapılmasının önlenmesi için görevlerin birbiri ile bağlantısı tanımlanmalı ve ilgili birimler arasında koordinasyon sağlanmalıdır.

Kritik altyapıların siber güvenliğin sağlanmasına yönelik faaliyetlerin her aşamasında sadece kamu kurumlarının faaliyet göstermesi yetersiz kalacağı için kamu kurumlarının kendi arasında ve diğer paydaşlarla koordinasyonun sağlanması önem arz etmektedir. Koordinasyondan sorumlu üst düzey bir kamu kuruluşu görevlendirilmelidir. Bu kuruluşun, ulusal siber güvenlik risk değerlendirmesinin koordinasyonu, kritik altyapıların korunmasına yönelik strateji ile uyumlu bir ulusal siber güvenlik stratejisinin geliştirilmesi, sürdürülmesi ve siber güvenlik kurulunun oluşturulması gibi merkezi görevleri bulunmaktadır. Kamunun, özel sektör, sivil toplum kuruluşları gibi diğer paydaşlarla koordinasyon içinde çalışması ile kritik altyapıların siber güvenliği konusunda risk yönetimi ve alınması gereken önlemleri daha gerçekçi bir şekilde ele alan siber güvenlik stratejilerinin hazırlanabileceği; bir siber güvenlik olayının meydana gelmesi durumunda da tüm paydaşların koordineli bir şekilde kriz yönetimini gerçekleştirebileceği değerlendirilmektedir.

Koordinasyon birimi, ulusal siber güvenlik stratejisinin diğer ulusal stratejilerle ve politikalarla, siber güvenlikle ilgili uluslararası kabul görmüş ve ulusal olarak onaylanmış anlaşmalar, mevzuat ve düzenlemeleri ile uyumluluğunu sağlayacak çalışmaların gerçekleştirilmesini koordine etmelidir. Yine bu birim kamu kurumlarının kendi yetki alanları dahilinde ulusal siber güvenlik stratejisi ile uyumlu eylemleri tanımlama çalışmalarını koordine etmelidir (Luiijf&Healey,2012:130-132).

Devletler ve sanayi sektörü tek başlarına siber güvenliği sağlayamazlar. Endüstri liderleri, devam eden tehditlerin tanımlanmasında ve bu tehditlere karşılık verilmesinde yönetişim mekanizmaları aracılığı ile birlikte çalışmalıdır. Sanayi sektörü DDOS veya yıkıcı kötücül yazılımlarla yapılan saldırılarla karşılaştıkları kriz durumlarında olduğu gibi gerektiğinde hükümetlerine güvenebilmelidir. Sanayi ve hükümet ortak amaçlarına uygun ve firmaların siber savunmalarına zarar vermeyecek siber politikaların geliştirilmesinde ve uygulanmasında iş birliği içinde çalışmalıdır. Sanayi sektörünün, karşı karşıya olduğu stratejik siber tehditlerin ve özellikle sistemik risklerin önlenmesi konusunda da hükümete güvenmesi ve birlikte çalışması gerekmektedir. Kamu-Özel sektör iş birliğinde ortak amaç ve ilgi iyi vurgulanmış olsa bile siber güvenlik alanında birtakım belirsizlikler gündeme gelebilmektedir. Artan siber tehditler nedeni ile uzun vadeli stratejik eğilimlerin analizlerinin yanı sıra özellikle önem seviyesi yüksek kritik altyapı sektörleri için daha sıkı hükümet-sanayi iş birliği ve koordinasyonu gereklidir. Bir sektördeki kritik altyapı kurumunun kendi siber güvenliğini artırması için sistem kaynaklı risklerin ele alınmasında ve tanımlanmasında kritik üçüncü taraflar ve temel kamu hizmetleri göz önünde bulundurulmalıdır (San Juan ve Martin,2019:109-111).

Devletler, kritik altyapıların siber güvenliğini sağlamak üzere sektörler arası ve sektöre özel siber güvenlik temellerinin geliştirilmesini, etkili koordinasyon yapıları ve bilgi paylaşım süreçlerinin ve protokollerinin oluşturulmasını, paydaşlar arasında güvenin tesis edilmesini, güvenliğin iyileştirilmesine katkıda bulunabilecek fikirlerin, yaklaşımların ve en iyi uygulamaların belirlenmesini ve paylaşımını sağlamak üzere resmi kamu-özel sektör ortaklıklarının oluşturulmasını teşvik etmelidir. Kamu-özel sektör ortaklıkları, sanayi ve devlet arasında güveni artırmak için gerekli olup kritik altyapıların etkin bir şekilde korunmasının ve hem kısa hem de uzun vadede güvenlik risklerini yönetmenin temel şartıdır.

Sürdürülebilir ortaklıkların kurulabilmesi için, katılan tüm paydaşların ortaklığın hedeflerini ve birlikte çalışmaktan kaynaklanan karşılıklı güvenlik yararlarını net bir şekilde anlaması gereklidir (ITU,2021:44; Susanto vd., 2014:95; OECD,2019:109).

Siber güvenlik stratejisinde amaçlar listelenerek ve hangi durumda hangi sürecin gerçekleştirileceği açıkça anlatılarak ve evrensel bir dille yayınlanarak şeffaflık sağlanmalı ve diğer paydaşların şüpheleri giderilmelidir. Politikaların kurumsal yapıların, prosedürlerin ve süreçlerin bir araya getirilmesi ile hazırlanmış olan strateji, kritik altyapıların siber güvenliğinin sağlanmasında önemli görevleri olan özel sektör firmalarına da hitap etmeli, bu firmaları kendi başlarına alabilecekleri önlemler hususunda teşvik etmelidir. Özel sektörün gerekli faaliyetlerde bulunmaya teşvik edilmesinde önemli bir etken siber güvenlik hakkında yeterli bilinçlendirmenin sağlanmasıdır. Stratejinin hazırlanması aşamasında, gerekli siber güvenlik bilincine sahip özel sektör temsilcileri ile birlikte çalışmak önemlidir (Lindstrom ve Luiijf, 2012:60). Stratejide belirtilen hususlarda sorumluluğu olan kurumlar arasında sürekli bir koordinasyon sağlanmalıdır.

4.2.2.4 Bilgi Paylaşımı ve İş Birliği

Teknolojik gelişmelerden kaynaklanan güvenlik risklerini azaltmak üzere kendiliğinden benimsenecek davranış kuralları ve etik standartlar ile bu teknolojilerin yıkıcı etkisini kontrol altına alacak mekanizmaları oluşturmak üzere kamu ve özel sektör arasında iş birliği geliştirilmelidir (Schwab, 2016:99-101).

Bilgi paylaşımı, devletlerin kritik altyapıların güvenlik açıkları hakkında kapsamlı bilgi edinebilmeleri ve kritik altyapıların işleticisi olan özel sektör operatörlerinin kendi güvenlik açıklarını, diğer altyapılara bağımlılıklarını ve hizmetlerindeki kesintilerin diğer altyapıları ve hatta kendilerini nasıl etkileyebileceğini anlamalarına yardımcı olur. Özel sektör, siber güvenlikle ilgili güvenlik açıkları, kritik bağımlılıkları ve herhangi bir güvenlik olayı ile ilgili hassas bilgilerini bu bilgilerin ifşa edilmesinin sorumluluğa yol açabileceği, piyasadaki rekabet gücünü etkileyebileceği ve firmanın itibarına zarar verebileceği endişesi ile güvenli çevreler dışında paylaşmaya meyilli değildir. Devletler de ulusal güvenlikle ilgili bilgileri ve siber güvenlikle ilgili risk bilgilerini paylaşmaktan kaçınabilmektedirler. Birbirine ağlarla bağlı siber dünyada birbirine bağlı kritik altyapıların dayanıklılığı da güvenliği en zayıf olanı kadar güçlüdür (OECD,2019:108-110).

Günümüzde siber güvenlik platformunun oluşturulmasında güvenin tesisi ve bilgi paylaşımı en önemli sorunlardan biridir. Kurumlar, kuruluşlar, devletler ve insanlar arasındaki güvensizlik önemli bir sorundur. Ortak sayısal sistemler ve operasyonel prosedürler, bu gruplar arasındaki güveni artırabilir (Rajamaki, 2017:247). Devletler, kritik altyapıları işletmekte olan ve özel sektör kapsamında yer alan operatörler ile güvenli bilgi paylaşımını sağlayacak platformlar oluşturmalıdır (OECD,2019:108-110). Bilgi paylaşımı, siber olayların önlenmesi, müdahale ve kurtarma aşamalarında önem arz eder. Kamu kurumları arasında ve gerektiğinde özel sektörle bilgi paylaşımının ne şekilde yapılacağının kuralları belirlenmiş olmalıdır. Kritik altyapıların siber güvenliğinin devletler seviyesinde sağlanmasında, önleyici-koruyucu faaliyetlerin, siber olaya müdahalenin ve kurtarmanın başarılı olabilmesi için bilgi alışverişi ve verilerin korunması en temel merkezi faaliyetlerinden biridir. İki veya daha fazla kuruluş arasında bilgi paylaşımı için kuruluşlar arasında karşılıklı güvenin tesis edilmiş olması gereklidir. Siber olay verileri, tehditler, riskler, güvenlik önlemleri, koordineli savunma faaliyetleri, operasyonel deneyimler ve en iyi uygulama örnekleri paylaşılabilecek bilgiler arasında sayılabilir. Bilgi paylaşımı, kritik altyapıların siber güvenliğinin sağlanması görevi kapsamında belirli bir amaca yönelik olarak ulusal topluluklar arasında olabileceği gibi farklı ülkelerdeki benzer yetkilere sahip topluluklar ve uluslararası kuruluşlar ile de yapılabilmelidir (Luiijf ve Healey,2012:132). Teknoloji seviyesinde pek çok farklı kaynaktan edinilen güvenlik verileri bir araya getirilmeli ve bir bütün halinde analiz edilmelidir. Aksi durumda değerli güvenlik bilgilerinin atlanması ya da yanlış yorumlanması sonucu, çığ etkisi yaratma potansiyeline sahip güvenlik olaylarına neden olabilecektir (Susanto vd., 2014:95).

Her seviyedeki kuruluşlar, tehdit göstergelerinin paylaşımını kolaylaştırmak üzere anlaşmalar ve kurumsal yapıları geliştirmektedirler. ABD'nde kritik endüstrilerin Bilgi Paylaşımı ve Analiz Merkezleri (ISAC) adı ile üst düzey kamu-özel sektör kuruluşları, tehditlerin önüne geçmek için hizmet vermektedir.

Avrupa'da Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından, bilgi paylaşımı ve analiz merkezleri ile ilgili çalışmalar yapılmıştır. 2017'de NATO, üye devletler arasında iş birliğini teşvik etmek üzere Siber Uzay Operasyon Merkezi geliştirme sürecini başlatmıştır.

Tüm düzeylerdeki bilgi paylaşımındaki artışa rağmen pek çok firma uğradıkları güvenlik ihlalleri konusunda gerekli paylaşımı yapmamaktadır (Puyvelde ve Brantly,2019:437).

Operasyonel siber güvenliği desteklemek için, bilgi paylaşımına dayalı kamu ve özel sektör iş birliğinin önemli faydaları olabilmektedir. Siber güvenlik risklerinin, tehditlerin, gerçekleşmiş saldırıların, bu saldırıları soruşturmak, faili bulmak üzere kullanılabilecek karşı önlem teknolojilerin ve çözüm yöntemlerinin tek bir havuz üzerinden paylaşıma açılması bazı devletler tarafından uygulanabilmektedir. Gönüllü davranış kurallarının geliştirilmesinin teşvik edilmesi, en iyi uygulamaları kapsayan bilgi havuzlarının oluşturulması ve özel sektörün sistemlerini sürekli test etmeye ve kurtarma süreçlerini gözden geçirmeye, daha geniş bir pencereden bakıldığında ise ülke çapında farkındalık oluşturmaya, eğitim ve bilinçlendirmeye teşvik edilmesi gibi faydalar sağlayabilmektedir (Hathaway ve Klimburg,2012:37-39).

Kritik altyapı sağlayıcıları gibi bazı önemli devlet dışı kuruluşlara ilişkin yasal düzenlemeler doğrudan devletlerin kendisi tarafından yapılmakta ve aralarındaki iletişim kanalları üzerinden bilgi alışverişi yapılmaktadır. Ancak genellikle bu kritik altyapılarda faaliyet göstermekte olan siber fiziki sistemlerin yazılım ve donanım üreticisi firmalar ve güvenlik firmaları ile devlet arasında doğrudan bir iletişim bulunmamakta; kritik altyapı mevzuatında bunlara ilişkin hiçbir madde yer almamaktadır. Küçük sivil toplum kuruluşları, siber savunma ve araştırma grupları, kimi blog yazarları gibi küçük bireysel boyutlu ve hiyerarşik olmayan organizasyonlardan oluşan küçük devlet dışı aktörler devlet kontrolü dışında kalmaktadır. Bu aktörler arasında gönüllü iş birliği devletler tarafından teşvik edilmelidir (Klimburg ve Healey,2012:102).

Devletler, kritik altyapıların siber güvenliğinin sağlanması için ulusal faaliyetlerinin yanında uluslararası faaliyetleri de desteklemeli, siber güvenliği dış politikasının bir bileşeni olarak kabul etmeli; bu alandaki yerel faaliyetleri uluslararası faaliyetlerle uyumlu hale getirmeyi taahhüt etmeli; uzun vadeli uluslararası iş birliği hedeflerini belirtmelidir. Ülkenin siber güvenlik konusunda iş birliği yapacağı bölgesel ve küresel kuruluşlar, standardizasyon kuruluşları, uluslararası ya da çok paydaşlı ağ yapıları, kamu/özel sektör ittifakları gibi uluslararası forumlar ve iş birliği mekanizmaları belirlenmiş olmalıdır (ITU,2021:50-52).

4.2.2.5 Araştırma-Geliştirme ve Eğitim

Araştırma geliştirme faaliyeti, kritik altyapıların siber güvenliğine yönelik önleyici, koruyucu unsurların sağlanmasında ve risk yönetiminde önemli faydalar sağlayabileceği için devlet politikaları ile desteklenmelidir. Siber güvenlik olaylarına yönelik kriz yönetimi, müdahale ve kurtarmaya yönelik yöntemlerin araştırılması, siber saldırıların potansiyel sonuçlarının derinlemesine araştırılması gerekmektedir. Bu faaliyetlerin kamu kurum ve kuruluşları ile özel sektör ve üniversiteler tarafından yürütülmesine destek verilmeli, yeterli mali destek sağlanmalıdır.

Ulusal seviyede siber güvenliğin sağlanabilmesi için kamu ve özel sektör kuruluşlarının, bu kuruluşların her seviyedeki çalışanlarının ve tüm vatandaşların siber güvenlik olayları sonucu ne tür çevresel felaketlerin yaşanabileceği ve bunların önlenebilmesi için neler yapılması gerektiği hususunda farkındalık seviyelerinin yükseltilmiş olması gerekmektedir. Devletler, bu farkındalığı oluşturmak üzere temel seviyede eğitimleri müfredata almalı; özel sektör kuruluşlarını bu eğitimleri vermek üzere yönlendirmeli ve desteklemelidir. Bu farkındalık eğitimlerinin ulusal seviyede koordinasyonu sağlanmalıdır. Kritik altyapıların siber güvenliği konusunda vatandaşlarda temel bir farkındalık oluşturmanın yanında kamu ve özel sektörde görev yapmakta olan ve önleyici ve koruyucu siber güvenlik önlemlerinin alınması, risk yönetimi faaliyetlerinin gerçekçi olarak yapılması gibi önemli alanlarda kararlar almak durumunda olan üst düzey yöneticilerin de farkındalığının artırılması çok önemlidir.

Devletler, siber güvenlik profesyonelleri için yeni görev tanımlarına sahip profesyonel siber kadrolar oluşturmalı; yeterli eğitim programlarının bulunmadığı EKS'nin siber güvenliği gibi alanlarda eğitilebilecek personeli istihdam etmeli; bu alanda çalışan tüm personel için akreditasyon, eğitim ve sertifikasyon programları kurmalı ve ilgili personeli gerekli eğitimlere tâbi tutarak uzmanlık alanlarında sertifika sahibi olmalarını sağlamalıdır (Bayuk vd. 2012:173-174).

Strateji, politikacılara temel hedefler, gerekli kaynaklar ve bu kaynakların etkin kullanımı konusunda rehberlik edebilmelidir (Lindstrom ve Luiijf, 2012:61-62). Siber güvenlik stratejisinde, önceden belirlenmiş kritik altyapı sistemlerinin korunması ve dayanıklılıklarının artırılmasına yönelik iyi uygulamalara değinilmelidir. Stratejide, kritik

altyapıların ve kritik bilgi altyapılarının güvenliğini ve sürekliliğini geliştirmenin önemi vurgulanmalı; bu tür yıkıcı siber olayların meydana gelme olasılığını azaltmaya yönelik yönetimsel çalışmalara değinilmeli ve teşvik etmelidir (ITU,2021:41).

4.2.2.6 Roller ve Görevler

Stratejide, ülke sınırları içinde yer alan kritik altyapıların siber güvenliğinin sağlanmasına yönelik kanunları uygulaması gereken tüm aktörlerin rol ve sorumlulukları net bir şekilde tanımlanmış olmalı; devam eden sorunları yönetmek için bir koordinasyon mekanizması işletilmeli; bu konudaki mevzuatın geliştirilmesine yönelik çalışmalar ve mevcut mevzuatın yetersiz kaldığı alanlar da belirlenmelidir.

Devlete ait olmayan ve özel sektör tarafından işletilmekte olan kritik altyapıların siber güvenliğinin sağlanması için koordinatör atanmalıdır. Bu sistemlerin korumasına yönelik yönetişim modeli ile, kritik altyapı operatörlerinin sorumlulukları da belirlenmiş olmalıdır. Kritik hizmetlerin ve altyapıların işletilmesini ve kurtarılmasını sağlamak için kamu ve özel kuruluşlar arasındaki kanallar ve iş birliği mekanizmaları ve sorumlu devlet kurumları tanımlanmalıdır. Yönetişim modeli, örtüşen misyonlara sahip devlet kurumları arasında koordinasyon ve uyumu sağlayan mekanizmaları içermelidir. Yönetişim ayrıca, sektörel düzenleyicilerin, görevlerin tekrarlanmasını önleyen ve hem kamu hem de özel sektör kuruluşları arasında önemli uyum çabalarını kolaylaştıran açık ve tutarlı güvenlik gereksinimleri oluşturmasını sağlamalıdır. Strateji, tüm kurumsal yapıların ve bireylerin, siber güvenlik sorumluluklarını yerine getirmeye gerçekten teşvik edilmesini sağlamak için geniş bir politika yelpazesini dikkate almalıdır (ITU,2021:42-44).

Planlamadan operasyonlara, bakım, yenileme ve güçlendirme gibi kritik altyapının tüm yaşam döngüsünü ele alacak dayanıklılık önlemlerini almak üzere hükümetler, operatörleri bu konuda yatırım yapmaya teşvik etmeli ve ortak hedeflere ulaşabilmek için politika araçlarını tanımlamalıdır (OECD,2019:110).

4.2.2.7 İlgili Diğer Mevzuat ile Uyum

Ulusal siber güvenlik stratejileri, devletin ulusal güvenlik vizyonunu tutarlı ve uygulanabilir politikalara dönüştürmesine olanak sağlamalı, kritik altyapıların siber güvenliğinin sağlanmasına yönelik terörle mücadele stratejisi, afet acil durum stratejisi gibi

alt stratejilerin üretilmesini de kolaylaştırmalıdır. Mevcut ulusal ve uluslararası güvenlik stratejileri ile bağlantılı olmalıdır. Diğer stratejilerle bağlantıyı, koordinasyon ve iş birliğini teşvik etmek için de yardımcı olabilmeli; uluslararası düzeyde bir topyekun savunma yaklaşımını kolaylaştırmaya da hizmet edebilmelidir. Tehditler ve zorluklar ana hatlarıyla belirtilmeli; en büyük endişe kaynağı olabilecek tehditler, ihtiyaç duyulabilecek kaynaklar veya müdahalenin hangi birimler tarafından gerçekleştirileceği, tehditlerin ve zorlukların ele alınma konuları ayrıntıya girilmeksizin kabaca belirtilmelidir.

4.2.2.8 Kritik Altyapı Sistemlerinin Sınır Aşan Boyutlarının Ele Alınması

Kritik altyapıların kurulmasında, işletilmesinde sadece o devlet içindeki özel sektör firmaları değil uluslar üstü özel sektör firmaları da faaliyet gerçekleştirdiğinden ya da bir devletin fiziki sınırları içinde yer alan kritik altyapı sistemi, ağlarla fiziki sınırlar dışındaki alanlara bağlı olduğu için sınır aşan durumlar ortaya çıkmaktadır. Kritik altyapılara yönelik siber güvenlik olayları sadece içinde bulunduğu devleti değil, bölgesel, kimi durumda küresel sonuçlar doğurabileceği için devletlerin siber güvenlik stratejilerinde bu konu ile ilgili tehditler, alınacak önlemler vb. benzerlikler gösterebilecektir. Ancak yine de kritik altyapının, sınırları içinde yer aldığı devletin hassasiyetleri göz önünde bulundurulmalı, gerçekçi yaklaşımlar sergilenmelidir (Lindstrom ve Luiijf, 2012:61-62).

Rajamaki, siber güvenliğin uluslararası iş birliği açısından en önemli konu olduğunu ve dijital dünyada güvenin geliştirilmesi ve korunmasında temel faktör olduğunu savunmakta ve siber güvenliğin engel olarak görüldüğü mevcut durumda siber güvenliğin yeni hizmetleri ve etkileşimleri harekete geçirici rolüne de dikkat çekmektedir. (Rajamaki, 2017:233). Bu bağlamda, kritik altyapıların siber güvenliğinin sağlanmasının çevresel güvenlik ve sürdürebilirlik açısından taşıdığı önem dikkate değerdir.

Birbirine bağlı ve birbirine bağımlı altyapılar, sınır ötesi konumları ile tehlikeler ve tehditleri de ulusal sınırlar ötesine taşınmaktadır. Kimi durumlarda kritik altyapılar birden fazla ülkede farklı yetki alanlarına hizmet vermektedir. Bu nedenle kritik altyapıların korunması için uluslararası entegrasyon ve iş birliği gereklidir. Hükümetler, sınır aşan bağımlılıkları ele almak üzere diğer devletlerin ulusal kritik altyapı dayanıklılık politikaları hususunda iş birliği yapmalıdır. Sınırlar ötesi riskleri ve güvenlik açıklarını değerlendirmek için, ortak yaklaşım geliştirmenin yanı sıra uluslararası bilgi paylaşım mekanizmaları

kurulmalıdır. Bilgi ve iyi uygulamaların paylaşılması; ortak yaklaşımların ve ortak standartların geliştirilmesi uluslararası ve sınır ötesi iş birliğinin teşvik edilmesi bu alandaki politika seçenekleri arasında sayılabilir (OECD,2019:113). Devletler, siber güvenliği dış politikalarının bir bileşeni olarak kabul etmeli, bu konuda gerçekleştirilecek olan yerel ve uluslararası çabaları uyumlu hale getirmeyi taahhüt etmeli; kamu, özel, bölgesel, küresel paydaşların dahil olacağı uzun vadeli uluslararası iş birliği hedeflerini belirtmelidir. Uluslararası siber güvenlik normlarının ve güven artırıcı önlemlerin oluşturulmasına destek olmalı, uluslararası siber güvenlik standartlarının geliştirilmesine katılım sağlamalı, mevcut bölgesel ve uluslararası süreçlere katılmalıdır (ITU,2021:50-53).

4.2.3 Kritik Altyapıların Siber Güvenliğine Yönelik Kriz Yönetimi

Demokratik devletler, tüm toplumu harekete geçirmek için gerekli kaynakların yönetimi ve büyük çaplı olağanüstü durumlara istenen ölçekte etkili değişikliklerle cevap verme kapasitesine sahiptirler (Orr,2014:xxii). Acil durumlarda nasıl davranılması gerektiğini belirlemek ve hızlıca yanıt verebilmek üzere, ulusal, bölgesel kimi durumlarda küresel seviyede toplumun tüm kesimleri için hayati öneme haiz kritik altyapıların neler olduğu önceden belirlenmiş ve bunlar da kendi aralarında önceliklendirilmiş olmalıdır (Lindstrom ve Luiijf, 2012:61). Stratejide, büyük ölçekli siber güvenlik olaylarına devlet seviyesinde hazırlanmak, olayın meydana gelmesini önlemek, meydana gelmesi durumunda tespit etmek, hasarı en aza indirgeyebilmek ve ülkenin siber dayanıklılığını geliştirmek için bir takım koruyucu önleyici faaliyetlere yer verilmelidir (ITU,2021:39). Bunlardan bazıları:

- Devletler, kritik altyapı sektörlerine yapılan saldırılara karşı, ilgili kurumlara yardımcı olmak üzere gerekli kurumsal yapıları oluşturmalıdır (Bayuk vd.,2012:153). Meydana gelebilecek siber olaylarda, ülkelerin ihtiyacı göz önünde bulundurularak kamu, özel sektör çalışanlarından Ulusal Siber Olay Müdahale Ekipleri (CERT/CSIRT/CIRT) oluşturulmalıdır. Kritik altyapı sistemlerinin otomasyonunu sağlayan endüstriyel kontrol sistemleri, geleneksel bilişim sistemlerinden farklılıklar gösterdiği için bu sistemlere özgü siber olay müdahale ekipleri ayrıca oluşturulmalı ve siber olay müdahale ekipleri ile koordinasyon içinde çalışmaları sağlanmalıdır.

- Bu ekiplerin, ulusal risk kayıtları ve belirli nesnelere, organizasyonlara veya süreçlere/hizmetlere yönelik risk faktörlerinin düzenli olarak yürütülen değerlendirmelerini kapsayan risk analizi çalışmalarına katılmaları sağlanmalıdır.

- Kritik altyapılara yönelik bir siber olayın meydana gelmesi durumunda oluşacak kriz dönemlerinde uygulanacak ayrıntılı acil durum müdahale planları geliştirilmelidir (Bayuk vd., 2012,s:153). Bu plan, ulusal seviyede risk değerlendirme sonuçlarını, kritik altyapı sektörlerinin birbiri ile olan bağımlılıkları da dikkate almış olmalıdır (ITU,2021:39).

- Siber olayın meydana gelmesi öncesinde koruyucu önleyici güvenlik önlemlerinin alınması; siber olay anında ve sonrasında zararı en aza indirgeyebilmek ve en kısa sürede normal duruma dönebilmek için, kamu ve özel sektör firmaları arasında bilgi paylaşımı teşvik edilmelidir.

- Devletler, ilgili yerel aktörler arasında kriz çözüm ağları oluşturmalıdır (Kastelic,2021:1).

- Devletler, diğer devletlerle iletişim kurma kapasitelerinin yanı sıra yardım ve hasarın azaltılması taleplerinin (özellikle iletişim kanalları, protokoller ve prosedürler) karşılanmasına yönelik uluslararası siber güvenlik tatbikatlarına düzenli olarak katılım sağlamalıdır (Kastelic,2021:1). Kritik altyapılara yönelik siber güvenlik olaylarına etkin bir şekilde müdahale edebilmeleri, kriz yönetimi süreçlerini test etme, ulusal siber olay müdahale ekiplerinin siber güvenlik olayları esnasındaki davranışlarını test ederek kapasitelerini geliştirmeleri, sektörler arası bağımlılıkların anlaşılması, ülkeler arasındaki siber olaylara müdahale kapasitesinin güçlendirilmesi, sınır ötesi bağımlılıkların anlaşılması, devletler arasında güvenin oluşturulması ve genel uluslararası dayanıklılık ve hazırlık düzeylerini iyileştirmeye yardımcı olabilir. Ulusal ve uluslararası seviyede gerçekleştirilecek siber güvenlik tatbikatlarının düzenlenmesi ve katılım teşvik edilmelidir (ITU,2021:39).

4.2.4 Türkiye'de Endüstriyel Kontrol Sistemlerinin Siber Güvenliğine Yönelik Politikalar

Bu kısımda, ülkemizde endüstriyel kontrol sistemlerinin kullanılmakta olduğu kritik altyapıların siber güvenliğinin sağlanmasına yönelik politika dokümanları ve faaliyetler ele alınacak, siber güvenliğe çevresel sürdürülebilirlik açısından yaklaşılıp yaklaşılmadığı araştırılacaktır.

5809 sayılı Elektronik Haberleşme Kanunu'nun 5'inci maddesinin birinci fıkrasının (h) bendi ile "Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmalarını yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak" görev ve sorumlulukları Ulaştırma ve Altyapı Bakanlığına verilmiştir. Bu kanun kapsamında, Ulaştırma Bakanlığının koordinatörlüğünde ilk "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanmış ve 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. 2 yıllık bu dönem içerisinde siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında çalışmalar yürütülmüştür. Yine bu kanun maddesi kapsamında 2013 yılında, BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, belirlenen kritik altyapı sektörlerinde ve diğer kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) faaliyetlerine başlamıştır. Merkezde USOM'un ve kritik sektörler ile diğer kurum kuruluşlarda ise SOME organizasyonunun oluşturulması ile ülkemizde kurumsal siber güvenlik yapılarının kurularak güçlendirilmesi sağlanmıştır. "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile de siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi için siber savunmanın

güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu konularında çalışmalar yürütülmüştür. Kritik altyapıların korunması programı kapsamında kritik altyapıların hizmet sürekliliğinin takibine yönelik izleme faaliyetleri, zafiyet tarama çalışmaları ve bilgi güvenliği açısından düzenleme ve denetleme çalışmaları yürütülmüştür.

Türkiye'de kritik altyapıların siber güvenliğinin sağlanmasına yönelik özel bir strateji dokumanı bulunmamaktadır. Ancak farklı politika dokümanlarında bu konu ele alınmaktadır. Bu amaçla öncelikle halen yürürlükte olan politika dokümanlarından On Birinci Kalkınma Planı (2019-2023), AFAD Stratejik Plan (2019-2023), Ulusal Siber Güvenlik Stratejisi ve Eylem Planı(2020-2023), Bilgi ve İletişim Güvenliği Genelgesi (2019), Bilgi ve İletişim Rehberi (2020) dokümanları ele alınacaktır.

4.2.4.1 On Birinci Kalkınma Planında (2019-2023) Kritik Altyapıların Siber Güvenliği

Diğer kalkınma politikalarının yanı sıra ekonomik ve sosyal faydanın artırılmasına paralel olarak çevrenin korunması ve yaşam kalitesinin iyileştirilmesine yönelik hedef ve politikalara; dijital dönüşüme ve siber güvenliğe yönelik politikaları da kapsayan On Birinci Kalkınma Planı, Türkiye Cumhuriyeti Cumhurbaşkanlığı koordinatörlüğünde, kamu çalışanları, özel sektör, STÖ temsilcileri, akademisyenlerin katılımı ile oluşturulan Özel İhtisas Komisyonları ve çalışma gruplarının faaliyetleri ile ve internet üzerinden uygulanan vatandaş anketi ile yani yönetişim yöntemi kullanılarak oluşturulmuştur (T.C. Cumhurbaşkanlığı,2019:5-6).

11. Kalkınma Planı kapsamında teknolojik gelişmelere bağlı olarak ülkemizin milli güvenliği açısından ortaya çıkabilecek muhtemel risklerin proaktif bir biçimde önlenebilmesini sağlamak için Türkiye'nin siber güvenlik ve teknolojilerini geliştirme yeteneğinin iyileştirmesi, nitelikli insan kaynağı eksikliğini gidermesi, kurumsal yapılanmasını tamamlaması ve mevzuat altyapısını değişen teknolojiye uyumlu, güncel tutması gerektiği (T.C. Cumhurbaşkanlığı,2019:12) belirtilmektedir. Bu kapsamda kritik altyapıların siber güvenliğine yönelik aşağıdaki faaliyetler planlanmıştır:

- Afetlere hazırlık ve afet sonrası müdahalede özel önem arz eden enerji, ulaştırma, su ve haberleşme gibi kritik altyapıların güçlendirilmesine öncelik verileceği ve kritik altyapı tesislerinin önceliklendirilmesi için yöntem belirleneceği (T.C. Cumhurbaşkanlığı,2019:171);
- Sanayi işletmelerinin siber güvenlik ihtiyaçlarının merkezi olarak planlanması ve yapılandırılması için mekanizma geliştirileceği (s.66); bu kuruluşların siber güvenlik konusunda farkındalık ve yetkinliklerinin artırılacağı, fabrika ve tedarik zincirlerinde koruyucu güvenlik önlemleri alınacağı, firmaların uçtan uca siber güvenliğinin periyodik olarak test edileceği (T.C. Cumhurbaşkanlığı,2019:75);
- Siber güvenlik teknolojilerinin de dahil olduğu ileri teknolojilere ilişkin gelişim yol haritalarının hazırlanmasının, gerekli altyapının tesisinin, ihtiyaç duyulan nitelikli insan kaynağının yetiştirilmesinin ve toplumsal yönelimin bu alanlara odaklanmasının sağlanacağı (T.C. Cumhurbaşkanlığı,2019:79);
- Yazılım alanında güvenlik risklerinin azaltılması amacıyla açık kaynak kodlu yazılım ekosisteminin geliştirileceği, bu alanda nitelikli insan gücünün yetiştirileceği (T.C. Cumhurbaşkanlığı,2019:109);
- Ulusal siber güvenliğin sağlanmasına yönelik düzenlemeler ile kurumsal yapılanmanın oluşturulacağı ve teknik altyapının güçlendirileceği (T.C. Cumhurbaşkanlığı, 2019:119);
- Ulusal Siber Güvenlik Stratejisinin güncelleneceği, siber güvenliğe yönelik düzenlemelerin ve teknik altyapının güçlendirileceği ve güçlü bir koordinasyon yapısının oluşturulacağı ((T.C. Cumhurbaşkanlığı, 2019:119);
- İhtiyaç duyulan alanlarda siber güvenlik standartlarının oluşturulacağı;
- Bilgi ve iletişim teknolojileri altyapılarına yönelik tehditlere ilişkin siber istihbarat paylaşım ağı kurularak ulusal siber güvenlik olaylarına müdahale ve koordinasyon kapasitesinin artırılacağı, siber tehdit istihbaratı sağlanan kaynakların çoğaltılacağı (T.C. Cumhurbaşkanlığı, 2019:109);
- Kritik önemi haiz enerji altyapısının güvenli bir şekilde işletilmesine yönelik Siber Güvenlik Operasyon Merkezinin kurulacağı; kritik altyapılarda bilgi güvenliği

yönetim sistemi kurulmasına yönelik usul ve esasların belirlenerek hayata geçirileceği (T.C. Cumhurbaşkanlığı, 2019:109);

- Siber güvenlik ekosisteminin faydalanması ve bu alanda katma değeri daha yüksek ürün ve çözümlerin geliştirilmesi amacıyla kamu araştırma kurumları ile üniversitelerin de dâhil olduğu siber güvenlik ürün ve teknoloji projelerinin geliştirileceği ve bu projelerin çıktılarının açık kaynak kodlu olarak siber güvenlik ekosistemiyle paylaşılacağı;
- Toplumun tüm kesimlerinde siber güvenlik kültürü ve insan kaynağının geliştirilmesinin sağlanacağı;
- Siber güvenlik tatbikatlarının düzenleneceği (T.C. Cumhurbaşkanlığı, 2019:183);
- Büyük endüstriyel kazalara karşı risk yönetimi ve acil müdahale kabiliyetlerinin geliştirileceği; uluslararası yükümlülükler kapsamında kimyasalların insan sağlığı ve çevreye olan etkilerini en aza indirecek şekilde etkin yönetimine yönelik mevzuat çalışmaları yapılacağı ifade edilmektedir (T.C. Cumhurbaşkanlığı,2019:170).

On Birinci Kalkınma Planının tüm faaliyetlerde ulusal ve uluslararası koordinasyonu ön planda tutarak çevresel güvenlik ve sürdürülebilirlik, afet ve acil durum yönetimi, siber güvenlik, kritik altyapıların siber güvenliği gibi konuları kapsama alanı içine aldığı; bu konularda gerçekleştirilmesi gereken hayati önemi haiz faaliyetleri gündeme getirdiği görülmektedir.

4.2.4.2 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)

On Birinci Kalkınma Planında da belirtildiği gibi, Ulusal Siber Güvenlik Stratejisi (2016-2019) güncellenerek hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), ülkemizin siber güvenlik alanındaki politikalarını konu almakta, bundan önce hayata geçirilen stratejilerde edinilen kazanımların daha da artırılmasını hedeflemektedir.

2013-2014 dönemi ile 2016-2019 döneminde gerçekleştirilen ve süreklilik arz eden eylemler, mevcut durum ve planlanan çalışmalar kapsamında gözden geçirilmiş ve gerekli iyileştirmelerin yapılması sağlanmıştır. Bu çerçevede, belirlenen stratejik amaçlar arasında

birinci sırada “Kritik Altyapıların Korunması ve Mukavemetin Artırılması” maddesine yer verilmiştir. Son amaç ise Uluslararası İş Birliğinin Geliştirilmesi olarak belirlenmiştir.

Stratejide yer alan amaçlara ulaşmak üzere gerçekleştirilmesi gereken eylemlerin belirlenmesi için ulusal paydaşların katılımıyla hazırlık çalıştayı düzenlenmiş; stratejik amaçlara ilişkin olarak kurum ve kuruluşlar tarafından gerçekleştirilecek eylemler ve uygulama adımları belirlenmiştir. Kritik altyapı sektörlerinin korunmasına yönelik düzenlemelerin hayata geçirilmesi, siber risk yönetiminin ve acil durum planlarının geliştirilmesi gibi eylemler belirlenmiştir. Siber olaylara müdahale ekiplerinin olgunluk seviyelerinin ölçülmesi, izlenmesi, artırılması ve siber güvenlik eğitim içeriklerinin zenginleştirilmesi ve yaygınlaştırılması ile insan kaynağının artırılması amaçlanmıştır. Oluşturulması planlanan organik siber güvenlik ağı çerçevesinde ise ileri düzey uzmanlık projelerinin geliştirilmesi ve ülke geneline yayılacak şekilde bu alanda çalışmalar gerçekleştiren kurum ve kişiler ile Ulusal Siber Olaylara Müdahale Merkezi (USOM) arasında bilgi paylaşımının artırılması öncelikli amaçlar arasında yer almaktadır. Ulusal faaliyetlerin yanında uluslararası iş birliğinin geliştirilmesinin önemine değinilmekte ve bu çerçevede ikili ve çoklu iş birliklerinin artırılması ve bilgi paylaşımının geliştirilmesine yönelik çalışmaların gerçekleştirilmesi; siber uzayda uluslararası ortak normların ve standartların oluşturulması için yürütülen faaliyetlere katkı sağlanması hedeflenmiştir (UAB,2020, Ulusal Siber Güvenlik Stratejisi 2020-2023).

Stratejide Kritik Altyapı, “işlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar” şeklinde tanımlanmıştır. Bu tanımlamada kritik altyapı sistemlerinin düzgün çalışmadığı durumda meydana gelebilecek olumsuz durumlar arasında can kaybı, büyük ölçekli ekonomik zarar, ulusal güvenlik açıkları veya kamu düzeninin bozulması sayılmıştır. Ancak çevre etiği açısından diğer canlı ve cansız varlıklar ile çevresel sürdürülebilirliğe verilebilecek zararlara değinilmemiştir. Bu çalışma kapsamında sayılan kritik altyapı sektörlerinden iletişim altyapısı, enerji ve su yönetimi sektörleri tanımlanmıştır. Ancak kimya sektörü gibi diğer bazı sektörleri kapsamamaktadır.

Siber güvenlik çalışmalarında kurumsallığın, sürekliliğin ve sürdürülebilirliğin önemine değinilmekte; dijitalleşmenin sürdürülebilirliği için siber güvenliğin hayati bir öneminin göz önünde bulundurulması gerektiği vurgulanmaktadır. Kritik altyapılar aracılığı ile verilen hizmetlerin kesintisiz ve etkin olarak sürdürülmesi; hizmet ve ürünlerin tüm yaşam döngüsü boyunca siber güvenliğin dikkate alınması da sayılmaktadır (s:18).

Hedefler arasında ise, kritik altyapıların siber güvenliğinin 7/24 sağlanması, proaktif siber savunma anlayışının geliştirilmesi, SOME ekiplerinin yetkinliklerinin geliştirilmesi, kurum ve kuruluşlar arası veri paylaşımının güvenli biçimde sağlanması, Kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi; kritik altyapı sektörlerinde, BT ürünlerinde üretici bağımlılığının önüne geçilmesi; insan kaynağının güçlendirilmesi; ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve iş birliğini sağlayacak mekanizmaların geliştirilmesi; caydırıcılığın artırılması da sayılmaktadır.

Uluslararası bilgi güvenliği standartlarının kamu ve özel sektörde uygulanmasının yaygınlaştırılması ile altyapılarda üreticiye bağımlılığın önüne geçilebileceği savunulmaktadır. Sektörel düzenlemelerin geliştirilmesi ve denetim mekanizmalarının oluşturulması, acil durum hazırlık planlarının hayata geçirilmesi öncelikler arasında yer almaktadır. Kritik altyapıların siber tehditlere karşı etkin şekilde korunması ve siber olaylara müdahale yeteneğinin daha da güçlendirilmesi; sektörel ve ulusal ölçekte bir risk yönetimi anlayışıyla tehditlerin ve oluşturdukları olumsuz etkilerin en aza indirgenmesi amaçlanmaktadır.

Ülkemizde ve dünyada siber olaylara müdahale yeteneklerinin güçlendirilmesine, bilgi ve hazırlık seviyelerinin artırılmasına yönelik siber güvenlik tatbikatları, konferanslar, seminerler, çalıştaylar gibi etkinlikler ile kapasite geliştirmeye yönelik uluslararası faaliyetler düzenlenmektedir. Bu dönemde de uluslararası siber güvenlik faaliyetlerine artan bir oranda katılım ve katkı sağlanarak ülkemizin bu alandaki söz sahibi konumunun daha da pekiştirilmesi ve dünyadaki iyi uygulama örneklerinin tespit edilerek ulusal siber güvenlik çalışmalarına sağlanan girdilerin artırılması amaçlanmakta olduğu belirtilmektedir.

Strateji, kamu, özel sektör, akademi ve STK'lardan temsilcilerin geniş katılımıyla hazırlanmıştır. Ulusal Siber Güvenlik Eylem Planı (2020-2023); her bir eylemin

açıklamasıyla beraber eylemlerden sorumlu kurumları, iş birliği yapılacak kurumları, eylemlerin amaçlarını ve uygulama adımlarını, bunların gerçekleştirilmeleri için belirlenen yöntemleri ve beklenen gerçekleştirilme sürelerini detaylı olarak ele almaktadır. Bu kapsamda Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)'de 40 adet eylem ve 75 adet uygulama adımı tanımlanmıştır.

Ulusal Siber Güvenlik Eylem Planının (2020-2023), başarısını ölçmek üzere kapsadığı eylemlerin içerdiği her bir uygulama adımına yönelik ölçüm kriterleri belirlenmiş olup Eylem Planı'nın gerçekleşme oranının bu kriterler üzerinden belirlenmesi planlanmıştır.

Ulusal Siber Güvenlik Stratejisi (20120-2023)'nde siber uzayda yer alan paydaşlarımız arasında ülkemizden kamu kurum ve kuruluşları, kritik altyapılarda faaliyet gösterenler başta olmak üzere özel sektör kurum ve kuruluşları, üniversiteler, sivil toplum kuruluşları, araştırma toplulukları ve ülkemizdeki bireyler ile uluslararası paydaşları sayılmaktadır.

Kritik altyapı sistemlerine özgü ayrı bir Siber Güvenlik Stratejisi bulunmamaktadır ancak Ulusal Siber Güvenlik Stratejisi ve Eylem Planının (2020-2023) kapsamı içinde kamu ve özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemleri de yer almaktadır. Eylem maddelerinde yer alan faaliyetlerin, belirli kamu kurumlarının sorumluluğunda farklı kamu kurumlarının iş birliği içinde çalışmalarıyla yürütüleceği belirlirtilmiştir. Bazı uygulama adımları için ise tüm bakanlıklar ile düzenleyici ve denetleyici kurumlar, üniversiteler ve STK'lar da sorumlu ve iş birliği yapılacak kurumlar arasında sayılmıştır.

Ulusal Siber Güvenlik Stratejisinin (2020-2023), On Birinci Kalkınma Planında yer alan hedefleri de kapsayacak şekilde, uluslararası standart kuruluşları ve örnek uygulamalar ile uyumlu olarak hazırlandığı ve kritik altyapıların siber güvenliği ile ilgili önemli stratejik maddeleri de kapsadığı değerlendirilmektedir. Ancak, siber güvenliğin daha çok ulusal güvenlik açısından ele alındığı bu strateji belgesinde dijitalleşmenin sürdürülebilir olmasına değinilirken bu çalışmanın araştırma soruları arasında yer alan çevresel sürdürülebilirlik ile siber güvenlik ilişkisine hiç değinilmediği gözlemlenmiştir.

4.2.4.3 Bilgi ve İletişim Güvenliği Tedbirleri Konulu Cumhurbaşkanlığı Genelgesi

10 Temmuz 2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 no'lu Cumhurbaşkanlığı Kararnamesi ile kurulan Dijital Dönüşüm Ofisine (DDO) "Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek" görevi verilmiştir. Bu çerçevede, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri yayımlanmıştır.

6 Temmuz 2019 Tarihli ve 30823 sayılı Resmî Gazetede Cumhurbaşkanlığı tarafından Bilgi ve İletişim Güvenliği Tedbirleri konulu ve 2019 /12 sayılı genelgede gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik verilerin güvenliğinin sağlanmasına yönelik önlemlerin alınması gerektiği belirtilmiştir. Bu önlemler arasında EKS'nin internete kapalı konumda tutulması; internete açık olması durumunda ise güvenlik önlemlerinin alınması; kritik altyapı tesis ve projelerinde görev alacak kritik personel hakkında güvenlik soruşturması ve arşiv araştırması yaptırılması gerektiği sayılmaktadır. Kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere Bilgi ve İletişim Güvenliği Rehberinin hazırlanacağı; kurum ve kuruluşların rehberin uygulanmasına yönelik denetim mekanizmalarını oluşturmaları istenmekte ve yılda en az 1 kez denetlenecekleri belirtilmektedir.

Bu genelgede de kritik altyapıların siber güvenliğinin çevresel güvenlik ve sürdürülebilirlik açısından değil de daha çok bilgi güvenliğini de kapsayacak şekilde ulusal güvenlik açısından ele alınan geçici yüzeysel önlemleri kapsadığı görülmektedir.

4.2.4.4 Bilgi ve İletişim Güvenliği Rehberi

Bu genelgenin yürürlüğe girmesini müteakiben, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, Bilgi ve İletişim Güvenliği Rehberi hazırlama çalışmaları başlatılmıştır. 16 Bakanlık ile 51 Kurum ve Kuruluştan 240 uzmanın katkısı ile Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır.

Rehberin temel amacı; bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve

belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır. Rehber, kritik altyapı hizmeti veren işletmeleri de kapsamaktadır. Rehberin hedefleri arasında; güvenlik tedbirlerinin üç seviyeli olacak şekilde derecelendirilmesi ve varlık gruplarına güvenlik dereceleri ile uyumlu asgari güvenlik tedbirlerinin uygulanması; güvenlik tedbirlerinin ürün ve teknoloji bağımsız olarak uygulanabilir olması; güvenlik tedbirlerinin uygulanıp uygulanmadığının denetlenebilmesi; güvenlik tedbirlerinin birbirinden bağımsız şekilde uygulanabilirliğini sağlayacak şekilde gruplandırılması ve rehberin modülerliğinin sağlanması; Tedbirlerin teknik olarak tüm kurum ve kuruluşlar tarafından uygulanabilir olması; ihtiyaçlar, gelişen ve değişen şartlar dikkate alınarak rehberin sürdürülebilirliğinin sağlanması; rehberin hem güvenlik tedbirlerini uygulayacak personele hem de bu tedbirlerin uygulanıp uygulanmadığını kontrol edecek denetçilere hitap etmesi; rehber içeriğinin bilgi güvenliği çerçevesinde oluşturulmuş mevzuat ve rehberler ile ulusal/uluslararası standartlara uyumlu olması yer almaktadır.

Rehberde, kritik altyapıların güvenliğine yönelik tedbirler ve denetim soruları ayrı bir bölümde ele alınmıştır. Kritik Altyapıların güvenliğine yönelik tedbirler;

• Genel Güvenlik Tedbirleri

• Enerji Sektörü Özelinde Güvenlik Tedbirleri

•Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri alt başlıklarında ele alınmıştır.

Kritik altyapı sistemlerinin geleneksel bilişim sistemleri ile bütünleşmiş olmalarından dolayı, bu kapsamda uygulanacak enerji ve elektronik haberleşme sektörü özelindeki güvenlik tedbirlerine ek olarak genel güvenlik tedbirlerinin de uygulanması gerektiği belirtilmektedir.

Enerji Sektörüne özel tanımlanan güvenlik önlemleri arasında;

- EKS içerisinde yer alan tüm cihaz konfigürasyonlarının bilgi güvenliği gereksinimlerine uygun olarak yapılması;
- EKS ağı ve kurumsal BT ağı arasındaki iletişimler için erişim kontrolünün sağlanması ve yetkisiz erişimlerin engellenmesi;

- Operasyonel faaliyetlerin kritikliğinin değerlendirilerek EKS ağının belirlenen kritiklik derecesine göre segmentlere ayrılmasının ve oluşturulan ağların birbirlerinden izole edilmesi li ve erişim güvenliğine yönelik kısıtlayıcı önlemlerin alınması;
- EKS kullanıcıları ve kurum ağı kullanıcıları için ayrı kimlik doğrulama sistemlerinin kullanılması;
- EKS ağının internete kapalı konumda tutulması ve bu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise internet ve uzaktan erişim faaliyetlerine güvenlik güncellemeleri ve sıkılaştırma politikaları uygulanarak asgari seviyede izin verilmesi;
- EKS 'ne, yetkisiz kişiler tarafından yapılacak fiziksel erişimi sınırlamak amacıyla çok faktörlü kimlik doğrulama, kamera ve/veya hareket dedektörleri kullanımı, ziyaretçi kabul kuralları için süreç tanımlanması ve uygulanması, alarm mekanizmaları gibi güvenlik önlemlerinin alınması;
- EKS sistem sürekliliğinin sağlanması amacıyla sistem mimarisi dağıtık ve/veya yedekli bir yapıda oluşturulması;EKS ağının pasif olarak izlenerek veri manipülasyonunu engellemeye yönelik önlemlerin alınması;
- IED ve RTU cihazlarında hizmet veren web sunucusu olması durumunda, internet üzerinden sunucuya erişimin kapatılması ve iç ağda kimlik doğrulama mekanizmaları doğrultusunda erişimin sağlanması; sunucuya internet üzerinden erişime ihtiyaç olduğu durumlarda VPN üzerinden erişim sağlanması; MMS protokolünde kimlik doğrulama özelliğinin aktif bir şekilde kullanılması;
- SSL/TLS Korumalı İletişim EKS ağındaki MMS protokolü ile sağlanan dikey iletişimin, SSL/TLS üzerinden şifreli bir şekilde sağlanması, IED'lerde ve HMI/SCADA cihazlarında desteklenmesi durumunda SSL/TLS özelliğinin aktif hale getirilmesi;
- Enerji alt yapılarında kullanılan GPS teknolojilerinin spoofing saldırılarına karşı korunması;
- Kullanılan ekipmanın, çevresel tehditlerden kaynaklanacak olumsuz etkilere karşı gerekli önlemler alınarak korunması;

- Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmalarının yapılması ve tehdit istihbaratı verilerinin yönetilmesi amacıyla bir süreç/mekanizma tanımlanması;
- Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesinin tanımlanması;
- Ağ üzerindeki verilerin iletimi için güvenli aktarım yöntemlerinin (hava boşluğu, veri diyodu vb.) kullanılması gerektiği belirtilmektedir.

Bu güvenlik önlemlerinin gerçekleştirilip gerçekleştirilmediğinin denetlenmesinde kullanılacak sorular da ayrıntılı bir şekilde hazırlanmıştır.

Elektronik Haberleşme Sektörü için de bu sektöre özgü güvenlik tedbirleri tanımlanmıştır;

- Hizmet Güvenliği ve Sürekliliği Sağlanan iletişim hizmetlerinin güvenliğini ve sürekliliğini ele alan bir güvenlik politikasının belirlenmesi ve uygulanması gerektiği vurgulanmakta ve güvenlik politikasının; geçmişte yaşanan güvenlik olayları ve ihlalleri, hizmet kesintileri ve sektördeki diğer sağlayıcıları etkileyen olaylar dikkate alınarak periyodik olarak güncellenmesi gerektiği ve özellikle kilit personelin belirlenen güvenlik politikasına yönelik farkındalığının artırılması gerektiği;
- Üçüncü taraflardan temin edilen/hizmet alınan BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, yardım masalarına, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimlerinin sözleşmelerde detaylı olarak ele alınması;
- İletişim hizmetlerindeki altyapı servislerinin kötüye kullanımından kaynaklanacak ve müşterileri/diğer hizmet sağlayıcıları olumsuz olarak etkileyebilecek tehditler için gerekli önlemlerin alınması;
- Sinyalleşme trafiğindeki olası sahtecilik işlemlerinin tanımlanması, tespit edilmesi ve önlenmesi için bir sistemin kurulması ve işletilmesi; sinyalleşme trafiğinin izlenmesi, gizlilik ve bütünlüğünü tesis edecek önlemlerin alınması;
- Sağlanan iletişim hizmetlerinde müşterilerin kaynak IP adreslerinin doğrulanmasına olanak tanıyan sistemlerin kullanılması, hatalı, değiştirilmiş (spoofed) IP adreslerinin şebekede dolaşımını engellemek için gerekli önlemlerin alınması;

- Sunucular, yönlendiriciler ve diğer şebeke elemanlarının saldırı yüzeyini azaltmak için gerekli sıkılaştırma kontrollerinin uygulanması;
- Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizmasının kurulması;
- Haberleşme sistemlerinde kullanılan ekipmanın, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korunması amacıyla gerekli önlemlerin alınması;
- Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmalarının yapılması ve tehdit istihbaratı verilerinin yönetilmesi amacıyla bir süreç/mekanizmanın tanımlanması;
- Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesinin tanımlanmış olması;
- Haberleşme hizmetinde, arayan numara manipülasyonunu (Caller ID Manipulation) engellemeye yönelik teknik ve hukuki tedbirlerin alınması gerektiği belirtilmekte ve bu tedbirlerin alınıp alınmadığının kontrolü için kullanılacak ayrıntılı soru önerilerine de yer verilmektedir. Bu kısımda da iletişim güvenliğine yönelik ayrıntılı güncel önlemler listesi hazırlandığı görülmektedir. Bu dokümanın internet üzerinde tüm paydaşların erişimine açık olduğu ve ihtiyaç duyuldukça gerekli değişikliklerin yapılarak güncel halinin muhafaza edileceği anlaşılmaktadır.

Rehberin hazırlanmasında, uluslararası geçerliliği olan standartlardan ve yayımlı kılavuzlardan yararlanılmıştır (T.C.CBDDO,2020:215).

Dokümanda, varlık grubunun etki alanı açısından değerlendirilmesinde uygulanan ankette varlık grubunun işlediği veri açısından incelendiğinde kritik bilgilerin gizlilik, bütünlük ve erişilebilirlik açısından değerlendirilmesinde varlık grubunun ele geçirilmesi, değiştirilmesi ya da devre dışı bırakılması durumunda oluşacak zarar bireysel, kurumsal, sektörel, milli güvenlik ve ulusal çıkarlar, toplumsal kargaşa ve bağımlılık açısından irdelenmektedir (T.C.CBDDO,2020:218-219).

Bilgi ve İletişim Güvenliği Rehberi stratejik bir doküman olmasının yanısıra kurumlara yönelik operasyonel faaliyetlerin nasıl yürütüleceği ve nasıl denetleneceği hususlarını da kapsayan önemli bir operasyonel faaliyet dokümandır. Kapsamında kritik

altyapılara da ayrıca yer verilmiştir. Bu dokümanda da kritik altyapıların siber güvenliğine daha çok ulusal güvenlik açısından yaklaşılmış ve oluşabilecek çevresel güvenlik sorunları gündeme getirilmemiştir.

4.2.4.5 Türkiye Afet Müdahale Planı (2022)

Kritik altyapıların siber güvenliği deprem, yangın, sel gibi afetler sonucu meydana gelebilecek siber güvenlik olaylarından etkilenebileceği ve bir siber güvenlik olayı meydana gelmesi durumunda oluşturabilecekleri çevresel güvenlik sorunları ve acil durumlar göz önünde bulundurularak Afet ve Acil Durum Yönetimi (AFAD) Başkanlığının da kapsama alanı içine girmektedir.

AFAD tarafından hazırlanan Türkiye Afet Müdahale Planında (TAMP) afet, "Toplumun tamamı veya belli kesimleri için fiziksel, ekonomik ve sosyal kayıplar doğuran, normal hayatı ve insan faaliyetlerini durduran veya kesintiye uğratan doğal, teknolojik veya insan kaynaklı olaylar" şeklinde tanımlanmıştır (T.C.İçişleri Bakanlığı,2022:57).

Türkiye Afet Müdahale Planının amacı; afet ve acil durumlara ilişkin müdahale çalışmalarında görev alacak hizmet grupları ve koordinasyon birimlerine ait rolleri ve sorumlulukları tanımlamak, afet öncesi, sırası ve sonrasındaki müdahale planlamasının temel prensiplerini belirlemektir. TAMP, ülkemizde yaşanabilecek her tür ve ölçekte, afet ve acil durumlara müdahalede görev alacak, bakanlık, kurum ve kuruluşlar, özel kuruluşlar, STK'lar ve gerçek kişileri kapsamaktadır (T.C.İçişleri Bakanlığı,2022:3).

Ulusal düzey hizmet grubu planlarının hazırlanması ve uygulanmasından hizmet grubundan sorumlu ana çözüm ortağı olan bakanlık, kurum ve kuruluşlar asli sorumlu olmakla birlikte, hizmet grubu planlarında görevlendirilen destek çözüm ortağı bakanlık, kurum ve kuruluşlar, özel sektör, STK'lar ve gerçek kişiler de ayrı ayrı sorumludur (T.C.İçişleri Bakanlığı,2022:3).

TAMP'nın hedefleri arasında;

- Hayat kurtarmak,
- Kesintiye uğrayan hayatı ve faaliyetleri en kısa sürede normale döndürmek,
- Müdahale çalışmalarını hızlı ve planlı bir şekilde gerçekleştirmek,
- Halk sağlığını korumak ve sürdürmek,

- Mülkiyet, çevre ve kültürel mirası korumak,
- Ekonomik ve sosyal kayıpları azaltmak,
- İkincil afetleri önlemek ya da etkilerini azaltmak,
- Kaynakların etkin kullanımını sağlamak sayılmaktadır (T.C.İçişleri Bakanlığı P,2022:11).

Afet türleri arasında su baskını, baraj patlaması, orman yangını, sanayi yangınları, toplu nüfus hareketleri, kimyasal, biyolojik afetler, radyolojik ve nükleer kazalar, kuraklık, deprem ve ulaşım kazalarının yanı sıra siber saldırılar da sayılmıştır. Her afet türü için faaliyette bulunması gereken afet çalışma grupları belirlenmiştir. Siber saldırı durumunda Teknik Destek ve İkmal, Güvenlik ve Trafik, Haberleşme, Enerji, Zarar Tespit, İletişim, Bilgi Yönetimi, Değerlendirme ve İzleme afet çalışma gruplarının faaliyette bulunacağı belirtilmektedir (T.C.İçişleri Bakanlığı,2022:11).

Varsayımlar arasında;

- Afetlerde yangınların çıkabileceği, sanayi ve enerji tesislerinde yangın, patlama, kimyasal sızma, akaryakıt veya petrol sızıntısı ve gaz kaçakları gibi ikincil afetler meydana gelebileceği, aynı anda birden fazla afetle birden mücadele edilmesi gerekebileceği;
- Elektrik, doğalgaz, içme suyu, arıtma ve kanalizasyon tesislerinin ağır hasar görebileceği ve çalışamaz hale gelebileceği, bu durumun susuzluğa ve salgın hastalıklara yol açabileceği, ısınma, aydınlatma ve enerji sorunlarının ortaya çıkabileceği,
- Afetlerin kritik tesislerde hasar yaratabileceği de sayılmıştır (T.C.İçişleri Bakanlığı,2022:17).

Afete müdahale için afetin etki derecesine bağlı olarak yerel, ulusal ve uluslararası destek faaliyetlerinin planlanması gerektiği belirtilmekte ve farklı hizmet birimlerinin tanımı yapılmaktadır (T.C.İçişleri Bakanlığı,2022:24-31).

İl afet ve acil durum koordinasyon kurulunun görevleri arasında Kritik tesislerin oluşturduğu riskleri önleme çalışmaları yapmak veya yaptırmak da sayılmıştır (T.C.İçişleri Bakanlığı,2022:22).

Afet durumunda ve öncesinde yerel, ulusal ve uluslararası çözüm ortaklarının görev ve sorumlulukları belirlenmiştir. Afet çalışma grupları ve bu çalışma gruplarının ana çözüm ortakları ve destek çözüm ortakları belirlenmiştir. Uluslararası destek ve koordinasyon alanında destek çözüm ortağı olarak Dışişleri Bakanlığı, Ticaret Bakanlığı, Türk Kızılayı belirlenmiştir (T.C.İçişleri Bakanlığı,2022:35-57).

Türkiye Afet Müdahale Planının, kritik altyapıların siber güvenliğine yönelik daha çok doğal afetler sonrası gerçekleşecek hasarı azaltmaya yönelik bir plan olduğu; bir kritik altyapıda meydana gelebilecek siber güvenlik olayı sonrası oluşabilecek hasarı gerektiği kadar adreslemediği ve bu tür bir afet için gerekli koordinasyon faaliyetlerine yer verilmediği anlaşılmıştır.

4.2.4.6 AFAD Stratejik Plan (2019-2023)

Türkiye Afet Müdahale Planınında yeteri derecede ele alınmamış olan Kritik Altyapıların güvenliğine yönelik faaliyetlere stratejik Planda daha çok yer verildiği gözlenmiştir. Kritik altyapı tesislerinin önceliklendirilmesi için metodolojinin belirlenmesi ve yazılım haline getirilmesi, Endüstriyel kazalara ilişkin modelleme yazılımının geliştirilmesi, iklim değişikliğinin neden olabileceği afetlere yönelik risklerin belirlenmesi faaliyetlerine yer verilmiştir (Afad Stratejik Plan 2019-2023,2019:88)

Stratejiler arasında, Büyük depremler sonrası kritik yapılarda meydana gelebilecek ikincil afetlere önlem alınması sağlanacağı ve bu konudaki farkındalığın artırılacağı ifade edilmektedir (Afad Stratejik Plan 2019-2023,2019:89).

Stratejik Planda da, TAMP-2022'de olduğu gibi riskler arasında siber saldırılar da sayılmış (Afad Stratejik Plan 2019-2023,2019:99) ancak konu ile ilgili ayrıntıya yer verilmemiştir.

İhtiyaçlar arasında ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nin kurulması; siber saldırılara karşı etkin tedbirlerin alınması; Güvenlik Operasyon Merkezi'nin kurulması; Bilgi Güvenliği Yönetim Sistemi uygulaması kapsamında personele farkındalık eğitimleri verilmesi; AFAD bilişim sistemlerinin iş sürekliliğinin sağlanması sayılmıştır (Afad Stratejik Plan 2019-2023,2019:114).

Meydana gelebilecek deprem, yangın, sel gibi doğal afetler sonrasında kritik altyapılarda ikincil hasarın oluşması ile ya da kritik altyapılarda istemli istemsiz insan

davranışları sonucu oluşabilecek bir siber güvenlik olayı sonrası oluşabilecek afet durumunun çevresel güvenliği ve sürdürülebilirliği engellemesinin önüne geçmek üzere yapılacak faaliyetlerin AFAD ve diğer ilgili kurumların koordinasyonu ile gerçekleştirilmesinin ve gerekli faaliyet planlarının hazırlanmasının çok önemli olduğu değerlendirilmektedir.

4.3 KÜRESEL SEVİYEDE KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK STRATEJİK FAALİYETLER

Bir önceki kısımda kritik altyapıların siber güvenliğinin sağlanmasında devletlerin rolü araştırılırken ulusal seviyede önleyici koruyucu güvenlik yaklaşımının emniyetli ve sağlam sistemler oluşturulmasına ve derinlemesine savunmaya evrildiği ve devletlerin bu alanlara yönelik politikalar belirlediği, risk yönetimi yaklaşımını, caydırıcı yaklaşımı ve temelde de devletlerin asıl görevlerinin kendi sınırları içinde yaşamakta olan vatandaşlarının güvenliğini sağlamaktan sorumlu oldukları için kamu yararı yaklaşımına uygun hareket ettikleri bilgilerine ulaşılmıştır. Günümüz modern toplumlarında kritik altyapı sistemlerinin önemli bir kısmının özel sektöre ait olduğu ve siber uzayın doğası gereği bu sistemleri devletlerin tek başlarına yönetemeyecekleri, konu ile ilgili kamu kurumları, özel sektör temsilcileri, devlet dışı küçük gruplar, üniversiteler ve uluslararası paydaşlarla yönetişim esasına uygun politikalar geliştirmeleri gerektiği anlaşılmıştır. Devletlerin kritik altyapıların siber güvenliğini sağlamak ve kriz yönetimini gerçekleştirmek üzere kendi içlerinde, paydaşlarla koordinasyon, bilgi paylaşımı ve iş birliği, araştırma geliştirme faaliyetlerini yönetişim esaslarına uygun olarak yerine getirebilmeleri için belirlenecek politikaları kapsayan ulusal siber güvenlik stratejilerinin ne tür özellikler taşıması gerektiği üzerinde durulmuştur.

Kritik altyapıların yazılım, donanım ve ağ bileşenleri devlet sınırlarına bağlı olmaksızın uluslararası alanda birbirlerine bağlı olduğu için ve bir kritik altyapı sistemindeki sorun diğerlerine de sıçrayabileceği için siber güvenlik alanında devletlerin tek başlarına yapabilecekleri sınırlıdır (Rajamaki,2017:233). Buradan hareketle kritik altyapıların siber güvenliğinin küresel seviyede ele alınması gerektiği anlaşılmaktadır. Bu amaçla bu kısımda öncelikle küreselleşmeden kaynaklanan siber güvenlik sorunları ele alınacak; daha sonra

küresel yönetişim ve küresel siber yönetişim kanalları üzerinde durulacak; uluslararası siber güvenlik paydaşları incelenecek; kritik altyapıların küresel seviyede siber güvenliğinin sağlanmasına yönelik yayımlanan ve kullanımda olan standartlar, en iyi uygulama rehberleri vb. dokümanlar incelenecektir. Yine bu bölümde küresel yönetişimin sorunları üzerinde durulacak ve çevre etiği açısından değerlendirilerek kozmopolitanizm kavramı gündeme getirilecektir.

4.3.1 Küreselleşmeden Kaynaklanan Siber Güvenlik Sorunları

Geçtiğimiz yüzyılın son dönemlerinden itibaren toplumsal hayatta önemli değişikliklerle yüz yüze gelinmiştir. Olumsuz çevre koşulları artmış ve küresel seviyede ekosistem üzerinde yıkıcı etkileri katlanarak artmaya başlamıştır (Rosenau,2014:271). İnsan sağlığına ve refahına zararlı maddelerin atmosfer veya okyanuslar üzerinden uzun mesafeli taşınması olarak tanımlanan çevresel küreselciliğin bazıları doğal yollarla gerçekleşirken son dönemlerde insan faaliyetlerinden kaynaklanan pek çok olay da yaşanmaya başlanmıştır (Keohane ve Nye,2014:98-99). Büyük oranda OECD ülkelerinde yoğunlaşan BT üretimi dünya üzerinde karmaşık teknolojik karşılıklı bağımlılık ilişkilerini oluşmuştur. 1990'larda dünya üzerindeki firmalar ve bireyler bu teknolojileri kullanarak ürünlerini pazarlayabildikleri yerlerde, kendi ulusal sınırlarının ötesindeki üreticiler ve piyasalarla birleşmişler ve çok uluslu şirketler temelli üretim ağlarını güçlendirmişlerdir. Bu tarz faaliyetler ile ulus ötesi üretim ağlarında teknolojik uygulama bilgisinin yoğunlaşması sonucu sınır ötesi üretim ağları gittikçe karmaşıklaşmış ve dünya üzerinde daha geniş alanlara yayılmıştır. Teknolojinin bu şekilde üretilmesi ve aktarılması ile, ulus ötesi üretim ağlarının yapısı ve dinamiği gelişmiş; küreselleşme daha da yaygınlaşmaya başlamıştır (Castells,2014:379-380).

Kritik altyapılara yönelik siber güvenlik olayları da küresel seviyede önemli çevre sorunlarına yol açabilecek, can ve mal kaybına neden olabilecek ve sürdürülebilirlik kavramına uygun olarak gelecek nesillerin de en az bugün yaşamakta olan nesillerin sahip oldukları kaynaklar ve doğal çevreye sahip olarak varlığını devam ettirmesine engel olacak küresel sorunlar arasında yerini almıştır. Kritik altyapıların korunması her geçen gün artan bir şekilde ağlara, elektriğe ve bilişim sistemleri altyapısına bağımlı hale gelmektedir. Doğal afetler ya da bilişim sistemlerine yönelik suçlar ile gerçekleşen siber olayların etkileri ulusal

sınırların dışına taşmaktadır. Bu tez kapsamında incelenmekte olan çevre etiği bağlamında sürdürülebilirliği engelleyebilecek olan kritik altyapıların siber güvenliği de önemli ölçüde insan faaliyetlerinden etkilenmektedir.

Devletin bireylere sağladığı en temel hizmet güvenliktir. Güvenlik, egemen bir ortamda hayati çıkarların korunması olarak tanımlanmaktadır. Nükleer silahların ortaya çıkması ile güvenlik küreselleşmiştir. Günümüz dünyasında devletlerin fiziki sınırlarını aşan siber uzaydan kaynaklı olarak sınır ötesi sorunların sıklıkla ortaya çıkması nedeni ile, belli sınırlar üzerinde mutlak egemenliğe dayanan Westpalia ilkesine göre oluşturulmuş mevcut dünya düzeni her geçen gün daha da yetersiz hale gelmektedir. Bu durumda etkin siyasi güç sadece ulus devletlerle sınırlı kalmayıp, ulusal gücün yanı sıra bölgesel ve uluslararası düzeyde farklı aktörler de değişik alanlarda etkin güç haline gelmektedir. Küresel seviyedeki gelişmeler çok kısa süreler içinde yerel sonuçlar oluşturabilmekte, yerel sorunlar da çok kısa süre içinde küresel sonuçlar doğurabilmektedir (Held ve McGrew,2014:53-54). Sahip olunan teknolojik olanaklarla sabit bir konuma yerleştirilmeksizin, fiziki mesafeden etkilenmeden, fiziki sınırları tümüyle görmezden gelerek küresel seviyede yürütülmekte olan pek çok faaliyet bulunmaktadır. Bir işlemin internet ya da diğer ağlar üzerinden bilişim teknolojileri kullanılarak gerçekleştirilmesinde mesafenin hiçbir önemi kalmamaktadır (Scholte,2014:108-110). Bilişim teknolojilerindeki gelişmeler ile ve özellikle internetin hayatımıza girmesi ile zaman ve uzaklık kavramları eski önemini yitirmiş; devletlerin egemenlik alanları ve sınırları laçkalaşmış ve bir karmaşıklık dönemi yaşanmaya başlanmıştır (Rosenau,2014:271). Artık güvenlik, iki devlet arasındaki sorunlardan çok küresel seviyede ortak sorunlara ya da bölgesel seviyede çok taraflı sorunlara ilişkin olabilmektedir. Bu da temel amacı vatandaşının güvenliğini sağlamak olan modern devletleri tartışmalı hale getirmektedir.

Bilişim teknolojilerindeki gelişmeler ile günümüz küresel dünyasında, siber uzay üzerinden devletler, kurumlar, insanlar arasında devletleri ve toplumları aşan çok karmaşık bağlantılar kurulmaya başlanmıştır (Held ve McGrew,2014:54-55). Ulus devletlerin kendi olanakları ile çözüm bulmakta yetersiz kaldığı, kaynakların yetersiz hale gelmesi, çevre sorunları gibi durumlarda güçlü devletler diğer toplumlar adına da kararlar alabilmekte ve ulus ötesi aktörler ve güçler ulus devletleri ve sınırlarını etkisiz hale getirebilmektedir.

Küresel seviyede etkin güç durumuna geçen tüm aktörlerin kime karşı ne tür sorumluluklar taşıyacağı ve nasıl davranacağının belirlenmesi ve belli kurallara bağlanması oldukça zordur. Mevcut durumda bölgeselleşmiş ve küreselleşmiş dünyanın ulusal ve birbirinden ayrı karar alma birimleri arasında uyumsuzluk, ulus ötesi sorunlar karşısında devletlerin sorumluluktan kaçması ve kalıcı ortak çözümlerin bulunamaması gibi sorunları gündeme gelmektedir. (Held ve McGrew,2014:56-58). Bu durum, ulusal sınırların etkisiz hale geldiği siber güvenlik konusunda da kendini gösterebilmektedir. Bir ulus devlet sınırları içinden başlatılmış siber saldırı sonrası fiziki olarak uzak bir devlet içindeki kritik altyapıda oluşacak siber güvenlik olayının kim tarafından, nereden başlatılmış olduğu net olarak anlaşılamayacağı için asıl sorumluların sorumluluğu üstlenmemesi; bu konu ile ilgili küresel seviyede alınan kararlara tüm devletlerin uymaması, ekonomik ve teknolojik olarak geri kalmış devletlerin kritik altyapıların siber güvenliğin sağlanmasına yönelik bütçe ayıramaması, gerekli güvenlik önlemlerini alamaması, nasıl bir güvenlik politikası izleyecekleri hususunda yeterli donanıma sahip olmamaları gibi durumlar yaşanabilmektedir.

Yirmi birinci yüzyılla birlikte siber saldırılar daha karmaşık hale gelmiş, kötü amaçlı yazılımlar dünya genelinde yayılmaya başlamıştır. Siber uzayın ulus devletlerin fiziki sınırlarından bağımsız olarak her yere ulaşması ile siber güvenlik küresel bir boyut kazanmıştır. Siber saldırılar 1990'lı yıllarda daha çok ABD ve Avrupa ülkelerinde meydana gelirken 2000'li yıllarla birlikte uluslararası hale gelmiştir. Bu bölümde incelenecek olan siber güvenlik olayları örneklerinden de siber tehditlerin küreselleştiği anlaşılacaktır. ABD'nin The Center for Strategic and International Studies (CSIS) adlı ünlü bir düşünce kuruluşu olan Stratejik ve Uluslararası Araştırmalar Merkezi, 2006- 2018 yılları arasındaki kamu kurumlarına, savunma, yüksek teknoloji şirketleri gibi yerlere karşı düzenlenen önemli siber güvenlik olaylarını derlemiştir. Bu araştırmaya göre de belirlenen önemli siber olayların çoğu İnternetin yaygın olarak kullanılmakta olduğu Kuzey Amerika, Avrupa ve Asya'daki kurbanları hedef almıştır (Puyvelde ve Brantly,2019:68).

Devletler en azından sivil kayıplara yol açmamak için dijital dünyada hiçbir devletin başka bir devletin kritik altyapılarına saldırmamasını sağlayan angajman kurallarını tanımalı ve bunlara bağlı kalmalıdır. Siber saldırganlar, fiziki olarak farklı konumlarda faaliyet

gösterdiği ve altyapıları çeşitli ülkeler arasında hızla değiştirebilecekleri için; devletler, özellikle başka devletlerin desteği ile gerçekleştirilen siber saldırıların kim tarafından yapıldığını tamamen ulusal bir yaklaşım ile çözemeyecektir; uluslararası iş birliğine ihtiyaç vardır (Inversini,2020:273-274). Clark, devlet ile güvenlik arasında köklü bir dönüşüm olduğunu, küreselleşmenin güvenlik sorunlarını dışarıdan etkilemenin yanı sıra devletin kendisini de denetlediğini savunmaktadır (Clark,2014:219-226). Devletler kendi başlarına, İnternet kullanımından kaynaklanan önemli sorunların üstesinden gelme konusunda çok geride kalmaktadır (Chatfield, 2012:131). Ulus devletlerin küresel risklerle tek başlarına mücadele edebilmeleri mümkün değildir (Beck, 2011: 364) ve bunu sağlamak üzere küresel seviyede iş birliğine ihtiyaç vardır.

4.3.2 Küresel Yönetişim

1999 yılında BMKP tarafından hazırlanan raporda, sınırların yok olduğu, mekânın ve zamanın kısıtlayıcılığının daraldığı küreselleşen dünyada günlük hayatın akışında insan güvenliğine yönelik ani ve zararlı kopuşlar oluşturan yeni tehditlere değinilmektedir. Bu tehditler arasında, bilişim teknolojilerindeki gelişmeler ile küresel suç gruplarının oluşması, etkili şebekeler geliştirmeleri de sayılmaktadır. Raporda yerel, ulusal, bölgesel, küresel güçlü bir yönetişim ile insanlık gelişiminin gereksinimlerinin karşılanabileceği belirtilmektedir. Yönetişimin sadece yönetim olmadığı, belli bir şekilde sınırlar çizen ve bireylerin, kuruluşların ve şirketlerin hareketlerini teşvik eden kurallar, kurumlar ve planlı eylemler bütünlüğü anlamına geldiği dile getirilmektedir. Küresel çatışma tehlikelerinin, ticaret savaşlarının, insanlık dışı küresel suçların güçlü bir yönetişim ile engellenebileceği vurgulanmaktadır (BMKP-1999,2014:505). İnsan hakları, göç, çevresel güvenlik gibi sınır aşan sorunları, herhangi bir önemli devletin desteğine bağımlı olmaksızın sonuç odaklı çözümler geliştirmek üzere yönetişim kavramı gündeme gelmeye başlamıştır. Küresel Yönetişim kavramı ilk kez, BM Küresel Yönetişim Komisyonu tarafından, 'Our Global Neighborhood' adıyla yayınlanan raporda kullanılmıştır. Bu raporda, yönetişim, bireylerin ve kurumların kamusal ve özel alanın kendi ortak sorunlarını yönetme yollarının toplamı şeklinde tanımlanmıştır. Geçmişte küresel yönetim ile sadece hükümetler arası ilişkiler anlatılırken bu komisyon, yönetişimin aktörleri arasında özel sektör ve devlet dışı kurumlar gibi aktörleri de saymıştır (Sinclair,2014:18). Bu dönemden itibaren BM, örgütsel

hedeflerine ulaşmak için özel sektörle temasa geçmeye başlamıştır (Syle ve King,2014:37). Yönetişimin uygulanması ile, devletler ve uluslararası kuruluşlara ek olarak toplumun çok farklı kesimlerinin de farklı alanlardaki karar alma süreçlerine katılımı hızla artmaya başlamıştır.

Yönetişim, insanların birbirleri ile sosyal, politik, ekonomik ilişkilerini ve ekosferi yönetmek için ortak kararlarını oluşturarak uygulamak üzere kullandıkları resmi, gayri resmi her türlü mekanizmalar ve süreçlerdir (Seyle ve King,2014:29). Yönetişim, devletler gibi resmî kurumların yanı sıra piyasalar ve sivil toplum gibi daha az resmi kuruluşların uygulamaları ile ilgilenmekte olup devletin eyleme geçme veya emir verme konusundaki yasama veya otoriter gücüne dayanmamaktadır (Juan ve Martin,2019:98). Küresel yönetişim kavramı, güvenlik, insan hakları, terörizm, çevre sorunları gibi ortak sorunların artışı ve bu sorunlar karşısında hükümetler arası ilişkileri yürütmekte olan ve günümüz koşullarında ortak bir amacı paylaşan birbirinden ayrı ancak birbirini tamamlayan yapıları anlatmak üzere kullanılmaktadır. Sinclair, küresel yönetişim tanımında devletleri ön plana çıkarmakta ve devletlerin ortaya çıkan ortak sorunlara yönelik ortak karar olmaları ve bu kararlar doğrultusunda hareket etme yöntemi olarak tanımlamaktadır (Sinclair,2016:1-2). Halliday bu tanımı genişleterek, devletlere ek olarak BM gibi hükümetler arası örgütlerin faaliyetlerini ve hükümet dışı STK'ları ve ulus ötesi hareketleri de kapsayan bir oluşum olarak tanımlamaktadır. Günümüz dünyasında devletlerin eylemi ile çözülemeyen, var olan mekanizmaların başa çıkmakta yetersiz kaldığı sorunların çözümüne yönelik reformlara ihtiyaç olduğuna da dikkat çekmektedir (Halliday,2014:578).

Soğuk savaş döneminden sonra devletlerin birbirine muhtaçlığının küresel sonuçları fark edilmeye başlanmıştır. Küresel ısınma, okyanusların kirlenmesi, asit yağmurları, nükleer kazalar sonucu oluşan hava kirliliği ulus devletlerin sınırlarına bağlı olmaksızın küresel olarak olumsuz etkiler yaratabilmektedir. Bu sorunların daha da artması ve insanlar için tehlike oluşturmasının önüne geçmek için birbirine muhtaçlık kavramını daha belirgin hale getirme amacıyla küresel yönetişim ihtiyacı hakkında tartışmalar yapılmaktadır. Küreselleşmenin yoğun olarak hissedildiği günümüzde ulusal iletişim ve ekonomi sistemleri hızlı bir şekilde karmaşık bölgesel ve küresel bağlantılara, yönetsel alanda ise geleneksel hükümetlerden çok katmanlı yönetişimlere geçilmeye başlanmıştır.

Uluslararası rejimlerin ve yürürlükteki uluslararası antlaşmaların sayısında önemli ölçüde artış olmuştur. Geçmişteki kapalı siyasal alanlar artık birbiri ile kesişen ve karmaşık güç ilişkilere sahip duruma gelmiştir (Held ve McGrew,2014:53-58). Uluslararası antlaşmaların konusu insanların yanı sıra küresel ortak mirası ve içinde yaşadığımız ekosistemi de kapsamaktadır (Held-1,2014:205-207).

Yönetimler, amaçlarına ulaşmak için kurumsal yapılanmalar kullanırken yönetişim, bu toplumsal işlevlerin çok çeşitli örgütler tarafından değişik yer ve zamanlarda, bazı durumlarda aynı zamanda çeşitli yöntemlerle uygulanan ve yürütülen süreçleri kapsamaktadır. Yönetimler, hükmetme ve anayasal düzenleme gibi ayrıcalıklar yoluyla itaat sağlarken, yönetişim geleneksel normlar ve alışkanlıklar, gayrı resmi anlaşmalar, ortak dayanak noktaları ve insanları talimatlara uymaya davet eden diğer uygulamaları kullanmaktadır (Rosenau,2014:271-272).

Günümüzde dünya üzerindeki ilişkiler, yasal sürecin egemen gücü olan devletlerin oluşturduğu devletlerarası sistem ve diğer çeşitli toplulukların çok merkezli sistemi tarafından yönetilmektedir. Küresel alan, küçük-büyük, resmi-gayri resmi, ekonomik, siyasi, toplumsal, kültürel, ulusal, ulusal sınırları aşan, uluslararası-ulus altı, saldırgan-barış yanlısı, liberal-otoriter, oldukça karmaşık ortaklaşa bir küresel yönetim sistemini oluşturan pek çok aktörden oluşmaktadır. Aralarındaki önemli farklılıklara rağmen dünya siyasetinin yönetim ve yönetişim mekanizmaları kendi kurallarını koruyarak ortak çıkarları için birlikte hareket ettiklerinde eşgüdümü sağlamak için melez kurumlar oluşturmaktadırlar (Krasner,1983:2'den aktaran Rosenau,2014:272). Devletler hâlâ küresel arenanın temel oyuncularındandır ancak artık tek ana kurum değildirler; otoriter ve yasal güç olmalarına rağmen önemli güçlerini her geçen gün daha da kaybetmektedirler. Bazı önemli faaliyetler devlet sınırları içinde değil, sınırlar arasında özel girişimler ile gerçekleştiği için küresel alandaki egemen karakterleri de aşınmaktadır (Rosenau,2014:272).

Küresel yönetişim, insanlar için önem taşıyan temel sorunları çözme potansiyeline sahiptir. Devletler, kendi iç hukuk ve kurumları ile çevresel standartlarını yasalaştırarak uygulayabilirler ancak çevresel sistemler kapalı sistemler olmadığı için çevresel sorunlar devletlerin fiziki sınırları içinde kalmamakta olup küresel yönetişimin konuları arasında yer almaktadır (Sinclair,2016:23). Dünya üzerinde farklı bir fiziki alandan gerçekleştirilebilecek

olan siber saldırı ile çok uzak fiziki alandaki nükleer santralde meydana gelecek bir siber güvenlik olayı sonucu oluşacak çevre felaketi sadece kendi bulunduğu alanla sınırlı kalmayacak, küresel seviyede tüm devletleri etkileyebilecektir. Buradan hareketle bu çalışmanın temel konusu olan çevre etiği bağlamında siber güvenliğin sağlanması kesinlikle ulus devletlerin kendi sınırları içinde kendi kuralları ile halledebilecekleri bir durum değildir; bölgesel, çoğu durumda da küresel seviyede yönetişim yönteminin kullanılmasını gerektirmektedir.

4.3.3 Küresel Siber Güvenlik Yönetişimi

Siber güvenlik yönetişimi, bilişim altyapılarına yönelik tehditlere karşı siber güvenlik olayı gerçekleşmeden önce ve bir siber olay sonrası yapılması gerekenleri belirlemek, siber olayın kapsamını ve sınırlarını belirlemek ve koordine etmek için paydaşlar tarafından kullanılmakta olan çeşitli yaklaşımları anlatmak üzere kullanılmaktadır. Siber ortamda etkileşimde bulunan oyuncuların sayısı her geçen gün arttığı için bu altyapıya ve bileşenlere yönelik tehditleri önlemek ve meydana gelmeleri durumunda da bu siber olaylarla başa çıkabilmek için iş birliği ve koordinasyon gereklidir. Siber güvenlik yönetişimi, sadece bilinen tehditlere yönelik kısa vadeli ve somut yaklaşımları değil, belirsizliği azaltmak ve uzun vadede beklenmeyen olaylardan kaynaklanan tehditlere yanıt verebilmek için gerekli süreçler ile yapıların geliştirilmesini ve uygulanmasını da içermelidir (Adams vd.,2019:133).

Yönetişim temelde etkileşimli, yönetenlerin, yönetilenlerin ve aracıların sürekli katılımını gerektiren; çok çeşitli teknikleri kullanabilen esnek bir güç ilişkisidir. (Shires,2019:108). İnternetin küresel erişim olanağına sahip olduğu için siber güvenlik olaylarının yerelleştirilmesi zordur ancak geniş küresel kurallar paralelinde bölgesel çözümler de kullanılabilmektedir.

Siber güvenlik yönetişimi için öncelikle daha geniş kapsamlı uluslararası internet yönetişimi bağlamına oturtulmalıdır. Dünya üzerinde devletler, kendi yönetim şekillerine göre İnternet yönetişimine farklı yaklaşımlar sergilemektedir. Liberal devletler, hükümet, sivil toplum ve özel sektörün tümünün katıldığı çok paydaşlı yaklaşıma uygun faaliyetler gösterirken otoriter devletler ulusal sınırları aşan bilgi akışının hükümet tarafından kontrol altına alınması şeklinde faaliyetler sergileyebilmektedir (Shires,2019:22).

Siber güvenliğin sağlanmasına yönelik uluslararası iş birliği kavramı, sadece 'devletler arasında" bir iş birliği değildir. Bu konu daha çok devlet dışı kuruluşlar tarafından ele alınan bir konudur. Örneğin, kökleri akademiye dayanmakta olan "akredite Bilgisayar Olaylarına Müdahale Ekiplerinden (CERT) oluşan Uluslararası Siber Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST) grubu, uluslararası siber güvenliğin kolaylaştırılmasında devletler açısından da önemli bir rol oynamaktadır. Büyük ölçüde gönüllülerden ve giderek artan bir şekilde özel sektör temsilcilerinden oluşan bu gruplarda devletin rolü oldukça sınırlıdır. Devlet, özellikle "çok paydaşlı yönetişim"i benimsemişse, bu grupların çalışmaları üzerinde çok fazla doğrudan etki iddiasında bulunamaz. Onları kendi kendini organize etmeye teşvik edebilir ve genellikle olası katılıma açık bir kapı sağlamaya çalışabilir. Hükümetler, daha çok İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) ve ITU gibi politika odaklı kuruluşlarla, ancak özellikle 'siber diplomasi' konularında etkili çalışmalar yapmaktadır Hızla gelişen bu alan, siber uzayda devlet davranış normları ve devletler arasında güven artırıcı önlemlerin tartışılması gibi konularla ilgilenmektedir.

4.3.4 Küresel Siber Güvenlik Yönetişiminin Kurumsal Yapıları

Küreselleşmenin uluslararası politika üzerinde, kurumlarla ilgili önemli etkileri vardır. Devletlerin, tek başlarına çözemedikleri sorunlar için küresel toplum olarak da adlandırılabilecek devletler arası organizmalar ortaya çıkmıştır. Ulusların tek başlarına halledemeyecekleri konularda uluslararası düzenleyici önlemler oluşturmanın da yolları aranmaktadır (Hoffman,2014:138).

Küresel yönetişimin aktörleri arasında, 4.2.1.2 de devletler seviyesinde ele alınan kamu kurumları, devlet içinde faaliyet göstermekte olan yerli özel sektör firmaları, devlet dışı küçük gruplar, üniversiteler ve bireylere ek olarak çoğu kez birlikte faaliyetler yürütmekte olan ve ayrıştırılmaları zor olan, geleneksel uluslararası ve bölgesel kuruluşlar, çok paydaşlı kuruluşlar ve yönetsel ağlar, çok uluslu şirketler, sivil toplum örgütleri de sayılmaktadır. Bilişim teknolojilerinde son dönemde yaşanan hızlı gelişmeler neticesinde siber uzayın doğası gereği her geçen gün yenileri kurulmakta olan siber güvenliğe yönelik kuruluşlardan bazıları aşağıda yer almaktadır:

4.2.4.1 Uluslararası ve Bölgesel Kuruluşlar

Bilişim teknolojilerinin kullanımının artması ile zaman ve uzaklık kavramlarının da anlamını yitirdiği küreselleşmiş günümüz dünyasında, geçmişte ulusal sınırlar çerçevesinde çalışmakta olan devlet kurumları yine merkezde olmaya devam ederek; küresel seviyedeki sorunların çözümü için devletlerin birlikte kurduğu uluslararası ve bölgesel kuruluşlar ile iş birliği içinde birtakım faaliyetleri başarılı bir şekilde yürütmektedirler. Artık devletler sadece kendi ulusal hukuk kurallarına göre davranmakla kalmamakta, uluslararası ve bölgesel kuruluşlarla yaptıkları sözleşmelere de uymak; dünyanın fiziki olarak çok uzak bölgelerindeki kurumlara uygun davranmak zorunda kalmaktadırlar.

Sınır aşan diğer sorunlara ek olarak siber güvenlik alanında da önemli faaliyetlerde bulunan; ulus devletlerin bir araya gelmesi ile kurulan ve İnversini'nin uzun vadede siber barışı oluşturabilecek önemli aktörler arasında gördüğü uluslararası ve bölgesel kuruluşlardan bazıları aşağıdadır (Inversini,2020:273-274):

i. Birleşmiş Milletler (BM): İkinci Dünya Savaşının bitmesini müteakip 1945'te ABD önderliğinde galip devletler tarafından, savaş dışında barışçıl ve istikrarlı bir dünya yaratmak üzere, çeşitli sorunlarla baş etmede bilim ve uzmanlık kullanılarak uluslararası barışı sağlayacak etkin bir örgüt olan Birleşmiş Milletler kurulmuştur (Sinclair, 2016:13). Sınır aşan küresel çevre sorunlarına yönelik Kyoto Protokolü, Rio Konferansı gibi faaliyetlerin yanı sıra siber güvenlik alanında da ulus devletlerin temsilcilerinin oluşturduğu gruplar ile önemli faaliyetler gerçekleştirilmeye devam edilmektedir.

ii. Şanghay İşbirliği Örgütü (ŞİÖ): Çin, Rusya, Kazakistan, Kırgızistan, Özbekistan, Tacikistan, Hindistan ve Pakistan'ın üye olduğu bölgesel bir kuruluştur. ŞİÖ tarafından 2009 yılında imzalanan Bilgi Güvenliği Anlaşmasında, batılı devletlerin "siber güvenlik" olarak adlandırdığı kavramı "bilgi güvenliği" olarak adlandırılmış; siber tehditler arasında siber uzaydaki hâkim devletlerin diğer devletlerin çıkarlarına ve güvenliğine zarar verecek şekilde davranma olasılığı ile küresel ve bilgi altyapısının güvenli ve istikrarlı operasyonlarına yönelik doğal ve/veya insani tehditler de sayılmıştır. ŞİÖ'nün 2011'de ve 2015'de BM Genel Kuruluna sunduğu taslaklar, aşırı devlet kontrolü önerdiği iddiası ile reddedilmiştir (Alcântara,2018:553).

iii. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD): Devletler, politika yapıcılar ve vatandaşlarla birlikte, çeşitli sosyal, ekonomik ve çevresel zorluklara çözüm bulmak üzere uluslararası standartlar oluşturmak için politikalar geliştirmekte olan uluslararası bir kuruluştur (https://www.oecd.org/about/). OECD, sıklıkla kritik altyapıların yönetişimi alanında önerileri kapsayan dokümanlar yayınlamaya devam etmektedir.

iv. Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT): 57 üyesi bulunan 2012 yılından itibaren, siber güvenlik alanında BİT kullanımından kaynaklanabilecek riskleri azaltmak için iş birliğini, öngörülebilirliği ve istikrarı artırarak güven artırıcı önlemler geliştirmeye çalışmaktadır. 2013 yılında siber güvenlik bilgi paylaşımına ilişkin güven artırıcı önlemler kabul edilmiş; 2016 yılında kritik altyapıların korunmasını da kapsayan önlemler kabul edilmiştir. AGİT, üzerinde anlaşmaya varılan güven verici önlemlerin uygulanması ile ilgili tartışmaları sürdürmek üzere sürekli bir çalışma grubu kurmuştur (Meyer,2020:354).

v. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA): Siber kriz yönetimi gibi alanlarda temel olarak bilgi ve rehberlik sağlamak üzere Avrupa Birliği (AB) kapsamında 2004 yılında kurulan ENISA'nın, 5 Haziran 2019 itibarı ile sorumlulukları ve kaynakları artırılmış; kalıcı bir yetki belirleyen AB Siber Güvenlik Yasası yürürlüğe girmiştir. Bu yasal düzenleme, BİT ürünleri için daha önce önerilen AB çapında siber güvenlik sertifikalandırma çerçevesini güçlendirmekte ve bunun denetimini düzenlemektedir. Avrupa komisyonu ve ENISA'nın yanı sıra Avrupa Konseyi'nin Siber Suç Sözleşmesi Konseyi (T-CY), Siber Suç Sözleşmesinin etkin kullanımını ve uygulanmasını, bilgi alışverişini ve gelecekte yapılacak güncellemeleri değerlendirilmesi görevlerini üstlenmiştir. Konsey, siber suçlarla ilgili değerlendirmeler ve raporlar yayımlamıştır (T-CY,2021). Avrupa genelinde politika/mevzuat, finans ve operasyonel önlemler alanlarında çalışmaların yapıldığı bu kurumsal yapılarla siber güvenlikle ilgili konularda kapsamlı ve uyumlu bir yönetişim sağlanması amaçlanmaktadır (https://www.enisa.europa.eu).

vi. Kuzey Atlantik Paktı (NATO): Askeri operasyonlar sırasında üyeleri ile bağlantı kuracağı kapsamlı siber altyapıya sahip olan NATO, kendi sistemlerinin siber güvenliğini iyileştirmeye yönelik faaliyetlerde bulunmaktadır (Luiijf&Healey,2012:135-137). NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE), çok uluslu ve disiplinler arası bir siber savunma merkezidir. Kritik altyapıların siber güvenliğinin sağlanmasına

yönelik CCDCOE, NATO'nun misyonu, teknoloji, strateji, operasyonlar ve hukukun odak alanlarını kapsayan siber savunma araştırmaları, eğitimleri ve tatbikatları alanında benzersiz disiplinler arası uzmanlıkla üye devletleri desteklemektir (https://ccdcoe.org/about-us).

vii. Dünya Bankası: 189 devletin üye olduğu Dünya Bankasının, gelişmekte olan ülkelerde yoksulluğu azaltarak küresel seviyede ortak refahı sağlamak üzere sürdürülebilir kalkınma için çalışan bir kurum olduğu vurgulanmaktadır (https://www.worldbank.org/en/who-we-are). Düşük ve orta gelirli ülkelerde, bilişim teknolojilerinin başlangıç yıllarında geliştirilmiş olan ve halen kullanılmakta olan ve siber saldırılara karşı korunmasız durumdaki kritik altyapılara ve birbirine ağlarla bağlı yeni nesil teknolojilerden kaynaklanabilecek siber risklere dikkat çekilmekte ve bu ülkelere riskler konusundaki farkındalığın artırılması, siber güvenlik ihtiyaçlarının belirlenmesi, teknik çözümler sunulması, gerekli altyapı yatırımları ve güven ilişkileri kurmak gibi konularda yardımcı olmak üzere ortaklık yaklaşımını benimsemektedir (https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview).

4.2.4.2 Çok Uluslu Şirketler

1990'lı yıllarla birlikte malların ve hizmetlerin üretimi, dağıtımı ve yönetiminin hızla uluslararasılaşması süreci ile doğrudan yabancı yatırım artmış, küresel seviyede çok uluslu şirketler belirleyici olmuş ve uluslararası üretim ağları oluşmuştur. Doğrudan yabancı yatırım küresel seviyedeki üreticiler olan çok uluslu şirketlerin büyümesi ile yakın ilişkilidir. Çok uluslu şirketlerin üst düzey elemanları, şirket kültürü ve kuruldukları ülkenin hükümetiyle ayrıcalıklı ilişkileri onların ulusal özellikleridir. Ulusal kökene bakılmaksızın en yetenekli olanlar şirket yönetiminde önemli görevlere getirilerek yüksek kademelerde çok kültürlülük sağlanmaktadır. İş ilişkileri ve siyasi ilişkiler, firmanın iş yaptığı ulusal bağlama özgüdür. Bu firmalar küresel seviyede büyüdükçe yayıldığı her ülkenin koşullarına göre iş ilişkileri ve siyasi bağlantıları da büyümektedir. Bu açıdan bakıldığında da bu firmalar ulus ötesi şirketler değil, iş yaptıkları uluslara bağlılıklarından hareketle çok uluslu şirketlerdir. 1990'larla birlikte küresel mal ve hizmetlerin üretimi artan bir şekilde çok uluslu şirketler tarafından değil, ağ üzerinden temel işlevleri yerine getirmek üzere birbiri ile bağlantılı çalışabilen ulus ötesi üretim ağları tarafından gerçekleştirilmektedir. Bazı ülkelerdeki küçük ve orta ölçekli işletmeler de küresel üretim sistemi içinde rekabet edebilme olanağı sağlayan,

iş birliği ağları oluşturarak bu ağlar üzerinden çok uluslu şirketlerle bağlantılı hale gelmektedirler. Küçük ve orta ölçekli firmaların oluşturduğu bu ağların çoğu, sınırlar ötesinde işleyen anlaşmalardan dolayı ulus-ötesi özelliktedir (Castells,2014:376-377). Çokuluslu şirketlerin ve küresel ekonominin yükselişi ile devletin güç ve yetkileri ile rekabet edebilecek kaynakları ortaya çıkmıştır (Orr,2014:xviii). Çok uluslu büyük bilişim firmaları, artık devletler ve uluslar ile karşılaştırılabilir veya bazı durumlarda daha büyük küresel siyasi nüfuz düzeylerine sahip oldukları; bu tür firmaların sadece kâra odaklanabilecekleri; kamu çıkarlarının korunması görevi ise tamamen devletlere bırakıldığı için küresel güç, adalet ve sorumluluk dağılımının yeniden şekillendirilmesini gerektirmektedir (Vallor ve Rewak,2018:3-4).

Gelişmiş ve gelişmekte olan ülkelerin günlük yaşamında çok önemli etkileri olması, devletleri ve ulus ötesi ekonomik ve toplumsal yaşamın pek çok alanını düzenlediği ve yönettiği için büyük uluslararası şirketler, bir başka deyişle çok uluslu şirketler küresel yönetişim aktörleri arasında sayılmaktadır (Sinclair,2016:21).

Çok uluslu şirketler, kritik altyapıların siber güvenliğin sağlanması ve bir siber güvenlik olayının meydana gelmesi durumunda kriz yönetiminin yürütülmesi gibi faaliyetlerde devletlerle birlikte görev almaktadır. Küresel seviyede kullanılmakta olan yazılım, donanım, ağ ürünleri ve bu ürünlerin güvenliğine yönelik kuralları belirleyen çok uluslu şirketler arasında Microsoft, Oracle, Siemens, Hp gibi şirketler sayılabilir.

4.2.4.3 Çok Paydaşlı Kuruluşlar ve Yönetsel Ağlar

Çok paydaşlı yönetişimde, devlet kurumları ve diğer paydaşların bir araya gelerek ortak hedeflere ulaşabilmek için güven, karşılıklılık ve fikir birliğine dayalı olarak karar vermeleri anlaşılmaktadır. Siber güvenlikle ilgili politikaları geliştirmek üzere oluşturulan forumlar, siber güvenlikle ilgili bilgi paylaşımı sağlamak üzere gerçekleştirilen faaliyetler bu kapsamda anılmaktadır. Karmaşık, yapısal olmayan, çok aktörlü olaylarda uygulanabilecek bir yaklaşımdır (Eggenschwiler,2019:87-91).

Slaughter, her devletin eşit söz hakkına sahip olduğu resmi ve tanımlı tartışma alanlarının yerine gayrı resmi, seçici bir kurumlar kümesi önermektedir. O, bilgi çağı için en iyi örgütsel biçim olarak tanımladığı yönetim ağlarının mevcudiyetinin devam edeceğini ve uluslararası yaşamın tüm alanlarında öneminin her geçen gün daha da artacağını tahmin

etmektedir. Yönetsel ağların, uluslararası kurumların yerini almaktan çok bu kurumları tamamlamaya ve onların içine girmeye eğilimli olduklarını düşünmektedir. Bu ağlar sayesinde daha küçük devletlerin pilot projeleri ve öncü inisiyatifler için tartışma alanları oluşturulmuş olacaktır. Bunun gerçekleşebilmesi için yönetim ağlarının uygulanabilirliği sınırlandırılmamalıdır. İçinde yaşadığımız bilgi toplumu döneminde devletlerin, yönetmeye çalıştıkları özel ve yarı kamusal aktörler ile verimli ağlar kurmaları sayesinde devlet, uluslararası sistemde siyasi, ekonomik ve toplumsal iktidarın sahibi olmaya devam edebilecektir. Örgütlenme ve işlevlerdeki değişiklikler sonucu devletin kendisi de dönüşmüş olacaktır (Slaughter, 2014:242-244).

Siyasi, ekonomik, askeri, sosyal, her alanda bilişim teknolojilerinin kullanılmaya başlanması ile, küresel seviyede herhangi bir noktanın bir başka nokta ile iletişime geçebileceği, tüm kanalların açık olduğu ağlar kullanıma girmiştir. Bu ağlar sayesinde güç, bu sisteme devletlerden daha kolay uyum sağlayan aktörlere kaymaktadır. Artık hiyerarşik yapılar değil ağ yapıları daha öndedir ve otoriteyi merkezilikten uzaklaştırmaktadır (Rosenau,2014:276). İletişim ağlarını kullanan yönetişim sistemleri yolu ile, bireyler, hükümetler, uluslararası kuruluşlar, sivil toplum ve özel sektör gibi çok farklı aktörleri bir araya getirerek birbirinden bağımsız aktörlerin birlikte çalışması sağlanabilmektedir. İletişim ağı tabanlı yönetişim sistemleri küçük grupların hızlı bir şekilde harekete geçmesi ve geçerli çözümlerin başka gruplar tarafından da uygulanmasını kolaylaştıran çok amaçlı, kıvrak, uyarlanabilir sistemlerdir (Matthew Wilburn King'den aktaran Gowdy,2014:48-49). Kritik altyapıların siber güvenliğine yönelik faaliyetlerin yürütülmesinde yönetsel ağlar, devlet kuruluşlarına göre daha verimli ve hızlı faaliyetlerde bulunabilmeleri açısından büyük önem taşımaktadır (Luiijf ve Healey,2012:138-139).

Günümüz dünyasında toplumsal etkileşimin küresel şebekeleri arasında, ulus içi yerel şebekeler; ulus devlet tarafından yapılandırılmış ulusal şebekeler; devletler arası savaş, barış ve ittifaklar ile hava kirliliği, ulaşım ilişkileri, vergi antlaşmaları gibi alanlarda ulusal şebekeler arası ilişkileri yürüten uluslararası şebekeler; ulusal sınırlardan, onlardan etkilenmeden geçen, toplumsal organizasyon biçimleri şeklinde ulus ötesi şebekeler ve tüm dünyayı çevreleyen küresel şebekeler sayılmaktadır (Mann,2014:165).

Bilişim teknolojilerinin ve siber uzayın doğası gereği, kritik altyapıların siber güvenliğinin sağlanmasında, dünyanın çok farklı fiziksel alanlarında, farklı devletlerin sınırları içinde yer alan devlet kuruluşlarının, devlet tabanlı uluslararası kuruluşların, özel sektör kuruluşlarının, sivil toplum örgütlerinin, bireylerden oluşan paydaşların yönetsel ağları kullanarak küresel yönetişim mantığına uygun faaliyetlerinin en uygun ve hızlı sonuçlar alınabilecek bir yöntem olduğu değerlendirilmektedir. Çok paydaşlı kuruluşlar ve yönetsel ağlardan bazıları aşağıdadır:

i. Dünya Ekonomik Forumu-World Economic Forum (WEF): Dünya Ekonomik Forumu bünyesinde kurulmuş olan Siber Güvenlik Merkezi, kendisini "kamu ve özel sektörden oluşan küresel siber güvenlik topluluğu içinde uluslararası diyalogları ve iş birliğini geliştirmeyi görev edinmiş bağımsız ve tarafsız bir küresel platform" olarak tanımlamaktadır. Siber güvenlik uzmanları ve karar vericiler arasındaki boşluğu en üst düzeyde kapatmak üzere siber direncin artırılması, küresel iş birliğinin güçlendirilmesi ve geleceğin siber uzayından kaynaklı siber güvenlik zorluklarının ve fırsatlarının iyi anlaşılması ve güven oluşturucu çözümler getirilmesi konularına odaklanmıştır. Kurucu ortakları arasında Accenture, Fortinet, Palo Alto Networks, Salesforce, Suudi Aramco gibi büyük teknoloji firmaları, devletler, uluslararası kuruluşlar, üniversiteler ve sivil toplum kuruluşları sayılmaktadır. (https://www.weforum.org/platforms/the-centre-for-cybersecurity).

Çok paydaşlı kuruluşların yönetsel ağlar üzerinden gerçekleştirdikleri faaliyetlere verilebilecek bir örnek, **Dünya Ekonomik Forumu** (WEF) Siber Güvenlik Merkezinin, 20 ülkeyi temsilen özel sektördeki en üst düzey yöneticiler olan 120 siber liderden oluşan **Siber Güvenlik Liderliği Topluluğu** ile yaptığı çalışmadır. Siber Güvenlik Merkezi'nin çalışmalarının odak noktası, siber liderlerin algılarını ve siber güvenlik ve siber dayanıklılığın gidişatını anlamak için bir Siber Outlook Anketi ve Siber Outlook Serisi aracılığıyla verilerin toplanması ve analiz edilmesidir. Bu analizin sonuçları, siber güvenlik durumu hakkında değerli iç görülere ve siber dayanıklılığın mevcut durumu hakkındaki algılara ışık tutmuştur (WEF,2022:5).

ii. Uluslararası Telekomünikasyon Birliği (ITU), geleneksel uluslararası kuruluş olan BM altında yer alan, 193 üye devletin yanı sıra yaklaşık 900 şirket, üniversite

ve uluslararası ve bölgesel kuruluşu içeren 20.000'den fazla profesyonelden oluşan küresel kamu-özel ortaklığıdır (https://www.itu.int/en/about/Pages/default.aspx). Küresel seviyede siber güvenliğin sağlanmasına yönelik olarak standart geliştirme, eğitim ve konferanslar düzenleme gibi faaliyetlerini yönetsel ağlar üzerinden sürdürmektedir.

iii. Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST): Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), uluslararası bilgisayar güvenlik olaylarının önlenmesinde iş birliği ve koordinasyonu geliştirmeyi, olaylara hızlı tepki vermeyi ve kamu, özel sektör, eğitim kuruluşları gibi paydaşların siber olay müdahale ekiplerinin konfederasyonudur. Küresel seviyede 600'den çok üyesi vardır (https://www.first.org/). FIRST, 2007 yılında Estonya'ya yönelik siber saldırılarda Estonya Bilgisayar Olayları Acil Durum Müdahale Ekibi (CERT) ile irtibata geçmiş; diğer ülkelerin CERTleri ve internet servis sağlayıcıları ile koordinasyonuna yardımcı olmuştur (Luiijf ve Healey,2012:138-139). FIRST ayrıca üyeleri arasında güncel en iyi uygulama belgelerine erişim, güvenlik uzmanları için teknik konferans, uygulamalı dersler, yıllık olay müdahale konferansı, yayınlar ve web hizmetleri gibi faaliyetlerde de bulunmaktadır (https://www.first.org/).

iv. Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC): ISO, küresel seviyede 167 devletin standart kuruluşunun üye olduğu, uluslararası bağımsız bir kuruluştur. Kişiler ya da şirketler ISO üyesi olamazlar ancak kendi devletlerinin standart organizasyonu içinde yer alarak standartların geliştirilmesinde aktif rol alabilmektedirler (https://www.iso.org/members.html). ISO, küresel zorlukları ele almak için yenilikçi uluslararası standartlar geliştiren uzmanların çalıştığı bağımsız ve hükümet dışı bir kuruluştur. Easterling, uluslararası standartların geliştirilmesi hususunda önemli faaliyetleri bulunan Uluslararası Standardizasyon Organizasyonunu (ISO), bu küresel standart oluşturma etkinliğinin devlet dışı parlamentosu olarak tanımlamıştır. Hem özel şirketleri hem de ulusal temsilcileri bünyesinde toplayan hükümet dışı özel bir kurum olan ISO, bilişim teknolojileri alanında küresel teknik standartları belirlemekte ve denetlemektedir (Easterling, 2014, s:20).

Veri iletişimi, ağ oluşturma ve siber güvenlik alanlarında standart oluşturma faaliyetleri bulunan ISO, elektrik ve elektronik mühendisliği standartları alanında faaliyetlerde bulunan **Uluslararası Elektroteknik Komisyonu (IEC)** ile bilişim teknolojileri

alanında birlikte bilgi güvenliği alanında iş birliği içinde çalışmakta olup ISO/IEC 27000 BGYS Standartlar ailesini geliştirmeye devam etmektedirler (Stallings,2019:46).

v. Uluslararası Otomasyon Topluluğu-The International Society of Automation (ISA): Endüstriyel otomasyonla uğraşan mühendisler, teknisyenler ve yönetimden oluşan kâr amacı gütmeyen bir profesyonel birliktir. Otomasyon yoluyla daha iyi bir dünya inşa etmeyi hedefleyen ISA kendisini, küresel seviyede mesleğe yönelik temel standartlara dayalı teknik kaynakların güvenilir sağlayıcısı olarak tanımlamaktadır. ISA yaygın olarak kullanılan küresel standartlar geliştirmekte; profesyonelleri sertifikalandırmakta; eğitimler vermekte; kitaplar ve teknik makaleler yayınlamakta olan çok paydaşlı, ağ yapılı bir kuruluştur. ISA, kritik altyapı tesisleri ve süreçlerinde siber güvenlik hazırlığını ve farkındalığını geliştirmek için ISA Küresel Siber Güvenlik Sözleşmesi-Global Cybersecurity Alliance'ı (isa.org/ISAGCA) oluşturmuştur. İttifak, artan tehditleri proaktif olarak ele almak için son kullanıcı şirketleri, otomasyon ve kontrol sistemleri sağlayıcıları, BT altyapı sağlayıcıları, hizmet sağlayıcıları, sistem entegratörleri ve diğer siber güvenlik paydaş organizasyonlarını bir araya getirmektedir (https://www.isa.org/about-isa).

vi. İnternet Güvenlik Merkezi (CIS Center for Internet Security, Inc.): CIS, bilişim teknolojileri sistemlerini ve verilerini güvence altına almak için dünya çapında kullanılmakta olan CIS Controls®' dan sorumlu, topluluk odaklı, görevi siber güvenlikteki en iyi uygulamaları belirlemek, geliştirmek, doğrulamak, teşvik etmek ve sürdürmek, siber olayları önlemek ve bunlara hızla yanıt vermek için birinci sınıf siber güvenlik çözümleri sunmak; ve siber uzayda bir güven ortamı sağlamak için topluluklar kurmak ve yönetmek olan kâr amacı gütmeyen çok paydaşlı bir kuruluştur (CIS-1:3). Sürekli değişen birbirine ağlarla bağlı dünyayı güvence altına almak için küresel topluluğa liderlik etmek amacı ile hareket eden CIS, misyonunu "insanların, işletmelerin ve devletlerin kendilerini yaygın siber tehditlere karşı korumalarına yardımcı olan en iyi uygulama çözümlerini zamanında geliştirerek, doğrulayarak ve teşvik ederek bağlantılı dünyayı daha güvenli bir yer haline getirmektir." şeklinde açıklamaktadır (https://www.cisecurity.org/about-us).

vii. IEEE: İnsanlığın yararına gelişen teknolojiye adanmış, 160 ülkeden 409.000'in üstünde üyesi olan dünyanın en büyük teknik profesyonel organizasyonudur.

IEEE ve üyeleri, çokça okunan yayınları, konferansları, teknoloji standartları ve mesleki ve eğitim faaliyetleri aracılığıyla küresel bir topluluğa hizmet etmektedir (https://www.ieee.org/about/at-a-glance.html).

4.2.4.4 Sivil Toplum Kuruluşları (STK)

Sinclair'in ulus ötecilik dediği, küresel yönetişimi etkileyen ya da değiştiren faktörlere odaklanan sivil toplum kuruluşları da küresel yönetişimin önemli aktörleri arasındadır. STK'ları, aşmak zorunda oldukları sorunları bulunan ve küresel yönetişimi şekillendirmede bireysel anlamda yeterliliği olmayanların bir araya gelerek kendi gruplarının yönetişimde temsilini sağlamak üzere oluşturulmuş örgütlerdir (Sinclair,2016:51-52). STK'ları sadece yerel birliktelikler değildir; ulusal devlet dışı örgütler ve çok uluslu devlet dışı örgütlerin de çeşitli ağlar yolu ile bağlantı halinde hedeflerine yönelik faaliyetlerini sürdürebildikleri yapılardır. Devletler altında örgütlenip ulus ötesi ağlar üzerinden uluslararası kuruluşlarla etkileşime geçerek yerel kaygı ve taleplerini devletler ve uluslararası kurumlar tarafından uygulanacak normlar haline getirme hedefleri bulunmaktadır (Sinclair,2016:57). Belirli alanlarda uzmanlık sahibi olan bu tarz kuruluşlar, uluslararası saygınlığa da sahiptir. Uluslararası alanda en iyi uygulamalar, bu örgütler tarafından taşınmakta ve devletleri belirli eylemleri yapmak için zorlayıcı rolleri bulunmaktadır. Scholte, sivil toplum ve küresel sivil toplum olarak adlandırdığı bu grubun çıkarlarını ve görüşlerini devlet sınırlarının dışındaki ortaklıklar aracılığı ile açıklayan toplulukları kapsadığını belirtmektedir (Scholte,2011'den aktaran Sinclair,2016:55).

i. Uluslararası Kızılhaç Komitesi (ICRC): Bu tarz sivil toplum örgütlerine örnek olarak verilebilir. Uluslararası Kızılhaç Komitesi siber uzaydaki devletlerin faaliyetlerini izlemeye ve endişelerini dile getirmeye başlamıştır. ICRC, 2017 yılında BM Genel Kurulu Birinci Komitesi oturumunda yaptığı açıklamada "elektrik şebekeleri, nükleer santral gibi kritik altyapıların işleyişini de etkileyen büyük siber saldırılardaki artışı gündeme getirmiş ve bu tür saldırıların sivil altyapının siber saldırılar karşısındaki savunmasızlığının ve oluşabilecek önemli insani sonuçların hatırlatıcısı olduğunu vurgulamışlardır (ICRC,2017:3). ICRC, siber uzayın askerleştirilmesine ve siber savaşa karşı çıkmaktadır. ICRC, 2016-2017 GGE başarısızlığından duyduğu üzüntüyü dile getirmiş ve tüm devletleri Uluslararası İnsan Hakları Mahkemesinin siber uzayın sivil kullanımına sağladığı koruma

hususunda ortak bir zemin bulmak amacıyla siber savaşın gündeme getirdiği kritik sorunlar hakkında uygun forumlarda tartışmaların devam ettirilmesini önermiştir (ICRC,2017:3).

4.3.5. Kritik Altyapıların Siber Güvenliğine Yönelik Standartlar ve Kılavuzlar

Devletler siber uzayın yoğun olarak kullanılmaya başlandığı 2000'li yıllara kadar, uluslararası hukuk alanında önemli ilerlemeler kaydetmiş ve sağlam bir uluslararası hukuk yapısı ve normlar (davranış standartları) geliştirmişlerdir (Puyvelde ve Brantly 2019:155). Ancak bilişim teknolojilerindeki çok hızlı gelişmeler nedeni ile özellikle siber güvenliğe yönelik hukuk kurallarının geliştirilmesi ve uygulamaya konulması, ihtiyacı karşılamaktan çok uzak kalmaktadır. Teknolojik değişim beraberinde toplumsal yapı değişikliklerini de getirmiş, özellikle sınır aşan sorunlar arasında yer alan siber güvenlik sorunlarının devletlerin yanı sıra özel sektör kuruluşlarından ve diğer aktörlerden de kaynaklanabildiği ve çözüm bulma aşamasında da sadece devletlerin çabaları yeterli olmadığı için özel sektör kuruluşlarının, sivil toplum kuruluşlarının, bireylerin vb.nin de katıldığı çok paydaşlılık kavramı kullanılmaya başlanmıştır.

Devletlerin kendi fiziki sınırları içinde ve küresel seviyede büyük ölçekli ağlarla birbirine bağlı siber uzayın yönetimi için devlet dışı güç olarak adlandırılan, devlet aygıtının dışında ona ilaveten ve bazen de onunla ortaklık içindeki, çoğu zaman açığa vurulmayan etkinliklerin yerine getirilmesine ihtiyaç vardır. Ulus devletler içinde uyulması gereken yasalar varken uluslararası örgütler ve çokuluslu şirketler standartlara uygun hareket ederler. ITU, ISA-IEC, NATO, Dünya Bankası, IMF ve Dünya Ticaret Örgütü gibi çok sayıda uluslararası örgütün etkisini artıran standartlar, küresel ilişkilerin esnek hukukunu oluşturmaktadır (Easterling, 2014:20).

Siber güvenlik standartları, üreticilerin ve kullanıcıların 1990'lı yıllardan itibaren, gerekli yetenekleri, politikaları ve uygulamaları gerçekleştirmek üzere yerel ve uluslararası forumlarda bir araya gelmeleri ile geliştirilmeye başlanmıştır. Sistemlerin tasarım aşamasından itibaren güvenlik ilkelerinin dikkate alınmasında ve bu sistemleri barındıran kuruluşların siber güvenliğinin sağlanmasında uygulama tekniklerini açıklayan standartlar ve kılavuzlar önem taşımaktadır Bir standart, belirli yöntemlerin tutarlı bir şekilde nasıl uygulanması gerektiğini ayrıntılarıyla anlatır. Örneğin, uygulanması gereken bilgi güvenliği

kontrol türleri için bir standart, organizasyonun tüm unsurlarının teknolojileri tek tip bir şekilde içermesini sağlayacaktır (Krutz, 2017:37-38).

Uluslararası bir standart, bir sorunu çözmek için normalde bir şeyi yapmanın kabul edilebilir bir yolunu tanımlayan bazı pratik bilgileri ve en iyi uygulamaları bir araya getiren bir belgedir. Siber güvenlik alanındaki standartlar, güvenliğin uluslararası bir sorun olduğunu göz önünde bulundurarak ortak güvenlik çözümleri sunulması; konunun uzmanları tarafından belirlenmiş en iyi güvenlik uygulamalarının tüm dünyadaki tüm kuruluşlar ile paylaşılması gibi önemli faydalar sağlamaktadır (Radulescu,2020:28-29). Siber güvenlik profesyonelleri, temel siber güvenlik risklerini hafifletmek, en iyi uygulamaları oluşturmak ve geliştirmek üzere uzun yıllar sonucu edindikleri deneyimleri standartlar olarak düzenlemektedirler. Bu standartlar, saldırganların başarı olasılığını azaltabilecek, bireylerin ve kurumların, firmaların kendilerini korumak için minimum adımlar atmalarına yardımcı olabilecek dokumanlardır (Herr,2019:137). Standart kuruluşları kapsamında, kamu kurumları, üretim sanayi, sendikalar, üniversiteler, tüketici dernekleri ve temsilcilerinin oluşturduğu komiteler kurulmakta ve pek çok ürün için standartlar hazırlanmaktadır (Renner ve Prugh,2014:17-18).

Siber güvenlik standartları, uluslararası kuruluşlar, bölgesel kuruluşlar ve çok paydaşlı kuruluşların yanı sıra bilişim teknolojilerinin geliştirilmesi alanında önde olan devletler ve bu devletlerin sınırları içinde faaliyet göstermekte olan çok uluslu şirketler tarafından da geliştirilerek küresel arenada söz sahibi olmaktadırlar. Küresel seviyede bilişim teknolojilerinin geliştirilmesi, üretilmesi ve pazarlanmasında önde gelen devletlerden olan ABD'nde de özellikle özel sektör sahipliğinde işletilmekte olan ve işlevsiz hale gelmeleri durumunda ülke çapında olumsuz etki oluşturabilecek endüstriyel tesislere ve faaliyetlere odaklanılmış ve her geçen gün artan önemlerine ve kritikliklerine binaen bu konuda 1990'lı yıllardan itibaren standartlar hazırlanmaya başlanmıştır (Herr, 2019:144). Ancak bu standartların uygulanması kamu politikası içinde kritik zorluklar olarak devam etmektedir (Herr,2019:137).

Genel anlamda standartlar, konu ile ilgili rehberlik görevini yerine getirmek, yeni programlar oluşturmak ve güvenlik kavramlarını tanımlamak için mükemmel, merkezileştirilmiş bilgi sağlamaktadır. Ayrıca, temel bir OT programı için değiştirilmeden

kullanılabilecek anahtar teslimi bir kaynak sunmaktadırlar. Standartlar, düzenli olarak güncellenmekte, değiştirilmekte ve genişletilmektedir. Konu ile ilgili herkes çeşitli alt komitelerde görev yapmak üzere standart hazırlama grubuna katılmaya davet edilmektedir (Brash,2021). Kurumlar, siber güvenliği sağlama çalışmalarında, mevcut ve gelecekteki ihtiyaçlarına göre standartlardan tamamen veya kısmen yararlanabilmektedirler. Siber güvenlik standartları, üreticiler, ürün sahipleri, satıcılar, BT uzmanları, mühendisler, risk yönetimi analistleri ve güvenlik uzmanları gibi bu alanda çalışanlar için eğitim materyali olarak da kullanılabilecek nitelikleri vardır. Kılavuzlar güvenli bilgi sistemleri oluşturmak için kullanılacak yöntemleri ayrıntılı olarak açıklayan dokümanlar olup tavsiye niteliğindedir ve uyum zorunluluğu yoktur.

ACM, IEEE gibi uluslararası kuruluşlar tarafından bilişim profesyonellerinin ve siber güvenlik profesyonellerinin faaliyetlerini yerine getirmesinde etik davranış sergilemelerine yardımcı olmak üzere kuralları içeren kitapçıklar da yayımlanmış olup küresel seviyede katılımcıların katkısı ile güncel tutulmaktadır.

EKS'nin siber güvenliğinin sağlanmasına yönelik standartlardan ve kılavuzlardan en çok kullanılan birkaç tanesi aşağıda yer almaktadır:

4.3.5.1 NERC Kritik Altyapıların Korunmasına Yönelik Siber Güvenlik Standardı

2006 yılında NERC (North America Electric Reliability Concuil) ABD'de elektrik alt yapılarının güvenli hale getirilmesi için elektrik sistemi üretim ve dağıtımdaki taraflara siber güvenlik standartları gerçekleme planını yayınlamıştır. Bu plan ile yıllar içerisinde alınması gereken önlemleri belirtilmiş; 2010 yılı sonuna kadar bütün elektrik üretim, dağıtımı yapan kurumların, olası siber saldırılara karşı, BT altyapı güvenliklerini denetlenebilir bir seviyeye getirmeleri istenmiştir. (Kara ve Çelikkol,2011). Dokümanda elektrik üreten ya da ileten kuruluşların güvenlik konusunda almaları gereken önlemler, Kritik Siber Varlıkların Tanımlanması, Güvenlik Yönetim Kontrolleri, Personel ve Eğitim başlıkları altında anlatılmıştır.

Bu plan, 2011 yılında 'Enerji Dağıtım Sistemlerinin Siber Güvenliğini Gerçekleştirmek için Yol Haritası' adı altında güncellenerek yeniden yayınlanmıştır. Yeni yol haritasında, değişen ortamı tanıtmak, başarıyı inşa etmek ve açıkları belirlemek, gelişen

tehdit yetenekleri hakkında bilgi vermek, güvenlik kültürünü pekiştirmek amaçlanmış; 2020 itibarı ile, kritik fonksiyonları devam ederken gerçekleşen bir siber olayda sistemin ayakta kalmasını sağlayacak esnek enerji dağıtım sistemlerinin tasarlanıyor, kuruluyor, işletiliyor ve bakımının yapılıyor olması vizyonu ortaya konulmuştur (ESCSWG, 2011:2).

4.3.5.2. ISA-62443

Endüstriyel kontrol sistemlerine ve operasyonel teknolojiye (OT) özgü güvenlik sorunlarını ele almak amacı ile oluşturulmuş standart grubudur. EKS'nin siber güvenliğinden sorumlu tüm paydaşlar tarafından kullanılabilecek ortak terimler, kavramlar ve modelleri tanımlamaya; varlık sahiplerinin güvenlik düzeyini belirlemelerine yardımcı olmaya; ürün geliştiriciler için ortak bir gereksinimler dizisi ve bir siber güvenlik yaşam döngüsü metodolojisi oluşturmaya; kontrol sistemlerini korumak için kritik olan risk değerlendirme süreçlerini tanımlamaya yönelik standartlar dizisidir. EKS'lerinin siber güvenliğini sağlamak üzere risk yönetimi yaklaşımının uygulanmasına yönelik Siber Güvenlik Yönetim Sisteminin (SGYS) tanımlandığı standarttır. EKS uzmanlarından edinilen bilgiler ışığında hazırlanan ve derinlemesine savunma modelinin önerildiği bu standart ailesi, bir siber güvenlik yönetim sisteminin (SGYS) nasıl oluşturulacağını açıklamakta ve EKS/OT ortamlarında risk değerlendirmeleri gerçekleştirmekte kullanılacak talimatları kapsamaktadır. IEC 62443, kuruluşların EKS güvenlik olgunluğunu ve duruşunu tanımlamasına yardımcı olur ve seçim kriterleri güvenlik ürünleri, programları ve hizmet sağlayıcıları sunar. IEC 62443'ün temel kılavuzu, belirli teknolojik durumları ve çözümleri kapsayan teknik raporlarla rutin olarak desteklenmektedir (https://www.isa.org/about-isa).

OT'in siber risk değerlendirmelerinin yapılması, OT siber güvenlik yönetim ekiplerinin oluşturulması, Yama uygulaması ve diğer koruyucu kontroller/yetenekleri ile çözümlerde ve ürünlerde izlenmesi ve iyileştirilmesi olmak üzere üç ana başlıktan oluşmaktadır.

OT'lerin kullanıldığı EKS'nin siber güvenliğinin sağlanmasında siber-fiziksel arızalar durumunda personel, çevre ve toplum için potansiyel tehlikeler, eski teknoloji ürünü ve halen kullanılmakta olan EKS/OT sistemlerini korumak için telafi edici kontrol ihtiyacının her geçen gün daha da artması, sistemde önemli değişiklikler yapılmaksızın

yaygın BT güvenlik tekniklerini uygulamanın göreceli zorluğu; endüstriyel ortamlarda sistemlerin güvenilirliğini ve bütünlüğünü sağlamaya yönelik benzersiz yaklaşımların kullanılmakta olması gibi zorluklar söz konusudur.

Çerçeveleme gereksinimleri, varlık ve sistem güvenliği yaşam döngüsünün göz önünde bulundurulması; Ağ bölgelerini ve kanalları izole etme, bölümlere ayırma ve güvenliğini sağlama; Süreçler ve yönetişim türetme; kullanıcılar veya kaynaklar için uygun rollerin ve sorumlulukların oluşturulması; siber risk azaltma faktörlerinin (CRRF'ler) değerlendirilmesi gibi konularda kapsamlı bilgilere yer verilmektedir. Bu standartların en çok kullanılanları aşağıdadır:

- **ISA-62443-1-1-2007** Endüstriyel Otomasyon ve Kontrol Sistemleri için Güvenlik Bölüm 1-1: Terminoloji, Kavramlar ve Modeller

Endüstriyel otomasyon ve kontrol sistemleri için güvenlik konusunu ele alan ISA standart dizisinin ilkidir. Bu sistemlerin siber güvenliği ile ilgili temel kavramların ve modellerin açıklandığı standarttır (ISA-62443-1-1-2007, 2007)

- **ISA-62443-2-1-2009** Endüstriyel Otomasyon ve Kontrol Sistemleri için Güvenlik Bölüm 2-1: Endüstriyel Otomasyon ve Kontrol Sistemleri Güvenlik Programının Oluşturulması

Bu standart, endüstriyel otomasyon ve kontrol sistemleri ortamında kullanılmak üzere bir siber güvenlik yönetim sisteminde yer alan unsurları açıklar ve her bir unsur için açıklanan gereksinimlerin nasıl karşılanacağı konusunda rehberlik sağlar (**ISA-62443-2-1-2009)**.

- **ISA-TR62443-2-3-2015, (2015), Endüstriyel otomasyon ve kontrol sistemleri için güvenlik, Bölüm 2-3: EOKS ortamında yama yönetimi**

Bu standart, güvenlik yamalarının EOKS ürün tedarikçileri tarafından geliştirilmesi ve varlık sahipleri tarafından konuşlandırılması ve kurulmasıyla ilgili bazı faaliyetlerin bir tanımını önerir (ISA-TR62443-2-3-2015).

- **ANSI/ISA-62443-3-2-2020, Endüstriyel otomasyon ve kontrol sistemleri için güvenlik, Bölüm 3-2: Sistem tasarımı için güvenlik riski değerlendirmesi**

Bir endüstriyel otomasyon ve kontrol sistemi (IACS) için değerlendirilmekte olan bir sistemin risk değerlendirmesi, hedef güvenlik seviyesinin oluşturulması ve güvenlik gereksinimlerinin belgelenmesi amacı ile kullanılan bir standarttır (ANSI/ISA-62443-3-2-2020).

- **ANSI/ISA-62443-4-1-2018 Endüstriyel otomasyon ve kontrol sistemleri için güvenlik, Bölüm 4-1: Güvenli ürün geliştirme yaşam döngüsü gereksinimleri**

Endüstriyel otomasyon ve kontrol sistemlerinde kullanılan ürünlerin geliştiricisi ve bakımcısı için güvenli bir şekilde geliştirilmesi ve sürdürülmesi amacıyla güvenli bir geliştirme yaşam döngüsü tanımlar. Bu yaşam döngüsü, güvenlik gereksinimleri tanımı, güvenli tasarım, güvenli uygulama (kodlama yönergeleri dahil), doğrulama, hata yönetimi, yama yönetimi ve ürün kullanım ömrünün sonunu içerir. Bu gereksinimler, yeni veya mevcut ürünler için donanım, yazılım veya ürün yazılımı geliştirmek, sürdürmek ve kullanımdan kaldırmak için yeni veya mevcut süreçlere uygulanabilir (ANSI/ISA-62443-4-1-2018).

4.3.5.3 NIST Siber Güvenlik Dokümanları

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), hükümetlerin, endüstrilerin ve akademinin standartlaştırılmış en iyi uygulamaları takip etmesine yardımcı olmak için güvenliğe özel 800 serisini yayınlamaktadır. NIST SP 800-53r4,2013 dışında, her 800 serisi SP, belirli bir konu alanında rehberlik sağlamaktadır. Yayınlar, değişen teknolojik gelişmeler paralelinde sürekli olarak güncellenmektedir. NIST-800 serisi, küresel olarak en yaygın kullanılan siber güvenlik önlemleri serisidir. Dünya genelinde birçok devlet ve kuruluş bu yayınları rehber olarak kullanmaktadır (Stallings,2019). Bu dokümanlar, kuruluşların siber güvenliğini sağlamak üzere güvenlik açıklarını azaltmak için en iyi uygulamaları ve belirli politikaların nasıl ve neden uygulamaları gerektiğini anlatmaktadır. NIST-800 serisinde çok sayıda yayın yer almaktadır. NIST-500 serisinde kritik altyapılarla ilgili dokümanlar bulunmaktadır. Bu dokümanlarda yer alan politika ve tavsiyeler, bilişim sistemleri ve ağlarının kullanıcılarının ve operatörlerinin karşılaştığı riskleri azaltmayı hedeflemektedir. Kritik altyapıların siber güvenliğinde sıklıkla kullanılmakta olan bu dokümanlardan bazıları aşağıdadır:

i. NIST 7628 Akıllı Şebekelerin Siber Güvenliği için Kılavuzlar

NIST 7628, Akıllı Şebeke uygulamaları için özelleştirilmiş siber güvenlik stratejilerinin uygulanmasına yönelik metodik bir yaklaşım sağlayan üç ciltlik bir dokümandır. Akıllı Şebeke Birlikte Çalışabilirlik Panelinin Siber Güvenlik Çalışma Grubu tarafından geliştirilmiştir ve elektrikli araç şarj istasyonları, kamu hizmetleri, üreticiler ve enerji yönetimi hizmetleri sağlayıcıları gibi akıllı şebeke ile ilgili çeşitli alanlara uygulanmak üzere tasarlanmıştır. Yaklaşımı ayrıca genel olarak proses tesislerine, üretim operasyonlarına ve otomasyon sistemlerine doğrudan uygulanabilir. Bilgi sistemi güvenliği, bilgi teknolojisi, kontrol sistemleri, telekomünikasyon ve üretimden teknikleri bir araya getirmektedir (Krutz,2017:272).

ii. NIST SP 800-39 Bütünleşik Kurumsal Risk Yönetimi Standardı

NIST SP 800-39, Bilgi Güvenliği Risk Yönetimi Standardı, Organizasyon, Misyon ve Bilgi Sistemi Görünümü, destekleyici olarak risk değerlendirmesi konusunda rehberlik sağlamak üzere revize edilen Bilgi Teknolojileri Sistemleri için NIST SP 800-30 Risk Yönetimi Kılavuzu'nun yerini almıştır. Bu standarda göre risk yönetimi, kuruluşların (riske dayalı kararlar için bağlamı oluşturmak anlamında risk çerçeveleme; risk değerlendirme; tespit edilen riske yanıt verme ve kuruluşların riskle ilgili faaliyetlerinde sürekli iyileştirme için etkin kurumsal iletişim ve bir geri bildirim döngüsü kullanarak riski sürekli olarak izleme aşamalarından oluşan kapsamlı bir süreçtir. Bu standart ile, risk yönetimine küresel bir bakış açısı getirilmekte ve risk yönetimi süreci bilgi sistemleri veya otomasyon ve kontrol sistemleri öğelerinin yanı sıra, organizasyonun misyonunu ve iş hedeflerini, ayrıca iş süreçlerini ve bilgi ve otomasyon sistemi bileşenlerinin sistem geliştirme yaşam döngüsünü içermesi gereken hiyerarşik bir yapı olarak görür.

Kurumsal operasyonlara (yani misyon, işlevler, imaj ve itibar), kurumsal varlıklara, bireylere ve diğer kuruluşlara yönelik bilgi güvenliği riskini yönetmek için kuruluş çapında uygulanacak bütünleşik bir program için rehberlik sağlamak amacı ile hazırlanan bu doküman geniş tabanlı risk yönetimi için yapılandırılmış olup esnek bir yaklaşım sağlamaktadır (NIST 800-39,2011).

iii. NIST SP 800-53r4,2013 Siber Güvenlik Çerçevesi

NIST tarafından, bir kuruluş genelinde siber güvenlik uygulamalarını aşamalı olarak iyileştirmek için bir süreç olgunluğu modeli olan Siber Güvenlik Çerçevesi (NIST SP 800-53r4,2013) yayınlanmıştır. Belirlenen güvenlik kategorisine ve bilgi sistemlerinin ilgili etki düzeyine göre seçilmesi gereken temel kontroller kavramı aracılığıyla güvenlik kontrollerinin seçiminde kuruluşlara rehberlik etmek üzere hazırlanan bu özel yayın, düşük etkili, orta etkili ve yüksek etkili bilgi sistemlerine karşılık gelen güvenlik kontrol temellerinin bir listesini sağlamaktadır.

NIST SP 800-53r4,2013'ün Ek F'si, bilgi sistemleri ve kuruluşlar için kapsamlı bir güvenlik kontrolleri kataloğu sağlamaktadır. EKS Ek Rehberi ayrıca, belirli bir güvenlik kontrolünün veya kontrol geliştirmesinin bazı EKS ortamlarında neden uygulanamayacağına ve uyarlama için aday olabileceğine (yani, kapsam belirleme kılavuzunun ve/veya telafi edici kontrollerin uygulanması) ilişkin bilgi sağlamaktadır (Krutz,2017:410).

iv. NIST SP 800-82 EKS Güvenliği için Rehber adlı dokümanı

ABD'nin Ulusal Standartlar ve Teknoloji Enstitüsü olan NIST tarafından "Kritik Altyapıların Siber Güvenliği için Rehber" adlı bu doküman hazırlanmıştır. Bu dokümanda kritik altyapıların tipik ihtiyaçları için alternatif süreç yaklaşımına yer verilmekte ve ISO 27000 standart ailesine de atıflar yapılmaktadır (Alexander ve Panguliri,2017:36).

NIST özel yayını olan EKS Güvenliği için Rehber 800-82 adlı bu doküman, kritik altyapıların en kritik bilgi varlığı olan EKS ile ilgili siber güvenlik olaylarına odaklanmıştır.

Bu doküman, SCADA sistemleri, Dağıtılmış Kontrol Sistemleri (DCS) ve Programlanabilir Mantık kontrolörleri (PLC) gibi diğer kontrol sistemi konfigürasyonları dahil olmak üzere Endüstriyel Kontrol Sistemlerinin (EKS) güvenli hale getirilmesi konusunda rehberlik sağlarken, bunların performans, güvenilirlik ve güvenlik gereksinimlerini de ele almaktadır. Belge, EKS'ye ve tipik sistem topolojilerine genel bir bakış sağlamakta, bu sistemlere yönelik tipik tehditleri ve güvenlik açıklarını tanımlayarak ve ilişkili riskleri azaltmak üzere güvenlik önlemlerini de kapsamaktadır.

Bu belge, benzersiz performans, güvenilirlik ve güvenlik gereksinimlerine değinirken fiziksel ortamla etkileşime giren (veya fiziksel ortamla etkileşime giren cihazları

yöneten), geniş bir programlanabilir sistem ve cihaz yelpazesini kapsayan ve bu cihazların, süreçlerin izlenmesi ve/veya kontrolü yoluyla doğrudan bir değişikliği tespit edebilen operasyonel teknoloji (OT) ürünlerinin güvenliğinin sağlanmasına yönelik bilgileri de kapsamaktadır.

v. NIST Tarafından Hazırlanan "Kritik Altyapıların Siber Güvenliği için Rehber" Adlı Doküman

Ulusal güvenliğinin kritik altyapıların güvenilir işleyişine bağlı olduğunu savunmakta olan Amerika Birleşik Devletleri'nde (ABD), kritik altyapıları işletmekte olan kurumsal yapıların karşı karşıya kaldığı siber güvenlik risklerini daha iyi ele alabilmek için Başkan tarafından 12 Şubat 2013'te ABD Ulusunun güvenliğini ve direncini artırma politikası olan "Kritik Altyapı Siber Güvenliğinin İyileştirilmesi" başlıklı 13636 sayılı Yürütme Kararı'nı yayınlamıştır. Yürütme kararı doğrultusunda, kamu ve özel sektör iş birliği ile kuruluşların siber güvenlik risklerini yönetmelerine yardımcı olmak üzere bazı endüstri standartlarını ve en iyi uygulamaları içeren bu rehber hazırlanmıştır. Bu rehber, kuruluşların büyüklüğü, risk derecesi veya siber güvenlik gelişmişliğine bakılmaksızın tüm kritik altyapıların güvenliğini ve direncini artırmak için risk yönetimi ilkelerini ve en iyi uygulamaları kullanmalarını hedeflemektedir. Rehber, günümüzde etkin olarak kullanımda olan ve dünya çapında kabul görmüş olan standartları, yönergeleri ve uygulamaları bir araya getirerek günümüz şartlarında siber güvenliğe yönelik çoklu yaklaşımların kullanılmasına imkân tanımaktadır.

2014 yılında ilk sürümü, 2018 yılında ise 1.1 sürümü hazırlanan bu doküman sürekli güncellenmekte olup kritik altyapı sektörleri arasında ortak olarak yürütülebilecek nitelikteki siber güvenlik faaliyetlerini kapsamaktadır (NIST,2014; NIST,2018). Doküman, risklerin önceliklendirilmesi ve önceliklendirilmiş riskler için risk yönetimi yaklaşımının geliştirilmesini kapsayan "Tanımlar"; politikalar ve kontrollerin uygulanması ile risklerin azaltılmasına yönelik "Koruma"; **s**iber güvenlik olaylarının araştırılmasına yönelik "Araştırma"; siber olay müdahale planı hazırlanması ve siber olay sonrası gözden geçirme, analiz etme ve süreçlerin iyileştirilmesi aşamalarına değinilmekte olan "Müdahale" ve siber olay sonrası gözden geçirme, analiz ve süreçlerin iyileştirilmesi aşamalarının anlatıldığı "Kurtarma" bölümü olmak üzere 5 temel bölümden oluşmaktadır:

4.3.5.4 Gelişmiş Ölçüm Altyapısı - Advanced Metering Infrastructure Security (AMI,2008) Güvenlik Gereksinimleri Dokümanı

Bu doküman, güvenilir bir sistemi sürdürmek için gerekli olan yüksek düzeyde bilgi güvenilirliği, kullanılabilirliği ve güvenliği sağlamak için uygulanması gereken bir dizi güvenlik gereksinimini destekleyici satıcı ve tüketici toplulukları ve diğer paydaşlarla birlikte kamu sektörüne de sağlamak amacı ile hazırlanmıştır. Dokümanda yer alan güvenlik gereksinimleri diğer ağ merkezli akıllı şebeke çözümlerini de kapsayacak şekilde genişletilebilir niteliktedir (Krutz,2017:194).

4.3.5.5 SCADA Ağlarının Siber Güvenliğini Sağlamak için 21 Adım

SCADA ağları, temel hizmetleri ve emtiaları (örneğin, elektrik, doğal gaz, benzin, su, atık arıtma, ulaşım) sağlamada temel işlevleri yerine getiren bilişim teknolojilerini ve uygulamaları içerdiği için kritik altyapı sektörünün parçasıdırlar ve siber uzayda var olan çeşitli tehditlere karşı korunmaya ihtiyaç duymaktadırlar. Bu sistemler, verilerin toplanmasına ve analizine; pompalar ve vanalar gibi ekipmanların uzak konumlardan kontrol edilmesine izin vererek, yaygın olarak kullanılmaktadırlar. Başlangıçta, güvenliğe çok az dikkat edilerek, işlevselliği en üst düzeye çıkarmak üzzere tasarlandıkları için SCADA sistemlerinin performansı, güvenilirliği, esnekliği ve emniyeti yeterli iken güvenlik özellikleri genellikle zayıftır. Bu nedenle, SCADA ağları, güvenliği endişelerine ve/veya kritik altyapılarda önemli kesintilere yol açabilecek hizmet kesintisine, süreç lerin yeniden yönlendirmesine veya operasyonel verilerin manipülasyonuna karşı potansiyel olarak savunmasız durumdadırlar. ABD Başkanlık Kritik Altyapıları Koruma Kurulu ve ABD Enerji Bakanlığı, tüm kuruluşlar tarafından kritik altyapıların korunması kapsamında SCADA ağlarının güvenliğin sağlanmasına yardımcı olmak üzere kullanılacak olan bu doküman hazırlamıştır (DOE-USA,2007).

4.3.5.6 ISO-IEC 27000 Serisi Bilgi Güvenliği Yönetim Sistemi Standart Serisi

Kritik altyapı sistemlerinde operasyonel teknolojiler ile birlikte bilişim teknolojileri de kullanılmakta olduğu için Bilgi Güvenliği Yönetim Sisteminin kurulması ve takibinde ISO-IEC 27000 serisi kullanılmaktadır.

Çeşitli konularda standartlar geliştirmek üzere görev yapmak olan uluslararası bir kuruluş olan Uluslararası Standartlar Örgütü (ISO) ve Uluslararası Elektroteknik

Komisyonunun (IEC) oluşturduğu Ortak Teknik Komite (JTC 1) tarafından ISO-IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standartlar serisi hazırlanmıştır. Bu grupta kurumsal yapının siber güvenirliğini göstermek üzere siber güvenlikten sorumlu kurumsal yöneticiler için sertifikasyon gereklilik listesinin yer aldığı ISO/IEC 27001; BGYS gerekliliklerini karşılamak için ihtiyaç duyulan kontroller ISO 27002'de; Bilgi güvenliği risk yönetimi sisteminin uygulama rehberi ISO 27005'de; Bilgi güvenliği yönetimi için uygulama kuralları ISO/IEC 27002:2013'de; Bilişim Sistemleri yönetişimi ISO 27014'de, olmak üzere farklı standartlar kullanılmaktadır (Stallings,2019:49). ISO 27001'in ekinde yer alan 114 bilgi güvenliği kontrolü de uygulanmaktadır. ISO 27001 BGYS'nin kurulması ve işletilmesi için gerekli adımları kapsamaktadır. Bu adımlar planlama, uygulama, kontrol etme ve önlem alma aşamalarından oluşmaktadır. Bu standart, bilgi sistemi yönetimi sırasında risk değerlendirme gerekliliklerini karşılamayı amaçlayan ve yaygın olarak kullanılmakta olan bilgi güvenliği kontrol hedeflerini ve kontrollerin önerilen en iyi uygulamalarını kapsamaktadır.

4.3.5.7 CIS Kritik Güvenlik Kontrolleri (Critical Security Controls®)

CIS Controls®), sistemlere ve ağlara yönelik en yaygın saldırıları azaltan, toplu olarak derinlemesine savunma en iyi uygulamaları oluşturan öncelikli bir eylemler dizisidir. CIS Kontrolleri, küresel olarak kabul edilen en iyi güvenlik uygulamalarını oluşturmak için siber savunucular olarak ilk elden deneyimlerini uygulayan ve çok çeşitli kritik altyapı sektörlerinde görev yapmakta olan bir BT uzmanları topluluğu tarafından geliştirilmiştir (https://www.cisecurity.org).

4.3.5.8. ACM Etik ve Mesleki Davranış Kuralları

1970'li yıllardan itibaren kullanılmakta olan ve her geçen gün gelişerek hayatın her alanına nüfuz etmekte olan bilişim teknolojilerinin ve dolayısı ile bu teknolojileri tasarlayan, geliştiren, kullanan bilişim profesyonellerinin kamusal alan ve özel yaşam üzerinde çok önemli rolleri vardır. Profesyonel bir kuruluş olan ACM, bilişim teknolojilerinin dünyayı daha iyi hale getirmek üzere kullanılmasına rehberlik etmeyi hedeflemektedir. ACM Etik ve Mesleki Davranış Kuralları, bilişim profesyonelleri arasındaki bir sözleşme olmanın yanı sıra, mesleğin hizmet ettiği daha geniş toplum kesimlerine karşı sahip olunması gereken

sorumlulukların da kamuya ilan edildiği bir dokümandır. Bilişim profesyonellerinin yaptığı iş, teknolojinin tüm insanların hayatlarını iyileştirmek için kullanılmasını sağlamak ve kötüye kullanılmasını önlemek olmalıdır. Geniş toplumsal kesimlerin, bilişim profesyonellerinin etik davranışa bağlı olduğundan kuşku duymaması gerekmektedir.

1990'lı yıllarda bilişim sistemleri sadece teknik sistemler olarak görülmekte idi. Oysa günümüz dünyasında çok farklı alanlarda kullanılmakta olan bu sistemlerin toplumsal yapılar üzerindeki etkisi gittikçe artmaya başlamıştır. Bilişim teknolojileri yalnızca karmaşık hesaplamaları yapmak için değil, daha önceki bölümlerde de ele alındığı gibi kritik altyapıların görevlerinin yerine getirilmesinde de kullanılmaya başlanmıştır.

Bu gelişmelere paralel olarak bilişim teknolojilerini tasarlayan, geliştiren, kullanan bilişim profesyonellerinin görevlerini yerine getirirken üstlendikleri sorumluluklarda da önemli değişiklikler ve dönüşümler olmaya başlamıştır. Çok hızlı değişen ve gittikçe karmaşıklaşan bilişim teknolojileri, yüksek seviyede teknik beceri gerektirmesinin yanı sıra hayatın tüm alanlarını etkileyecek önemli kararların da çok kısa bir süre içerisinde alınması durumlarını gündeme getirebilmektedir. Bireysel seviyede etik kararlar genellikle çocukluk ve gençlik dönemlerinde öğrenilen etik karar becerilerinin otomatik olarak uygulanmaktadır. Ancak teknolojik gelişmeler, geçmişte hiç karşılaşılmayan ve üzerinde hiç düşünülmemiş sorunları gündeme taşımaktadır.

ACM tarafından, bilişim profesyonellerinin, görevlerini yerine getirirken etik analiz becerilerini de geliştirmek amacı ile Kuralları ve Kuralların uygulanmasına ilişkin örnekleri içeren ACM Etik ve Mesleki Davranış Kuralları kitapçığı hazırlanmıştır. Bu kitapçık, yalnızca başlangıç noktası olarak alınmakta olup küresel seviyede tüm katılımcılara açık çevrim içi bir blog üzerinden gerçek yaşamda ortaya çıkmakta olan senaryolar veya ikilemleri paylaşmaktadır (ACM,2018:1).

4.3.6. Küresel Yönetişimin Sorunları ve Kozmopolitanizm

Kritik altyapıların siber güvenliğinin sağlanmasında küresel siber yönetişimin önemi büyüktür; ancak egemenlik ve birbirine bağımlılık ilişkilerinin karmaşık hale geldiği günümüz dünyasında küresel yönetişimin sorunlu olduğu durumlar da mevcuttur. Bu olumsuz yönler arasında, uluslararası kuruluşların ve çok paydaşlı yönetsel ağların yaptırım uygulama yetkilerinin ve otoritelerinin bulunmaması, hızla değişen güncel yasalar ve

teamüller oluşturulsa da bunların devlet, küresel ve bölgesel otoriteler arasındaki yerinin belirsiz oluşu, meşruiyet kazanmamış olmaları yer almaktadır (Held-1,2014:205-207). Sinclair ise bu olumsuzluklara, küresel yönetişim birimlerinin karmaşık yapılarından dolayı içsel çatışma ve başarısızlık olasılığının yüksek olması; yönetişimi kimin yürüteceği ve kim için yapılacağının tartışma konusu olması; bireylerin ya da kurumların bilgeliğine ya da deneyimine dayanan otoritenin zorlayıcılığı ya da yaptırım gücünün bulunmaması hususlarını eklemektedir (Sinclair,2016:24). Küresel yönetişim faaliyetlerinin yasal ve hukuki dayanaklarının tam olarak belirlenememiş ve uygulamaya konulamamış olmasına karşılık, çok uzun bir süredir demokrasi ve karşılıklılık ilkesine uygun faaliyetler yürütmekte olan devletler de tamamen aşınmamış olup önemli faaliyetleri yerine getirerek varlığını sürdürmektedir (Keohane, 2014:191).

Küresel yönetişimin olumsuz yönleri olarak sayılan bu özelliklere karşılık iyimser bir yaklaşım olan Kozmopolitanizm kavramı kullanılmaya başlanmıştır. Kozmopolitanizm, bir hükümet, bir devlet ya da sivil örgütün temsilcisi olduğuna bakılmaksızın tüm insanların uyması gereken standartları ya da sınırları belirleyen temel değerleri anlatmak üzere kullanılmaktadır. İnsanların içinde doğdukları ya da geliştikleri topluluğa bakılmaksızın eşit ölçüde önemsenip göz önünde bulundurulmasına dayanan davranıştır (Held,2014-2:609). Norris daha yalın bir ifade ile "Kendilerini sadece içinde yaşadıkları devletle değil dünyanın tümüyle özdeşleştiren ve küresel yönetişim kurumlarına daha fazla inananlar, kozmopolitlerdir." demiş ve bu grup mensuplarının çevrenin küresel seviyede korunmasının ön planda tutulmasını savunmakta olduklarını belirtmiştir (Norris,2014:342). Değişimi ve sınır aşan yeni küresel tehditlere uyum sağlamak üzere küresel yönetişimin yeniden şekillendirilmesi gerektiğini ve yeni otorite faillerinin varlığını kabul eden bu yaklaşım iyimser bir kavrayıştır. Kozmopolitanizme göre, küreselleşmeyi temsil eden uluslararası kuruluşlar; devletlerin bağımsız hareket etmesinin önüne geçmiş iken küresel yönetişim tamamen farklı bir kavramdır (Sinclair,2016:83). Kozmopolitan yaklaşımda, sorunları üreten temel süreçleri değiştirmek yerine sorunlarla muhatap olunan temel düzeneklerin değiştirilmesi düşünülür. Hakkaniyet ve adalet gibi normatif sorunları önemsedikleri için Küresel yönetişimi, dünyayı daha adil, daha iyi daha yaşanır bir yer kılmak üzere uygulayacakları dayanışmacı bir yaklaşım olarak görmektedirler (Sinclair,2016:78-79).

Siber güvenlik yönetişimi bağlamında çok paydaşlı kuruluşlar ve yönetsel ağların faaliyetleri incelendiğinde, özellikle kritik altyapıların siber güvenliğine yönelik faaliyetlerin hangi devlet sınırları içinde olduğuna bakılmaksızın tüm insanların ve hatta tüm canlı ve cansız varlıkların, sürdürülebilirlik kavramına uygun olarak mevcudiyetlerinin devam ettirilebilmesi için gerçekleştirildiği anlaşılmaktadır. Siber güvenlik bağlamında çevrenin küresel seviyede korunması temel hedef olduğundan dolayı, sınır aşan siber güvenlik sorunlarının çözümünde, BT alanında gelişmiş devletlerin, standartları hazırlayan çok paydaşlı uluslararası kuruluşların, yönetsel ağların ve çok uluslu şirketlerin getirdikleri çözüm önerilerine uyulmasının küresel seviyede fayda sağlayacağı düşünülmektedir. Tüm canlı ve cansız varlıklar için hakkaniyet ve adaletin önemli olduğundan hareketle uluslararası kamu yararına yönelik olarak yürütülmekte olan siber güvenlik yönetişimi faaliyetlerinin de kozmopolitanizm kavramına uygun olarak gerçekleştirilmesi gerektiği sonucuna varılmıştır.

4.4 KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK STRATEJİK FAALİYETLERİN DEĞERLENDİRİLMESİ

Kritik altyapı sistemlerinin siber güvenliğinin nasıl sağlanacağına yönelik gerçekleştirilmekte olan faaliyetler araştırılmıştır. Bu sistemlerin küresel seviyede her alanda yaygın kullanımı nedeni ile siber güvenliğin artık sadece teknolojik boyutu değil, bireysel, kurumsal, ulusal ve uluslararası boyutlarının da gündeme getirilmekte olduğu görülmüştür. Bu bölümde, siber güvenlik faaliyetleri ulusal ve küresel seviyede incelenmiştir. Bireysel seviyede belirli görevlerin nihai olarak yürütüldüğü ve kurumsal seviyede farklı görevlerin koordine edildiği operasyonel faaliyetlerin; devletler seviyesinde ise hedeflere uygun kurumsal yapıların görevlendirilmesi ve uzun vadeli siyasi hedeflerin tanımlandığı strateji ve politika faaliyetlerinin gerçekleştirilmekte olduğu anlaşılmıştır. Bireysel ve kurumsal seviyede siber güvenlik faaliyetlerinin gerçekleştirilmesinde; ulusal ve küresel seviyede hazırlanmış siber güvenlik politikalarına ve stratejilerine uygun olarak uluslararası standartlar ve en iyi uygulama örnekleri kullanılmaktadır.

Kritik altyapıların siber güvenliğinin sağlanmasına yönelik stratejik faaliyetler, devletler tarafından ve küresel seviyede çok paydaşlı kuruluşlar tarafından yürütülmektedir. Stratejik faaliyetlerde, önleyici koruyucu güvenlik yaklaşımı ve risk yönetimi yaklaşımına

ek olarak caydırıcılık yaklaşımı ve kamu siber güvenlik yaklaşımı da kullanılmaktadır. Caydırıcılık yaklaşımının günümüz teknolojik olanakları ile sadece saldırganın tam olarak tespit edilebildiği durumda uygulanabileceği, bunun da daha çok devletler kapsamında ya saldırıyı gerçekleştirene yönelik ağır cezai müeyyideler uygulanarak ya da uluslararası seviyede saldırıyı gerçekleştiren devlete müeyyideler uygulanarak gerçekleştirilebileceği değerlendirilmektedir. Bu konuda da çok paydaşlı kuruluşların bilgi paylaşımı ve iş birliği sayesinde failin tespiti mümkün olabilecektir. Kamu siber güvenliği yaklaşımı, bir kritik altyapıda meydana gelebilecek siber güvenlik olayının fiziki çevre üzerinde önemli hasar oluşturarak ya da doğrudan canlıların hayatını yitirmesine neden olabileceği ya da sürdürülebilirlik için gerekli kaynakların tüketilmesine neden olabileceği için bireysel, kurumsal, ulusal ve küresel olmak üzere her seviyede göz önünde bulundurulması gereken bir yaklaşımdır.

Çalışma kapsamında Türkiye'de endüstriyel kontrol sistemlerinin kullanılmakta olduğu kritik altyapıların siber güvenliğine yönelik halen yürürlükte olan strateji ve politika dokümanları incelenmiştir. On Birinci Kalkınma Planında kritik altyapıların siber güvenliğine hem ulusal güvenlik açısından hem de çevresel güvenlik açısından yaklaşılmıştır. Konu ile ilgili kurumsal yapıların oluşturulduğu ve aralarında bir koordinasyon kurulmasına yönelik faaliyetler bulunduğu görülmüştür. Ancak aynı görevin farklı kurumlar tarafından üstlenildiği ve aralarında tam bir iş birliği ve koordinasyonun bulunmadığı anlaşılmaktadır. Bu sistemlere yönelik siber güvenlik olayları daha çok gizliliği kapsayan ulusal güvenlik açısından ele alınmış ve çevresel güvenlik ile ilişkisinin kurulmamıştır. İçişleri Bakanlığına bağlı olarak görev yapmakta olan Afet ve Acil Durum Yönetimi Başkanlığı, kendilerinin sadece afet olduktan sonra değil afet öncesi de hazırlık risk azaltma faaliyetlerini yerine getirme görevleri olduğunu dile getirmektedir. Bu görevlerin nasıl gerçekleştirileceğine yönelik Türkiye Afet Müdahale Planının günümüz koşullarına uygun güncellenmediği, kritik tesis tanımının sadece okul hastane gibi kamu binaları ile sınırlı tutulduğu; daha çok doğal afet sonrası durumlara yönelik bir yapılanma olduğu anlaşılmaktadır. Ancak On Birinci Kalkınma Planı paralelinde gerçekleştirilmesi gereken faaliyetlere yüzeysel olarak da olsa AFAD'ın Stratejik Planında yer verildiği görülmektedir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından kurumların operasyonel

faaliyetlerini yürütürken kullanımı için Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır. Bu dokümanda kritik altyapıları da kapsayacak şekilde ayrıntılı, güncel, uluslararası standartlara uygun operasyonel faaliyetlere yönelik bilgilere yer vermektedir. Kritik altyapıların siber güvenliğine yönelik faaliyetlerin ulusal ve küresel seviyede daha ayrıntılı olarak ele alınmasının ve bu konu ile ilgili stratejilerin ilgili tüm paydaşları kapsayacak şekilde geliştirilmesinin ve takip edilmesinin yararlı olacağı değerlendirilmektedir.

Bilişim teknolojilerinin küreselleşmeyi hızlandırması, küreselleşme sonucu zaman ve mekân kavramlarının önemini yitirmesi ve buna bağlı olarak her alandaki üretimin fiziki mekanlara bağlı olmaksızın dünyanın herhangi bir yerinde gerçekleştirilmesi ve kullanıma sunulması; dünya üzerinde pek çok alanın ağlarla birbirine bağlı hale gelmesi ve bu sistemlerde meydana gelebilecek bir sorunun küresel seviyede etki yaratma olasılığı meydana gelmeye başlamıştır. Teknolojideki bu hızlı gelişim toplumsal yapıları da etkilemiş, devletlerin fiziki sınırları da gittikçe önemsizleşmeye başlamıştır. Mevcut durumda, küresel seviyede sınır aşan sorunlar için hukuki kurallar tam olarak belirlenemediği ve bir geçiş dönemi yaşanmakta olduğu için mevcut sistemlere ek yeni kurumsal yapılarla sorunlar çözülmeye çalışılmaktadır. İkinci Dünya Savaşı sonrası kurularak faaliyete geçen BM, Dünya Bankası, NATO, OECD gibi uluslararası kuruluşlar tarafından devletler arasındaki ve küresel seviyedeki siber güvenlik sorunları ile ilgili politikaların oluşturulmasına yönelik çalışmalar gerçekleştirilmektedir. Bu uluslararası kuruluşlarda görev yapmakta olan hükümet yetkililerinin, siber güvenlik alanında gerekli teknolojik donanıma sahip olmadıkları için bu çalışmalara özel sektör çalışanları da dahil edilmeye başlanmıştır. Bu dönemin en önde gelen değişiklikleri güvenliğin sadece devletler tarafından sağlanamayacağının anlaşılması, özel sektör, sivil toplum kuruluşları gibi paydaşların katkısı ile yönetişim faaliyetlerinin kullanılmaya başlanması olmuştur.

Son dönemde sınır aşan sorunların çözümü için yoğun olarak kullanılmakta olan küresel yönetişimde, çok paydaşlı yönetsel ağların yaptırım uygulama yetkilerinin ve otoritelerinin bulunmaması, meşruiyet kazanmamış olmaları, küresel yönetişim birimlerinin karmaşık yapılarından dolayı içsel çatışma ve başarısızlık olasılığının yüksek olması; yönetişimi kimin yürüteceği ve kim için yapılacağının tartışma konusu olması; bireylerin ya da kurumların bilgeliğine ya da deneyimine dayanan otoritenin zorlayıcılığı ya da yaptırım

gücünün bulunmaması gibi olumsuzluklar gündeme getirilmektedir. Buna karşılık, kendilerini sadece içinde yaşadıkları devletle değil dünyanın tümüyle özdeşleştiren; insanların içinde doğdukları ya da geliştikleri topluluğa bakılmaksızın eşit ölçüde önemsenip göz önünde bulundurulmasını isteyen; çevrenin küresel seviyede korunmasının ön planda tutulmasını savunan kozmopolitler küresel yönetişim kurumlarına daha fazla inanmaktadır. Kozmopolitlere göre, küreselleşmeyi temsil eden uluslararası kuruluşlar; devletlerin bağımsız hareket etmesinin önüne geçmiş iken küresel yönetişim, tüm devletlerin, özel şirketlerin, bireylerin katılım sağlayabildiği tamamen farklı bir kavramdır. Yine bu gruba göre hakkaniyet ve adalet önemli olduğu için küresel yönetişim, dünyayı daha adil, daha iyi daha yaşanır bir yer kılmak üzere uygulanacak dayanışmacı bir yaklaşımdır.

Küresel siber güvenlik yönetişimi kapsamında, çok paydaşlı kuruluşlar ve yönetsel ağların faaliyetleri incelendiğinde, özellikle kritik altyapıların siber güvenliğine yönelik faaliyetlerin hangi devlet sınırları içinde olduğuna bakılmaksızın tüm insanların ve hatta tüm canlı ve cansız varlıkların, sürdürülebilirlik kavramına uygun olarak mevcudiyetlerinin devam ettirilebilmesi için gerçekleştirildiği anlaşılmaktadır. Siber güvenlik bağlamında çevrenin küresel seviyede korunması temel hedef olduğundan dolayı, sınır aşan siber güvenlik sorunlarının çözümünde, BT alanında gelişmiş devletlerin, standartları hazırlayan çok paydaşlı uluslararası kuruluşların, yönetsel ağların ve çok uluslu şirketlerin getirdikleri çözüm önerilerine uyulmasının küresel seviyede fayda sağlayacağı düşünülmektedir. Tüm canlı ve cansız varlıklar için hakkaniyet ve adaletin önemli olduğundan hareketle, siber güvenlik yönetişimi faaliyetlerinin de kozmopolitanizm kavramına uygun olarak gerçekleştirilmesinin sürdürülebilirlik açısından önemli faydalar sağlayacağı değerlendirilmektedir.

SONUÇ ve DEĞERLENDİRME

Jeolojik dönemlerin sonuncusu olan Antroposen Çağda (insan çağı), insan yeryüzü sistemlerine hükmetmeye başlamış ve müdahaleleri ile doğayı değiştirmiştir. İnsanın doğa üzerindeki faaliyetleri kendisinin de içinde yaşadığı, tüm insanların ve diğer canlıların ortak varlığı olan doğaya zarar vermeye başlamış; tüm canlıların yaşam ortamlarının kirlenmesine ve olumsuz etkilenmesine neden olmuştur. Bu olumsuz etki özellikle Endüstri Devrimi sonrası hızlanmış ve 1980'li yıllarda başlayan küreselleşme ile had safhaya ulaşmıştır.

Bilişim teknolojilerinin hızlı bir şekilde gelişmeye başladığı 1970'li yıllardan itibaren bilgi ve iletişim sistemleri insan hayatının her alanında kullanılmaya başlanmış ve Dördüncü Sanayi Devrimi ya da Sanayi 4.0 olarak adlandırılan dönem ile birlikte içinde yaşadığımız fiziki dünya üzerinde insan eli ile geliştirilmiş yeni bir alan olan siber uzay oluşturulmuştur. Her geçen gün artan sayıda yazılım, donanım, ağ ürünü ile siber uzay genişlemeye başlamış ve daha çok insan tarafından kullanılır hale gelmiştir. İnsanların siyasi, ekonomik toplumsal açıdan çok fazla ilişki içinde olduğu küreselleşme olgusunun başlangıcı bu dönemlere denk gelmektedir. Küreselleşmeyi teknolojik açıdan destekleyen bilişim teknolojilerinin yaygın kullanımı ve tüm dünyadaki sistemlerin birbirlerine ağlarla bağlanmaya başlaması ile siber uzay daha da genişlemiş ve ulus devletler arasındaki sınırlar pek çok durumda geçersiz hale gelmiştir.

Bilişim teknolojilerinin her alanda yoğun olarak kullanıldığı günümüz modern dünyası bilgi toplumu olarak adlandırılmaktadır. Ulrick Beck ise sonucu kestirilemeyen güvenlik olaylarının meydana gelmesine dikkat çekerek günümüz toplumunu risk toplumu olarak adlandırmıştır.

Geleneksel güvenlik anlayışında güvenliğin sağlayıcısının devlet olduğundan hareketle devlete yönelik askeri tehditlere odaklanılmakta iken 1980'li yıllardan itibaren, hayati bir tehdit unsurunun belirlenmesi sonrasında bu tehdidin ortadan kaldırılabilmesi için olağanüstü tedbirlerin alınması gerektiği kabul edilerek askeri sektöre ek olarak siyasi,

ekonomik, toplumsal ve çevresel güvenlik sektörleri de tanımlanmıştır. Askeri, ekonomik, toplumsal hayatın her alanında bilişim teknolojileri kullanılmakta olduğu için ve hayati önemde tehdit oluşturmaya başladığı için siber güvenlik kavramı da güvenlik literatürüne girmiştir. Günümüzde güvenlik, sadece iki devlet arasında değil küresel ya da bölgesel seviyede ortak ve çok taraflı sorunlara ilişkin olabilmektedir.

Bilişim teknolojilerinde önemli değişikliklerin yaşanmaya başlandığı 1970'li yıllardan itibaren, insanların içinde yaşadıkları çevrenin önemi ve çevreye verilen zararlar da fark edilmeye başlanmıştır. Bu dönemden itibaren çevre sorunlarının giderilmesine yönelik alınacak önlemleri belirleme kapsamında, insanların birbirlerine, diğer canlılara ve çevreye karşı davranışlarını, ahlaki sorumluluklarını konu edinen çevre etiği kavramı kullanılmaya ve bu alanda yayınlar yapılarak çözüm yolları aranmaya başlanmıştır. Bu bağlamda felsefeciler tarafından doğadaki canlı, cansız varlıkların ve işlevlerin tümünün, ahlaki değere sahip tek varlık olan insan için olduğunu savunan insan merkezli çevre etiği; insan dışındaki canlı varlıkların sırf doğada var oldukları için ahlaki değere sahip olduğunu savunan canlı merkezli çevre etiği ile doğanın, ekolojik sistemin mevcudiyetinden dolayı kendi içinde, kendisi için bir değere sahip olduğunu savunan çevre merkezli çevre etiği geliştirilmiştir. Çevre etiği düşüncesi içinde çevresel sorunlara çözüm getirebilme amacı ile felsefeciler tarafından farklı yaklaşımlar benimsenmiştir. Leopold yeryüzü etiği düşüncesi ile insanların doğanın sağlığını ve bütünlüğünü korumak için etkin ve uygulanabilir yöntemler geliştirmeye gayret etmesi gerektiğini dile getirmiştir. Naess, insanın merkezde olmadığı bütüncül yaklaşımı, derin ekoloji olarak tanımlamıştır. Derin ekoloji kavramının ilkeleri arasında ekosistemde yer alan her şeyin değerli olduğunun kabul edilerek türlerin varlığının sürdürülmesi, insanların çevreyi yok etmeksizin ve ekosistemin dengesini bozmaksızın yaşamaları için zorunlu ihtiyaçlarını karşılamaları; çevreye müdahalede bulunmaktan rahatsızlık hissetmeleri; maddeci, faydacı ve rekabetçi yaşam felsefelerinin değiştirilmesi; ekonomik ve ideolojik kurumları etkileyecek değişikliklerin yapılması hususlarını saymaktadır. Bookchin ise, derin ekoloji savunucularını insanın doğada yer alan diğer varlıklardan üstün bir tarafının bulunmadığını düşündükleri için ve ekolojik sorunların tek sorumlusu olarak insanı gördükleri için baskıcı ve insan karşıtı olmakla suçlamış ve toplumsal ekoloji fikrini geliştirmiştir. Toplumsal ekoloji düşüncesine göre insan, doğal

evrim ile ekosistem içindeki diğer varlıklardan farklılaşmış, sahip olduğu önemli özellikler ile evrim sürecinin yönünü belirleyebilir duruma gelmiştir. Bookchin, insan dışındaki fiziki ortamı anlatmak üzere biyolojik/birinci doğa; insanlık tarafından geliştirilen ussallık, kültür ve toplum özelliklerini anlatmak üzere ise toplumsal/ikinci doğa terimlerini kullanmış; insanın fiziki varlığı ile birinci/fiziki doğa içinde yer aldığını; ancak gerçekleştirdiği olumlu olumsuz tüm eylemlerin insan tarafından kurulmuş toplumun özellikleri ile yani toplumsal/ikinci doğa ile ilişkili olduğunu belirtmektedir. Bookchin'in toplumsal ekoloji düşüncesine göre, doğal çevrenin yıkımının önlenmesi için insanın doğa üzerindeki egemenliği kaldırılmalı ve ekolojik bir topluma en uygun yapısal temel oluşturulmalıdır. Bunun için, doğanın çok çeşitlilik içeren, ögelerinin birbirini tamamlama ilkesine göre kurulmuş adem-i merkeziyetçi yapısına uygun olarak çeşitlilikler içeren, merkeziyetçi olmayan, ögeleri hiyerarşik yapıda olmayan, bunun yerine birbirlerini tamamlayacak şekilde düzenlenmiş bir toplumsal yapı önermektedir.

Bu çalışmada, çevre etiği yaklaşımlarından insan merkezli yaklaşımın doğadaki her şey insan içindir fikrinin de insanın doğadaki diğer varlıklardan hiçbir farkı bulunmadığı ve çevre sorunlarının tek sorumlusu olduğu derin ekoloji yaklaşımının da çok abartılı olduğu kanaatine varılmıştır. Doğada var olan tüm canlı ve cansız varlıkların mevcudiyetlerinden dolayı bir değerleri olduğu ve varlıklarının sürdürülmesi gerektiği temel varsayımından hareketle, bütüncül çevre etiği yaklaşımı benimsenmiştir. Değer bakımından mevcudiyeti ile doğada yer alan diğer canlı cansız varlıklarla bir farkı olmadığı düşünülen insanın ahlaki ehliyeti olduğu ve yaptıklarından sorumlu tutulması gerektiği de kabul edilmektedir. Bütüncül çevre etiği yaklaşımı kapsamında Bookchin'in de vurguladığı gibi insan, ekosistemdeki diğer varlıklardan farklılaşmış ve evrim sürecinin yönünü belirleyebilir duruma gelmiştir. Genel anlamda insan davranışlarının tümü doğaya zarar verecek şekilde değildir; insan geliştirdiği teknoloji ile kendi ihtiyaçları doğrultusunda doğa üzerinde olumlu değişiklikler de yapmaktadır. Yazılım, donanım, ağ bileşenlerinden oluşan siber fiziki sistemler ile bu sistemleri üreten, yöneten, kullanan, bu sistemlerden etkilenen insanlar ve kurumsal yapılardan oluşan siber uzay bu tanıma göre toplumsal/ikinci doğa üzerinde bir katman olarak yer almaktadır.

İçinde yaşadığımız dönemde, bilişim teknolojilerindeki ve siber güvenlik alanındaki gelişmeler paralelinde, kamu ve özel sektör kuruluşları tarafından işletilmekte olan ve işlevlerini yerine getiremedikleri ya da yanlış sonuçlar ürettikleri durumlarda toplumsal kaos, can ve mal kaybına neden olabilecek kritik altyapı sistemleri de hızlı bir şekilde siber uzaya dahil olmaya başlamıştır. Siber uzay üzerinden birbirleri ile bağlı olarak faaliyette bulunan enerji sektörü, baraj, su ve kanalizasyon sektörü, kimya sektörü ile iletişim sektörü gibi pekçok alanda bilişim teknolojileri ve operasyonel teknolojilerin yararı inkâr edilemeyecek sistemler olup günlük hayatın vazgeçilmezleri arasında yerini almıştır. İnsanların ve canlı-cansız tüm varlıkların küresel seviyede birbirlerine ağlarla bağlı siber uzayı kullanarak hayatlarını sürdürdüğü günümüz dünyasında, bu teknolojilerin yararlı kullanımı yanında pek çok yüksek dereceli riskler de gündeme gelmeye başlamıştır. Dünya üzerindeki varlıkların birbirlerine ağlarla bağlanması ile hızlı bir şekilde gelişen siber uzayın tüm canlılar için ve çevre için ne tür sorunlar oluşturabileceği henüz tam olarak bilinmemektedir. Ancak, insan eli ile oluşturulan bir ortam olması nedeni ile siber uzaydan kaynaklanabilecek tüm sorunların insanın çevreye karşı sorumluluğu kapsamında ele alınması gerektiği düşünülmektedir. Toplumsal ekolojinin, insanın insan üzerindeki ve doğa üzerindeki tahakkümünün önüne geçilebilmesi için çözüm olarak sunduğu adem-i merkeziyetçi yapıların siber uzay üzerinden de oluşturulması ve merkezi hiyerarşik yapının devre dışı bırakılması gerekmektedir. Siber uzayda merkezsizleştirilmenin sağlanması için geliştirilmesine başlanan blok zincir teknolojileri bulunmakla birlikte henüz tam olarak uygulamaya giremediği için en azından günümüz dünyasında sistemlerin birbirlerinden ayrı olarak faaliyetlerini sürdürmeleri mümkün değildir. Temelinde ağ yapılanması olan siber uzayın yönetiminde hiyerarşik bir yapı yer almaktadır. Bu durumda toplumsal ekoloji yaklaşımının siber uzay için tam olarak geçerli olamayacağı, onun yerine pragmatik yaklaşım ile çevresel sürdürülebilirliğin benimsenmesinin daha uygun olacağı değerlendirilmektedir.

Çevresel sürdürülebilirliğin sağlanmasına önemli katkıları olan bilişim teknolojilerinin, kötü niyetli kişilerin eline geçmeleri durumunda insanlar, toplumlar, diğer canlı ve cansız varlıkların oluşturduğu çevre için oluşturabilecekleri yıkıcı etkileri de göz ardı edilmemelidir. Siber güvenlik olaylarının sürdürülebilirliği engelleyecek boyutta çevre

sorunları oluşturup oluşturmayacağını araştırmak üzere siber güvenlik kavramı üzerine yoğunlaşılmıştır. Siber güvenlik, insanlar tarafından fiziki dünya paralelinde oluşturulan ve her türlü işlemin yürütülmesi için kullanılmakta olan siber uzayın, gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olarak güvenliğinin sağlanmasına yönelik faaliyetleri kapsamaktadır. Siber güvenlik faaliyetleri ile siber tehditlerin gerçekleştirilmeden önce tespit edilmesi ve gerekli önlemlerin alınması, gerçekleşmekte olan siber ya da fiziki saldırının tespit edilebilmesi ve en kısa süre içerisinde etkisiz hale getirilebilmesi, saldırıya uğrayan sistemin saldırı öncesindeki çalışır durumuna getirilebilmesi hedeflenmektedir. Siber güvenliğin kapsama alanı içinde, saldırgan niyeti olmaksızın kaza eseri gerçekleştirilmiş siber güvenlik olaylarının ve insan etkisi olmadan deprem, sel, yangın gibi doğal afetler sonucu oluşacak fiziki hasarlara karşı da bilginin ve bilişim sistemlerinin korunması ve eğer bir hasar oluştu ise eski haline döndürülmesi işlemleri de yer almaktadır. Sürdürülebilirlik yaklaşımı kapsamında, gelecek nesillerin kullanımını kısıtlamadan bugünkü kaynakların verimli kullanımı ile siber uzayda yer alan kritik altyapı sistemlerinin faaliyetlerinin devam ettirilmesi gerektiği, bu nedenle de bu sistemlere yönelik siber güvenlik olaylarının engellenmesi gerektiği değerlendirilmektedir.

Bu çalışma kapsamında, siber güvenliğin, tüm canlıların, varlıkların ve doğa olaylarının mevcudiyetinin devam ettirilmesi; günümüzdeki nesillerin ihtiyaçlarının gelecek nesillerin kullanımını etkilemeksizin sürdürebilmesi olarak açıklanabilecek olan sürdürülebilirlik yaklaşımı açısından ele alınması nedeni ile çevre üzerinde fiziki etki oluşturabilecek siber güvenlik olayı örnekleri incelenmiştir. Ulus devletlerin ya da özel sektör kuruluşlarının ulusal güvenlik ve prestij kaygısı gibi nedenlerle şeffaf davranmadığı, tüm olayları açıklamadığı günümüz dünyasında açık kaynaklardan kısıtlı sayıda örnek olay bilgisi edinilebilmiştir. Bu kısıtlı sayıdaki örnek olayda bile, petrol boru hatlarına, nükleer santrallere, elektrik üretim ve dağıtım hatlarına, sulama, kanalizasyon, su arıtma tesislerine, kimyasal tesislere vb.ne yönelik siber güvenlik olaylarının çevreye önemli ölçüde zarar verdiği durumların yaşandığı ya da çevre üzerinde önemli olumsuz etkiler oluşturma kapasitesinin yüksek olduğu görülmüştür.

Bahsi geçen kritik altyapılar birbirlerine ağlarla bağlı olduğu için oluşan hasar sadece küçük bir fiziki alanla sınırlı değildir, birbirlerini tetikleyebilecek çok önemli çevre

felaketlerinin yaşanmasına neden olabilecektir. Günümüz modern dünyasında pek çok işlem ağlarla birbirine bağlı bilişim sistemleri üzerinden gerçekleştirildiği için bu sistemlerde oluşacak bir siber güvenlik olayı diğer sektörlerdeki faaliyetlerin de yerine getirilememesine, önemli aksamalara neden olabilecektir.

İşlevlerini yerine getiremedikleri durumda önemli çevresel sorunlara yol açabilecek enerji üretim, dağıtım, su ve kanalizasyon, nükleer tesisler ve kimyasal tesisler gibi kritik altyapılarda son dönemlerde endüstriyel kontrol sistemlerinin yoğun olarak kullanılmaya başlandığı, endüstriyel kontrol sistemlerinin de bilgi ve iletişim teknolojilerindeki gelişmeler sonrası her geçen gün daha da artan bir şekilde dijitalleştiği ve siber fiziki sistemler olarak adlandırıldığı görülmüştür. Kritik altyapı sistemlerine yönelik kasıtlı insan faaliyetleri ile siber saldırılar gerçekleştirilmesi; kasıtsız insan hatası sonucu sistemlerin planlandığı şekilde çalışmaması; sistemlerin korunmasına yönelik işlemlerin düzgün bir şekilde gerçekleştirilememesi ya da deprem, yangın, sel gibi doğal felaketler sonucunda oluşan siber güvenlik olaylarının fiziki çevre üzerinde canlı ve cansız varlıkların sürdürülebilirliğini olumsuz yönde etkileyebileceği sonucuna varılmıştır.

Kritik altyapı sistemlerinin zarar görmeksizin planlandıkları gibi faaliyetlerine devam etmeleri, çevre etiği açısından sürdürülebilirliğin sağlanması yani bugün yaşamakta olan kuşağın gereksinimlerinin, gelecek nesillerin kendi ihtiyaçlarını karşılama yeteneğini ortadan kaldırmaksızın karşılanmasının sağlanabilmesi için gerekli güvenlik önlemleri alınmalıdır. Bu sistemlerin siber güvenliğinin sağlanmasına yönelik önleyici/koruyucu yaklaşım, risk yönetimi yaklaşımı, caydırıcılık yaklaşımı ve kamu siber güvenlik yaklaşımı olmak üzere 4 farklı siber güvenlik yaklaşımı bulunmaktadır:

Hizmetlerini EKS kullanarak yerine getirmekte olan kritik altyapılarda beklenmeyen bir siber güvenlik olayı sonrasında meydana gelebilecek ve önemli çevre felaketlerine neden olabilecek hasarın kapsamını sınırlamak, bu siber olayın neden olabileceği hizmet kesintisinin süresini olabildiğince azaltmak ve beklenmeyen siber olayın meydana gelmesinden önceki duruma tam olarak dönülemese de yeni duruma uyum sağlamak ve zaman içinde sistemlerin faaliyetlerinde iyileştirme sağlayabilmek için önleyici/koruyucu güvenlik yaklaşımı kapsamında sistemlerin emniyeti ve dayanıklılığını sağlamak üzere, bu

sistemlerin tasarlanması aşamasından itibaren üretimi, kullanılması ve kullanım dışı kalması aşamalarını kapsayan tüm yaşam döngüsü boyunca uygulanılması kaçınılmazdır.

Sistemlerin tüm güvenlik açıklarının kapatılamayacağı; güvenliğe yapılacak yüksek miktardaki yatırımların sonuçta önlenecek saldırıdan kaynaklanan zarara değmeyeceği; karşılaşılabilecek risklerin oluşturacağı hasarın kurumsal yapıya, verilen hizmetin niteliğine ve hizmetin verildiği hedef kitleye göre de değişebileceği göz önünde bulundurularak risklerin belirlendiği, değerlendirildiği, önemine binaen gerekli önlemlerin alındığı risk yönetimi yaklaşımı kullanılmaya başlanmıştır. Bu yaklaşıma göre, kritik altyapıların güvenlik açıklarının analiz edilmesi ve uygun güvenlik önlemlerinin uygulanması ile siber güvenlik olayı meydana gelme riski azaltılabilecektir. Kritik altyapı varlıklarının tanımlanması, bu varlıkların kurum açısından değerlerinin belirlenmesi, bu varlıklara yönelik tehditlerin ve güvenlik açıklarının belirlenmesi, risk analizinin yapılması, güvenlik açıklarından kaynaklanabilecek risk olasılıklarını azaltmak amacı ile uygulanabilecek önlemlerin işleme konulması ve riskin yeniden değerlendirilmesi aşamalarından oluşan risk yönetimi döngüsü belirli aralıklarla yinelenmelidir.

Siber caydırıcılık yöntemi kullanılarak siber güvenlik önlemlerinin artırılması ile kötü niyetli saldırganın maliyet fayda analizi yapmasını sağlayarak ağ etkisini azaltması yolu ile saldırıdan cayma ya da saldırganı durdurmaya zorlayabileceği; ceza yoluyla, saldırganın eylemlerinin sonucunda ortaya çıkacak maliyeti fark etmesi ve cesaretinin kırılması ile eylemi yapmaktan vazgeçirilebileceği; devletler arası karşılıklı bağımlılığın devletler arası çatışmayı azaltabileceği; siber uzayda devletlerin davranışlarını düzenleyecek ve zamanla kötü davranışı genel bir kısıtlama ilkesine dönüşecek norm ve kuralların oluşturulmasına odaklanan gayrı meşrulaştırma yoluyla caydırıcılığın işlev kazanacağı değerlendirilmektedir.

Siber güvenliğin, çoğunluğun ortak faydası için gerçekleştirileceğinden hareketle kamu yararı niteliği taşıdığı ve önemli bir ihtiyaç olduğu için kamu siber güvenlik yaklaşımı, bireysel, kurumsal ve ulusal seviyede ve daha da ileri gidilerek küresel seviyede kullanılabilecek siber güvenliğin sağlanmasına yönelik bir düşünce tarzıdır. Bu yaklaşımda toplumsal felaketleri önlemek düşüncesi ile hareket edilmesi öngörülmektedir. Burada bahsedilen kamu ya da toplum, dünyanın her yerinde yaşamakta olan aileler, dostlar, mesai

arkadaşları, işverenler, komşular, hemşehriler, vatandaşlar, kadınlar gibi farklı biçimde tanımlanabilecek insanlardan oluşmaktadır. Herkese yönelik güvenlik önlemleri alınması, bu alanda görevli siber güvenlik çalışanlarının kendi yakınlarını da kapsadığı düşünüldüğünde daha anlamlı hale gelmektedir. Gelecek nesillerin de en az bugünkü olanaklara sahip olarak yaşamlarını devam ettirebilmeleri için sürdürülebilirlik kavramına uygun olarak siber güvenlik faaliyetlerinin sürdürülmesi, bu alanın her seviyesinde görev yapmakta olan bireyler için işin anlamlı hale gelmesine yardımcı olacaktır.

Günümüzde kullanılmakta olan bilişim sistemlerinin teknolojik karmaşıklığı, kullanım amaçlarının ve ürettikleri hizmetlerin çeşitliliği; kullanıcıların farklı seviyelerdeki teknik bilgi ve becerisi, hassasiyeti; siber saldırganların teknik bilgilerindeki ve motivasyonlarındaki farklılıklar; saldırılardaki çeşitlilikler gibi nedenlerle günümüz siber dünyasında siber güvenlik, bu dört yaklaşımın çoğu kez birlikte kullanılmasını gerektirmektedir. Siber güvenliğin sadece teknolojik boyutu değil, bireysel, kurumsal, ulusal ve uluslararası boyutları da gündeme getirilmeye başlanmıştır. Bu çalışmada endüstriyel kontrol sistemlerinin dolayısı ile kritik altyapıların siber güvenliğinin sağlanmasına yönelik faaliyetler operasyonel faaliyetler ve stratejik faaliyetler olarak 2 grupta toplanmıştır. Bu sistemlerin tasarımı, geliştirilmesi, üretilmesi, kullanımda olması ve kullanım dışı kalması aşamalarını kapsayan tüm yaşam döngüleri boyunca doğrudan ilişkili bireyler ve kuruluşlar tarafından gerçekleştirilen faaliyetler, operasyonel faaliyetler olarak adlandırılmıştır. Operasyonel faaliyetler altında bireyler ve kuruluşlar tarafından gerçekleştirilmesi gereken önleyici-koruyucu yaklaşım ve risk yönetimi yaklaşımına yer verilmiştir. Sistemlerin siber güvenliğinin sağlanmasına yönelik politika ve stratejilerin geliştirilmesi faaliyetleri ise stratejik faaliyetler olarak adlandırılmıştır. Stratejik faaliyetler altında devletler, küresel ya da bölgesel seviyede uluslararası kuruluşlar, çok uluslu şirketler, sivil toplum örgütleri, bireyler vb.den oluşan paydaşların katılımı ile gerçekleştirilmekte olan caydırıcı yaklaşım ve kamu siber güvenlik yaklaşımına yer verilmiştir.

Teknolojideki hızlı gelişmeler paralelinde kritik altyapılara yönelik tehditlere ve siber güvenlik açıklarına her gün yenilerinin eklenmekte olduğu ve önemli belirsizliklerin ortaya çıktığı görülmektedir.

Siber güvenlik alanında çalışmakta olan profesyonellerin, uygulamalarının insanların yaşam kalitesini önemli ölçüde etkileyebileceği birçok yol konusunda dikkatli olmaları ve etkili bir şekilde ele alınabilmeleri için potansiyel zararlarını ve faydalarını daha iyi tahmin etmeyi öğrenmeleri gerekir. Kritik altyapıların faaliyetlerini yerine getirmek üzere kullanılmakta olan endüstriyel kontrol sistemlerinin tasarlanmasında, üretiminde, kullanımında rol alan tüm insanların kendilerini sorumluluklarının bilincinde dünya vatandaşı olarak görüp, küresel seviyede sürdürülebilirliği sağlamak üzere ihmal veya sorumsuz hareketlerden kaçınmaları gereklidir. Çoğu durumda artık bu sistemleri kullanan personel teknik personel olmadığı için kullanıcı dostu sistemler üretilmeli ve bu sistemlerin kurallarına uygun kullanıldığından emin olunmalıdır. Siber güvenliğe yönelik uygulamaların doğru bir şekilde kullanılması, çok bilinen ve uygulanan en iyi teknik uygulamaların takip edilmesi yerinde olacaktır.

Endüstriyel kontrol sistemlerinin siber güvenliğinin sağlanmasında teknolojik çözümler kullanılmaktadır ancak mevcut durumda bu alanda faaliyet göstermekte olan kuruluşların genellikle sorunları tespit etmek için teknolojiye değil, çalışan personele güvendiği görülmüştür. Bu sistemleri tasarlayan, geliştiren, kullanan insan faktörünün önemi göz ardı edilmemelidir. Kritik altyapı sistemlerinin tasarımı, üretimi, faaliyete geçirilmesi, güvenliklerinin sağlanması tek başına bireylerin yapamayacağı görevler olup bu sistemleri tasarlayan, geliştiren, işleten kurumsal yapılara ihtiyaç vardır. Kurumsal seviyede kritik altyapıların siber güvenliğinin sağlanması için BT risklerini ele alarak bu risklerin azaltılması için tanımlanmış olan ve teknolojideki gelişmelere paralel olarak yenileri eklenen siber güvenlik kontrolleri tanımlamıştır. Yönetimsel, operasyonel ve teknik başlıkları altında toplanan bu kontroller yardımı ile etkili sonuçlar meydana getirebilecek riskleri denetim altında tutmak üzere kullanılacak faaliyetler ve yöntemler gözden geçirilebilmektedir. Sistemlerin oluşturabileceği riskleri ve tehditleri anlamak üzere bu sistemlerin tasarımından kullanım dışı kaldığı duruma kadar her seviyede kurumlar tarafından risk yönetimi yaklaşımı uygulanmalı, bu kapsamda belirli aralıklarla sistemlere yönelik tehditler ve güvenlik açıkları belirlenmeli, risk olasılıkları hesaplanmalı ve bu riskleri azaltmak ve yok etmek için gerekli önlemler alınmalıdır.

Kritik altyapıların bireysel ve kurumsal seviyede siber güvenliğini sağlamaya yönelik faaliyetler, bu alanda ilerleme kaydetmiş gelişmiş devletlerin kurumsal yapıları ve uluslararası kuruluşlar ile çok uluslu şirketler tarafından geliştirilmiş standartlara ve rehber dokümanlara uygun olarak yürütülmektedir.

Geleneksel güvenlik anlayışına göre devletler, kendi fiziki sınırları içinde yer alan tüm varlıklarını koruyabilecekleri emniyetli ve güvenilir bir ortamı, kendi hukuki düzenlemelerini kullanarak tesis etmeyi hedeflemektedir. Ancak teknolojinin hızlı gelişimi ve aynı hızla günlük hayata dahil olması nedeni ile bu teknolojilere yönelik mevzuat henüz tam olarak geliştirilememiş ve nihai halini alamamıştır. Tüm devletlerin aynı gelişmişlik seviyesinde olmadığı göz önünde bulundurulduğunda da yasal düzenlemelerin hızlı bir şekilde devletlerde uygulamaya konulamayacağı değerlendirilmektedir. Bu sistemlerde yaşanmakta olan çok hızlı teknolojik gelişmelerden kaynaklı belirsizlikler ve öngörülemezliklerden dolayı mevcut politikaların bu tehditlerle etkili bir şekilde başa çıkamayacağı da göz önünde bulundurulmalıdır. Devletlerin bu tür belirsizlikleri dikkate alarak duruma uyarlanabilir politikalar geliştirmeleri gerekmektedir.

Ortak toplumsal faydayı ve vatandaşın güvenliğini ön planda tutan devletler, bir kritik altyapıdaki siber güvenlik olayının diğer kritik altyapılara da sıçrayabileceğini ve önemli çevresel güvenlik sorunlarına yol açabileceğini göz önünde bulundurarak bu sistemlere yönelik riskleri yönetmek amacıyla en uygun ve etkili güvenlik önlemlerinin alınabilmesi için gerekli politikaları belirlemeli ve uygulamalıdır. Bu politikaların, kritik altyapı sistemlerinin amaçlarına uygun olarak hizmetlerini yerine getirmesine engel olmaksızın siber güvenlik önlemlerinin alınmasını da sağlaması gerekmektedir.

Devletler seviyesinde siber güvenliğin sağlanmasına yönelik politikaların, stratejilerin belirlendiği ve yayımlandığı ulusal siber güvenlik stratejilerinde, devletlerin koruyucu önleyici güvenlik yaklaşımı kapsamında, ilgili paydaşları kritik altyapı sistemlerinin emniyeti ve sağlamlığını sağlamaya ve derinlemesine savunma yöntemlerini kullanmaya teşvik etmesi önem arz etmektedir. Kritik altyapıyı ve temel hizmetleri belirlemek ve korumak için yerel endüstrinin küresel BİT tedarik zincirleriyle bütünleşmesini sağlamak ve ulusal sınırların ötesinde birlikte çalışabilirlik sorunlarından kaçınmak için, uluslararası standartlara uygun risk yönetimi yaklaşımı kullanılmalıdır.

Devletler, esneklik ve sağlamlık çabalarına öncelik verebilmek için kritik altyapı sistemleri arasındaki karşılıklı bağımlılık ve güvenlik açıklarının iyi anlaşılmasını sağlamak üzere diğer altyapı, hizmet ve etki kapsamı ile bağımlılıklar ve karşılıklı bağımlılıklar ve minimum hizmeti sürdürmek için gereken kriterleri belirlemelidir. Devletlerin, kritik altyapılarının siber güvenliğini sağlamak üzere, potansiyel düşmanlarını caydırmak amacı ile ulusal siber güvenlik stratejilerinde, hangi yeteneklere ve nasıl bir teknolojiye sahip oldukları hakkında sadece konunun uzmanları tarafından anlaşılabilecek şekilde bilgi vermeleri yerinde olacaktır.

Günümüz modern toplumlarında kritik altyapı sistemlerinin önemli bir kısmının özel sektöre ait olduğu; kaynaklarının planlanması, yönetilmesi, güvenilir bağlantının sağlanması, trafik ve hizmetlerin dağıtımı gibi faaliyetlerin de özel sektör firmaları tarafından gerçekleştirilmekte olduğu görülmüştür. Siber uzayın doğası gereği bu sistemleri devletlerin tek başlarına yönetemeyecekleri, konu ile ilgili kamu kurumları, özel sektör temsilcileri, devlet dışı küçük gruplar, üniversiteler ve uluslararası paydaşlarla yönetişim esasına uygun politikalar geliştirmeleri gerektiği anlaşılmıştır.

Devletler, kritik kamu hizmetlerinin yerine getirilmesi işlevine sahip kritik altyapıların siber güvenliğinin sağlanması hususunda özel sektör firmalarına düzenleyici kurallar getirerek ve özel sektöre uygulanan vergi teşvikleri, teşvik hibeleri, düşük maliyetli ya da karşılıksız krediler, düşük sübvansiyonlar, sigorta gibi yöntemlerle sağlayarak yardımcı olmalıdır. Risk yönetimi yaklaşımının uygulanmasında da kamu, yarı kamu ve/veya özel altyapı operatörleri dahil olmak üzere tüm ilgili paydaşların sürekli katılımı sağlanmalıdır.

Kamu güvenliğinden devletler sorumlu olduğu için ve özel sektör firmalarının daha çok kâr odaklı olmaları nedeni ile güvenliği çok önemsemeyebilecekleri fikrinden hareketle kritik altyapıların siber güvenliğinin sağlanmasında devletlerin önemli rolleri olduğu değerlendirilmektedir. Ancak teknolojiyi geliştiren özel sektör firmalarının etkisi de yadsınamaz bir gerçektir. Kritik altyapıların yazılım, donanım ve ağ bileşenleri, farklı devletlerde kurulmuş bulunan çok uluslu şirketler tarafından geliştirilmekte olduğu; bu sistemlerin devlet sınırlarına bağlı olmaksızın siber uzay üzerinden birbirlerine bağlı ve bağımlı olarak faaliyet gösterdikleri ve bir kritik altyapı sistemindeki sorunun o devletin

sınırları dışında konumlanmış olan diğer kritik altyapılara da sıçrayabileceği gibi durumlar göz önünde bulundurulduğunda, siber güvenlik alanında devletlerin kendi sınırları içinde faaliyet göstermekte olan yerel özel sektör kuruluşları ile birlikte yapabileceklerinin sınırlı olduğu ve kritik altyapıların siber güvenliğinin küresel seviyede ele alınması gerektiği daha iyi anlaşılmaktadır.

Mevcut durumda, küresel seviyede sınır aşan sorunlar için hukuki kurallar tam olarak belirlenemediği ve bir geçiş dönemi yaşanmakta olduğu için bu sistemlere ek yeni kurumsal yapılarla sorunlar çözülmeye çalışılmaktadır. Fiziki dünya paralelinde insan eli ile geliştirilmiş olan ve her geçen gün bağlantılarının ve dolayısı ile kullanıcılarının katlanarak arttığı siber uzayın da etkisi ile günümüzde, dünya genelinde oluşan ve her geçen gün daha da önemli hale gelen ekonomik, kültürel sorunlar, çevresel güvenlik sorunları gibi sınır aşan küresel sorunların çözümleri için küresel yaklaşımlar kullanılmaya başlanmıştır. Bu dönemde dünya devletleri arasında karşılıklı bölgelerarası ve küresel seviyede siyasi, ekonomik, kültürel alanlarda oluşan rekabetin mevcut hiyerarşileri sarstığı; terör, çevre sorunları, ekonomik sorunlar gibi sınır ötesi sorunların her geçen gün artarak ulus devletlerin geleneksel rolleri sorgulanır hale gelmiştir. Ulus devletlerin yetersiz kaldığı bu tarz sınır aşan sorunlar için küresel yönetişim mekanizmasının uygulanmasının bir zorunluluk olduğu değerlendirilmektedir.

Siber uzay, doğası gereği devletlerin fiziki sınırlarından bağımsız olduğu için ulusal siber güvenlik de ulus ötesi olup farklı aktörlerin bir arada çalışmasını gerektirmektedir. Dünya üzerindeki tüm toplumları, devletleri birbirine bağımlı kılan olay, toplumun ortak malı sayılan çevrenin korunması ve kaynakların verimli kullanımlarının sağlanması olduğundan hareketle "Siber güvenlik olaylarının sürdürülebilirliği engelleyecek boyutta çevre sorunları oluşturma riskini önlemek üzere nasıl bir siber güvenlik yönetimi uygulanmalıdır?" araştırma sorusuna çözüm olarak küresel seviyede yönetişim uygulanması gerektiği sonucuna ulaşılmıştır.

İkinci Dünya Savaşı sonrası kurularak faaliyete geçen BM, Dünya Bankası, NATO, OECD gibi uluslararası kuruluşlar tarafından devletler arasındaki ve küresel seviyedeki siber güvenlik sorunlarına yönelik politikaları oluşturmak üzere çalışmalar gerçekleştirilmektedir. Bu tarz uluslararası kuruluşlarda görev yapmakta olan hükümet yetkililerinin, teknolojik bir

alan olan siber güvenlik alanında gerekli donanıma sahip olmadıkları için bu seviyedeki çalışmalara özel sektör kuruluşları da dahil edilmeye başlanmış yani resmi olarak çok paydaşlı yönetişim mantığı kullanılmaya başlanmıştır. Sınır aşan sorunlar arasında yer alan kritik altyapıların siber güvenliğinin ulus devletlerin kendi aralarındaki ikili ya da bölgesel iş birliğinin ve hatta bu ulus devletlerin hükümet yetkilileri ile temsil edilmekte oldukları uluslararası kuruluşların çalışmalarının yeterli olmadığı görülmüştür. Bu uluslararası kuruluşların kendi bünyelerinde ya da onlardan bağımsız olarak çok uluslu şirketler ve kamu özel sektör iş birliği ile kurulmuş Dünya Ekonomik Forumu (WEF), Uluslararası Telekomünikasyon Birliği (ITU), Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC), Uluslararası Otomasyon Topluluğu (ISA), İnternet Güvenlik Merkezi (CIS), IEEE gibi çok paydaşlı kuruluşlar ve yönetsel ağlar ortak siber güvenlik hedeflerine ulaşabilmek için birlikte çalışmaya başlamıştır.

Çok paydaşlı küresel yönetişim yöntemi ile siber güvenlik alanında yürütülmekte olan faaliyetlerin en önemlisi, siber güvenlik alanında uluslararası hukuk kuralları bulunmadığı için modern devletler tarafından kullanılmakta olan standartların, kılavuzların ve en iyi uygulama örneklerinin geliştirilmesi ve diğer devletlere de bu standartların kullanımının önerilmesidir. Bu standartlar, dünyanın farklı ülkelerinde geliştirilen donanım ve yazılımlarının birlikte çalıştırılabilir olması ve aynı niteliklere sahip olarak üretilebilmesini sağlayabilmektedir. Yine bu standartlar sayesinde, siber güvenlik alanında kullanılabilecek yaklaşımların uygulanmasına yönelik yöntemlerin çok paydaşlı olarak geliştirilebilmesinin, küresel toplumun tüm kesimleri için hayati önem taşıyan çevresel güvenlik ve sürdürülebilirlik için önemli çabalar olduğu değerlendirilmektedir.

Sınır aşan sorunların çözümü için yoğun olarak kullanılmakta olan küresel yönetişime, çok paydaşlı yönetsel ağların yaptırım uygulama yetkilerinin ve otoritelerinin bulunmaması, meşruiyet kazanmamış olmaları, küresel yönetişim birimlerinin karmaşık yapılarından dolayı içsel çatışma ve başarısızlık olasılığının yüksek olması; yönetişimi kimin yürüteceği ve kim için yapılacağının tartışma konusu olması; bireylerin ya da kurumların bilgeliğine ya da deneyimine dayanan otoritenin zorlayıcılığı ya da yaptırım gücünün bulunmaması eleştirileri getirilmektedir.

Buna karşılık, kendilerini sadece içinde yaşadıkları devletle değil dünyanın tümüyle özdeşleştiren; insanların içinde doğdukları ya da geliştikleri topluluğa bakılmaksızın eşit ölçüde önemsenip göz önünde bulundurulmasını isteyen; çevrenin küresel seviyede korunmasının ön planda tutulmasını savunan kozmopolitler küresel yönetişim kurumlarına daha fazla inanmaktadır. Kozmopolitlere göre, küreselleşmeyi temsil eden uluslararası kuruluşlar; devletlerin bağımsız hareket etmesinin önüne geçmiş iken küresel yönetişim, tüm devletlerin, özel şirketlerin, bireylerin katılım sağlayabildiği tamamen farklı bir kavramdır. Yine bu gruba göre hakkaniyet ve adalet önemli olduğu için küresel yönetişim, dünyayı daha adil, daha iyi daha yaşanır bir yer kılmak üzere uygulanacak dayanışmacı bir yaklaşımdır.

Küresel siber güvenlik yönetişimi kapsamında, çok paydaşlı kuruluşlar ve yönetsel ağların faaliyetleri incelendiğinde, özellikle kritik altyapıların siber güvenliğine yönelik faaliyetlerin hangi devlet sınırları içinde olduğuna bakılmaksızın tüm insanların ve hatta tüm canlı ve cansız varlıkların, sürdürülebilirlik kavramına uygun olarak mevcudiyetlerinin devam ettirilebilmesi için gerçekleştirildiği anlaşılmaktadır. Siber güvenlik bağlamında çevrenin küresel seviyede korunması temel hedef olduğundan dolayı, sınır aşan siber güvenlik sorunlarının çözümünde, BT alanında gelişmiş devletlerin, standartları hazırlayan çok paydaşlı uluslararası kuruluşların, yönetsel ağların ve çok uluslu şirketlerin getirdikleri çözüm önerilerine uyulmasının küresel seviyede fayda sağlayacağı düşünülmektedir. Tüm canlı ve cansız varlıklar için hakkaniyet ve adaletin önemli olduğundan hareketle, siber güvenlik yönetişimi faaliyetlerinin de kozmopolitanizm kavramına uygun olarak gerçekleştirilmesinin sürdürülebilirlik açısından önemli faydalar sağlayacağı değerlendirilmektedir.

KAYNAKLAR

ACM,(2018), **ACM Code of Ethics and Professional Conduc**t

https://www.acm.org/code-of-ethics (Erişim Tarihi: 19 Mayıs 2022).

Adams, S.A.,Silva, K. ,Koops, B.J., ., (2019), "The Regulation of Botnets", **Rewired: Cybersecurity Governance**, First Edition. Edited by Ryan Ellis and Vivek Mohan. 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc., s:117-136).

Akkoç, Y.S.(2014), **Kentsel Dönüşüm Projelerinin Çevre Etiği Bağlamında Değerlendirilmesi**, Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Mart 2014, Ankara.

Alcântara, B.T.(2018), **SCO and Cybersecurity: Eastern Security Vision for Cyberspace, International Relations and Diplomacy**, October 2018, Vol. 6, No. 10, 549-555 doi: 10.17265/2328-2134/2018.10.003

https://www.researchgate.net/publication/330732964_SCO_and_Cybersecurity_Eastern_Security_Vision_for_Cyberspace (Erişim Tarihi: 14 Temmuz 2020).

Alcaraz, C.,Lopez, J, Zhou, J., Roman, R.(2015),"Secure SCADA Framework for the Protection of Energy Control Systems", **Concurrency and Computation Practise** &Experience, vol. 23, pp. 1414-1430,2015.

Alexander, R.D., Panguluri, S. (2017), "Cybersecurity Terminology and Frameworks", s:19-47, **Cyber Physical Security Protecting Critical Infrastructure at the State and Local Level**, Ed. Robert M. Clark, Simon Hakim, 2017, Springer-Switzerland, s:19-47.

Anderson, B.G., & Michelle L. B.(2012), 'Lights Out: Impact of the August 2003 Power Outage on Mortality in New York, NY.' **Epidemiology** 23 (2): 189–193. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3276729 (Erişim Tarihi: 20 Eylül 2017)

Altınsoy, S.Ö.(2008),**Siber Güvenlik Yönetimi ve Türkiye**, Türkiye ve Ortadoğu Amme İdaresi Enstitüsü Kamu Yönetimi Yüksek Lisans Programı, Yüksek Lisans Tezi, Ankara.

AMI, (2008), **System Security Requirements. V1.01,** Advanced Metering Infrastructure Security Task Force (AMI-SEC). 2008.

ANSI/ISA-TR99.00.01-2007 **Security Technologies for Industrial Automation and Control Systems** Copyright 2007

https://www.isa.org/products/ansi-isa-tr99-00-01-2007-security-technologies-for

(Erişim Tarihi: 15 Eylül 2022).

ANSI/ISA-62443-3-3 (99.03.03),(2013), **Security for Industrial Automation and Control Systems – Part 3-3**: System Security Requirements and Security Levels. Research Triangle Park, NC: ISA (International Society of Automation).

Arcesati, R.(2020), "**The Digital Silk Road is a development issue**", Merics, Short Analysis, Apr 28,2020

https://merics.org/en/short-analysis/digital-silk-road-development-issue

Aristoteles, **Nikomakhos'a Etik**, Çev. Furkan Akderin, Say Yayınları, 2. Baskı, İstanbul, 2015.

Azari, R., 2003, **Current Security Management & Ethical Issues of Information Technology**, IRM Press, Hershey.

Barami, B.,(2013), **Infrastructure Resiliency: A Risk-Based Framework**, draft White paper,

Infrastructure Resiliency: A Risk-Based Framework (dot.gov) (Erişim Tarihi: 22 Kasım 2021.

Bauman, Zygmunt, 1988, **Postmodern Etik**, Çev. Alev Türker, Üçüncü Basım:2016, Ayrıntı Yayınları, İstanbul.

Bayuk,J.L., Healey, J., Rohmeyer, P., Sachs, Marcus H., Schmidt, J., Weiss, Joseph(2012), **Cyber Security Policy Guidebook**, Wiley, 2012, New Jersey.

Beck, Ulrich, 2011, **Risk Toplumu**, Çev. Kazım Özdoğan, Bülent Doğan, 1. Baskı, Kasım 2011, İthaki Yayınları, İstanbul.

Belous, Saladukha, (2020),**Viruses,Hardware and Software Trojans**,Springer Nature Switzerland AG 2020

https://doi.org/10.1007/978-3-030-47218-4

Bennett, B.T., (2007), **Understanding, Assesing, and Responding to Terrorism**, Wiley&Sons, 2007, First Edition, New Jersey.

Bennett, B.T., (2018), **Understanding, Assesing, and Responding to Terrorism**, Wiley&Sons, 2018, Second Edition, New Jersey.

Berry,T.,(1999), **The Great Work:Our Way Into the Future**,New York:Bell Tower,1999.

Billo, Charles G. and Chang, Welton (2004**). Cyber Warfare An Analysıs Of The Means And Motıvatıons Of Selected Nation States.** ABD: Instıtute For Securıty Technology Studies At Dartmouth College.

Bingöl,Ö.(2016), *Yeni Güvenlik Yaklaşımları ve 21. Yüzyıl Güvenlik Sorunları*, **Uluslararası Güvenlik "Yeni Politikalar, Stratejiler ve Yaklaşımlar,** Ed. Prof.Dr. Hasret Çomak, Doç.Dr. Caner Sancaktar, Doç. Dr. Sertif Demir, İstanbul, 2016, Beta Basım, İstanbul, s:17-44.

Bisson, D., (2016), "**Black Energy Malware Caused Ukranian Power Outage, Confirms Researchers**", 5 Jan 2016, http://www.tripwire.com/state-of-security/latest-security-news/blackenergy-malware-thought-to-have-caused-ukrainian-power-outage/ (Erişim Tarihi: 27 Haziran 2016.

BMKP Raporu-1999, (2014), "Küresel Eşitsizlik Biçimleri", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ali Serkan Mercan, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 502-509.

Bookchin, M. (1994), **Özgürlüğün Ekolojisi: Hiyerarsinin Ortaya Çıkısı ve Çözülüşü**, Çev.Alev Türker, İstanbul:Ayrıntı Yayınları.

Bookchin, M. (1996), **Ekolojik Bir Topluma Doğru**, Çev.Abdullah Yılmaz, İstanbul: Ayrıntı Yayınları.

Bookchin M. (2014). **Toplumsal Ekolojinin Felsefesi: Diyalektik Doğalcılık Uzerine**. Çev. R.G. ÖĞDÜL, İstanbul:Sümer Yayınları

Bozlağan, R., (2010), SÜRDÜRÜLEBİLİR GELİŞME DÜŞÜNCESİNİN TARİHSEL ARKA PLANI . **Journal of Social Policy Conferences** , 0 (50) , 1011-1028 . Retrieved from https://dergipark.org.tr/tr/pub/iusskd/issue/891/9943

Bridges, A., (2013), "Industrial Control Systems: The Human Threat", **Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection**, Editors: Christopher Laing , Atta Badii, Paul Vickers, 2013, IGI Global, s:82-104.

Brown, Casey, "Emergent Sustainability:The Concept of Sustainable Development in a Complex World", **Globalization and Environment Changes**, Editors: Hans Günter Brauch, Ursula Oswald Spring, Czeslaw Mesjasz, John Grin, Pal Dunay, Navnita Chadha Behera, Bechir Chourou, Patricia Kameri,P.H.Liotta, Springer Berlin Heidelberg, 2008, s:141-149.

Brown, P.G.,Schmidt, J.J.,(2014), "İnsan Çağında (Antroposen) Yaşamak:Her Zamanki Gibi Yaşamak mı, Şefkatli Bir Geri Çekiliş mi", **Worldwatch Enstitüsü Dünyanın Durumu 2014 Sürdürülebilirlik için Yönetişim**, Ed. Lisa Mastny, Çev. Gülru Hotinli, Worldwatch Institute, Türkiye İş Bankası Kültür Yayınları I. Basım: Aralık 2014, İstanbul, s: 85-96.

Brundage M, Avin S, Clark J ve diğerleri (2018), **The malicious use of artificial intelligence: forecasting, prevention, and mitigation**. ArXiv:1802.07228. http://arxiv.org/abs/1802.07228 (Son Erişim Tarihi 1 Haziran 2020)

Burley, D., Bishop, M., Kaza, S., Gibson, D., Hawthorne, E., and Buck, Scott. 2017. "ACM Joint Task Force on Cybersecurity Education." SIGCSE '17 **Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education**. March 8– 11, 2017. ACM: Seattle, Washington.

Buzan, B., Wæver O., and Jaap de Wilde,(1998), **Security: A New Framework for Analysis.** Boulder,Colorado: Lynne Rienner.1998, s. 208.

Cantzen, Rolf,(2015), **Daha Az Devlet Daha Çok Toplum**, Çev. Veysel Atayman, Ayrıntı Yayınları, 3. Baskı, İstanbul, 2015.

Castells,M., (2014), "Küresel Enformasyon Kapitalizmi?", Küresel Dönüşümler-**The Global Transformations**, Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ezgi Sarıtaş, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 367-388.

Cavelty, Myriam Dunn, (2008), **Cyber Security and Threat Politics**, Routledge, 2008, New York.

CCDCOE https://ccdcoe.org/about-us/ (Erişim Tarihi :5 Kasım 2022)

Cavelty, Myriam Dunn, (2010), **The Reality and Future of Cyberwar**, Parliamentary Brief. ,

Cevizci, Ahmet,(2014), **Etik-Ahlak Felsefesi**, Say Yayınları, 1. Baskı, 2014.

Chatfield, Tom, 2012, **Digital Çağa Nasıl Uyum Sağlarız**, Çev. Levent Konca, Ocak 2013, Sel Yayıncılık.

Chien, Eric, "**Stuxnet: A Breakthrough**", 12 Nv 2010, Symantec Official Blog, http://www.symantec.com/connect/blogs/stuxnet-breakthrough Erişim Tarihi: 4 Temmuz 2016.

CIS-1 (Center for Internet Security), **CIS Controls, Implementation Guide for Industrial Control Systems,** v7, Ed. Ramsey Williams, Adam Boeckman.

https://www.cisecurity.org/insights/white-papers/cis-controls-implementation-guide-for-industrial-control-systems (Erişim Tarihi:20 Kasım 2022).

CIS-2, ”**About Us**”, https://www.cisecurity.org/about-us (Erişim Tarihi:20 Kasım 2022)

Clark,I.,(2014), ”Güvenlik Devleti”, **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ali Rıza Güngen, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 215-228.

Clark, R.M., Hakim, S. (2017), “*Protecting Critical Infrastructure at the State, Provincial and Local Level: Issues in Cyber-Physical Security*”, **Cyber Physical Security Protecting Critical Infrastructure at the State and Local Level**, Ed. Robert M. Clark, Simon Hakim, 2017, Springer-Switzerland, s:1-17.

Clarke, R. A., Knake, Robert K. (2010). ***Cyber War-The Next Threat to National Security and What to Do About It,*** New York: Harper Collins Publishers.

Cohen, Fred, (2015), “Protecting and Engineering Design Issues in Critical Infrastructures”, **Cybersecurity**, Ed. Thomas A. Johnson, 2015, CRC Press, New York, s:67-154.

Curi, K. (2009), “Meslek Etiklerinde Yeni Bir Boyut: Çevre Etiği”, **Etik ve Meslek Etikleri,** Yay.Haz. Harun Tepe, TFK, İkinci Baskı, 2009, Ankara, s: 83-89.

Izuakor, C., (2021), What We Can Learn From The Most Alarming 2021 **Breaches So Far**”

https://www.cyberpopup.com/post/what-we-can-learn-from-the-most-alarming-2021-breaches-so-far?

Çifci, H., (2013), **Her Yönüyle Siber Savaş**, Tübitak, Ankara.

Çobanoğlu, N., (2009), **Kuramsal ve Uygulamalı Tıp Etiği**, Eflatun Yayınevi, 2009, Ankara.

Demiröz,Ö.,(2018), “*A Pragmatic and Structured Method to Secure the Systems That Control the Nuclear Environment* “, **Cyber Security Policies And Critical Infrastructure Protection**, Ed. Guido GLUSCHKE, Prof. Dr. Mesut Hakkı CAŞIN, Marco MACORI 2018, Institute for Security and Safety GmbH, Germany, s:341-370.

Denning, D., (2003), *Cyber Security As Emergent Infrastructure,* **Security Education and Critical Infrastructures,** Ed. Irvine, Cynthia, Armstrong, Helen, 2003, Springer, New York, s: 1-2.

Des Jardins, J. R., (2006), **Çevre Etiği Çevre Felsefesine Giriş**, Çev. Ruşen Keleş, İmge Yayınevi, Ankara, 2006.

DOE-USA, (2002), "**21 Steps To Improve Cyber Security of SCADA Networks**" https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (Erişim Tarihi:3 Mayıs 2022).

Easterling, K., (2014), **Devlet Dışı Güç, Altyapı Mekanı ve İktidar**, Çev. Şahika Tokel, İlk Basım Nisan 2017, Metis Yayınları, İstanbul.

Eggenschwiler,J.(2019), "*An Incident-Based Conceptualization of Cybersecurity Governance*", **Rewired: Cybersecurity Governance**, First Edition. Edited by Ryan Ellis and Vivek Mohan. © 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc., s:81-96.

ENISA (2012), **National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace**. https://www.enisa.europa.eu/publications/cyber-security-strategies-paper (Erişim Tarihi: 5 Aralık 2021)

Erbil, A. Ö. & İdemen, B. (2010), "*Planlama ve Çevre Etiği: Uygulamalı Disiplinlerde Çevre Etiği*", **Planlama**, 2010/2, s. 3- 13.

Ergün, T.,(2008), "Yönetişim", Kamu Yönetimi Sözlüğü, Ed.Seriye Sezen, TODAİE, İkinci Baskı, Ankara, 2008.

Ergün, T. ve Çobanoğlu, N. (2012) Sürdürülebilir Kalkınma ve Çevre Etiği. Ankyra: **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, *2012, 3(1) DOI: 10.1501/sbeder_0000000041*

Ermiş,U. (2014), *Siber Güvenliğin Sağlanmasında Kritik Altyapıların Korunmasının Önemi*, **Uludağ Uluslararası İlişkiler Kongresi Konferans Bildirisi**,2014, Bursa.

Ertan, K.A. (1998), "Çevre Etiği", **Amme İdaresi Dergisi**, Cilt 31, Sayı 1, s.125-139.

Ertürk, H.,(2009), **Çevre Bilimleri**, 3. Baskı, Mart 2009, Ekin Yayınevi, Bursa.

Esterle, A.,Ranck, H., Schmitt,B.,(2005), **Information Security A New Challange For The EU**, Institute For Security Studies, Paris.

EU,(2018), ,"European Programme for Critical Infrastructure Protection" **Summaries of EU Legislation,** http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/133260_en.htm, (Erişim Tarihi: 8 Haziran 2018)

Farooq-i-Azam, M., Ayyaz, M., 2012, *Embedded Systems Security*, **Cyber Security Standards, Practices and Industrial Applications**, Ed. Zubairi, J. Ahmed, Mahboob, Athar, 2012, IGI Global. s: 179-198.

ESCSWG, (2011), **Roadmap to Achive Energy Delivery Systems Cybersecurity**, September 2011. http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf (Erişim Tarihi: 27 Şubat 2018).

Flaus, J.M., (2019), **Cybersecurity of Industrial Systems**, First Edition, ISTE Ltd and John Wiley&Sons, Inc.

Friedman, T.,(1999), **Küreselleşmenin Geleceği**, Çev. Elif Özsayar, Boyner Holding Yayınları, İstanbul, 1999, s: 30-33.

Friedman, T., (2000), **Lexus ve Zeytin Ağacı**, New York, New York.

Gartzke,E.,(2013),"The Myth of Cyberwar:Bringing War in Cyberspace Back Down to Earth",**International Security** 38/2 2013:41-73.

https://watermark.silverchair.com/isec (Erişim Tarihi:2 Kasım 2021).

Gaycken S. and Martellini M., (2013) "*Cyber as deterrent*", Ed. Maurizio Martellini, **Cyber security, deterrence and IT protection for critical Infrastructures**, Springer, London, 2013, 1-10.

Geers, K, (2015), "*Coder, Hacker, Soldier, Spy*", **Cyber Security:Analytics, Technology and Automation**, Ed. Martti Lehto, Pekka Neittaanmaki, 2015, Springer Switzerland, 2015, s:73-87.

Gelbstein, E., Kamal, A.,(2002), **Information Insecurity A Survival Guide To The Uncharted Territories Of Cyber Threats And Cyber Security**, UN ICT Task Force,UNITAVAR,NY 100017, Second Edition.

Gowdy, J.M, (2014), "*Yönetişim, Sürdürülebilirlik ve Evrim*", **Worldwatch Enstitüsü Dünyanın Durumu 2014 Sürdürülebilirlik için Yönetişim**, Ed. Lisa Mastny, Çev. Gülru Hotinli, Worldwatch Institute, Türkiye İş Bankası Kültür Yayınları I. Basım: Aralık 2014, İstanbul, s: 41-70.

Gruhl, H., (1978) **Ein Planet wird geplündert**, Frankfurt.

Hahn, A.,(2016), *Operational Technology and Information Technology in Industrial Control Systems*, **Cyber-security of SCADA and Other Industrial Control Systems**, Ed. Edward J.M. Colbert, Alexander Kott, Springer, 2016, s:51-68.

Halliday, F.,(2014), "Küresel Yönetişim: Beklentiler ve Sorunlar", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ezgi Sarıtaş, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 578-590.

Han.A., Çelikpala, M., (2016), *Uluslararası Çerçevede Siber Güvenlik ve Nükleer Enerji*, **EDAM Türkiyede Siber Güvenlik ve Enerji** /74, 5 Nisan 2016 , s:75-99.

Harp, D., Gregory-Brown,B.,(2015), **The State of Security in Control Systems Today,** SANS, SANS Institute Infosec Reading Room, June 2015. https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042 Erişim Tarihi: 28 Temmuz 2016.

Hathaway,M.E., Klimburg, A.,(2012), Preliminary Considerations: On National Cyber Security, **NATIONAL CYBER SECURITY FRAMEWORK MANUAL**, Ed. Alexander Klimburg, 2012 by NATO Cooperative Cyber Klimburg Defence Centre of Excellence, NATO CCD COE Publications Tallinn, Estonia, s: 1-43.

Held, D.,(2006), "Reframing Global Governance:Apocaliypse Soon or Reform!", **New Political Economy,**11,2:157-76.

Held, D.,(2014-1), "Uluslararası Hukukun Değişen Yapısı:Egemenlik Dönüştü mü?", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ezgi Sarıtaş, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 609-627.

Held, D.(2014-2), "*Kozmopolitanizm:Küreselleşmeyi Evcilleştirmek*", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ali Rıza Güngen, Eray Sarıot, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 269-281.

Held D., McGrew, A.,(2014), "*Büyük Küreselleşme Tartışması*", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ali Serkan Mercan, Eray Sarıot, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 7-70.

Hemsley, K.E., Fisher, Dr. Ronald E., (2018), **History of Industrial Control System Cyber Incidents,** December 2018, Idaho National Laboratory Idaho Falls, Idaho 83415, INL/CON-18-44411-Revision-2

Henrie, M., (2012), Cyber Security in Liquid Petroleum Pipelines, **Cyber Security Standards, Practices and Industrial Applications,** Ed. Zubairi, J. Ahmed, Mahboob, Athar, 2012, IGI Global. S: 200-222.

Herr, T.,(2019), "Governing Risk", **Rewired: Cybersecurity Governance**, First Edition. Edited by Ryan Ellis and Vivek Mohan. © 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc., s:137-157).

Herrman, D., Pridöhl,H., (2020), "Basic Concepts and Models of Cybersecurity", **The Ethics of Cybersecurity**, Ed. Markus Christen, Bert Gordijn, Michele Loi, The İnternational Library of Ethics, Law and Technology 21, Springer Open, s:10-44.

Hessel, Stephan, 2011, **Kayıtsız Kalmayın Mücadeleye Devam**, Cumhuriyet Kitapları, Kasım 2011.

Hoffman, G.M.,(2008), *Ethical Challenges for Information Systems Professionals*, **Information Security and Ethics:Concepts, Methodologies, Tools, and Applications**, Ed. Hamid Nemati, IGI Global, Hershey, s:191-199.

Hoffman, S.,(2014), "Küreselleşmelerin Çarpışması", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Mehmet Celil Çelebi, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara, sayfa:133-139.

Hutchinson,W., (2015), "Deception in The Cyber World", **Cyber Security:Analytics, Technology and Automation**, Ed. Martti Lehto, Pekka Neittaanmaki, 2015, Springer Switzerland, 2015, s:101-107.

IBM,(2014),"**IBM Security Services 2014 Cyber Security Intelligence Index**" https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF (Erişim tarihi:28 Ekim 2021.

Inversini, R.,(2020), "Cyber Peace: And How It Can Be Achieved", **The Ethics of Cybersecurity**,Ed. Markus Christen, Bert Gordijn, Michele Loi, The İnternational Library of Ethics, Law and Technology 21, Springer Open, s:347-360.

Irion, K.,(2013), *The Governance of Network and Information Security in The European Union:The Euroean Public-Private Partnership for Resilliance(EP3R)*, **The Secure Information Society-Ethical, Legal and Political Challenges**, Ed. Krüger,Jörg., Nickolay, Bertram., Gaycken, Sandro., 2013,, Springer-Verlag, London 2013, s:17-53.

ISA, International Society of Automation, "**About ISA**"

https://www.isa.org/about-isa (Erişim Tarihi: 12 Ağustos 2022).

ISA-62443-1-1-2007,(2007), ***Security for Industrial Automation and Control Systems Part 1-1***: Terminology, Concepts, and Models,2007. https://www.isa.org/products/isa-62443-1-1-2007-security-for-industrial-automat (Erişim Tarihi: 12 Ağustos 2022).

ISA-62443-2-1-2009, (2009), ISA-62443-2-1-2009, **Security for Industrial Automation and Control Systems Part 2-1**: Establishing an Industrial Automation and Control Systems Security Program https://www.isa.org/products/isa-62443-2-1-2009-security-for-industrial-automat (Erişim Tarihi: 12 Ağustos 2022).

ISA-TR62443-2-3-2015, (2015), **Security for industrial automation and control systems, Part 2-3**: Patch management in the IACS environment https://www.isa.org/products/ansi-isa-tr62443-2-3-2015-security-for-industrial (Erişim Tarihi: 12 Ağustos 2022).

ANSI/ISA-62443-3-2-2020, (2020), **Security for industrial automation and control systems, Part 3-2:** Security risk assessment for system design https://www.isa.org/products/ansi-isa-62443-3-2-2020-security-for-industrial-a (Erişim Tarihi: 12 Ağustos 2022).

ANSI/ISA-62443-4-1-2018, **Security for industrial automation and control systems, Part 4-1**: Secure product development lifecycle requirements

ITU, "**About International Telecommunication Union** (ITU)" https://www.itu.int/en/about/Pages/default.aspx. (Erişim tarihi:20 Kasım 2022)

ITU-T (International Telecomunication Unit), (2008), **Overview of Cybersecurity**, ITU-T, X.1205,x.1205, (04/2008).

ITU, (2021), Strategic Engagement in Cybersecurity, **Guide to Developing a National Cybersecurity** Strategy, 2nd Edition 2021, Geneva 20, Switzerland. https://ncsguide.org/ (Erişim Tarihi: 13 Şubat 2022).

IULA-EMME, (1997), **Yerel Gündem 21**, Türkiye'de Yerel Gündem 21'lerin Teşviki ve Gelitirilmesi Projesi Bülteni, S. 1, İstanbul, Kasım 1997.

Jiow,H.J. (2017), "Efforts to Get People Involved in Cyber-Physical Security: Case Studies of Australia and Singapore", s:1-17, **Cyber Physical Security Protecting Critical Infrastructure at the State and Local Level**, Ed. Robert M. Clark, Simon Hakim, 2017, Springer-Switzerland, s:221-232.

Johnsen,S.O., Skramstad, T., Hagen, J.,(2009),"Enhancıng The Safety, Securıty And Resilience of Ict And Scada Systems Using Action Research**", Critical Infrastructure Protection III,** Ed. C. Palmer and S. Shenoi,, IFIP AICT 311,. c IFIP International Federation for Information Processing 2009. s. 113–123, 2009.

Johnsen,S.O., (2013), "Safety and Security in SCADA Systems Must be Improved Through Resilience Based Risk Management", **Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection,** Editors: Christopher Laing , Atta Badii, Paul Vickers, 2013, IGI Global, s:286-300.

Kara, M.,Çelikkol,S.,(2011), "**Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği",** Kasım 2011,

https://www.researchgate.net/publication/279659520_4_Ag_ve_Bilgi_Guvenligi_Sempozyumu_Kritik_Altyapilar_Elektrik_Uretim_ve_Dagitim_Sistemleri_SCADA_Guvenligi (Erişim Tarihi: 25 Eylül 2018).

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

Karakuş, C. ***Kritik Alt Yapılara Siber Saldırı***. https://silo.tips/download/krtk-alt-yapilara-sber-saldiri (Erişim Tarihi: 28 Şubat 2019).

Kastelic, A., (2021**), International Cooperation to Mitigate Cyber Operations Against Critical Infrastructure, Normative Expectations and Emerging Good Practices**, UNIDIR. https://unidir.org/publication/international-cooperation-mitigate-cyber-operations-against-critical-infrastructure (Erişim Tarihi:5 Mayıs 2022).

Keidanren, (2016)**Toward Realization Of The New Economy And Society**, 19 April, 2016, http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf (Erişim tarihi: 15 Temmuz 2018

Keleş, R., Ertan, B. (2002), **Çevre Hukukuna Giriş**, Ankara: İmge.

Keleş,R, Hamamcı, C., (1993), **Çevrebilim**, 4. Baskı, Ağustos 2002, İmge Kitapevi, Ankara.

Keleş,R, Hamamcı, C, Çoban, A., 2009, **Çevre Politikası,** 6. Baskı, Ekim 2009, İmge Kitapevi, Ankara.

Keohane,R.O., (2014), "Uluslararası Toplumda Egemenlik", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Mehmet Cemil Boyraz, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara, sayfa:178-195.

Keohane,R.O., Nye Jr.,J.,(2014), "Küreselleşme:Yeni Olan Ne,?Olmayan Ne?", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Mehmet Celil Çelebi, Eray Sarıot, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara, sayfa:97-115.

Kizza, J. M.,(2007), **Ethical and Social Issues in The Information Age**, Editors: David Gries, Fred B. Schneider, Third Edition, 2007, Springer-Verlag London.

Kizza, J. M., (2014), **Computer Network Security and Cyber Ethics**, Forth Edition, 2014, McFarland&Company, Inc Publishers, Jeferson, North Carolina.

Klimburg,A., Healey,J.,(2012), Stratejic Goals&Stakeholders, **National Cyber Security Framework Manual**, Ed. Alexander Klimburg, 2012 by NATO Cooperative

Cyber Defence Centre of Excellence, NATO CCD COE Publications Tallinn, Estonia, s: 66-107.

Klinke, A., & Renn, O. (2002). **A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies**. Risk Analysis , 1071 - 1094.

Kott, A,Gonzales, C.A., Colbert, J.M.,(2016), Introduction and Preview, **Cyber-security of SCADA and Other Industrial Control Systems**, Ed. Edward J.M. Colbert, Alexander Kott, Springer, 2016, s:1-14.

Krasavin, S., **What is Cyber Terrorism**?,

http://www.crime-research.org/library/Cyber- terrorism. htm (erişim tarihi 4.11.2012).

Krasner, S. A., (1983) **İnternational regimes**. Ithaca:Cornel University Press

Krotofil, M., Cardenas, A., and Angrishi, K., (2014), "Timing of Cyber-Physical Attacks on Process Control Systems", **Critical Infrastructure Protection VIII, 8th IFIP WG 11.10 International Conference**, ICCIP 2014 Arlington, VA, USA, March 17-19, 2014 Revised Selected Papers, Ed. Onathan Butts,, Sujeet Shenoi, Springer, IFIP 2014.

Krüger,J., Nickolay, B., Gaycken, S., (2013), **The Secure Information Society-Ethical, Legaland Political Challenges,** Springer-Verlag, London.

Krutz, Ronald L., (2006), **Securing SCADA Systems**, Wiley Publishing, İndianapolis.

Krutz, Ronald L., (2017**), Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure Second Edition**, Ed. Chloe Tuck, Liegh Elrod, and Susan Colwell, International Society of Automation (ISA).

Kuçuradi, İ.,(2009), "Felsefi Etik ve Meslek Etikleri", sayfa: 27-43, **Etik ve Meslek Etikleri,** Türkiye Felsefe Kurumu, Yay. Haz. Harun Tepe, İkinci Baskı, 2009 Ankara.

Kumar, K., (1995), **Sanayi Sonrası Toplumdan Post-Modern Topluma Çağdaş Dünyanın Yeni Kuramları**, Çev. Mehmet Küçük, Dost Kitabevi, Üçüncü Baskı, Ağustos 2010, Ankara.

Kuusisto,T,Kuusisto,R.,(2015), "Cyberworld as a Social System", **Cyber Security:Analytics, Technology and Automation**, Ed. Martti Lehto, Pekka Neittaanmaki, 2015, Springer Switzerland, 2015, s:31-43.

Küçükşahin, Şafak, Dedeoğlu, (2009), "Güvenlik Bağlamında Risk ve Risk Yönetimi", **Güvenlik Stratejileri Dergisi**, Aralık 2009, s:9-34.

https://www.msu.edu.tr/GuvenlikStratejileriDergisi/dokuman/GSD_10/GSD_10_Art_1_122009.pdf (Erişim tarihi 25 nisan 2020).

Leclair, Jane, Burns, Scott,(2018), "A Pragmatic and Structured Method to Secure the Systems That Control the Nuclear Environment ", **Cyber Security Policies And Critical Infrastructure Protection**, Ed. Guido GLUSCHKE, Prof. Dr. Mesut Hakkı CAŞIN, Marco MACORI 2018, s:70-76.

Lehto, M., (2015), "Phenomena in The Cyber World", **Cyber Security:Analytics, Technology and Automation**, Ed. Martti Lehto, Pekka Neittaanmaki, 2015, Springer Switzerland, 2015, s:3-29.

Lewis, T. G.,(2015), **Critical Infrastructure Protection in Homeland Security**,Wiley, Second Edition, 2015, New jersey.

Libicki, M. C. (2009). **Cyberdeterrence and Cyberwar**. USA: RAND Corporation.

Lin, H., (2013), *Laying an Intellectuel Foundation for Cyberdeterrence:Some Initial Steps*, **The Secure Information Society-Ethical, Legal and Political Challenges**, Ed. Krüger,Jörg., Nickolay, Bertram., Gaycken, Sandro., 2013, Springer-Verlag, London 2013, s:17-53.

Lindstrom,G.,Luiijf E.,(2012), Political Aims & Policy Methods, **NATIONAL CYBER SECURITY FRAMEWORK MANUAL**, Ed. Alexander Klimburg, 2012 by NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publications Tallinn, Estonia, s:44-65.

Luallen, M.,(2014), **Breaches on the Rise in Control Systems: A SANS Survey**, SANS Institute, https://www.qualys.com/docs/sans-survey-breaches-rise-control-systems.pdf (Erişim Tarihi: 20 Aralık 2021).

Luiijf, E., Healey,J.,(2012), Organisational Structures & Considerations , **NATIONAL CYBER SECURITY FRAMEWORK MANUAL**, Ed. Alexander Klimburg, 2012 by NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publications Tallinn, Estonia, s: 108-140.

Lukszo, Z.,Deconinck, G., Weijnen M., (2010), **Securing Electricity Supply in the Cyber Age**, 2010, Springer.

Macaulay, T., (2009), **Critical Infrastructure**, CRC Press, Boca Raton.

Macaulay, T., Singer, B., (2011), **Cybersecurity for Industrial Control Systems**, CRC Press, New York.

Maglaras LA, Kim K, Janicke H., Ferrag M.A., Rallis, S.,Fragkou, P.,Maglaras, A.,Cruz, T., (2018), **Cyber security of critical infrastructures**. ICT Express 4(1) sayfa:42–45. https://doi.org/10.1016/j.icte.2018.02.001 (Erişim Tarihi: 12 Eylül 2021).

Manjikian, M., (2018), **Cybersecurity Ethics An Introduction**, Routledge Taylor &Francis Group London and New York, 2018, New York.

Mann,M.,(2014), "Küreselleşme Ulus Devletin Yükselişine Son mu Verdi?", **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Cemil Boyraz, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara, sayfa:164-177.

Mansbach, R.W., Taylor, K.L.,(2018), **Introduction To Global Politics**, Third Edition, Routledge, Taylor &Francis Group London and New York.

Meadows, Donella H. ve d. (1973), **Limits to Growth**: (A Report for the Club of Rome's Project on the Predicament of Mankind), Twelfth Edition, Universe Books, New York, August.

Mengi, A. (2012), "Çevre Etiği", **Kentsel Planlama: Ansiklopedik Sözlük,** Der: M. Ersoy, s.68-71, Ankara: Ninova.

Meyer, P.,(2020), "Norms of Responsible State Behaviour in Cyberspace", **The Ethics of Cybersecurity**,Ed. Markus Christen, Bert Gordijn, Michele Loi, The İnternational Library of Ethics, Law and Technology 21, Springer Open, s:347-360.

Meral, M. (2015),**Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi**, Harp Akademileri Stratejik Araştırmalar Enstitüsü, Savunma Kaynakları Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul.

Merlo, C.,(2017), "**How an Entire Nation Became Russia's Test Lab for Cyberwar**", Wired, June 20,2017, www.wired.com/story7russian-hackers-attack-ukraine (Erişim tarihi: 7 Ağustos 2021

Merriam-webster **çevrimiçi sözlük**,(2021) https://www.merriam-webster.com/dictionary/cyber (Erişim tarihi : 4 Mayıs 2021.

Mulligan D K ve Schneıder, F B (2011). **Doctrine for Cybersecurity**. *Dædalus, Journal of the* American Academy of Arts and Sciences. 140 (4), 70-92.

Miller, B., Rowe, D., (2012), "**A Survey SCADA of and Critical Infrastructure Incidents**", Proceedings of the 1st Annual conference on Research in information technology, s:51-56, ACM New York, NY, USA, 2012. http://docplayer.net/2789900-A-survey-of-scada-and-critical-infrastructure-incidents.html (Erişim Tarihi: 13 Haziran 2016).

Misbahuddin, S., Al-holou, N., (2012), *Fault Tolerant Remote Terminal Units (RTUs) in SCADA Systems*, **Cyber Security Standards, Practices and Industrial Applications,** Ed. Zubairi, J. Ahmed, Mahboob, Athar, 2012, IGI Global. s: 168-178.

Naess, A., (1994),"Derin Ekolojinin Temelleri", **Derin Ekoloji**, Der. Günseli Tamkoç, İzmir Ege Yayınları,1994.

National Science Foundation. (2017). "**Cyber-Physical Systems," grant solicitation,** https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286&org=CISE&sel_org=CISE&from=fund (Erişim Tarihi: 24 Ocak 2020).

Nemati, H.,(2008), **Information Security and Ethics: Concepts, Methodoligies, Tools, and Applications, Volume 1**, Information Science Reference, 2008, Editor-in-Chief Mehdi Khroshow-Pour.

Nicholson, A., Webber, S., Dyer, S., Patel, T., (2012), **SCADA Security in The Light of Cyber-Warfare** Computers & Security, Volume 31, Issue 4, Mar. 2012, s:418-436.

NIST (2011), SP 800-39 **Managing Information Security Risk: Organization, Mission, and Information System View**. Washington, DC: NIST (National Institute of Standards and Technology), 2011.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST, (2013), SP 800-53 r4, **Recommended Security Controls for Federal Information Systems. Special Publication** 800-53 Revision 4. Washington, DC: NIST (National Institute of Standards and Technology), 2013.

NIST, (2014), **Framework for Improving Critical Infrastructure Cybersecurity** Version 1.0, February 12, 2014.

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf (Erişim Tarihi: 20 Temmuz 2021).

NIST, (2015), SP 800-82r2(2015), ***Guide to Industrial Control Systems (ICS) Security, NIST Special Publication Revision 2***, Ed. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, May 2015, Washington, DC: NIST (National Institute of Standards and Technology), 2015

NIST, (2018), **Framework for Improving Critical Infrastructure Cybersecurity** Version 1.1 April 16, 2018.

https://www.baltimorecityschools.org/sites/default/files/inline-files/NIST.CSWP_.04162018.pdf (Erişim Tarihi: 12 Temmuz 2021)

NIST SP 800-82r3 ipd, (2022), ***Guide to Operational Technology (OT) Security, Initial Public Draft, NIST Special Publication*** , Ed. Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, April 2022, U.S. Department of Commerce 51 Gina M. Raimondo, Secretary.

Norris, P.,(2014), "Küresel Yönetişim ve Kozmopolit Vatandaşlar", **Küresel Dönüşümler-The Global Transformations Reader**, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Bülent Özçelik, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 340-351.

Nye, J.(2011), "The Future of Power", **Diffusion and Cyber Power**, Ed. J.Nye, New York :Public Affairs, s: 113-151.

Oakley, J., Cocking, D., (2003), **Virtue Ethics and Professional Roles**, Cambridge.

OECD, (2019), **Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies**, OECD Publishing, Paris, https://read.oecd-ilibrary.org/governance/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en#page111 (Erişim Tarihi : 20 Ekim 2022)

Orr, D.W.,(2014), Önsöz, **Worldwatch Enstitüsü Dünyanın Durumu 2014** Sürdürülebilirlik için Yönetişim, Ed. Lisa Mastny, Çev. Gülru Hotinli, Worldwatch Institute, Türkiye İş Bankası Kültür Yayınları I. Basım: Aralık 2014, İstanbul, s: xvii-xxiv.

Önder, T. (2003), **Ekoloji, Toplum ve Siyaset**, Ankara: Odak Yayınevi.

Örs, Y., (1997), "Etik Açısından Doğal Çevremiz", **İnsan, Çevre ve Toplum**, Yayıma Haz. Ruşen Keleş, İmge Yayınevi, 2. Baski, Ağustos 1997, s: 361-371.

Özer, M., (2017), **Doğa Etiği**, İmge Kitabevi, 1. Baskı, Nisan 2017, Ankara.

Özlem, D.,(2014), **Etik Ahlak Felsefesi**, Notos Kitap, Nisan 2014, Birinci Basım, İstanbul.

Öztürk, Ö. (2014). **Digital Dark Side: Cyber Warfare**. Boston University, Metropolitan College.

Panguluri, S., Nelson, T. D., Wyman, R. P. (2017), "Creating a Cyber Security Culture for your Water/Waste Water Utility", **Cyber Physical Security Protecting Critical Infrastructure at the State and Local Level**, Ed. Robert M. Clark, Simon Hakim, 2017, Springer-Switzerland, s:133-159.

Perdikaris, J., (2014), **Physical Security and Environmental Protection**, 2014, CRC Press, Boca Raton.

Perkins,E.,2015,"**Top Cybersecurity Trends**", 2016-2017",Gartner,

http://www.gartner.com//it/content/3169000/3169018/december_3_top_cybersecurity_trends_2016_2017_eperkins.pdf?userId=55807060 Erişim Tarihi: 8 Temmuz 2016.

Perkins, E., Byrnes, F.C., (2015), "Cybersecurity Scenario '2020 Phase 2: **Guardians for Big Change**", Gartner, G00279414, 20 July 2015.

https://www.gartner.com/doc/3097027/cybersecurity-scenario--phase- (Erişim Tarihi: 9 Temmuz 2016).

Pieper, A. M., **Etiğe Giriş**, Ayrıntı Yayınları, İstanbul, 2012 (İkinci Basım).

Poulsen, K.,(2003), **Slammer Worm Crashed Ohio Nuke Plant Network**, SecurityFocus, 2003-08-19,

http://www.securityfocus.com/news/6767 (Erişim Tarihi: 24 Mayıs 2021).

Puyvelde,D.V., Brantly, A.F.,(2019), **Politics, Governance and Conflict in Cyberspace**, Politly Press, Medford,USA.

Radu, R.,(2014), 'Power Technology and Poweful Technologies:Global Governmetality and Security in the Cyberspace", **Cyberspace and International Relations**, Ed. J.-F Kremer ,B. Müller, DOI: 10.10007/978-3-642-37481-4_1,Springer-Verlag Berlin Heidelberg 2014. S:3-20.

Radvanovsky, R.,(2018), "Critical Infrastructure Security Paradigm And Modern Protection Policies", **Cyber Security Policies And Critical Infrastructure Protection**, Ed. Guido GLUSCHKE, Prof. Dr. Mesut Hakkı CAŞIN, Marco MACORI 2018, Institute for Security and Safety GmbH, Germany, s:57-68.

Rajamaki, J., (2017), "*Cyber Security Trust Building, and Trust Management: As Tools for Multiagency Cooperation within the Functions Vital To Society*", **Cyber Physical Security Protecting Critical Infrastructure at the State and Local Level**, Ed. Robert M. Clark, Simon Hakim, 2017, Springer-Switzerland, s:233-249.

Renner, M., Prugh, T.,(2014), "*Yönetişim Başarısızlığı, Sürdürülemez Gezegen*", **Worldwatch Enstitüsü Dünyanın Durumu 2014 Sürdürülebilirlik için Yönetişim,** Ed. Lisa Mastny, Çev. Gülru Hotinli, Worldwatch Institute, Türkiye İş Bankası Kültür Yayınları I. Basım: Aralık 2014, İstanbul, s: 3-25.

Resnik, D. B.,(2004), **Bilim Etiği**, Ayrıntı, İstanbul, 2004, Birinci Basım.

Robertson, J ve Riley, M.,(2014), "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era," **Bloomberg**, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar ,2014, (Erişim Tarihi: 20 Haziran 2021.)

Rosenau, J. N. (2014), ”Yeni Bir Küresel Düzende Yönetişim”, **Küresel Dönüşümler-The Global Transformations** Reader, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ali Rıza Güngen, Eray Sarıot, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 269-281.

Ruddiman, W.F., The Antropocene,(2009),”Annual Review of Earth and Planetary Sciences, cilt 41 (2013), Dipesh Chakrabarty, “**The Climate of History: For Theses,”Critical Inquiry**,cilt 35, No.2(2009), s. 197-222.

Ruivenkamp G., Jongerden, J., Öztürk, M., (2010), “Başka Bir Teknoloji ve Teknolojinin İmkanları ile Başka Bir Dünya Mümkün (mü?)”, **Teknoloji ve Toplum**, Ed. Ruivenkamp Guido, Jongerden, Joost, Öztürk, Murat, Kalkedon Yayıncılık Eylül 2010, İstanbul, s:9-21.

Sadowsky, G., Dempsey, J., Greenberg, A., Mack, B, Schwartz, A., (2003), **Information Technology Security Handbook**, infodew, Worldbank.

Sağıroğlu, Şeref, (2019), “A Pragmatic and Structured Method to Secure the Systems That Control the Nuclear Environment “, **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,** Ed. Prof.Dr.Şeref SAĞIROĞLU, Prof.Dr. Mustafa ALKAN, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Aralık 2018, Grafiker Yayınları, Ankara, s:

Sale, K.(2010), “Başka Bir Teknoloji ve Teknolojinin İmkanları ile Başka Bir Dünya Mümkün (mü?)”, **Teknoloji ve Toplum**, Ed. Ruivenkamp Guido, Jongerden, Joost, Öztürk, Murat, Kalkedon Yayıncılık Eylül 2010, İstanbul, s:199-209.

San Juan,V.,Martin,A,(2019), “Cyber Governance and the Financial Services Sector: The Role of Public–Private Partnerships”, **Rewired: Cybersecurity Governance**, First Edition. Edited by Ryan Ellis and Vivek Mohan. © 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc., s:97-115).

Schmitt, M. N., (2013), **Tallinn Manual On The Internatıonal Law Applıcable To Cyber Warfare**, ed. Michael N. Schmitt, 2013,Cambridge University Press, The Edinburgh Building, Cambridge, UK.

Schultz, R. A., (2010), **Information Technology and the Ethics of Globalization,** Information Science Referance, 2010, Hershey-Newyork.

Schwab, K., (2016), **Dördüncü Sanayi Devrimi**, Çev. Zülfü Dicleli, Optimist Yayın, Eylül 2016, İstanbul.

Scholte, J.A. Keohane,R.O.,(2014), ”Küreselleşmede Küresel Olan Ne?”, **Küresel Dönüşümler-The Global Transformations Reader**, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Mehmet Celil Çelebi, Eray Sarıot, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara, sayfa:107-115.

Scholte,J.A.(2011). "Global Governance, Accountability and Civil Society", Ed. J.A. Scholte, **Building Global Democracy? Civil Society and Accountable Global Governance** , Cambridge:Cambridge University Press.

Sevim, C., (2009),"Geçmişten Günümüze Enerji Güvenliği ve Paradigma Değişimleri", **Stratejik Araştırmalar Dergisi,** S. 13, Mayıs 2009. s. 93.

Seyle, D.C., King,M.W.,(2014), "Yönetişimi Anlamak", **Worldwatch Enstitüsü Dünyanın Durumu 2014 Sürdürülebilirlik için Yönetişim**, Ed. Lisa Mastny, Çev. Gülru Hotinli, Worldwatch Institute, Türkiye İş Bankası Kültür Yayınları I. Basım: Aralık 2014, İstanbul, s: 27-37.

Sharma, A., (2010). *Cyber Wars: A Paradigm Shift from Means to Ends*. **Strategic Analysis**, 34 (1), 62-73.

Shires, J., (2019), "Cybersecurity Governance in the GCC", **Rewired: Cybersecurity Governance**, First Edition. Edited by Ryan Ellis and Vivek Mohan. © 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc., s:105-168.

Silvers, R., (2021), November 10. Decoding Ransomware: Leadership, Cryptocurrency and Cooperation 2 [Plenary session]. **Annual Meeting on Cybersecurity**, Geneva, Switzerland

Sinclair, T.J.,(2016), **Küresel Yönetişim**, Çev.H.Hande Orhan Özdağ, İstanbul Kültür Üniversitesi Yayınevi, Kasım 2016.

Singer, P. (1986). Introduction, **All Animals Are Equal**. Applied Ethics (ed. by P. Singer) içinde (Syf.3, 215-228), Oxford University Press, Oxford.

Skovira, R. J., (2003), "The Social Contract Revised: Obligation and Respossibility in the Information Society", **Current Security Management & Ethical Issues of Information Technology,** Ed. Rasool Azari, IRM Press, Hershey, s:165-186.

Slaughter, A.M.,(2014), "Küresel Ekonomiyi Yönetim Şebekeleri Aracılığıyla Yönetmek", **Küresel Dönüşümler-The Global Transformations Reader**, Polity Press 2003, Haz. David Held, Anthony McGrew, Çev. Ali Rıza Güngen, Phoneix Yayınevi, İkinci Baskı, Haziran 2014, Ankara sayfa: 229-246.

Slay, J., Miller, M.,(2008), "Lessons Learned From The Maroochy Water Breach", **Critical Infrastructure Protection,** Ed. E.Goetz, S.Shenoi, Springer, s:73-82.

Smetters, D. K., (2014),"Cyber Security Technology Usability and Management", **Cyber Security**, Ed. John G. Voeller, John Wiley&Sons, 2014, New Jersey, s:41-56.

Soesanto, S., Smeets,M.,(2020),"Cyber Deterrence:The Past, Present, and Future" NL ARMS Netherlands Annual Review of Military Studies 2020 **Deterrence in the**

21st Century-Insights from Theory and Practice, Ed. Frans Osinga, Tim Sweijs,Springer:385-400

Stallings,W.,(2019), **Effective Cybersecurity Understanding and Using Standards and Best Practices**, Addison-Wesley, Upper Saddle River, NJ • Boston • San Francisco • New York Toronto • Montreal • London • Munich • Paris • Madrid Cape Town • Sydney • Tokyo • Singapore • Mexico City.

Stückelberger,C.(2018), "Cyber Society: Core Values And Virtues", **Global Ethics 4.0. Serving Humanity with Values**, Ed.Christoph Stückelberger & Pavan Duggal, Globethics.net Global 17, Geneva, Switzerland Website: www.globethics.net, October 2018, s:23-54.

Stouffer, K., Pillitteri, V., Ligtman, S., Abrams, M., Hahn, A., (2015), **Guide to Industrial Control Systems (ICS) Security**, NIST Special Publication 800-82 Revision 2, May 2015, NIST Gaithersburg.

Stouffer, K.,Pease M.,Tang C.Y.,Zimmerman T.,Pillitteri V., Lightman S.,(2022), **Guide to Operational Technology (OT) Security**, Initial Public Draft, NIST Special Publication NIST SP 800-82r3 ipd, April 2022, U.S. Department of Commerce 51 Gina M. Raimondo, Secretary.

https://doi.org/10.6028/NIST.SP.800-82r3.ipd

Sullivan, D.,Luiijf, E. Colbert, E.,(2016), **Components of Industrial Control Systems, Cyber-security of SCADA and Other Industrial Control Systems**, Ed. Edward J.M. Colbert, Alexander Kott, Springer, 2016, s:15-28.

Susanto, I., Jackson, R., Paul, D. L., "Industrial Process Control System", **Cyber Security**, Ed. John G. Voeller, John Wiley&Sons, 2014, New Jersey, s:87-96.

Symantec, (2017), **Dragonfly: Western energy sector targeted by sophisticated attack group**, Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks), October 20, 2017.

Tabansky, L., (2017), "Cyber Security Challenges: The Israeli Water Sector Example", s:205-218, **Cyber Physical Security Protecting Critical Infrastructure at the State and Local Level,** Ed. Robert M. Clark, Simon Hakim, 2017, Springer-Switzerland, s:205-218.

Tangör, B.,(2008), **Avrupa Güvenlik Yönetişimi**, Seçkin Yayıncılık,Ankara.

Taddeo, M.,(2017), **The Limits of Deterrence Theory in Cyberspace**, Philos. Technol. (2018) 31:339–355 https://doi.org/10.1007/s13347-017-0290-2

Tamkoç, G. (1994), "**Derin Ekolojinin Genel Çizgileri**", Ege Yayıncılık, İzmir.

Tanczer, L.M.,Brass, I., Elsden, M., Carr,M. Blackstock J., (2019), "The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape", **Rewired: Cybersecurity Governance**, First Edition. Edited by Ryan Ellis and Vivek Mohan. © 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc., s:37-56.

T.C. Cumhurbaşkanlığı, (2019), **On Birinci Kalkinma Plani** (2019-2023), 100. Yıl Türkiya Planı, Temmuz 2019.

https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf (Erişim Tarihi :12 Ocak 2022)

T.C.İçişleri Bakanlığı,(2017), **Güvenlik Terimleri Sözlüğü**, Kamu Düzeni ve Güvenliği Müsteşarlığı Yayınları, 2. Baskı, Mayıs 2017, Uluslararası Piri Reis Kültür Ajansı, Ankara.

T.C.İçişleri Bakanlığı,(2019), **AFAD Stratejik Plan Güncellenmiş Versiyon** (2021)

https://www.afad.gov.tr/kurumlar/afad.gov.tr/e_Kutuphane/Planlar/AFAD_2019_2023_STRATEJIK_PLAN.pdf (Erişim Tarihi: 20 Ocak 2023).

T.C. İçişleri Bakanlığı,(2022), **Türkiye Afet Müdahale Planı (TAMP)**, Afet ve Acil Durum Yönetimi Başkanlığı

https://www.mevzuat.gov.tr/MevzuatMetin/20.5.6053.pdf (Erişim Tarihi: 22 Ocak 2023)

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

http://www.sp.gov.tr/tr/temel-belge/s/202/Ulusal+Siber+Guvenlik+Stratejisi+ve+Eylem+Plani+_2020-2023 (Erişim Tarihi:12 Ocak 2022)

T.C.CBDDO (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi), (2020), **Bilgi ve Iletişim Güvenliği Rehberi**, Temmuz 2020, Sürüm N0:2020/1.0 https://cbddo.gov.tr/bgrehber (Erişim Tarihi: 10 Kasım 2022)

T-CY, The Cybercrime Convention Committee, https://www.coe.int/en/web/cybercrime/tcy Son erişim:15 Kasım 2021).

Tepe, Harun, (2007), Doğu Batı Etik, Ed.Takış, Taşkın, "Bir Felsefe Dalı Olarak Etik", sayfa:11-28, Sayı:4, **Doğu Batı Yayınları**, 4. Baskı, Mart 2007, Ankara.

Tessari,P.,Muti, K.,(2021), **Strategic or Critical Infrastructures**, A Way To Interfere in Europe: State Of Play And Recommendations, Policy Department for External Relations Directorate General for External Policies of the Union PE 653.637 – European Parliament, July 2021

The United Nations (1972), The Documents of the United Nations Conference on Human Environment-1972: **Declaration on the Human Environment**, Declaration of Principles, Recommendations for Action, Stockholm.

The White House, (1998**), Presidential Decision Directive**/Nsc-63 http://fas.org/irp/offdocs/pdd/pdd-63.ht (Erişim Tarihi: 26 Temmuz 2016)

The White House, (2003), **National Strategy for the Physical Protection of Critical Infrastructures And Key Assets**, Washington, February 2003, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf Erişim Tarihi: 26 Temmuz 2016.

The White House (2013). **Presidental Policy Directive** Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21, February 12,2013.

Trivellato,D ve Murphy,D., (2018), "Elektrikler Gitti Sırada Ne Var? Ukrayna'daki "siber kesinti"nin analizi", **Security Matters**, http://www.biznet.com.tr/wp-content/uploads/2018/02/whitepaper-lights_out_who_is_next-TR.pdf (Erişim Tarihi: 10 Nisan 2018)

Turk, Robert J., (2005), **Cyber Incidents Involving Control Systems**, US-CERT Control Systems Security Center Idaho Falls, Idaho 83415, October 2005, https://inldigitallibrary.inl.gov/sti/3480144.pdf (Erişim Tarihi: 27 Haziran 2015).

UN, (2015), **Sustainable Developments Goals**

https://www.un.org/sustainabledevelopment/ (Erişim Tarihi:13 Mart 2022).

UNGA (30 Dec 2002**) Developments in the field of information and telecommunications in the context of international security** A/RES/57/53

UNGA (14 Sep 2011) International Code of Conduct for information security A/66/359 18 **Norms of Responsible State Behaviour in Cyberspace**

UNGA (13 Jan 2015) **International Code of Conduct for information security** A/69/723

UNGA (11 Dec 2018) Developments in the field of information and telecommunications in the context of international security A/RES/73/27 and 2 Jan 2019 Advancing responsible state behaviour in cyberspace in the context of international security A/RES/73/266

Ural, S.S. .(2013), **Temel Hak ve Özgürlüklerin Korunması Bağlamında Bireysel Başvuru**, Seçkin Kitabevi, Ankara, 2013, s:320.

Uz, A.,(2020), **Sürdürülebilir Kalkınma Ekseninde Konut Üretimi ve Konut Yapı Malzemeleri,** Doktora Tezi, Ankara Üniversitesi SBE Sosyal Çevre Bilimleri ABD, Ankara, 2020.

Ünal, F., (2010), Toplumsal Ekoloji, **Dumlupınar Üniversitesi Sosyal Bilimler Dergisi**, Sayı 26, Nisan 2010, s:114-123. https://dergipark.org.tr/tr/download/article-file/55600 (Erişim tarihi:5 Temmuz 2021).

Ürker, O.,(2014),Çevre Etiği Bağlamında Anadolu Sığla Ormanları, **Doktora Tezi**, Ankara Üniveritesi Sosyal Çevre Bilimleri Bölümü, Ankara.

Vallor, S., Rewak, W.J.,(2018), **An Introduction to Cybersecurity Ethics** Santa Clara University. https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf (Erişim Tarihi: 30 Aralık 2018).

Waever,Ole, "Peace and Security: Two Evolving Concepts and Their Changing Relationship", **Globalization and Environment Changes,** Editors: Hans Günter Brauch, Ursula Oswald Spring, Czeslaw Mesjasz, John Grin, Pal Dunay, Navnita Chadha Behera, Bechir Chourou, Patricia Kameri,P.H.Liotta, Springer Berlin HEidelberg, 2008, s:99-111.

Warren, M.J.,Leitch, S., (2015), "Cyber Security and Protection of ICS Systems:An Australian Example", **Cyber Security:Analytics, Technology and Automation**, Ed. Martti Lehto, Pekka Neittaanmaki, 2015, Springer Switzerland, 2015, s:215-228.

World Commission on Environment and Development (WCED), (1987), Report of World Commission on Environment and Development:**Our Common Feature**,Oxford Universty Press.

https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf (Son Erişim tarihi: 2 Haziran 2021)

Weckert,J., Henschke, A., (2010), "Computer Ethics and Applied Contexts", **The Cambridge Handbook of Information and Computer Ethics,** Ed. Luciano Floridi, Cambridge University Press, 2010, s: 182-197.

Wenger,A.,Cavelty,MD.,(2022), "Conclusion", **Cyber Security Politics Socio-Technological Transformations and Political Fragmentation**, Ed. Myriam Dunn Cavelty, Andreas Wenger,Routledge, Taylor&Franchis Group, New York.

Wiener, Norberth, 1968, **The Human Use of Human Beings:Cybernetics and Society (1954), Londra:Sphere Books.**

Witheford, N. D., 2004, **Siber-M@rx**, Çev. Ali Çakıroğlu, Aykırı Yayıncılık, Mart 2004, İstanbul.

Vigano E., Loi M., Yaghmaei, E. (2020), Cybersecurity of Critical Infrastructure, **The Ethics of Cybersecurity**, Ed. Markus Christen, Bert Gordijn, Michele Loi, The

İnternational Library of Ethics, Law and Technology 21, Springer Open, s:1157-178.

Virtanen, T., (2003), *Changes in The Profile of Security Managers*, **Security Education and Critical Infrastructures**, Ed. Irvine, Cynthia, Armstrong, Helen, 2003, Springer, New York, s: 41-49.

Woods, A., Ying He, Maglaras, L.A., Helge Janicke H.,(2016), "A Security Architectural Pattern for Risk Management of Industry Control Systems within Critical National Infrastructure", **Int. J. Electric and Hybrid Vehicles,** Vol. x, No. x, 1–26. authorFinalVersion.pdf (dmu.ac.uk) Erişim tarihi : 13 Mart 2022.

Working Group on Internet Governance (WGIG),(2005), **Report of the Working Group on Internet Governance**, Chateau de Bossey, June 2005, s:4. http://www.wgig.org/docs/WGIGREPORT.pdf Son erişim tarihi:27 Ekim 2021.

WEF,(2022), World Economic Forum ***Global Cybersecurity Outlook 2022 INSIGHT REPORT,*** JANUARY 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

Yayla, M.(2014),"Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", **Hacettepe HFD**, 4(2) 2014,s:181-200. Erişim Tarihi: 12 Ekim 2021.

Yeşilyurt, Hamdi, (2015), 'Ulusal Güvenlik Perspektifinde Siber Güvenlik', s:169-191, **Siber Suçlar**, Ed. Fatih Tombul, Murat Güneştaş, Oguzhan Başıbüyük, Global Politika ve Strateji Yayınları, 2015,Ankara.

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2003_004_001_14198.pdf emniyet ve güvenlik tanımı

http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

https://lostar.com.tr/2014/11/advanced-persistent-threat-apt.html (Erişim Tarihi 10 Haziran 2018)

ÖZET

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SOSYAL ÇEVRE BİLİMLERİ ANABİLİM DALI

Tezin Adı	Çevre Etiği Bağlamında Siber Güvenlik
Türü	Doktora Tezi
Yazar	Sema ALTINSOY
Tez Danışmanı	Prof. Dr. Nesrin ÇOBANOĞLU
Anahtar Kelimeler	Çevre Etiği, Sürdürülebilirlik, Siber Güvenlik, Kritik Altyapılar, Kozmopolitanizm
Sayfa Adedi	326

Özet

Bilişim teknolojilerindeki hızlı gelişmeler ile fiziki dünya paralelinde insan eli ile siber uzay oluşturulmuştur. Her geçen gün artan sayıda yazılım, donanım, ağ ürünleri ile genişlemekte olan siber uzay, küresel seviyede yaygınlaşmaya ve daha çok insan tarafından kullanılmaya başlanmış ve günlük hayatın vazgeçilmezi haline gelmiştir. Yetersizlikleri ya da yok edilmeleri durumunda can ve mal kaybına neden olabilen, toplumsal kaos doğurabilen kritik altyapılar da bilişim teknolojilerindeki gelişmelere paralel olarak siber uzay üzerinden faaliyetlerini sürdürmeye başlamıştır. Doğal afetler sonucu ya da istemli-istemsiz siber güvenlik olayları sonucu kritik altyapıların faaliyetlerini yerine getirememesi, sürdürülebilirliği önleyebilecek önemli çevre sorunlarına neden olabilecektir. 1980 yılından itibaren kritik altyapılara yönelik siber güvenlik olayları örnekleri incelenmiş ve önemli çevre sorunlarına neden olabileceği görülmüştür.

Kritik altyapıların siber güvenliği için bu sistemlerin yaşam döngüleri boyunca bireysel, kurumsal ve ulusal seviyede önleyici koruyucu, risk yönetimi, caydırıcılık ve kamu siber güvenlik yaklaşımları kullanılarak önlemler alınmalıdır. Ancak siber uzayın sınır tanımayan doğası gereği kritik altyapıların siber güvenliği için kamu kurumlarının yanı sıra, özel sektör, sivil toplum kuruluşları, bireyler vb.den oluşan paydaşların da katılımı ile uluslararası kuruluşların alt birimleri, çok uluslu şirketler, çok paydaşlı kuruluşlar ve yönetsel ağlar tarafından siber güvenlik standartları oluşturulması gibi küresel yönetişim faaliyetleri yürütülmektedir. Bu faaliyetler kozmopolitanizm kavramı doğrultusunda tüm dünya üzerindeki canlı cansız varlıkların sürdürülebilirliğini sağlayabilecektir.

ABSTRACT

REPUBLIC OF TURKEY
ANKARA UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF SOCIAL ENVIRONMENT SCIENCES

Thesis	Cyber Security in the Context of Environmental Ethics
Type	Philosophy of Doctorate
Author	Sema ALTINSOY
Advisor	Prof. Dr. Nesrin ÇOBANOĞLU
Key Words	Environmental Ethics, Sustainability, Cybersecurity, Critical Infrastructures, Cosmopolitanism
Total Page	326

Abstract

With the rapid developments in information technologies, cyber space has been created by human hands in parallel with the physical world. The cyber space, which is expanding day by day with an increasing number of software, hardware and network products, has become widespread at the global level and used by more people and has become an indispensable part of daily life. Critical infrastructures, which can cause loss of life and property and cause social chaos in case of their insufficiency or destruction, have started to operate in the cyber field in parallel with the developments in information technologies. The inability of critical infrastructures to perform their activities as a result of natural disasters or voluntary or involuntary cyber security events may cause significant environmental problems that may prevent sustainability. Since 1980, examples of cyber security incidents for critical infrastructures have been examined and it has been seen that they can cause significant environmental problems.

For the cyber security of critical infrastructures, measures should be taken by using preventive, risk management, deterrence and public cyber security approaches at the individual, institutional and national level throughout the life cycles of these systems. However, due to the borderless nature of the cyberspace, for the cyber security of critical infrastructures, cybersecurity services are provided by sub-units of international organizations, multinational companies, multi-stakeholder organizations and administrative networks with the participation of stakeholders such as the private sector, non-governmental organizations, individuals, etc., as well as public institutions. Global governance activities such as establishing security standards are carried out. These activities will be able to ensure the sustainability of living and non-living beings all over the world in line with the concept of cosmopolitanism.