TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SİBER OLAYLARA MÜDAHALE KONUSUNDA AMERİKA BİRLEŞİK DEVLETLERİ, FRANSA VE TÜRKİYE'NİN İDARİ YAPILARININ İNCELENMESİ – NÜKLEER SANTRAL ÖRNEĞİ

Abdullah GENÇAY

DİSİPLİNLERARASI ADLİ BİLİMLER ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç Dr. Nergis CANTÜRK
2. DANIŞMAN
Doç. Dr. Sait ÖZSOY

ANKARA
2018

Etik Beyan

Ankara Üniversitesi

Sağlık Bilimleri Enstitüsü Müdürlüğü'ne

Yüksek Lisans tezi olarak hazırlayıp sunduğum "Siber Olaylara Müdahale Konusunda Amerika Birleşik Devletleri, Fransa Ve Türkiye'nin İdari Yapılarının İncelenmesi – Nükleer Santral Örneği" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Abdullah GENÇAY

Tarih:

İmza:

Kabul ve Onay

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Bilimler Anabilim Dalı
Fizik İncelemeler ve Kriminalistik Tezli Yüksek Lisans Programında

Abdullah GENÇAY tarafından hazırlanan

"Siber Olaylara Müdahale Konusunda Amerika Birleşik Devletleri, Fransa ve Türkiye'nin İdari Yapılarının İncelenmesi – Nükleer Santral Örneği" adlı tez çalışması

aşağıdaki jüri tarafından **YÜKSEK LİSANS TEZİ** olarak

OY BİRLİĞİ ile kabul edilmiştir.

15.01.2018

Prof.Dr. H.Sinan SÜZEN
Ankara Ü. Eczacılık Fakültesi
Jüri Başkanı

Prof. Dr. Aysun BARANSEL ISIR
Gaziantep Ü. Tıp Fakültesi
Üye

Doç.Dr.Nergis CANTÜRK
Ank.Ü. Adli Bilimler Enstitü
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof.Dr. Mehmet AKAN
Sağlık Bilimleri Enstitüsü Müdür V.

İçindekiler

Önsöz

Siber suç dünyası asimetrik yapısı nedeniyle geleneksel suç ortamının aksine suçluların daha çabuk kamufle olmasına olanak sağlamaktayken, nükleer saldırıların meydana geldiği tarihten 20-30 yıl sonra bile olumsuz etkilerinin devam etmesi bu iki alanın ne kadar önemli olduğunu gözler önüne sermektedir. Nükleer ve Siber suç dünyasını birleştiren detaylı bir çalışmanın ülkemiz için yapılmamış olması ve yakın gelecekte bu alanda yapılacak saldırılara hazır olma zorunluğumuz beni bu çalışmaya yapmaya iten önemli etkenlerdendir. İlerisi için karar vericilere önemli bilgiler sunulması hedefiyle hazırlanmış bu çalışmanın ülkemiz adına ilgili kurumlar nezdinde önemli faydalar sağlayacağı düşünülmektedir.

Öncelikle yüksek lisans eğitimim boyunca akademik anlamda bana özgün bir bakış açısı kazandıran, bilgi ve tecrübelerini benimle paylaşan tez danışmanlarım Sayın Doç. Dr. Nergis CANTÜRK'e, Doç. Dr. Sait ÖZSOY'a, Sayın Prof. Dr. Halit Sinan SÜZEN'e, Sayın Prof. Dr. Gürol CANTÜRK'e, yüksek lisans eğitimim boyunca her ihtiyaç duyduğumda bilgi alabildiğim öğrenci arkadaşlarıma, Türkiye Atom Enerjisi Kurumu Nükleer Güvenlik Dairesi personeline,

Yüksek lisans dersleri döneminde ve teze konu alana yönelmem sürecinde desteğini hep yanıma hissettiğim Siber Suçlarla Mücadele ve Haberleşme Daire Başkanlıklarındaki başkanıma, abilerime ve kardeşlerime,

Yoğun tez hazırlama dönemi ve öncesinde desteğini her zaman hissettiğim eşim ve kızıma, eğitim hayatım boyunca varlığıyla yanımda olan aile üyelerime, biricik torunu olduğum merhum Hasan GENÇAY'a, en içten dileklerimle şükranlarımı sunarım.

Simgeler ve Kısaltmalar

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AEC	Atomic Energy Commission – ABD Atom Enerjisi Komisyonu
AFAD	Afet ve Acil Durum Yönetimi Başkanlığı
ANDRA	Agence Nationale Pour la Gestion des Déchets Radioactifs – Fransa Ulusal Radyoaktif Atık Yönetim Ajansı
ANSSI	Agence nationale de la sécurité des systèmes d'information – Fransa Ulusal Siber Emniyet Ajansı
ASN	Autorite De Sûreté Nucléaire – Fransa Nükleer Güvenlik Kurumu
BBC	The British Broadcasting Corporation – İngiliz Yayın Kuruluşu
BİLGEM	TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BSI	Bundesamt für Sicherheit in der Informationstechnik – Almanya Federal Bilgi Güvenliği Ajansı
BSTB	Bilim, Sanayi ve Teknoloji Bakanlığı
BTC	Bakü Tiflis Ceyhan Boru Hattı
BTE	Bilişim Teknolojileri Enstitüsü
CAT	Cyber Action Team – Siber Savaş Takımı
CEA	Commissariat à l'énergie atomique et aux énergies alternatives – Fransa Atom Enerjisi ve Alternatif Enerjiler Komisyonu
CI	Critical Infrastructure – Kritik Altyapı

CIA	Central Intelligence Agency – Merkezi Haberalma Teşkilatı
CIRG	Critical Incident Response Group - Kritik Olaylara Müdahale Grubu
CPPNM	Convention On The Physical Protection of Nuclear Material and Nuclear Facilities – Nükleer Madde ve Tesislerin Fiziksel Korunması Sözleşmesi
DHS	Department of Homeland Security – ABD İç Güvenlik Bakanlığı
DoD	Department of Defence – ABD Savunma Bakanlığı
DOS	Denial of Service – Hizmet Dışı Bırakma (Bir siber saldırı türü)
DDOS	Distributed Denial of Service – Dağıtık Hizmet Dışı Bırakma (Bir siber saldırı türü)
DPT	Devlet Planlama Teşkilatı
EC	European Commission - Avrupa Komisyonu
ECI	European Commission Infrastructure – Avrupa Kritik Altyapısı
EDAM	Ekonomi ve Dış Politika Araştırma Derneği
EDF	Électricité de France – Fransa Elektrik İdaresi
ENISA	European Union Agency for Network and Information Security – AB Ağ ve Bilgi Güvenliği Ajansı
EP	Emergency Plan – Acil Durum Planı
EPDK	Enerji Piyasası Denetleme Kurumu
ETKB	Enerji ve Tabii Kaynaklar Bakanlığı
EÜAŞ	Elektrik Üretim A.Ş.
FBI	Federal Bureau of Investigation – ABD Federal Soruşturma Bürosu
FEMA	Federal Emergency Management Agency – ABD Federal Acil Durum Yönetim Ajansı
IAEA	International Atomic Energy Agency – Uluslararası Atom Enerjisi Ajansı

INES	International Nuclear Events Scale – Uluslararası Nükleer Olay Ölçeği
IP	Internet Protokol
IRSN	Institut de Radioprotection et de Sûreté Nucléaire – Fransa Radyoaktif Korunma ve Nükleer Güvenlik Enstitüsü
ISAC	Information Sharing and Analysis Centre – ABD Bilgi Paylaşımı ve Analiz Merkezi
İLTAREN	İleri Teknoloji Araştırma Enstitüsü
LAN	Local Area Network – Yerel Alan Ağı
MASAK	Mali Suçları Araştırma Kurulu
MİT	Milli İstihbarat Teşkilatı
MW	Megawatt
NCCIC	National Cybersecurity and Communication Integration Center – ABD Ulusal Siber Emniyet ve İletişim Entegrasyon Merkezi
OECD NEA	OECD Nuclear Energy Agency – OECD Nükleer Enerji Ajansı
NGS	Nükleer Güç Santrali
NIST	National Institute of Standarts and Technology – ABD Ulusal Standartlar ve Teknoloji Enstitüsü
NRC	Nuclear Regulatory Commission – ABD Nükleer Düzenleme Komisyonu
NSA	National Security Agency – ABD Ulusal Güvenlik Ajansı
NPT	Treaty on the Non-Proliferation of Nuclear Weapons – Nükleer Silahların Yayılmasının Önlenmesi Antlaşması
NTI	Nuclear Threat Initiative – Nükleer Tehdit İnisiyatifi
OECD	The Organisation for Economic Co-operation and Development – Ekonomik Kalkınma ve İşbirliği Teşkilatı

PLC	Programmable Logic Controller – Programlanabilir Mantıksal Kontrol Cihazı
RESA	Radyasyon Erken Uyarı Sistemi Ağı
ROP	Reactor Oversight Process – Reaktör Denetim Süreci
SCADA	Supervisory Control and Data Acquisition – Veri Toplama ve Kontrol Destek Sistemi Endüstriyel tesislerde tesisin yönetimi ve kontrolü için kullanılan genelde elektronik tabanlı sistemlerin genel adı
SGDSN	General Secretariat for Defence and National Security - Fransa Savunma ve Ulusal Güvenlik Genel Sekreterliği
SGE	TÜBİTAK Siber Güvenlik Enstitüsü
SOME	Siber Olaylara Müdahale Ekibi
TAEK	Türkiye Atom Enerjisi Kurumu
TBMM	Türkiye Büyük Millet Meclisi
TDK	Türk Dil Kurumu
TET	Tasarıma Esas Tehdit Nükleer Güç Santrallerinin henüz tasarım aşamasında istekli tarafından lisans alabilmek için hazırlanan çok boyutlu doküman
THY	Türk Hava Yolları
TİB	Telekomünikasyon İletişim Başkanlığı
TSK	Türk Silahlı Kuvvetleri
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB	Ulaştırma Denizcilik ve Haberleşme Bakanlığı
UEKAE	TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UN	United Nations – Birleşmiş Milletler
USB	Universal Serial Bus
USCYBERCOM	United States Cyber Command – ABD Siber Komutanlığı
US-DoE	United States Department of Energy – ABD Enerji Bakanlığı

USOM	Ulusal Siber Olaylara Müdahale Merkezi
WNA	World Nuclear Association – Dünya Nükleer Birliği
YTE	TÜBİTAK Yazılım Teknolojileri Araştırma Merkezi

Çizelgeler

1. GİRİŞ

Bilgisayar ağlarının iletişim amacıyla kullanılmaya başlandığı 1960'lı yıllardan günümüze, bilgi ve iletişim teknolojilerinin insan yaşamında sağladığı faydalar kadar kişisel ve kurumsal bilgi güvenliğine yönelik tehditlerin de araştırılması ve tartışılması gerekmektedir. Siber evren, siber terörizm, siber çeteler, siber espiyonaj, siber suç, siber istihbarat, nükleer siber güvenlik gibi birçok "siber" ön ekli kavram hayatımıza girmiş ve olup sınırları net bir şekilde çizilemeyen, suçun asimetrik olarak işlenebildiği bu sanal dünyada güvenli bir şekilde kalabilmek için farkındalık seviyesi yüksek kullanıcılara duyulan ihtiyaç her geçen gün artmaktadır. Farkındalık seviyesi düşük kullanıcılar ile farkındalık seviyesi yüksek bireysel, grupsal -ya da zaman zaman devlet destekli de oldukları iddia edilen- suç organizasyonları suçtan zarar gören mağdurlar listesine kısa sürede devletleri de eklemişlerdir.

Başka bir devlete hasmane ya da politik sebeplerle zarar verme hedefindeki gruplar ilk olarak elektronik hizmet alanları, barajlar, elektrik dağıtım şebekeleri, nükleer tesisler, askeri tesisler gibi kritik altyapıları hedeflemektedirler. 2023 yılına kadar çalışan en az bir nükleer reaktör bulundurmayı hedefleyen ülkemizde henüz çok yeni olan nükleer siber emniyetin sağlanması büyük önem arzetmektedir. Nükleer siber emniyetin sağlanabilmesi hususu yasal çerçevenin hazır olması, düzenleyici ve denetleyici kurumların doğru bilgiyle yeterince donatılmış olması gibi önşartlara bağlı olmakla birlikte hiçbir zaman bitmeyecek, güvenlik kurallarının sürekli olarak kontrol edildiği canlı bir emniyet atmosferi olarak değerlendirilmelidir.

Emniyet atmosferini doğru değerlendirmek için 2012 yılında Amerika Birleşik Devletleri'ndeki (ABD) Y-12 OAK Ridge Ulusal Güvenlik Tesisi içerisindeki Yüksek Oranda Zenginleştirilmiş Uranyum bulunan bir yerleşkede meydana gelen olayı çok iyi değerlendirmek gerekmektedir. Megan Rice (83), Michael Walli (63) ve Greg Boertje-Obed (57) isimli üç aktivist tarafından tesisi çevreleyen teller kesilip tesis arazisine girilmesi sonrasında tesisin iç bölgelerini çevreleyen telleri de sırasıyla keserek toplam dört katmanlık bir iç içe güvenlik yapısını ihlal etmişlerdir. Saatler süren bu ihlal boyunca kimseyle karşılaşmayan aktivistler yüksek oranda zenginleştirilmiş uranyum içeren bir binanın duvarına spreyle protestolarına dair ifadeler yazmışlardır. Sonrasında kendi iradeleriyle güvenliğe giderek teslim olmuşlardır. 2012 mali yılında tesisin fiziksel güvenliği için 150 milyon dolar ödenek ayrılmış olması ve tesisin ABD'deki en güvenli tesis olarak ün yapmış olması ayrıca önemli bir detaylar olarak ABD Enerji Bakanlığı (US-DoE) tarafından olayla ilgili hazırlanan raporda yer almaktadır (US-DoE, 2012). Emniyet atmosferi, ancak düzenleyicisinden denetleyicisine işletmecisinden çalışanına kadar geniş alanda bir emniyet kültürü oluşturmakla sağlanabilecektir.

Türkiye Cumhuriyeti'nin "Yap-Sahip ol-İşlet" modeliyle nükleer enerji üretimiyle tanışacak olması, bu tesisleri hedef alabilecek siber saldırılara hazırlık süreci konusunda deneyimimizin olmaması, önemli bir eksiklik olarak önümüzde durmaktayken, ülkemizin ilgili kurumları arasındaki görev paylaşımında çakışmaların ve muhtemel eksikliklerin varlığı, ilerleyen süreçte hangi seviyede sıkıntılar yaşanabileceğini öngörme konusunda dahi daha çok model incelemeyi gerekli kılmıştır.

Bu çalışmada nükleer enerji alanında dünyada oldukça yol katetmiş iki ülkenin mevcut idari yapıları incelemeye alınmış ve ülkemiz idari yapısı üzerinden değerlendirmelerde bulunulmuştur. Konunun doğru anlaşılabilmesi amacıyla

öncelikle “Siber Alan” tanıtılarak örnek olaylar, olay dinamikleri, muhtemel failler gibi öğeler paylaşılmıştır. Sonrasında “Nükleer Alan” hakkında bilgi verilerek bu alanda yaşanmış olaylar paylaşılmıştır. Kritik altyapılarla ilgili dünya örnekleri de verilerek detaylı bilgilerin paylaşılması sonrasında ülkemiz, ABD ve Fransa’nın nükleer tesislere yönelik siber saldırılara karşı koyma, etkilerini azaltma konularında idari yapıları incelenmiş elde edilebilen bilgiler karşılaştırılmıştır. Yapılan tüm bu paylaşım sonrasında tartışma, sonuç ve öneriler bölümlerinde ülkemizle ilgili dikkate değer hususlar tartışılmış ve önerilerle ilgili değerlendirmelere yer verilmiştir.

1.1. Siber Alan

Gelişen teknoloji ile birlikte ev eşyalarını bile uzaktan (internet üzerinden) verilen talimatlarla yönetmek mümkün hale gelmiştir. 2016 yılı itibariyle yaklaşık 4,6 milyar mobil telefon kullanıcısının bulunduğu dünyada siber alan her an her yere ulaşmıştır. "Siber Alan"ı anlamak, bu alandaki saldırı türleri hakkında fikir edinmek ve yaşanmış olayları öğrenmek tanımak amacıyla bu bölüm hazırlanmıştır (Statista, 2017).

1.1.1. Siber Terminoloji

Türkçe kaynaklar incelendiğinde “siber” kelimesinin Türkçe sözlüklerde yer almadığı görülmektedir. İngilizce kaynaklar incelendiğinde ise “cyber” kelimesi

“bilgisayar, bilgisayar ağları ve sanal gerçeklik kelime anlamlarının bir araya gelmesiyle oluşmuş birleşik kelime” olarak tanımlanmaktadır (Dictionary, 2017; TDK Sözlük, 2017).

Amerikalı Bilim Adamı N. Weiner tarafından ilk kez 1948 yılında “hayvanlarda ve makinelerde iletişim ve kontrol bilimi” anlamında kullanılmıştır (Beer, 2017). Günümüzde dilimizin kullanımı esnasında da sık sık kullanımına rastlanmaktadır. Ancak bu kullanım Fransızca “informatique” sözcüğünden gelen enformatik kelimesinin türediği “bilişim” kelimesinin yoğun kullanımıyla karşımıza çıkmaktadır (Karagülmez, 2005).

“Bilişim” kelimesi, “insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi” anlamına gelmektedir (TDK, 2017). Bu tanımdan da anlaşılacağı üzere, “bilişim”, “siber” kavramından daha kapsamlı bir alanı ifade etmektedir.

Siber kavramının daha iyi anlaşılması için siber uzay, siber saldırı, siber savaş, siber suç, siber terör vb. kavramların da açıklanması gerekmektedir.

1.1.1.1. Siber Uzay

ABD Savunma Bakanlığının tanımına göre "siber uzay"; bilgi teknolojileri altyapıları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerinden meydana gelen birbirine bağımlı ağlardan oluşan alan şeklinde tanımlanmaktadır (DoD, 2017b). ABD İç Güvenlik Bakanlığı için hazırlanmış olan Ulusal Strateji Belgesinde ise siber uzay, ülkenin tamamını kontrol eden bir sinir sistemine benzetilmiş ve ayrıca binlerce bilgisayarın, sunucunun, yönlendiricinin (router), anahtarın (switch) ve kabloların birbirine bağlandığı kritik altyapıların çalışmasını sağlayan yapı olarak tanımlanmıştır (White House, 2003).

"Siber uzay" enerji dağıtım ağları, kapalı askeri ağlar, iletişim ağları, cep telefonları, yazılım tabanlı telsizler, elektronik komuta sistemleri, Supervisory Control and Data Acquisition (SCADA) sistemleri, uydu sistemleri, insansız hava araçları, uçaklar (özellikle uçaktaki sistemleri kontrol eden temel yazılım ve donanımlar) gibi birçok sistem ve donanımı barındıran bir yapıdadır (Çifci, 2013).

1.1.1.2. Siber Savaş

"Siber savaş" "bir devlet tarafından, başka bir devletin bilgisayar veya bilişim ağlarına veri eklemek, değiştirmek ya da bozmak veya bilgisayarları, ağ üzerindeki cihazları ya da bilgisayar sisteminin kontrol ettiği nesneleri kesintiye uğratmak veya onlara hasar vermek amacıyla yetkisiz giriş yapılması"; "siber savaş, bilgi savaşı ile birlikte aynı anlamda "bilgi ve bilgi sistemlerinin savunma ya da saldırı amaçlı olarak –kendi sistemleri korunurken düşman bilgi, bilgi süreci ya da bilgi sistemleri üzerinde-durdurma, zarar verme, bozma veya tahrip etme gibi amaçlarla kullanılması," şekillerinde tanımlanmaktadır (Clarke & Knake, 2011a)(UN, 2017a).

1.1.1.3. Siber Terörizm

Çifçi'ye göre terörizmin tanımı konusunda uluslararası alanda mevcut belirsizlik siber terörizme de sirayet etmiş durumdadır(Çifci, 2013). Lewis, Denning ile Çakmak&Demir siber terörizmi aşağıdaki gibi tanımlamıştır;

- "Bilgisayar ağlarında kullanılan yazılımların kritik ulusal altyapıları (enerji taşıma, kamu hizmetler vb.) kapatmak veya toplum ya da devlet üzerinde korku ve panik yaratmak amaçlı kullanılmasıdır" (Lewis, 2002).
- "Siber terörizm, terörizm ile siber uzayın kesişimidir. Genel olarak politik ya da sosyal hedeflerle insanlarda ya da kamuda korku ve panik yaşatma amaçlı bilgisayarlara, ağlara ya da özel bilgilere karşı yapılan hukuki olmayan saldırılar ve tehditler olarak algılanır" (Denning, 2000).
- "Toplumlarda korku ve endişe yaratmak hedefiyle elektronik tabanlı donanımların kullanıldığı teknoloji imkânlarına yönelik eylemlerdir. Bu eylemlerde siyasi motivasyon ön plana çıkmaktadır" (Çakmak & Demir, 2009).

Terör örgütleri devlet kurumlarında kullanılan bilgisayarlara ulaşarak gizli veya kişisel bilgi ve belgelere ulaşabilirler. Örneğin Diyarbakır'da polisin hırsızlık yaptığı şüphesiyle yakaladığı ve elindeki dizüstü bilgisayarında Milli İstihbarat Teşkilatı (MİT) ve Genelkurmay Başkanlığı başta olmak üzere devlete ait gizli bilgiler tespit edilen 19 yaşındaki hacker R.C.'nin, bir terör örgütünün 'hacker'i olduğu ve örgütün elebaşlarından Murat Karayılan'a kuryelik yaptığı ortaya çıkmıştır. Ele geçen film ve müzik Compact Disklerinin (CD) içine sakladığı gizli bilgileri şifreleyen örgüt üyesi

R.C. vicdan azabı çektiği için polisin çözemediği CD'lerdeki şifreleri kaldırınca gerçek ortaya çıkmıştır. Bu olay bir "Siber Terörizm" eylemi olarak değerlendirilebilir (Hürriyet, 2008).

1.1.1.4. Siber Emniyet

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB) tarafından yayımlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi Belgesinde "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini" siber emniyet olarak tanımlanmıştır (UDHB, 2016).

Siber Emniyet ülkelerin bilgi sistemlerini ve kritik altyapılarını gün geçtikçe daha fazla bilgi teknolojileri altyapısıyla oluşturmuş olmaları önemli bir koruma çabasını da beraberinde getirecektir. Özellikle 2025 yılında internet kullanıcısı sayısının 4 milyarı geçeceğine dair tahminler bu çabanın azımsanamayacak düzeyde olması gerektiğini göstermektedir (Yılmaz, Ulus, & Gönen, 2015).

1.1.1.5. Siber İstihbarat

"Siber istihbarat" geleneksel istihbarat anlayışından emek ve mali açıdan bazı farklılıkları bulunan, bilgi elde ederken avantaj sağlayan metotlar olarak değerlendirilmektedirler. Sinyal istihbaratı olarak da adlandırılan siber istihbarat, Amerika Birleşik Devletlerinin temel güvenlik kuruluşu olan Ulusal Güvenlik Teşkilatının (NSA) yaklaşık 40bin çalışanıyla dünya çapında yaptığı bilgi toplama faaliyetidir (Ersanel, 2001).

1.1.1.6. Siber Suç

Bilgisayar, bilgi teknolojileri ve yüksek teknoloji suçları gibi isimlerle de tanımlanmaktadır. "Siber suç" hedefin bilgisayar olduğu ya da geleneksel bir suçun bilgisayar kullanılarak işlenmesi şeklinde iki ana başlık altında incelenir (Goodman & Brenner, 2002). Kabul gören ve yaygınca kullanılan terim "siber suçlar"dır (Moitra, 2005).

Siber suçlarla mücadele alanında çok önemli bir belge olan ve Avrupa Birliği (AB) tarafından 2001'de imzalanan ve 2004 yılında yürürlüğe giren "Sanal Ortamda İşlenen Suçlar Sözleşmesi"ni ülkemiz 2010 yılında imzalamıştır. 2014 yılında Resmi Gazete'de yayımlanması ile yürürlüğe girmiştir (TBMM, 2014b). Bu belge Avrupa Konseyi (EC) tarafından imzaya açılmış olmasına rağmen Avrupa'da bulunmayan ABD, Kanada, Avustralya, Japonya, Şili, İsrail, Senegal, Sri Lanka, gibi ülkeler de hukuksal anlamda yürürlüğe koymuşlardır (EC, 2001).

1.1.1.7. Siber Saldırı

Verinin değiştirilmesi, çalınması, erişimin kısıtlanması/kesilmesi gibi durumların siber ortamdaki veri üzerinde yetkisiz yapılması işlemidir. Saldıranın genelde fiziksel sonuç beklentisinde olduğu siber saldırılar aşağıdaki gibi sınıflandırılabilir (Janczewski & Colarik, 2008):

- Virüs saldırıları,
- E-Kamu hizmetlerinin kesintiye uğratılması,
- E-Kamu hizmetlerinin değiştirilerek dezenformasyona ya da propagandaya neden olunması,
- Elektronik tabanlı bir bilişim sistemine yetkisiz erişim,

Bir siber saldırı ile ilgili temel sınıflandırma aşağıdaki şekilde yapılabilir (Çakmak & Demir, 2009; Çifci, 2013; Clarke & Knake, 2011b; Ersanel, 2001):

- Saldırı Araçları:
  - Virüs (Virus),
  - Truva Atı (Trojen),
  - Solucan (Worm),
  - Klavye Kaydedici (Keylogger),
  - Casus Yazılım (Spyware),
  - Botnet,
  - Exploit,

- Rootkit
- Sniffer (Koklayıcı)

- Saldırı Yöntemleri:
  - Hizmet Dışı Bırakma (Denial of Service - DOS),
  - Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service - DDOS),
  - Oltalama/Yemleme (Phishing),
  - Sosyal Mühendislik (Social Engineering),
  - Arka kapı (Backdoor),
  - Kabloya saplama yapma (Wire Tapping),
  - Yerine Geçme (Masquerading),
  - Hukuka Aykırı İçerik Sunulması,
  - Salam Tekniği (Salami Techniques),
  - Çöpe Dalma (Scavenging),
  - Veri Aldatmacası (Data Diddling),
  - Tarama (Scanning)
- Siber Saldırıların Muhtemel Sonuçları:
  - Dijital Verinin Çalınması,
  - Dijital Verinin Eksilmesi,
  - Dijital Verinin Değiştirilmesi,
  - Dijital Verinin Kullanılamaz Hale Getirilmesi,
  - Dijital Verinin Gizliliğinin İhlali,
  - Sistemin Durması,
  - Sistemin Kesintiye Uğraması,

1.1.1.7.1. Siber Saldırı Araçları

1.1.1.7.1.1. Virüs (Virus)

Çalıştırıldığında kendisini bulunduğu bilgisayarda ya da diğer bilgisayarlara ya da diğer kod ağaçlarının içerisine kendisini kopyalamaya çalışarak bulaşma diye tabir edilen faaliyeti gerçekleştiren yazılım parçası ya da bütünüdür (William & Brown, 2015).

1.1.1.7.1.2. Truva Atı (Trojen)

Faydalı bir amaç için var oluyor görünen ancak kullanıcıdan gizli olarak kullanıcı bilgilerini/erişim haklarını gizli bir şekilde ele geçiren bu yönüyle de Klasik Truva Atı mitine benzeyen programdır (Landwehr, Bull, Mcdermott, & Choi, 1994).

1.1.1.7.1.3. Solucan (Worm)

Bağımsız bir şekilde çalışabilen ve ağdaki diğer bilgisayarlarda kendisini çoğaltabilen, genel olarak hedef sistemdeki zayıflıkları kullanarak bulaşan bilgisayar programıdır. Sürekli bulaşabileceği yeni hedefler arama özelliğine sahiptir (William & Brown, 2015).

1.1.1.7.1.4. Klavye Kaydedici (Keylogger)

Klavyeden yapılan her türlü hamle kayıt altına alarak bir yere aktarabilen ya da depolayabilen yazılım ya da donanıma denir. Şifre hırsızlığı (E-posta, kredi kartı, Hassas projelere/sistemlere giriş vb.) amacıyla yaygın olarak kullanılır. Donanım olarak kullanıldığı durumlarda klavyenin kişisel bilgisayara (PC) bağlandığı noktada ikisinin arasında takılarak kullanılır. (Baraz & vd, 2013)(Subramanyam, Frank, & Galli, 2017).

1.1.1.7.1.5. Casus Yazılım (Spyware)

Farklı hedeflere dönük olarak kullanıcı bilgilerini ve faaliyetlerini izleyen, toplayan ve ileten yazılımlardır. Geçmişten günümüze etkin olarak kullanılmaya devam edilmektedir. Öncelikle açıklık tespiti yapılır ve bu açıklıklar kullanılarak sistemlere sızılır. Sonrasında elde edilen bilgilerin iletimi sağlanır (Altunok & Katman, 2009).

1.1.1.7.1.6. Botnet

Başka bir noktadan yönetilen zombi haline getirilmiş bilgisayarlar olarak da tanımlanabilirler. Bir noktadan zombi haline getirilmiş birçok bilgisayarın yönetilebilmesi mümkündür. Ele geçmiş her bir bilgisayara zombi, zombi bilgisayarları yöneten noktaya/kişiye/bilgisayara ise botmaster adı verilir. (Bıçakçı, 2013).

1.1.1.7.1.7. İstismar Kodu (Exploit)

Hackerların herhangi bir bilgisayara yetkisiz giriş elde edebilmek için yaptığı saldırı türlerinin genel adıdır. Bu iş için mevcutta bulunan basit uygulamalar olduğu gibi ileri seviye hackerlar tarafından yazılmış uygulamalar da kullanılabilmektedir (Techopedia, 2017).

1.1.1.7.1.8. Rootkit

Genelde çekirdek (kernel) seviyesinde çalışan ve sistemdeki verileri sistemin bilgisi dışında alıp paylaşabilen kötücül yazılımlardır (Önal, 2012) Türkçe'ye tercüme edilirken "kök kullanıcı takımı" ifadesi kullanılan rootkit'in çekirdek düzeyinde çalışması tespit edilmesini zorlaştırmaktadır (Çifci, 2013).

1.1.1.7.1.9. Koklayıcı (Sniffer)

Bir bilgisayar ağındaki dijital olarak meydana gelen iletişimi kaydeder, kaydettiği veriler üzerinde inceleme yaparak özel verileri elde etmeye çalışır. Özellikle aynı kablosuz cihaza bağlı (aynı Yerel Alan Ağındaki (LAN)) cihazlarının birbirlerinin iletişimini takip edebilmeleri daha kolaydır (Canbek & Sağıroğlu, 2008a).

1.1.1.7.2. Siber Saldırı Yöntemleri

Asimetrik bir yapısı da bulunan siber suçlar klasik suçların aksine mekan bağımsız da işlenebilmektedir. Suçluların yakalanmasının daha zor olduğu siber dünyada işlenen suçlarla büyük zararlar meydana gelebilmektedir. (Dülger, 2004). Günden güne siber uzayda yeni saldırı araç türlerinin de türetilmesi nedeniyle bilinen araç türlerini tanımak çok önemlidir.

1.1.1.7.2.1. Hizmet Dışı Bırakma (Denial of Service – DOS)

Hizmetin verildiği hattın sürekli meşgul edilerek hizmetin hiçbir yere ulaştırılamaması ya da çok yavaş ulaştırılmasına neden olan saldırı türüdür. Genelde birden fazla noktadan hizmetin çıkış noktasına yapılır. Bu saldırı kritik bir altyapıya yapıldığında önemli sorunlara neden olmaktadır (Baraz & vd., 2013).

Zaman zaman ülkemizde de ses getiren DOS saldırıları yaşanmaktadır. 2012 yılında THY sitelerine yapılan saldırı büyük miktarda mali zararın yanında prestij kaybına neden olmuştur. 2012 yılında bu yöntemle 10'dan fazla kuruma saldırı gerçekleştirilmiştir (Milliyet, 2012; Tübitak, 2013).

1.1.1.7.2.2. Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service – DDOS)

Hizmet dışı bırakma saldırılarının birden fazla kaynak tarafından eşzamanlı olarak tek hedefe yapılmasıdır. Çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. 2015 yılı yılbaşı akşamı İngiliz yayın kuruluşu The British Broadcasting Company (BBC) büyük bir DDOS saldırına maruz kalmıştır. BBC 3 saat boyunca bu saldırılar nedeniyle hizmet verememiştir (Abusix, 2017).

1.1.1.7.2.3. Yemleme/Oltalama (Phishing)

Güven kazanarak bilgi edinme türlerinden birisidir. Birçok farklı şekilde yapılabilir. İngilizcesi "phishing" olan sözcük Türkçe'ye "yemleme" olarak çevrilmiştir. Örnek olarak herhangi bir bankanın web sitesinin bir kopyası yapılarak kullanıcıların hesap bilgilerini girmelerini sağlamak ve sonrasında elde ettikleri bilgilerle illegal yoldan kazanç elde etme ülkemizde de sıkça görülebilen bir yemleme saldırısıdır (Polonyadan, 2014; William & Brown, 2015).

1.1.1.7.2.4. Sosyal Mühendislik (Social Engineering)

İnsanın ustalıkla tasarladığı manevraları kullanarak istediğini elde etmesi olarak tanımlanmıştır (Hadnagy, 2010). Sosyal mühendisliğin bir ilişkiyi kullanarak/istismar ederek hedefe ulaşmak olarak tanımlandığı başka bir kaynakta bu başlık detaylandırıldığında "Bir şey her zaman bildiğiniz ya da tanıdığınız gibi değildir ya da bir ürün için aldığınız fiyat gerçekten iyi fiyat olmayabilir ya da bir tatil için kazandığınız bedava yer aslında ilginizi çekmek için hazırlanmış bir tuzağın insan tasarımı manevraları olabilir." çerçevesine önemli benzetmeler yapılmıştır. Hedef bir kişinin sosyal medya üzerinden zaaflarını öğrenerek bir reklam hazırlama ve bu kişiye e-posta ile bu reklamı göndererek şifrelerini elde etmeye yönelik yapılan bir yemleme saldırısı hem yemleme hem sosyal mühendislik içeren birleşik bir saldırı olarak değerlendirilmiştir (Dolan, 2004).

1.1.1.7.2.5. Arka Kapı (Backdoor)

Bir sistem ya da bilgisayara farklı yollarla yetkisiz erişim sağlayan yazılımlardır. Bir kere sisteme erişildiyse sürekli bu erişim yolu kullanılır ve düzenli olarak bilgi hırsızlığı faaliyeti yürütülür. Fark edilmesi zordur. Zafiyete neden olan uygulamada/işletim sisteminde yapılan güncellemelerle yazılımın erişimi son bulabilir (Canbek & Sağıroğlu, 2008b).

1.1.1.7.2.6. Kabloya Saplama Yapma (Wire Tapping)

Telefonun dolayısıyla iletişimin gizli amaçlarla dinlenmesi olayıdır. İnternet veya telefon iletişiminin mahkeme kararları ile dinlenebilmesinin yanında illegal olarak da kötü niyetli kişiler tarafından bu suçun işlendiği görülebilmektedir. Hattın güvenliğinin alınmış olması bu iletişimin dinlenmesini zorlaştırmaktadır (Sherr, Cronin, Clark, & Blaze, 2005).

1.1.1.7.2.7. Yerine Geçme (Masquerading)

Bu saldırı türünde sahte bir kimlikle öncelikle yetkili birinin yerine geçilir ve sisteme erişilmeye çalışılır. Bu saldırıyı gerçekleştirebilmek için öncelikle kullanıcı hesabı, parolası, kişisel diğer bilgiler gibi bazı bilgiler elde edilir (Techopedia, n.d.).

1.1.1.7.2.8. Hukuka Aykırı İçerik Sunulması

Birçok suç çeşidi (ırkçılık, kişisel bilgilerin gizliğini ihlal, insan ticareti, çocuk istismarı) içerik bilgisinin erişime açık bulundurulması suçudur. Ülkemizde özellikle Twitter, Youtube gibi büyük hizmet sağlayıcıların kişisel hakları ihlal etmeleri sonucunda sık sık yaptırıma maruz kalmaları bu suç kapsamında kabul edilmektedir (TBMM, 2007).

1.1.1.7.2.9. Salam Tekniği (Salami Techniques)

Bankalarda genel olarak ortaya çıkan bir saldırı türüdür. Banka sistemlerine sızma işleminden sonra hesaplarda bulunan paranın virgülden sonraki kısmının başka bir hesaba aktarılmasıyla uygulanır. Hesap sayısı arttıkça saldırganın kazancı büyür. Banka çalışanlarının şikayeti olmadığı sürece farketmeleri zor bir saldırı türüdür (Dülger, 2004).

1.1.1.7.2.10. Çöpe Dalma (Scavenging)

Çöpe atılmış herhangi bir müsveddeden veri elde etme, bir bellekteki silinmemiş verilerin elde edilmesi, verileri silinmiş bir belleğin ele geçmesi sonrasında yapılan veri kurtarma işlemiyle veri elde etme ya da yazıcıların belleklerinde kalan verilerin alınması işlemlerine denir (Yazıcıoğlu, 1997).

1.1.1.7.2.11. Veri Aldatmacası (Data Diddling)

Veride yapılan illegal ya da yetkisiz değişikliğe denir. Verinin önceki haliyle sonraki hali arasından değişiklik olması gerekir. Genel olarak banka kayıtları, emlak verilerinde, kredi kayıtların, okul transkriptlerinde vb. uygulamalarda görülür (Kabay, 2009).

1.1.1.7.2.12. Tarama (Scanning)

Herhangi bir hedefte ele geçirebilecek bilgilerin araştırıldığı saldırı türüdür. Sosyal mühendislik saldırılarının ön hazırlığı olarak da görülebilir. İlk olarak tarama

esnasında IP, Port bilgilerine bakılarak elde edilen verilerin değerlendirilerek daha kompleks saldırıların planlandığı bir aşamadır (Aydın, 1992).

1.2. Siber Olaylar

Geleneksel suç anlayışı siber alanın suç işleme amaçlı boyut genişletmesi nedeniyle suçla mücadelede önemli ölçüde yeni bir bakış açısına ihtiyaç duymaktadır. Suç sonrası suçlunun çok çabuk kamufle olabildiği, devletlerin devletlere savaş ilan etmeden saldırılarda bulunabildiği, savaşın ışık hızında gerçekleşebildiği bu yeni suç ortamının kullanım şekli konusunda yapılan bilgilendirme sonrasında bu ortam kullanılarak gerçekleşmiş olan ya da olduğu düşünülen olaylar bu bölümde incelenmiştir (Çifci, 2013).

1.2.1. Ülkemizde Yaşanmış Siber Olaylar

1.2.1.1. Batman Hidroelektrik Barajı (2003)

2003 yılında Batman Hidroelektrik Barajı'nın yapımını üstlenen firmanın yaklaşık 4 milyon dolar tahsil edemediği alacağını bahane ederek şirket bilgisayarlarını şifre ile kilitleyip şehri terk etmeleri ve sonuçta barajın üç ünitesinde enerji üretimin durmasıdır (Hürriyet, 2003a; Milliyet, 2003).

1.2.1.2. IMKB Hizmet Durması (2007)

Bir operatörün (kepçe operatörü) kavşak çalışması esnasında İMKB'nin fiber optik kablosunu koparması nedeniyle en az 24 saat süreyle hizmetin durması olayıdır. 28 Kasım 2007 tarihinde yaşanan olayı Hürriyet gazetesi "255 milyar dolarlık borsaya kepçe darbesi" başlığıyla duyurmuştur (Hürriyet, 2007).

1.2.1.3. Bakü Tiflis Ceyhan Boru Hattı Patlaması (2008)

BTC (Bakü Tiflis Ceyhan) boru hattında 2008 yılında meydana gelen patlama olayıdır. Patlama sonrasında bir terör örgütü sorumluluğu aldığını duyurmuş olmasına rağmen 2014 yılında Bloomberg isimli organizasyon, web sayfasından farklı bir iddiada bulunmuştur. Bloomberg'in isimlerini paylaşmadığı 4 kişilik kaynağa dayandırdığı haberinde bunun bir siber saldırı olduğu, öncelikle 60 saatlik kamera kaydının silindiği, patlama öncesinde elinde laptoplarla boruların etrafında dolaşan şahıslar bulunduğu, alarmların kapatıldığı ve siber anlamda sistemi zorlayacak talimatlar verildiği belirtilmiştir (Bloomberg, 2014).

1.2.1.4. Atatürk Havalimanı Hizmet Durması (2009)

30 Ocak 2009 tarihinde Windows işletim sisteminin açıklarından yararlanıp güncelleme yapılmamış olan sistemlere bulaşan ve USB disklerle yayılan "downadup" ismi verilen solucan Atatürk Havalimanı Dış Hatlar Terminali sistemlerinde soruna sebep olmuştur. SITA-CUTE adı verilen ve bilet, bagaj işlemlerinin yapıldığı sistemler işlemez hale gelince işlemler elle yapılmak zorunda kalınmış ve birçok yolcu bagajlarını havalimanından alamamıştır. Los Angeles, Miami, Oslo, JFK, Arlanda ve Bremen havalimanları da bu solucandan etkilenmişlerdir (Hürriyet, 2009).

1.2.1.5. Gümrük Sistemlerinin Çökmesi (2011)

Ülkemiz gümrük işlemleriyle ilgili işlemlerinin merkezi olarak faaliyet gösteren Gümrük Müsteşarlığı Merkezi Bilgi İşlem Sistemi'nin veritabanında oluşan arıza nedeniyle 1 Şubat 2011 18:30 ile 2 Şubat 2011 13:00 arasında kara sınır kapılarından araç geçişlerinin kontrolünü sağlayan veritabanları hizmet verememiştir. Kara sınır kapılarında gümrük işlemi gerçekleştirilemeyince sınır kapılarında kilometrelerce araç kuyrukları oluşmuştur. Bu olaydan bir süre önce yolsuzluk ve rüşvet soruşturması nedeniyle yedi gümrük müdürünün görevden alınmış olması içerden yapılmış bir siber saldırı olabileceği ihtimalini gündeme getirmiştir (Hürriyet, 2011).

1.2.1.6. Ülke Çapında Elektrik Kesintisi (2015)

Türkiye'de 2015 yılında 6,5 saat süren ve neredeyse tüm ülkeyi etkileyen (İran'dan elektrik alan Van gibi bir kaç yerleşim yeri hariç) geniş çaplı bir elektrik kesintisi yaşanmıştır. Kesintinin nedeni üzerine resmi raporda yedekli çalışan sistemde 4 hattan üçünde hırdavat takılması birinde ise bakım nedeniyle servis dışı kalması bahane gösterilmiştir. Ancak kesintinin siber saldırı nedeniyle de yaşanmış olabileceği iddiaları ortaya atılmıştır. Observer'in bir malware kullanılarak saldırı yapıldığını ve bu saldırıyı İran'ın yaptığını belirtmesi akıllarda soru işareti oluşmasına neden olmuştur (NTV, 2015; Observer, 2015).

1.3. Nükleer Alan

1.3.1. Ulusal ve Uluslararası Kuruluş ve Anlaşmalar

1.3.1.1. Uluslararası Atom Enerjisi Ajansı (UAEA) ve Birleşmiş Milletler (BM)

Birleşmiş Milletler Örgütü ya da kısaca Birleşmiş Milletler (BM, United Nations-UN), 1945'te uluslararası barışı ve güvenliği sağlamak, insan haklarını korumak, insani yardım ulaştırmak, sürdürülebilir geliştirme ortamını sağlamak, uluslararası yasaları sürdürmek amaçlarıyla kurulmuştur. Günümüz itibariyle üye sayısı 193 olan örgüte Türkiye kurucu üye olarak 1945 yılında katılmıştır. Birleşmiş Milletler anılan görevlerini New York'ta bulunan genel merkezinden yürütülür ve üye ülkelerle her yıl düzenli olarak yapılan toplantılar yine bu genel merkezde gerçekleştirilir. Ayrıca Cenevre, Viyana ve Nairobi'de de ofisleri bulunmaktadır (UN, 2017b).

Uluslararası Atom Enerjisi Ajansı (UAEA, International Atomic Energy Agency-IAEA), Birleşmiş Milletler bünyesinde faaliyet gösteren bağımsız, uluslararası bilim ve teknoloji temelli bir organizasyon olup 29 Temmuz 1957 yılında kurulmuştur. Nükleer Bilim ve Teknolojinin barışçıl amaçlarla kullanılması ve planlanmasında üye ülkelere destek sağlamaktadır. Nükleer Güvenlik Standartlarını hazırlamaktadır. Bünyesindeki denetim mekanizması ile ülkelerin taahhütlerini yerine getirmesini kontrol etmektedir. Türkiye'nin de dâhil olduğu 168 üye devleti vardır. UAEA Tüzüğü 23 Ekim 1956'da Genel Konferansta onaylanmış, 29 Temmuz 1957 'de yürürlüğe girmiştir. Türkiye, 1957 yılında tüzüğünü onaylamak suretiyle UAEA'na üye ülkeler arasında yer almıştır. Nükleer santraller UAEA'nın yapacağı denetimlere açıktır (ETKB, 2016; TAEK, 2017h; UAEA, 2017d).

Nükleer Güvenlik ve Emniyet Dairesinin altında Nükleer Emniyet Şubesinin içerisindeki Bilgi Yönetimi Birimi tarafından santrallerin siber emniyeti ile ilgili süreçler takip edilmekte ve koordinasyon sağlanmaktadır. Direkt olarak siber güvenlik dairesi adıyla bir birim kurulmamış olup siber emniyet fiziksel emniyet içerisinde değerlendirilmektedir (UAEA, 2017d; UN, 2017b).

1.3.1.2. Siber Olaylara Müdahale Ekibi (CERT – Computer Emergency Response Team)

CERT (Computer Emergency Response Team - Bilgisayar Acil Durum Müdahale Ekibi ya da Siber Olaylara Müdahale Ekibi(SOME)) ya da

CSIRT(Computer Security Incident Response Team – Bilgisayar Emniyeti Olayların Müdahale Takımı) kısaltmalarıyla bilinmektedirler 1988 yılından Carnegie Mellon Üniversitesi Yazılım Mühendisliği Bölümü içerisinde hükümet fonuyla kurulan ve kar amacı gütmeyen bir kuruluştur. CERT adının patent haklarına sahip olan kuruluş içerisinde kısa süre sonra The CERT/CC (Computer Emergency Response Team Coordination Center) isimli ve uluslararası hedefli bir koordinasyon merkezi kuruldu. CERT ve CSIRT kısaltmalarının yayılması sonrasında 2003 yılında ABD İç Güvenlik Bakanlığı içerisinde US-CERT kuruldu ve The CERT/CC kapasitesini kullanarak ABD adına siber saldırıların önlenmesi, sistemlerin korunması ve müdahale süreçlerine katıldı. Bu kuruluş ülkemizdeki USOM'la (TR-CERT) benzer görevlere sahiptir (CarnegieMellonUni, 1989; FIRST, 2017; US-CERT, 2017).

Zafiyet analiz yazılımları konusunda da geliştirmeler yapan kuruluş bu yazılımların bir bölümünü ücretsiz olarak yayınlamaktadır. Ulusal bir CSIRT oluşturmak için yapılması gerekenlerin adım adım anlatıldığı, ulusal bilgisayar emniyeti olaylarıyla mücadele yönetimi konularında farklı klavuzlar yayımlanmış olup bu klavuzlarda ayrıca başarılı uygulamalar, kamu kurumlarının, akademik dünyanın, üreticilerin, sektörlerin ve yabancı ülkelerin iletişimleri konusunda öneriler bulunmaktadır (CarnegieMellonUni, 2004; Haller, Merrell, Butkovic, & Willke, 2011; West-Brown et al., 2003).

1.3.1.3. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA - European Union Agency for Network and Information Security)

2004 yılında Avrupa Parlamentosu ve Konseyinin kararıyla Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA - European Network and Information Security Agency) adıyla kurulmuş 2013 yılında yapılan düzenlemeyle adı Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA - European Union Agency for Network and Information Security olarak değiştirilmiştir (European Parliament v Council, 2004, 2013).

ENISA tüm Avrupa'ya siber emniyet alanında uzmanlık ve Avrupa Komisyonunun Ağ ve Bilgi Emniyet alanında yapacağı yasal düzenlemelerde güncelleme ve geliştirme desteği veren bir kuruluştur. Üye ülkelerle ve sektördeki kuruluşlarla işbirliği içerisinde faaliyet yürüten ajans Siber Emniyet Tatbikatları, her üye ülke için Ulusal Siber Emniyet Stratejileri, CSIRT isimli merkezlerin koordinasyonu ve güçlendirilmesi faaliyetleri yürütmektedir (ENISA, 2017).

ENISA koordinasyonunda birçok Siber Emniyet Tatbikatı düzenlenmiştir. Her ülkeden siber alanla ilgilenen bakanlıklar, siber alanda düzenleme yapmaktan sorumlu yetkili otorite, istihbarat servisleri, siber suç birimleri, CERT birimleri ve özel sektörün katılımıyla 2010 yılından beri 2 yılda bir düzenli olarak tatbikatlar yapılmaktadır. Her yeni tatbikatta büyüyen organizasyonda 2016 tatbikatına CSIRT takımları, siber emniyet birimleri, AB kurum ve ajansları, bakanlıklar, internet ve bulut hizmeti veren servis sağlayıcılar, siber emniyet yazılım ve servis sağlayıcılar, bankalar, enerji şirketleri ve diğer kritik altyapı operatörleri olmak üzere 30 Avrupa ülkesi (28 AB üyesi, Norveç ve İsviçre), 300'den fazla organizasyon katılmıştır (ENISA, 2016).

1.3.1.4. Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (NPT Treaty on the Non-Proliferation of Nuclear Weapons)

1968 yılında imzaya açılan ve 1970 yılında yürürlüğe giren, Nükleer Silaha Sahip Ülkelerin bu silahları ve teknolojisini paylaşmayacağının, Nükleer Silaha Sahip Olmayan Ülkelerin ise bu tip silahlanmaya gitmeyeceğinin, nükleer teknolojinin barışçıl amaçlarla kullanılacağının, UAEA'ya bu anlamda denetim yetkisinin verildiğinin taahhüt edildiği bir anlaşmadır. Ülkemizde "Nükleer Silahların Yayılmasının Önlenmesi Antlaşmasının Onaylanmasının Uygun Bulunduğu Hakkında Kanun"un 1979'da yürürlüğe girmesiyle hukuken uygulanmaya başlamış olan bu anlaşmayı bugün itibariyle 191 ülke onaylamıştır. Bu anlaşma ile 5 ülkenin nükleer silaha sahip olduğu kabul edilmiştir. Bu ülkeler Çin, Fransa, Rusya, Birleşik Krallık ve Amerika Birleşik Devletleridir (NTI, 2017a; TBMM, 1979; UN, 2017b).

1.3.1.5. Nükleer Madde ve Tesislerin Fiziksel Korunması Sözleşmesi (CPPNM Convention On The Physical Protection of Nuclear Material And Nuclear Facilities)

Sözleşme, "Özel Nükleer Maddelerin Fiziksel Korunması Sözleşmesi" (Convention On The Physical Protection of Nuclear Material) adıyla 8 Şubat 1987 tarihinde yürürlüğe girmiştir (UAEA, 2016a). Türkiye Sözleşmeye 1996'dan bu yana taraftır (Bakanlar Kurulu, 1996).

2005 yılında sözleşmede tesisleri de içerecek şekilde değişiklik yapılmış ve sözleşmenin adı "Nükleer Madde ve Tesislerin Fiziksel Korunması Sözleşmesi" olarak düzenlenmiştir. Aynı yıl ülkemiz tarafından imzalanan sözleşme 2012 yılında yürürlüğe girmiştir (TBMM, 2015b). Bu belge ile Uluslararası Atom Enerjisi Kurumu tarafından siber emniyetle ilgili hususlar "Bilgi Emniyeti" başlığı altında kural olarak belirtilmiştir (UAEA, 2016a).

1.3.2. Nükleer Enerji

İş yapabilme yeteneği ya da kapasitesi olarak tanımlanabilen enerji insanoğlu varoluşundan itibaren ihtiyaç duyduğu temel bir gereksinimdir. Elde edilen kaynağın yenilenebilir olması ve olmaması temel sınıflandırma olmakla birlikte yatırım maliyetleri, çevre kirliliği, insan sağlığı, coğrafi koşullar, doğal kaynaklar, teknolojinin elde edilebilirliği gibi faktörlerin ülkelerin enerji yatırımlarına yön vermektedir (ETKB, 2017b).

Koç ve Şenel tarafından enerji Yenilenemez ve Yenilenebilir Enerji olarak ikiye ayrılmıştır. Bu sınıflandırma içerisinde Yenilenemez Enerji başlığı altında Petrol, Doğalgaz, Kömür, Uranyum ve Toryum; Yenilenebilir Enerji başlığı altında ise Güneş, Rüzgar, Jeotermal, Hidroelektrik, Biyokütle, Hidrojen, Dalga ve Git-Gel Enerji türleri yer almıştır (KOÇ & ŞENEL, 2013). 2016 yılında dünya genelinde tüketilen toplam enerjinin %33'ü petrolden, % 28'i kömürden, % 24'ü doğalgazdan, %6'sı hidroelektrik santrallerden, %4'ü nükleer santrallerden, %3'ü ise diğer yenilenebilir enerji kaynaklarından üretilmiştir (BP, 2017).

Nükleer enerji üretiminin ülkelerin yıllık öz tüketimine katkısı açısından konu değerlendirildiğinde 13 ülkenin yıllık tüketiminin %25'ten fazlasını kendi ürettiği nükleer enerjiden karşılamaktadır. Dünyanın en çok nükleer reaktörüne sahip olan ABD yıllık tüketiminin ancak % 10'unu kendi ürettiği nükleer enerjiden karşılayabilmektedir. Bu 13 ülke ve ABD'nin enerji üretimlerindeki nükleerin oranı, aktif reaktör sayıları ve üretim güçleri çizelge 4-1'de sunulmuştur (EIA, 2017; NEI, 2017b).

Çizelge 1-1 Ülkelerin Nükleer Enerji Üretimin Tüketimdeki Payı, Aktif Reaktör Sayısı ve Nükleer Enerji Üretim Gücü (NEI, 2017b; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş, n.d.; UAEA, 2016b)

Sıra No	Ülke	Kendi Üretiminden Karşılanan Nükleer Enerji Miktar (2016 - %)	Aktif Reaktör Sayısı (2015)	Üretim Gücü (2015-MWe)
1	Fransa	72,3	58	63 130
2	Slovakya	54,1	4	1 814
3	Ukrayna	52,3	15	13 107
4	Belçika	51,7	7	5 913
5	Macaristan	51,3	4	1 889
6	İsveç	40	10	9 648
7	Slovenya	35,2	1	688
8	Bulgaristan	35	2	1 926
9	İsviçre	34,4	10	9 648
10	Finlandiya	33,7	4	2 752
11	Ermenistan	31,4	1	375
12	Güney Kore	30,3	24	21 733
13	Çek Cumhuriyeti	29,4	6	3 930
14	ABD	10	99	99 185

Nükleer enerji radyoaktif bir element olan uranyum atomunun çekirdeğinden elde edilen bir enerji türüdür. Temel olarak nükleer reaktörler ve santrallerde elektrik üretimi için kullanılır. Uranyum elementinin nötronla tepkimeye girmesiyle parçalanması ve yüksek ısının ortaya çıkmasının kullanılmasıyla enerji üretimi gerçekleşir (Tombakoğlu et al., 2011).

Nükleer Enerjinin dünyadaki tarihçesi incelendiğinde; uranyum maddesi 1789: Martin Klaproth tarafından uranyum bulundu ve 1986 yılında Fransız fizikçi Henri Becquerel tarafından kazara fotoğraf plakaları ile yan yana durması ve karanlıkta yayılan radyoaktif ışınların fark edilmesi ile radyoaktiflik özelliği keşfedilmiş ve Mendeleyev'in çalışmalarıyla radyoaktif olduğu ispatlanmıştır. 1942 yılında Chicago Üniversitesinde İtalyan Fizikçi Enrico Fermi'nin Manhattan Projesi'nin bir parçası olarak yaptığı testle ilk zincirleme nükleer reaksiyon gözlemlenmiştir. 1945 yılına gelindiğinde ABD New Mexico Çölünde kod adı "Trinity" olan ilk nükleer silahı testmiş ve sonrasında aynı yıl Japonya'nın Hiroşima ve Nagazaki kentlerine ilk atom bombası atılmıştır. Nükleer enerjiden ilk elektrik enerjisi üretim işlemi 1951 yılında ABD Idaho Eyaletinde deneysel bir üretken reaktörde gerçekleştirilmiştir. Nükleer enerjisinin bir denizaltında kullanılması ilk defa ABD tarafından 1955 yılında inşa edilen Nautilus isimli nükleer denizaltı ile gerçekleşirken, ticari bir nükleer reaktörden üretilen elektrik enerjisinin ilk şebeke bağlantısı 1954 yılında Rusya tarafından gerçekleştirildi. 1957 yılı Birleşmiş Milletler bünyesinde Uluslararası Atom Enerjisi Ajansı kuruldu. 1965 yılına gelindiğinde ise SNAP-10A isimli ilk nükleer reaktöre sahip uzay aracı uzaya gönderildi (Moore, Banuelos, & Gray, 2016; Ucael, 2015; Zararsız, 2005).

1.3.2.1. Uranyum

Uranyum elementinin doğada değişik izotopları ile karşılaşılabilir. En çok kullanılan 2 izotopu u-235 ve u-238 çekirdekleridir. Nükleer güç santralleri günümüzde yaygın olarak U-235 çekirdeklerinin fisyon yani bir nötron ile parçalanması sonucu ortaya çıkan enerjiyi elektriğe çeviren tesislerdir. U-235 çekirdekleri nötronlarla tepkimeye girmeleri sonucunda daha kararsız bir yapı, sonrasında bu yeni çekirdeğin daha kararlı iki veya üç çekirdeğe bölünmesiyle de enerji açığa çıkması sağlanır. Bu işlem esnasında açığa çıkan nötronların ortamda bulunan diğer U-235 çekirdekleriyle tepkimeye girmeleriyle birlikte de sürekli bir üretim sağlanır. Bu tepkime süreci de "Zincirleme Tepkime" olarak adlandırılır (Elektrikport, 2017; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş, n.d.; Tombakoğlu et al., 2011).

Uranyum kaynakları görünür üretim maliyetlerine göre sınıflandırılırlar. Üretim maliyeti kategorileri OECD/Nuclear Energy Association ve Uluslararası Atom Enerjisi Ajansı tarafından kg'ı 80 ABD dolarına mal edilebilen ve kg'ı 80-130 ABD dolarına mal edilebilen şekilde sınıflandırılmıştır (UAEA, 1998a).

2014 yılı verilerine göre dünyada bu şekilde hesaplanan 5,90 milyon ton görünür uranyum rezervi vardır. Uranyum rezervi açısından dünyayı incelediğimizde toplam rezervin %50'si Avustralya (%29), Kazakistan (%12) ve Rusya'da (%9) bulunduğu bildirilmektedir (OECD NEA & UAEA, 2004).

2012 yılında 21 ülke uranyum ürettiği bu ülkelerden 9 tanesinin dünyadaki üretimin %93'ünü karşılamakta olduğu en belirgin üreticilerin Kazakistan, Kanada ve Avustralya olup bu 3 ülke dünyadaki üretimin %63'ünü karşıladığı bildirilmektedir (DPT, 1996; TAEK, 2017e).

Türkiye'de uranyum aramalarına 1990 yılı sonuna kadar devam edilmiş ve 5 yatakta toplam 9.129 ton görünür uranyum rezervi ortaya konulmuştur. Bu 5 yatağın ortalama tenör (Rezerv, Yatağın Durumu (Yüzeye yakınlık, çevresel faktörler...), Pazara Mesafe, Piyasa Değeri, Üretim Masrafları ve Diğer Tüm Masraflar)ve rezervleri, o yıllarda, ekonomik sınırlarda iken bugün nükleer santral planlamalarındaki önemli değişmeler ve özellikle Kanada ve Avustralya'da yüksek tenörlü, üretim maliyetleri çok düşük uranyum yataklarının bulunmasıyla ekonomik sınırların altında kalmıştır (NükleerAkademi, 2017a)

1.3.2.2. Uranyum Zenginleştirme

Uranyum yataklarında U-235 ve U238 çekirdekleri bir arada bulunur. Doğadaki toplam uranyum oranının binde yedisini (%0.7) U-235 çekirdekleri binde dokuzyüzdoksanüçünü(%99.3) U-238 çekirdekleri oluşturur (UAEA, 2005).

Nükleer reaktörler yakıt olarak sıklıkla % 0,7 ile %3-5 arasında yoğunluğa sahip (U-235 açısından zenginleştirilmiş) uranyum U-235 çekirdeği kullanmaktadır. Uranyum elementinin U-235 çekirdeği açısından zenginleştirme yoğunluğuna göre Çizelge 4-2'de belirtildiği gibi Düşük ve Yüksek Seviye Zenginleştirilmiş Uranyum olarak ikiye ayrılmıştır.

Zenginleştirme işlemi konusunda bugüne kadar Gaz Difüzyonu ve Gaz Santrifüjü olmak üzere 2 yöntem kullanılmıştır. Gaz Difüzyonu yönteminin kullanıldığı tesisler günümüzde teknolojik olarak eski sayılması daha maliyetli oluşu gibi nedenlerle yerini Gaz Santrifüjü yöntemini kullanan tesislere bırakmıştır (TAEK, 2017e).

Çizelge 1-2 Uranyum Elementinin Zenginleştirme Oranına Göre Kullanım Yerleri (Jaffer, 2011; Moore et al., 2016; WNA, 2015)

Sıra No	Zenginleştirilmiş Uranyum Sınıfı	Zenginleştirme Oranı	Kullanım Alanı
1	LEU (Düşük Seviye Zenginleştirilmiş Uranyum - Low Enriched Uranium)	% 0,7 - % 20 arası	Nükleer Santral, Araştırma Reaktörü, Askeri Denizaltı
2	HEU (Yüksek Seviye Zenginleştirilmiş Uranyum - High Enriched Uranium)	% 20 ve üzeri	Uçak Gemisi, Askeri Denizaltı, Nükleer Silah

Amerika Birleşik Devletleri, Arjantin, Brezilya, Çin, Fransa, Almanya, Pakistan, Japonya, Hollanda, Rusya ve İngiltere gibi ülkeler tesis sayıları Çizelge 4-3'te de belirtildiği üzere uranyum zenginleştirme tesisi işleten ülkelerdir. Bu ülkelerden İsrail, Kuzey Kore ve İran'ın Uranyum Zenginleştirme programlarını gizlilik içerisinde yürütmeleri nedeniyle bu alandaki durumları/kapasiteleri net olarak bilinmemektedir (UAEA, 2009b).

Zenginleştirilme işleminden arta kalan Uranyum-238'e *indirgenmiş* veya Zayıflatılmış Uranyum denir. Zayıflatılmış uranyum doğal uranyumdan daha az

radyoaktiftir ve özellikle sert zırhların ve zırh delici mermilerin üretiminde veya metal sanayiinde yoğunluk olarak yüksek alaşımların üretimi ve işlenmesinde kullanılmaktadır (TAEK, 2017e; WNA, 2015).

Çizelge 1-3 Dünya'daki Başlıca Uranyum Zenginleştiren Ülkeler* ve Kapasiteleri (TAEK, 2017e; UAEA, 2009b; Wise-Uranium, 2017)

Sıra No	Ülke	Tesis Adedi	Kapasite (1000 SWU[1]/yıl)
1	ABD	1	11 300
2	Almanya	1	1 800
3	Çin	2	1 000
4	Fransa	1	10 800
5	Hollanda	1	3 500
6	İngiltere	1	4 000
7	Japonya	1	1 050
8	Pakistan	1	5
9	Rusya	4	15 000

*Bu ülkeler dışında Arjantin, Brezilya, Hindistan, İran, Kuzey Kore gibi ülkelerin de uranyum zenginleştirme tesisi işlettiklerine dair açık kaynaklarda bilgiler bulunsa da UAEA kayıtları baz alınarak tablo hazırlanmıştır.

[1] SWU – Seperative Work Unit: Zenginleştirme sürecinde santrifüj ya da gaz difüzyonu donanımlarının girdi miktarı, zenginleştirilmiş çıktı ve atıkların toplam miktarından elde edilen bir hesaplama verisidir.

1.3.2.3. Nükleer Reaktör ve Santraller

Nükleer reaktörler zenginleştirilmiş uranyum çekirdeklerinin kullanılmasıyla elektrik üretiminde 1950'li yıllardan beri kullanılan tesislerdir. Nisan 2017 yılı itibariyle dünyada 30 ülkede toplam 449 adet aktif, 15 ülkede toplam 60 adet inşa haline reaktör bulunmaktadır (NEI, 2017b).

Reaktörlerin gücü ifade edilirken üretmiş olduğu elektrik enerjisinin MW (Megawatt) değeri esas alınır. Araştırma reaktörleri saatte 0-100 MW aralığında ticari reaktörler ise saatte 20-1561 MW aralığında yıllık net enerji üretimi gerçekleştirirler. Bu değerlerin daha anlaşılabilir olması açısından ülkemizin 2016 yılında saatte 278 milyon MW elektrik tüketmiştir (NTI, 2017b; Tombakoğlu et al., 2011; UAEA, 2016b).

Nükleer santraller ise nükleer enerjiyle açığa çıkan hammaddelerin kullanıldığı enerji üretim tesisleridir. Nükleer reaktör (buhar kazanı, reaktör kabı), buhar türbini, elektrik jeneratörü, yoğuşturucu, atık birimleri ve diğer güvenlik ve idari birimlerden oluştur. Reaktörlerin güçlerinin toplamı doğrultusunda toplam güç hesaplanır. Nükleer yakıt çubuklarının tepkimeye sokulmasıyla elde edilen ısı enerjisi ile (266^0-300^0 C arasında) suyun sıcaklığı arttırılır, suyun yüksek enerjili buharı ile türbinler döndürülerek elektrik enerjisine çevrim işlemi gerçekleştirilir (NRC, 2017g).

Buharın hızlı bir şekilde suya dönüştürülebilmesi(soğutma ihtiyacı) için nükleer santraller genel olarak deniz, göl ya da nehirlerin kenarına kurulur. Santrallerde

enerjiyle ısınan suyun kaynamasının engellenmesi için 150 atm'ye kadar basınç uygulanmaktadır (UAEA, 2012).

İlk kamu şebekesine elektrik veren santral 1954 yılında açılmış olan Rusya'nın Obninsk Santrali olup ticari amaçla kurulmuş ilk santral ile 1956 yılında İngiltere'de açılmış olan Calder Hall Santrali'dir. Çalışan en yaşlı santral 7 Kasım 1967 yılında hizmete girmiş olan İngiltere'deki Oldbury Santralidir. 7 reaktörüyle 8121 MW toplam kurulu kapasiteye sahip olan Japonya'daki Kashiwazaki Santrali en güçlü santraldir. Tek başına en güçlü reaktör ise 1561 MW brüt kapasiteye sahip olan Fransa'daki Civaux 2 reaktör ünitesidir (WNA, 2017d). Ayrıca dünyada Çizelge 4-4'te üretilen güç bakımından Dünya'daki en iyi 10 ülkenin reaktör bilgileri sunulmuştur.

Çizelge 1-4 Reaktör Sayıları (UAEA, 2016b)

Sıra No	**Ülke**	**Çalışan Reaktörler**		**İnşa Halindeki Reaktör Sayısı**	**Kapatılan Reaktör Sayısı**
		Reaktör Sayısı	**Üretilen Güç MWe**		
1	ABD	99	99.185	5	33
2	Fransa	58	63.130	1	12
3	Çin	31	26.774	24	-
4	Rusya	35	25.443	8	5
5	Güney Kore	24	21.733	4	-
6	Kanada	19	13.524	-	6
7	Ukrayna	15	13.107	2	4
8	Almanya	8	10.799	-	28
9	İsveç	10	9.648	-	3
10	İngiltere	15	8.918	-	30
11	Diğer	127	90.594	23	36
	TOPLAM	441	382.855	67	157

1.3.2.4. Nükleer Santral İşletme, Lisanslama,

Ülkenin yetkili otoritesi tarafından bir nükleer santralin tüm süreçlerini -nükleer sit alanı santralin tüm faaliyetlerinin sonlanıp tüm radyolojik tehdidin son bulmasına kadar - kontrol etmesi amacıyla lisans verilen özel ya da tüzel kişiliğe kurucu adı verilir. Kurucu, nükleer güvenlik ve nükleer emniyetin tam olarak sağlanmasında daima sorumluluk sahibidir. Ülkenin yetkili otoritesi nükleer güvenlik ve emniyetle ilgili kurucunun faaliyetlerini denetleme, test sonuçlarını değerlendirme testleri tekrarlatma, yaptırım ve lisanslama iptali gibi haklarını daima saklı tutar. (EDAM, 2011).

Akkuyu NGS'nin işletme esnasında 2500, bakım onarım dönemlerinde 1200 çalışanı inşaat döneminde ise 10.000 çalışanı istihdam edeceği öngörülmektedir. Bir nükleer reaktörün yılda en az bir defa yakıt değişimi ve bakım için durdurulması, üç yılda bir defa da reaktör gövdesinin de kontrolden geçirildiği geniş kapsamlı bakıma alınması gerekmektedir (ETKB, 2016; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş, n.d.; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş., n.d.).

Ülkemizde 13 Temmuz 1982 tarih ve 2690 sayılı Türkiye Atom Enerjisi Kanunu ile Türkiye Atom Enerjisi Kurumu ülkemizdeki yetkili otorite olarak belirlenmiştir. Ayrıca ülkemizde nükleer bir tesisin işletmeye alınabilmesi için kurucunun almasına ihtiyaç duyulan lisanslar ilgili tüzükte 3 başlıkta toplanmıştır (TBMM, 1983):

1. Yer Lisansı
2. İnşaat Lisansı
3. İşletme Lisansı

Yine ülkemiz yasal mevzuatında işletmecinin sorumluluğu tehlike sorumluluğu olarak adlandırılmakta ve bu sorumluluk türü kusursuz sorumluluk hallerinin en ağır türünü oluşturur. (Tiftikçi, 2005)

Ayrıca yetkili otoriteden alınacak lisanslar dışında kurucu sorumluluğunda olan Çevresel Etki Değerlendirmesi, ülkenin yetkili otoritelerinin inşaat ve işletmeye ilgili prosedürleri (Belediyelerin, ETKB, EPDK inşaat/lisans prosedürleri), ülkenin bağlı bulunduğu uluslararası anlaşmaların ve organizasyonların prosedürleri, radyoaktif maddelerin ithalatı ve ihracatına ilişkin yasal prosedürler toplu olarak lisanslama sorumluluğu içerisinde kabul edilir (EDAM, 2011).

1.3.2.5. Nükleer Hizmetten Çıkarma/Faaliyet Durdurma/Kapatma

Nükleer santraller ortalama 40-60 yıl arasında bir çalışma süresi için tasarlanırlar. Akkuyu NGS'nin 2020 yılında işletme süresi 2020-2083 arasını kapsayan 63 yıl olarak hesaplanmıştır. Hizmetten çıkarma işlemi lisans alımı esnasında yeterince hesaba katılmayan bir sorundur. Oysa santralin işletmede olduğu süreç içerisinde hizmetten çıkarma sürecinin de planlanması gerekir. Ekonomik ve sosyal maliyetleri yüksek bir işlemdir. İlk yatırım maliyetinin yaklaşık %10-20'sine karşılık gelmektedir (EDAM, 2011; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş, n.d.; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş., n.d.; UAEA, 2014a).

Farklı isimlerle anılan bu işlem lisans sahibi şirketin üretimi durdurması ile başlayan ve nükleer sit alanının halkın artık radyasyondan korunmasını gerektirmeyecek seviyede arındırılması işlemidir. Bu işlem sonuçlanıncaya kadar tüm sorumluluk lisans sahibindedir. Bütün radyoaktivitenin temizlenmesi, santralin sökülmesi, radyoaktivite içeren her bir parçanın güvenli depolama alanlarına götürülmesini kapsar. (UAEA, 2010b).

DECON (Dekontaminasyon): Derhal yapılan sökme işlemidir. Operasyonlar biter bitmez sökme başlar. Yaklaşık 9 yıl sürer. Diğer hizmetten çıkarma yöntemlerine göre daha maliyetli, çalışacak kişilerin radyasyona maruz kalma ihtimali daha yüksek, daha geniş bir radyoaktif atık depolama alanına ihtiyaç duyulur. 4 dönemi kapsar (UAEA, 1999):

- Kapatma öncesi planlama ve mühendislik
- Santral deaktivasyonu ve depolamaya ilişkin hazırlıklar
- Santralde güvenli depolama ve kullanılmış yakın havuzu envanteri sıfırlama operasyonları
- Sökme işlemleri

SAFSTOR: Derhal yapılmaz. Bir süre radyoaktif komponentler tesiste bekletilir. Sonrasında radyoaktivitesi devam eden komponentlerin sökme işlemleri gerçekleştirilir. Çalışacak personelin radyasyona maruz kalma ihtimali düşüktür, ihtiyaç duyulacak radyoaktif atık depolama alanı daha küçüktür, 60 yıl sürer, 60 yıl sonra yapılacak sökme işlemi için tesisi tanıyan personel sayısı bir dezavantajdır (EDAM, 2011).

- Kapatma öncesi planlama ve mühendislik
- Santral deaktivasyonu ve depolamaya ilişkin hazırlıklar

- Santralde güvenli depolama ve kullanılmış yakın havuzu envanteri sıfırlama operasyonları
- 50 yıl güvenli bekleme süresi
- Radyoaktivitesi devam eden komponentlerin sökülmesi.

Lisansın sona ermesi sonrasında radyoaktif olmayan tesislerin demontesi tesis sahibinin takdirine bırakılır.

ENTOMB: Radyoaktif kontaminantların beton gibi dayanıklı bir malzemenin içerisine gömülmesi işlemidir. Gömme işlemi sonrasında tesisin diğer alanlarının 100 yıl kadar sonra kullanıma açılması hedeflenir. İhtiyaç duyulacak radyoaktif atık depolama alanı yoktur (UAEA, 2014a).

- Kapatma öncesi planlama ve mühendislik
- Santral deaktivasyonu ve depolamaya ilişkin hazırlıklar
- Santralde güvenli depolama ve kullanılmış yakın havuzu envanteri sıfırlama operasyonları
- Gömme hazırlıkları ve radyoaktif malzemelerin taşınması
- 60 ila 300 yıl depolama

Hizmetten çıkarma maliyetleri ile ilgili ülkelere göre elde edilen bulgular:

- 1998 dolar değeriyle ABD'de reaktör başına 325 milyon dolardır.
- Fransa'da 70 MW'lık bir santralin maliyeti ilk başta 24 milyon Euro planlanmışken işlemler başladıktan sonra 480 milyon Euro'yu bulmuştur (Brennilis NGS).
- Almanya'da 100 MW'lık bir santralin hizmetten çıkarma maliyeti 143 milyon Euro'yu aşmıştır (Niederaichbach).
- İngiltere'deki 32 MW'lık bir santralin hizmetten çıkarma maliyeti 117 milyon Euro'yu bulmuştur (Windscale).

(EDAM, 2011; NRC, 2017d; Perrier, 2017; TAEK, 2017a)

1.3.2.6. Kullanılmış Yakıt ve Nükleer Atık

Genel olarak santralden çıkan yakıtın %1', U-235, %90dan fazlası U-238 ve %05-1 arasındaki kısmı Plütonyum ve küçük miktarda aktinit bulundurur. Bu çıktıların büyük kısmı yeniden işleme tesislerinde yakıt haline getirilir ve santrallere kullanılması amacıyla gönderilir (Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş., n.d.; TAEK, 2017c).

Geriye kalan küçük kısmı (yüksek radyoaktiviteye sahip atık) bir süre soğutularak depolandıktan sonra camlaştırılarak paslanmaz çelik kaplarda sürekli soğutulan ve radyasyon seviyesi sürekli kontrol edilen geçici depolarda depolanır. Nihai depolama için gelecekte yerin yaklaşık 600-1000 m altında, yer altı sularının bulunmadığı ve deprem riski olmayan kayalık bölgelerde oluşturulmuş depolama alanları kullanılacaktır (TAEK, 2017d).

Yeraltı depolaması konusunda ABD 1999'da ilk tesisini açmış olup Finlandiya ise 2020'de açacağını duyurmuştur. Bu ülkelerin dışında yer altı depolama tesisi açan herhangi bir ülke bulunmamaktadır (TAEK, 2017b).

1.3.3. Nükleer Emniyet

Nükleer Emniyet terimi ile Nükleer Güvenlik terimi sıklıkla anlamsal olarak birbirleriyle karıştırılmaktadır (UAEA, 2007). Bu sebeple bu bölümde ilk olarak bu ayrımın net ortaya konulduğu değerlendirmeler yapılmıştır.

Nükleer Güvenlik "Nükleer kazaların önlenmesi, nükleer kaza sonuçlarının tüm olumsuz etkilerinin azaltılması, radyasyonun zararlı etkilerinden çalışanların, halkın ve çevrenin etkilenmesinin engellenmesi, doğru işletme şartlarının kazanılması olarak tanımlanmaktadır. Güvenlik normal şartlardaki riskler, olay sonrası riskler, reaktör çekirdeğinin kontrolünün kaybedilmesi, nükleer zincir tepkimesinin kontrolden çıkması ya da herhangi bir kaynaktan radyasyondan yayılımının yaşanması birçok durumu göz önünde bulundurarak risk değerlendirmesinin yapılmasını gerektirir(UAEA, 2007).

Nükleer Emniyet: "Nükleer maddenin, diğer radyoaktif maddelerin, ilgili tesislerin çalınma, sabotaj, yetkisiz erişim, yasadışı transferi ve diğer zararlı etkilere karşı korunma, tespit etme, yanıtlama faaliyetleri olarak tanımlanmaktadır. Tesisin fiziksel olarak korunması, siber saldırılara karşı korunması, maddenin ulusal/uluslararası taşıma esasında korunması gibi önemli faaliyetler Nükleer Emniyet içerisinde değerlendirilir (UAEA, 2017c).

Ortak noktaları insan hayatı ve çevrenin korunması olan bu iki eylemden; emniyet kötü niyetli eylemlerle ilgili, gizli ve tehdit temelli iken güvenlik şeffaf, olasılıklı güvenlik analizinin kullanıldığı, açık faaliyetlerle ilgili bir yapıdadır. Emniyet ve güvenlikten sorumlu personeller ayrıdır. Zaman zaman tesisin sağlıklı işletimi için bir araya gelseler de farklı geçmişe/uzmanlıklara sahip, farklı süreçlerle ilgilenen kişilerden oluşurlar (UAEA, 2010c).

Nükleer Emniyet Kültürü "nükleer güvenliği sağlamak, sürdürmek ve desteklemek için -bireylerin, kurum ve kuruluşların- karakteristik, tutum ve davranışları sağlama faaliyetleri" olarak tanımlanmaktadır. İnsanların ve toplumun ve çevrenin radyasyonun zararlı etkilerinden korunması için oluşturulmasına ihtiyaç duyulan bu kültürün her bir çalışan için kazanılması önemlidir. Emniyet kültürünü benimsemiş çalışanların öncelikle kendisini sürekli olarak değerlendirebilmesi ve denetleyebilmesi beklenir (UAEA, 2008a).

Nükleer alanla ilgili sorumlulukların sınırlarının net olarak belirlendiği ve sorumlularına uygun görevlendirmenin yapıldığı, önlemlerin uygulanması için uygun iletişim ve işbirliği ortamının sağlandığı, denetleme kurumunun/kuruluşunun bağımsız karar yapısına sahip olduğu, nükleer ya da radyoaktif maddelerin envanter, denetim ve koruma faaliyetlerinin sorunsuz yerine getirildiği, bilginin gizliliği kuralına riayet edildiği, yetkisiz tüm erişim türlerinin engellendiği, yetkili personelin güvenlik ve emniyet algısının sürekli canlı durabildiği, tüm önlemlerin yasalara göre alındığı ortam **Nükleer Emniyet Rejimi'**nin tam olarak sağlandığı ortam olarak kabul edilmektedir (UAEA, 2013b).

Derinlemesine Güvenlik, fiziksel korunma yapısıyla ilgili bir yaklaşımı ifade eder. Bu yaklaşım Emniyet ve Güvenlik alanlarının her ikisine de kullanılır. Bir güvenlik/emniyet duvarını/önlemini/metodunu ihlal eden kişinin başka biriyle karşılaşması ve amacına ulaşamaması üzerine kurgulanmaktadır. Dikkatli hazırlanması sık sık önlemlerin/metotların kontrol edilmesi gerekir. Derinlemesine güvenlik ortamının sağlandığı nükleer tesislerde; kazaların oluşumunun önlenmesi, kaza meydana gelirse sonuçlarının hafifletilmesi, kaza sonrası olası radyolojik boyutların sınırların altında tutulması, büyük radyolojik sonuçları olan kazaların yaşanma ihtimalinin kabul edilebilir düzeyde düşük tutulması/olması sıralamasına uygun bir güvenlik/emniyet yapısının oluşturulmuş olması beklenir (Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş., n.d.; UAEA, 1996).

Köstebek, tesisle ilgili bazı yetkilere sahip olan kötü niyetli herhangi bir kişi olarak tanımlanmaktadır. Bu kişi eskiden tesiste çalışmış ve sonrasında ayrılmış bir kişi olabileceği gibi mevcut çalışanlardan biri de olabilir. ABD'de bulunan Nükleer Enerji Enstitüsü köstebek tehdidine karşı alınması gereken birçok önlemin yanında davranış analizinin de gerekli olduğunu söyler. **Tasarıma Esas Tehdit** devletin tehdit değerlendirmesi sonrasında fiziksel korunmanın geliştirilebilmesi için tehdit değerlendirmesinden türetilen bir dokümandır. Bu tehdit değerlendirmesi dokümanında; köstebek ya da dış düşmanlar, zararlı hareket ve kabul edilemez sonuçlar arasındaki ilişki, tutum ve davranışlar, tasarım ve değerlendirme gibi önemli hususları içerir (NEI, 2016; UAEA, 2008b).

"Tasarıma Esas Tehdit" dokümanı nükleer tesisin inşası başlamadan önce onaylanır. Bu sebeple doğru kurguda bir Nükleer Emniyet Rejiminin sağlanabilmesi tesisin inşası süresinde atılacak sağlam adımlarla mümkün olacaktır. Buna ek olarak her Nükleer Emniyet Rejimi sağlıklı olması Nükleer Emniyet Kültürünün oluşturulması ve yaşatılmasıyla doğrudan ilişkilidir. Bu süreçte köstebekler önemli bir

risk unsudur. Bir olayın meydana gelmesi sonrasında yapılan soruşturmalarda çabuk fark edilebilen köstebekleri kaza öncesinde belirleyebilmek ya da önlemek oluşturulan emniyet rejiminin önemli amaçlarından biri olmalıdır. Ayrıca doğru bir derinlemesine güvenlik modelinin inşa edildiği bir tesiste köstebeklerin uzun süre stabil kalabilmesinin sağlanması muhtemeldir (UAEA, 2009a).

Çalışanlar tarafından önemsiz gibi görünen çoğu kuralı uygulatabilecek yegane unsur emniyet kültürüdür. Emniyet kültürünün yeterince yerleşmediği bir tesiste yapılan her kural ihlalinin tesise o gün için zarar verme ihtimali olmasa, ya da ihlali yapan çalışanın niyeti kötü olmasa dahi ilerleyen zaman içerisinde o çalışanın ya da ihlalin normalleşmesi sürecine tanık olan çalışanların işten çıkarılması durumunda zararsız görünen ihlal önemli bir risk haline dönüşmektedir (UAEA, 2008a).

Saldırı hedefindeki bir gruba içerden bir köstebeğin bilgi sağlaması ihtimalinin yanında, uyanık olmayan (emniyet kültürüyle yeterince donatılmamış) bir çalışanın ağzından laf alma diye tabir edilen yöntemle ve herhangi bir sosyal ortamda yaşanabilecek kurgularla ya da aklı çelinerek/ikna edilerek bilgi sağlanma ihtimali mevcuttur (UAEA, 2008a).

Bu karmaşık riskler sürekli olarak bir tehdit değerlendirmesi sürecinin yürütülmesi ve özellikle bu işten sorumlu ekibin emniyet kültürünü benimsemiş ve çalışma disiplini pozitif bireylerden oluşması riskleri sürekli minimum seviyede tutacaktır. Ayrıca bir nükleer tesiste emniyetten sorumlu ekibin personelin emniyet kültürünü, tesisin emniyet rejimini düzenli olarak denetlemesi beklenir. Ölçütlerin çok titiz çalışmalarla belirlenmesi gereken bu denetleme süreçlerinin süresinden,

sıklığından ve denetleme esnasındaki katılığından taviz verilmeyecek şekilde yürütülmesi gerekir (UAEA, 2008b, 2008b, 2010a).

1.3.4. Türkiye ve Çevresinde Nükleer Enerji

1.3.4.1. Nükleer Enerji ve Santral Tarihçemiz

Ülkemizde nükleer enerji ile ilgili çalışmalar 1950'li yıllara dayanmaktadır. Bir nükleer santrale sahip olabilmek için müteaddit defa girişimlerde bulunulmuş ancak bazen siyasi bazen ticari nedenlerle bu girişimler sonuçsuz kalmıştır. Ülkemizin bugüne kadar nükleer enerjiyle ilgili hamleleri ve sonuçları detaylıca incelenerek kronolojik olarak aşağıda sunulmuştur.

- 1956 – Başbakanlığa Bağlı Atom Enerjisi Komisyonu kuruldu. 1982'de adı Türkiye Atom Enerjisi Kurumu (TAEK) olarak değişti.
- 1957 – Türkiye, Uluslararası Atom Enerjisi Ajansının bir üyesi oldu.
- 1961 – Ülkemiz bünyesinde İstanbul Küçükçekmece gölü kenarında TR-1 isimli ilk araştırma reaktörü kuruldu. (1 MW)
- 1968 – 1. Nükleer Santral Kurma Hamlesi: İsviçreli bir konsorsiyum 1977 yılında bitirilmek üzere çalışmalara başlanmıştır. Ancak 1970 ve 1971 yıllarının ekonomik ve politik şartları nedeniyle kurulum gerçekleşmemiştir..
- 1970 – TEK bünyesinde Nükleer Santraller Dairesi kuruldu. 1988'de kapatıldı.

- 1976 – Mersin Silifke ilçesinin batısında Akkuyu için yapılan geniş kapsamlı araştırmalara dayanarak Başbakanlık Atom Enerjisi Komisyonu'ndan yer lisansı alınmıştır.
- 1977 – 2. Nükleer Santral Kurma Hamlesi: Uluslararası ihaleye çıkılmıştır. 1978-1980 arasında İsveç Konsorsiyumu(ASEA-ATOM&STALLAVAK Firmaları) ile yapılan sözleşme aşamasının son safhasında, gerek %5'lik ön ödemenin karşılanamaması ve gerekse 1980 ihtilali nedeniyle sonuç alınamamıştır.
- 1980 – Türkiye, Nükleer Silahların Yayılmasının Önlenmesi Anlaşmasını (NPT) imzaladı.
- 1982 – 2690 sayılı kanunla Atom Enerjisi Komisyonunun adı Atom Enerjisi Kurumu olarak değiştirildi.
- 1982 – 3. Nükleer Santral Kurma Hamlesi: Herhangi bir ihale açılmadan TAEK aracılığı ile Atomic Energy of Canada Limited (AECL), Siemens-Kraftwerk Union (KWU) ve General Electric (GE) firmalarından teklifler toplantı. 30 Ağustos 1984'te bu firmalarla yapılan pazarlık görüşmelerinde anlaşma sağlandı. Sonrasında hükümet Santrallerin anahtar teslimi esasına göre başlattığı ihalenin temel şartını "Yap-İşlet-Devret" şartına dönüştürdü. Bu gelişmeler üzerine KWu ihaleden çekildi. Sonrasında kendisine Akkuyu yerine Sinop Nükleer Siti teklif edilen GE firması da ihaleden çekildi. İhale iptal oldu.
- 1983 –166 sayılı kanun hükmünde kararname ile ülke elektrik enerjisi ihtiyacının bir bölümünü karşılamak üzere Nükleer Enerji Santralleri Kurumu kurulmuş; ancak 1991 yılında çıkarılan 3743 Sayılı Yasa, kuruluş kararnamesi şartları yerine getirilmediği için iptal edilmişti1991'de iptal edildi.
- 1984 – TR-2 isimli 2. Araştırma reaktörümüz İstanbul Küçükçekmece gölü kenarındaki TR-1 ile aynı alanda kuruldu (5 MW)
- 1989 – Arjantin'le ortak küçük bir santral kurma girişiminde bulunuldu (25 MW'lık pasif sistemli). 1991 yılı başlarında yeterli görülmeyen bu girişimden vazgeçildi.

- 1992 – Dünyadaki önemli firmalara birer mektup gönderilerek, 2002 yılında devreye girecek biçimde ve 1000 MW gücünde bir veya iki üniteli santralin anahtar teslimi veya "Yap-İşlet-Devret" modeli ile kurulması için teknik ve mali konularda bilgi istenmiştir. Önemli firmalara Yap-İşlet-Devret modeliyle çağrıda bulunuldu. Cevap alınamadı.
- 1993 – Bilim ve Teknoloji Yüksek Kurulu tarafından Nükleer Enerjiden Elektrik üretimi ülkemizin 3. öncelikli meselesi olarak belirlendi.
- 1995 – Enerji Bakanlığı Bünyesinde Nükleer Proje Uygulama Daire Başkanlığı kuruldu. Halen aktif olarak bulunmaktadır.
- 1997 – 4. Nükleer Santral Kurma Hamlesi: 1996 yılında ihaleye çıkıldı. Ekim 1997de teklifler toplandı. İhaleye NPI (Fransa-Almanya), AECL (Kanada-Japonya), WESTİNGHOUSE (ABD-Japonya) konsorsiyumları katılmıştır. Ana teklif 1218MW-1482 MW ve alternatif teklif 2678-2964 MW arasında değişen teklifler olmuştur. Böylece 3000 MW' a yaklaşan nükleer enerji programının başlatacak önemli bir aşama kaydedilmiştir. 2000 yılında hükümet projeyi sonlandırdığı ve ülkede nükleer santral kurulmasından vazgeçtiğini açıkladı.
- 2002 – Türkiye Atom Enerjisi Kurumu, Enerji ve Tabii Kaynaklar Bakanlığına bağlandı.
- 2007 – 2010-2020 arasında 5000 MW'lık 3 nükleer santral kurmayı amaçlayan "Nükleer Enerji Yasası" çıkarıldı. Ancak dönemin Cumhurbaşkanı Ahmet Necdet Sezer, santrali kuracak şirketin yapısı, denetimi, söküm masrafı gibi alanlarda anayasaya aykırılıklar olduğu gerekçesiyle yasanın üç maddesini veto etti.
- 2008 – Nükleer Güç Santrallerinin kurulmasına yönelik yönetmelik Resmi Gazetede yayımlanarak yürürlüğe girdi.
- 2010 – 5. Nükleer Santral Kurma Hamlesi "Türkiye Cumhuriyeti Hükümeti ile Rusya Federasyonu Hükümeti Arasında Türkiye Cumhuriyeti'nde Akkuyu Sahası'nda Bir Nükleer Güç Santralinin Tesisine ve İşletimine Dair İşbirliğine

İlişkin Anlaşma" imzalandı. Aynı yıl Resmi Gazetede yayımlanarak yürürlüğe girdi. Rusya ile Akkuyu Nükleer Güç Santralinin yapılması için anlaşıldı.

- 2010 – Akkuyu NGS Elektrik Üretim A.Ş. projenin yüklenicisi olarak kuruldu.
- 2011 – Akkuyu NGS Elektrik Üretim A.Ş.'ye Nükleer Güç Santralinin işletmesi ve inşaatı için arazi tahsisi yapıldı.
- 2012 – Elektrik Üretim Anonim Şirketi (EÜAŞ), TAEK tarafından Sinop'ta inşa edilmesi planlanan NGS Projesinde "Kurucu" olarak yetkilendirildi.
- 2013 – "Türkiye Cumhuriyeti Hükümeti ile Japonya Hükümeti Arasında Nükleer Enerjinin Barışçıl Amaçlarla Kullanımına Dair İşbirliği Anlaşması" imzalandı.
- 2014 – Çevre ve Şehircilik Bakanlığı Akkuyu NGS ile ilgili "Çevre Etki Değerlendirme" raporunu onayladı.
- 2015 – "Türkiye Cumhuriyeti Hükümeti ile Japonya Hükümeti Arasında Nükleer Enerjinin Barışçıl Amaçlarla Kullanımına Dair İşbirliği Anlaşması" Resmi Gazetede yayımlanarak yürürlüğe girdi.
- 2015 – Akkuyu için ilk temel atma töreni yapıldı.
- 2017 – TAEK, Akkuyu NGS Elektrik Üretim A.Ş.'ye "Sınırlı Çalışma İzni" verdi. Bu izinle doğrudan radyoaktivite içermeyen tesislerin inşaatlarının yapılabilmesi onaylanmıştır (AkkuyuNPP, 2017c, 2017b; ETKB, 2016; İTÜ, 2006; NTV, 2017; NükleerAkademi, 2017b; Özemre, 2006; TBMM, 2010, 2014c, 2015a; Ucael, 2015; WNA, 2017e).

1.3.4.2. Akkuyu ve Sinop Nükleer Güç Santrallerine (NGS) Genel Bakış

AKKUYU Nükleer Güç Santrali ile ilgili olarak Türkiye Cumhuriyeti Hükümeti ile Rusya Federasyonu Hükümeti arasında bir anlaşma imzalanmış olup bu anlaşma gereği NGS kurmaya başlanması için gerekli tüm izinlerin verilmesinden itibaren yedi yıl içinde 1. Ünite'nin (Reaktörün) işletmeye alınması öngörülmektedir. Ünite 1'in ticari işletmeye başlanmasından itibaren, Ünite 2, Ünite 3 ve Ünite 4'ü artarda bir yıl aralıklarla ticari işletmeye alınmış olacaktır. Her biri 1200 MWe enerji üretebilen bu 4 ünitenin devreye girmesiyle yıllık 35 milyar kWh elektrik üretilmesi planlanmıştır (TBMM, 2010).

Anlaşmanın imzalanması sonrasında 2010 yılı Aralık ayında Akkuyu NGS Elektrik Üretim A.Ş. isimli bir şirket kurulmuştur. Rusya devlet kuruluşu olan ROSATOM bu şirketim tamamına sahip olmakla birlikte bu şirkete %49'a kadar yerli ya da yabancı yatırımcılar şirket hissedarı olabilmektedir. Bu şirketin %49'luk hisselerinin 3 büyük Türk İnşaat Şirketi tarafından satın alınacağına dair basında bilgiler yer almıştır. Akkuyu NGS'de çalışacak Türk mühendislerin eğitimi kapsamında toplam 600 öğrenciye eğitim verilmesi planlanmıştır. Bu kapsamda 2010 yılından beri Rusya'daki Ulusal Nükleer Araştırma Üniversitesi Moskova Fizik Mühendisliği Enstitüsü'nde 307 öğrencinin eğitimi süreci başlamıştır(AkkuyuNPP, 2015, 2017a; ETKB, 2016; Rosatom ve Akkuyu NGS Elektrik Üretim A.Ş, n.d.; Sabah, 2017).

Rusya (Rosatom), Yap-Sahip Ol-İşlet (Built-Own-Operate) modelini Akkuyu NGS projesinde ilk kez kullanacaktır. Nükleer sektörde gelişmemiş durumda olan ve eğitimli personeli bulunmayan ülkeler için ideal bir model olarak değerlendirilen bu model ülkemiz dışında ülkeleri de kapsayacağı yönünde bilgiler bulunsa da henüz resmi olarak bu modelle ilerlenecek bir proje görülmemiştir. Rosatom; Akkuyu dışında farklı modellerle Çin, Hindistan, Belarus, İran, Vietnam ve Bangladeş'te NGS

projelerini sürdürmektedir (Nucnet, 2013; Reuters, 2013b; Sokolov, 2013; WNA, 2017c).

Sinop'ta yapılması muhtemel NGS için Türkiye Cumhuriyeti Hükümeti ile Japonya Hükümeti Arasında bir anlaşma imzalanmış olup anlaşma gereği Proje Sahasında dört (4) ünite (Reaktör) inşa edilecektir. Dört (4) ünitenin işletmeye alma yılları sırasıyla Ünite1 için 2023, ünite 2 için 2024, ünite 3 için 2027 ve ünite 4 için 2028'dir. Aynı anlaşma içerisinde Proje Sahası ifadesi "*Türkiye Cumhuriyeti'nin Sinop ilinde ya da şartların gerektirmesi durumunda başka bir yerde, Proje'nin uygulanması için Proje Şirketi'ne tahsis edilecek arazi*" olarak tanımlanması Sinop'un yer lisansı alması sürecinin devam ettiğini göstermektedir. Japon Mitsubishi Heavy Industries Ltd.(MHI) ile Fransız Areva ortak girişimi olan ATMEA tarafından geliştirilen ATMEA1 tipi reaktörün bu projede uygulanmasına karar verildi. Projenin uluslararası bir konsorsiyum (Japon MHI, Japon ITOCHU, Fransız GDF SUEZ ve Türk EÜAŞ) tarafından gerçekleştirilmesi beklenmektedir. Bu projenin devreye girmesiyle yıllık 34 milyar kWh elektrik üretilmesi planlamıştır. Bu anlaşmanın koşulları arasında teknoloji transferini de içerecek şekilde Japon tarafına "yerli tedarik, insan kaynakları geliştirme, teknoloji transferi ve sosyal sorumluluk planlarının bulunduğu ekonomik etki değerlendirme" raporunun hazırlanması ve ETKB'ye onaylatılması yükümlülüğünü vermiştir (ETKB, 2016; MHI, n.d.; TBMM, 2015a).

TEİAŞ'ın 2015 yıl sonu raporlarına göre ülkemizin yıllık elektrik talebi 269 milyar kWh olmuştur. Yani 2015 yılında her iki NGS çalışıyor olsaydı yıllık elektrik ihtiyacımızın %25'ini karşılayabilecek sonucuna ulaşılmıştır (ETKB, 2016).

1.3.4.3. Yakın Çevremizde Bulunan Nükleer Santraller

Nükleer santrallerle ilgili tehlikeler düşünüldüğünde yaşanmış olan ilk örnek olarak Çernobil faciası akla gelmektedir. Çernobil NGS'nin ülkemize yakın bir noktada bulunması ve Karadeniz bölgesini etkilediğine dair önemli bulgular çevremizde bulunan ve risk taşıyan başka nükleer santrallerin olup olmadığının incelenmesini gerektirmiştir. Yakın çevremizde Ermenistan ve Bulgaristan'da nükleer santraller bulunmaktadır (CarbonBrief, 2017).

1.3.4.4. Metsamor Nükleer Santrali - Ermenistan

Iğdır sınırımıza 30 km mesafede Metsamor isimli bir nükleer santral bulunmaktadır. Erivan'a 32 km mesafededir. 1977 yılında inşaa edilmiştir. 375 MW'lık 2 reaktörden oluşur. Reaktörlerden biri kalıcı olarak kapatılmış, diğeri aktiftir. İlk çalışmaya 1980 yılında başlamıştır. Avrupa Birliği santrali "Bölgenin Tamamı İçin Tehlike", ABD ise "Yaşlı ve Tehlikeli" olarak nitelendirmiştir (National Geographic, 2017).

Santral 1988'de kapatılmış ancak tüm Ermenistan'ın elektrik ihtiyacının %40'ından fazlasını karşıladığından dolayı sonra yeniden aktifleştirilmiştir. Santralde Birincil koruma yapısı bulunmamaktadır (Hürriyet, 2003b; National Geographic, 2017; WNA, 2017a).

1.3.4.5. Kozloduy Nükleer Santrali - Bulgaristan

Bulgaristan'ın Romanya sınırında bulunur. Sınırlarımıza kuş uçuşu 350 km mesafededir. 4 adet 408 MW ve 2 adet 963 MW olmak üzere 6 reaktörden oluşur. Bu reaktörlerden 408 MW olan 4'ü kalıcı olarak kapatılmıştır. 963 MW'lık reaktörler aktiftir (CarbonBrief, 2017; WNA, 2017b).

1.3.4.6. Radyasyon Erken Uyarı Sistemi Ağı (RESA)

Yakın çevremizde olabilecek ve radyoaktivite salınımı içeren bir olayın yaşanması durumunda önlem alınabilmesi için pek çok ülkede kullanılan ölçüm istasyonları ülkemize de kurulmuştur. 1986 yılında kurulmuş olan Radyasyon Erken Uyarı Ağı Sistemi (RESA) istasyon sayısı riskler doğrultusunda arttırılmakta ve teknolojik gelişmelere paralel olarak sistemde iyileştirmeler de yapılmaktadır. Bu ağ ile anlık radyasyon bilgisi alınabilen istasyon sayısı 1995 yılında 32 iken bugün itibariyle 193'e çıkarılmıştır. Bu 193 istasyondan 5'i Ermenistan sınırımızda bulunan Metsamor NGS'ye çok yakın olacak şekilde konuşlandırılmıştır (TAEK, 1995, 2017f).

1.3.5. Nükleer Olaylar

1.3.5.1. Uluslararası Nükleer ve Radyolojik Olay Ölçeği (INES International Nuclear Events Scale Information Service)

1990 yılında Uluslararası Atom Enerjisi Ajansı ve OECD Nükleer Enerji Ajansının işbirliği ile başlatılan çalışma ile nükleer tesisler, radyasyon kaynakları ve taşıma esnasında meydana gelen olaylarla ilgili nükleer alanla ilgilenen kurum ve kuruluşlara, halka ve medyaya kaynağından doğru bilgi verilmesini sağlayacak bir yapı oluşturulmuştur. UAEA üyesi 60 farklı ülkedeki sorumluların Olay Ölçeklendirme Formlarını kullanarak yaptıkları bilgilendirme ile INES veritabanında kaynağından elde edilmiş verilerin bulunması sağlanmaktadır. Çizelge 4-5'te formlardan gelen bilgilerle birlikte seviyelere göre inceleme yapıldığında Büyük Kaza kategorisinde iki büyük kazanın yer aldığı görülmektedir (UAEA & OECD NEA, n.d.).

Çizelge 1-5 INES Ölçeği Aşamaları ve Meydana Gelen Olaylar (TAEK, 2017i, n.d., UAEA, 1988, 1992, 2013a, 2014b, 2015; UAEA & OECD NEA, n.d.)

Olay Seviyesi	Seviye Adı	Meydana Gelen Olay
Seviye 7	Büyük Kaza	1. Çernobil Kazası (1986), 2. Fukuşima Daiichi Kazası (2011)
Seviye 6	Ciddi Kaza	1. Kyshtym Kazası (1957)
Seviye 5	Geniş Sonuçları Olan Kaza	1. Windscale Yangını (1957), 2. Three Mile Island kazası (1979), 3. First Chalk River kazası (1952), 4. Lucens reaktör korunun erimesi kazası (1969), 5. Goiania Kazası (1987)
Seviye 4	Yerel Sonuçları Olan Kaza	1. Sellafield (1955-1979), 2. SL-1 Experimental Güç İstasyonu kazası (1961),

		3. Buenos Aires RA-2 kazası (1983), 4. Jaslovske Bohunice Kazası (1977), 5. Tokaimura Kazası (1999)
Seviye 3	Ciddi Olay	1. THORP Santrali Olayı (2005), 2. Paks Santrali Olayı (2003), 3. Vandellos I Olayı (1989), 4. Davis-Besse Olayı (2002)
Seviye 2	Olay	1. Blayais Santrali (1999), 2. Asco Santrali (2008), 3. Forsmark Santrali (2006), 4. Gundremmingen Santrali (1977), 5. Shika Santrali (1999), 6. Fukushime Daiichi Santrali (2011)
Seviye 1	Anomali	1. Penly (2012), 2. Gravelines (2009), 3. TNPC France (2008)
Seviye 0	Güvenlik Açısından Önemsiz Olay	1. Krsko Slovenia (2008), 2. Atucha Argentina (2006)

Seviyelerin Anlamları: (UAEA & OECD NEA, n.d.)

1) **Anomali:**
   a) **Güvenlik Önlemleri Açısından:** Halktan birinin yıllık izin verilenin üzerinde radyasyon dozu alması seviyesinde olaydır. Güvenlik bileşenlerindeki küçük problemlerden kaynaklanabilir. Derinlemesine savunma anlayışı zarar görmemiştir. Düşük aktiviteli kaynak, cihaz ya da taşıma paketi kaybolmuştur ya da çalınmıştır.

2) **Olay:**
   a) **Sağlık ve Çevre Açısından:** Halktan bir bireyin 10 mSv'in üzerinde radyasyon dozuna maruz kalması ya da bir çalışanın yıllık izin verilen miktarının üzerinde radyasyon dozu alması seviyesinde olaydır.
   b) **Çalışma Ortamı Açısından**: Çalışma alanında doz hızının 50 mSv/saat'in üzerinde olması ya da tasarım açısından beklenemeyen bir tesis içi alanda önemli radyasyon seviyesinin olması seviyesinde olaydır.
   c) **Güvenlik Önlemleri Açısından:** Gerçek bir sonuca yol açmayan önemli arızalar oluşması, önlemlerin hasar görmediği yüksek aktivitedeki kayıp kaynak, cihaz ya da taşıma paketi fark edilmesi, yüksek aktiviteli radyasyon

kaynağının uygun olmayan şekilde paketlenmesi ya da bir çalışanın yıllık izin verilen miktarının üzerinde radyasyon dozu alması seviyesinde olaydır.

3) **Ciddi Olay**:
   a) **Sağlık ve Çevre Açısından:** Çalışanlar için izin verilen yıllık doz miktarının on katını aşan radyasyona maruz kalma ya da radyasyonun yanık gibi ölümcül olmayan deterministik etkilerinin görülmesi seviyesinde olaydır.
   b) **Çalışma Ortamı Açısından:** Bir çalışma alanında 1 Sv/saat'in üzerinde doz hızına maruz kalma ya da tasarımsa bir alanda tasarımda beklenmeyen şekilde, halkın etkilenmesi olasılığı düşük olan ciddi kontaminasyonun olması seviyesinde olaydır.
   c) **Güvenlik Önlemleri Açısından:** Bir nükleer tesiste alınacak güvenlik önleminin bulunmadığı kazaya yakın durum, kayıp ya da çalınmış yüksek aktiviteli, zırhlı radyasyon kaynağı, doğru prosedürler izlenmeden yanlış adrese gönderilmiş radyasyon açısından doğru paketlenmiş kaynak olması seviyesinde olaydır.

4) **Yerel Sonuçları Olan Kaza**:
   a) **Sağlık ve Çevre Açısından:** Az miktarda radyoaktif madde salımı gerçekleşmiş ve yerel besin kontrolünden başka bir önlemin uygulanmasının beklenmediği ya da radyasyon sebebiyle en az bir ölümün gerçekleştiği seviyede olaylardır.
   b) **Çalışma Ortamı Açısından:** Yakıt erimesi veya yakıt hasarı sonucu kor envanterinin %0.1'inden fazlasının salımı ya da tesis içerisinde halkı etkileme olasılığı yüksek olan, sınırlı miktarda radyoaktif madde salımının yaşanması seviyesindeki olaylardır.

5) **Geniş Sonuçları Olan Kaza:**
   a) **Sağlık ve Çevre Açısından:** Sınırlı miktarda radyoaktif madde salımı gerçekleşmiştir. Planlanmış önlemlerin bir kısmının uygulanmasının gerekli olması ya da radyasyon sebebiyle ölümlerin gerçekleşmesi seviyesinde olaylardır.
   b) **Çalışma Ortamı Açısından:** Reaktör korunda ciddi hasar meydana gelmesi, tesis içerisinde halkı etkileme olasılığı yüksek olan, büyük miktarda radyoaktif madde salımı(Büyük bir kritiklik kazası ya da yangın bu tür bir olaya sebep olabilir) seviyesinde olaylardır.

6) **Ciddi Kaza:**
   a) **Sağlık ve Çevre Açısından:** Önemli miktarda radyoaktif madde salımı gerçekleşmesi, planlanmış önlemlerin uygulanmasının gerekli olması seviyesinde olaylardır.

7) **Büyük Kaza:**
   a) **Sağlık ve Çevre Açısından:** Büyük miktarda radyoaktif madde salımı gerçekleşmesi ve geniş alanda sağlık ve çevresel etkilerle karşılaşılacağından planlanmış ve genişletilmiş önlemlerin uygulanmasının gerekli olduğu seviyedeki olaylardır.

1.3.5.2. Önemli Nükleer Olaylar

Seviye 7 – Büyük Kaza

1.3.5.2.1. Çernobil Kazası (1986)

Sovyet Sosyalist Cumhuriyetler Birliğinin (Günümüzde Ukrayna içerisinde kalan) Kiev iline bağlı Çernobil bölgesinde bulunan Nükleer Güç Santralinin 4. Reaktöründe 1986'da meydana gelen kazadır. 4 yıldır tekrarlanan ve başarı elde edilemeyen bir testin hesaplarının bir daha yapılması sonrasında; güvenlik sistemlerinin devreden çıkarılması, operatör hataları, tasarımın koruma kabı içermemesi, test prosedürlerinde belirtilen adımların atlanması gibi bir dizi etken sonucunda reaktörün kararsız hale gelerek büyük bir patlama yaşanmasına neden olmuştur (UAEA, 2006).

Avrupa'yı da içerisine alan yaklaşık 200.000 km^2'lik bir alana nükleer serpinti bulutu yayıldı. Radyoaktif fisyon ürünü olan Sezyum 137 ile Avrupa ülkeleri ve Türkiye'de önemli ölçüde radyoaktif kirlilik oluştu. Kazadan 2 hafta sonra İngiltere'nin Galler bölgesinde saptanan yüksek radyoaktivite nedeniyle yeşil alanlara koyun ve sığırların girişi engellenmiştir. Kaza sonrasındaki ilk aylarda radyoaktif iyodin düzeyi yüksek sütlerden içen çocuklar yüksek radyasyon dozları almışlardır. 2002 yılına kadar bu grup içerisinde 4000'den fazla tiroit kanseri teşhis edilmiştir.

Kaza anında 30 kişi ölmüş, 30 km olarak belirlenen etki alanından aynı yıl 116.000 kişi tahliye edilmiştir (Tombakoğlu et al., 2011; UAEA, 1998b).

1.3.5.2.2. The Fukuşima Daiichi Kazası (2011)

2011 yılında Japonya'da meydana gelen 9.0 büyüklüğündeki deprem anında The Fukuşima Daiichi Nükleer Santralinin 6 reaktörünün tamamı kapatılmıştır. Düzenli olarak soğutulmaya ihtiyacı olan reaktörün soğutma sistemleri ihtiyaç duyduğu enerjiyi deprem nedeniyle şehir şebekesinden sağlayamamıştır. Devreye giren jeneratörler tsunami sonrasında devre dışı kalmış olup son güvenlik önlemi olan bataryalarla kısa süre soğutma sağlanabilmiştir. Tüm bu sorunlar sonrasında santralde patlamalar meydana gelerek radyoaktif serpinti yaşanmıştır (UAEA, 2015).

Kaza anında 3 kişi ölmüş, 20 km olarak belirlenen etki alanında 80.000 kişi tahliye edilmiştir (Tombakoğlu et al., 2011).

Seviye 6, Ciddi Kaza

1.3.5.2.3. Kyshtym (Mayak) Kazası (1957)

Rusya'nın Kyshtym bölgesindeki MAYAK isimli silah yapımı için radyoaktif maddelerin kullanıldığı tesiste sıvı atık tankında Eylül 1957'de yaşanan yangın sonrasında meydana gelen patlamaya verilen isimdir. Tesis uranyum ve plütonyum kullanarak silah üretmeye çalışmaktadır. 70-80 ton civarında sıvı radyoaktif atık depolanan sıvı atık tankında artan ısıdan dolayı meydana gelen patlama ile toplamda 20.000 km^2'lik alan radyoaktif serpintiye maruz kalmıştır. Resmi bilginin çok az olduğu olayla ilgili birçok iddia mevcuttur. Bu alanda yaşayan 270.000 kişinin 11.000'inin alanı boşaltması sağlandığı ve bu boşaltma işleminin 2 yıl sürdüğü, boşaltma işlemine sadece etnik Rusların dahil edildiği, halkın korunmasız temizleme faaliyetlerine zorlandığı bu iddialar arasındadır. 1958 Nisan'ında (7 ay sonra) batı medyasında konu yer almış, Medvedev isimli Biyolog tarafından 1976'da 1980'de yayınlanan kitaplarla olayın ayrıntıları öğrenilmiştir. 1992'de yapılan bir çalışmaya göre devam eden 32 yıl içinde 8015 kişi kaza sonucunda ölmüştür. Yakınlarda bulunan nehir kenarında yaşayan insanlardan 6000 kişinin de kaza nedeniyle dolaylı olarak öldüğü tahmin edilmektedir (Mentalfloss, 2017; UAEA & OECD NEA, n.d.).

Seviye 5 Geniş Alanda Etkileri Olan Kaza

1.3.5.2.4. Three Mile Island Kazası (1979)

1979 yılında ABD'de bulunan Three Mile Island Nükleer Santralinin 2. Ünitesinin düzenli soğutulamaması sonucunda yakıt erimesi ve sonrasında basınç rahatlatma vanalarının kapatılamaması gibi bir dizi sorun sonrasında atmosfere radyoaktivitenin çıkmasıyla sonuçlanan kazadır. Her ne kadar radyoaktivitenin büyük bölümü koruma kabında tutulmuş olsa da atmosferdeki ölçümler doğal radyasyon seviyesinin çok az üstünde olduğunu göstermiştir. Acil durum ilan edilmiş ve 144.000 kişi başka yerlere sevkedilmiştir. Can kaybı yaşanmamış olmakla birlikte tesisin içi

zarar görmüş ve kapatılmak zorunda kalmıştır. İlk temizlikler 12 yıl sürmüş yaklaşık bir milyar dolara mal olmuştur (NRC, 2013, 2016).

ABD'nin o güne kadarki en büyük nükleer kazasıdır. Birçok ders çıkarılmış olup bu derslerin uluslararası toplumla paylaşımı sağlanmıştır. Kaza sonrasında ABD'de Nükleer Enerji Uygulamaları Enstitüsü (INPO – Institute of Nuclear Power Operations) kurulmuştur. Ayrıca ABD'de bulunan Nükleer Düzenleme Komisyonu tarafından yeni ölçüm cihazları geliştirilmiş ve mevcut olanlarda da iyileştirmeye gidilmiştir. Kaza anında ölen olmamış, 8 km olarak belirlenen etki alanından 140.000 kişi tahliye edilmiştir (Pate, 1986; Tombakoğlu et al., 2011).

1.3.5.2.5. Goiania (1987)

Brezilya'nın Goiania şehrinde, bir radyoterapi kliniği (The Institute Goiano de Radioterapia (IGR)) başka bir binaya taşınırken, Sezyum-137 teleterapi cihazlarından birinin götürülmemesi, boş binaya giren hurdacıların bu cihazı alarak evine götürmesi sonrasında yaşanan olaydır. Hurdacılar bir süre cihazı tamamen parçalamaya uğraştılar ve radyoaktif madde olan sezyum klorid haznesini kırarak bir miktar açığa çıkardılar. Mavi ışınlar saçan bu toz maddeyi bir süre sonra başka bir hurdacıya sattılar. Hazneyi tamamen açmayı başaran yeni sahibin ev halkı bir süre sonra şiddetli bulantı ve ishal yaşamaya başladı. Tozdan şüphe edilmesi üzerine toz hastaneye götürüldü (UAEA, 1988).

Tüm bu süreçte tozun hastaneye götürülmesi sürecinde otobüsteki yolcular dahil radyasyona maruz kalan 249 kişiden 4'ü öldü. Olay sonrasında olayın yaşandığı mahalle boşaltıldı, 40 kadar ev yıkıldı, bölgede bulunan toprak tabakasının 30 cm'lik kısmı sökülerek radyoaktif bir depolama alanına götürülmüştür. Bu atıkların bu alanda en az 300 yıl bekletilmesi gerekmektedir (UAEA, 2017a).

Seviye 4, Lokal Sınırlı Etkileri Olan Kaza

1.3.5.2.6. Saint Laurent Des Eaux (1980)

Fransa'da bulunan Saint Laurent Des Eaux Santrali'nde Mart 1980'de soğutma sisteminde bir arıza nedeniyle A2 reaktöründe bir yakıt kanalının erimesine neden olan olaydır. Dışarıya radyoaktif sızıntı gerçekleşmemiştir. Fransa'nın yaşadığı en kötü nükleer kaza olarak nitelendirilmektedir (Power Technology, 2017).

Seviye 3 Ciddi Vaka

1.3.5.2.7. İkitelli (1999)

Ülkemizde yaşanmış en önemli radyoaktif olaydır. Radyoaktivite alanında lisans sahibi bir şirket tarafından Ankara'da bulunan 3 adet Kobalt 60 kaynağının üretim yeri olan ABD'ye geri gönderilmek üzere ambalajlanması ve geri gönderme işlemi için 1994 yılında ihracat lisansı alınmasına rağmen gönderme işlemini gerçekleştirmemesi

sonrasında devam eden olaylarla yaşanan vakadır. Gazeteler bu olayla ülkemizin hiç nükleer santrale sahip olmadan "dünyanın en önemli 20 radyoaktif kazası" listesine girdiğini duyurmuşlardır. TAEK tarafından mağdur durumda kalan hurdacı aileye tazminat ödendiği ayrıca belirtilmiştir (HaberTürk, 2011; Sabah, 2006).

Şirket 1994 yılından 1998 yılına kadar geri gönderme işlemini yapmadığı bu kaynaklardan 2'sini İstanbul'a taşımış ve sonrasında İkitelli'de bulunan şirketin deposuna bitişik boş tesislere konulmuştur. Tesisin el değiştirmesiyle yeni sahipler bu kaynakları hurdacıya satarlar. Hurdacı evine götürerek bu kapları söker, zırh fişinin dahi çıkarıldığı kapların söküm işlemi kötü hava koşulları nedeniyle ertelenir. Devam eden süreçte kapların söküm işlemi gerçekleştirilir. Söküm işlemini gerçekleştirenler ve orada bulunanlar hasta hissederler ve bir sağlık kuruluşuna başvururlar. Radyasyon etkilerinden şüphelenilmediğinden kişiler bir süre sonra taburcu edilmişlerdir (TAEK, n.d.).

Kaynaklar evin yakınında bulunan hurdalıkta bir hurda yığının altında bırakılır. Bir süre sonra İzmit'te bulunan büyük bir hurda alıcısına gönderilir. Hurdalara müdahale anında rahatsızlanan iki kişinin özel hastaneye başvurması ve radyasyondan şüphelenilmesi sonrasında olay ortaya çıkar. Sonrasında TAEK yetkililerine olay bildirilir. Olayda 7'si çocuk olmak üzere toplam 18 kişi tedavi görmüştür. Ölüm yaşanmamıştır (TAEK, n.d.; UAEA, 2002).

1.4. Kritik Altyapılar

1.4.1. Türkiye'de Kritik Altyapılar

Kritik altyapı terimi üzerine benzer tanımlar dünyada ve ülkemizde kabul görmektedir. Bu tanımlardan bazıları şu şekildedir:

- "Kritik Altyapılar: 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" (Bakanlar Kurulu, 2012)
- "İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünü" (AFAD, 2014).

Bir hizmetin kritikliğini ülkemizde yokluğunda yaşatabileceği durumlar üzerinden değerlendiren başka benzer tanımlar görülebilmekte ise de yukarıda alıntı yapılan 2 metin kritik altyapılarla ilgili belirleyici rolündedir.

Ülkemizde kritik altyapılara ilişkin tanım ilk defa 2012 yılında yayımlanan Bakanlar Kurulu kararında belirtilmiş olup bu kararın amaçlarından birinin de "Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin

güvenliğinin sağlanması" olduğu belirtilmiştir. Aynı belgenin "Eylemler" bölümünde bazı eylemlerden sorumlu birim olarak "Kritik Sektörleri Düzenlemek ve Denetlemekle Sorumlu Kurumlar" ifadesi belirtilmiş olsa da bu kurumların hangileri olduğuna açıklık getirilmemiştir. Ayrıca aynı belgede Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri sektörleri kritik altyapı sektörleri olarak belirlenmiştir (Bakanlar Kurulu, 2012).

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" isimli belge 2013 yılında Bakanlar Kurulu kararıyla resmi gazetede yayımlanarak yürürlüğe girmiştir. Bu belgede kritik altyapılarla ilgili olarak TÜBİTAK ve Kritik Sektörleri düzenlemek ve denetlemekle sorumlu kurumlar'a "Siber tehditlerin doğrudan hedefi haline gelen ve zarar görmesi halinde toplum düzenini bozabilecek kritik altyapıların tespit edilmesi" ve "Belirlenecek bir kritik altyapının sektörel risk analizinin yapılması" görevleri verilmiştir. TÜBİTAK tarafından hazırlanan "Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı" isimli dokümanda bu doğrultuda önemli görülen hususlar açıklanmıştır (TÜBİTAK, n.d.; UDHB, 2013).

Devamında AFAD tarafından 2014 yılında yayımlanan 2014-2023 Teknolojik Afetler Yol Haritası Belgesi ile *Enerji, Ulaştırma, Su Yönetimi ve Barajlar, Haberleşme, Bankacılık ve Finans, Tarım ve Gıda, Kültür ve Turizm, Kritik Üretim/Ticari Servisler, Kritik Kamu Hizmetleri ve Sağlık'ın* kritik altyapı tanımının içinde bulunan sektörler olduğu belirtilmiştir (AFAD, 2014).

Aynı belgede Kritik altyapıların korunması konusunda paydaş kurumlar olarak;

- İçişleri Bakanlığı
- Çevre ve Şehircilik Bakanlığı

- Enerji ve Tabii Kaynaklar Bakanlığı
- Enerji Piyasası Düzenleme Kurumu
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
- Sağlık Bakanlığı
- Bilim, Sanayi ve Teknoloji Bakanlığı
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
- Türkiye Atom Enerjisi Kurumu Başkanlığı
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanlığı
- Jandarma Genel Komutanlığı
- Kamu Düzeni ve Güvenliği Müsteşarlığı
- Hacettepe Üniversitesi

gösterilmiştir.

Aynı belgenin eylemler bölümünde AB Mevzuatı ile ulusal mevzuatın incelendiği ve bir boşluk analizi yapıldığı belirtilmiştir. Bu analiz sonrasında ihtiyaç duyulan eylemlerin sıralandığı bölümde

- Her sektörün bir sorumlusunun belirleneceği,
- Tüm kritik altyapı sektörlerini içine alan bir çalışmanın AFAD koordinasyonunda yapılacağı (AFAD'ın sorumlu ve çatı kurum olarak görüldüğü belirtilerek),
- Kritik altyapı tesislerinin belirleneceği ve envanterinin çıkarılacağı,
- AB'nin ilgili irtibat noktaları ile koordinasyon sağlanacağı,
- Sektörlere özel kritik altyapı koruma programlarının detaylandırılması gibi çalışmaların yürütülmesinin beklendiği,
- Kritik altyapı sahiplerinin ve işletmecilerinin koruma konusunda kendi kararlarını vermeleri gerektiği,

- Her kritik tesisten sorumlu kamu kurum ve kuruluşunun İşletmeci Güvenlik Planına[2] sahip olup olmadığını, ilgili ölçütleri uygulayıp uygulamadığını değerlendireceği,
- Ulusal bir Kritik Altyapı Koruma programı hazırlanacağı, bu programla farkındalık artışı, diyaloğun artırılması, ar&ge faaliyetlerinin arttırılması hususlarının sağlanmasının hedefleneceği,

öne çıkmıştır (AFAD, 2014).

Öte yandan 2016 yılında UDHB tarafından yayımlanan 2016-2019 Ulusal Siber Güvenlik Strateji belgesinde Elektronik-Haberleşme, Enerji, Su Yönetimi, Kritik Kamu Hizmetleri, Ulaştırma ve Bankacılık ve Finans sektörleri Kritik Altyapı Sektörleri içerisinde olduğu belirtilmiştir. Çizelge 5-1'de de belirtildiği üzere AFAD ile UDHB tarafından farklı tarihlerde hazırlanmış belgelerde 4 farklı sektörün UDHB tarafından kritik olarak değerlendirilmediği görülmektedir (UDHB, 2016).

Çizelge 1-6 Kritik Altyapı Sektörlerinin Farklı Belgelerde Kıyaslanması (AFAD, 2014; UDHB, 2016)

	1. 2014 Afad Çalışması	2016 Siber Güvenlik Kurulu Çalışması
Kritik Altyapı Sektörleri	1. Haberleşme 2. Enerji 3. Su Yönetimi ve Barajlar 4. Kritik Kamu Hizmetleri 5. Ulaştırma 6. Bankacılık ve Finans 7. Tarım ve Gıda 8. Kültür ve Turizm 9. Kritik Üretim/Ticari Servisler 10. Sağlık	1. Elektronik Haberleşme 2. Enerji 3. Su Yönetimi 4. Kritik Kamu Hizmetleri 5. Ulaştırma 6. Bankacılık ve Finans

[2] İşletmeci Güvenlik Planı: Önemli varlıkların tanımlandığı, tehdit senaryo/zayıf nokta/olası etkileri içeren bir risk analizinin yapıldığı, karşı önlemler ve prosedürleri barındıran, işletmecinin seçimlerini ve belirlediği önem sırasının belirtildiği plan.

UDHB tarafından yayımlanan 2016-2018 Ulusal Siber Güvenlik Stratejisi Belgesinin sonunda bir Sektörel SOME (Siber Olaylara Müdahale Ekibi) listesi yayımlanmış olup bu listede enerji sektöründeki sektörel SOME olarak "Enerji Piyasası Düzenleme Kurumu Başkanlığı (EPDK)" belirtilmiştir.

1.4.2. Amerika'da Kritik Altyapılar

Kritik altyapılar konusunda Amerika Birleşik Devletleri'nde (ABD) yayımlanmış ilk belge 1996 yılındaki kararnamedir (Executive Order). 8 sektörün kritik olarak tanımlandığı bu kararnamede kritik altyapılar için tehdit unsurlarının 2 kategoriye ayrıldığı belirtilmiştir. Fiziksel tehditler ve siber tehditler olarak yapılmış bu kategorizasyona ek olarak kamu ile özel sektörün tehditlerin oluşturacağı riskleri minimize edebilmesi için birlikte çalışması gerektiğine vurgu yapılmıştır (US-GOV, 1996).

Kararnamenin devamında "Kritik Altyapı Koruma Komisyonu" isimli ve 10 farklı kurumdan üyenin bulunduğu bir komisyon kurulmuştur. Dışarıdan birinin de başkan tarafından başkan olarak atanabildiği bu komisyona bağlı Yönetim Kurulu ve Yürütme Kurulu bulunmaktadır. Çizelge 5-2'de sunulmuş olan yürütme kurulunda bulunan üyeler ülkemizin 2012 yılında yaptığı düzenlemeyle benzeşmektedir.

Çizelge 1-7 Kritik Altyapı Koruma Komisyonu Yürütme Kurulu Üyeleri

1. Hazine Bakanı
2. Savunma Bakanı
3. Adalet Bakanı
4. Ticaret Bakanı
5. Ulaştırma Bakanı
6. Enerji Bakanı
7. Merkezi İstihbarat Başkanı
8. Yönetim ve Bütçe Ofisi Direktörü
9. Ulusal Acil Durum Yönetim Ajansı Direktörü
10. Başkanın Ulusal Güvenlik Asistanı
11. Başkan Yardımcısının Ulusal Güvenlik Asistanı

Terminolojik olarak detaylı tanımın yapıldığı ilk belge olan ve 2001'de çıkarılan Patriot Yasası içeriğinde "Kritik Altyapılar yetersizliği ya da tahribatı durumunda güvenlik, ulusal ekonomik güvenlik, kamu sağlığı veya emniyeti üzerinde zayıflatıcı bir etkisi olan –fiziksel ya da sanal- sistemler ve varlıklardır" şeklinde tanımlama yapılmıştır (American Congress, 2001).

Devam eden süreçte Temmuz 2002'de yayımlanan İç Güvenlik Ulusal Stratejisi belgesi içerisinde belirlenen kritik görev alanları içerisinde "Kritik Altyapıların ve Önemli Varlıkların" korunması ifade olarak eklenmiştir. 2007 yılında güncellenen belge içerisinde 17 farklı Kritik Altyapı Sektörü tanımlanmıştır (DHS, 2007). 2013 yılında yayımlanan Başkanlık Talimatı içerisinde listede küçük değişiklikler yapılmış ve sektör sayısı 16 olarak belirlenmiştir. Farklı yıllarda yapılan kritik altyapı sektörü belirleme çalışmalarının sunulduğu Çizelge 5-3'te kritik altyapı sektörlerinin 1996 yılına göre arttığı görülmektedir (White House, 2013a).

Çizelge 1-8 ABD 1996, 2007 ve 2013 Kritik Altyapı Sektörleri

1996 Yılı Kritik Altyapı Sektörleri	2007 Yılı Kritik Altyapı Sektörleri	2013 Yılı Kritik Altyapı Sektörleri
1. Telekomünikasyon 2. Elektrik Enerjisi Sistemleri 3. Gaz ve petrol ve taşımacılık 4. Bankacılık ve Finans 5. Taşımacılık 6. Su Destek Sistemleri 7. Acil hizmetler (sağlık, polis, yangın ve kurtarma) 8. Devletin sürekliliği	1. Tarım ve Gıda 2. Bankacılık ve Finans 3. Kimya 4. Ticari Tesisler 5. Ticari Nükleer Reaktörler, Maddeler ve Atık 6. Barajlar 7. Savunma Sanayii 8. İçme Suyu ve Su Arıtma Sistemleri 9. Acil Hizmetler 10. Enerji 11. Kamu Tesisleri 12. Bilgi Teknolojileri 13. Ulusal Anıt ve İkonlar 14. Posta Hizmetleri ve Taşıma Hizmetleri 15. Kamu sağlığı ve Sağlık Hizmetleri 16. Telekomünikasyon 17. Ulaştırma Hizmetleri	1. Tarım ve Gıda 2. Finans Hizmetleri 3. Kimya 4. Ticari Tesisler 5. Nükleer Reaktörler, Maddeler ve Atık 6. Barajlar 7. Savunma Sanayii 8. Su ve Atık Su Sistemleri 9. Acil Hizmetler 10. Enerji 11. Kamu Tesisleri 12. Bilgi Teknolojileri 13. Kamu Sağlığı ve Sağlık Hizmetleri 14. İletişim 15. Ulaştırma Hizmetleri 16. Kritik Üretim

2003 yılında yayımlanan "Siber Uzayın Emniyeti için Ulusal Strateji" belgesiyle her kritik sektöre "Bilgi Paylaşımı ve Analiz Merkezi (ISAC – Information Sharing and Analyze Center)" kurma zorunluluğu getirilmiştir. Bu merkezler üzerinden her sektördeki kurumun/kuruluşun kendilerine yapılan siber saldırıları takip etmeleri ve bu alanda trendler, zafiyetler ve iyi uygulamaları paylaşma görevi verildi. İç Güvenlik Bakanlığı (DHS – Department of Homeland Security) tarafından koordinasyonu yapılan bu süreçle kamu ve özel sektörden birçok ISAC ile düzenli iletişim sağlanmaktadır. Çizelge 5-4 ile bugün itibariyle 20 farklı ISAC'ın varolduğu görülmektedir (White House, 2003).

Çizelge 1-9 Bugün İtibariyle Kurulu Bulunan ISAC'lar (DHS, 2017c)

1. Otomotiv ISAC
2. Havacılık ISAC
3. İletişim ISAC
4. Savunma Sanayii ISAC
5. Aşağı Akım Doğalgaz ISAC
6. Elektrik ISAC
7. Acil Durum Yönetimi ve Müdahale ISAC
8. Finans Hizmetleri ISAC
9. Sağlık Hizmetleri ISAC
10. Bilgi Teknolojileri ISAC
11. Deniz ISAC
12. Ulusal ISAC
13. Ulusal Sağlık ISAC
14. Petrol ve Doğalgaz ISAC
15. Emlak ISAC
16. Araştırma ve Eğitim Ağı ISAC
17. Son Kullanıcı ve Satıcı Siber ISAC
18. Tedarik Zinciri ISAC
19. Raylı Sistemler, Kamu Taşımacılığı, Karayolu Yolcu Taşımacılığı ISAC
20. Su ISAC

1.4.3. Avrupa'da Kritik Altyapılar

AB'de Kritik altyapılarla ilgili ilk önemli belge 2004 yılında yayımlanan "Terörle Mücadele Sürecinde Kritik Altyapıları Koruma" başlıklı 2004/702 nolu Avrupa Konseyi talimatıdır. Bu talimat içerisinde kritik altyapılar "bozulmaları ya da tahrip edilmeleri durumunda vatandaşların sağlığı, güvenliği, emniyeti veya ekonomik refahı üzerinde ya da devletin fonksiyonlarını yerine getirme konusunda önemli olumsuz etkilere sahip fiziksel ve bilgi teknolojilerini içeren tesisler, ağlar, servisler

ve varlıklar" olarak tanımlanmıştır (EC, 2004). Bu belgede tanımlanan 9 kritik sektör aşağıda belirtilmiştir.

Çizelge 1-10 Avrupa Komisyonu 2004 yılı Kritik altyapı sektörleri (EC, 2004)

1. Enerji tesisleri ve ağları (Elektrik enerjisi, petrol ve gaz üretimi, depolanması, rafinerileri, iletim ve dağıtım sistemleri)
2. İletişim ve Bilgi Teknolojileri (telekomünikasyon, yayın sistemleri, donanımlar, yazılımlar ve internet ağları)
3. Finans (Bankacılık, emniyet ve yatırım)
4. Sağlık Hizmetleri (Hastaneler, kan bankaları, laboratuvarlar, ilaç depolama, araştırma ve geliştirme, acil servisler)
5. Gıda (gıda güvenliği, üretimi, toptan dağıtımı ve endüstrisi)
6. Su (barajlar, depolama, iyileştirme ve ağları)
7. Taşıma (havalimanları, limanlar, karma ulaşım alanları, raylı sistemler, toplu taşıma ağları, trafik kontrol sistemleri)
8. Tehlikeli ürünlerin üretim, depolama ve taşıma (kimyasal, biyolojik, radyolojik ve nükleer tesisler)
9. Kamu (kritik hizmetler, tesisler, bilgi ağları, varlıklar ve anahtar ulusal tesis ve anıtlar)

Devam eden süreçte öncelikle 2006 yılında "Kritik Altyapıların Korunması için Avrupa Programı EPCIP (European Programme for Critical Infrastructure Protection)" yayınlanmış olup bu programla konunun çerçevesinin yatay bir kurguyla detaylandırılması sağlanmıştır (EC, 2006). Kritik altyapılara maruz kalabileceği olumsuz durumlarla ilgili risklerin minimize edilmesi gerektiğinin vurgulandığı belgede karşılıklı işbirliği vurgusu yapılmıştır.

2008 yılında yayımlanan 2008/114/EC sayılı "Avrupa kritik altyapılarının belirlenmesi ve koruyucu tedbirlerin arttırılması" isimli Avrupa Konseyi talimatı yayımlanmıştır. Bu belgede "Kritik Altyapı – CI (Critical Infrastructure)" terimi "bozulması ya da tahribatı durumunda üye ülkelerde bulunan, vatandaşların temel

yaşam fonksiyonlarını sürdürmeleri için gerekli olan sağlık, güvenlik, emniyet, toplumsal hizmetler, ekonomik veya sosyal refahın etkilenmesine neden olacak varlık, sistem ya da bunların herhangi bir parçası" şeklinde tanımlanmıştır. Ayrıca bu belgede ilave olarak "Avrupa Kritik Altyapısı – ECI (European Critical Infrastructure)" isimli yeni bir terim türetilmiş olup bu terimin tanımı "zarar görmesi ya da tahrip olması durumunda üye ülkelerden en az ikisinin olumsuz etkileyecek ve üye ülkelerde bulunan kritik altyapılar" şeklinde yapılmıştır (EC, 2008).

Kritik altyapı sektörlerinin yenilenmediği 2008 talimatında Enerji sektöründe Elektrik, Petrol ve Gaz; Taşıma sektöründe ise Karayolu, Raylı Sistem, Havayolu, İç Suyolları, Okyanus ve Kısa Deniz Taşımacılıkları ve Limanlar ECI'lar arasında yer almıştır (EC, 2008).

Fransa özelinde kritik altyapıların güvenliği konusu irdelendiğinde Savunma ve Ulusal Güvenlik Genel Sekreterliği (General Secretariat for Defence and National Security (SGDSN)) tarafından 2013 geliştirilip yayımlanan "Kritik Altyapı Koruma – CIP (Critical Infrastructure Protection)" yürürlüktedir. Bu programa göre Çizelge 5-7'de sunulan 12 farklı sektör kritik altyapı sektörü olarak tanımlanmıştır (ANSSI, 2017b).

Çizelge 1-11 Fransa'daki Kritik Altyapı Sektörleri

1. Gıda
2. Su Yönetimi
3. Sağlık
4. Sivil Aktiviteler
5. Yasal Aktiviteler
6. Askeri Aktiviteler
7. Enerji
8. Finans
9. Taşıma
10. İletişim, teknoloji ve yayın
11. Endüstri
12. Uzay ve araştırma

Çizelge 5-8'de ve 5-9'da sunulan ülkemiz, ABD, Fransa ve AB'nin kritik altyapı sektörleri ve sektörlerin ilk oluşturma tarihleri incelendiğinde ABD'nin 16, Fransa'nın 12, Türkiye'nin 6 sektörü kritik olarak belirlediği, ülkemizin ABD'den 20 yıl sonra, Fransa'dan ise ilk defa 12 yıl sonra kritik altyapı sektörlerini oluşturduğu görülmektedir.

Çizelge 1-12 Kritik Altyapı Sektörleri Karşılaştırma Çizelgesi

Türkiye[3]	ABD	Fransa	AB
1. Elektronik Haberleşme 2. Enerji 3. Su Yönetimi 4. Kritik Kamu Hizmetleri 5. Ulaştırma 6. Bankacılık ve Finans	1. Tarım ve Gıda 2. Finans Hizmetleri 3. Kimya 4. Ticari Tesisler 5. Nükleer Reaktörler, Maddeler ve Atık 6. Barajlar 7. Savunma Sanayii 8. Su ve Atık Su Sistemleri 9. Acil Hizmetler 10. Enerji 11. Kamu Tesisleri 12. Bilgi Teknolojileri 13. Kamu Sağlığı ve Sağlık Hizmetleri 14. İletişim 15. Ulaştırma Hizmetleri 16. Kritik Üretim	1. Gıda 2. Su Yönetimi 3. Sağlık 4. Sivil Aktiviteler 5. Yasal Aktiviteler 6. Askeri Aktiviteler 7. Enerji 8. Finans 9. Taşıma 10. İletişim, teknoloji ve yayın 11. Endüstri 12. Uzay ve araştırma	1. Enerji tesisleri ve ağları 2. İletişim ve Bilgi Teknolojileri 3. Finans 4. Sağlık Hizmetleri 5. Gıda 6. Su 7. Taşıma 8. Tehlikeli ürünlerin üretim, depolama ve taşıma 9. Kamu

[3] Ülkemizin kritik altyapıları ile ilgili sorumlu bir kurum belirlenmediğinden en son yapılmış düzenlemeye burada yer verilmiştir.

Çizelge 1-13 Kritik Altyapı Sektörlerini ilk oluşturma ve son güncelleme tarihleri

Türkiye[4]	ABD	Fransa	AB
2016	1996, 2013	2004, 2013	2004

1.4.4. Dünya Genelinde Kritik Altyapılarda Yaşanan Siber Olaylar

1.4.4.1. Stuxnet (2010)

2010 yılı Haziran ayında varlığı bir zararlı yazılımdır. Büyük antivirüs yazılımlarının uzmanları tarafından uzun bir süre detayları üzerine incelemeler yapılarak raporlanmıştır. İran'ın uranyum zenginleştirme programını hedef almıştır. Uranyum zenginleştirme tesisindeki santrifüjlerin dönüş hızlarını yöneten donanımlara bulaşarak santrifüjlerin kullanılamaz hale gelmesine neden olmuştur. Politik olarak kullanıldığının değerlendirilmesi ve yayılma tarzı açılarından bir ilktir (Falliere, Murchu, & Chien, 2011; Reuters, 2013a; VirusBlokAda, 2010).

Symantec ve Eset isimli antivirüs üreticilerinin yaptığı geniş inceleme sonucunda yazılımın Siemens'in S7 300 model cihazıyla karşılaşmadığı sürece hiçbir zararının olmadığı ve bu cihazla karşılaşana dek düzenli yayılma politikası güttüğü belirlenmiştir. Windows işletim sistemi üzerinde hareket eden ve Sıfırıncı Gün

[4] Ülkemizin kritik altyapıları ile ilgili sorumlu bir kurum belirlenmediğinden en son yapılmış düzenlemeye burada yer verilmiştir.

Zafiyetlerini kullanarak yayılan solucan çalıntı dijital bir imza kullanarak bulaştığı bilgisayarların kendisini zararlı olarak farketmelerinin önüne geçmiştir. S7 300'ü farkettiği anda bu cihazı yöneten Programlanabilir Mantıksal Kontrol Cihazını (PLC - Programmable Logical Controller) ele geçirerek bu cihazın çalışma kodlarını değiştirmiştir. Kod değişimi sonrasında Santrifüjün dönüş frekansları ana izleme merkezinden farkedilmeyecek hızlarda ama sisteme zarar verir şekilde değiştirilmiştir (Falliere et al., 2011; Matrosov, Rodionov, Harley, & Malcho, n.d.).

Uluslararası haber kaynakları bu saldırının ABD ve İsrail ortaklığında yapıldığını ve İran'ın Natanz Uranyum Zenginleştirme Tesisi'ni hedef aldığını duyurdu. İran'ın 5000 santrifüjünün 1000 adedinin bu saldırıyla kullanılamaz duruma geldiğinin belirtildiği haberler ve UAEA'ın rutin hazırladığı envanter bilgisi raporları bu iddiaları doğrular niteliktedir (Albright, Brannan, & Walrond, 2010; NyTimes, 2012; Reuters, 2013a; UAEA, 2010a).

1.4.4.2. Monju NGS Olayı (2014)

2014 yılında Japonya'da bulunan Monju Nükleer Enerji Santralinin ana kontrol odasında bulunan 8 bilgisayara sızılarak 42.000 email'in ve bazı personel eğitim raporlarının elde edilmesi olayıdır Bilgi İşlem yöneticisinin dışarıya giden ağ trafiğinde rutin dışı bir davranış gözlemlemesiyle farkedilmiştir. Bir çalışanın ücretsiz bir yazılımı (video player) bilgisayarına indirmesiyle harekete geçen bir malware olduğu tespit edilmiştir (Dine, Assante, & Stoutland, 2016; NTI, 2017c; SecurityAffairs, 2014).

1.4.4.3. Almanya Çelik Fabrikası Olayı (2014)

Almanya Federal Bilgi Güvenliği Ajansı'nın (Bundesamt für Sicherheit in der Informationstechnik) yayımladığı Bilgi Teknolojileri Güvenliğine ilişkin raporda Almanya'daki bir çelik fabrikasının siber saldırıya maruz kaldığı belirtildi. Bu olay Stuxnet'ten sonra fiziksel zararın meydana geldiği önemli bir siber saldırı olarak değerlendirilmiştir. Hasarla ilgili detay verilmeyip "Büyük Hasar" ifadeleri kullanılan rapora göre saldırganlar öncelikle fabrikanın yerel ağına erişti ve endüstriyel kontrol donanımlarına müdahale ederek, yüksek ısı fırınlarının kapanmasını engellediler (BSI, 2014; Lee, Assante, & Conway, 2014; wired, 2015).

1.4.4.4. Korea Hydro & Nuclear Power Co Olayı (2014)

Güney Kore'de 23 nükleer reaktör işleten şirket siber saldırıya maruz kaldığını, kritik olmayan verilerin çalındığı, reaktör operasyonlarının risk altında olmadığını açıkladı. 10binin üzerinde çalışanı bulunan şirkette çalışan bilgilerinin, reaktörlerle ilgili bazı verilerin, destek sistemleriyle ilgili detayların çalındığının belirtildiği olayda sıklıkla Kuzey Kore'li hackerlar tarafından kullanılan "Kimsuky" isimli bir malware'in kullanılması ayrıca önemli bir detaydır (MIN, 2017; Reuters, 2016b; TheGuardian, 2014).

1.4.4.5. The Gundremmingen Nükleer Güç Santrali (2016)

Alman bir haber ajansına dayandırılan bilgilerde The Grundremmingen isimli Nükleer Güç Santralinde tespit edilen W32.Rammit ve Conficker isimli iki virüs santralin operasyonlarının yürütüldüğü kısıtlı ağa erişmeden tespit edildi. Kendisini sürekli kopyalamak ve veri çalmak için yazılmış bu virüslere sıklıkla USB disklerde rastlanmış olması kısıtlı ağlarda güncelleme gibi amaçlarla USB disk kullanma süreçlerinin güçlü politikalarla yürütülmesi gerektiğini birkez daha ortaya koymuştur (Reuters, 2016a; SecurityAffairs, 2016; TrendMicro, 2016).

1.4.4.6. Davis-Besse NGS Olayı (2003)

ABD Ohio'da bulunan Davis-Besse isimli NGS'nin Slammer solucanından etkilenmesi olayıdır. Çok hızlı bir şekilde yayılan solucan Microsoft SQL 2000 isimli veritabanı sunucu uygulamasında bulunan zafiyetleri kullanarak ağdaki bilgisayarları tarayarak rastgele IP adreslerine kendisini yaymaktadır. Santralde ağlar arasında atlayan solucan operasyonun yürütüldüğü ağa erişmiş ve operasyonu yürüten bilgisayarlara bulaştıktan sonra yarattığı trafik sebebiyle bilgisayarların hizmet verememesine neden olmuştur. Yaklaşık 5 saat kadar soğutma sistemleri, ısı sensörleri ve radyasyon tespit donanımlarına erişilememiştir. Santralin güç üretmediği ve tatbikat amaçlı sistemlerinin çalıştırıldığı bir dönemde bu olayın yaşanmış olması olası problemlerin önüne geçmiştir, Microsoft firması tarafından bu solucan için olaydan 6 ay önce yama yayınlamış ancak santralin ilgili ekibi tarafından bu yamanın uygulanmamıştır. Bu detay santrallerin siber güvenlik ekiplerinin Yama Yönetimi

(Patch Management) konusunda dijital varlıklarının üreticilerini düzenli takip görevlerinin önemini ortaya koymaktadır (Baylon, Brunt, & Livingstone, 2015; Kesler, 2011; Poresky, Adreades, Kendrick, & Peterson, 2017).

1.4.4.7. Orchard Operasyonu (2007)

Suriye'nin Dair Alzour kentinde bir tesiste Kuzey Kore ile ortak ve gizli bir şekilde nükleer santral inşaa ettiği ve ABD ve İsraillin ortak bir hava harekatında inşaa halindeki tesisi bombalaması olayıdır. İsrail ve Suriye basını olayla ilgili uzun süre sessiz kalmış ancak ABD basını olayı dünyaya duyurmuştur. UAEA resmi inceleme talebini Suriye 8 ay sonra onaylamıştır. Bombalamaya dair herhangi bir emarenin kalmadığı alansa UAEA uzmanlarının yaptığı inceleme sonucunda bölgeden alınan toprak numunelerinde insan yapımı olağan dışı radyoaktif maddelere rastlandığı belirtildi. Konunun siber tarafı ise Suriye'nin Rusya'dan aldığı hava savunma sistemi İsrail savaş uçaklarını farketmemişti. İsraillin bu süreçte kullandığı siber yöntemlerle ilgili teyitli bilgi bulunmamakla birlikte uzmanlar tarafından köstebek yardımı, sinyalle sistemi uyutma, bozuk sinyal gönderimi, gibi birçok ihtimalden bahsedilmektedir (Clarke & Knake, 2011a; Reuters, 2009; TheGuardian, 2007; YnetNews, 2011).

1.4.4.8. Shamoon Virüsü (2012)

2012 yılında varlığı tespit edilen bir virüstün. Temel olarak 3 bileşeni (Sızma, Silme, Raporlama) bulunan virüs bir sisteme sızdıktan sonra sistemdeki verileri bir merkeze göndermek ardından silerek son durumu raporlamaktadır. Enerji sektörüne

önemli saldırılar yaptığı bildirilmiştir. Suudi Arabistan'ın büyük petrol devi Saudi Aramco isimli şirketin bilgisayarlarına sızarak verilerin büyük bölümünü çalarak bilgisayarları silmiştir. Resmi açıklamalarda şirketin operasyonlarını engellemediği belirtilse de gerçekte ne kadar zarar verdiği bilinmemektedir. ABD, Aramco saldırısı konusunda İran'ı suçlamıştır (BBC, 2012; ICS-CERT, 2012; NYTimes, 2012; Symantec, 2012).

1.4.4.9. Estonya (2007)

Estonyalıların Rusya'nın desteğiyle İkinci Dünya Savaşı'nda Nazi İşgalinden kurtulması sonrasında 1947 yılında Talin'e Rusya tarafından dikilen Kızıl Ordu Anıtı ya da diğer adıyla Bronz Asker Anıtı isimli heykel 2007 yılında Estonya tarafından yerinin değiştirilmesi amacıyla kaldırılması sonrasında siber saldırılar yaşanmıştır. Estonya'ya ait kamu internet siteleri ve bankacılık sistemi hizmet veremez hale gelmiştir. Rusya'nın Estonya'daki konumunu simgelemesi, bazı Rus sitelerinde Estonya internet sitelerinin nasıl çökertileceğine dair bilgilerin bulunması muhtemel şüpheliyi Rusya haline getirse de resmi olarak Rusya bu saldırıları hiçbir zaman üstlenmemiştir (Çifci, 2013).

1.4.4.10. Gürcistan (2008)

Gürcistan'a ait bazı web sitelerine sanal ortamda yapılan saldırılar olarak bilinir. 2008 yılında Rusya ile Gürcistan arasında yaşanan çatışmaların sonrasında gerçekleşmiştir. Gürcistan hükümet siteleri bir süre hizmet verememiştir. Gürcistan Başkanı Mikhail Saakashvili'nin kişisel web sitesi hacklenmiştir (BBC, 2008).

1.4.4.11. Wikileaks (2006)

2006 yılı aralık ayında wikileaks.org isimli sitenin isminin (domain) satın alınması sonrasında başlayan devletlere ait gizli bilgilerin yayınlanması süreci olarak bilinmektedir. Guantanamo Esir Kampı, Irak Savaşı, Afganistan Savaşı, Kenya Yolsuzluk Soruşturması ve ülkemizle ilgili birçok belge yayımlanmıştır (Domscheit-Berg, Klopp, & Chase, 2011).

1.4.4.12. Avustralya Atık Sistemi SCADA Olayı (2000)

40'lı yaşların sonunda işten çıkarılan Avustralyalı bir yazılımcı/hacker Maroochyshire Atık Su İşleme Tesisi kontrol sistemlerine yaklaşık 2 ay boyunca bağlanarak kanalizasyon pompalarına rutinin dışında emirler vererek toplamda 800.000 litre işlenmemiş atığı kontrolsüz alana yönlendirmiştir. Bu olay yakında bulunan nehire atıkların ulaşmasıyla canlı yaşamını ve kötü kotu nedeniyle de sakinlerin yaşamını önemli ölçüde etkilemiştir (Abrams & Weiss, 2017).

2. GEREÇ ve YÖNTEM

Tezle ilgili tüm araştırmalar ulusal ve uluslararası kurumlardan edinilen kamuya açık dokümanlar, teze konu alanla ilgili özel ya da kamuya ait kurum ve kuruluşların web kaynakları, ulusal ve uluslararası katılım sağlanan toplantılardan edinilen kamuya açık belgeler, kütüphanelerden elde edilen diğer dokümanlar kullanılarak elde edilen bilgilerin derlenmesi sonucu hazırlanmıştır. Derleme sonucunda elde edilen her bir bilgiyle ilgili; ülkeler, her bir alt alanın sorumlu kuruluşunun belirlenmesi, her bir kurumun sorumluluk sınırlarının çizilmesi ve bunların karşılaştırılması yöntemine başvurulmuştur.

3. BULGULAR

3.1. Siber Olaylara Müdahale Konusunda Ülkelerin İdari Yapıları

3.1.1. Türkiye

Bu bölümde ülkemizdeki siber güvenlikle ilgili idari yapı nükleer tesisler çerçevesinden incelenmiştir. Bu sebeple siber güvenliğe dönük atılan tüm adımlar kurulan tüm kurumlarla ilgili detaylı bilgi içermemektedir.

3.1.1.1. Ülkemizdeki Nükleer Tesisler

Ülkemizde aktif olarak çalışan Nükleer Santral bulunmamaktadır. 2 adet araştırma reaktörü bulunmaktadır. TAEK tarafından 1961 yılında kurulumu gerçekleştirilen TR-1 isimli reaktörün yanında, 1984 yılında TR-2 adıyla 2. Araştırma reaktörü hayata geçmiştir. TR-1 1 MW gücünde olup TR-2 5 MW gücündedir (TAEK, 2010b).

Ayrıca 1967 yılında da Ankara'da bir Nükleer Araştırma Merkezi açılmıştır. Bu merkez günümüzde Sarayköy Nükleer Araştırma ve Eğitim Merkezi adıyla faaliyet yürütmektedir (TAEK, 2017g).

3.1.1.2. Nükleer Siber Güvenlikle İlgili Kurumlar, Yapıları, Görev Alanları

3.1.1.2.1. Enerji ve Tabii Kaynaklar Bakanlığı

Bakanlık nükleer alanla ilgili faaliyetlerini ana hizmet birimlerinden birisi olan **Nükleer Enerji Proje Uygulama Dairesi (NEPUD)** üzerinden yürütmektedir. Bu birimin; nükleer enerji alanında; mevzuat, insan kaynağı oluşturma, eğitim, sanayi ve teknoloji gibi alanlarda düzenlemelerin yapılması amacıyla gerekli çalışmaları yapmak, bu çalışmaları yaparken paydaş sayılabilecek tüm kurum ve kuruluşların bir araya gelmesini sağlamak, görev alanlarıyla ilgili kamuoyunu bilgilendirmek, ulusal/uluslararası kuruluşlar tarafından yürütülen çalışmalara katılmak gibi görevleri bulunmaktadır (TAEK, 2016; TBMM, 1985).

Enerji ve Tabii Kaynaklar Bakanlığı'na bağlı kuruluş statüsünde faaliyet gösteren diğer bir birim ise **Türkiye Atom Enerji Kurumu**dur (TAEK). 1956 yılında Atom Enerjisi Komisyonu adıyla kurulmuş olup Uluslararası Atom Enerjisi Ajansının ülkemizdeki iletişim noktası olmakla birlikte, bu ajansın dünya genelindeki görevlerini ülkemizde uygulayabilmek için çalışmalar yapmaktadır (UAEA, 2010d).

2690 sayılı kanunla kurulmuş olan TAEK'in görevleri nükleer enerjiden elektrik üretme çalışmalarını düzenleme, teşvik, lisanslama ve denetleme olarak belirlenmiştir. Bahse konu lisanslamalar nükleer güvenlik, nükleer emniyet ve radyasyondan korunma alanlarındadır. Kurum siber emniyetle ilgili birim bulundurmamakta olup

kuruluş kanununda da geçtiği üzere fiziksel korunmayla ilgili süreçler Nükleer Güvenlik Dairesi tarafından yürütülmektedir (TAEK, 2009; TBMM, 1982).

2002 yılında kadar Başbakanlık'a bağlı faaliyet gösteren kurum 2002 yılında Enerji ve Tabii Kaynaklar Bakanlığına bağlı kuruluş statüsünde bağlanmıştır. Kuruma ait İstanbul Küçükçekmece Gölü kenarında bir araştırma reaktörü (Çekmece TR-1, 1 MW) bulunmaktadır. 1962 yılında bilimsel araştırmalar amacıyla açılan bu reaktörden sonra 1967 yılında da Ankara'da bir Nükleer Araştırma Merkezi açılmıştır. Bu merkez günümüzde Sarayköy Nükleer Araştırma ve Eğitim Merkezi adıyla faaliyet yürütmektedir (DPB, 2017; Kestane, 2002; TAEK, 2016, 2017h).

3.1.1.2.2. Ulaştırma Denizcilik ve Haberleşme Bakanlığı - Siber Güvenlik Kurulu

2012 yılında 2012/3842 sayılı Bakanlar Kurulu kararıyla Ulaştırma Denizcilik ve Haberleşme Bakanlığına bağlı olarak Siber Güvenlik Kurulu oluşturulmuş, 2014 yılında Elektronik Haberleşme Kanununda yapılan değişiklikle aynı bakanlığa kurul adına sekretarya yapma görevleri verilmiştir. Kurul üyeleri ile ilgili oluşum aşağıdaki şekildedir (Bakanlar Kurulu, 2012; TBMM, 2014a):

- Ulaştırma, Denizcilik ve Haberleşme Bakanı (Kurul Başkanı olarak)
- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,

- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,
- Genel Kurmay Başkanlığı MEBS Başkanı,
- Bilgi Teknolojileri ve İletişim Kurumu Başkanı,
- TÜBİTAK Başkanı,
- MASAK Başkanı,
- TİB başkanı
- Ulaştırma Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticileri

Kurul ilk toplantısını Aralık 2012 yapmış ve bu toplantıda aldığı kararlar Haziran 2013'te **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı** Bakanlar Kurulu kararıyla yayımlanarak yürürlüğe girmiştir (BTK, 2017). Kararın giriş bölümünde kamu kurumlarının yanında enerji, su kaynakları, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşların da bilgi ve iletişim sistemlerini yoğun olarak kullandıkları belirtilmiştir. Aynı kararda kritik altyapılara ait bilişim sistem ve verilerini hedef alan ısrarcı ve gelişmiş siber saldırıların kimler tarafından finanse ve organize edildiğinin tespitinin neredeyse imkansız olduğu ayrıca siber ortamdaki risk ve tehditlerin asimetrik karakterinin mücadeleyi zorlaştırdığına vurgu yapılmıştır. 2013-2014 yıllarını kapsayan 7 ana başlıkta 29 adet eylemle ilgili 31 farklı kurum, kuruluş ve organizasyonun sorumlu tutulduğu planda bu yılları aşan periyodik faaliyetler, eğitim çalışmaları ve bilinçlendirme çalışmalarının ayrıca belirtildiği kararda kritik altyapı aşağıdaki şekilde tanımlanmıştır (Bakanlar Kurulu, 2012).

“Kritik Altyapılar: 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 altyapı”dır

Kararda kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanması, olayların etkilerinin en düşük düzeyde kalması, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesi durumlarını oluşturmaya dönük bir altyapının hazırlanması amaç olarak belirtilmiştir. Merkezi bir yapı ile siber olaylar konusunda düzenli iletişim, destek ve koordinasyonun planlandığı kararda USOM (Ulusal Siber Olaylara Müdahale Merkezi) isimli bir çatı yapı kurulmuş ve bu yapıya “bağlı” her kamu kurumunda her sektörde SOME (Siber Olaylara Müdahale Ekibi) isimli alt kuruluşların kurulacağı belirtilmiştir.

Kararda kritik altyapılara ülkemizde hangi sektörlerin girdiğine dair herhangi bir ifade görülmemiştir.

Karar sonrasında Kasım 2013’te **SOME’lerin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esasları Belirleyen Tebliğ** yayımlanmıştır. Bu tebliğle SOME’lerin Kurumsal SOME ve Sektörel SOME olarak ikiye ayrıldığı, Kurumsal SOME’lerin Bakanlıklar bünyesinde bakanlık birimlerini kapsayacak şekilde ihtiyaç

adedince, Sektörel SOME'lerin ise düzenleyici ve denetleyici kurumlar bünyesinde kendi sektörlerini kapsayacak şekilde kurulacağı belirtilmiştir (TBMM, 2013).

Kritik sektörlerde sektörel SOME'lerin kurulmasının zorunlu olduğu ve bu sektörlerin Siber Güvenlik Kurulu tarafından belirtileceğinin ifade edildiği SOME tebliğinde USOM'un tüm SOME'lerle koordinasyon içerisinde olacağı, karşılıklı bilgi paylaşımının esas olduğu, yaşanan siber olaylara her SOME'nin kendi imkanları ölçüsünde yanıt vermesi gerektiği, her SOME'nin destek ihtiyacını öncelikle kendi Sektörel SOME'sine sonrasında USOM'a bildirebileceği, siber olaya müdahale esnasında farkedilen suçların kanunen yetkili birime bildirmesi işleminin SOME'nin kendisi tarafından yapılacağı ama sonrasında USOM'a da bildirileceği ayrıca belirtilmiştir (TBMM, 2013).

Bahse konu tebliğ sonrasında Eylül 2016'da **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı** açıklandı. Planın ayrıca resmi gazetede yayımlandığına dair herhangi bir tespit yapılamadı. UDHB web sitesinden erişimin mümkün olduğu planda kritik altyapı tanımına ek olarak kritik altyapı sektörleri ilk defa tanımlandı (UDHB, 2016).

"**Kritik altyapı sektörleri**: 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma", ve "Bankacılık ve Finans" sektörlerini ifade eder."

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının Siber Güvenlik Riskleri bölümünde kritik altyapıların kullanıldığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırıların, kritik altyapılara yapılacak saldırılar sonucunda vatandaşa ait ya da kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi önemli riskler olarak değerlendirilmiştir (UDHB, 2016).

Aynı eylem planında kritik altyapıların bağlı oldukları düzenleyici kurum tarafından denetlenmesi, kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması, her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması gerektiği, farkındalık arttırıcı çalışmalar yapılması gerektiği, kamu ve özel sektörden alanla ilgili tüm kuruluşlarının katılımıyla ulusal bir siber güvenlik eko-sistemi oluşturulması gerektiği hususlar amaçlar olarak sıralanmıştır (UDHB, 2016).

Belgenin sonunda "Ek-B" başlığı altında "Düzenleyici ve Denetleyici Kurum Listesi"nin paylaşıldığı ve ülkemizde nükleer santrallerin fiziksel ve siber emniyetiyle ilgili düzenleyici ve denetleyici yetkisi bulunan Türkiye Atom Enerjisi Ajansının bu listede yer almadığı nükleer santral lisans sahibinin enerji arzı ile ilgili düzenleyici kurumu olan Enerji Piyasası Düzenleme Kurumu Başkanlığının (EPDK) yer aldığı, ayrıca "Ek-C" başlığı altında "Sektörel SOME Listesi"nin paylaşıldığı ve enerji sektöründeki Sektörel SOME'nin EPDK olarak gösterildiği görülmüştür (Webrazzi, 2017).

UDHB ile ilgili yapılan bu inceleme sonucunda nükleer santrallerin her iki strateji belgesinde Kritik Altyapı tanımına uyduğu, SOME tebliği içeriğinde belirtilen

Sektörel SOME'sinin kurulmasının zorunlu olduğu, 2016-2019 Eylem Planı Belgesinde bir enerji üretim tesisi olan nükleer santrallerle ilgili sektör sorumlusunun EPDK olduğu belirtilmiştir (UDHB, 2016).

3.1.1.2.3. TSK Siber Savunma Komutanlığı

İlk olarak 2012 yılında "Siber Savunma Merkezi Başkanlığı" adıyla bir başkanlık kurulmuş 2013 yılında bu başkanlık "TSK Siber Savunma Komutanlığı"na dönüştürülmüştür. Hürriyet gazetesinin komutanlığa yaptığı ziyaret ve yetkililerden aldığı bilgilere dayandırdığını belirttiği haberde; Komutanlık bünyesinde 7/24 hizmet veren Siber Savunma Hareket merkezi oluşturulduğu, TSK sistemlerine yönelik saldırı veya siber olayların yaşanması durumunda önleyici faaliyet yürütüldüğü, TÜBİTAK, USOM, NATO gibi kurumlarla eşgüdüm içerisinde hareket edildiği belirtilmektedir(Akşam, 2016; Hürriyet, 2016). Başka bir kaynakta ise bu komutanlığın görevleri şöyle tanımlanmıştır:

> "*1. TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunmasını sağlamak.*
>
> *2. Siber olaylara 7/24 esasına göre müdahale etmek.*
>
> *3. Ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak etmek.*
>
> *4. TSK çağında bilinçlendirme ve eğitim faaliyetleri yürütmek.*
>
> *5. TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeler ve testleri yapmak.*(Çelikpala, Bıçakçı, & Ergün, 2015)"

2016 yılında ise Savunma Sanayii Müsteşarlığı (SSM)'e TSK Siber Savunma Merkezi Projesi (SİSAMER) projesinin hayata geçirilmesi için yetki verildi. Projenin detayları ile açık kaynaklarda bilgi paylaşımı görülmemiş olup Temmuz 2017 SİSAMER'in Harekat Merkezi Tesisi ilk safha modernizasyonunun tamamlandığı duyurulmuştur (Akşam, 2016; TSK, 2017; @TSKGnkur, 2017).

3.1.1.2.4. Başbakanlık – AFAD

Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) 2009 yılında Başbakanlığa bağlı olarak 5902 sayılı kanunla kurulmuştur. Afet tanımı içerisinde giren her türlü durumla ilgili hazırlık, zarar azaltma, müdahale, iyileştirme sürecinde koordinasyon gibi görevler bu kanunla AFAD'a verilmiştir. Aynı kanun içerisinde yapılan Afet tanımında "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 olayları yapılacak Kanunda yapılan afet tanımı" denilerek teknoloji kaynaklı olaylarla ilgili sorumluluk da AFAD'a verilmiş görünmektedir (TBMM, 2009).

Eylül 2014 de AFAD tarafından "**2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi**" yayımlanmıştır (AFAD, 2014). Bu belgede de bir kritik altyapı tanımı yapılmıştır:

"**Kritik Altyapı**: İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür."

2012 yılında 2012/3842 sayılı Bakanlar Kurulu kararıyla kurulan Siber Güvenlik Kurulu üyeleri arasında AFAD bulunmamaktadır. 2012'deki bu karar sonrasında 2014 yılında AFAD tarafından hazırlanmış yol haritası belgesinin sunuş bölümünde siber tehlikelerin günümüzde doğal afetler kadar ses getirdiği, özellikle kritik altyapılara gerçekleştirilecek siber saldırıların ülke genelinde büyük afetlere neden olabileceği, AFAD başkanlığı olarak konu ile ilgili kritik altyapı ve tesislerin belirlenip risk analizlerinin yapılması ve önceliklendirme çalışmalarının sürdüğü belirtilmiştir. Aynı belgenin devam eden bölümlerinde Siber Güvenlik Kurulunun kurulmuş olmasının Kritik Altyapıların siber güvenliği alanında idari, teknik ve hukuki yapıların oluşturulması sürecini hızlandırabileceği değerlendirilmiştir. Bu belgede herhangi bir siber güvenlik krizinin nasıl yönetileceğine dair detay bulunmamaktadır(AFAD, 2014; TBMM, 2009).

3.1.1.2.5. Bilim Sanayi ve Teknoloji Bakanlığı - TÜBİTAK

1963 yılında Bilim Sanayi ve Teknoloji Bakanlığına ilgili kuruluş statüsünde bağlı olarak kurulmuştur. Siber Güvenlik Kurulunun kurulmasına kadar ülkemizde siber güvenlikten sorumlu kuruluş olarak da faaliyetlerini yürütmüştür. 2012 yılında bu görevini devretmiş olsa dahi Siber Güvenlik Kurulu'nun Siber Güvenlik Strateji Belgesi ve Eylem Planı hazırlamakla sınırlı bir görev üstlendiğinden ve siber bir olayın içeriği, müdahalesi, iyileştirmesi süreçleriyle ilgili TÜBİTAK konuya müdahil olan kurumlardan birisidir. Ülkemizin akredite olmuş ilk CERT ekipleri TÜBİTAK BİLGEM bünyesinde kurulmuş olan TR-BOME ve TÜBİTAK ULAKBİM bünyesinde bulunan Ulak-CSIRT'tür (BSTB, 2017; Şentürk, Çil, & Sağıroğlu, 2012;

TÜBİTAK, 2017c; Ulakbim, 2010). Bünyesinde önemli hizmetler veren kuruluşlar bulunmaktadır.

BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi): bilgi güvenliği, ileri serviye elektronik alan çalışmaları ve bilişim alanlarında ihtiyaçlara dönük çözümler üretmek amacıyla 2010 yılında oluşturulmuş bir ar-ge merkezidir. Tübitak bünyesinde bulunan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ile Bilişim Teknolojileri Enstitüsünün (BTE) birleştirilmesiyle oluşturulmuştur. 2012 yılında BİLGEM bünyesinde Yazılım Teknolojileri Araştırma Enstitüsü (YTE), Siber Güvenlik Enstitüsü (SGE) ve İleri Teknoloji Araştırma Enstitüsü (İLTAREN) olmak üzere 3 tane enstitü kurulmuştur (TÜBİTAK, 2017a).

SGE (Siber Güvenlik Enstitüsü): 1997 yılından hayata geçirilmiş olan Ağ Güvenliği Grubu adıyla kurulmuş laboratuvarın 2010 yılında BİLGEM'in kuruluşuyla birlikte BİLGEM bünyesinde faaliyet göstermeye başladı. 2012 yılında ise ismi değiştirilerek SGE oldu. 1997 yılında bilişim sistemleri ve ağ seviyesindeki saldırıları önlemek amacıyla kurulmuşken zaman içerisinde Microsoft ve açık kaynak kodlu sistemlerin, e-posta sunucularının, veritabanlarının, aktif ağ cihazlarının savunması alanında da çalışmalar yaptı. Ülke genelinde siber dünya konusunda farkındalık arttırma faaliyetleri amacıyla kamu ve kritik özel sektör kurumlarına(bankacılık, telekomünikasyon ve otomotiv) Risk Analiz, Bilgi Güvenliği Yönetim Sistemleri konularında kurulum ve danışmanlık hizmetleri, kamu kurumlarında çalışan personellere yönelik Kamu Bilgi Güvenliği Projesi kapsamında eğitimler vermektedir (TÜBİTAK, 2017b).

Bünyesinde başka kuruluşları da barındıran kuruluş tarafından geliştirilmiş ürünler/hizmetler aşağıda belirtilmiştir:

- TSK ağının güvenliği için Demet Kripto Cihazının (MİLON-5) geliştirilmesi ve üretimi,
- Kriptolu Cep Telefonu (MİLCEP-K1) geliştirilmesi,
- IP Kripto Cihazı'nın (IPKC-G) geliştirilmesi,
- Kriptolu USB Belleğin (SIR) geliştirilmesi,
- Akıllı Kart İşletim Sisteminin (AKİS) geliştirilmesi,
- Sahil Gözetleme Radarı (SAGRAD) ve Gemi Gözetleme Radarlarının (GEMRAD),
- Kamu Sertifikasyon Merkezinin kurulumu, geliştirilmesi
- İlk mikroçip üretimi
- Elektronik Harp Araştırma Merkezinin açılması
- İlk Elektronik İmza Sisteminin geliştirilmesi,
- İlk Linux Tabanlı İşletim Sistemi Pardus (2007)

Ayrıca bu alanların tamamında test ve değerlendirmeleri yapabilen ve muteber raporlamayı yapan laboratuvarlara sahiptir (Çelikpala et al., 2015; TÜBİTAK, 2017d).

3.1.1.2.6. Nükleer Düzenleme Kurumu

Ülkemizde böyle bir kurum bulunmamaktadır. Ancak basında çıkan iddialar sonrasında TAEK'in sitesinde de bu doğrultuda bilgi bulunması bu bilgilerin içeriği ile ilgili değerlendirmeler yapılmasına neden olmuştur. İlk olarak 2010 yılında

TAEK'in web sitesine yerleştirilmiş bilgilendirme sayfasında Nükleer Düzenleme Kurumu'nun oluşturulması için kanun çalışmasının devam ettiği belirtilmiştir (TAEK, 2010a).

Sonrasında 2014 yılında bir gazetenin detaylandırdığı haberde nükleer düzenleme kurumu isimli bir kurumun kurulması için ETKB bünyesinde yasa taslağı hazırlandığı, bu yasa gereği TAEK'in yetkilerini Nükleer Düzenleme Kurumuna (NDK) devredeceği, NDK'nın Başbakanlığa bağlı hareket edeceği, NDK'nın üyelerinin Başbakan tarafından seçilen adaylar arasından Meclis tarafından belirleneceği, NDK'nın denetimden muaf olacağı, devletin üzerinde mali kontrol yetkisi bulunmayacağı hususları belirtilmiştir (sendika62, 2014)

3.1.1.2.7. Siber Güvenlik Tatbikatları

Farklı kurumların organizesinde ülkemizde Siber Güvenlik Tatbikatı, Siber Kalkan Tatbikatı gibi isimlendirilmiş tatbikatlar düzenlenmiştir. Bu tatbikatların bilgi ve iletişim teknolojilerinin hızlı ve etkin kullanımı, yaygınlaşması, güvenliğinin sağlanması gibi hedefleri bulunmaktadır. Tüm dünyada siber tehditlerin hızlı tespiti, önlenmesi, etkisinin azaltılmasına yönelik çalışmaların ülkemizde yapılması ihtiyacı ayrıca siber güvenlik konusunda politika ve strateji belirlenmesi, alan mevzuatının hazırlanması, kurumsal yapıların oluşturulması ve standartların belirlenmesi gibi ihtiyaçların doğru karşılanabilmesi sürecinde bu tatbikatların etkili çıktılar oluşturduğu söylenebilir (BTK, 2015; TÜBİTAK, 2014).

Tatbikatlarla katılımcıların siber saldırılara karşı koyma yeteneklerini görmesi ve geliştirmesi, saldırı anında kurum için ve kurumlararası koordinasyonun geliştirilmesi, farkındalığı artması gibi sonuçlarda ortaya çıkmaktadır. Amerika'da 2006 yılından beri iki yılda bir kere, Avrupa'da ise 2010 yılından beri ikiyıldabir kere benzer tatbikatlar yapılmaktadır. Çizelge 6-1'de de belirtildiği üzere ülkemizde ise 2008 yılından itibaren ortalama yılda 2 defa siber tatbikatlar gerçekleştirilmiştir (BTK, 2015; Çifci, 2013; TÜBİTAK, 2014).

Çizelge 3-1 Günümüze Kadar Yapılan Tatbikatların, Katılım Oranının Ve Koordinasyon Kurumları (BTK, 2015; TÜBİTAK, 2014).

Sıra No	Tatbikatın Adı	Tarih	Katılımcı Durumu	Düzenleyen Kurum
1	BOME 2008 Bilgi Sistem Güvenliği Tatbikatı	2008	8 kamu kurum ve kuruluşu	TÜBİTAK
2	Ulusal Siber Güvenlik Tatbikatı	2011	41 kamu, özel sektör ve sivil toplum kuruluşu	TÜBİTAK ve BTK işbirliğiyle
3	Ulusal Siber Güvenlik Tatbikatı	2013	61 kamu, özel sektöre ve sivil toplum kuruluşunun katılımıyla	UDHB koordinesinde TÜBİTAK ve BTK işbirliğiyle
4	Uluslararası Siber Kalkan Tatbikatı	2014	Çeşitli ülkelerin Ulusal SOME'lerinin katılımıyla	Uluslararası Telekomünikasyon Birliği (ITU) BTK ve işbirliğiyle

3.1.2. Fransa

3.1.2.1. Fransa'daki Nükleer Tesisler

Dünyanın 2 numarası olarak da kabul edilmektedir. ABD'den sonra en büyük elektrik üreticisidir. Fransa'da nükleer enerji ve santrallerle ilgili faaliyetler kamu ve özel kuruluşların kesişen çalışmalarıyla yürütülmektedir. Kamu tarafında ASN, ANDRA, IRSN, CEA olarak kısaltılmış kuruluşlar özel sektör tarafında Areva ve EDF bulunmaktadır (French Washington Embassy, 2013).

3.1.2.2. Nükleer Siber Güvenlikle İlgili Kurumlar, Yapıları, Görev Alanlar

3.1.2.2.1. Nükleer Güvenlik Kurumu (ASN Autorite De Sûreté Nucléaire)

Nükleer Güvenlik Kurumu (ASN – Autorite De Sûreté Nucléaire): Nükleer güvenlik ve radyasyondan korunma alanlarında bağımsız yetkili kuruluştur. Nükleer aktivitelerden toplumun, çevrenin, nükleer teknolojiler kullanılarak tedavi altındaki hastaların ve nükleer tesis çalışanlarının korunması süreçleriyle ilgili düzenleme faaliyetlerinden sorumlu bu kuruluş 2006 yılında kurulmuştur (Aciers, 2010; ASN, 2017; French Government, 2006).

3.1.2.2.2. Fransa Ulusal Siber Emniyet Ajansı (ANSSI Agence nationale de la sécurité des systèmes d'information)

Fransa Ulusal Siber Emniyet Ajansı (ANSSI Agence nationale de la sécurité des systèmes d'information) Başbakanlığa bağlı Ulusal Savunma ve Güvenlik Sekreterliğine (Secrétariat général de la défense et de la sécurité nationale) bağlı olarak 2009 yılında kurulmuş bir kurumdur. Kamuya ait bilgi sistemlerinin savunması görevinin yanında kritik ulusal altyapı operatörlerine ve devlete bilgi sistemlerinin güvenliği ile ilgili destek vermek, öneride bulunmak da görevleri arasındadır. Ulusal Mesleki Sertifikasyon Komisyonu (National Directory of Professional Certifcations) tarafından da onaylanmış bir eğitim merkezini (Safety Training Centre for Information Systems) bünyesinde barındırmaktadır. 500 çalışanı bulunmaktadır (ANSSI, 2017b; French National Assemble, 2013; leparisien, 2017; SFEN, 2016; Tromparent, 2012).

Kuruluş yasasında geçen görevleri:

- Cumhurbaşkanı ve hükümet tarafından istenen bakanlıklar arası güvenli bir iletişim ortamını tasarlamak ve uygulamak,
- Bilgi sistemlerinin güvenliği üzerine bakanlıklar arası çalışmalar koordine etmek
- Başbakana sunulan bilgi sistemlerinin korunması üzerine önlemleri inceler. Kabul edilenlerin adaptasyonunu gerçekleştirir.
- Ulusal servislerin bilgi sistemlerinde incelemeler/denetlemeler yapar.
- Kamu bilgi sistemlerinin güvenliğini sağlamak için bir olay tespit sistemi kurar ve işletir. Kamu bilgi sistemlerinin etkilendiği olaylarla ilgili bilgilerin toplanması ve değerlendirilmesi
- Devlet sırlarına ait bilgileri barındırmak için tasarlanmış sistemlerin (cihaz yada mekanizmaların) kontrolünü sağlamak ve onaylamak
- Uluslararası paydaşlarla bilgi paylaşımında bulunmak

- Bilgi sistemlerinin güvenliği alanında kalifiye personel yetiştirmek
- Bilgi sistemlerinin korunması için gerekli olan ve servis sağlayıcılar tarafından sunulan hizmet ya da donanımların güvenliği ile ilgili destek vermek.
- Halka açık elektronik iletişim ağlarının güvenliği ve entegrasyonu alanlarında ilgili bakanlığa destek vermek
- Hayati alanlarda (nükleer gibi) bulunan bilgi sistemlerinin güvenliği konusunda ilgili bakanlıklara destek vermek(French Government, 2009).

3.1.2.2.3. Atom Enerjisi ve Alternatif Enerjiler Komisyonu (CEA Commissariat à l'énergie atomique et aux énergies alternatives)

Atom Enerjisi ve Alternatif Enerjiler Komisyonu (CEA - Commissariat à l'énergie atomique et aux énergies alternatives): 1945 yılında kurulmuştur Atom Enerjisi Komisyonu adıyla kurulmuştur. 2010 yılında şimdiki adını almıştır. Reaktör teknolojileri araştırma, geliştirme ve kazandırma faaliyetlerini yürütür. Hidrojen, yakıt hücreleri, bio-kütle, enerji depolama alanlarında araştırmalar yapar. İletişim ve nükleer tıp alanlarında mikro ve nano teknolojileri araştırır. Nükleer savaş başlıkları ile ilgili çalışmalar yürütür. Enerji Bakanlığımız seviyesindedir. 9 araştırma merkezi, farklı disiplinlerden 16.000 çalışan, 51 ortak araştırma merkezi, üniversite ve okullarla 55 çerçeve anlaşma, 742 öncelikli patent, 63 farklı mükemmeliyet merkezi, 422 devam eden projenin sahibidir. Hükümetin ve Savunma Bakanlığının siber emniyeti sağlamanın yanında nükleer, radyolojik, biyolojik, kimyasal ve patlayıcılarla mücadeleyi içeren Global Emniyet Programının yürütücüsüdür (CEA, 2016, 2017a, 2017b).

3.1.2.3. Diğer Kurumlar

Radyoaktif Korunma ve Nükleer Güvenlik Enstitüsü (**IRSN** - Institut de Radioprotection et de Sûreté Nucléaire); Çevre, Sağlık, Endüstri, Araştırma ve Savunma Bakanlığı'nın bir kuruluşudur. Güvenlik araştırmaları ve nükleer ve radyolojik halk sağlığı konularıyla ilgilenmektedir (IRSN, 2017).

Ulusal Radyoaktif Atık Yönetim Ajansı (**ADNRA** – Agence Nationale Pour la Gestion des Déchets Radioactifs): 1991 yılında kurulmuştur. Atık prosedürleriyle ilgili endüstriyel ve ticari bir organizasyondur. İlgili bakanlıkların gözetim ve denetimi altındadır (Dupuis, 2010).

Areva: Reaktör üretimi, yaktı döngüsünün sağlanması ve hizmet sağlayıcılığı alanlarında faaliyet yürütür. %54,4'ü CEA'nın, %28,9'i Fransız devletinin, %3,3 BPIFrance(bir Fransız bankası) ve %4,8'i bir Kuveyt yatırım kuruluşunundur. Sinop'ta yapılacak nükleer santraldeki ATMEA1 reaktör tipi Mitsubishi ile Areva'nın ortak girişimleriyle üretilmiştir. 100'den fazla reaktör inşa etmiş olan şirket; nükleer tesislerle ilgili pompa ve motor ünitesi bakımı değişimi, diğer ekipmanların yedek parça ve tamiri, teknik merkezler, bölgesel geliştirme merkezleri, mühendislik servisleri, söküm merkezleri gibi farklı birimlerle 43'ü üretim tesisi şeklinde olmak üzere toplam 100 ülkede 14.745 çalışanla varlık göstermektedir. Yaşadığı mali ve teknik sorunlar nedeniyle üstlendiği işlerin büyük bölümünü 2017 yılında EDF'ye devredeceğine dair bilgiler bulunmaktadır (AREVA, 2017; CEA, 2016, 2017a; French Energy Ministry, 2016).

EDF (Électricité de France): Reaktör işletmecisi olarak faaliyet yürütür. Fransa'da bulunan 20 ayrı santraldeki 58 reaktörün işletmecisidir. %84'ü Fransız devletinindir. Nükleer enerji dışında, güneş, rüzgar, kömür, gaz, bio-kütle ve su temelli üretim tesisleriyle Avrupa, Amerika, Asya ve Afrika kıtalarında 584 TWh'tan daha fazla enerji üretim kapasitesini yönetmektedir. Avrupa'nın en büyük elektrik üreticisidir. 2015 yılı sonu itibariyle çalışan sayısı 154.845 dir. Türkiye'de kurulu bulunan rüzgar çiftliklerinin bir bölümünde hissedardır (CEA, 2017b; EDF, 2014; Le Point, 2010; TAEK, 2010c).

3.1.3. ABD

3.1.3.1. Amerika Birleşik Devletlerindeki Nükleer Tesisler

Amerika birleşik devletlerinde 99 adet nükleer reaktör çalışmakta, 4 nükleer reaktör inşa aşamasında, 34 nükleer reaktör ise kalıcı olarak kapatılmış durumdadır. Aktif reaktör sayısı olarak dünya lideri olan Amerika'yı aktif 58 reaktörle Fransa takip etmektedir (UAEA, 2016b, 2017b).

Bugün enerji üretim kapasitesi 518 Mw ile 1419 Mw arasında olan bu 99 aktif reaktörden 2016 yılında 805.327 Gw/h enerji üretilmiştir. Bu miktar Amerika Birleşik Devletlerinin 4.078.670 Gw/h olan yıllık enerji üretiminin %19'luk kısmına denk gelmektedir (ETKB, 2017a; UAEA, 2017b).

3.1.3.2. Nükleer Siber Güvenlikle İlgili Kurumlar, Yapıları, Görev Alanları

3.1.3.2.1. Nükleer Düzenleme Komisyonu (NRC Nuclear Regulatory Commission) -

Nükleer Düzenleme Komisyonu Amerika Birleşik Devletleri sınırlarında nükleer enerjiyle ilgili halk sağlığını ve emniyetini ilgilendiren tüm konularla ilgili düzenleme yapmakla görevli bağımsız bir kuruluştur. Yıllık bütçesi 1 milyar dolar olan ve Amerika'daki 5 farklı bölgede 4.000 çalışanı bulunan bir organizasyondur. NRC bütçesinin çoğunu lisans başvurusunda bulunan ve lisans sahibi işletmelerden elde etmektedir (NRC, 2017e).

Amerika'da nükleer enerjinin üretimi ve kullanımı konusunda ilk düzenleme 1954 yılında Atom Enerjisi Kanunu (Atomic Energy Act) olup bu kanun 1974 yılında yapılan güncelleme ile Enerjinin Yeniden Organizasyonu Kanunu (Energy Reorganization Act) adıyla genişletilerek yürürlüğe girmiştir. 1974 yılında yapılan bu genişlemeyle Atom Enerjisi Komisyonu (Atomic Energy Commission - AEC) isimli kurum kapatılarak Nükleer Düzenleme Komisyonu (Nuclear Regulatory Commission – NRC) isimli bağımsız bir kuruluş kurulmuştur (American Congress, 1974).

NRC reaktör güvenliği ve emniyet konusunda denetleme yapma, reaktörlerin lisanslanması ve lisans uzatımı süreçlerini yönetme, radyoaktif maddelerin lisanslanması, radyonükleid güvenliği, kullanılmış yakıtın depolanması-güvenliği-yeniden kullanılması ve imha edilmesi, süreçleri ile ilgili tüm düzenleme ve denetleme faaliyetlerini yönetir (NEI, 2017a; NRC, 2017e). Bu kurumun misyonu ülkenin radyoaktif maddelerin; toplum sağlığı ve güvenliğinin korunmasına, yaygın bir

savunma ve emniyet anlayışı oluşturulmasına ve çevrenin korunmasına dikkat ederek sivil amaçlarla kullanımı için lisans vermek ve düzenleme yapmaktır. AEC'den sonra NRC de radyasyon güvenliğinden geniş marjlı korunmayı sağlama amaçlı standartlar yayınlamaktadır. Bu standartlar lisans sahibi katılımcıların deneyimlerinden ve bilimsel araştırmaların somutlaştırılmasıyla elde edilmiştir. Siber emniyetle ilgili olarak ABD'de NGS işleten her işletmecinin 2009 yılı itibariyle NRC tarafından onaylanmış bir siber emniyet programına sahip olması gerekmektedir (NEI, 2016; NRC, 2017b, 2017a).

Ayrıca yine NRC tarafından hastaların NRC'nin yetkisi altındaki prosedürlerden uygun radyasyon dozu almalarını sağlayacak radyasyon tıbbı alanında düzenlemeler yapmaktadır. NRC'nin Komisyon olarak kabul edilen en üst yönetim heyeti 1 başkan ve 4 üyeden oluşmaktadır. Amerika Başkanının önerisi ve Senatonun onaylaması sonrasında her bir Komisyon üyesi 5 yıllığına seçilir (NRC, 2017b, 2017c).

Komisyonun altında bulunan idari yapı aşağıdaki gibidir.

- Komisyon
    - Komite ve Kurullar
        - Reaktör Güvenlik Önlemleri Danışma Komitesi
        - İzotopların Tıbbi Kullanımı Danışma Komitesi
        - Atom Güvenliği ve Lisanslama Jürisi Komitesi
    - **İcra Birimleri**
        - **Nükleer Emniyet ve Olaylara Müdahale Dairesi**
        - Nükleer Madde Emniyeti ve Korunma Dairesi
        - Nükleer Soruşturma Dairesi
        - Yeni Reaktörler Dairesi
        - Reaktör Düzenleme Dairesi

- Destek Birimleri
    - Bütçe Dairesi
    - Uluslararası Programlar Dairesi
    - Halkla İlişkiler Dairesi
    - Kongreyle İlişkiler Dairesi
    -
- Teftiş Birimi

3.1.3.2.1.1. Nükleer Emniyet ve Olaylara Müdahale Dairesi

Nükleer emniyet ve olaylara müdahale konusunda Ajansın (NRC) genel politikasını geliştirir, konuların değerlendirilmesi için yönetime yönlendirme sağlar, korunma ve emniyetle ilgili paydaş kurumlarla iletişimin sağlanması görevlerini üstlenmiştir. Ayrıca mevcut nükleer reaktörler ile muhtemel yeni nükleer reaktörler için acil durum hazırlık politikaları, düzenleme programları ve klavuzları geliştirir. Acil durum hazırlık konularına ve senaryolarına ilişkin teknik uzmanlık sağlar, olaylara müdahale konusunda NRC'nin acil durum hazırlığı ve olay müdahalesi konusunda programını yönlendirir ve yönetir, kurumun DHS, Federal Acil Durum Yönetim Ajansı **(FEMA)** ve diğer federal ajanslarla iletişimini sağlar (NRC, 2017f).

Bu birim 3 şubeden oluşmaktadır:

1. Fiziksel ve Siber Emniyet Politikası Şubesi
2. Emniyet Operasyonları Şubesi
3. Hazırlık ve Müdahale Şubesi

3.1.3.2.1.2. Fiziksel ve Siber Emniyet Politikası Şubesi

NRC tarafından lisans verilmiş tesislerde siber emniyet, korunma ve fiziksel emniyet alanları için düzenleme politikaları ve lisanslamanın incelenmesi konularında politikalar ve programlar geliştirir. Emniyet Operasyonları Şubesiyle koordinasyonu sağlayarak politika, gözetim ve teknik destek konularının tüm yönleriyle teknik süreçlere entegre olmasını sağlar. Bu entegrasyonda asıl amaç siber ve radyolojik sabotaja ve hırsızlığa karşı hassas maddelerin korunmasını sağlamaktır. Bünyesinde bulunan **Siber Emniyet Bürosu** ile NRC tarafından lisanslanmış tesislerdeki siber emniyetle ilgili ajans çapındaki aktiviteleri planlar, koordine eder ve yönetir. Bu büro ayrıca enerji reaktörlerinin siber emniyet ihtiyaçları ile ilgili yasalaştırma, lisanslama ve politika konularını adresleme, klavuz sağlama ve gözlemleme faaliyetlerinden sorumludur. Lisanslının siber emniyet planları ve düzenlemelere bağlılığına dönük teknik denetimi yönetir ve lisanslama uygulamalarının incelenmesindeki standartları ve tutarlılığı sağlamak için denetim planlarını geliştirir. Diğer federal ajanslarla (diğer bağımsız düzenleyici ajanslar ve kamusal olmayan oluşumlarla) siber olayları soruşturması, en iyi uygulamaları paylaşması, sorumluluğu azaltması ve potansiyel konuları adreslemesi konularında yakın çalışır (FBI, 2017a).

3.1.3.2.1.3. Emniyet Operasyonları Şubesi

Nükleer tesisler ve materyallerin güvenliği ve emniyeti için programların uygulanmasını yönetir. Tehdit ortamını istihbarat ve kolluk birimleri arasındaki bağı içerecek şekilde gözlemler ve değerlendirir. Lisanslı tesisler ve emniyet biriminin müdahale etkinliğini değerlendiren aktiviteler için performans değerlendirme programlarını uygular. NRC ihtiyaçlarının ve NRC tarafından lisanslandırılmış

tesislerin ve emniyet ve güvenlik personeli ile ilgili aktivitelerinin uygulanmasını değerlendiren NRC gözetim programını geliştirir ve denetler. NRC tesislerindeki, NRC müteahhitlerindeki, NRC lisanslılarındaki ve sertifika sahibi kurumlardaki sınıflandırılmış ve hassas sınıflandırılmamış **bilginin** (güvenlik personeli bilgisi ve korunaklı kritik altyapı bilgisi) **korunmasını** sağlar. Lisanslı tesislerde ve korunacak lisanslı radyoaktif maddelerin bulunduğu yerlerdeki giriş yetkilendirmesi ve göreve uygunluğu içeren personel güvenliği ile ilgili programların uygulamasını denetler. Güvenlik personeli ve emniyet için zorunlu ve mazeret programlarının uygulanmasını denetler (NRC, 2017f).

Bünyesinde Emniyet Denetimi ve Destek, Emniyet Performansı Değerlendirme, İstihbarat ve Tehdit Değerlendirme, Bilgi Emniyeti gibi alt birimler bulunmaktadır. Bu birimlerden **Bilgi Emniyet Bürosu** ajansın Bilgi Emniyeti Programı'nı planlar, koordine eder ve yönetir; İstihbarat ve Tehdit Değerlendirme Bürosu ise hazırlanan Tasarıma Esas Tehdit (TET) dokümanının uygunluğunu kontrol eder ve Karşı İstihbarat ve Köstebek Tehdit programlarını yönetir (NRC, 2017f).

3.1.3.2.1.4. Hazırlık ve Müdahale Şubesi

Lisanslı tesisler ve lisans talebinde bulunulan tesisler için acil durum hazırlık politikalarını, düzenlemelerini, programlarını ve klavuzlarını geliştirir. Acil durum hazırlık konuları ve sunumlarına ilişkin teknik uzmanlık sağlar ve acil durum hazırlık uygulamalarının ve düzeltmelerinin (değişikliklerin) teknik ve düzenleyici teftişlerini yönetir. Acil durum konularıyla ilgili NRC organizasyonlarının iletişimini ve NRC ile diğer kurumların iletişimini koordine eder. Ajansın, lisanslı tesislerdeki ve maddelerdeki olaylara müdahale edebilmesi için politikaların ve programların uygulanmasını geliştirir ve yönlendirir. Bölgesel müdahale programlarının gözetimini

deneyimler. NRC Operasyon Merkezini yönetir. Federal seviyede, eyalet seviyesinde, yerel devlet kurumlarında ve lisanslı kurumlarla olay müdahale programlarını koordine eder (NRC, 2017f).

Bünyesinde Koordinasyon, Operasyon, Reaktör Lisanslama, Düzenleme Politikaları ve Denetim gibi birimler bulunmaktadır. Bu birimlerden Reaktör Lisanslama Bürosu tüm reaktör tiplerinin acil durum hazırlıklarıyla ilgili lisanslama faaliyetlerini yönetmekte ve Federal Acil Durum Yönetim Ajansıyla yakın çalışmalar yürütmektedir (NRC, 2017f).

3.1.3.2.2. Savunma Bakanlığı (DoD Department of Defence)

ABD Savunma Bakanlığı 2011 yılında siber ortamda faaliyetleri yürütmek ve harekât icra edebilmek için belirlediği beş stratejik girişim ile ilgili bilgi vermek maksadıyla ABD Savunma Bakanlığı Siber Ortamda Harekât Stratejisi (DoD Strategy for Operating in Cyberspace) belgesini yayımlamıştır. Yayımlandığı yıl itibariyle DoD'nin siber uzayı onlarca ülkede yer alan 15.000 adet ağ ve 7 milyon cihaz üzerinde askerî ve istihbarat faaliyetleri ile personel, malzeme hareketlerini ve komuta kontrol sistemleri için kullandığı belirtilmiştir (US-DoD, 2011).

Söz konusu stratejide belirtilen beş stratejik girişim şunlardır:

- Birinci Girişim: DoD'nin siber uzayın tüm imkanlarından faydalanabilecek şekilde organize edilmesi, eğitimi ve donanımı için tüm siber uzayın harekât alanı olarak değerlendirilmesi.

- İkinci Girişim: DoD ağ ve sistemlerinin korunması için yeni savunma işletim konseptlerinin uygulanması.
- Üçüncü Girişim: Devletin topyekûn siber güvenlik stratejisinin etkinleştirilmesi için, ABD'deki diğer bakanlıklar, kamu kurumları ve özel sektör ile ortak çalışmalar yapılması.
- Dördüncü Girişim: Topyekûn siber güvenliğin güçlendirilmesi için ABD'nin müttefikleri ve uluslararası ortakları ile güçlü ilişkiler kurması.
- Beşinci Girişim: Kalifiye siber işgücü ve hızla elde edilecek teknolojik yenilikler vasıtasıyla milli yeteneklerin geliştirilmesi.

3.1.3.2.2.1. Siber Komutanlığı (USCYBERCOM)

Savunma Bakanlığı altında 2010 yılında faaliyete başlamıştır. Ülkenin siber saldırılara karşı savunulması, ağların ve askeri sistemlerin siber korunmasının sağlanmasından sorumludur. Kritik altyapıların korunması sürecinde İç Güvenlik Bakanlığına (DHS) destek olur. 2017 yılı bütçesi 7 milyar dolardır (Çifci, 2013).

Bünyesinde tamamı siber saldırılarla ilgilenen 13 Ulusal Görev Takımı, 68 Siber Savunma Takımı, 26 Muharip Görev Takımı ve 25 Destek Takımı olmak üzere toplam 133 farklı ekibi bulunmaktadır. Bu yönüyle nükleer tesislere dönük bir siber saldırı yapıldığında ilk olarak USCYBERCOM tarafından savunmanın gerçekleştirileceği söylenebilir (DoD, 2017a).

3.1.3.2.2.2. Ulusal Güvenlik Ajansı (NSA National Security Agency)

Ülkenin iletişim ve bilgi sistemlerinin korunmasından sorumlu olan askeri istihbarat kuruluşudur. Bu sorumluluğu yerine getirirken ülke sınırları dışından da edindiği sinyal bilgilerini istihbari olarak işler ve kullanır. Sinyal istihbaratı (SIGINT) olarak bilinen bu işlem karşı istihbarat ya da istihbarat faaliyetleri kapsamında telsiz yayınları, internet ve telefon konuşmaları gibi her türlü dijital sinyalin (iletişim türünün) gözlenmesi, kayda alınması ve işlenmesi süreçlerini kapsar. Bu görevinin yanında ayrıca ülkenin iletişim ağları ve bilgi sistemlerinin korunmasıyla da görevlidir. NSA başkanı ayrıca USCYBERCOM'un da başkanıdır(DoD, 2015).

3.1.3.2.3. İç Güvenlik Bakanlığı (DHS Department of Homeland Security)

11 Eylül 2001 saldırılarından sonra 25 Kasım 2002 kurulmuştur. Ülkenin terör saldırılarından korunması ve güvenliğin sağlanması, sınırların güvenli bir şekilde yönetimi, göçmenlik yasalarının uygulanması ve yönetimi, siber uzayın korunması ve güvenliği, her türlü olumsuz olaya karşı hazırlıklı olma ve iyileştirme faaliyetlerinin güçlendirilmesi İç Güvenlik Bakanlığının ana görev alanlarıdır. Bu görevleri yerine getirirken hem fiziksel hem siber alanda devlet birimleri bünyesindeki sistemlerin ve ağların güvenliğini sağlar, kritik ağların güvenliklerini güçlendirir ve muhtemel saldırılara karşı ulusal hazırlığın geliştirilmesini sağlar. Önemli siber saldırıların yaşanması durumunda koordinasyon yetkisi bulunan bu bakanlık özel sektöre ihtiyaç duyulduğunda siber alanda destek verir. 2017 bütçesi 40 milyar dolardır (DHS, 2017a).

Bünyesinde Ulusal Siber Emniyet ve İletişim Entegresyon Merkezi (National Cybersecurity and Communication Integration Center, **NCCIC**) ve Federal Acil Durum Yönetim Ajansı'nı (Federal Emergency Management Agency – **FEMA**) barındıran bakanlık bu birimler üzerinden görev alanındaki ulusal ve uluslararası tüm paydaşlarla koordinasyonu sağlar. Muhtemel saldırı faktörlerini düzenli olarak değerlendirme, önleme, korunma, yanıtlama, zarar azaltma, iyileştirme erek önlemlerin güçlendirilmesi süreçlerini kontrol eder (DHS, 2017d, 2017b).

3.1.3.2.3.1. Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC National Cybersecurity and Communication Integration Center)

Ülkemizdeki USOM'un karşılığı olan US-CERT (Ulusal Siber Olaylara Acil Müdahale Ekibi – US National Computer Emergency Response Team) bu bakanlığa bağlı olarak faaliyet yürütür. Ayrıca NCCIC Operasyon ve Entegrasyon Birimi (NCCIC Operations & Integration), Endüstriyel Kontrol Sistemleri Siber Olaylarına Acil Müdahale Ekibi (ICS-CERT – Industrial Control Systems Cyber Emergency Response Team), Ulusal İletişim Koordinasyon Merkezi (National Coordinating Systems for Communication) gibi birimler de yine bu merkezin alt birimleridir. 2011 yılı bütçesi 98,8 milyar dolardır (US-CERT, 2017).

3.1.3.2.3.2. Federal Acil Durum Yönetim Ajansı (FEMA Federal Emergency Management Agency)

İç Güvenlik Bakanlığının ulusal düzeyde yaşanabilecek her türlü acil durumun önlenmesi, acil durumdan korunulması, zararın azaltılması, yanıtlanması ve önceki duruma dönülmesi süreçlerini yürüten ve yöneten ajansıdır. Ulusal Hazırlık konulu 8 nolu Başkanlık Politika Yönergesinde (Presidential Policy Directive 8 – National Preparedness) ile bu kuruma büyük felaketler, terörist saldırılar, salgınların yanında siber saldırılara karşı hazırlıklı olunması süreçleri ile ilgili önemli görevler verilmiştir (Brown, 2011) .

3.1.3.2.4. Adalet Bakanlığı

3.1.3.2.4.1. Federal Soruşturma Bürosu (FBI Federal Bureau of Investigation)

FBI, ABD Adalet Bakanlığı bünyesinde, federal suçların araştırılması ve ülke içinde istihbarata karşı koyulmasından sorumludur. Yaklaşık 35000 personele sahip olan FBI'ın 2016 yılı bütçesi 8,7 milyar dolardır. FBI, ülke sınırları içerisinde suçla veya istihbarata karşı koyma ile ilgili siber olayların araştırılması ve engellenmesinden sorumludur. Yasa uygulama ve istihbarata karşı koymaya ek olarak, ülke içi siber tehdit istihbaratının en üst düzeydeki yetkili kurumudur. FBI ayrıca siber güvenlik konularında DHS'e bilgi ve destek sağlamaktadır (FBI, 2017d).

Birçok kurumu bünyesinde barındıran Adalet Bakanlığı altında bulunan kurumlardan biri de Federal Soruşturma Bürosu (FBI – Federal Bureau of Investigation)dur. 1908 yılında The Bureau of Investigation adıyla kurulmuş olup

zaman içerisinde değişik isimler almıştır. 1935 yılında bugünkü ismini almıştır (Justice Department, 2017; Weiner, 2012).

Amerikan halkını ve kurumlarını koruma ve destekleme hedefiyle faaliyet yürüten bir kurumdur. Washington DCde bulunan ana merkezinin yanında 56 Bölge Ofisi, 380 yerel ofisi ve 64 uluslararası ofisi bulunan kurumun 35.000 çalışanı bulunmaktadır (FBI, 2017c, 2017e).

Kurum önceliklerini

- Ülkeyi terörist saldırılardan korumak,
- Ülkeyi yabancı istihbarat kuruluşları ve casusluk faaliyetlerine karşı korumak,
- Ülkeyi siber temelli saldırılara ve yüksek teknoloji suçlarına karşı korumak,
- Her seviyedeki yolsuzlukla mücadele etmek,
- İnsan haklarını korumak
- Ulusal ve sınır ötesi suç organizasyonları ve girişimleriyle mücadele etmek
- Büyük görev suçlarıyla mücadele etmek,
- Önemli şiddet suçlarıyla mücadele etmek

olarak tanımlamaktadır (FBI, 2017d)

Alt birimlerinden 2 tanesinin birçok görevinin yanında ayrıca nükleer alanda meydana gelecek olaylarla ilgili de görevleri bulunmaktadır;

3.1.3.2.4.2. Kritik Olaylara Müdahale Grubu (CIRG Critical Incident Response Group)

1994 yılında kurulmuş olan bu ekip, özel ajanların ve profesyonel destek personellerinden oluşmaktadır. Kriz yönetimi, rehine kurtarma, gözetleme, havacılık, tehlikeli cihazlardan korunma, kriz müzakereciliği, davranış analizi ve taktik operasyonlar gibi önemli alanlarda hizmet veren bu personeller zorlu koşulları içeren bir eğitim programından geçirilirler (FBI, 2017a).

Ulusal ve uluslararası kollukla koordine çalışan bu grup son teknoloji donanımlar, ileri seviye araştırmalar, taktik ve soruşturmacı teknikleri kullanarak suçları aydınlatmaya çalışmaktadır. Bomba Teknisyeni Özel Ajan Programı, Kitle İmha Silahları Programı gibi programları Patlayıcı Cihazlar Analiz Merkezi gibi özel merkezleri bulunan birim, nükleer dünyadan gelecek her türlü tehlikeyle Kitle İmha Silahları Programı içerisinde mücadele etmektedir (FBI, 2017a).

3.1.3.2.4.3. Siber Suçlar Şubesi (Cyber Crime)

Siber dünyadaki suçlular, deniz aşırı düşmanlar ve teröristler tarafından yapılan siber saldırılar konusunda FBI federal seviyede öncü kurumdur. Günden güne büyüyen, tehlikeli ve sofistike hale gelen siber suç ve suçlular özellikle özel ve kamu ağlarına, kritik altyapılara, şirketlerin ticari sırlarına, üniversitelerin ileri seviye araştırma geliştirme faaliyetlerine ait bilgileri hedef almaktadırlar. Bu yapıların korunması amacıyla faaliyet gösteren siber suçlar şubesi alanında deneyimli birçok uzmanı barındırmaktadır. 11 Eylül saldırıları sonrasında soruşturma kapasitesini güçlendiren FBI, Siber Müdahale Takımı (CAT – Cyber Action Team) isimli dağıtık yapıda çalışan bir ekip kurmuştur. Bu ekip içerisindeki uzmanlarla 48 saat içinde

dünya genelinde ihtiyaç duyulan noktaya giderek soruşturma desteği ve kritik soruların cevap bulması konusunda yardımda bulunmaktadır (FBI, 2017b, 2017d).

3.1.3.2.5. Merkezi Haberalma Teşkilatı (CIA Central Intelligence Agency)

1947 yılında Ulusal Emniyet Yasası ile kurulan CIA, Amerika Birleşik Devletleri adına politika belirleyicilere ulusal emniyet konuları ile ilgili geniş çaplı istihbarat sağlamaktan sorumludur. Federal hükümetinin yabancı istihbarat servisi olarak hizmet verir. İstihbarat sağlama görevini dünya genelinde yürütmekle birlikte elde edilen istihbaratın işlenmesi ve analiz edilmesi görevlerini de yerine getirir. Birincil bilgi kaynağı herhangi bir teknik donanım içermeyen salt insan iletişimleri yoluyla elde edilebilen insan istihbaratıdır. İlk olarak Başkana ve Kabineye istihbarat sağlamaya odaklanmış olan kurumun günümüz itibariyle 21.000in üzerinde çalışanı olduğu tahmin edilmektedir. Ülke içi emniyet hizmeti görevi bulunan FBI'ın aksine CIA deniz aşırı yerlerden bilgi toplamaya odaklanmıştır (CIA, 2017; WashingtonPost, 2013).

Açık kaynaklardan 5 farklı daire başkanlığı tarafından hizmetlerin yürütüldüğü belirtilmektedir.

1. Analiz Dairesi Başkanlığı
2. Operasyon Dairesi Başkanlığı
3. Bilim ve Teknoloji Dairesi Başkanlığı
4. Destek Dairesi Başkanlığı
5. Dijital İnovasyon Dairesi Başkanlığı

3.1.3.2.5.1. Dijital İnovasyon Dairesi Başkanlığı

Ajansın en yeni dairesidir (1 Ekim 2015). Ajans aktivitelerinin en yeni dijital ve siber tekniklerle ve Bilgi Teknolojileri (BT) altyapısıyla donatılabilmesini sağlamaya odaklanmıştır. Zorlukların ve fırsatların eşit yeraldığı da değerlendirilebilecek olan hızlı değişen dünyamızda bu çağın ihtiyaçlarına uygun bir yaratıcılık, titizlik ve tamamlayıcılık konularında güçlü bir yapıya kavuşmayı hedeflemektedir. Geleneksel silahlar kadar dijital silah ve tekniklerin de kazandırılması başka bir hedefleri olarak belirtilmektedir (CIA, 2015).

4. TARTIŞMA

Kömür rezervlerimizin büyük bölümünün düşük kaliteli linyit kömüründen oluşması, rüzgar ve güneş enerji üretimi açısından uygun potansiyelimize rağmen bu enerji türlerinin yüksek maliyet ve mevcut şebeke koşullarının uygunsuzluğu gibi dinamikler ülkemizde enerji türleri açısından nükleer enerji üretimi ihtimalinin öne çıktığını göstermektedir. Nükleer enerjinin risklerinin yanında düşük fiyata elektrik sağlaması, sera gazı emisyonlarını düşürmesi, deneyim ve uzmanlık bilgisi sağlayacak olması ihtimalleri de nükleer enerjiden elektrik üretimini teşvik edici diğer konular olarak değerlendirilebilir. Ülkemizde yakın zamanda 2 farklı Nükleer Güç Santrali'nin (NGS) kurulması yasal zemine oturmuştur (Han et al., 2015).

Yap Sahip Ol İşlet modeli sadece Rusya için değil dünya için yeni bir model olmakla birlikte bu modelin başarılı olması durumunda Rusya'nın başka ülkelere aynı modelle kurulum yapmayı planladığına dair açık kaynaklarda bilgiler bulunmaktadır. Bu sebeple proje Rusya için önemli bir reklam anlamına gelmektedir. Ülkemiz adına bu projenin hazine garantisi gerektirmemesi Rusya'nın vazgeçmesi durumunun Rusya adına boşa yapılmış masraf olacağı ayrıca önemli bir diğer detaydır. Akkuyu NGS işletmeye alındıktan sonra ortaya çıkan hatalar sonucunda yaşanabilecek hizmetten çıkarma, zararın tazmini gibi durumlar da yine Rus tarafına finans, ün gibi anlamlarda kayıp olarak yazılacaktır. Bu nedenler Rusya'nın tüm riskleri çok iyi değerlendirerek konuya yaklaşmasını gerektirecektir (Reuters, 2013b; Sokolov, 2013).

İran'ın Natanz Uranyum Zenginleştirme Tesisini hedef alan **Stuxnet** isimli siber saldırının arkasında Amerika Birleşik Devletleri (ABD) ve İsrail'in bulunduğuna dair belirgin işaretler, Akkuyu NGS'nin Rusya tarafından inşa edilecek ve işletilecek olması, Suriye politikası konusunda ABD ve Rusya'nın farklı kutuplarda yer alıyor görünmeleri yakın dönem riskleri açısından ülkemizde dikkate alınması gereken hususlardır.

Uluslararası Atom Enerjisi Ajansı'nın (UAEA) referans klavuzuna göre bir nükleer tesise yapılan siber saldırı; bilgilere/verilere izinsiz erişim, bilginin/verinin değiştirilmesi, bilginin/verinin kullanılabilirliğinin engellenmesi, bilgi sistemlerine izinsiz giriş gibi riskleri barındırmaktadır. Bu risklerin üzerine siber emniyetle ilgili olarak tasarım esnasında dikkate alınan önlemlerin yanında siber kabiliyetlerin her geçen gün değişmesi tesiste –tesis çalışmaya başlamadan önce dahi- sürekli değerlendirilmesi gereken bir **siber emniyet rejimi** oluşturulmasını gerektirmektedir.

Dünya genelinde nükleer tesislerin de **kritik altyapı** olarak değerlendirilmesi tüm kritik altyapılarla ilgili dünyadaki durumun ve ülkelerin bakış açısının dikkatlice irdelenmesini gerektirmiştir. Ülkemizde kritik altyapılarla ilgili 2014 yılında Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) tarafından yapılan çalışmada 10 farklı sektör Kritik Altyapı Sektörü olarak belirlenmişken 2016 yılında Siber Güvenlik Kurulu tarafından yapılan çalışmada 6 farklı sektör Kritik Altyapı Sektörü olarak belirlenmiş olması ülkemiz adına giderilmesi gereken bir çelişkidir. 4 sektör (Tarım ve Gıda, Kültür ve Turizm, Kritik Üretim/Ticari Servisler, Sağlık) AFAD tarafından Kritik Altyapı Sektörü olarak değerlendirilmişken Siber Güvenlik Kurulu tarafından değerlendirilmemiştir. Bu alanda yasal olarak belirleyici olan kurumun netleştirilmesi büyük önem arzetmektedir. Kanunla afet tanımı içerisine giren her türlü durumla önleme/mücadele etme/ zarar azaltma görevleri AFAD'a verilmiş, Bakanlar Kurulu kararıyla ise siber güvenlik konusunda koordinasyon görevi Siber Güvenlik Kurulu'na

verilmiştir. Kritik altyapıları ya da kritik altyapı sektörlerini belirleme görevine ilişkin herhangi bir mevzuat bulunmamaktadır. Sektör işletmecilerinin bu durumda hangi kurumun kararına uyacağı konusu ayrıca belirsizliğini korumaktadır. Yasal sorumlunun netleşmesi sonrasında ABD ve Fransa'nın ayrıca Kritik Altyapı Sektörü içerisinde değerlendirdiği diğer sektörlerle ilgili bir çalışma yapılması önemlidir.

Kritik Altyapı Sektörleriyle ilgili ABD'de 2003 yılından beri kurulma zorunluluğu getirilmiş olan ISAC (Bilgi Paylaşımı ve Analiz Merkezi – Information Sharing and Analyze Center) isimli merkezler yapı olarak ülkemizde kurulma zorunluluğu getirilmiş olan Siber Olaylara Müdahale Ekibi (SOME) yapısına benzemektedir. Bu durum ülkemizin benzer bir modelle idari yapısını kurguladığını göstermektedir.

Nükleer güç santralleriyle ilgili olarak; ülkemizde Enerji ve Tabi Kaynaklar Bakanlığı Nükleer Proje Uygulama Dairesi'ne "*mevzuat alanında gerekli çalışmaları yapmak veya yaptırmak*" yetkisi verilmişken Türkiye Atom Enerjisi Kurumu'na (TAEK) da "*her türlü amaç için gerekli teknik mevzuat, tüzük ve yönetmelikleri hazırlamak*" görevi verilmiştir. ABD'de ise yasal düzenleme lisanslama ve denetleme yetkilerinin tamamı Nükleer Düzenleme Komisyonu'na (NRC) verilmiş olup ABD Enerji Bakanlığının ilgili birimlerine sadece nükleer silahlarla ilgili görevler verilmiştir. Fransa'da ise tüm düzenleme, lisanslama ve denetleme yetkileri Nükleer Güvenlik Kurumu'nda (ASN) toplanmış siber anlamda ihtiyaç duyulması durumunda Ulusal Siber Emniyet Ajansı'ndan (ANSII) destek alınmaktadır.

Ülkemizde siber alanda yasal anlamda **ilk düzenleyici faaliyet** ABD'den 16 yıl sonra, Fransa'dan 8 yıl sonra yapılmıştır. Geç gelen bu düzenleyici faaliyetlerin ABD

ve Fransa ile benzer olarak yürütüldüğü görülmektedir. Dünya geneline yayılmış olan CERT (Cyber Emergency Response Team)/ISAC yapılarının yaygınlaştırılması ülkemizde aynı işleve sahip SOME'lerin (Siber Olaylara Müdahale Ekibi) kurulumu ve yaygınlaştırılması süreçleriyle benzeşmektedir. 2013 yılında SOME'lerin kuruluşları ile ilgili düzenleyici olması açısından yayımlanan tebliğle sektörlerin bir koordinasyon noktası olması planlanmıştır. 2016 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgesiyle enerji sektörünün tamamından Enerji Piyasası Düzenleme Kurumu (EPDK) sorumlu olarak gösterilmiştir.

Nükleer güç santrallerinin kuruluşu sürecinde işletmeciye sadece elektrik enerjisi satışı ile ilgili **lisans** veren EPDK'nın bağımsız bir kuruluş olan TAEK üzerinde herhangi bir yaptırım gücü bulunmamaktadır. Ancak TAEK'in SOME kurması durumunda enerji sektöründe bulunması nedeniyle EPDK'nın SOME'sine bağlı hareket etme gerekliliğinin çeşitli problemlere yol açacağı düşünülmektedir. Mesela ülkemizde ilk nükleer santrali işletecek olan Akkuyu NGS Elektrik Üretim A.Ş.'nin bir SOME kurması ve bu SOME'nin EPDK'nın SOME'sine bağlı olması gerekmektedir. Ana başlığı altında Siber Emniyeti de bulunduran Fiziksel Güvenlik ile ilgili denetmen kuruluşu TAEK iken ayrıca SOME'sinin EPDK SOME'sine bağlı olması siber olaylar konusunda EPDK ile TAEK'in çelişkili bir uygulamaya gitmesi durumu bir karmaşa yaratabilecektir. Ya da Akkuyu NGS'de yapılmasına ihtiyaç duyulan bir siber sızma testinin TAEK ve EPDK tarafından farklı/çelişen şekillerde ya da çerçevede, farklı yüklenicilerce yapılmasının istenmesi durumunda işletmecinin kimin kararına göre hareket edeceği de başka bir çelişki örneği olarak belirmektedir.

Nükleer alanın risklerini anlama konusunda **Çernobil ve Goiania olayları** önemli örneklerdir. Goiania'daki olayda yaklaşık 90 gr radyoaktif madde barındıran bir teleterapi cihazının kapsülünün açılması sonrasında meydana gelen olayda 4 kişi ölmüş ve 245 kişi radyasyona maruz kalmış olması, ortaya çıkan radyasyona belirlenen

eşik değerlerin üzerinde maruz kalmış her türlü maddenin 275 kamyon yüküne eşdeğer olması çok önemli detaylardır. Bu ve buna benzer detayların farkındalık arttırıcı faaliyetlerde kullanılması gerekmekte ve ayrıca tüm bu risklerle doğru mücadele edebilmek ancak iyi bir **nükleer emniyet kültürünün** edinilmesi ile sağlanabilecektir.

Ülkemizde kritik altyapılarla ilgili tanımların yapılmış olması, hangi sektörlerin kritik altyapı sektörleri içerisinde olduğunun belirlenmesi önemli adımlar olarak değerlendirilebilir. Ancak **kurumlar arasında sorumluluk** konusunda bir karmaşa ve nükleer bir tesisin SOME'sinin bağlı bulunacağı kurum olarak EPDK'nın belirlenmiş olması bir eksiklik olarak göze çarpmaktadır. EPDK'nın enerji üretimi ile ilgili lisanslama ve denetleme yetkisi dışında nükleer bir tesisin neredeyse tüm denetim görevleri TAEK koordinasyonunda yürütülecektir.

Amerika Birleşik Devletleri'nde siber emniyetin ulusal anlamda sağlanması konusunda farklı kurumların farklı görev alanı tanımları doğrultusunda sorumluluğu bulunduğu değerlendirilebilir. Ancak bunların yanında nükleer alanda tüm sorumluluk Nükleer Düzenleme Komisyonuna (NRC-Nuclear Regulatory Commission) verilmiştir. Dolayısıyla nükleer siber alanda yapılacak denetlemeler, lisanslama prosedürleri, korunma programlarının hazırlanması gibi faaliyetlerde sorumluluk NRC'de olsa da bu faaliyetlerin veriminin artabilmesi için siber alanda da görevleri bulunan; Federal Soruşturma Bürosu (FBI-Federal Bureau of Intelligation), Merkezi Haberalma Teşkilatı (CIA-Central Intelligence Agency), Ulusal Güvenlik Teşkilatı (NSA-National Security Agency), İç Güvenlik Bakanlığı (DHS-Department of Homeland Security) gibi önemli devlet kurumlarıyla işbirliği faaliyetleri yürütülmektedir.

ABD'de düzenleme ve denetleme yetkileri NRC'ye bırakılmış olup araştırma ve geliştirme faaliyetleri ulusal laboratuvarlarda gerçekleştirilmektedir. Ülkemizdeki siber korunma düzenlemeleriyle ilgili önemli bir adım olarak değerlendirilebilecek olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Ekibi (SOME) yapılarının getirilmiş olması sonrasında Nükleer Santralleri denetleme, lisanslama gibi yetkileri yasal olarak elinde bulunduran TAEK'in SOME'sini kurmamış olması siber alanda yapacağı çalışmaları diğer devlet kurumlarından destek alarak yürüteceği şeklinde değerlendirilmektedir. Destek alınabilecek TÜBİTAK, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı veya Türk Silahlı Kuvvetleri gibi kurumların alana (nükleer siber emniyet) yabancı olmaları, destek sürecinde çalışanlarının mevcut iş yüklerinin yanında ikinci bir görev gibi algılayarak yaklaşma ihtimalleri, TAEK'in doğru değerlendirme veya doğru düzenleme gibi alanlarda elini zayıflatacaktır. TAEK'in siber emniyet alanında deneyimli uzmanlardan oluşan bir birim oluşturması (**Siber Güvenlik Dairesi, Şubesi, Bürosu** vb) ve sonrasında da SOME'sini kurması önemli bir adım ilk adım olarak değerlendirilebilir.

Bir nükleer tesise yapılacak siber saldırıya müdahale ya da bu saldırının engellenmesi gibi süreçleri yetkin personeli çalıştırıyor olmaktan, doğru kuruma doğru yetkiyi vermiş olmaya kadar geniş bir yelpazede kurumların **sorumluluk paylaşımı**nın değerlendirilmesi ve ülkemiz dinamiklerinin de göz önünde bulundurulduğu ideal yapının oluşturulması için önemli bir gerekliliktir. Yapılan saldırı ile radyasyonun olumsuz etkilerinin de gerçekleşmiş olması durumunda iyileştirme aşamalarında görev alacak ekipteki personel çeşitliliğinin önemli ölçüde artması, farklı alanlardaki personellerin yapacağı çalışmaların doğru koordinasyonu ve önemli bir koordinasyon planlaması gerekecektir.

Proje şirketlerinin zenginliğinden kaynaklı denetleme ekiplerine ülkemiz koşulları doğrultusunda nüfus edebilme ihtimali dikkatlice ele alınması gereken bir

risk olarak değerlendirilmelidir. Güvenlik ya da emniyet'e ayrılacak kaynakların belirlenmesinde ekonomik durumun ön planda tutulması da diğer önemli bir risk olarak değerlendirilmektedir.

İhtiyaç duyulacak tüm yasal düzenlemelerde özel sektörün deneyimlerinden faydalanılması gerekmektedir. Özellikle nükleer siber alan için gerekecek olan bu kapsamlı çalışma için hem nükleer alanla ilgilenen hem siber alanla ilgilenen özel ve kamu temsilcilerinin bir araya gelerek çalışma yürütmelerinin faydalı olacağı değerlendirilmektedir.

Akkuyu projesinde bugüne kadar doğru ekiple aktif katılım sağlanması, ROSATOM'un sunduğu lisansa tabi dokümanların titiz incelemelere tabi tutulmasının ötesinde dokümanların sunuluş şekline kadar karar verebilecek paydaşların bir araya getirilmesi önemli bir şarttır.

Tüm bunların yanında dünya genelinde risklerinden ve organizasyon yapısından dolayı, nükleer güvenlik/emniyet alanlarında oluşturulmuş önlemler bütünü diğer enerji türlerine kıyasla daha derinlikli, özenlidir. Bu duruma örnek Enerji ve Tabii Kaynaklar Bakanlığı tarafından hazırlanan "Türkiye'nin Nükleer Santral Projeleri: Soru-Cevap" isimli belgede bulunan "*Nükleer güvenlik/emniyet kültürünün ülkemize kazandırılması ve maden işletmeleri dahil her alana uygulanabilmesine nükleer santral yatırımları vesile olabilir. Nükleer güvenlik kültürü seviyesindeki güvenlik önlemlerinin diğer alanlara da kazandırılmasıyla ülkemizde iş kazaları minimum seviyeye düşecektir."* ifadeleri maden işletmeleri alanında faaliyet gösteren işletmelerin tabi oldukları denetim çerçevesinin nükleer emniyetle ilgili çerçeveye kıyasla nasıl değerlendirildiğinin de bir göstergesidir.

Konuya; bir nükleer tesisin siber anlamda denetlenmesi için oluşturması gereken klavuz/şablon dokümanların hangi kurum tarafından hazırlanması gerektiği, kritik altyapıların hangi kurum tarafından belirlendiği ve bu tesislerin tamamının siber emniyet politikalarının geliştirilmesi ve uygulanması yönleriyle bakılan aşağıdaki çizelge incelendiğinde ülkemizdeki çok başlı yapı daha net anlaşılacaktır.

Çizelge 4-1 Nükleer Tesislerin ve Kritik Altyapıların Sorumluluk Kıyaslama Tablosu(ANSSI, 2017a; ASN, 2017; Bakanlar Kurulu, 2012; French Government, 2006, 2017, French National Assemble, 2013, 2013; French Washington Embassy, 2013; NRC, 2017c; SFEN, 2016; TBMM, 1982, 2009, 2013, UDHB, 2013, 2016; White House, 2013b)

Sıra No	Sorular	Sorumlu Kurum(lar)		
		ABD	Fransa	Türkiye
1	Nükleer Tesislerde Yapılacak Siber Denetimlerin Planlanması, Koordinasyonu Süreci	NRC	ASN	TAEK, EPDK SOME (USOM adına), AFAD
2	Nükleer Tesislerde Yapılacak Siber Denetimlerde Kullanılacak Dokümanların Hazırlanması	NRC	ANSSI	TAEK, EPDK SOME (USOM adına), AFAD
3	Nükleer Tesislerde Yapılacak Siber Denetimlerin Uygulanması	NRC	ASN	TAEK, EPDK SOME (USOM adına), AFAD
4	Nükleer Tesis İşletmecisi Tarafından Kurulması Gereken SOME'lerin (CERT/ISAC) denetimi	NRC	ASN	TAEK, EPDK SOME (USOM adına), AFAD
5	Hangi Altyapıların Kritik Altyapı Kapsamında Değerlendirileceğinin Belirlenmesi	DHS	ANSSI	UDHB, AFAD
6	Kritik Altyapıların Siber Güvenliğinin Sağlanması İçin Politika Geliştirme	DHS	ANSSI	UDHB, AFAD

NRC – Nuclear Regulatory Commission – ABD Nükleer Düzenleme Kurumu
DHS – Department of Homeland Security – ABD İç Güvenlik Bakanlığı
ASN – Autorite De Sûreté Nucléaire – Fransa Nükleer Güvenlik Kurumu
ANSSI – Agence nationale de la sécurité des systèmes d'information – Fransa Ulusal Siber Emniyet Ajansı
TAEK – Türkiye Atom Enerjisi Kurumu
EPDK – Enerji Piyasası Düzenleme Kurumu
SOME – Siber Olaylara Müdahale Ekibi
USOM – Ulusal Siber Olaylara Müdahale Merkezi
AFAD – Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı
UDHB – Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Çizelgede detayları belirtilmiş çok başlılığın yanında siber altyapısı bulunan her kurum zaman zaman altyapısı üzerinde sızma testleri yaptırmaktadır. Yapılan sızma testleri sonrasında kurumun altyapısındaki zafiyetler belirlenmekte ve kurum bu doğrultuda bilgilendirilmektedir. Kamu kaynaklarının/iş gücünün genelde tercih edilmediği ya da yeterli bulunmadığı bu testler sızma testi yapan özel siber güvenlik şirketleri tarafından uygulanmaktadır. Testi yapacak şirketle bir gizlilik anlaşması imzalanarak testin uygulanacağı altyapıya ilişkin en mahrem bilgi ve şifreler bu şirketlere teslim edilmektedir. Herhangi bir NGS için sızma testlerini yapma görevinin özel siber emniyet şirketlerine bırakılıp bırakılmayacağı, kamu kaynaklarıyla yapılacaksa kalifiye iş gücünün hangi kurum çatısı altında toplanacağı hususlarının ileride karar verilmesi gereken önemli konular olacağı değerlendirilmektedir.

5. SONUÇ VE ÖNERİLER

Günden güne büyük bir hızla yaygınlaşmaya devam eden siber dünyanın nimetleri kadar güvenlik problemleri de artmaktadır. Bankacılık işlemlerini yapamamak ya da uzun pasaport kuyruklarında beklemek zorunda kalmak siber alan güvenliğinin yaşamın vazgeçilmez bir parçası geldiğinin önemli göstergeleridir. Ayrıca siber alanın asimetrik yapısı çok önceden hazırlanmış saldırı araçlarının kullanımını geniş alanlara ve farklı zamanlara yaymaktadır. Bu alanla ilgili farkındalık seviyesi yüksek bireylere sürekli ihtiyaç duyulmaktadır.

Başka bir devlete hasmane ya da politik sebeplerle zarar verme hedefindeki gruplar ilk olarak barajlar, elektrik dağıtım şebekeleri, nükleer tesisler, askeri tesisler gibi kritik altyapıları hedeflemektedirler. 2023 yılına kadar çalışan en az bir nükleer reaktör bulundurmayı hedefleyen ülkemizde henüz çok yeni olan nükleer siber emniyetin sağlanabilmesi gün geçtikçe daha önemli bir hal almaktadır.

Yap Sahip Ol İşlet modeliyle yeni tanışacak olan ülkemizin aynı zamanda nükleer enerji üretimi ile de yeni tanışıyor olması bu tesisleri hedef alan siber saldırılara hazırlık süreci konusunda deneyimimizin olmaması önemli bir eksiklik olarak önümüzde durmaktayken ülkemiz sorumlu kurumları arasında görev paylaşımında çakışmaların da bulunması ilerleyen süreçte hangi seviyede sıkıntılar yaşanabileceğini öngörme konusunda dahi farklı modeller incelemeyi gerekli kılmıştır.

Nükleer siber emniyetin sağlanabilmesi için sağlam bir çerçevenin oluşturulması gerekmektedir. Siber emniyet, nükleer tesis henüz proje aşamasındayken başlayan ve alandaki tüm radyoaktivitenin son bulmasına kadar devam edecek en az 80[5] yıllık bir süre boyunca güvenliğin hiçbir zaman terkedilmediği bir **yaşam döngüsü** haline getirilmelidir. Bu döngü içerisinde siber tehdidin asimetrik olması muhtemel güvenlik açıklarına dönük sürekli bir değerlendirme gerektirmektedir. Bu döngü sadece lisans sahibi ya da işletmeciyi değil denetleme, düzenleme yetkisi bulunan kurumları da içine alması gerektiğinden bu döngünün oluşturulması görevi denetleme ve düzenleme yetkisi olan kurumda olmalıdır.

Nükleer tesislerin işletilmesi sürecinde önemli bir **farkındalık** faaliyetinin de yine güvenlik döngüsü gibi işletilmesi gerekmektedir. Sürekli yeni siber tehditlerin ortaya çıkması, siber açıdan riskli her davranış sonrasında zararın ortaya çıkmayışı, yatırımlar planlanırken ekonominin emniyet ya da güvenlikten zaman zaman önce gelmesi gibi durumlar ciddi riskler doğurabileceğinden yaşayan bir farkındalık döngüsü yaratılmalıdır. Yine bu döngünün oluşturulması görevi de denetleme ve düzenleme yetkisi olan kurumda olmalıdır.

Bahse konu döngülerin oluşturulması Uluslararası Atom Enerjisi Ajansı literatüründe emniyet alanıyla ilgili olarak detaylıca açıklanan **Nükleer Emniyet Kültürü**'nün sağlanması ile mümkün olacaktır. Nükleer Emniyet Kültürü "her zaman önemle değerlendirilmesi gereken bir tehdit vardır ve bu tehdidin olası zararlarının önüne geçmek için Nükleer Emniyet önemlidir" şeklinde tanımlanabilmektedir.

[5] 10 yıl inşaat süresi, 60 yıl işletme süresi 10 yıl en hızlı söküm süresi olarak hesaplanmıştır.

Nükleer Emniyet Kültürü içerisinde de var olan en iyi uygulamalardan faydalanma konusunda etkili faaliyetlerin yürütülmesi bu kültürün doğru yerleşmesini sağlayacaktır. Ayrıca emniyet için çok para harcamaktan daha öte düzenleyicisinden denetleyicisine işletmecisinden çalışanına kadar geniş alanda oluşturulabilen ortak bir bakış açısı da emniyet kültürünün başka önemli bir bileşenidir.

Emniyetli bir nükleer tesis hedefi için görevi, konumu, değerleri birbirinden farklı birçok insanın çabalamak durumunda olması nedeniyle her hedef grup için (düzenleyici kurum yöneticileri, düzenleyici kurum siber güvenlik personeli, işletmeci kurum yöneticileri, tesis siber güvenlik ekibi, tesis koruma görevlileri vb) detaylı **eğitim, bilgilendirme, farkındalık arttırma** faaliyetleri düzenlenmelidir. Bu faaliyetleri düzenlemek ve denetlemekle sorumlu kişiler kamu tarafından alanında uzman kişiler arasından seçilmelidir.

Ülkemiz özelinde bir nükleer tesisin denetlenmesi ile ilgili sorumluluk Türkiye Atom Enerjisi Kurumu'na bırakılmış durumdadır. Bu kurumun siber emniyetle ilgili bir birimi bulunmadığından dolayı santrallerin siber anlamda denetlenmeleri işini düzenli olarak Tübitak, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Türk Ordusunun Siber Komutanlıkları, USOM gibi kurumlardan uzman desteği alarak yürütecektir. Bir düzenleme ve denetleme kuruluşunun siber alan gibi özel bir alanda personel istihdamı sağlaması önemlidir. Denetleme görevlerinin asıl yükünün kurum personeli üzerinden sağlanacak şekilde ilave olarak dışardan destek alınarak yapılması tesis başına en az 80 yıl sürecek bir sürecin doğru işletilebilmesini sağlayacağı değerlendirilmektedir. Sürekli dışarıdan destekle bu sürecin yürütülmeye çalışılması; desteği verecek personelin sürekli değişmesi, desteği verecek personelin mevcut iş yüküne ilave olarak bu işi yapacak olması, desteği verecek personelin bağımsız bir kurumdan olmaması, desteği verecek ekibin kendi kurumlarının farklı öncelikleri nedeniyle çelişen denetleme değerlendirmelerinde bulunma ihtimalleri, bu kurumların

arasında denetleme görevi esnasında yatay bir hiyerarşik yapı bulunması gibi riskler barındırmaktadır.

Nükleer anlamda düzenleyici kuruluşun ideal yapısını oluşturması sürecine kadar siber güvenlikle ilgili paydaş olarak değerlendirilebilecek olan TÜBİTAK, EGM, JGK, TSK gibi kurumların TAEK tarafından uyumlu koordinasyonu sağlanmalı, bu kurumlardan destek veren personelin konuya deneyimlerini aktarma sürecini ayrı bir iş gibi görmelerinin önüne geçecek önlemler alınmalıdır.

Yine ülkemizdeki mevcut süreç özelinde Akkuyu ve Sinop tesislerini inşa eden/edecek şirketlerin siber emniyetle ilgili alacağı önlemleri doğru değerlendirebilecek bir ekibin oluşmasına ilk aşamada ihtiyaç vardır. Bu ekibin sadece teknik geçmişinin üzerine bilgi güvenliği alanında da çalışmalar yapmış personelden olması yeterli değildir. Özellikle UAEA'nın yayınlarına, önerdiği uygulamalara hakim, bir ya da daha fazla kritik tesisin çalışma düzenini görmüş, başka görevlerinin yanında ilaveten bu görevi de yerine getirmek durumunda kalmayan, nükleer kazaları/olayları derinlemesine bilen farkındalık seviyesi yüksek, bağımsız düşünebilen teknokratlardan, güvenlik personelinden, bilim insanlarından oluşması gerekmektedir. Bu kalifikasyonda bireylerden oluşan bir ekibi bir araya getirmenin zorluğu denetleme ve değerlendirme faaliyetlerini doğru orantılı olarak etkileyecektir.

Kritik altyapılarda ya da nükleer tesislerde yabancı ülkelerden uzmanların gelmesi yapılan işi doğası gereği kabul edilebilir ancak bu durum ülkeler arası ciddi bir istihbarat paylaşımı ihtiyacını da beraberinde getirecektir. Bu sebeple varolan ya da kurulması planlanan düzenleyici kurumların ülkemizin istihbarat teşkilatlarıyla da irtibat noktaları mutlaka planlanmalıdır.

Kritik altyapılarla ilgili olarak **sorumlu kuruluş**un belirlendiği, çelişkisiz olarak sektörlerin paylaşıldığı bir çerçevenin oluşturulmasına ihtiyaç duyulmaktadır. Kritik altyapılara ya da nükleer tesislere yapılacak siber saldırıların asimetrik olma, öngörülemez riskleri barındırma durumları doğru yasal çerçevenin oluşturulması için acele edilmesi gerektiğini göstermektedir.

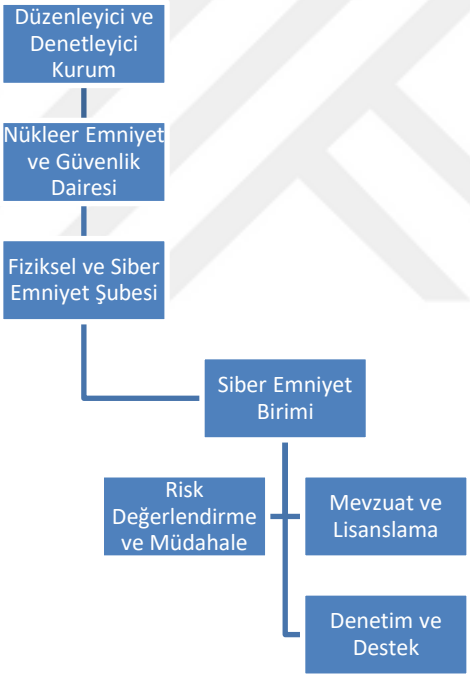
Kritik altyapı ya da nükleer tesislerle ilgili yapılacak yasal düzenlemelere hazırlık sürecinde bu tesislerin işletmecisi konumunda bulunan şirketlerin de katkısı mutlaka sağlanmalıdır. Nihai olarak kamu yararı öncelikli olarak gözetilerek düzenlemeler yapılacak da olsa bu şirketlerin tecrübelerinin dinlenmesi yapılacak düzenlemelerin hatalar nedeniyle değiştirilmesi ihtiyacı gibi sonuçları da ortadan kaldıracaktır.

Akkuyu projesinde tüm sorumluluk Rus tarafına yüklenmiş olsa da yaşanabilecek bir kazada Türk tarafının zarar göreceği düşünülerek pasif kalınmadan hareket edilmelidir. Bu hareket sürecinin doğru yönetilebilmesi için alanla ilgili yeterli bilgi birikimi oluşturacak çalışmaların yapılması ve uluslararası kuruluşlarla düzenli işbirliği faaliyetlerinin yürütülmesi gerekmektedir.

Başbakan'a bağlı iken 2002 yılında Enerji ve Tabii Kaynaklar Bakanlığına bağlı kuruluş statüsünde bağlanan TAEK'in hem bu statüsü hem ABD'de bulunan NRC'nin bağımsızlığı seviyesinde bağımsız olması durumunun ilgili kamu kurum ve kuruluşlarınca yeniden değerlendirilmesi gerekmektedir.

Nükleer tesislerin siber emniyeti ile ilgili kalifiye işgücünün Düzenleyici ve Denetleyici bir kurum (TAEK ya da Nükleer Düzenleme Kurumu) bünyesinde oluşturulması ve bu kurumun direkt devlet başkanına bağlı olarak faaliyet yürütmesi ihtiyacının karar vericiler nezdinde oluşması sonrasında ülkemiz adına **teze konu alana özel** ideal hiyerarşik yapının çizelgede detaylandırıldığı gibi olabileceği değerlendirilmektedir.

Çizelge 5-1 Organizasyon Şeması[6]



[6] Hazırlanan şema sadece Siber Emniyet alanı ile ilgili birimlerden oluşmaktadır. Tüm birimler gözetilerek **hazırlanmamıştır**.

Siber Emniyet Birimi

Ülkemizde bulunan lisanslanmış tesislerde siber emniyet alanı için düzenleme politikaları ve lisanslamanın incelenmesi konularında politika ve programlar geliştirir ve uygular. Diğer ilgili birimlerle koordinasyonu sağlar. Siber korunma programının tüm yönleriyle yönetimini sağlar.

Risk Değerlendirme ve Müdahale Alt Birimi

Tesislerin ve kurumun siber emniyetiyle ilgili sürekli risk analizi yapar. Nükleer tesislerin Sektörel SOME'si olarak faaliyet yürütecek olan kurum SOME'sini kurar ve yönetir. Nükleer tesislerin SOME'leriyle iletişim ve bilgi paylaşımı faaliyetlerini yürütür. Kuruma ait altyapının siber saldırılardan korunması faaliyetlerini yürütür. Kolluk ve istihbarat birimleriyle koordinasyonu sağlar. Paydaş kurumlarla ve kurumun diğer siber emniyet kısımlarıyla siber emniyet alanında; siber olayların soruşturulması, deneyimlerin paylaşılması, risklerin belirlenmesi ve hızlı bir şekilde değişen siber alana uyum konularında ortak çalışmalar yürütür. Ulusal ve uluslararası programlara katılım, kurum adına bilgilendirme faaliyetlerini yürütür.

Kurumu ilgilendiren her türlü iletişim faaliyetlerinin emniyetini sağlar. Kuruma bağlı yerleşkeler arasındaki iletişim yapısının kontrolünü sağlar. Kurumun ve tesislerin siber emniyetle ilgili acil durum planlarını ve programlarını yürütülmesini sağlar. Acil durum anında müdahale personelinin hazır bulunmasını sağlar. Siber tatbikatları yürütür. Siber olay sonrasında yapılmasına ihtiyaç duyulan adli

incelemeler için dijital materyale ilk müdahaleyi yapar. Siber emniyeti kapsayacak şekilde oluşturulmuş olan bir köstebek (insider) programının uygulanması sürecinde görev alır.

Siber Mevzuat ve Lisanslama Alt Birimi

Siber emniyetle ilgili düzenleyici ve denetleyici faaliyetlerin ve programların planlanması, koordinasyonu ve yönetimini gerçekleştirir. Reaktörlerin siber emniyeti konusunda kural oluşturma, lisanslama, varolan kuralların yerindelik denetimlerini gerçekleştirme faaliyetlerini yürütür. İşletmecilerin siber emniyet planlarının mevcut düzenlemelere uyumunu inceler. İşletmecinin siber emniyet planını değerlendirme şablonları oluşturur. Tasarıma Esas Tehdit (TET) doküman şablonunun siber emniyet açısından geliştirilmesini sağlar. Tesislerce hazırlanan TET dokümanının siber emniyet açısından incelenmesi faaliyetini yürütür. Kurumun ve tesislerin siber emniyetle ilgili acil durum planlarının ve programlarının geliştirilmesini sağlar.

Siber Denetim ve Destek Alt Birimi

Tesislerin siber emniyet açısından denetlenmesi faaliyetini yürütür. Planlı ve ani denetim faaliyetlerini belirler ve uygular. Kurum içi tüm bilgilerin sınıflandırılması ve korunması süreçleriyle ilgili altyapıyı ve mevcut altyapının kontrolünü sağlar. Tüm giriş yetkilendirme, şifreleme, şifre dağıtımı, şifre değişimi gibi süreçlere ait altyapıyı oluşturur ve mevcut altyapının siber emniyet açısından uygunluk denetimini sağlar. Giriş ve çıkış kayıtlarına ait loglama yapısını yönetir.

Siber emniyet açısından bir eğitim programı hazırlar ve uygular. Mevcut eğitim programının uygunluk denetimi faaliyetini yerine getirir. Farkındalık faaliyetlerini hazırlar ve uygular. Yapılan denetim, verilen eğitim ve farkındalık faaliyetlerinin tamamının uygunluk denetimi ve verim kontrolünü sağlar. Siber emniyetin dahil olduğu tüm alanlarda klavuzların hazırlanmasını sağlar/hazırlanması sürecine katkıda bulunur. Siber emniyet kültürü programını oluşturur, programın tüm verim kontrolleri ve uygulanması süreçlerini kontrol eder. Diğer birimlere ihtiyaç duyulması halinde siber emniyet alanında destek verir.

ÖZET

Siber Olaylara Müdahale Konusunda Amerika Birleşik Devletleri, Fransa ve Türkiye'nin İdari Yapılarının İncelenmesi – Nükleer Santral Örneği

Dünyada olduğu gibi Türkiye'de de internet kullanımı, devlet ağının nitelikleri ve özel sektörün artan gereksinimleri dolayısıyla giderek artmaktadır. Bu artışın yanında farklı görevler verilebilen birçok eşya da siber uzayda yerini almaktadır. Siber uzaydaki büyüyen çeşitlilik siber suçların da sık yaşanmasına neden olmaktadır. Suçtan etkilenen bazen vatandaşlarken bazen de kritik altyapılar yani devletlerin kendileridir. Geleneksel suçlarda alışılagelmiş simetri siber suçlarda asimetrik olarak karşımıza çıkmakta ve soruşturulmasını zorlaştırmaktadır.

2010 yılında İran Natanz Uranyum Zenginleştirme Tesisine Stuxnet olarak isimlendirilen bir siber saldırı yapılmıştır. Bu saldırı fiziksel bir tesise dijital yollarla yapılmış en büyük saldırıdır ve devletlerin siber güvenliğe konservatif bakışı değiştirmiştir. Nükleer siber emniyet dünyasının her seferinde "Stuxnet'ten Sonra" diye söze başlaması saldırının dünyada yarattığı şok etkisini göstermektedir. 2008 yılında Bakü Tiflis Ceyhan boru hattına ülkemiz sınırlarında yapılmış saldırı ve 2015 yılında ülke genelinde meydana gelen elektrik kesintilerinin siber saldırı olup olmadığı konusunda şüpheler hala devam etmektedir. Tüm bu gelişmeler nükleer tesisleri de kapsayan kritik altyapıların tamamına yönelik siber saldırılardan korunmanın ülkemiz için de önemli olduğunu göstermektedir.

Ülkemiz önümüzdeki 10 yıl içerisinde 2 farklı nükleer tesiste 8 nükleer reaktöre sahip olma yolunda ilerlemektedir. Bu nükleer tesisler hedef alınarak ya da hatalı uygulamalar sonucu meydana gelebilecek olumsuzluklar radyoaktivite yayılımı ihtimalini de gündeme getirecektir. Siber korunma sadece saldırı anını içeren kısa dönemli reaktif eylemlerden öte, saldırı öncesinde düzenli olarak güvenlik açıklarının araştırıldığı, tüm cihazların yazılımsal olarak güncelliğinin sürekli kontrol edildiği, personelin farkındalık seviyesinin düzenli olarak güçlendirildiği, paket çözümü bulunmayan, güçlü bir denetleme çerçevesinin oluşturulması gerekliliklerinin sürekli üzerinde durulması gerekmekte olan dinamik bir yapıdadır.

Bu çalışma ile nükleer siber emniyet konusunda ülkemizin mevcut yapısının yanında Amerika Birleşik Devletleri ve Fransa gibi nükleer reaktör işletimi alanında iki öncü ülkenin mevcut yapıları incelenmiş ve ülkemizde bu anlamda mevcut rejimin doğru bir değerlendirmesinin yapılması amaçlanmıştır.

Çalışma sonucunda ülkemizde nükleer tesislerin ve kritik altyapıların siber emniyetinin sağlanması konusunda çok başlı bir yapının var olduğu, bu alandaki sorumlulukların netleştirilmesi gerektiği, nükleer emniyet kültürünün bir yaşam döngüsü şeklinde algılanarak oluşturulması gerektiği, öncelikle ilgili kurumlar, sonrasında ülke genelini kapsayacak farkındalık faaliyetlerinin gerçekleştirilmesi gerektiği sonuçlarına ulaşılmıştır.

Anahtar Kelimeler: Kritik Altyapı, Nükleer Emniyet Kültürü, Nükleer Tesis, Siber Korunma, Siber Saldırı,

SUMMARY

Reviewing to Cyber Incident Response Structure of USA, French and Turkey–Nuclear Power Plant Example

Internet usage is increasing in Turkey as well as in the world because of the nature of the governmental network and the growing need of the private sector. In addition to this increase, many items that can be assigned different functions are also located in the cyber space. The growing variation on cyber space causes cybercrime to be committed more frequently. Sometimes citizens and sometimes critical infrastructures, which means the state itself, may be affected by the crime. In spite of symmetric nature of traditional crime, cybercrime is in an asymmetric form which causes to be investigated harder.

In 2010, Iranian Natanz Uranium Enrichment Facility was exposed to a cyber attacked named as Stuxnet. This attack is the biggest cyberattack on any physical facility and has changed the conservative view of states on cyber security. Nuclear cyber security world is always shocked of the Stuxnet. There are still doubts on whether attacks on the Baku Tbilisi Ceyhan pipeline in 2008 and the blackout in the country in 2015 were cyber ones. All these instances show that protecting the critical infrastructure which includes nuclear facilities from cyber-attacks is also important for our country.

In the next decade, it is planned for Turkey to construct 8 nuclear reactors in 2 different nuclear power plant. The potential damages occurring as a result of attacks to these facilities or misusage of them may arise risks of radioactivity spread. Cyber protection has a dynamic structure that requires constant consideration of security vulnerabilities, constantly checking the software update of all devices, regularly strengthening the level of awareness of the stuff, requiring to create a robust audition framework and constantly investigating security vulnerabilities at pre-incident term with no package solution instead of short-term reactive actions during attack

This study examines the existing nuclear security structures of USA and France, two leading countries in the field of nuclear reactor operations, as well as the existing structure of the our country, and aims to make an accurate assessment of the current situation in our country in this respect.

As a result of this work, some findings have been reached. We have more than an authority on ensuring cyber security of nuclear facilities and critical infrastructure in our country. We need to make clear responsibilites on this field and to constitute a nuclear security culture which perceived like a lifecycle besides an awareness action that cover not only related institutions but also whole country.

Keywords: Critical Infrastructure, Cyber Attack, Nuclear Facility, Cyber Protection, Nuclear Security Culture

KAYNAKLAR

ABRAMS, M., & WEISS, J. (2017, March 3). Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia. Retrieved from https://pdfs.semanticscholar.org/78df/bff3c64097ef061035839b7254f7f4dceacd.pdf Erişim Tarihi: 01.12.2017

Abusix. (2017). DDOS, BBC. Retrieved from https://www.abusix.com/blog/5-biggest-ddos-attacks-of-the-past-decade Erişim Tarihi: 12.03.2017

Aciers. (2010). Portrait d'André-Claude LACOSTE, le président de l'Autorité de Sureté Nucléaire (US). Retrieved from https://web.archive.org/web/20110720215942/http://aciers.free.fr/index.php/2010/02/08/portrait-de-andre-claude-lacoste-le-president-de-lautorite-de-surete-nucleaire-us/ Erişim Tarihi: 11.12.2017

AFAD. (2014). 2014-2023 Teknolojik Afetler Yol Haritası Belgesi. AFAD - Planlama ve Zarar Azaltma Dairesi Başkanlığı.

AKKUYUNPP. (2015). Rusya'da Egitim. Retrieved from http://www.akkunpp.com/rusyada-egitim Erişim Tarihi: 11.12.2017

AKKUYUNPP. (2017a). Akkuyu Projesi`ne ortak olmak için yerli-yabancı şirketlerden talepler var; inşaat için 30`dan fazla şirketle görüşüldü. Retrieved from http://www.akkunpp.com/akkuyu-projesine-ortak-olmak-icin-yerli-yabanci-sirketlerden-talepler-var-insaat-icin-30dan-fazla-sirketle-gorusuldu Erişim Tarihi: 11.12.2017

AKKUYUNPP. (2017b). Akkuyu Tarihçe. Retrieved from http://www.akkunpp.com/projenin-tarihcesi Erişim Tarihi: 18.10.2017

AKKUYUNPP. (2017c). Sınırlı Çalışma İzni Akkuyu. Retrieved from http://www.akkunpp.com/akkuyu-nukleer-as-sinirli-calisma-iznini-aldi/update Erişim Tarihi: 21.10.2017

Akşam. (2016, October 30). Siber Ordu güçleniyor... SİSAMER. Retrieved from http://www.aksam.com.tr/ekonomi/siber-ordu-gucleniyor/haber-561733 Erişim Tarihi: 10.11.2017

ALBRIGHT, D., BRANNAN, P., & WALROND, C. (2010). Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security Report.

ALTUNOK, T., & KATMAN, F. (2009). "Siber Tehdit Altyapısı ve Araçları", Suç, Terör ve Savaş Üçgeninde Siber Dünya (p. 73). Ankara: Barış Platin Kitabevi.

American Congress. ENERGY REORGANIZATION ACT OF 1974, 93–438 § (1974).

American Congress. UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, 107–56 § (2001).

ANSSI. (2017a). ANSSI Genel Bilgilendirme. Retrieved from https://www.ssi.gouv.fr/actualites/ Erişim Tarihi: 13.12.2017

ANSSI. (2017b). https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/. Retrieved from https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/ Erişim Tarihi: 01.10.2017

AREVA. (2017). BALANCED INTERNATIONAL IMPLEMENTATION. Retrieved from http://www.new.areva.com/EN/group-727/partner-to-the-world-s-power-companies-with-offices-around-the-globe.html Erişim Tarihi: 30.10.2017

ASN. (2017). ASN Strategy. Retrieved from http://www.french-nuclear-safety.fr/ASN/About-ASN/The-ASN-strategy Erişim Tarihi: 22.11.2017

AYDIN, E. (1992). Bilişim Suçları ve Hukukuna Giriş. Ankara: Doruk Yayınları.

Bakanlar Kurulu. (1996, August 7). Nükleer Maddelerin Fiziksel Korunması Sözleşmesi.

Bakanlar Kurulu. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar KuruluKarar, 2012/3842 Karar Sayısı § (2012).

BARAZ, B., & vd. (2013). Büro Teknolojileri. In Anadolu Üniversitesi Yayınları (pp. 146–147). Eskişehir.

BAYLON, C., BRUNT, R., & LIVINGSTONE, D. (2015). Cyber Security at Civil Nuclear Facilities Understanding the Risks - Chatham House Report.

BBC. (2008). BBC Georgia Cyberwar. Retrieved from http://news.bbc.co.uk/2/hi/europe/7559850.stm Erişim Tarihi: 03.03.2017

BBC. (2012, August 17). Shamoon virus targets energy sector infrastructure. Retrieved from http://www.bbc.com/news/technology-19293797 Erişim Tarihi: 09.11.2017

BEER, S. (2017, February 28). WHAT IS CYBERNETICS? Retrieved from https://pdfs.semanticscholar.org/a852/6b324bc7b236c57ed0e0b65a4e6311cd1295.pdf Erişim Tarihi: 28.22.2017

BIÇAKÇI, S. (2013). 21. Yüzyılda Siber Güvenlik (p. 40). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Bloomberg. (2014). BTC Explosion. Retrieved from https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar Erişim Tarihi: 10.12.2017

BP. (2017). BP Statistical Review of World Energy Report June 2017.

BROWN, J. T. (2011). Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress - Congressional Research Service. ABD.

BSI. (2014). Die Lage der IT in Deutchland 2014-Sicherheit 2014 - Bilgi Teknolojileri Güvenliği Almanya 2014.

BSTB. (2017). Bilim, Sanayi ve Teknoloji Bakanlığı. Retrieved from http://www.sanayi.gov.tr/teskilat.html

BTK. (2015). Uluslararası Siber Kalkan Tatbikatı 2014. Retrieved from https://www.btk.gov.tr/tr-TR/Uluslararasi-Etkinlik/Uluslararasi-Siber-Kalkan-Tatbikati-2014-20-Ulkenin-Katilimiyla-Gerceklestirildi Erişim Tarihi: 11.12.2017

BTK. (2017). Siber Güvenlik Kurulu. Retrieved from https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK-KURULU Erişim Tarihi: 26.11.2017

ÇAKMAK, H., & DEMİR, C. K. (2009). "Siber Dünyadaki Tehditler ve Kavramlar", Suç, Terör ve Savaş Üçgeninde Siber Dünya (p. 39). Barış Platin Kitabevi.

CANBEK, G., & SAĞIROĞLU, Ş. (2008a). Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler. Gazi Üniv. Müh. Mim. Fak. Dergisi, 23(1), 207.

CANBEK, G., & SAĞIROĞLU, Ş. (2008b). Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler. Gazi Üniv. Müh. Mim. Fak. Dergisi, 23(1), 184.

CarbonBrief. (2017). CarbonBrief Nucelar Power Plant Map. Retrieved from https://www.carbonbrief.org/mapped-the-worlds-nuclear-power-plants Erişim Tarihi: 22.11.2017

CarnegieMellonUni. (1989). 1989 CERT Advisories. Carnegie MellonUniversity Software Engineering Institute CERT Division.

CarnegieMellonUni. (2004). Steps for Creating National CSIRTs.

CEA. (2016). CEA - Defence and Security. Retrieved from http://www.cea.fr/english/Pages/research-areas/defence-and-security.aspx Erişim Tarihi: 01.05.2017

CEA. (2017a). CEA Technological Research. Retrieved from http://www.cea.fr/english/Pages/cea/the-cea-a-key-player-in-technological-research.aspx Erişim Tarihi: 01.10.2017

CEA. (2017b). CEA Web Sitesi. Retrieved from https://www.edf.fr/en/the-edf-group/who-we-are/edf-at-a-glance Erişim Tarihi: 09.02.2017

ÇELİKPALA, M., BIÇAKÇI, S., & ERGÜN, D. (2015). Türkiye'de Siber Güvenlik. EDAM.

CIA. (2015). Digital Innovation. Retrieved from https://www.cia.gov/offices-of-cia/digital-innovation/index.html

CIA. (2017). CIA - who we are. Retrieved from https://www.cia.gov/about-cia/todays-cia/who-we-are Erişim Tarihi: 12.08.2017

ÇİFCİ, H. (2013). Her Yönüyle Siber Savaş (p. 5). Ankara: Tübitak Popüler Bilim Kitapları.

CLARKE, R. A., & KNAKE, R. K. (2011a). Siber Savaş (p. 46). İstanbul: İkü Yayınevi.

CLARKE, R. A., & KNAKE, R. K. (2011b). Siber Savaş (p. 119). İstanbul: İkü Yayınevi.

DENNING, D. E. (2000, May 23). Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.

DHS. (2007). National Strategy for Homeland Security.

DHS. (2017a). Budget-in-Brief Fiscal Year 2017 Report.

DHS. (2017b). DHS Nuclear Reactors Materials and Waste Sector. Retrieved from https://www.dhs.gov/nuclear-reactors-materials-and-waste-sector Erişim Tarihi: 03.10.2017

DHS. (2017c). ISAC Üye Listesi. Retrieved from https://www.nationalisacs.org/member-isacs Erişim Tarihi: 01.11.2017

DHS. (2017d). National Infrastructure Protection Plan. Retrieved from https://www.dhs.gov/national-infrastructure-protection-plan Erişim Tarihi: 05.10.2017

DICTIONARY. (2017). Cyber İngilizce Szlük. Retrieved from http://www.dictionary.com/browse/cyber?s=t Erişim Tarihi: 09.03.2017

DINE, A. V., ASSANTE, M., & STOUTLAND, P. (2016). Outpacing Cyber Threats - Priorities For Cybersecurity at Nuclear Facilites - Nuclear Threat Inıtiative.

DoD. (2015). THE DEPARTMENT OF DEFENSE CYBER STRATEGY. Department of Defence.

DoD. (2017a). US Department Of Defence. Retrieved from https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ Erişim Tarihi: 12.10.2017

DoD. (2017b, February 28). Department of Defense Dictionary of Military and Associated Terms. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf Erişim Tarihi: 28.02.2017

DOLAN, A. (2004, February 10). Social Engineering. SANS Institute.

DOMSCHEIT-BERG, D., KLOPP, T., & CHASE, J. (2011). Inside Wikileaks : My Time With Julian Assange at The World's Most Dangerous Website (1.). New York: Crown Publishers.

DPB. (2017). Devlet Personel Başkanlığı. Retrieved from http://euygulama.dpb.gov.tr/devletteskilati/kontrollu/Idare.aspx Erişim Tarihi: 05.06.2017

DPT. (1996). NÜKLEER ENERJİ HAMMADDELERİ URANYUM – TORYUM (No. 2429).

DÜLGER, M. V. (2004). Bilişim Suçları. Ankara: Seçkin Yayıncılık.

DUPUIS, M. C. (2010). Status, responsibilities and missions of ANDRA (France). Presented at the Technical meeting on RWMO. Retrieved from https://www-ns.iaea.org/downloads/rw/conventions/fourth-review-cycle/tm-paris/Session%201/andra-france.pdf Erişim Tarihi: 26.11.2017

EC. (2001). Conventin on a cybercrime - Full Liste - Entry Force - Ratification. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=9vXWmibS

EC. (2004, October 20). Critical Infrastructure Protection in the fight against terrorism.

EC. (2006). European Programme for Critical Infrastructure Protection. Retrieved November 2, 2017, from http://publications.europa.eu/resource/cellar/841c4851-bf45-4ac3-884d-a748e667bfd8.0005.02/DOC_2 Erişim Tarihi: 11.09.2017

EC. (2008, December 8). COUNCIL DIRECTIVE 2008/114/ECon the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

EDAM. (2011). Nükleer Enerjiye Geçişte Türkiye Modeli Raporu - Ekonomi ve Dış Politika Araştırmalar Merkezi.

EDF. (2014). EDF Energies Nouvelles commissions a 150 MW wind farm in Turkey - EDF Energies Nouvelles Türkiyede toplam 150 MW'lık rüzgar enerjisi tesisi siparişi. Retrieved from https://www.edf-energies-nouvelles.com/en/edf-energies-nouvelles-commissions-a-150-mw-wind-farm-in-turkey/ Erişim Tarihi: 11.08.2017

EIA. (2017, May 19). US Energi Information Administration - US Energy Consumption by Energy Source 2016. Retrieved from https://www.eia.gov/energyexplained/?page=us_energy_home Erişim Tarihi: 09.11.2017

Elektrikport. (2017). Ayda Nükleer Enerji. Retrieved from http://www.elektrikport.com/teknik-kutuphane/ayda-nukleer-enerji/4341#ad-image-0 Erişim Tarihi: 20.08.2017

ENISA. (2016). Cyber Europe 2016 After Action Report.

ENISA. (2017). ENISA. Retrieved from https://www.enisa.europa.eu/about-enisa Erişim Tarihi: 08.11.2017

ERSANEL, N. (2001). Siber İstihbarat: Siber ve Dijital Casusluğun Anatomisi (p. 10). Ankara: Asam Yayınları.

ETKB. (2016). Türkiye'nin Nükleer Santral Projeleri: Soru-Cevap - Enerji ve Tabi Kaynaklar Bakanlığı Yayınları Ocak 2016.

ETKB. (2017a). Elektrik. Retrieved from http://www.enerji.gov.tr/tr-TR/Sayfalar/Elektrik) Erişim Tarihi: 01.08.2017

ETKB. (2017b). Enerji Tanım ETKB YEGM. Retrieved from http://www.yegm.gov.tr/ Erişim Tarihi: 01.01.2017

European Parliament v Council. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, 460/2004 § (2004).

European Parliament v Council. REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 526/2013 § (2013).

FALLİERE, N., MURCHU, L. O., & CHIEN, E. (2011). W32.Stuxnet Dossier Report.

FBI. (2017a). Critical Incident Response Group - CIRG. Retrieved from https://www.fbi.gov/services/cirg Erişim Tarihi: 10.05.2017

FBI. (2017b). CYBER. Retrieved from https://www.fbi.gov/investigate/cyber Erişim Tarihi: 05.09.2017

FBI. (2017c). FBI Field Offices. Retrieved from https://www.fbi.gov/contact-us/field-offices Erişim Tarihi: 28.11.2017

FBI. (2017d). FBI Mission. Retrieved from https://www.fbi.gov/about/mission Erişim Tarihi: 20.08.2017

FBI. (2017e). FBI Overseas Offices - Legal Attache Offices. Retrieved from https://www.fbi.gov/contact-us/legal-attache-offices Erişim Tarihi: 28.11.2017

FIRST. (2017). FIRST Org Member Teams. Retrieved from https://www.first.org/members/teams/tr-cert Erişim Tarihi: 09.11.2017

French Energy Ministry. (2016). PANORAMA SECTORIEL ENERGIE 2015-2016. Retrieved from https://www.economie.gouv.fr/files/files/directions_services/agence-participations-etat/PANORAMA_SECTORIEL_ENERGIE_2015-2016_-_APE.pdf Erişim Tarihi: 05.09.2017

French Government. Fransa - Nükleer Alanda Saydamlık ve Emniyet Yasası - Loi n° 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire

(1). (2006). Retrieved from https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000819043 Erişim Tarihi: 11.12.2017

French Government. Agence nationale de la sécurité des systèmes d'information - Bilgi Sistemlerinin Güvenliği için Ulusal Ajans, 2009–834 § (2009). Retrieved from https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212&dateTexte=&categorieLien=id Erişim Tarihi: 20.10.2017

French Government. (2017). France and Cyber security. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/ Erişim Tarihi: 13.12.2017

French National Assemble. (2013). 14th legislature - Question 29424. Retrieved from http://questions.assemblee-nationale.fr/q14/14-29424QE.htm Erişim Tarihi: 25.10.2017

French Washington Embassy. (2013). Nuclear Power in France – French Washington Embassy 2013. Retrieved from https://franceintheus.org/IMG/pdf/Nuclear_power_in_France.pdf Erişim Tarihi: 26.10.2017

GOODMAN, M. D., & BRENNER, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. Int'l JL & Info. Tech., 10, 139–223.

HaberTürk. (2011). Nükleer santralsız kaza listesindeyiz. Retrieved from http://www.haberturk.com/dunya/haber/611217-nukleer-santralsiz-kaza-listesindeyiz Erişim Tarihi: 25.11.2017

HADNAGY, C. (2010). Social Engineering The Art Of Human Hacking.

HALLER, J., MERRELL, S. A., BUTKOVIC, M. J., & WILLKE, B. J. (2011). Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0 (Technical Report No. CMU/SEI-2011-TR-015 ESC-TR-2011-015). Carnegie Mellon.

HAN, A. K., STEIN, A., KİBAROĞLU, M., ERGUN, D., KASAPOĞLU, C., ÇELİKPALA, M., & ÜLGEN, S. (2015). Türkiye'de Enerji Emniyeti - EDAM (No. ISBN 978-9944-0133-6-9).

Hürriyet. (2003a). Batman Barajı Şifre Krizi. Retrieved from http://www.hurriyet.com.tr/batman-barajinda-sifre-krizi-cozuluyor-151841 Erişim Tarihi: 05.11.2017

Hürriyet. (2003b). Metsamora Karşı Erken Uyarı Sistemi. Retrieved from http://www.hurriyet.com.tr/metsamora-karsi-erken-uyari-sistemi-123641 Erişim Tarihi: 24.10.2017

Hürriyet. (2007). Hürriyet IMKB. Retrieved from http://www.hurriyet.com.tr/255-milyar-dolarlik-borsaya-kepce-darbesi-7777722 Erişim Tarihi: 10.11.2017

Hürriyet. (2008). PKK'nın en önemli 'hacker'ı yakalandı. Retrieved from http://www.hurriyet.com.tr/gundem/10393202.asp Erişim Tarihi: 04.11.2017

Hürriyet. (2009). Hürriyet Atatürk Havalimanı. Retrieved from http://www.hurriyet.com.tr/virus-havalimanini-felc-etti-10894278 Erişim Tarihi: 01.11.2017

Hürriyet. (2011). Hürriyet Gümrük Veritabanı. Retrieved from http://www.hurriyet.com.tr/gumrukte-sistem-coktu-1-milyar-dolarlik-ticaret-durdu-16920642 Erişim Tarihi: 02.11.2017

Hürriyet. (2016, June 6). Türk ordusunun yeni kuvveti siber savunma. Retrieved from http://www.hurriyet.com.tr/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652 Erişim Tarihi: 10.11.2017

ICS-CERT. (2012, October 16). ICS Information for Shamoon. Retrieved from https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B Erişim Tarihi: 09.11.2017

IRSN. (2017). IRSN ANNUAL REPORT 2016 ISSN 2493-593X.

İTÜ. (2006). İstanbul Teknik Üniversitesi Enerji Çalıştayı ve Sergisi Raporu.

JAFFER, M. (2011). Uranium Enrichment. Retrieved from http://large.stanford.edu/courses/2011/ph241/jaffer1/ Erişim Tarihi: 22.11.2017

JANCZEWSKI, L. J., & COLARIK, A. M. (2008). Cyber warfare and cyber terrorism. In IGI Global (pp. 13–25). London.

Justice Department. (2017). US - Justice Department. Retrieved from https://www.justice.gov/about

KABAY, M. E. (2009). A Brief History of Computer Crime: An Introduction for Students.

KARAGÜLMEZ, A. (2005). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri. Ankara: Seçkin Yayıncılık.

KESLER, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010 - Monterey, California. Naval Postgraduate School.

KESTANE, D. (2002). Kamu Kesiminde İdari Kuruluşların Genel Görünümü ve İdari Yapıda Yeni Organizasyonlar Olarak Ba-ğımsız İdari Otoriteler (Üst Kurullar). Maliye Dergisi, (139). Retrieved from https://dergiler.sgb.gov.tr/calismalar/maliye_dergisi/yayinlar/md/md139/kestane.pdf Erişim Tarihi: 29.12.2017

KOÇ, & ŞENEL, M. C. (2013). DÜNYADA VE TÜRKİYE'DE ENERJİ DURUMU - GENEL DEĞERLENDİRME, 54(639), 32–44.

LANDWEHR, C. E., BULL, A. R., MCDERMOTT, J. P., & CHOI, W. S. (1994). A Taxonomy of Computer Security Flaws, with Examples.

LE POINT. (2010). Les dix principaux producteurs d'électricité dans le monde - Dünyanın İlk 10 Elektrik Üreticisi. Retrieved from http://www.lepoint.fr/economie/les-dix-principaux-producteurs-d-electricite-dans-le-monde-10-08-2010-1223756_28.php Erişim Tarihi: 12.06.2017

LEE, R. M., ASSANTE, M., & CONWAY, T. (2014). German Steel Mill Cyber Attack - Sans Institute Report - ICS Defense Use Case (DUC).

LeParisien. (2017). Cyberattaque : les centrales nucléaires françaises sont-elles en sécurité ? Retrieved from http://www.leparisien.fr/high-tech/cyberattaque-les-centrales-nucleaires-francaises-sont-elles-en-securite-28-06-2017-7094979.php Erişim Tarihi: 11.12.2017

LEWIS, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:

MATROSOV, A., RODIONOV, E., HARLEY, D., & MALCHO, J. (n.d.). Stuxnet Under the Microscope. Retrieved from https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf Erişim Tarihi: 08.11.2017

Mentalfloss. (2017). Kyshtym Disaster. Retrieved from http://mentalfloss.com/article/71026/kyshtym-disaster-largest-nuclear-disaster-youve-never-heard Erişim Tarihi: 30.10.2017

MHI. (n.d.). Mitsubishi Heavy Industry - Sinop. Retrieved from http://www.mhi.com.tr/news/20130508.html Erişim Tarihi: 20.10.2017

Milliyet. (2003). Milliyet Web Batman. Retrieved from http://www.milliyet.com.tr/batman-baraji-

sifrelendi/ekonomi/haberdetayarsiv/28.05.2003/11905/default.htm Erişim Tarihi: 20.06.2017

Milliyet. (2012). THY Dos Saldırısı. 6 saatte 400binlira zarar. Retrieved from http://www.milliyet.com.tr/thy-6-saatte-400-bin-lira-zarar-etti-ekonomi-1586632/ Erişim Tarihi: 10.10.2017

MIN, J. (2017, February 11). North Korea's Asymmetric Attack on South Korea's Nuclear Power Plants - Stanford University Jesse Min Coursework. Retrieved from http://large.stanford.edu/courses/2017/ph241/min1/ Erişim Tarihi: 02.11.2017

MOITRA, S. D. (2005). Developing policies for cybercrime. European Journal of Crime Criminal Law and Criminal Justice, 13(3), 435–464.

MOORE, G. M., BANUELOS, C. A., & GRAY, T. T. (2016). Replacing Highly Enriched Uranium in Naval Reactors.

National Geographic. (2017). Most Dangerous Nuclear Plant most-dangerous-nuclear-plant-armenia/. Retrieved from https://news.nationalgeographic.com/news/energy/2011/04/110412-most-dangerous-nuclear-plant-armenia/ Erişim Tarihi: 10.12.2017

NEI. (2016). Cyber Security for Nuclear Power Plants - Nuclear Energy Institute. Retrieved from https://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants Erişim Tarihi: 11.12.2017

NEI. (2017a). 4 Things to Know About Nuclear Plants and Cyber Security - Nuclear Energy Institute. Retrieved from https://www.nei.org/News-Media/News/News-Archives/2017/4-Things-to-Know-About-Nuclear-Plants-and-Cyber-Se Erişim Tarihi: 11.12.2017

NEI. (2017b). Nuclear Energy Institute - World Statistics - Nurclear Energy Around the World. Retrieved from https://www.nei.org/Knowledge-Center/Nuclear-Statistics/World-Statistics Erişim Tarihi: 09.11.2017

NRC. (2013). Three Mile Island Accident - US NRC. NRC.

NRC. (2016). Three Mile Island Accident of 1979 Knowledge Management Digest - Overview. NRC.

NRC. (2017a). NRC - Nuclear Regulatory Comission. Retrieved from www.nrc.gov.html Erişim Tarihi: 06.07.2017

NRC. (2017b). NRC History. Retrieved from https://www.nrc.gov/about-nrc/history.html Erişim Tarihi: 09.10.2017

NRC. (2017c). Nuclear Regulatory Commission. Retrieved from https://www.nrc.gov/about-nrc.html Erişim Tarihi: 09.09.2017

NRC. (2017d). Nuclear Regulatory Commission - Decommissioning. Retrieved from https://public-blog.nrc-gateway.gov/category/decommissioning-2/ Erişim Tarihi: 28.10.2017

NRC. (2017e). Nuclear Regulatory Commission - NRC - Licensing Fees. Retrieved from https://www.nrc.gov/about-nrc/regulatory/licensing/fees.html Erişim Tarihi: 06.09.2017

NRC. (2017f). Nuclear Security and Incident Response. Retrieved from https://www.nrc.gov/about-nrc/organization/nsirfuncdesc.html#funcdesc Erişim Tarihi: 09.08.2017

NRC. (2017g). United States Nuclear Regulatory Commission - PWR Animation. Retrieved from http://www.nrc.gov/reading-rm/basic-ref/students/animated-pwr.html Erişim Tarihi: 11.08.2017

NTI. (2017a). Nuclear Threat Initiative. Retrieved from http://www.nti.org/learn/treaties-and-regimes/treaty-on-the-non-proliferation-of-nuclear-weapons/ Erişim Tarihi: 07.10.2017

NTI. (2017b). Nuclear Threat Initiative - India 100 Mw Research Reactor. Retrieved from http://www.nti.org/learn/facilities/837/ Erişim Tarihi: 29.10.2017

NTI. (2017c). References for Cyber Incidents at Nuclear Facilities. Retrieved from http://www.nti.org/analysis/tools/table/133/ Erişim Tarihi: 08.11.2017

NTV. (2015). 31 mart kesintisi raporu. Retrieved from https://www.ntv.com.tr/ekonomi/turkiyeyi-karanliga-gomen-kesintiye-iliskin-rapor-tamamlandi,S3v0HDcG-kySzCeBTFrbTQ Erişim Tarihi: 06.11.2017

NTV. (2017). Nükleer Enerjinin Türkiye'deki Tarihçesi. Retrieved from https://www.ntv.com.tr/ekonomi/nukleer-enerjinin-turkiyedeki-tarihcesi,LI7qG7zm-0q6yZLV0rHy7g Erişim Tarihi: 20.10.2017

Nucnet. (2013). Turkey Has Made Important Progress In Nuclear Power Programme, Says UAEA. Retrieved from https://www.nucnet.org/all-the-news/2013/11/18/turkey-has-made-important-progress-in-nuclear-power-programme-says-iaea Erişim Tarihi: 11.12.2017

NükleerAkademi. (2017a). Türkiye Uranyum ve Toryum Yatakları. Retrieved from http://nukleerakademi.org/turkiye-uranyum-ve-toryum-yataklari/ Erişim Tarihi: 01.10.2017

NükleerAkademi. (2017b). Ülkemizde Nükleer Enerji. Retrieved from http://nukleerakademi.org/nukleer-enerji/ulkemizde-nukleer-enerji/ Erişim Tarihi: 11.11.2017

NyTimes. (2012). Obama ordered wave of cyberattacks against Iran. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html Erişim Tarihi: 15.10.2017

NyTimes. (2012, October 23). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back Shammon NYTimes. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html Erişim Tarihi: 09.11.2017

Observer. (2015). Observer 31 Mart. Retrieved from http://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/ Erişim Tarihi: 15.08.2017 Erişim Tarihi: 11.12.2017

OECD NEA, & UAEA. (2004). Uranium, Resources, Production and Demand (No. 7209).

ÖNAL, H. (2012). Hedef Odaklı Sızma Testleri. Bilgi Güvenliği Akademisi. Retrieved from http://docplayer.biz.tr/751529-Hedef-odakli-sizma-testleri.html Erişim Tarihi: 05.09.2017

ÖZEMRE, A. Y. (2006). Türkiye'nin nükleer enerji macerası. Anlayış Dergisi.

PATE, Z. T. (1986). INPO's impact in the USA. UAEA. Retrieved from https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull28-3/28304796062.pdf Erişim Tarihi: 22.11.2017

PERRIER, Q. (2017). The French nuclear bet. FAERE Policy Paper,.

Polonyadan. (2014). Banka Phishing Yemleme. Retrieved from http://www.polonyadan.com/2014/09/22/millenium-bank-musterilerine-phishing-saldirisi/ Erişim Tarihi: 05.11.2017

PORESKY, C., ADREADES, C., KENDRICK, J., & PETERSON, P. (2017). Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies (No. UCBTH-17-004). University of California, Berkeley.

Power Technology. (2017). World Worst Nuclear Power Disasters. Retrieved from http://www.power-technology.com/features/feature-world-worst-nuclear-power-disasters-chernobyl/ Erişim Tarihi: 13.08.2017

Reuters. (2009, February 19). IAEA finds graphite, further uranium at Syria site - Orchard. Retrieved from https://www.reuters.com/article/us-nuclear-iaea-syria-sb/iaea-finds-graphite-further-uranium-at-syria-site-idUSTRE51I45R20090219 Erişim Tarihi: 09.11.2017

Reuters. (2013a). Researchers Say Stuxnet Was Deployed Against Iran in 2007. Retrieved from https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226 Erişim Tarihi: 02.10.2017

Reuters. (2013b). Rosatom offers emerging nations nuclear package - paper. Retrieved from https://uk.reuters.com/article/uk-rosatom-nuclear-russia/rosatom-offers-emerging-nations-nuclear-package-paper-idUKBRE94C09G20130513 Erişim Tarihi: 11.12.2017

Reuters. (2016a). German Nuclear Pland Infected with Computer Viruses. Retrieved from https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS Erişim Tarihi: 06.10.2017

Reuters. (2016b). IAEA chief: Nuclear power plant was disrupted by cyber attack. Retrieved from https://www.reuters.com/article/us-nuclear-cyber/iaea-chief-nuclear-power-plant-was-disrupted-by-cyber-attack-idUSKCN12A1OC Erişim Tarihi: 08.11.2017

Rosatom ve AKKUYU NGS Elektrik Üretim A.Ş. (n.d.). 1956'dan günümüze Türkiye'nin ilk nükleer güç santrali Akkuyu.

Rosatom ve AKKUYU NGS Elektrik Üretim A.Ş. (n.d.). Nükleer enerji hakkında merak ettikleriniz.

Sabah. (2006). Radyasyon Mağduru Aile AİHM'ye Gitti. Retrieved from http://arsiv.sabah.com.tr/2006/10/14/gnd107.html Erişim Tarihi: 25.11.2017

Sabah. (2017). Cengiz-Kalyon-Kolin Akkuyu'ya ortak oldu. Retrieved from https://www.sabah.com.tr/ekonomi/2017/06/20/cengiz-kalyon-kolin-akkuyuya-ortak-oldu Erişim Tarihi: 11.12.2017

SecurityAffairs. (2014). Monju NPP Attack. Retrieved from http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html Erişim Tarihi: 01.11.2017

SecurityAffairs. (2016). According to the German BR24 News Agency, a computer virus was discovered in a system at the Gundremmingen nuclear plant in Germany. Retrieved from http://securityaffairs.co/wordpress/46708/security/virus-gundremmingen-nuclear-plant.html Erişim Tarihi: 06.11.2017

sendika62. (2014). Nükleer Düzenleme Kurumu haberi. Retrieved from http://sendika62.org/2014/04/nukleer-duzenleme-kurumu-yetkisi-tam-sorumlulugu-sifir/ Erişim Tarihi: 08.08.2017

ŞENTÜRK, H., ÇİL, C. Z., & SAĞIROĞLU, Ş. (2012). Cyber Security Analysis of Turkey. International Journal of Information Security Science, 1(4).

SFEN. (2016). La cyber-sécurité des installations nucléaires françaises : enjeux et opportunités - French Nuclear Society. Retrieved from http://www.sfen.org/fr/rgn/la-cyber-securite-des-installations-nucleaires-francaises-enjeux-et-opportunites Erişim Tarihi: 11.12.2017

SHERR, M., CRONIN, E., CLARK, S., & BLAZE, M. (2005, November 8). Signaling vulnerabilities in wiretapping systems.

SOKOLOV, Y. A. (2013). Multiple approaches on supporting nuclear program development and contracting of NPPs. Technichal Meeting presented at the Development and Management of National Capacity for Nuclear Power Program, UAEA. Retrieved from https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-02-11-02-14-TM-INIG/11.sokolov.pdf Erişim Tarihi: 11.12.2017

Statista. (2017). Mobile Phone Users. Retrieved from https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ Erişim Tarihi: 07.11.2017

SUBRAMANYAM, K., FRANK, C. E., & GALLI, D. F. (2017, March 1). Keyloggers: The Overlooked Threat to Computer Security. Retrieved from http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html Erişim Tarihi: 01.01.2017

Symantec. (2012, August 16). The Shamoon Attacks. Retrieved from https://www.symantec.com/connect/blogs/shamoon-attacks Erişim Tarihi: 09.11.2017

TAEK. (1995). TAEK 1995 Çalışma Raporu. Retrieved from http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/29/024/29024451.pdf Erişim Tarihi: 26.11.2017

TAEK. (2009). Nükleer Güvenlik Dairesi. Retrieved from http://www.taek.gov.tr/kurumsal/birimler/daire-baskanliklari/nukleer-guvenlik-dairesi-ngd.html Erişim Tarihi: 26.11.2017

TAEK. (2010a). Nükleer Düzenleme Kurumu İddiası - Taek Web. Retrieved from http://www.taek.gov.tr/nukleer-enerji-ve-nukleer-reaktorler/632-turkiyede-nukleer-alanda-bir-duzenleyici-kurum-var-midir-nukleer-enerji-ile-ilgili-duzenlemeler-hangi-kanunda-yer-almaktadir Erişim Tarihi: 26.11.2017

TAEK. (2010b). TR-2 Research Reactor Operation Unit. Retrieved from http://www.taek.gov.tr/en/institutional/affiliates/cekmece-nuclear-research-and-training-center/348-nuclear-technology-division/869-reactor-operation-unit.html Erişim Tarihi: 26.11.2017

TAEK. (2010c). Türkiye'de Nükleer Alanda Bir Düzenleyici Kurum Var mıdır? Nükleer Enerji ile İlgili Düzenlemeler Hangi Kanunda Yer Almaktadır? Retrieved from http://www.taek.gov.tr/nukleer-enerji-ve-nukleer-reaktorler/632-turkiyede-nukleer-alanda-bir-duzenleyici-kurum-var-midir-nukleer-enerji-ile-ilgili-duzenlemeler-hangi-kanunda-yer-almaktadir Erişim Tarihi: 30.10.2017

TAEK. (2016). A FULL REPORT TO THE 7 TH REVIEW MEETING OF CONVENTION ON NUCLEAR SAFETY.

TAEK. (2017a). Hizmetten Çıkarma Atıkları. Retrieved from http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/168-nukleer-atiklar/454-hizmetten-cikarma-atiklari.html Erişim Tarihi: 10.10.2017

TAEK. (2017b). Kullanılmış Nükleer Yakıtların Depolanması. Retrieved from http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/168-nukleer-atiklar/453-kullanlm-nuekleer-yaktlarn-depolanmas.html Erişim Tarihi: 11.10.2017

TAEK. (2017c). Kullanılmış Yakıtların Yeniden İşlenmesi. Retrieved from http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/168-nukleer-atiklar/452-kullanilmis-yakitlarin-yeniden-islenmesi.html Erişim Tarihi: 12.10.2017

TAEK. (2017d). Nükleer Reaktör Atıkları. Retrieved from http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/168-nukleer-atiklar/450-nukleer-reaktor-atiklari.html Erişim Tarihi: 11.10.2017

TAEK. (2017e). Nükleer Yakıt Çevrimi. Retrieved from http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/166-gunumuzde-nukleer-enerji-rapor/437-bolum-03-nukleer-yakit-cevrimi.html Erişim Tarihi: 14.09.2017

TAEK. (2017f). RESA - Radyasyon Erken Uyarı Sistemi Ağı. Retrieved from http://www.taek.gov.tr/radyasyon-izleme/radyasyon-erken-uyari-sistemi-agi-resa.html Erişim Tarihi: 26.11.2017

TAEK. (2017g). Sarayköy Nükleer Araştırma ve Eğitim Merkezi. Retrieved from http://www.taek.gov.tr/kurumsal/birimler/bagli-kuruluslar/sanaem.html Erişim Tarihi: 26.11.2017

TAEK. (2017h). TAEK. Retrieved from www.taek.gov.tr Erişim Tarihi: 05.05.2017

TAEK. (2017i). TAEK INES Ölçeği Tanıtım Sayfası. Retrieved from http://www.taek.gov.tr/acil-durumlar/kaza-ve-tehlike-durumu/372-uluslararasi-nukleer-olay-olcegi-ines.html Erişim Tarihi: 15.10.2017

TAEK. (n.d.). İKİTELLİ KAZASI TAEK RAPORU. Retrieved from http://www.taek.gov.tr/attachments/kazalar/ikitelli_tr.pdf Erişim Tarihi: 10.10.2017

TBMM. Nükleer Silahların Yayılmasının Önlenmesi Andlaşmasının Onaylanmasının Uygun Bulunduğu Hakkında Kanun, 2225 § (1979).

TBMM. TÜRKİYE ATOM ENERJİSİ KURUMU KANUNU, 2690 § (1982).

TBMM. NÜKLEER TESİSLERE LİSANS VERİLMESİNE İLİŞKİN TÜZÜK, Tüzük No: 2765 § (1983).

TBMM. ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN, 3154 ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN § Madde 10/D (1985).

TBMM. İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUN, 5651 § (2007).

TBMM. AFET VE ACİL DURUM YÖNETİMİ BAŞKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN, 5902 § (2009).

TBMM. TÜRKİYE CUMHURİYETİ HÜKÜMETİ İLE RUSYA FEDERASYONU HÜKÜMETİ ARASINDA TÜRKİYE CUMHURİYETİNDE AKKUYU SAHASINDA BİR NÜKLEER GÜÇ SANTRALİNİN TESİSİNE VE İŞLETİMİNE DAİR İŞBİRLİĞİNE İLİŞKİN ANLAŞMANIN ONAYLANMASININ UYGUN BULUNDUĞU HAKKINDA KANUN, 6007 § (2010).

TBMM. (2013, November 11). SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ.

TBMM. AİLE VE SOSYAL POLİTİKALAR BAKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN HÜKMÜNDE KARARNAME İLE BAZI KANUN VE KANUN HÜKMÜNDE KARARNAMELERDE DEĞİŞİKLİK YAPILMASINA DAİR KANUN, 6518 § (2014).

TBMM. SANAL ORTAMDA İŞLENEN SUÇLAR SÖZLEŞMESİNİN ONAYLANMASININ UYGUN BULUNDUĞUNA DAİR KANUN, 6533 § (2014).

TBMM. (2014c). Yazılı Soru Önergesi ve Cevabı.

TBMM. TÜRKİYE CUMHURİYETİ HÜKÜMETİ İLE JAPONYA HÜKÜMETİ ARASINDA TÜRKİYE CUMHURİYETİNDE NÜKLEER GÜÇ SANTRALLERİNİN VE NÜKLEER GÜÇ SANAYİSİNİN GELİŞTİRİLMESİ ALANINDA İŞBİRLİĞİNE İLİŞKİN ANLAŞMA İLE TÜRKİYE CUMHURİYETİNDE NÜKLEER GÜÇ SANTRALLERİNİN VE NÜKLEER GÜÇ SANAYİSİNİN GELİŞTİRİLMESİNE DAİR İŞBİRLİĞİ ZAPTININ ONAYLANMASININ UYGUN BULUNDUĞUNA DAİR KANUN, 6642 § (2015).

TBMM. (2015b, April 24). Nükleer Maddelerin Fiziksel Korunması Sözleşmesinde Değişiklik.

TDK. (2017). Türk Dil Kurumu Resmi İnternet Sayfası. Retrieved from http://www.tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.58b5b18dea3099.51909024 Erişim Tarihi: 09.03.2017

TDK Sözlük, S. (2017). TDK Sözlük “Siber.” Retrieved from http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.58be8e3d5d1816.12859374 Erişim Tarihi:28.02.2017

Techopedia. (2017). Exploit Definition. Retrieved from https://www.techopedia.com/definition/4275/exploit Erişim Tarihi: 05.11.2017

Techopedia. (n.d.). Masquerade. Retrieved from https://www.techopedia.com/definition/4020/masquerade-attack Erişim Tarihi: 02.03.2017

TheGuardian. (2007, September 16). Orchard Was Israeli raid a dry run for attack on Iran? Retrieved from https://www.theguardian.com/world/2007/sep/16/iran.israel Erişim Tarihi: 09.11.2017

TheGuardian. (2014). South Korea NPP Cyber Attack Hack. Retrieved from https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack Erişim Tarihi: 10.03.2017

TİFTİKÇİ, M. (2005). Türk Hukukunda Tehlike Sorumluluklarının Genel Kural ile Duzenlenmesi Sorunu. Yetkin Yayıncılık.

TOMBAKOĞLU, M., ERGÜN, Ş., ATAK, H., ÇELİKTEN, O. Ş., DUMAN, V., KAYRIN, K., … BAYRAKTAR, B. N. (2011). Nükleer Enerji Raporu. ANKARA.

TrendMicro. (2016). Malware Discovered in German Nuclear Power Plant. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant Erişim Tarihi: 04.09.2017

TROMPARENT, P. (2012). French Cyberdefence Policy - 2012 4th International Conference on Cyber Confl ict. NATO CCD COE Publications.

TSK. (2017, November 10). TSK Siber Savunma Merkezi Projesi. Retrieved from http://www.tsk.tr/TSKdanHaberler/Haber_234 Erişim Tarihi: 10.11.2017

@TSKGnkur. (2017, July 12). Sisamer Twitter. Retrieved from https://twitter.com/TSKGnkur/status/885056765703933952 Erişim Tarihi: 10.11.2017

TÜBİTAK. (2013). Siber Saldırılara Karşı Yerli Savunma Aracı. Retrieved from http://www.tubitak.gov.tr/tr/haber/siber-saldirilara-karsi-yerli-savunma-araci-gelistirildi Erişim Tarihi: 05.11.2017

TÜBİTAK. (2014). Siber Güvenlik Tatbikatları. Retrieved from http://sge.bilgem.tubitak.gov.tr/tr/siber-guvenlik-tatbikatlari Erişim Tarihi: 10.11.2017

TÜBİTAK. (2017a). BİLGEM tarihçe. Retrieved from http://bilgem.tubitak.gov.tr/tr/kurumsal/biz-kimiz Erişim Tarihi: 10.11.2017

TÜBİTAK. (2017b). SGE Tarihçe Tübitak. Retrieved from http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce Erişim Tarihi: 10.11.2017

TÜBİTAK. (2017c). Tübitak kronoloji. Retrieved from http://bilgem.tubitak.gov.tr/tr/kurumsal/kronoloji Erişim Tarihi: 10.11.2017

TÜBİTAK. (2017d). TÜBİTAK Tarihçe. Retrieved from http://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce Erişim Tarihi: 29.101.2017

TÜBİTAK. (n.d.). Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı.

UAEA. (1988). The Radiological Accident In Goiania, Brazil (No. 815). Vienna: UAEA.

UAEA. (1992). INSAG-7 The Chernobyl Accident: Updating fo INSAG-1 (No. STI/PUB/913). Vienna: UAEA.

UAEA. (1996). Defence in Depth in Nuclear Safety.

UAEA. (1998a). Classification of Uranium Reserves/Resources -UAEA - TECDOC 1035 - ISSN 1011-4289. UAEA.

UAEA. (1998b). The Atlas of Caesium-137 Contamination of Europe after the Chernobyl Accident.

UAEA. (1999). On-site disposal as a decommissioning strategy - UAEA-TECDOC-1124.

UAEA. (2002). THE RADIOLOGICAL ACCIDENT IN ISTANBUL (No. 1102). UAEA.

UAEA. (2005). Management of high enriched uranium for peaceful purposes: Status and trends UAEA TECDOC 1452. UAEA.

UAEA. (2006). Environmental Consequences of the Chernobyl Accident and their Remediation: Twenty Years of Experience (No. 1239). Vienna: UAEA.

UAEA. (2007). UAEA Safety Glossary - Terminology Used in Nuclear Safety and Radiation Protection. UAEA STI/PUB/1290.

UAEA. (2008a). Nuclear Security Culture.

UAEA. (2008b). Preventive and Protective Measures against Insider Threats - UAEA Implementing Guides STI/PUB/1359. UAEA.

UAEA. (2009a). Development, Use and Maintenance of the Design Basis Threat.

UAEA. (2009b). Nuclear Fuel Cycle Information System. UAEA.

UAEA. (2010a). Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran (No. GOV/2010/62). Viyana: UAEA.

UAEA. (2010b). Licensing Process for Nuclear Installations - Specific Safety Guide No.SSG-12 -STI/PUB/1468.

UAEA. (2010c). The Interface Between Safety and Security at Nuclear Power Plants - INSAG-24 (No. STI/PUB/1472). Vienna: UAEA.

UAEA. (2010d). Turkey - UAEA Publication. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/CNPP2010_CD/countryprofiles/Turkey/CNPP2010Turkey.htm Erişim Tarihi: 26.11.2017

UAEA. (2012). Effi cient Water Management in Water Cooled Reactors No NP-T-2.6. UAEA.

UAEA. (2013a). Decommissioning and Remediation after a Nuclear Accident (No. IEM/4). Vienna: UAEA.

UAEA. (2013b). Objective and Essential Elements of a State's Nuclear Security Regime.

UAEA. (2014a). Decommissioning of Facilities General Safety Req Part 6 - STI/PUB/1652. UAEA.

UAEA. (2014b). Experiences and Lessons Learned Worldwide in the Cleanup and Decommissioning of Nuclear Facilities in the Aftermath of Accidents (No. 1644). Vienna.

UAEA. (2015). The Fukushima Daiichi Accident Report (No. 1710). Vienna: UAEA.

UAEA. (2016a). CPPNM Status. Retrieved from https://www.iaea.org/Publications/Documents/Conventions/cppnm_status.pdf Erişim Tarihi: 01.11.2017

UAEA. (2016b). Nuclear Power Reactors in the World. Viyana: UAEA.

UAEA. (2017a). Goiania's legacy two decades. Retrieved from https://www.iaea.org/newscenter/news/goi%C3%A2nia%C2%B4s-legacy-two-decades Erişim Tarihi: 25.11.2017

UAEA. (2017b). UAEA - Power Reactor Information System (PRIS). Retrieved from https://www.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=US Erişim Tarihi: 25.07.2017

UAEA. (2017c). UAEA Nuclear Security and Safety Definition. Retrieved from http://www-ns.iaea.org/standards/concepts-terms.asp Erişim Tarihi: 03.11.2017

UAEA. (2017d). UAEA Web Sitesi. Retrieved from www.iaea.org Erişim Tarihi: 04.05.2017

UAEA, & OECD NEA. (n.d.). The International Nuclear and Radiological Event Scale.

UCAEL, O. (2015). Nükleer Enerji ve Sinop. Salmat Basım Yay. ANKARA.

UDHB. (2013, June 20). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.

UDHB. (2016). 2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı.

Ulakbim. (2010). Ulakbim - Ulak-CSIRT. Retrieved from http://csirt.ulakbim.gov.tr/

UN. (2017a). Cyberwarfare. Retrieved from http://unterm.un.org/UNTERM/Display/record/UNHQ/NA?OriginalId=bfde24673f1b1f6e85256afd006732a3 Erişim Tarihi: 28.02.2017

UN, B. (2017b). Birleşmiş Milletler. Retrieved from www.un.org

US-CERT. (2017). National Cybersecurity and Communications Integration. Retrieved from https://www.us-cert.gov/nccic Erişim Tarihi: 14.10.2017

US-DoD. (2011). DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE.

US-DoE. (2012). Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex (No. DOE/IG-0868). ABD Enerji Bakanlığı.

US-GOV. (1996, July 15). CRITICAL INFRASTRUCTURE PROTECTION.

VirusBlokAda. (2010). Stuxnet Ortaya Çıkış. Retrieved from http://www.anti-virus.by/en/tempo.shtml Erişim Tarihi: 08.11.2017

WashingtonPost. (2013). 'Black budget' summary details U.S. spy network's successes, failures and objectives. Retrieved from https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?utm_term=.cf686da3106e Erişim Tarihi: 10.10.2017

Webrazzi. (2017). 2016-2019 Eylem Planı Tarih. Retrieved from https://webrazzi.com/2016/09/09/bugun-aciklanan-ulusal-e-devlet-ve-siber-

guvenlik-strateji-ve-eylem-planlarinda-hangi-hedefler-var/ Erişim Tarihi: 20.06.2017

WEINER, T. (2012). “Revolution”. Enemies a history of the FBI. New York: Random House.

WEST-BROWN, M. J., STIKVOORT, D., KOSSAKOWSKI, K.-P., KILLCRECE, G., RUEFLE, R., & ZAJICEK, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University Software Engineering Institute Pittsburgh, PA 15213-3890.

White House, T. (2003). THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003.

White House, T. (2013a). Presidential Policy Directive -- Critical Infrastructure Security and Resilience.

White House, T. (2013b). Presidential Policy Directive -- Critical Infrastructure Security and Resilience PRESIDENTIAL POLICY DIRECTIVE/PPD-21 The White House Office of the Press Secretary For Immediate Release.

WILLIAM, S., & BROWN, L. (2015). Computer Security Principles and Practice Third Edition. University of New South Wales, Australian Defence Force Academy.

Wired. (2015, August 1). A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. Retrieved from https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ Erişim Tarihi: 01.10.2017

Wise-Uranium. (2017, May 6). World Nuclear Fuel Facilities. Retrieved from http://www.wise-uranium.org/efac.html Erişim Tarihi: 09.11.2017

WNA. (2015). Uranium Enrichment. Retrieved from http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/conversion-enrichment-and-fabrication/uranium-enrichment.aspx Erişim Tarihi: 29.10.2017

WNA. (2017a). Nuclear Power in Armenia. Retrieved from http://www.world-nuclear.org/information-library/country-profiles/countries-a-f/armenia.aspx Erişim Tarihi: 10.07.2017

WNA. (2017b). Nuclear Power in Bulgaria. Retrieved from http://www.world-nuclear.org/information-library/country-profiles/countries-a-f/bulgaria.aspx Erişim Tarihi: 10.08.2017

WNA. (2017c). Nuclear Power in Russia. Retrieved from http://www.world-nuclear.org/information-library/country-profiles/countries-o-s/russia-nuclear-power.aspx#.UZEvKRx8dUo Erişim Tarihi: 11.12.2017

WNA. (2017d). World Nuclear Association - Reactor Databese. Retrieved from http://www.world-nuclear.org/information-library/facts-and-figures/reactor-database.aspx? Erişim Tarihi: 29.10.2017

WNA. (2017e). World Nuclear Performance Report - World Nuclear Association 2017.

YAZICIOĞLU, Y. (1997). Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları. İstanbul: Alfa Yayınevi.

YILMAZ, E. N., ULUS, H. İ., & GÖNEN, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. Bilişim Teknolojileri Dergisi, 8(133).

YnetNews. (2011, April 28). UAEA: Syria tried to build nuclear reactor - orchard. Retrieved from https://www.ynetnews.com/articles/0,7340,L-4062001,00.html Erişim Tarihi: 09.11.2017

ZARARSIZ, S. (2005). URANYUM.

ÖZGEÇMİŞ

I. Bireysel Bilgiler

Adı: : Abdullah

Soyadı: : GENÇAY

Doğum Yeri ve Tarihi : Tokat/Reşadiye 02/06/1983

Uyruğu : Türk

Medeni Durumu : Evli

Askerlik Durumu : 327 KSD Jandarma

İletişim Adresi ve Telefonu : abdullahgencay@gmail.com, Emniyet Genel Müdürlüğü Haberleşme Daire Başkanlığı, 05055447527,

II. Eğitimi

(2014- ….) Ankara Üniversitesi Adli Bilimler Enstitüsü Disiplinlerarası Adli Bilimler Anabilim Dalı Fizik İncelemeler ve Kriminalistik Yüksek Lisans Eğitimi (Tezli),

(2001-2005) Ankara Üniversitesi, Eğitim Bilimleri Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Lisans Eğitimi

(2001-2005) Polis Akademisi, Güvenlik Bilimleri Fakültesi, Lisans Eğitimi,

(1998-2001) Ankara Polis Koleji, Lise Eğitimi

Yabancı Dili: İngilizce

III. Ünvanları

-

IV. Mesleki Deneyimi

(2013-…..) – Emniyet Genel Müdürlüğü

(2005-2013) – İstanbul Emniyet Müdürlüğü

V. Üye Olduğu Bilimsel Kuruluşlar

-

VI. Bilimsel İlgi Alanları

-

VII. Bilimsel Etkinlikleri

1. ODTÜ Mezunları Derneği Kritik Altyapılar, Panelist, 8 Nisan 2016, Ankara

2. LOCARD Global Cyber Security Summit, Konuşmacı, 21 Mayıs 2016, İstanbul

VIII. Diğer Bilgiler

Katıldığı Kurslar

1. Kent Güvenliği ve Yönetimi Semineri 15-17 Mart 2011, Ankara
2. TCP/IP Eğitimi 11-15 Kasım 2013, Ankara
3. Kerticide Tehice Hacker Eğitimi 20-24 Ekim 2014, Ankara
4. Malt ego Açık Kaynak Eğitimi 7-8 Şubat 2015, Ankara
5. National Workshop on Evaluation of Nuclear Security Plan 2-6 Mart 2015, Ankara
6. Temel Adli Bilişim 11-23 Mayıs 2015, Ankara
7. Avrasya Siber Suç Soruşturmaları 3-7 Ağustos 2015, İstanbul
8. Regional Training Course on Information Computer Security Advanced for Nuclear Security 19-23 Ekim 2015, Karlsruhe/Almanya
9. Online Undercover Eğitimi 6-10 Haziran 2016, Ankara