Adli Tıp Bülteni, 2019; 24(3): 252-261

Adli Tıp Bülteni
The Bulletin of Legal Medicine

www.adlitipbulteni.com

DERLEME / REVIEW

Türkiye'de Nükleer Siber Emniyet ve Nükleer Güvenlik

Nuclear Cyber Security and Nuclear Safety at Turkey

Abdullah Gençay*, Nergis Cantürk, Sait Özsoy

Öz

Siber kavramı son on yılda ülkemiz kurumsal hayatına olumlu ve olumsuz yönleriyle birlikte hızlı ve etkin bir şekilde giriş yapmıştır. Nükleer alanda da hızlı girişim ve gelişmeler yaşamakta olan ülkemizde nükleer siber emniyetin sağlanabilmesi önemlidir. Siber alanda ve nükleer alanda yeterliliğe sahip uzmanların hem düzenleyici ve denetleyici kuruluşlarda hem de nükleer tesis işletmecisi kuruluşlar bünyesinde bulunması gereklidir. Nükleer siber emniyetin sağlanması sürecinde yapılacak hataların yaratacağı kalıcı hasar riski, ülkelere bu alanda emekleme süreci yaşama fırsatı tanımamaktadır. Bu sebeple nükleer tesis kurmayı/işletmeyi hedefleyen ülkemizde nükleer siber emniyetle yaşamanın öğrenilmesi, bu alanın risklerini değerlendirme ve vakit kaybetmeden olası risklere yönelik önlemlerin alınması gerekmektedir.

Anahtar Kelimeler: Siber; Nükleer Siber Emniyet; Nükleer Güvenlik; Nükleer Tesis; Nükleer Siber Risk.

Abstract

In the last decade, the concept of cyber has entered the institutional life of our country quickly and efficiently with its positive and negative aspects. It's important that to provide nuclear cyber security in our country, which is experiencing rapid actions and developments in the nuclear field. It requires experts in cyber and nuclear field to be in both national authority agencies and nuclear facility operators. The risk of permanent damage caused by mistakes in the process of providing nuclear cyber security does not give countries the chance to experience the process of crawling in this field. For this reason, it is necessary to learn how to live with nuclear cyber security in our country which aims to build/operate a nuclear facility, to evaluate the risks of this field and to take measures for these risks without wasting time.

Keywords: Cyber; Nuclear Cyber Security; Nuclear Safety; Nuclear Facility; Nuclear Cyber Risk

DOI: 10.17986/blm.2019250196

Abdullah Gençay: MSc., Emniyet Genel Müdürlüğü Haberleşme Daire Başkanlığı, Ankara
Eposta: abdullahgencay@gmail.com
ORCID iD: https://orcid.org/0000-0002-4137-192X

Nergis Cantürk: Prof. Dr., Ankara Üniversitesi Adli Bilimler Enstitüsü, Ankara
Eposta: nergiscanturk@yahoo.com
ORCID iD: https://orcid.org/0000-0001-8739-0723

Sait Özsoy: Doç. Dr., Sağlık Bilimleri Üniversitesi Gülhane Tıp Fakültesi Adli Tıp Anabilim Dalı, Ankara
Eposta: drsaitozsoy71@gmail.com
ORCID iD: https://orcid.org/0000-0002-0851-5733

Bildirimler/ Acknowledgement
Yazarlar bu makale ile ilgili herhangi bir çıkar çatışması bildirmemişlerdir.

Finansal Destek/Support Resources
Yazarlar bu makale ile ilgili herhangi bir finansal destek bildirmemişlerdir.
The authors declare that they have no conflict of interests regarding content of this article.
The Authors report no financial support regarding content of this article.
*Sorumlu Yazar/ Corresponding Author:
**Bu makale "GENCAY A (2018). Siber Olaylara Müdahale Konusunda Amerika Birleşik Devletleri, Fransa ve Türkiye'nin İdari Yapılarının İncelenmesi – Nükleer Santral Örneği, Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Disiplinlerarası Adli Bilimler." Yüksek Lisans Tezinden üretilmiştir.

Geliş: 15.01.2019
Düzeltme: 31.01.2019
Kabul: 13.02.2019

p-ISSN: 1300-865X
e-ISSN: 2149-4533

Giriş

Bilgi ve iletişim teknolojileri, bilgisayar ağlarının iletişim amacıyla kullanılmaya başlandığı 1960'lı yıllardan günümüze, insan yaşamına sağladığı faydalar kadar kişisel ve kurumsal bilgi güvenliğine yönelik tehdit aracı olarak da kullanılmaktadır. 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 (1,2). 2018 yılı itibariyle yaklaşık 5,13 milyar mobil telefon kullanıcısının bulunduğu dünyada siber alan her an her yere ulaşmıştır. Bununla birlikte siber evren, siber terörizm, siber çeteler, siber espiyonaj, siber suç, siber istihbarat, nükleer siber emniyet gibi birçok "siber" ön ekli kavram hayatımıza girmiştir. Sınırları net bir şekilde çizilemeyen, suçun asimetrik olarak işlenebildiği bu sanal dünyada güvenli kalma ihtiyacı her geçen gün artmaktadır. Bireysel, grupsal ya da zaman zaman devlet destekli de olduğu iddia edilen siber suç organizasyonları suçtan zarar gören mağdurlar listesine kısa sürede devletleri de eklemişlerdir (3).

Bu çalışmada Nükleer Tesislerin Siber Emniyetinin sağlanması sürecinde alınmış olması gereken önlemlerin vurgulanması amaçlanmıştır.

Siber Emniyet, Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB) tarafından yayımlanan 2016-2019

Siber Saldırı Araçları:	Saldırı Yöntemleri:	Siber Saldırıların Muhtemel Sonuçları:
Virüs (Virus)	Hizmet Dışı Bırakma (Denial of Service - DOS)	Dijital Verinin Çalınması
Truva Atı (Trojen)	Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service - DDOS)	Dijital Verinin Eksilmesi
Solucan (Worm)	Oltalama/Yemleme (Phishing)	Dijital Verinin Değiştirilmesi
Klavye Kaydedici (Keylogger)	Sosyal Mühendislik (Social Engineering)	Dijital Verinin Kullanılamaz Hale Getirilmesi
Casus Yazılım (Spyware)	Arka kapı (Backdoor)	Dijital Verinin Gizliliğinin İhlali
Botnet	Kabloya saplama yapma (Wire Tapping)	Sistemin Durması
Exploit	Yerine Geçme (Masquerading)	Sistemin Kesintiye Uğraması
Rootkit	Hukuka Aykırı İçerik Sunulması	
Sniffer (Koklayıcı)	Salam Tekniği (Salami Techniques)	
	Çöpe Dalma (Scavenging)	
	Veri Aldatmacası (Data Diddling)	
	Tarama (Scanning)	

Şekil 1. Siber saldırı araçları, siber saldırı yöntemleri ve siber saldırıların muhtemel sonuçları (50–53)

Tablo 1. Ülkelerin Nükleer Enerji Üretiminin Tüketimdeki Payı, Aktif Reaktör Sayısı ve Nükleer Enerji Üretim Gücü (7,9,54)

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

Ulusal Siber Güvenlik Stratejisi Belgesinde "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber emniyet olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber emniyet olayı öncesi durumlarına geri döndürülmesi" olarak tanımlanmıştır.

Siber Saldırı, yetkisiz olarak siber ortamdaki verinin değiştirilmesi, çalınması, erişimin kısıtlanması/kesilmesi durumları olarak tanımlanmaktadır (4). Yaygın rastlanan Siber saldırı araçları, siber saldırı yöntemleri ve siber saldırıların muhtemel sonuçları Şekil 1'de gösterilmiştir.

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 girerek parçalanması ve oluşan yüksek ısının kullanılmasıyla enerji üretimi gerçekleşir (5).

Nükleer enerji üretiminin ülkelerin yıllık öz tüketimine katkısı değerlendirildiğinde 2018 yılında dünyada 13 ülke yıllık enerji 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. Yıllık enerji ihtiyacının %25'ten fazlasını kendi ürettiği nükleer enerjiden karşılayan 13 ülke ve ABD'nin enerji üretimlerindeki nükleer enerjinin oranı, aktif reaktör sayıları ve üretim güçleri Tablo 1'de sunulmuştur (6,7).

Uranyum, nükleer güç santrallerinde enerji üretiminde hammadde olarak kullanılmaktadır. 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 fisyonu (bir nötron ile parçalanması) sonucu ortaya çıkan enerjiyi elektriğe çeviren tesislerdir. U-235 çekirdekleri nötronlarla tepkimeye girmeleri sonucunda daha kararsız bir yapı elde edilir. Bu yeni çekirdeğin daha kararlı iki veya üç çekirdeğe bölünmesiyle de enerji açığa çıkar. Bu işlem esnasında açığa çıkan nötronların ortamda bulunan diğer U-235 çekirdekleriyle tepkimeye girmeleriyle birlikte sürekli bir üretim sağlanır. Bu tepkime süreci ***"Zincirleme Tepkime"*** olarak adlandırılır (5,8,9).

Uranyum yataklarında U-235 ve U-238 çekirdekleri bir arada bulunur. Doğadaki toplam uranyumun binde yedisi (%0,7) U-235 çekirdekleri iken binde dokuz yüz doksan üçü (%99,3) U-238 çekirdekleridir (9). Nükleer reaktörler yakıt olarak sıklıkla %0,7 ile % 3-5 arasında yoğunluğa sahip (U-235 açısından zenginleştirilmiş) uranyum U-235 çekirdeğini kullanmaktadır. Bu nedenle reaktörde kullanılacak Uranyumun öncelikle yoğunluk açısından zenginleştirilmesi gerekmektedir. Uranyum zenginleştirme işlemleri *Uranyum Zenginleştirme Tesislerinde* gerçekleştirilmektedir. Uranyum elementi U-235 çekirdeği zenginleştirme yoğunluğuna göre Tablo 2'de belirtildiği gibi Düşük ve Yüksek Seviye Zenginleştirilmiş Uranyum olarak ikiye ayrılmaktadır.

Tablo 2. Uranyum Elementinin Zenginleştirme Oranına Göre Kullanım Yerleri (55–57)

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 uranyum zenginleştirme tesisi işleten ülkeler olup tesis sayıları Tablo 3'te belirtilmiştir. Bu ülkelerden İsrail, Kuzey Kore ve İran Uranyum Zenginleştirme programlarını gizlilik içerisinde yürütmeleri nedeniyle kapasiteleri net olarak bilinmemektedir (10).

Tablo 3. Dünya'daki Başlıca Uranyum Zenginleştiren Ülkeler* ve Kapasiteleri (11,58,59)

Sıra No	**Ülke**	**Tesis Adedi**	**Kapasite (1000 SWU/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.

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.

Nükleer Reaktörler, 1950'li yıllardan beri zenginleştirilmiş uranyum çekirdeklerinin kullanılarak elektrik üretimi sağlayan tesislerdir. Nisan 2017 yılı itibariyle dünyada 30 ülkede toplam 449 aktif, 15 ülkede toplam 60 inşaa haline reaktör bulunmaktadır (11) (Tablo 4). ***Nükleer santraller*** ise nükleer enerjiyle açığa çıkan enerjiyi elektrik enerjisine çeviren, şebeke dağıtımını başlatan ve bu amaçlara dönük alt tesisleri barındıran enerji üretim ve dağıtım tesisleridir.

Nükleer reaktör (buhar kazanı, reaktör kabı), buhar türbini, elektrik jeneratörü, yoğuşturucu, atık birimleri ve diğer güvenlik ve idari birimlerden oluştur. 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. Reaktörlerin güçlerinin toplamı doğrultusunda bir nükleer santralin toplam gücü hesaplanır.

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 (12,13).

Ülkenin yetkili kurumu tarafından bir nükleer santralin tüm süreçlerini -nükleer sit alanında 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 her basamakta sorumluluk sahibidir. Ülkenin yetkili kurumu nükleer güvenlik ve emniyetle ilgili kurucunun faaliyetlerini denetleme, test sonuçlarını değerlendirme testleri tekrarlatma, yaptırım ve lisanslama iptali gibi haklarını kendinde saklı tutar (14).

Ülkemizde 13 Temmuz 1982 tarih ve 2690 sayılı Türkiye Atom Enerjisi Kanunu ile ***Türkiye Atom Enerjisi Kurumu*** ülkemizdeki ***yetkili kurum*** olarak belirlenmiştir. Ayrıca ülkemizde nükleer bir tesisin işletmeye alınabilmesi için kurucunun almasına ihtiyaç duyulan lisanslar 1983 tarihli 2765 sayılı 'Nükleer Tesislere Lisans Verilmesine İlişkin Tüzük' 3 başlıkta toplanmıştır:

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

Mersin ili Silifke ilçesinin batısında bulunan Akkuyu bölgesine Nükleer Güç Santrali (NGS) inşa edilebilmesi için 1976 yılında Yer Lisansı verilmiştir. Bu bölgede bir NGS inşa edilmesi için Akkuyu NGS Elektrik Üretim A.Ş. isimli şirkete Nisan 2018 tarihi itibariyle inşaat lisansı (Kurucu) verilmiştir (15,16). Ayrıca 2015 yılında Türk Hükümeti ile Japonya Hükümeti arasında imzalanan 6642 sayılı kanunla nükleer tesis inşaa ve nükleer teknoloji paylaşımı detayları içeren anlaşmada Sinop iline ya da şartların uygunluğu ölçüsünde başka bir alana ülkemizdeki 2. NGS'nin kurulması resmileşmiştir. Bu santral ile ilgili Sinop ilinde belirlenen sit alanı için yer lisansı alınması çalışmaları devam etmektedir.

Tablo 4. Nükleer Reaktör Sayıları (54)

		Çalışan Reaktörler			
Sıra No	**Ülke**	**Reaktör Sayısı**	**Üretilen Güç MWe**	**İnşa Halindeki Reaktör Sayısı**	**Kapatılan Reaktör Sayısı**
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**	

Bir NGS'nin yapım süresi tüm proje dönemi düşünüldüğünde 10-12 yıl civarındadır. Proje maliyeti ise reaktör tipi, gücü, yeri, yasal ve yerel koşullar gibi birçok detaya bağlıdır.

Nükleer santraller ortalama 40-60 yıl arasında bir çalışma süresi öngörülerek tasarlanmaktadır. Bu santrallerin ilk kurulum maliyetleri birçok faktöre göre değişmekle birlikte reaktör başına 2 milyardan başlayıp 9 milyar dolara kadar çıkmaktadır. Ülkemizde kurulumu gerçekleşecek Akkuyu NGS ile ilgili 2017 yılında yapılan bir çalışma ilk yatırım maliyeti 33 Milyon Dolar, İnşaat Maliyeti 13.9 milyar dolar, İşletme Maliyeti 6.1 milyar dolar ve hizmetten çıkarma maliyeti 147 milyon dolar olmak üzerek toplam maliyetinin 20.3 milyar dolar olduğu belirtilmektedir (17,18). ***Nükleer Hizmetten Çıkarma/ Faaliyet Durdurma/Kapatma***, lisans alımı esnasında dikkate alınması gereken önemli bir iş ve maliyet kalemidir. Santralin işletmede olduğu süre içerisinde hizmetten çıkarma sürecinin de planlanması gerekir. Hizmetten çıkarma ekonomik ve sosyal maliyeti yüksek bir işlemdir. İlk yatırım maliyetinin yaklaşık %10-20'sine karşılık gelmektedir (9,14,19,20).

Akkuyu NGS'nin 2020 yılında işletme süresi 2020-2083 arasını kapsayan 63 yıl olarak hesaplanmıştır.

Farklı isimlerle anılan hizmetten çıkarma işlemi 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. Radyoaktivitenin temizlenmesi, santralin sökülmesi, radyoaktivite içeren her bir parçanın güvenli depolama alanlarına götürülmesini kapsar (21).

Hizmetten çıkarma maliyetleri:

- 1998 değeriyle ABD'de reaktör başına 325 milyon Amerikan Doları
- Fransa'da 70 MW'lık bir santralin maliyeti 24 milyon Euro planlanmışken işlemler başladıktan sonra 480 milyon Euro (Brennilis NGS).
- Almanya'da 100 MW'lık bir santralin hizmetten çıkarma maliyeti 143 milyon Euro üstü (Niederaichbach).
- İngiltere'deki 32 MW'lık bir santralin hizmetten çıkarma maliyeti 117 milyon Euro (Windscale) olduğu bildirilmektedir (14,22–24).

Nükleer Emniyet terimi ile Nükleer Güvenlik terimi sıklıkla anlamsal olarak birbirleriyle karıştırılmaktadır (25). ***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. Nükleer 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. ***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 (26). Ortak noktaları insan hayatı ve çevrenin korunması olan bu iki kavramdan; emniyet kötü niyetli eylemlerle ilgili, gizli ve tehdit temelli iken güvenlik şeffaf, olasılıklı güvenlik analizinin kullanıldığı, açık faaliyetlerle ilgilidir. Emniyet ve güvenlikten sorumlu personeller farklı kişilerdir. Zaman zaman tesisin sağlıklı işletimi için bir araya gelseler de farklı geçmişe/uzmanlıklara sahip, farklı süreçlerle ilgilenen kişilerden oluşurlar (27). Emniyet atmosferi; düzenleyicisinden denetleyicisine, işletmecisinden çalışanına kadar geniş bir alanda nükleer emniyet kültürü oluşturmakla sağlanabilir.

Nükleer Emniyet Kültürü "nükleer güvenliği sağlamak, sürdürmek ve desteklemek için -bireylerin, kurum ve kuruluşların- karakteristik, tutum ve davranışları sağlama faaliyetleri" olarak tanımlanmaktadır. İnsanların, toplumun ve çevrenin radyasyonun zararlı etkilerinden korunması için oluşturulmasına ihtiyaç duyulan bu kültürün her bir çalışana kazandırılması önemlidir. Emniyet kültürünü benimsemiş çalışanların öncelikle kendisini sürekli olarak değerlendirmesi ve denetlemesi beklenir (28).

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 Rejiminin*** tam olarak sağlandığı ortam olarak kabul edilmektedir (29).

Derinlemesine Emniyet/Güvenlik, fiziksel korunma yapısıyla ilgili bir yaklaşımı ifade eder. Bu yaklaşım Emniyet ve Güvenlik alanlarının her ikisinde de kullanılır.

Bir güvenlik ya da emniyet duvarını/önlemini/metodunu ihlal eden kişinin başka biriyle karşılaşması ve amacına ulaşamaması varsayımı 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 risk boyutunun sınırların altında tutulması, büyük radyolojik sonuçları olan kazaların yaşanma ihtimalinin kabul edilebilir düzeyde düşük tutulması/olması sıralamasına uygun bir Derinlemesine Güvenlik/Emniyet yapısının oluşturulmuş olması beklenir (9,30).

Tasarıma Esas Tehdit devletin tehdit değerlendirmesi sonrasında fiziksel korunmanın geliştirilebilmesi için 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 hususlar bulunur. ***Köstebek,*** tesisle ilgili bazı yetkilere/bilgilere 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 çalışanlarının davranış analizini de gerekli bulmaktadır (31,32).

"Tasarıma Esas Tehdit" dokümanı nükleer tesisin inşası başlamadan önce belirlenmelidir. Bu sebeple doğru kurguda bir Nükleer Emniyet Rejiminin sağlanabilmesi, tesisin inşası süresinde önceden belirlenmiş güvenlik ilkelerine uygun atılacak sağlam adımlarla mümkün olmaktadır. Buna ek olarak her Nükleer Emniyet Rejiminin sağlıklı olması Nükleer Emniyet Kültürünün oluşturulması ve yaşatılmasıyla doğrudan ilişkilidir. Bu süreçte köstebekler önemli bir risk unsurudur. Bir olayın meydana gelmesi sonrasında yapılan soruşturmalarda çabuk fark edilen köstebekleri kaza öncesinde belirleyebilmek ya da önlemek oluşturulan emniyet rejiminin en önemli amaçlarından biridir. Doğru bir derinlemesine güvenlik/emniyet modelinin inşa edildiği bir tesiste, köstebeklerin saldırı için uygun ortamı bulamaması muhtemeldir (33).

Çalışanlar tarafından önemsiz gibi görünen pek çok 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 çalışan algısında normalleşen ihlaller özellikle işten çıkarılan çalışanların başarılı saldırılar gerçekleştirebileceği önemli problemlere dönüşebilir. 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 sızması ihtimali mevcuttur (28).

Nükleer Emniyet Kültürünün istenen seviyede sağlanamaması, köstebek tehdidine yeterince önlem alınmamış olması, ihtiyaç duyulan farkındalık seviyesine ulaşılamamış olması gibi durumlar birçok riski de beraberinde getirmektedir. Bu risklerle mücadelede ilk olarak ***sürekli olarak bir tehdit değerlendirmesi*** sürecinin yürütülmesi ve özellikle bu işten sorumlu ekibin emniyet kültürünü benimsemiş ve çalışma disiplini pozitif bireylerden oluşması, riskleri minimum seviyede tutacaktır. Ayrıca bir nükleer tesiste emniyetten sorumlu ekibin/personelin emniyet kültürünü, tesisin emniyet rejimini düzenli olarak denetlemesi gerekir. Ölçütlerin çok titiz çalışmalarla belirlenmesi gereken bu denetleme süreçlerinin süresinden, sıklığından ve denetleme esnasındaki katılığından taviz verilmeyecek şekilde yürütülmesi gerekir (28,32,34).

Nükleer Emniyet Kültürü açısından 1999 yılında İstanbul İkitelli'de yaşanan olay değerlendirildiğinde; 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 ile başlayan olaylar zincirinde lisans sahibi bir şirkete lisansın veriliş şekli, lisans verilmesi sürecinde işletilen prosedürlerin farkındalık seviyesine etkisi, denetleyici kurumun geri gönderme işlemi için lisans vermesine rağmen işlemin gerçekleşip gerçekleşmediğini denetlememiş olması gibi değerlendirilmesi gereken birçok husus ortaya çıkmaktadır (35).

2010 yılında yaşanan Stuxnet ismi verilen ve İran'ın uranyum zenginleştirme programını hedef alarak Natanz Uranyum Zenginleştirme tesisindeki 5000 civarında santrifüjün 1000 adedinin kullanılmaz hale geldiği bir siber saldırı yaşanmıştır. Hiçbir fiziksel (geleneksel) saldırı aracının kullanılmadığı bu saldırı hem bu yönüyle hem de verdiği zarar nedeniyle tüm dünyanın önemli derece ilgisini çekmiştir. Nükleer alan özelinde tüm dünyadaki fiziksel/siber güvenlik prosedürlerinin gözden geçirilmesine neden olmuştur. Radyasyona bağlı olarak görülen sağlık problemleri ile ilgili İran makamlarından hiçbir zaman kamuoyuna bilgi paylaşılmamış yaşananlar gizli tutulmuştur. Ancak Stuxnet ismi verilen bu zararlı yazılımın hazırlanma, yayılma, zarar verme şekilleri hangi bölgelere kadar yayıldığı gibi birçok detaylar büyük antivirüs yazılımlarının uzmanları tarafından aylarca in-

celenmiştir. Bu zararlı yazılım Natanz Uranyum Zenginleştirme Tesisindeki santrifüjlerin dönüş hızlarını yöneten donanımlara bulaşarak santrifüjlerin kullanılamaz hale gelmesine neden olmuştur.

Stuxnet olayı Nükleer Siber Emniyet Kültürü perspektifinden; zararlı bir yazılımın tesisin dış dünyaya kapalı bir ağ olan iç ağına bulaşması sürecinde varolan "USB disk kullanma(ma)" prosedürlerinin nasıl aşıldığı, düzenlenmesi gereken Düzenli Farkındalık Faaliyetlerinin düzenlenip düzenlenmediği, düzenlendi ise etkililik seviyesi, iç ağa bağlı donanımlara kullanılabilir USB portlarının neden kullanım dışı bırakılmadığı gibi değerlendirilmesi gereken birçok hususu ortaya çıkarmaktadır (36–38).

Nükleer Emniyet'in sağlanması sürecinde hayati bir role sahip olan ***Nükleer Siber*** *Emniyet,* nükleer enerjinin üretildiği, depolandığı ve kullanıldığı tesislerin yanı sıra nükleer maddenin taşınması sürecini de kapsayacak şekilde önleme, tespit ve yanıtlama faaliyetlerini içeren siber müdahale yöntemleridir.

Nükleer Siber Emniyet, ülkedeki birçok farklı kurumun birlikte, ayrı ayrı ve titiz çalışmalarla oluşturulması gereken çok katmanlı bir yapıya sahiptir. Bu katmanların tamamının doğru kurgulanmış, günümüz ihtiyaçlarına cevap verir nitelikte olması gerekmektedir. Yasal düzenlemelerin ülke mevzuatına ve alan ihtiyaçlarına uygun olarak hazırlanması sonrasında, idari uygulamaların aynı titizlikte hazırlanması önemlidir. Tüm bunların hazırlanması sürecinde hem kamu hem de özel sektörün birlikte çalışması risklerin net olarak ortaya konulabilmesi ve doğru çözümler üretilebilmesi için başvurulan genel kabul gören bir uluslararası yöntemdir (39).

Nükleer tesislere yapılacak siber saldırılar sonrasında yaşanmış en büyük olay olan Stuxnet ile Uluslararası haber kaynaklarındaki İran'ın Natanz Uranyum Zenginleştirme Tesisindeki 5000 santrifüjünün 1000 adedinin kullanılamaz duruma geldiğinin belirtildiği haberler ve UAEA'ın rutin hazırladığı envanter bilgisi raporları bu iddiaları doğrular niteliktedir (34,37,40,41). Nükleer santrallerde genel olarak ağların önemine göre farklı katmanlarda bulunması önemli bir emniyet adımı olarak görülse de saldırganların ulaşabildiği ağlardaki verileri elde ederek farklı amaçlarla kullanması ihtimali önemli bir risk olarak değerlendirilmelidir.

Stuxnet saldırısında kullanılamaz hale gelen 1000 santrifüjün yanında, 2014 yılında Almanya'daki bir çelik fabrikasına yapılan siber bir saldırı ile yüksek ısı fırınlarının kapanması engellenerek tesiste zarar oluşmasına neden olunmuş, 2007 yılında ABD'de bulundan Idaho Ulusal Laboratuvarlarında yapılan testte dizel bir jeneratör siber bir saldırıyla kullanılamaz hale getirilmiş, 2014 yılında Güney Kore'deki bir nükleer reaktör işletmecisi şirkete yapılan siber saldırı ile çalışan bilgilerinin yanında reaktörlerle ilgili bazı veriler saldırganlarca ele geçirilmiştir. Nükleer santrallere yapılacak siber saldırılarla ilgili olası zararlar perspektifinden bu olayların dikkatle değerlendirilmesi ve gerekli derslerin çıkarılarak önlem alınması önemli bir gerekliliktir (42–47).

Uluslararası Atom Enerjisi Ajansı'nın (UAEA) referans kılavuzuna göre bir nükleer tesise yönelik 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 (26).

Bir nükleer tesise yönelik siber saldırıya müdahale ya da bu saldırının engellenmesi süreci yetkin personel çalıştırıyor olmaktan, doğru kuruma doğru yetkiyi vermiş olmaya kadar geniş bir yelpazede kurumların ***sorumluluk payla***şımının değerlendirilmesi ve ülkemiz dinamiklerinin de göz önünde bulundurulduğu ideal yapının oluşturulması için önemli bir gerekliliktir. Olası saldırı ile radyasyonun olumsuz etkilerinin de gerçekleşmiş olması durumunda iyileştirme aşamalarında görev alacak ekipteki personel çeşitliliğinin önemli ölçüde artması, farklı alanlarda uzman personellerin yapacağı çalışmaların doğru koordinasyonu da ön planlama gerektirir (48).

Yasal düzenlemelerde özel sektörün deneyimlerinden faydalanılması söz konusu olabilir. Özellikle nükleer siber alanda, hem nükleer alanla ilgilenen hem siber alanla ilgilenen özel ve kamu temsilcilerinin bir araya gelerek çalışma yürütmeleri faydalı olacaktır.

Siber emniyet, nükleer tesis henüz proje aşamasındayken başlayan ve alandaki tüm radyoaktivitenin son bulmasına kadar devam eden en az 80 yıllık bir süre boyunca güvenliğin hiçbir zaman terk edilmediği bir yaşam döngüsü gerektirir. 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 (26).

Nükleer tesislerin işletilmesi sürecinde önemli bir farkındalık faaliyetinin 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 (49).

Sektörlerin geneline yayılmış olan emniyet ve güvenlik önlemlerinin alınması maliyeti yüksektir. Nükleer tesislerde güvenlik açığı olası olumsuz etkilerinin akut ve uzun dönemdeki büyüklüğü nedeniyle ülkedeki denetleme ve düzenleme yetkilerine sahip kuruma çok önemli bir sorumluluk yüklemektedir. Çünkü bu tesislerde meydana gelebilecek olayların bedelleri yıllar boyu ödenmeye devam edebilmektir.

Sonuç

Yukarıda belirtilen bilgiler ışığında bir nükleer tesiste aşağıda başlıklar halinde belirtilen nükleer siber emniyet önlemlerinin alınmış olması çok önemlidir:

- Siber emniyet politikasının hazırlanması (tesis işletmecisi tarafından),
- Siber emniyet politikasının denetlenmesi ve uygunluk verilmesi (yetkili otorite tarafından),
- Tesisin siber emniyetinin sağlanması ile ilgili yönetim modelinin oluşturulması ve bu modelin tesisin ana yönetimiyle olan bağının ortaya konulması,
- Siber Emniyet Ekibi kadrolarının belirlenmesi ve bu kadrolara önemli ön kabul aşamaları sonrasında istihdam sağlanması,
- Siber Emniyet Kültürü değerlendirme ve uygulama ekibinin oluşturulması (Bu ekibin siber emniyet ekibinden ayrı olması, tesisin tüm çalışanlarına dönük politikaları yürütmesi gerekecektir),
- Hem siber emniyet ekibi hem de siber emniyet kültürü değerlendirme ve uygulama ekiplerinin ayrı ayrı eğitim programlarının hazırlanması ve yetkili otorite tarafından bu eğitimlerin kontrolünün yapılması (yetkili otoritenin bir eğitim programının doğru değerlendirilmesinin sağlanabilmesi için bünyesinde uzman bulunmaması durumunda en az 2 farklı üniversitenin ilgili birimlerinden akademik destek alması),
- Siber Emniyet Planının hazırlanması, denetlenmesi ve uygulanması
- Diğer emniyet önlemlerinin siber emniyete ilişkin etki değerlendirmesinin yapılması (Örnek olarak tesiste bulunan bir kartlı geçiş sisteminin yetkilendirme yapısının ve kodlarının güvende olması, düzenli değiştirilmesi gibi önlemler alınması)
- Güvenlik ve Emniyet ekiplerince yapılacak değerlendirme çalışmalarında siber emniyet ekibinden de personel bulundurulmasının sağlanması,
- Tehdit değerlendirme çalışmalarının yapılması ve önlem paketlerinin hazırlanması (Bu çalışmalara siber emniyet, emniyet, güvenlik, siber emniyet kültürü gibi ekiplerin tamamının katılması/katkı sağlaması),
- Köstebek tehdidi plan ve politikasının hazırlanması ve düzenli olarak gözden geçirilmesi.

Nükleer Siber Emniyet Kültürü içerisinde 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 emniyet personeli, işletmeci kurum yöneticileri, tesis siber emniyet ekibi, tesis koruma görevlileri, tesis güvenlik ekibi vb.) detaylı ***eğitim, bilgilendirme, farkındalık arttırma*** faaliyetleri düzenlenmelidir. Bu faaliyetleri düzenlemek ve denetlemekle sorumlu kişiler tesis ve de kamu tarafından alanında uzman kişiler arasından seçilmelidir.

Kaynaklar

1. Cyber Word Meaning. URL: http://www.dictionary.com/browse/cyber?s=t. [Son Erişim Tarihi: 09.03.2017]
2. Türk Dil Kurumu Web Sitesi Sözlüğü Siber Kelimesi Sözlük Anlamı. URL: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.58be8e3d5d1816.12859374 [Son Erişim Tarihi: 09.03.2017]
3. We Are Social LTD. Web Sitesi 2018 Global Digital Report. URL: https://wearesocial.com/us/blog/2018/01/global-digital-report-2018 [Son Erişim Tarihi: 05.12.2018]
4. Janczewski LJ, Colarik AM. Cyber Warfare and Cyber Terrorism. London: IGI Global, 2008: p. 13-25.
5. Tombakoğlu M, Ergün Ş, Atak H, Çelikten OŞ, Duman V, Kayrın K, Tiftikçi A, Türkmen M, Ayhan H, Aksoy B, Ayanoğlu M, Güler A, Pınarbaşı B, Taş FB, Bayraktar BN. Nükleer Enerji Raporu. Ankara: TMMOB Fizik Mühendisleri Odası, 2011.
6. US Energy Information Administration US Energy Consumption. URL: https://www.eia.gov/energyexplained/?page=us_energy_home [Son Erişim Tarihi: 09.11.2017]
7. Nuclear Energy Institute Nurclear Energy Around the World. URL: https://www.nei.org/Knowledge-Center/Nuclear-Statistics/World-Statistics [Son Erişim Tarihi: 09.11.2017]
8. Elektrikport Ayda Nükleer Enerji URL: http://www.elektrikport.com/teknik-kutuphane/ayda-nukleer-enerji/4341#ad-image-0 [Son Erişim Tarihi: 20.08.2017]

9. Uranium Mining Overview. URL: http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/mining-of-uranium/uranium-mining-overview.aspx [Son Erişim Tarihi: 02.01.2018]
10. Management of high enriched uranium for peaceful purposes: Status and trends. Vienna: UAEA Publications, 2005.
11. Nuclear Energy Institute World Statistics Nurclear Energy Around the World. URL: https://www.nei.org/KnowledgeCenter/Nuclear-Statistics/World-Statistics [Erişim Tarihi: 09.11.2017]
12. United States Nuclear Regulatory Commission Pressurized Water Reactor Animation. URL: http://www.nrc.gov/reading-rm/basic-ref/students/animated-pwr.html [Son Erişim Tarihi: 11.08.2017]
13. Efficient Water Management in Water Cooled Reactors No NP-T-2.6. Vienna: UAEA Publications, 2012.
14. TAEK ve Nükleer Santral Lisanslama. http://www.taek.gov.tr/tr/2016-06-09-00-43-55/44-akkuyu-nukleer-guc-santrali/695-taek-ve-nukleer-santral-lisanslama.html [Son Erişim Tarihi: 05.07.2017]
15. AkkuyuNPP Akkuyu Tarihçe. URL: http://www.akkunpp.com/projenin-tarihcesi [Son Erişim Tarihi: 18.10.2017]
16. AkkuyuNPP Sınırlı Çalışma İzni. URL: http://www.akkunpp.com/akkuyu-nukleer-as-sinirli-calisma-iznini-aldi/update [Son Erişim Tarihi: 21.10.2017]
17. Toprak S, Dal S. Akkuyu Nuclear Power Plant Cost & Benefits Analysis. Energy Policy Turkey 2017. p. 85-91.
18. Union of Concerned Scienstists Websitesi Cheap Dreams, expensive realities. URL: https://www.ucsusa.org/nuclear-power/cost-nuclear-power#.XALmZdszaUk [Son Erişim Tarihi: 02.12.2018]
19. Hizmetten Çıkarma (Decommissioning) Atıkları URL: http://www.taek.gov.tr/tr/2016-06-09-00-43-55/161-nukleer-atiklar/1062-hizmetten-cikarma-atiklari.html [Son Erişim Tarihi: 09.12.2017]
20. Decommissioning of Facilities General Safety Req Part 6. Vienna: UAEA Publications, 2014.
21. Licensing Process for Nuclear Installations Specific Safety Guide No.SSG-12 Vienna: UAEA Publications, 2010.
22. US Nuclear Regulatory Commission Decommissioning. URL: https://public-blog.nrc-gateway.gov/category/decommissioning-2/ [Son Erişim Tarihi: 28.10.2017]
23. Perrier Q. The French nuclear bet. Faere Policy Paper. 2017.
24. TAEK Hizmetten Çıkarma Atıkları. URL: http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/168-nukleer-atiklar/454-hizmetten-cikarma-atiklari.html [Son Erişim Tarihi: 10.10.2017]
25. Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection. Vienna: UAEA Publications, 2007.
26. UAEA Nuclear Security and Safety Definition. URL: http://www-ns.iaea.org/standards/concepts-terms.asp [Son Erişim Tarihi: 03.11.2017]
27. The Interface Between Safety and Security at Nuclear Power Plants. Vienna: UAEA Publications, 2010.
28. Nuclear Security Culture. Vienna: UAEA Publications, 2008.
29. Objective and Essential Elements of a State's Nuclear Security Regime. Vienna: UAEA Publications, 2013.
30. Defence in Depth in Nuclear Safety. Vienna: UAEA Publications, 1996.
31. Nuclear Energy Institute Cyber Security for Nuclear Power Plants. URL: https://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants [Son Erişim Tarihi: 11.12.2017]
32. Preventive and Protective Measures against Insider Threats Implementing Guide. Vienna: UAEA Publications, 2008.
33. Development, Use and Maintenance of the Design Basis Threat. Vienna: UAEA Publications, 2009.
34. Implementation of the NPT Safeguards Agreement and Relevant Provisions Of Security Council Resolutions In The Islamic Republic Of Iran. Vienna: UAEA Publications, 2010.
35. TAEK İkitelli Kazası Raporu. URL: http://www.taek.gov.tr/attachments/kazalar/ikitelli_tr.pdf [Son Erişim Tarihi: 10.10.2017]
36. Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier Report. 2011.
37. Reuters Researchers Say Stuxnet Was Deployed Against Iran in 2007. URL: https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226 [Son Erişim Tarihi: 02.10.2017]
38. VirusBlokAda Stuxnet Ortaya Çıkış. URL: http://www.anti-virus.by/en/tempo.shtml [Son Erişim Tarihi: 08.11.2017]
39. Stakeholder Involvement in Nuclear Issues. Vienna: UAEA Publications, 2006
40. NyTimes Obama ordered wave of cyberattacks against Iran. URL: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [Son Erişim Tarihi: 15.10.2017]
41. Albright D, Brannan P, Walrond C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security Report. 2010.
42. A Cyberattack Has Caused Confirmed Physical Damage For The Second Time Ever URL: https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [Son Erişim Tarihi:15.10.2017]
43. Lee RM, Assante MJ, Conway T. German Steel Mill Cyber Attack. Sans ICS Defense Use Case. 2014.
44. Stanford University Jesse Min Coursework North Korea's Asymmetric Attack on South Korea's Nuclear Power Plants. URL: http://large.stanford.edu/courses/2017/ph241/min1/ [Son Erişim Tarihi: 02.11.2017]
45. Reuters German Nuclear Pland Infected with Computer Viruses. URL: https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS [Son Erişim Tarihi: 06.10.2017]

46. TheGuardian South Korea NPP Cyber Attack Hack. URL: https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack [Son Erişim Tarihi: 10.03.2017]
47. Wired A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. URL: https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [Son Erişim Tarihi: 01.10.2017]
48. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities. Vienna: UAEA Publications, 2011.
49. Computer Security at Nuclear Facilities. Vienna: UAEA Publications, 2011.
50. Clarke Ra, Knake RK. Siber Savaş. İstanbul: İkü Yayınevi, 2011. p. 119.
51. Çakmak H, Demir CK. Siber Dünyadaki Tehditler ve Kavramlar. In: Suç, Terör ve Savaş Üçgeninde Siber Dünya. Ankara: Barış Platin Kitabevi, 2009. p. 39.
52. Çifci H. Her Yönüyle Siber Savaş. Ankara: Tübitak Popüler Bilim Kitapları, 2013. p. 154.
53. Ersanel N. Siber İstihbarat: Siber ve Dijital Casusluğun Anatomisi. Ankara: Asam Yayınları, 2001. p. 10.
54. Nuclear Power Reactors in the World. Vienna: UAEA Publications, 2016.
55. Stanford Courses Jaffer M. Uranium Enrichment. URL: http://large.stanford.edu/courses/2011/ph241/jaffer1/ [Son Erişim Tarihi: 02.11.2017]
56. Moore GM, Banuelos CA, Gray TT. Replacing Highly Enriched Uranium in Naval Reactors Report. 2016.
57. World Nuclear Association Uranium Enrichment. URL: http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/conversion-enrichment-and-fabrication/uranium-enrichment.aspx [Son Erişim Tarihi: 29.10.2017]
58. TAEK Nükleer Yakıt Çevrimi. URL: http://www.taek.gov.tr/nukleer-guvenlik/nukleer-enerji-ve-reaktorler/166-gunumuzde-nukleer-enerji-rapor/437-bolum-03-nukleer-yakit-cevrimi.html [Son Erişim Tarihi: 14.09.2017]
59. Wise-Uranium World Nuclear Fuel Facilities. URL: http://www.wise-uranium.org/efac.html [Son Erişim Tarihi: 09.11.2017]