DERLEME REVIEW

DOI: 10.5336/forensic.2021-84226

Kritik Altyapılardan Nükleer Santrale Yönelik Olası Siber Saldırılara Müdahale Konusunda Amerika Birleşik Devletleri, Fransa ve Türkiye'nin İdari Yapılarının İncelenmesi: Geleneksel Derleme

Investigation of the Administrative Structures of the United States of America, France and Turkey on Response to Possible Cyber Attacks from Critical Infrastructures to the Nuclear Power Plant: Traditional Review

Abdullah GENCAY[a], Esra ARSLAN[b], Sait ÖZSOY[c], Nergis CANTÜRK[b]

[a]Ankara Emniyet Genel Müdürlüğü, Ankara, TÜRKİYE
[b]Ankara Üniversitesi Tıp Fakültesi, Adli Tıp ABD, Ankara, TÜRKİYE
[c]Ankara Gülhane Eğitim ve Araştırma Hastanesi, Adli Tıp Kliniği, Ankara, TÜRKİYE

ÖZET Dünyada olduğu gibi Türkiye'de de internet kullanımı giderek artmaktadır. Bu durum siber suçların da sık yaşanmasına neden olmaktadır. Bazen vatandaşlar bazen de devletin kritik altyapıları suçtan etkilenmektedir. 2010 yılında İran Natanz Uranyum Zenginleştirme Tesisine Stuxnet olarak isimlendirilen siber saldırının fiziksel bir tesise dijital yollarla yapılmış en büyük saldırı olduğu kabul edilir ve devletlerin siber güvenliğe muhafazakâr bakışını değiştirmiştir. 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 hâlâ devam etmektedir. Tüm bu gelişmeler nükleer tesisleri de kapsayan kritik altyapıların tamamına yönelik siber saldırılardan korunmanın ülkemiz için de önemli olduğunu göstermektedir. Ülkemiz, 2023 yılında 2 farklı nükleer tesiste 8 nükleer reaktöre sahip olma yolunda ilerlemektedir. 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 yapıda olmalıdır. Bu çalışma ile nükleer siber emniyet konusunda ülkemizin mevcut yapısının yanında Amerika Birleşik Devletleri ve Fransa gibi nükleer reaktör işletimi alanında 2 öncü ülkenin idari yapıları incelenmiş ve ülkemizde bu anlamda mevcut durumun değerlendirmesi amaçlanmıştır. Çalışma sonucunda, ülkemizde nükleer tesislerin ve kritik altyapıların siber emniyetinin sağlanması konusunda sorumlulukların daha net tanımlanması 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 tesis; siber saldırı; siber güvenlik; nükleer enerji

ABSTRACT Internet usage is increasing in Turkey as well as in the world. 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 2010, a cyber attack on the Iranian Natanz Uranium Enrichment Facility named Stuxnet was the biggest attack on a physical facility. 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. Our country is on the way to own 8 nuclear reactors in 2 different nuclear facilities in 2023. Cyber protection requires constant consideration of security vulnerabilities, regularly strengthening the level of awareness of the stuff instead of short-term reactive actions during attack. With this study, in addition to the current structure of our country in nuclear cyber security, the existing structures of two leading countries in the field of nuclear reactor operation, such as the United States of America and France, were examined and it was aimed to evaluate the current situation in our country in this sense. It was concluded that the responsibilities for ensuring the cyber security of nuclear facilities and critical infrastructures in our country should be defined more clearly, that the nuclear safety culture should be perceived as a life cycle.

Keywords: Critical infrastructure; nuclear facility; cyber attack; cyber security; nuclear energy

Correspondence: Abdullah GENCAY
Ankara Emniyet Genel Müdürlüğü, Ankara, TÜRKİYE/TURKIYE
E-mail: abdullahgencay@gmail.com

Peer review under responsibility of Turkiye Klinikleri Journal of Forensic Medicine and Forensic Sciences.

Received: 05 May 2021 ***Received in revised form:*** 15 Sep 2021 ***Accepted:*** 16 Sep 2021 ***Available online:*** 22 Sep 2021

Teknolojinin gelişmesiyle birlikte, gerek kamu kuruluşları gerek özel kuruluşların işleyişlerinde meydana gelen en önemli değişiklik sistemlerin otonomlaşmasıdır. Bilgisayar kontrollü sistemlerin ön plana çıkmasıyla insan kaynaklı hataların azalmasını sağlasa da sistemleri dış merkezli saldırılara açık hâle getirmektedir. Devlete zarar verme hedefindeki gruplar; elektronik hizmet alanları, barajlar, elektrik dağıtım şebekeleri, nükleer tesisler, askerî tesisler gibi kritik altyapıları hedefleyebilirler. 2023 yılına kadar çalışan en az bir nükleer reaktör sahip olmayı hedefleyen ülkemizde henüz çok yeni olan nükleer enerji alanında siber güvenliğin sağlanması büyük önem arzetmektedir.

Türkiye Cumhuriyeti'nin "Yap-Sahip Ol-İşlet" modeliyle nükleer enerji üretimiyle tanışacak olması, bu tesisleri hedef alabilecek siber saldırıları önleme konusunda deneyimimizin olmaması önemli bir eksikliktir. Ülkemizin ilgili kurumları arasındaki görev paylaşımının tanımlanması yaşanabilecek sıkıntıları öngörme ve önleme basamakları açısından gereklidir.

Bu çalışmada, nükleer enerji alanında dünyada oldukça yol katetmiş 2 ülkenin mevcut idari yapıları incelemeye alınmış ve ülkemiz idari yapısı üzerinden değerlendirmelerde bulunulmuştur. Bu sayede, ülkemizin siber güvenlik açısından durumunun değerlendirilmesi ve varsa eksiklerin önümüzdeki örneklerle ne şekilde giderebileceğinin belirlenmesi amaçlanmaktadır.

Gelişen teknoloji ile ev eşyalarını bile internet üzerinden verilen talimatlarla yönetmek mümkün hâle gelmiştir. 2021 yılı itibarıyla yaklaşık 6,4 milyar akıllı telefon kullanıcısının bulunduğu dünyada siber alan her an her yere ulaşmıştır.[1]

"Siber" kelimesi İngilizcedeki "cyber" kelimesinden dilimize girmiş olup "bilgisayar, bilgisayar ağları ve sanal gerçeklik kelime anlamlarının bir araya gelmesiyle oluşmuş birleşik kelime" olarak tanımlanmaktadır.[2]

Amerikalı bilim adamı N. Weiner tarafından ilk kez 1948 yılında "hayvanlarda ve makinelerde iletişim ve kontrol bilimi" anlamında kullanılmıştır.[3]

"Siber suç" hedefin bilgisayar olduğu ya da geleneksel bir suçun bilgisayar kullanılarak işlenmesi şeklinde 2 ana başlık altında incelenir.[4]

Siber saldırı, siber ortamdaki verinin değiştirilmesi, çalınması, erişimin kısıtlanması/kesilmesi gibi durumların işlemlerinin yetkisizce yapılmasıdır.[5]

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.[6]

Nükleer reaktörler, zenginleştirilmiş uranyum çekirdeklerinin kullanılmasıyla elektrik üretiminde 1950'li yıllardan beri kullanılan tesislerdir. Aralık 2020 yılı itibarıyla dünyada 30 ülkede toplam 443 adet aktif, 19 ülkede toplam 54 adet inşa hâlinde reaktör bulunmaktadır (Tablo 1).[7] Reaktörlerin gücü ifade edilirken üretmiş olduğu elektrik enerjisinin MW (Megawatt) değeri esas alınır. Araştırma reaktörleri saatte 0-100 MW aralığında ticari reaktörler ise saatte 20-1.561 MW aralığında yıllık net enerji üretimi gerçekleştirirler.

Uluslararası Atom Enerjisi Ajansı (UAEA), Birleşmiş Milletler bünyesinde faaliyet gösteren bağımsız, uluslararası bilim ve teknoloji temelli bir organizasyon olup 29 Temmuz 1957 yılında kurulmuştur. Bünyesindeki denetim mekanizması ile ülkelerin taahhütlerini yerine getirmesini kontrol etmektedir. Türkiye'nin de dâhil olduğu 168 üye devleti vardır. UAEA Tüzüğü 23 Ekim 1956 yılında Genel Konferansta onaylanmış, 29 Temmuz 1957 yılında yürürlüğe girmiştir. Türkiye, 1957 yılında tüzüğünü onaylamak suretiyle UAEA'ya üye ülkeler arasında yer almıştır. Nükleer santraller, UAEA'nın yapacağı denetimlere açıktır.[8]

Dünya çapında 9 ülkede [Amerika Birleşik Devletleri (ABD), Rusya, Birleşik Krallık, Fransa, Çin, Hindistan, Pakistan, Kuzey Kore, İsrail] nükleer silah bulunduğu bilinmektedir.[9] Nükleer güvenlik oluşturulabilmesi amacıyla; Nükleer Silahların Yayılmasının Önlenmesi Antlaşması ve Nükleer Madde ve Tesislerin Fiziksel Korunması Sözleşmesi imzalanmış ve dünya çapında birçok ülkede yürürlüğe girmiştir.[9]

Ülkenin yetkili otoritesi, nükleer güvenlik ve emniyetle ilgili kurucunun faaliyetlerini denetleme,

TABLO 1: Dünyada faaliyette olan ve yapım aşamasında olan nükleer enerji reaktörleri (31 Aralık 2019 itibarıyla).[7]

Ülke	Operasyonel reaktör sayısı		İnşa sürecindeki reaktörler		2019 tedarik edilen nükleer elektrik	
	Sayı	Total MW	Sayı	Total MW	Tw/h	% Total
ABD	96	98.152	2	2.234	809,4	19,7
Arjantin	3	1.641	1	25	7,9	5,9
Almanya	6	8.113				
Bangladeş			2	2.160		
Belarus			2	2.220		
Belçika	7	5.930			41,4	47,6
Birleşik Arap Emirlikleri			4	5.380		
Birleşik Krallık	15	8.923	2	3.260	51	15,6
Brezilya	2	1.884	1	1.340	15,2	2,7
Bulgaristan	2	2.006			15,9	37,5
Çek Cumhuriyeti	6	3.932			28,6	35,2
Çin	48	45.518	11	10.564	330,1	4,9
Ermenistan	1	375			2	27,8
Finlandiya	4	2.794	1	1.600	22,9	34,7
Fransa	58	63.130	1	1.630	382,4	70,6
Güney Afrika	2	1.860			13,6	6,7
Güney Kore	24	23.172	4	5.360	138,8	26,2
Hindistan	22	6.255	7	4.824	40,7	3,2
Hollanda	1	482			3,7	3,1
İran	1	915	1	974	5,9	1,8
İspanya	7	7.121			55,9	21,4
İsveç	7	7.740			64,4	34
İsviçre	4	2.960			25,4	23,9
Japonya	33	31.679	2	2.653	65,7	7,5
Kanada	19	13.554			94,9	14,9
Macaristan	4	1.902			15,4	49,2
Meksika	2	1.552			10,9	4,5
Pakistan	5	1.318	2	2.028	9	6,6
Romanya	2	1.300			10,4	18,5
Rusya	38	28.437	4	4.525	195,5	19,7
Slovakya	4	1.814	2	880	14,3	53,9
Slovenya	1	688			5,5	37
Türkiye			1	1.114		
Ukrayna	15	13.107	2	2.070	78,1	53,9

test sonuçlarını değerlendirme testleri tekrarlatma, yaptırım ve lisanslama iptali gibi haklarını daima saklı tutar.[10]

ABD'de aktif 96 adet nükleer reaktör mevcut olup, 2 nükleer reaktör inşa aşamasındadır. Aktif reaktör sayısı olarak dünya lideri olan Amerika'yı aktif 58 reaktörle Fransa takip etmektedir.[11]

Nükleer Düzenleme Komisyonu [Nuclear Regulatory Commission (NRC)], ABD sınırlarında nükleer enerjiyle ilgili halk sağlığını ve emniyetini ilgilendiren tüm konularla ilgili düzenleme yapmakla görevli bağımsız bir kuruluştur.

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.[12]

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.[13]

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. Bünyesindeki Siber Emniyet Bürosu ile NRC tarafından lisanslanmış tesislerdeki siber emniyetle ilgili ajans çapındaki aktiviteleri planlar, koordine eder ve yönetir.[14]

Emniyet Operasyonları Şubesi, nükleer tesisler ve materyallerin güvenliği ve emniyeti için programların uygulanmasını yönetir. NRC ihtiyaçlarının ve NRC tarafından lisanslandırılmış tesislerin,emniyet ve güvenlik personeliyle ilgili aktivitelerinin uygulanmasını değerlendiren NRC gözetim programını geliştirir ve denetler.[15]

ABD Savunma Bakanlığı, 2011 yılında siber ortamda faaliyetleri yürütmek ve harekât icra edebilmek için belirlediği 5 stratejik girişim ile ilgili bilgi vermek maksadıyla ABD Savunma Bakanlığı Siber Ortamda Harekât Stratejisi (DoD Strategy for Operating in Cyberspace) belgesini yayımlamıştır. Yayımlandığı yıl itibarıyla DoD'un siber uzayı onlarca ülkede yer alan 15.000 adet ağ ve 7milyon cihaz üzerinde askerî ve istihbarat faaliyetleri ile personel, malzeme hareketlerini ve komuta kontrol sistemleri için kullandığı belirtilmiştir.[16]

Birleşik Devletleri Siber Komutanlığı [United States Cyber Command (USCYBERCOM)], Savunma Bakanlığına bağlı olarak 2010 yılında faaliyete başlamıştır. Kritik altyapıların korunması sürecinde İç Güvenlik Bakanlığına [Department of Homeland Security (DHS)] destek olur. 2017 yılı bütçesi 7 milyar dolardır.[17] Bünyesinde tamamı siber saldırılarla ilgilenen 133 farklı ekibi bulunmaktadır.

Ulusal Güvenlik Ajansı [National Security Agency (NSA)], ülkenin iletişim ve bilgi sistemlerinin korunmasından sorumlu olan askerî istihbarat kuruluşudur. Bu sorumluluğu yerine getirirken, ülke sınırları dışından da edindiği sinyal bilgilerini istihbari olarak işler ve kullanır. Bu görevinin yanında ayrıca iletişim ağları ve bilgi sistemlerinin korunmasıyla görevlidir. NSA başkanı ayrıca USCYBERCOM'un da başkanıdır.[18]

DHS, 11 Eylül 2001 saldırılarından sonra 25 Kasım 2002 yılında 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 DHS'nin ana görev alanlarıdır. Önemli siber saldırıların yaşanması durumunda koordinasyon yetkisi bulunan bu bakanlık özel sektöre ihtiyaç duyulduğunda siber alanda destek verir. 2021 bütçesi 69,8 milyar dolardır.[19]

Federal Acil Durum Yönetim Ajansı, DHS'nin ulusal düzeyde yaşanabilecek her türlü acil durumun önlenmesi, acil durumdan korunulması, zararın azaltılması ve önceki duruma dönülmesi süreçlerini yürüten ve yöneten ajansıdır.[20]

Federal Soruşturma Bürosu [Federal Bureau of Investigation (FBI)], ABD Adalet Bakanlığı bünyesinde, federal suçların araştırılması ve ülke içinde istihbarata karşı koyulmasından sorumludur. Yaklaşık 35.000 personele sahip olan FBI'nın 2021 yılı bütçesi 9,8 milyar dolardır. FBI ayrıca siber güvenlik konularında, DHS'ye bilgi ve destek sağlamaktadır.[21]Alt birimlerinden 2 tanesinin birçok görevinin yanında ayrıca nükleer alanda meydana gelecek olaylarla ilgili de görevleri bulunmaktadır.

Merkezi Haberalma Teşkilatı [Central Intelligence Agency (CIA)], 1947 yılında Ulusal Emniyet Yasası ile kurulmuştur. ABD adına politika belirleyicilere ulusal emniyet konuları ile ilgili geniş çaplı istihbarat sağlamaktan sorumludur. Federal hükümetinin yabancı istihbarat servisi olarak hizmet verir. Ülke içi emniyet hizmeti görevi bulunan FBI'nın aksine CIA deniz aşırı yerlerden bilgi toplamaya odaklanmıştır.[22]

Fransa, nükleer enerji üretim ve kullanımında, dünyanın 2 numarası olarak kabul edilmektedir. ABD'den sonra en büyük elektrik üreticisidir. Fransa'da nükleer enerji ve santrallerle ilgili faaliyetler, kamu ve özel kuruluşların kesişen çalışmalarıyla yürütülmektedir.[23] Nükleer Güvenlik Kurumu [Autorité de Sûreté Nucléaire (ASN)], nükleer güvenlik ve radyasyondan korunma alanlarında bağımsız yetkili kuruluştur. Bu kuruluş, 2006 yılında kurulmuştur.[24]

Fransa Ulusal Siber Emniyet Ajansı, Başbakanlık ile ilişkili Ulusal Savunma ve Güvenlik Sekreterliğine 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 tarafından da onaylanmış bir eğitim merkezini bünyesinde barındırmaktadır. Beş yüz çalışanı bulunmaktadır.[25]

ATOM ENERJİSİ VE ALTERNATİF ENERJİLER KOMİSYONU

1945 yılında Atom Enerjisi Komisyonu adıyla kurulmuştur, 2010 yılında ise 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. Ülkemizdeki Enerji Bakanlığı seviyesindedir. Dokuz 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.[26]

Ülkemizde aktif olarak çalışan Nükleer Santral bulunmamaktadır. İki adet araştırma reaktörü bulunmaktadır. Türkiye Atom Enerji Kurumu [Turkish Atomic Energy Authority (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, 1956 yılında Atom Enerjisi Komisyonu adıyla kurulmuş olup, UAEA'nın ülkemizdeki iletişim noktası olmakla birlikte bu ajansın dünya genelindeki görevlerini ülkemizde uygulayabilmek için çalışmalar yapmaktadır. 2020 yılında TAEK, yetkileri artırılarak Türkiye Enerji, Nükleer ve Maden Araştırma Kurumu (TENMAK) olarak ismi değiştirilmiştir.[27]

TENMAK'ın görevleri; enerji, maden, iyonlaştırıcı radyasyon, parçacık hızlandırıcıları ve nükleer teknoloji alanında hizmet etmek, Türkiye'nin rekabet gücünü artırmak ve sürekli kılmak, inovasyon ihtiyacını karşılamak, yeni ürünlerin üretimini ve var olanların geliştirilmesini sağlamak, araştırmacılara bilimsel ortam temin etmek, kamu ve özel hukuk kişileriyle iş birliği içinde bilimsel araştırmalar yapmak, yaptırmak, bu araştırmaları koordine etmek, teşvik etmek, araştırma ve geliştirme faaliyetlerine katkı sağlamak, bilimsel, teknik ve idari çalışmaları yapmak, yaptırmak, düzenlemek, desteklemek, iş birlikleri kurmak ve koordine etmektir.[27]

Ülkemizde nükleer enerji ile ilgili çalışmalar1950'li yıllara dayanmaktadır. Bir nükleer santrale sahip olabilmek için pek çok girişimlerde bulunulmuş ancak bazen siyasi bazen ticari nedenlerle bu girişimler sonuçsuz kalmıştır. 2010 yılında 5. nükleer santral kurma hamlesi "Türkiye Cumhuriyeti Hükümeti ile Rusya Federasyonu Hükümeti Arasında Türkiye Cumhuriyetinde Akkuyu Sahası'nda Bir Nükleer Güç Santrali'nin (NGS) Tesisine ve İşletimine Dair İş Birliğine İlişkin Anlaşma" imzalandı. Aynı yıl Resmî Gazete'de yayımlanarak yürürlüğe girdi. Rusya (Rosatom) ile Akkuyu NGS'nin yapılması için anlaşıldı.[28] 2015 yılında Akkuyu NGS'nin temeli atılarak, Türkiye'nin ilk nükleer santralinin inşasına başlandı.[29]

Atılan teknolojik adımların ardından, ulusal güvenliğinin tam anlamıyla sağlanabilmesi için girişimlerde bulunulmuştur. "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" isimli belge 2013 yılında Bakanlar Kurulu kararıyla Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.[30] Bu belgede, kritik altyapılarla ilgili olarak Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlara "Siber tehditlerin doğrudan hedefi hâline

gelen ve zarar görmesi hâlinde toplum düzenini bozabilecek kritik altyapıların tespit edilmesi" ve "Belirlenecek bir kritik altyapının sektörel risk analizinin yapılması" görevleri verilmiştir.[31] Merkezî bir yapı ile siber olaylar konusunda düzenli iletişim, destek ve koordinasyonun planlandığı kararda Ulusal Siber Olaylara Müdahale Merkezi (USOM) isimli bir çatı yapı kurulmuş ve bu yapıya "bağlı" her kamu kurumunda her sektörde Siber Olaylara Müdahale Ekibi (SOME) isimli alt kuruluşların kurulacağı belirtilmiştir.

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 Kurulunun 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 Bilgisayar Acil Müdahale Ekibi [Computer Emergency Response Team (CERT)] Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (TÜBİTAK BİLGEM) bünyesinde kurulmuştur.[32] Bünyesinde BİLGEM ve Siber Güvenlik Enstitüsü (SGE) kuruluşlarını bulundurur. BİLGEM bilgi güvenliği, ileri serviye elektronik alan çalışmaları ve bilişim alanlarında ihtiyaçlara dönük çözümler üretmek amacıyla 2010 yılında oluşturulmuş bir Ar-Ge merkezidir. SGE 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 artırma 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.[33]

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.[34]

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.[34]

Enerji ve Tabii Kaynaklar Bakanlığı, nükleer alanla ilgili faaliyetlerini ana hizmet birimlerinden birisi olan Nükleer Enerji Proje Uygulama Dairesi 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.[35]

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın 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.[36] Nükleer santraller de bu eylem planında kritik altyapı statüsünde yer almaktadır.

2016 yılında Savunma Sanayii Müsteşarlığına Türk Silahlı Kuvvetleri (TSK) Siber Savunma Merkezi (SİSAMER) projesinin hayata geçirilmesi için yetki verildi. Bu proje, TSK'ye ait bilgi sistemlerinin siber güvenliğinin millî yazılımlar vasıtasıyla güçlendirilmesi ve TSK'nin siber olaylara anında tepki vererek söz konusu olayların muhtemel etkilerinin azaltılması amacıyla başlatılmıştır. Projenin detayları ile açık kaynaklarda bilgi paylaşımı görülmemiş olup Temmuz 2017 SİSAMER'in Harekât Merkezi Tesisi ilk safha modernizasyonunun tamamlandığı duyurulmuştur.[37] 2017 yılı içerisinde Siber Savunma Harekât

Merkezi kurulumu tamamlanarak TSK'nin hizmetine sunulmuştur. Müteakiben 2020 yılı ilk çeyreğinde ise millî olarak geliştirilen siber güvenlik yazılımlarının geçici kabulü yapılarak bu yazılımlar TSK'nin kullanımına verilmiştir.

Nükleer Düzenleme Kurumu, Temmuz 2018 tarihinde kurulmuş olup, Türkiye'de nükleer enerji sektöründeki faaliyetler ile radyasyonla ilgili tesis ve faaliyetleri düzenlemek ve denetlemekle görevli kurumdur. Kurumun görev ve yetkileri arasında, ulusal radyasyon kaynakları kayıt sistemini, ulusal merkezi doz kayıt sistemini ve ulusal nükleer madde sayım ve kontrol sistemini kurmak ve işletmek, ulusal radyasyon izleme faaliyetini yürütmek veya yürütülmesini temin etmek, nükleer tesislerde, radyasyon tesislerinde ve radyoaktif atık tesislerinde emniyetin sağlanması amacı ile düzenleyici kontrolün uygulanmasına ilişkin iş ve işlemleri yürütmek bulunmaktadır.[38]

Ülkemizde farklı kurumların organizasyonunda Siber Güvenlik Tatbikatı, Siber Kalkan Tatbikatı gibi isimlendirilmiş tatbikatlar düzenlenmiştir. 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 tatbikatlardan etkili kazanımlar elde edilmiştir.[39]

TARTIŞMA

Ülkemizin başlıca enerji üretim kaynakları olarak hidroelektirik santraller, termik santraller ve rüzgâr elektrik santraller sayılabilir. Bunların arasında termik santraller, maliyet açısından en uygun olanıdır. Kömür rezervlerimizin büyük bölümünün düşük kaliteli linyit kömüründen oluşması, rüzgâr 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 nükleer enerjiden elektrik üretimini teşvik edici konular arasındadır.

"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 olması ayrıca önemli bir noktadır. Akkuyu NGS işletmeye alındıktan sonra ortaya çıkan hatalar sonucunda yaşanabilecek hizmetten çıkarma, zararın tazmini gibi durumlar da yine Rus tarafına finans, şöhret gibi anlamlarda kayıp olarak yazılacaktır. Bu nedenler, Rusya'nın tüm riskleri çok iyi değerlendirerek konuya dikkatli bir şekilde yaklaşmasını gerektirmektedir.[40]

Dünya çapındaki nükleer santraller Tablo 1'de sunulmuş olup, bunlara yönelik olası bir siber saldırının sonuçları küresel felaketle sonuçlanabilir. Bu nedenle nükleer tesislerin siber güvenliğinin yeterince sağlanması, sadece ülkeler olarak değil küresel olarak da büyük önem arz etmektedir.

UAEA Referans Kılavuzu'na 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 yanı sıra siber kabiliyetlerin her geçen gün değişmesi, tesistetesis çalışmaya başlamadan önce dahi-sürekli değerlendirilmesi gereken bir siber emniyet rejimi oluşturulmasını gerektirmektedir.[41]

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 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

belirlenmiştir.[17,34] Dört 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 durumu netleştirmesi büyük önem arzetmektedir. Kanunla afet tanımı içerisine giren her türlü durumu önleme/mücadele etme/zarar azaltma görevleri AFAD'a verilmiş, Bakanlar Kurulu kararıyla ise siber güvenlik konusunda koordinasyon görevi Siber Güvenlik Kuruluna 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 sorumluluğun netleşmesi sonrasında ABD ve Fransa'nın ayrıca Kritik Altyapı Sektörü içerisinde değerlendirdiği diğer sektörlerle ilgili bir çalışma yapılması önemlidir.

Kritik altyapılar konusunda ABD'de yayımlanmış ilk belge 1996 tarihli bir kararnameye aittir.[42] 2018 yılında Başkan Trump tarafından imzalanan Siber Güvenlik ve Altyapı Güvenliği Ajansı Yasası ile birlikte DHS'nin yetkilerini artırarak Siber Güvenlik ve Altyapı Güvenliği Ajansı [Cybersecurity and Infrastructure Security Agency (CISA)] kurulmuştur. CISA tarafından fiziksel veya sanal olsun; varlıkları, sistemleri ve ağları ABD için çok hayati kabul edilen ve bunların yetersizliği veya yıkımı; ulusal ve ekonomik güvenlik, ulusal halk sağlığı veya güvenliği üzerinde zayıflatıcı bir etkiye sahip olan 16 kritik altyapı sektörü tanımlamıştır.[43]

Fransa özelinde kritik altyapıların güvenliği konusu irdelendiğinde, Savunma ve Ulusal Güvenlik Genel Sekreterliği tarafından 2013 yılında geliştirilip yayımlanan "Kritik Altyapı Koruma" yürürlüktedir. Bu programa göre 12 farklı sektör, kritik altyapı sektörü olarak tanımlanmıştır.[44]

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 12 yıl sonra kritik altyapı sektörlerini oluşturduğu görülmektedir. Ayrıca ülkemizin kritik olarak kabul ettiği altyapıların sayısının da diğer ülkelere oranla az olduğu dikkat çekmektedir (Tablo 2).

Ülkemizde, kritik altyapılarla ilgili tanımların yapılmış olması, hangi sektörlerin kritik altyapı sektörleri içerisinde olduğunun belirlenmesi önemli adımlardır.

TABLO 2: Kritik altyapı sektörleri karşılaştırma çizelgesi.[34,43-45]

Türkiye	ABD	Fransa
1. Elektronik haberleşme	1. Tarım ve gıda	1. Gıda
2. Enerji	2. Finans hizmetleri	2. Su yönetimi
3. Su yönetimi	3. Kimya	3. Sağlık
4. Kritik kamu hizmetleri	4. Ticari tesisler	4. Sivil aktiviteler
5. Ulaştırma	5. Nükleer reaktörler, maddeler ve atık	5. Yasal aktiviteler
6. Bankacılık ve finans	6. Barajlar	6. Askerîaktiviteler
	7. Savunma Sanayii	7. Enerji
	8. Su ve atık su sistemleri	8. Finans
	9. Acil hizmetler	9. Taşıma
	10. Enerji	10. İletişim, teknoloji ve yayın
	11. Kamu tesisleri	11. Endüstri
	12. Bilgi teknolojileri	12. Uzay ve araştırma
	13. Kamu sağlığı ve sağlık hizmetleri	
	14. İletişim	
	15. Ulaştırma hizmetleri	
	16. Kritik üretim	

Ülkemizde nükleer bir tesisin SOME'sinin bağlı bulunacağı kurum Enerji Piyasası Düzenleme Kurumudur (EPDK). EPDK'nin enerji üretimi ile ilgili lisanslama ve denetleme yetkisi bulunmaktadır. Nükleer bir tesisin neredeyse tüm denetim görevleri TENMAK sorumluluğundadır.

Nükleer güç santrallerinin kuruluşu sürecinde işletmeciye sadece elektrik enerjisi satışı ile ilgili lisans veren EPDK'nin bağımsız bir kuruluş olan TENMAK üzerinde herhangi bir yaptırım gücü bulunmamaktadır. Ancak TENMAK'ın SOME kurması durumunda, enerji sektöründe bulunması nedeniyle EPDK'nin SOME'sine bağlı hareket etmesi gerekmektedir. Mesela ülkemizde ilk nükleer santrali işletecek olan Akkuyu NGS Elektrik Üretim A.Ş.'nin bir SOME kurması ve bu SOME'nin EPDK'nin SOME'sine bağlı olması gerekmektedir. Ana başlığı altında Siber Emniyeti de bulunduran Fiziksel Güvenlik ile ilgili denetmen kuruluş TENMAK iken ayrıca SOME'sinin EPDK SOME'sine bağlı olması, siber saldırı konusunda EPDK ile TENMAK'ın olası koordinasyonsuzluğu bir karmaşa yaratabilecektir. Benzer şekilde Akkuyu NGS'de yapılmasına ihtiyaç duyulan bir siber sızma testinin TENMAK veya EPDKkuruluşlarından hangisinin sorumluluğunda olduğu belirlenmelidir. Her kurumun görev tanımı tam olarak yapılmalı ve kesişen görev tanımlarının yol açacağı çelişkilerin bir an önce ortadan kaldırılması ülkemizin güvenliği açısından son derece hayati bir önem teşkil etmektedir (Tablo 3).

Dünya geneline yayılmış olan CERT/ISAC yapılarının yaygınlaştırılması, ülkemizde aynı işleve sahip SOME'lerin kurulumu ve yaygınlaştırılması süreçleriyle benzeşmektedir. 2016 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgesiyle enerji sektörünün tamamından EPDK sorumludur.[36]

ABD'de siber emniyetin sağlanması konusunda, farklı kurumların farklı görev alanlarında sorumluluk sahibi olduğu değerlendirilebilir. Ancak bunların yanında nükleer alanda tüm sorumluluk NRC'ye verilmiştir. Dolayısıyla nükleer siber alanda yapılacak denetlemeler, lisanslama prosedürleri, korunma programlarının hazırlanması gibi faaliyetlerde sorumluluk NRC'dir.[46]

Nükleer güç santralleriyle ilgili olarak; ülkemizde Enerji ve Tabii Kaynaklar Bakanlığı Nükleer Proje Uygulama Dairesine "*mevzuat alanında gerekli çalışmaları yapmak veya yaptırmak*" yetkisi verilmişken TENMAK'a "*her türlü amaç için gerekli teknik mevzuat, tüzük ve yönetmelikleri hazırlamak*" görevi verilmiştir.[27]ABD'de yasal düzenleme lisanslama ve denetleme yetkilerinin tamamı NRC'ye verilmiş olup, ABD Enerji Bakanlığının ilgili birimler sadece nükleer silahlarla ilgili görevler verilmiştir.[13] Fransa'da tüm düzenleme, lisanslama ve denetleme

TABLO 3: Nükleer tesislerin ve kritik altyapıların kurumlar sorumluluk kıyaslama tablosu.[15,16,24,27,36,38,43,44]

		Sorumlu kurum(lar)		
Sıra no	**Sorular**	**ABD**	**Fransa**	**Türkiye**
1	Nükleer tesislerde yapılacak siber denetimlerin planlanması, koordinasyonu süreci	NRC	ASN	TENMAK, EPDK SOME (USOM adına), AFAD
2	Nükleer tesislerde yapılacak siber denetimlerde kullanılacak dokümanların hazırlanması	NRC	ANSSI	TENMAK, EPDK SOME (USOM adına), AFAD
3	Nükleer tesislerde yapılacak siber denetimlerin uygulanması	NRC	ASN	TENMAK, EPDK SOME (USOM adına), AFAD
4	Nükleer tesis işletmecisi tarafından kurulması gereken SOME'lerin (CERT/ISAC) denetimi	NRC	ASN	TENMAK, EPDK SOME (USOM adına), AFAD
5	Hangi altyapıların kritik altyapı kapsamında değerlendirileceğinin belirlenmesi	DHS	ANSSI	UDHB, AFAD
6	Kritik altyapıların siber güvenliğinin sağlanması için politika geliştirme	DHS	ANSSI	UDHB, AFAD

NRC: Nükleer Düzenleme Komisyonu; DHS: İç Güvenlik Bakanlığı; ASN: Nükleer Güvenlik Kurumu; CERT: Bilgisayar Acil Cevap Timi; ISAC: Bilgi Paylaşımı ve Analizi Merkezi; ANSSI: Fransa Ulusal Siber Emniyet Ajansı; TENMAK: Türkiye Enerji, Nükleer ve Maden Araştırma Kurumu; EPDK: Enerji Piyasası Düzenleme Kurumu; SOME: Siber Olaylara Müdahale Ekibi; USOM: Ulusal Siber Olaylara Müdahale Merkezi; AFAD: Afet ve Acil Durum Yönetimi Başkanlığı.

yetkileri ASN'de toplanmış siber anlamda ihtiyaç duyulması durumunda Fransa Ulusal Siber Emniyet Ajansı (ANSSI)'dan destek alınmaktadır.[24]

Bir nükleer tesise yönelik olası 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 paylaşımının değerlendirilmesi ve ülkemiz dinamiklerinin de göz önünde bulundurulduğu ideal yapının oluşturulması için önemli bir gerekliliktir. Proje şirketlerinin, denetleme ekiplerine nüfuz edebilme ihtimali dikkatlice ele alınması gereken bir risk olarak değerlendirilmelidir. Özellikle nükleer siber alan için hem nükleer alanla ilgilenen hem siber alanla ilgilenen özel ve kamu temsilcilerinin bir araya gelerek çalışma yürütmeleri faydalı olacaktır.

Bir nükleer tesisin siber anlamda denetlenmesi, kritik altyapıların belirlenmesi ve bu tesislerin tamamının siber emniyet politikalarının geliştirilmesi ve uygulanması basamaklarında sorumlu kurumlar Tablo 3'te sunulmuştur.

SONUÇ

Günden güne büyük bir hızla yaygınlaşmaya devam eden siber, dünyanın nimetleri kadar güvenlik problemlerini de artırmaktadır. Bankacılık işlemlerini yapamamak ya da uzun pasaport kuyruklarında beklemek zorunda kalmak, siber alan güvenliğinin yaşamın vazgeçilmez bir parçası hâline geldiğinin önemli göstergeleridir.

Nükleer santrallerle ilgili tehlikeler düşünüldüğünde yaşanmış ilk kaza olarak Çernobil faciası akla gelmektedir. Çernobil Kazası Sovyet Sosyalist Cumhuriyetler Birliğinin (Günümüzde Ukrayna içerisinde kalan) Kiev iline bağlı Çernobil bölgesinde bulunan Nükleer Güç Santralinin 4. reaktöründe 1986 yılında meydana gelen kazadır. Dört 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 hâle gelerek büyük bir patlama yaşanmasına neden olmuştur.[47] Çernobil NGS'nin ülkemize yakın bir noktada bulunması ve facianın Karadeniz bölgesini etkilediği bildirilmiştir.

Fukuşima Daiichi kazası 2011 yılında Japonya'da meydana gelen 9.0 büyüklüğündeki deprem anında The Fukuşima Daiichi Nükleer Santrali'nin 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.[48]

İkitelli Vakası (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 işleminin gerçekleşmemesi sonrasında devam eden olaylarla yaşanan vakadır. Gazeteler bu olayla ülkemizin hiç nükleer santrale sahip olmadan "dünyanın en önemli 20 radyoaktif kazası" listesine girdiğini duyurmuşlardır.[49]

Ülke için çok hayati kabul edilen ve bunların yetersizliği veya yıkımı; ulusal ve ekonomik güvenlik, ulusal halk sağlığı veya güvenliği üzerinde zayıflatıcı bir etkiye sahip olan sektörlere kritik altyapı adı verilmiştir. Dünya genelinde kritik altyapılarda yaşanan siber olaylar değerlendirildiğinde, en önemlileri arasında 2005 yılında Mastercard şirketinin saldırıya uğraması nedeniyle 40 milyona kadar kart sahibinin hesap bilgilerinin çalınmış olabileceğini duyurması, 2006-2012 yıllları arasında ABD ve İsrail istihbarat teşkilatları tarafından İran nükleer tesislerine yapılan siber saldırılar, 2007 yılında Estonya bankaları, bürokratları, yayın organlarına Rusya tarafından yapılan siber saldırı, 2008 yılında Rusya-Gürcistan savaşı sırasında her 2 ülkenin internet sitelerine yapılan siber saldırılar, 2010 yılında İran Natanz nükleer tesislerine yapılan Stuxnet siber saldırısı, 2013 yılında Anonymous grubu tarafından Singapur'daki internet sansürlerine karşı bazı hükümet sitelerine siber saldırı yapılması, 2016 yılında Hindistan bankalarına ait

3,2 milyon banka kartı bilgilerinin çalınması, 2020 yılında bilgisayar korsanlarının Dünya Sağlık Örgütü yetkililerinin oturum açma kimlik bilgileriyle ilgili bilgileri sızdırması sayılabilir.[50-57]

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

Nükleer santral ile yeni tanışacak olan ülkemizin aynı zamanda nükleer enerji üretimi ile de yeni tanışıyor olması, bu tesisleri hedef alabilecek siber saldırıları öngörme ve önleme konusunda deneyimimizin olmaması önemli bir eksiklik olarak önümüzde durmaktayken ülkemiz sorumlu kurumları arasında görev paylaşımında çakışmalar da bulunmaktadır.

Sürekli yeni siber tehditlerin ortaya çıkması, siber güvenlik açısından 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.

Bahse konu döngülerin oluşturulması UAEA 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 tanımlanır. Nükleer Emniyet Kültürü 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 artırma faaliyetleri düzenlenmelidir.

Ülkemiz özelinde, bir nükleer tesisin denetlenmesi ile ilgili sorumluluk TENMAK'ın sorumluluğundadır. Bu kurumun siber emniyetle ilgili bir birimi bulunmadığından santrallerin siber anlamda denetlenmeleri işini düzenli olarak TÜBİTAK, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, TSK Siber Savunma Komutanlığı, USOM gibi kurumlardan uzman desteği alınabileceği değerlendirilmektedir. Bir düzenleme ve denetleme kuruluşunun, siber alan gibi özel bir alanda personel istihdamı sağlaması önemlidir. 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 risk yaratmaktadır.

Yine ülkemizdeki mevcut süreç özelinde Akkuyu tesisini inşa eden şirketlerin siber emniyetle ilgili alacağı önlemleri değerlendirecek bir ekibin oluşmasına ihtiyaç vardır. Bu ekibin sadece teknik geçmişinin üzerine bilgi güvenliği alanında da çalışmalar yapmış personelden olması yeterli değildir. Özellikle UAEA'nın yayınlarına, önerdiği uygulamalara hâkim, 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 güvenlik personelinden, bilim insanlarından oluşması gerekmektedir.

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 kuruluşun belirlendiği, çelişkisiz olarak sektörlerin paylaşıldığı bir çerçevenin oluşturulmasına ihtiyaç duyulmaktadır. Kritik altyapılara ya da nükleer tesislere yönelik olası 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.

Finansal Kaynak

Bu çalışma sırasında, yapılan araştırma konusu ile ilgili doğrudan bağlantısı bulunan herhangi bir ilaç firmasından, tıbbi alet, gereç ve malzeme sağlayan ve/veya üreten bir firma veya herhangi bir ticari firmadan, çalışmanın değerlendirme sürecinde, çalışma ile ilgili verilecek kararı olumsuz etkileyebilecek maddi ve/veya manevi herhangi bir destek alınmamıştır.

Çıkar Çatışması

Bu çalışma ile ilgili olarak yazarların ve/veya aile bireylerinin çıkar çatışması potansiyeli olabilecek bilimsel ve tıbbi komite üyeliği veya üyeleri ile ilişkisi, danışmanlık, bilirkişilik, herhangi bir firmada çalışma durumu, hissedarlık ve benzer durumları yoktur.

Yazar Katkıları

Fikir/Kavram: *Abdullah Gencay;* ***Tasarım:*** *Nergis Cantürk;* ***Denetleme/Danışmanlık:*** *Sait Özsoy;* ***Analiz ve/veya Yorum:*** *Abdullah Gencay;* ***Kaynak Taraması:*** *Esra Arslan;* ***Makalenin Yazımı:*** *Abdullah Gencay, Esra Arslan;* ***Eleştirel İnceleme:*** *Nergis Cantürk, Sait Özsoy;* ***Kaynaklar ve Fon Sağlama:*** *Nergis Cantürk.*

KAYNAKLAR

1. Statista [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Number of smartphone users worldwide from 2016 to 2021. Erişim linki: [Link]
2. Türk Dil Kurumu [İnternet]. © 2019-TDK [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Link]
3. Beer S. What is cybernetics? Kybernetes. 2002; 31(2):209-19. [Crossref]
4. Goodman M. The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology. 2002;10(2):139-223. [Crossref]
5. Janczewski LJ, Colarik AM. Cyber Warfare and Cyber Terrorism. 1st ed. New York: Hershey; 2007. [Crossref] [PubMed]
6. Tombakoğlu M, Ergün Ş, Atak H, Çelikten OŞ, Türkmen M, Tiftikçi A, et al; eds. Nükleer Enerji Raporu. Ankara: Tmmob Fizik Mühendisleri Odası (Fmo); 2011. [Link]
7. IAEA [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Nuclear Technology Review. 2020. Erişim linki: [Link]
8. IAEA [İnternet]. © 1998-2021 IAEA [Erişim tarihi: 10 Eylül 2021]. History of IAEA. Erişim linki: [Link]
9. Institute, S.I.P.R. SIPRI YEARBOOK 2020: Armaments, Disarmament and International Security. 2020. Erişim linki: [Link]
10. Ekonomi ve Dış Politika Araştırmalar Merkezi. Nükleer Enerjiye Geçişte Türkiye Modeli Raporu. 2011. Erişim linki: [Link]
11. IAEA [İnternet]. Copyright © 2021 International Atomic Energy Agency (IAEA) [Erişim tarihi: 10 Eylül 2021]. Nuclear Share of Electricity Generation in 2020. Erişim linki: [Link]
12. American Congress A.Energy Reorganization Actof 1974. 1974. p.93-438. [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Link]
13. U.S.NRC [İnternet]. [Erişim tarihi: 10 Eylül 2021]. OIG Reports: Nuclear Regulatory Commission (NRC)-FY 2017 Index. 2017. Erişim linki: [Link]
14. FBI [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Critical Incident Response Group. Erişim linki: [Link]
15. U.S.NRC [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Current Event Notification Report for September 17, 2021. Erişim linki: [Link]
16. Crsc [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Department of Defense Strategy for Operating in Cyberspace. 2011. Erişim linki: [Link]
17. Çiftçi H. Her Yönüyle Siber Savaş. 2. Baskı. İstanbul: Tübitak Popüler Bilim Kitapları; 2017. p.4-5. Siber Savaşın Temelleri. Hasan Çiftçi. [Link]
18. NSA [İnternet]. [Erişim tarihi: 10 Eylül 2021]. National Security Strategy. Erişim linki: [Link]
19. Department of Homeland Security [İnternet]. [Erişim tarihi: 10 Eylül 2021]. FY 2021 Budget-in-Brief. 2021. Erişim linki: [Link]
20. FEMA [İnternet]. [Erişim tarihi: 10 Eylül 2021]. About Us. 2021. Erişim linki: [Link]
21. FBI [İnternet]. [Erişim tarihi: 10 Eylül 2021]. About. 2021. Erişim linki: [Link]
22. CIA [İnternet]. [Erişim tarihi: 10 Eylül 2021]. 2021. Erişim linki: [Link]

23. French Washington Embassy [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Nuclear Power in France. 2013. Erişim linki: [Link]
24. Scottish Government [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Strategy for the learning provision for children and young people with complex additional support needs 2017-2026: full consultation analysis. 2017. Erişim linki: [Link]
25. ANSSI [İnternet]. © ANSSI 2021 LES PRODUITS CSPN [Erişim tarihi: 10 Eylül 2021]. 2013. Erişim linki: [Link]
26. Légifrance [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Arrêté du 26 juillet 2016 relatif au conseil scientifique du Commissariat à l'énergie atomique et aux énergies alternatives. 2016. Erişim linki: [Link]
27. TENMAK [İnternet]. Copyright © 2020 Her Hakkı Saklıdır, TENMAK [Erişim tarihi: 10 Eylül 2021]. 2020. Erişim linki: [Link]
28. Resmî Gazete (6.10.2010, Sayı: 27721) sayılı Yürütme ve İdare Bölümü. [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Link]
29. Hurriyet [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Akkuyu Nükleer Santrali ile ilgili ilk tören yapıldı. 2015. Erişim linki: [Link]
30. Resmî Gazete (20.06.2013, Sayı: 28683) sayılı Bakanlar Kurulu Kararı. [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Link]
31. UDHB [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. 2013. [Link]
32. Şentürk H, Çil Z, Sağıroğlu Ş. Cyber security analysis of Turkey. International Journal of Information Security Science. 2012;1(4):112-25. [Link]
33. Tübitak SAGE [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Savunma Sanayii Araştırma ve Geliştirme Enstitüsü. 2021. Erişim linki: [Link]
34. Ak T. İç güvenlik yönetimi açısından kritik altyapılarını korunması [Protection of critical infrastructures in terms of internal security administration]. ASSAM Uluslararası Hakemli Dergi. 2019:42-51. [Link]
35. T.C. Enerji ve Tabii Kaynaklar Bakanlığı [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Görev ve Yetkiler. 2019. Erişim linki: [Link]
36. T.C.UDHB [İnternet]. [Erişim tarihi: 10 Eylül 2021]. 2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı. 2016. Erişim linki: [Link]
37. T.C. Savunma Sanayi Başkanlığı [İnternet]. T.C. Cumhurbaşkanlığı - Savunma Sanayii Başkanlığı - Telif Hakkı © 2017 [Erişim tarihi: 10 Eylül 2021]. TSK Siber Savunma Merkezi Projesi. 2017. Erişim linki: [Link]
38. ResmîGazete (25.04.2019, Sayı: 30755) sayılı Nükleer Düzenleme Kurumu Teşkilat Yönetmeliği. 2019. [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Link]
39. Bilgi Teknolojileri ve İletişim Başkanlığı [İnternet]. © 2021 Bilgi Teknolojileri ve İletişim Kurumu [Erişim tarihi: 10 Eylül 2021]. Uluslararası Siber Kalkan Tatbikatı 2019. Erişim linki: [Link]
40. Thompson FJ. The Rise of Rosatom & Russia's Nuclear Revival. University of Washington. 2018. [Link]
41. IAEA [İnternet].© 1998-2021 IAEA. IAEA Safety Glossary [Erişim tarihi: 10 Eylül 2021]. 2018. Erişim linki: [Link]
42. Executive Order EO 13010 CriticalInfrastructure Protection July 15, 1996. [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Link]
43. Cybersecurity & Infrastructure Security Agency [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Communications sector-specific plan - 2010. 2010. Erişim linki: [Link]
44. ANSSI. © ANSSI 2021 [Erişim tarihi: 10 Eylül 2021]. The French national digital security strategy. 2013. LAW No. 2013-1168. Erişim linki: [Link]
45. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union. L 345/75. 2008. [Link]
46. U.S. NRG [İnternet]. [Erişim tarihi: 10 Eylül 2021]. About NRC. 2021. Erişim linki: [Link]
47. Higley KA. Environmental consequences of the chernobyl accident and their remediation: twenty years of experience. Report of the chernobyl forum expert group 'environment': STI/PUB/1239, 2006, International Atomic Energy Agency, Vienna, Austria ISBN: 92-0-114705-8, 166 pp, 40.00 Euros (softbound). Radiation Protection Dosimetry. 2006;121(4): 476-77. [Erişim tarihi: 10 Eylül 2021]. Erişim linki: [Crossref]
48. National Research Council. Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants. Washington, DC: The National Academies Press; 2014. [Link]
49. International Atomic Energy Agency. The Radiological Accident in Istanbul. Vienna: International Atomic Energy Agency; 2000. [Link]
50. The New York Times [İnternet]. © 2021 The New York Times Company [Erişim tarihi: 10 Eylül 2021]. Lost Credit Data Improperly Kept, Company Admits. 2005. Erişim linki: [Link]
51. The New York Times [İnternet].© 2021 The New York Times Company [Erişim tarihi: 10 Eylül 2021]. Obama Order Sped Up Wave of Cyberattacks Against Iran. 2012. Erişim linki: [Link]
52. The Economist [İnternet]. Copyright © The Economist Newspaper Limited 2021 [Erişim tarihi: 10 Eylül 2021]. War in the fifth domain. Are the mouse and keyboard the new weapons of conflict? 2010. Erişim linki: [Link]
53. Hollis D. Cyberwar Case Study: Georgia 2008. Small Wars Journal. 2008. [Link]
54. The New York Times [İnternet]. © 2021 The New York Times Company [Erişim tarihi: 10 Eylül 2021]. Iran's Nuclear Agency Trying to Stop Computer Worm. 2010. Erişim linki: [Link]
55. AsiaOne [İnternet]. [Erişim tarihi: 10 Eylül 2021]. Singapore threatened by "Anonymous" hacker group. 2013. Erişim linki: [Link]
56. The Economic Times [İnternet]. Copyright © 2021 Bennett, Coleman & Co. Ltd [Erişim tarihi: 10 Eylül 2021]. 3.2 million debit cards compromised SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit. 2016. Erişim linki: [Link]
57. REUTERS [İnternet]. © 2021 Reuters [Erişim tarihi: 10 Eylül 2021]. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike. 2020. Erişim linki: [Link]