SİBER GÜVENLİK PERSPEKTİFİNDEN TÜRKİYE'NİN NÜKLEER ENERJİ STRATEJİSİ

RAPOR

ŞUBAT 2025

Milli İstihbarat Akademisi

SİBER GÜVENLİK PERSPEKTİFİNDEN TÜRKİYE'NİN NÜKLEER ENERJİ STRATEJİSİ

RAPOR / ŞUBAT 2025

Milli İstihbarat Akademisi

Telif

Yayın Tarihi: Şubat 2025

Millî İstihbarat Akademisi

E-Posta : bilgi@mia.edu.tr

"Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5'inci maddesinin 2'nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir."

SİBER GÜVENLİK PERSPEKTİFİNDEN TÜRKİYE'NİN NÜKLEER ENERJİ STRATEJİSİ

RAPOR / Şubat 2025

İÇİNDEKİLER

TABLO

GRAFİK

HARİTA

ŞEKİL

ÖN SÖZ

Enerji, modern toplumların kalkınmasında ve sürdürülebilir bir gelecek inşa edilmesinde temel bir yapı taşıdır. Hızla artan nüfus, kentleşme ve sanayileşme gibi dinamikler, enerji talebini her geçen gün artırırken aynı zamanda bu talebi karşılayacak sürdürülebilir ve güvenilir enerji kaynaklarının önemini de vurgulamaktadır. Bu bağlamda nükleer enerji yalnızca enerji arz güvenliği sağlamada değil, aynı zamanda ekonomik kalkınma, çevresel sürdürülebilirlik ve millî güvenlik hedeflerine ulaşmada da stratejik bir araç olarak karşımıza çıkmaktadır.

Türkiye, enerji arz güvenliği ve bağımsızlığına yönelik adımlarıyla jeopolitik konumunu güçlendirme ve bölgesel liderlik pozisyonunu pekiştirme hedefi taşımaktadır. Bu kapsamda Akkuyu Nükleer Güç Santrali gibi projeler, ülkemizin enerji portföyünü çeşitlendirmekle kalmayıp enerji ithalatına olan bağımlılığını da azaltma potansiyeline sahiptir. Nükleer enerji, düşük karbon emisyonları ve sürdürülebilir üretim kapasitesi ile Türkiye'nin çevresel taahhütlerini yerine getirmesine katkıda bulunurken aynı zamanda enerji diplomasisi ve uluslararası iş birliği mekanizmaları için de önemli fırsatlar sunmaktadır.

Bu rapor, Türkiye'nin nükleer enerji stratejilerini başta siber güvenlik olmak üzere ekonomik kalkınma ve uluslararası ilişkiler bağlamında analiz etmeyi ve bu stratejilerin geleceğe yönelik yol haritasını çizmeyi amaçlamaktadır. Rapor; enerji arz güvenliği, siber tehditler, uluslararası iş birliği ve yerli kapasitenin geliştirilmesi gibi kritik konuları ele alarak nükleer enerjinin ülkemiz için neden vazgeçilmez bir araç olduğunu ortaya koymaktadır.

Nükleer enerji projelerinin başarıya ulaşmasında yalnızca teknik ve ekonomik boyutlar değil, aynı zamanda halkın güvenini kazanmak, çevresel sürdürülebilirlik ilkelerine bağlı kalmak ve uluslararası güvenlik standartlarına uyum sağlamak gibi unsurlar da belirleyici olacaktır. Bu bağlamda toplumun tüm kesimlerini kapsayan şeffaf ve kapsayıcı bir yaklaşım benimsenmesi büyük önem

taşımaktadır. Bu rapor, tüm paydaşlara rehberlik ederek nükleer enerji alanındaki mevcut durumu değerlendirirken aynı zamanda Türkiye'nin bu alandaki potansiyelini tam anlamıyla gerçekleştirebilmesi için gereken siber güvenlik adımlarını da önermektedir.

Son olarak bu raporun hazırlanmasında emeği geçen tüm ekip üyelerine teşekkür eder, bu çalışmanın Türkiye'nin enerji politikalarının güçlendirilmesi ve millî güvenlik hedeflerinin desteklenmesi yolunda anlamlı bir katkı sağlayacağına olan inancımı belirtmek isterim. Türkiye, sahip olduğu güçlü vizyon ve kararlı adımlarla nükleer enerji alanında bölgesel ve küresel ölçekte lider bir aktör olma yolunda ilerlemeye devam edecektir.

Prof. Dr. Talha Köse
Millî İstihbarat Akademisi Başkanı

YÖNETİCİ ÖZETİ

- Bu rapor, Türkiye'nin nükleer enerji stratejisini siber güvenlik perspektifinden ele alarak enerji arz güvenliğinin sağlanması, ekonomik kalkınmanın desteklenmesi ve uluslararası iş birliklerinin geliştirilmesi için nükleer enerji projelerinin önemini analiz etmektedir. Nükleer enerji; düşük karbon emisyonları, yüksek enerji yoğunluğu ve sürdürülebilirlik avantajlarıyla Türkiye'nin artan enerji ihtiyacını karşılamada stratejik bir rol oynamaktadır. Ancak bu projelerin başarılı bir şekilde hayata geçirilmesi; güvenlik, toplumsal kabul ve uluslararası standartlara uyum gibi temel unsurların etkin bir şekilde yönetilmesini gerektirir.
- Nükleer tesislerin emniyeti hem fiziksel hem de siber tehditlere karşı korunmayı gerektirir ve bu durum, ulusal güvenlik stratejilerinin merkezinde yer alır. Türkiye'nin Akkuyu Nükleer Güç Santrali (Akkuyu NGS) gibi projeleri yalnızca enerji üretimi için değil, aynı zamanda stratejik altyapının korunması açısından da büyük öneme sahiptir. Bu tesisler; olası terör saldırıları, sabotaj ve doğal afetlere karşı çok katmanlı bir koruma sistemi gerektirir.
- Fiziksel koruma açısından nükleer tesisler, uluslararası standartlara uygun koruma protokolleri ile donatılmalıdır. Güvenlik personeli, gelişmiş izleme sistemleri ve fiziksel engeller gibi önlemler, tesislerin yetkisiz erişimlere karşı korunmasını sağlar. Türkiye, nükleer tesislerinde bu tür koruma önlemlerini uygulamak için Uluslararası Atom Enerjisi Ajansı (UAEA) standartlarına uyum sağlamaktadır.
- Siber güvenlik ise modern nükleer tesislerin korunmasında giderek daha önemli hâle gelmiştir. Dijital kontrol sistemlerinin artan kullanımı, tesisleri siber saldırılara karşı savunmasız hâle getirebilir. Bu durum, Stuxnet gibi geçmişte yaşanmış saldırılarla somut bir tehdit hâline gelmiştir. Türkiye, bu tür tehditlere karşı siber güvenlik altyapısını geliştirmekte ve tesislerini bu tehditlere karşı dayanıklı hâle getirmek için uluslararası iş birliklerinden yararlanmaktadır.
- Nükleer tesislerdeki dijitalleşme, operasyonel süreçlerin verimliliğini artırsa da siber tehditleri beraberinde getirmektedir. Türkiye'nin Akkuyu NGS gibi projelerinde kullanılan modern dijital

sistemler, potansiyel siber saldırılara karşı korunmalıdır. Bu durum, nükleer enerji projelerinin başarılı bir şekilde sürdürülmesi için kritik bir gerekliliktir.

- Siber tehditler, nükleer tesislerde kullanılan enstrümantasyon ve kontrol sistemlerine yönelik saldırılarla somut bir risk oluşturmaktadır. Bu sistemler, reaktörlerin operasyonel süreçlerini kontrol eder ve herhangi bir saldırı, ciddi güvenlik risklerine yol açabilir. Türkiye, bu sistemlerin güvenliğini sağlamak için gelişmiş güvenlik protokolleri uygulamakta ve siber güvenlik stratejilerini ulusal düzeyde geliştirmektedir.
- Türkiye, nükleer tesislerin siber güvenliğini artırmak için uluslararası iş birliklerini güçlendirmektedir. UAEA gibi kuruluşlarla yapılan iş birlikleri, siber tehditlere karşı en iyi uygulamaların benimsenmesini sağlamaktadır. Bunun yanı sıra Türkiye'nin Ulusal Siber Olaylara Müdahale Merkezi (USOM), nükleer tesislerin dijital altyapılarında olası tehditlere karşı sürekli izleme sağlamaktadır.
- Türkiye'nin nükleer enerji politikaları; enerji güvenliği, ekonomik kalkınma ve çevresel sürdürülebilirlik hedefleri doğrultusunda şekillenmektedir. Akkuyu NGS'nin tamamlanması, bu hedeflere ulaşmada önemli bir adım olsa da gelecekteki projelerin başarısı için bir dizi stratejik yaklaşım benimsenmelidir.
- Halkın nükleer enerji projelerine yönelik algısı, bu politikaların başarısını etkileyen önemli bir faktördür. Türkiye, halkın güvenini artırmak için bilinçlendirme kampanyaları ve şeffaf iletişim stratejileri geliştirmelidir. Çernobil ve Fukuşima gibi kazalar, halkın nükleer enerjiye yönelik endişelerini artırmış olsa da Türkiye'nin uluslararası standartlara uygun güvenlik protokolleri uygulaması bu algıyı değiştirebilir.
- Yerli teknolojilerin geliştirilmesi, Türkiye'nin nükleer enerji politikalarında sürdürülebilirliği sağlamak için kritik bir öneme sahiptir. Yerli üretimin teşvik edilmesi hem maliyetleri azaltacak hem de Türkiye'nin teknik kapasitesini artıracaktır. Bunun yanı sıra yenilenebilir enerji kaynaklarıyla nükleer enerji arasında bir entegrasyon sağlanması, enerji portföyünü çeşitlendirecek ve arz güvenliğini artıracaktır.
- Nükleer enerji; Türkiye'nin enerji güvenliği, millî güvenlik, ekonomik kalkınma ve çevresel sürdürülebilirlik hedeflerini destekleyen stratejik bir araç olarak öne çıkmaktadır. Akkuyu NGS başta olmak üzere mevcut ve planlanan projeler, enerji bağımsızlığını artırarak Türkiye'nin uluslararası arenadaki jeopolitik konumunu güçlendirme potansiyeline sahiptir. Ancak bu projelerin başarısı yalnızca teknolojik altyapıya değil, aynı zamanda halkın güveninin artırılması, uluslararası standartlara uyum ve güçlü bir güvenlik çerçevesine dayanmaktadır. Türkiye'nin; yerli teknolojilerin geliştirilmesi, enerji diplomasisinin güçlendirilmesi ve sürdürülebilir politikalar oluşturulması yönündeki çabaları, nükleer enerjiyi stratejik bir avantaj olarak kullanmasına olanak sağlayacaktır. Bu rapor, Türkiye'nin nükleer enerji stratejilerinde karşılaşabileceği zorluklara rağmen bu alandaki potansiyelin etkin bir şekilde değerlendirilmesi için bir yol haritası sunmaktadır.

GİRİŞ

21. yüzyılda enerji güvenliği; ülkelerin ekonomik büyüme, ulusal güvenlik ve sürdürülebilir kalkınma hedeflerini destekleyen stratejik bir gereklilik hâline gelmiştir. Artan enerji talebi, çevresel kaygılar ve enerji kaynaklarının jeopolitik önemi, enerji politikalarını yalnızca ekonomik bir konu olmaktan çıkararak çok boyutlu bir strateji hâline getirmiştir. Bu bağlamda nükleer enerji; düşük karbon emisyonları, yüksek enerji yoğunluğu ve uzun vadeli enerji arz güvenliği sağlamasıyla öne çıkan bir seçenek olarak değerlendirilmektedir.

Nükleer enerji, yalnızca enerji üretim kapasitesini artırmakla kalmaz; aynı zamanda teknolojik gelişim, ekonomik kalkınma ve uluslararası alanda stratejik güç elde etme açısından da önemli fırsatlar sunar. Ancak bu fırsatların gerçeğe dönüşebilmesi, nükleer tesislerin emniyetini sağlamaktan geçer. Modern dünyada nükleer tesisler yalnızca fiziksel tehditlerle değil, aynı zamanda siber saldırılar, tedarik zinciri güvenliği ve içeriden kaynaklanan tehditlerle de karşı karşıyadır. Geçmişte yaşanan Stuxnet, Kudankulam ve Natanz saldırıları gibi örnekler, nükleer tesislerin emniyetinin yalnızca ulusal düzeyde değil, küresel bir perspektifle de ele alınması gerektiğini açıkça göstermiştir.

Türkiye de enerji ihtiyacını karşılamak, dışa bağımlılığını azaltmak ve enerji arz güvenliğini artırmak amacıyla nükleer enerji projelerine yönelmiş durumdadır. Bu bağlamda Türkiye'nin nükleer enerji projeleri olan Akkuyu NGS ve diğer potansiyel santral projeleri, enerji sektöründe yeni bir dönemi temsil etmektedir. Ancak bu projelerin başarısı, yalnızca teknik altyapı ve ekonomik fizibiliteyle sınırlı değildir. Güvenlik, bu projelerin sürdürülebilirliği ve uluslararası kabulü için temel bir unsurdur. Nükleer tesislerin emniyeti; fiziksel koruma önlemlerinden başlayarak siber güvenlik protokollerine, tedarik zinciri denetimlerinden uluslararası standartların uygulanmasına kadar geniş bir çerçevede ele alınmalıdır.

Türkiye'nin nükleer enerji stratejisi, ulusal güvenlik perspektifinden değerlendirildiğinde hem iç hem de dış tehditleri önleyici ve riskleri minimize eden bir yaklaşıma ihtiyaç duymaktadır. Siber saldırıların

artan karmaşıklığı yalnızca teknik altyapıyı değil, aynı zamanda insan faktörünü de hedef alarak güvenlik açıklarını artırmaktadır. Bu nedenle hem çalışanların farkındalığını artırmaya yönelik eğitim programları hem de teknolojik sistemlerin sürekli güncellenmesi gibi önlemler hayati önem taşımaktadır. Örneğin, siber güvenlik kültürünün tüm çalışanlar tarafından benimsenmesi, insan hatalarından kaynaklanan tehditlerin azaltılmasında kilit bir rol oynar. Ayrıca dijitalleşmenin nükleer tesislerdeki güvenlik dinamiklerini değiştirdiği bir dönemde, siber tehditlere karşı dayanıklı bir altyapı oluşturulması kritik hâle gelmiştir. Bu durum yalnızca mevcut teknolojilerin güncellenmesini değil, aynı zamanda aktif savunma stratejilerinin geliştirilmesini de gerektirir. Yapay zekâ tabanlı tehdit algılama sistemleri ve gerçek zamanlı izleme mekanizmaları, nükleer tesislerin karşılaşabileceği potansiyel tehditleri önceden tespit etme kapasitesine sahiptir. Ancak bu tür çözümler yalnızca teknolojik değil, aynı zamanda organizasyonel bir dönüşümü de zorunlu kılar.

Tedarik zinciri güvenliği, nükleer enerji projelerinin güvenliğinde giderek daha önemli bir konu hâline gelmektedir. Nükleer tesislerde kullanılan ekipman ve yazılımlar genellikle uluslararası tedarik zincirlerinden temin edilir ve bu süreçlerde herhangi bir güvenlik açığı, tüm sistemin tehlikeye girmesine neden olabilir. Bu nedenle tedarikçi firmaların sıkı denetimlere tabi tutulması ve uluslararası güvenlik standartlarına uygunluğunun sağlanması şarttır. Tedarik zinciri güvenliğinin sağlanması yalnızca mevcut tehditleri bertaraf etmekle kalmaz, aynı zamanda gelecekteki risklere karşı da proaktif bir koruma sağlar.

Nükleer enerji projelerinin bir diğer önemli boyutu, uluslararası iş birliği ve standartlaşmadır. Siber tehditlerin sınır tanımayan doğası, uluslararası düzeyde koordinasyonu ve bilgi paylaşımını zorunlu kılar. UAEA gibi kuruluşlar, nükleer emniyet standartlarının oluşturulmasında kritik bir rol oynamaktadır. Türkiye, bu tür uluslararası iş birliklerinden faydalanarak nükleer tesislerinin güvenliğini küresel standartlara uygun bir şekilde geliştirebilir. Aynı zamanda bölgesel iş birlikleri ve ortak tehdit izleme mekanizmaları, siber tehditlere karşı erken uyarı ve savunma kapasitesini artırabilir.

Sonuç olarak nükleer enerji, Türkiye'nin enerji politikalarında bir dönüm noktasıdır ve bu enerji kaynağından en üst düzeyde fayda sağlanabilmesi için nükleer emniyet konularına öncelik verilmelidir. Bu rapor, Türkiye'nin nükleer enerji stratejisini siber güvenlik perspektifinden analiz ederek enerji altyapısının korunmasına yönelik öneriler sunmaktadır. Nükleer enerji projelerinin sadece ekonomik ve teknik açıdan değil, aynı zamanda emniyet boyutunda da sürdürülebilir bir çerçeveye oturtulması, bu projelerin başarısını belirleyecek en önemli faktörlerden biridir. Türkiye'nin bu alandaki stratejik hedeflerine ulaşabilmesi; ulusal güvenlik, ekonomik büyüme ve uluslararası iş birliği arasında dengeli bir yaklaşımı benimsemesiyle mümkün olacaktır. Bu bağlamda nükleer enerji projelerinin yönetimi ve güvenliği, Türkiye'nin enerji bağımsızlığı vizyonunun temel taşlarından biri olarak ele alındığında başarılı olunacaktır.

BÖLÜM 1

NÜKLEER ENERJİNİN STRATEJİK ÖNEMİ

Dünyada Nükleer Enerji Görünümü

Aralık 2023 sonu itibarıyla dünya genelinde faaliyette olan nükleer enerji kapasitesi, 31 ülkedeki 411 reaktör tarafından sağlanan 369,6 GW(e) olarak kaydedilmiştir (bk. Tablo 1).[1] Nükleer enerji kapasitesi son 10 yılda istikrarlı bir seviyede kalmış olup 2013 yılının başından bu yana şebekeye 69,8 GW(e) ek nükleer kapasite bağlanmıştır. Bu kapasite artışının %79'undan fazlası Asya'da gerçekleşmiştir. Asya'da bu dönemde toplam 55,4 GW(e) kapasite (54 reaktör) şebekeye bağlanmıştır. Bölgenin büyümesine liderlik eden Çin, 2013 yılından bu yana şebekeye 40,02 GW(e) yeni kapasite eklemiştir.

2023 yılında nükleer elektrik üretiminde ilk üç sırayı ABD, Çin ve Fransa almıştır. Dünyanın en çok nükleer enerji santrallerine sahip olan ABD, toplam nükleer elektrik üretiminin %31'ini oluşturarak 779,2 teravatsaat (TWh) üretmiştir. Çin, %16 (406,5 TWh) ile ikinci sırada yer alarak üst üste dört yıl Fransa'yı geride bırakmıştır. Fransa ise 323,8 TWh üreterek küresel toplamın %13'üne katkıda bulunmuştur.

Türkiye yapım aşamasında olan 4 yeni reaktörüyle Çin (24 reaktör) ve Hindistan'ın (8 reaktör) yapım aşamasında bulunan reaktörlerinden sonra üçüncü sırada gelmektedir. Ayrıca faaliyette olan reaktörlerin yaşları incelendiğinde 234 reaktör, 35 ve üzeri yaşta olup ömürlerini tamamlamak üzeredir.

Tablo 1: Aralık 2023 İtibarıyla Nükleer Reaktörler ve Nükleer Enerji Payı[1]

Ülke	İşletimdeki Reaktör Sayısı	Net Kapasite [MW(e)]	Yapım Aşamasındaki Reaktör Sayısı	Yapım Aşamasındaki Kapasite [MW(e)]	Nükleer Elektrik Üretimi (TWh)	Toplam Elektrik İçindeki Pay (%)
ABD	**93**	**95.835**	1	1.117	**779,2**	18,5
Fransa	56	61.370	1	1.630	323,8	**64,8**
Çin	55	53.152	**24**	**24.948**	406,5	4,9
Rusya	37	27.727	3	2.700	204	18,4
Güney Kore	26	25.825	2	2.680	171,6	31,5
Kanada	19	13.699	-	-	83,5	13,7
Hindistan	19	6.290	8	6.028	44,6	3,1
Ukrayna	15	13.107	2	2.070	-	-

Japonya	12	11.046	2	2.653	77,5	5,5
Birleşik Krallık	9	5.883	2	3.260	37,3	12,5
İspanya	7	7.123	-	-	54,4	20,3
Çekya	6	3.934	-	-	28,7	40
Pakistan	6	3.262	-	-	22,4	17,4
İsveç	6	6.944	-	-	46,6	28,6
Belçika	5	3.908	-	-	31,3	41,2
Finlandiya	5	4.394	-	-	32,8	42
Slovakya	5	2.308	1	440	17	61,3
Macaristan	4	1.916	-	-	15,1	48,8
İsviçre	4	2.973	-	-	23,4	32,4
Arjantin	3	1.641	1	25	9	6,3
BAE	3	4.011	1	1.310	31,2	19,7
Belarus	2	2.220	-	-	11	28,6
Brezilya	2	1.884	1	1.340	13,7	2,2
Bulgaristan	2	2.006	-	-	15,5	40,5
Meksika	2	1.552	-	-	12	4,9
Romanya	2	1.300	-	-	10,3	18,9
Güney Afrika	2	1.854	-	-	8,2	4,4
Ermenistan	1	416	-	-	2,5	31,1
İran	1	915	1	974	6,1	1,7
Hollanda	1	482	-	-	3,8	3,4
Slovenya	1	688	-	-	5,3	36,8
Bangladeş	-	-	2	2.160	-	-
Mısır	-	-	3	3.300	-	-
Türkiye	**-**	**-**	**4**	**4.800**	-	-

Türkiye'de Enerji Görünümü

Türkiye, enerji talebindeki artışı karşılamak ve enerji arz güvenliğini sağlamak için enerji sektörünü çeşitlendirme, altyapıyı modernize etme ve yerli kaynakların kullanımını artırma hedefleri doğrultusunda politika ve projeler geliştirmektedir. Türkiye Ulusal Enerji ve Maden Politikası; enerji arz güvenliği, yerli üretim ve öngörülebilir bir piyasa yapısı oluşturma gibi stratejik hedefler üzerine kurulmuştur.

Türkiye'nin enerji üretiminde çeşitlilik sağlama hedefi, kaynakların dengeli bir şekilde kullanımını teşvik etmektedir. Fosil yakıtlar hâlâ önemli bir yer tutarken yenilenebilir enerji kaynakları Türkiye'nin üretim kapasitesinde giderek daha büyük bir pay almaktadır. Özellikle hidrolik, rüzgâr ve güneş enerjisi projeleri ön plana çıkmaktadır. Tablo 2, Türkiye kurulu gücünün birincil enerji kaynaklarına göre son 15 yıldaki gelişimini göstermektedir.

Tablo 2: Türkiye Kurulu Gücünün Enerji Kaynaklarına Göre Gelişimi (GW)[2]

Kaynak Türü	2008	2013	2018	2024
Termik	27,54	38,37	46,08	46,8
Hidrolik	13,8	22,3	28,3	32,2
Jeotermal	0,03	0,3	1,3	1,7
Rüzgâr	0,3	2,7	7	12,6
Güneş	-	-	5	19,6
Biyokütle	0,06	0,23	0,82	2,1
TOPLAM	**41,73**	**63,9**	**88,5**	**115**

Türkiye'nin enerji politikalarının odak noktaları şunlardır:

- **Arz güvenliği:** Enerji kaynaklarının ve tedarikçi ülkelerin çeşitlendirilmesi, doğal gaz ve petrol depolama kapasitesinin artırılması ve enerji altyapısının iyileştirilmesi.
- **Yerli üretim:** Yenilenebilir enerji, yerli kömür ve nükleer enerji kullanımının artırılması, ithalata olan bağımlılığın azaltılması.
- **Karbon emisyonları:** 2053 net sıfır karbon hedefi doğrultusunda yenilenebilir enerji projelerinin genişletilmesi, enerji verimliliği ve hidrojen gibi düşük karbonlu teknolojilere geçiş.

Türkiye enerji sektörünü hem iç tüketimi karşılamak hem de bölgesel bir enerji ticaret merkezi hâline gelmek için yeniden yapılandırmaktadır. Bu doğrultuda enerji arzında sürdürülebilirlik ve ekonomik kalkınma öncelikli hedefler arasındadır.

Türkiye'nin Nükleer Enerjiye Geçiş Sürecinin Tarihsel Gelişimi

Türkiye'nin nükleer enerjiye geçiş süreci, enerji güvenliğini sağlama ve enerji arzında çeşitliliği artırma çabalarının bir parçası olarak başlamıştır. Bu süreç, Türkiye'nin artan enerji ihtiyacını karşılamak, ekonomik büyümeyi desteklemek ve dışa bağımlılığı azaltmak için geliştirilmiştir. Nükleer enerjiye geçiş süreci, 1950'lerden günümüze kadar süren uzun ve zorlu bir yolculuğu kapsamaktadır.[3]

Türkiye'nin nükleer enerjiyle ilgili ilk çalışmaları, 1955 yılında UAEA'nın kurulmasıyla hız kazandı. 1956'da Türkiye Atom Enerjisi Kurumu (TAEK) kurularak nükleer enerji alanında bilimsel ve teknik çalışmalar başlatıldı. Bu dönemde Türkiye'nin temel amacı, nükleer enerji teknolojilerini öğrenmek ve altyapı oluşturmak oldu.

1960'larda Türkiye, nükleer enerji alanında uluslararası iş birliğini artırarak teknik bilgi birikimi sağlamayı hedefledi. ABD ve Batı Avrupa ülkeleriyle yapılan anlaşmalar sayesinde, Türk mühendis ve bilim insanları nükleer enerji alanında eğitim aldı. Ülkemizde ilk reaktör 1962 yılında 1 MW güçle araştırma reaktörü (TR-1) olarak Küçükçekmece'de açıldı.

1970'lerde Türkiye, ilk nükleer enerji santralini kurmayı planladı. Ancak ekonomik zorluklar ve siyasi istikrarsızlık nedeniyle bu projeler gerçekleştirilemedi. Sinop ve Akkuyu'da planlanan santral projeleri, maliyetler ve teknik kapasite eksiklikleri nedeniyle ertelendi. İTÜ TRIGA Mark-II araştırma reaktörü, 11 Mart 1979 tarihinde işletmeye açıldı.

1980'lerde Türkiye, Akkuyu'da bir nükleer enerji santrali kurma çalışmalarını yeniden başlattı. Ancak bu dönemde de siyasi istikrarsızlık, finansman eksikliği ve halkın nükleer enerjiye olan güven eksikliği projelerin ilerlemesini engelledi. Küçükçekmece'de bulunan araştırma reaktörüne daha yüksek güçte ikinci bir reaktör (TR-2) yapılarak 1984 yılında 5 MW güçle hizmete alındı.

1990'larda Türkiye'nin nükleer enerji planları, ekonomik krizler ve uluslararası politik baskılar nedeniyle bir kez daha ertelendi. Bu dönemde, yenilenebilir enerji kaynaklarına yönelim artırılarak nükleer enerji ikinci planda bırakıldı.

2000'li yılların başında, artan enerji talebi ve ithal enerjiye bağımlılık, nükleer enerjiyi yeniden Türkiye'nin enerji politikasının merkezine taşıdı. Enerji çeşitliliğini artırmak ve dışa bağımlılığı azaltmak amacıyla nükleer enerji projelerine öncelik verildi.

Türkiye'nin nükleer enerjiye geçiş sürecinde en somut adım, Akkuyu NGS'nin inşasıyla atılmıştır. 2010 yılında Rusya ile yapılan anlaşma kapsamında başlatılan bu proje, Türkiye'nin enerji güvenliği stratejisinde önemli bir kilometre taşıdır. Santral, tamamlandığında 4,8 GW (4x1.200 MW) kapasiteyle Türkiye'nin elektrik ihtiyacının %10'unu (~35 TWh) karşılayacaktır.[4] Akkuyu NGS'nin yanı sıra Sinop ve İğneada'da planlanan nükleer enerji projeleri, Türkiye'nin nükleer kapasitesini artırma hedeflerini yansıtmaktadır.[5] Türkiye, nükleer enerji projelerinde hem yerli kapasiteyi geliştirmeye hem de uluslararası iş birliklerini artırmaya önem vermektedir. Türk mühendislerin projelere entegrasyonu ve uluslararası standartlara uyum, bu süreçte temel stratejiler arasında yer almaktadır.

Türkiye'nin Nükleer Enerji Politikalarının Stratejik Hedefleri

Türkiye'nin nükleer enerji politikaları; enerji arz güvenliğini sağlama, ekonomik büyümeyi destekleme ve enerji bağımsızlığını artırma hedeflerine dayanır. Bu politikalar, aynı zamanda teknolojik kalkınma, çevresel sürdürülebilirlik ve uluslararası iş birliklerini geliştirme stratejilerini de içermektedir.

Türkiye, nükleer enerji projelerini enerji politikalarının temel bir unsuru hâline getirerek uzun vadeli kalkınma hedeflerine ulaşmayı amaçlamaktadır.

a. Teknolojik kapasitenin geliştirilmesi:

Nükleer enerji, yüksek teknoloji gerektiren bir enerji üretim yöntemi olarak yalnızca enerji sektörüne değil, aynı zamanda bir ülkenin genel teknolojik kapasitesine ve bilgi altyapısına da önemli katkılar sunar. Türkiye'nin nükleer enerji politikalarının temel stratejik hedeflerinden biri, bu teknolojik kapasiteyi geliştirmek ve sanayinin niteliklerini yükseltmektir. Bu hedef, enerji arz güvenliği sağlamanın ötesinde; bilim, teknoloji ve sanayi alanlarında daha geniş bir dönüşümü desteklemeyi amaçlar.

Teknolojik kapasitenin geliştirilmesi; yerli mühendislik ve teknik bilgi birikiminin artırılmasını gerektirir. Türkiye, Akkuyu NGS gibi projelerle nükleer enerji teknolojisinin temel bileşenlerini öğrenmekte ve bu alanda kendi insan kaynağını yetiştirmektedir. Proje kapsamında Türk mühendislerin ve teknisyenlerin yurt dışında eğitim alması ve uluslararası standartlara uygun teknik bilgi edinmesi, yerli kapasitenin geliştirilmesinde kritik bir rol oynamaktadır.[6] Ayrıca nükleer enerji teknolojisinin geliştirilmesi yalnızca enerji sektöründe değil, savunma sanayisi ve sağlık teknolojileri gibi diğer kritik alanlarda da yan faydalar yaratabilir. Radyasyon teknolojilerinin medikal alanda kullanımı, ileri malzeme teknolojilerinin geliştirilmesi ve reaktör tasarımı gibi alanlar, nükleer enerji projelerinden elde edilen teknik bilgi birikimiyle paralel olarak gelişebilir. Bu, Türkiye'nin teknoloji üretim kapasitesini artırırken aynı zamanda küresel rekabet gücünü de yükseltecektir.

Bir diğer önemli husus, yerli üretimin teşvik edilmesidir. Nükleer enerji projelerinde kullanılan ekipmanların ve malzemelerin yerli üretimle sağlanması, Türkiye'nin sanayi altyapısını güçlendirme potansiyeline sahiptir. Bu, aynı zamanda dışa bağımlılığı azaltarak enerji projelerinde daha sürdürülebilir bir yapının oluşmasına katkı sağlar. Akkuyu NGS projesinde yerli tedarikçilerin dâhil edilmesi ve bu projeler aracılığıyla küçük ve orta ölçekli işletmelerin desteklenmesi, sanayinin daha geniş bir teknolojik tabana yayılmasına olanak tanımaktadır.[7]

Bu bağlamda nükleer enerji projeleri, Türkiye'nin teknolojik kapasitesini geliştirme hedefinde yalnızca bir araç değil, aynı zamanda ulusal kalkınmanın katalizörü olarak değerlendirilebilir. Bu projeler, bilimsel araştırma ve yerli sanayinin modernizasyonu için uzun vadeli bir fırsat sunmaktadır. Teknolojik kapasitenin artırılması, Türkiye'nin nükleer enerji politikalarının başarılı bir şekilde uygulanmasının temel taşlarından biridir.

b. Ekonomik kalkınmanın desteklenmesi:

Nükleer enerji politikalarının bir diğer stratejik hedefi, ekonomik kalkınmayı teşvik etmek ve ülke ekonomisine çok yönlü katkılar sağlamaktır. Nükleer enerji projeleri yalnızca enerji üretimini artırmakla kalmayıp geniş bir ekonomik etki alanı oluşturarak istihdam, sanayi üretimi ve ticaret hacmini artırma potansiyeline de sahiptir. Türkiye, Akkuyu NGS ve gelecekte hayata geçirilecek diğer nükleer santral projeleriyle bu hedefe yönelik somut adımlar atmaktadır.

Nükleer enerji projelerinin doğrudan ekonomik etkilerinden biri, enerji üretim maliyetlerini düşürerek sanayi ve hizmet sektörlerindeki rekabetçiliği artırmasıdır. Türkiye, ithal fosil yakıtlar yerine nükleer enerjiyi enerji portföyüne ekleyerek enerji maliyetlerini kontrol altına almayı ve bu alandaki dışa bağımlılığını azaltmayı hedeflemektedir. Akkuyu NGS, tamamlandığında Türkiye'nin enerji ithalatını önemli ölçüde düşürerek cari açığın azalmasına katkı sağlayacaktır. Bu durum yalnızca enerji sektöründe değil, genel ekonomik istikrarın sağlanmasında da kritik bir role sahiptir.

Ekonomik kalkınma açısından bir diğer önemli boyut, nükleer enerji projelerinin uzun vadeli getirisidir. Nükleer enerji santralleri, yüksek başlangıç maliyetlerine rağmen uzun ömürlü ve düşük işletme maliyetlerine sahiptir. Bu da enerji üretiminde maliyetlerin zamanla azalmasını sağlayarak ekonomik faydaların sürdürülebilirliğini artırır. Uzun vadeli ekonomik faydaların yanı sıra nükleer enerji projeleri, bölgesel kalkınmaya da katkı sağlar. Proje bölgelerinde altyapı yatırımları, eğitim programları ve yerli ekonominin canlandırılması gibi etkiler, projelerin kalkınma üzerindeki olumlu etkilerini artırmaktadır.

Uluslararası ticaret ve yatırım açısından da nükleer enerji projeleri, Türkiye'ye önemli fırsatlar sunmaktadır. Akkuyu NGS gibi projeler, uluslararası ortaklıklarla finanse edilmekte ve bu ortaklıklar Türkiye'nin ekonomik diplomasi kapasitesini artırmaktadır. Yatırımların çeşitlendirilmesi ve uluslararası teknoloji transferi, Türkiye'nin küresel ekonomideki konumunu güçlendirmektedir.

c. Karbon sıfır hedeflerine ulaşma:

Paris İklim Anlaşması'na taraf olan Türkiye, karbon sıfır hedeflerine ulaşmak ve karbon emisyonlarını azaltmak için kapsamlı politikalar benimsemektedir. Bu bağlamda nükleer enerji, temiz enerji üretimi sağlayarak Türkiye'nin çevresel hedeflerine ulaşmasında kritik bir rol oynamaktadır.

Nükleer enerji, elektrik üretiminde doğrudan karbon salınımı yapmaması nedeniyle fosil yakıtlar gibi karbon yoğun enerji kaynaklarına bir alternatif sunar. Türkiye'nin enerji üretim portföyünde yenilenebilir enerji kaynakları ile birlikte kullanılacak nükleer enerji, enerji arz güvenliğini sağlarken aynı zamanda karbon salınımını da önemli ölçüde azaltacaktır. Akkuyu NGS'nin tamamlanmasıyla yılda yaklaşık 35 milyon ton karbon emisyonunun engellenmesi beklenmektedir.[8] Bu rakam, Türkiye'nin karbon sıfır hedefleri doğrultusunda enerji sektöründe atılan en önemli adımlardan biridir.

Türkiye'nin karbon sıfır hedeflerine ulaşma stratejisinde, nükleer enerji projelerinin istikrarlı ve sürekli enerji üretme kapasitesi, yenilenebilir enerji kaynaklarının üretim dalgalanmalarını dengeleyici bir rol oynar. Rüzgâr ve güneş gibi yenilenebilir enerji kaynakları, hava koşullarına bağlı olarak değişkenlik gösterirken nükleer enerji, kesintisiz enerji sağlama yeteneğiyle bu boşluğu giderir. Bu durum, karbon sıfır enerji üretiminin sürekliliğini sağlayarak enerji altyapısında karbonsuzlaşmayı destekler.

Nükleer enerji, Türkiye'nin enerji sektöründe karbon emisyonlarını azaltma hedefine ulaşırken aynı zamanda sanayi ve ulaşım gibi diğer yüksek karbon emisyonlu sektörlere de dolaylı katkılar sağlar. Elektrifikasyon stratejileri ile nükleer enerji kullanılıp bu sektörlerdeki karbon salınımı azaltılarak

daha çevre dostu üretim süreçleri teşvik edilir. Ayrıca nükleer enerji projeleri, çevresel etkilerin minimize edilmesi için ileri teknoloji kullanımı ve sıkı denetim mekanizmaları gerektirir. Türkiye, bu projelerde uluslararası standartlara uygun çevre yönetim sistemleri geliştirerek karbon sıfır hedeflerini destekleyecek bir altyapı oluşturmayı amaçlamaktadır.

Ek olarak Türkiye'nin karbon sıfır hedeflerine ulaşma çabaları, uluslararası iş birlikleri ve finansal mekanizmalarla güçlendirilmektedir. Yeşil finansman ve karbon ticareti gibi uygulamalar, nükleer enerji projelerinin çevresel hedeflerle uyumlu bir şekilde geliştirilmesine olanak tanır.

d. Uluslararası iş birliklerinin güçlendirilmesi:

Nükleer enerji, karmaşık teknolojik altyapılar ve yüksek düzeyde düzenlemeler gerektiren bir alan olduğu için uluslararası iş birliğini kaçınılmaz kılar. Türkiye, nükleer enerji projelerinde teknolojik bilgi transferi, güvenlik standartlarına uyum ve finansal kaynaklara erişim sağlamak amacıyla uluslararası iş birliklerini güçlendirmeye büyük önem vermektedir. Bu iş birlikleri yalnızca enerji üretimiyle sınırlı kalmayıp ekonomik kalkınma, diplomatik ilişkiler ve küresel enerji güvenliği çerçevesinde geniş bir etki alanına da sahiptir.

Türkiye'nin nükleer enerji alanındaki uluslararası iş birlikleri, büyük ölçüde teknoloji transferi ve bilgi paylaşımına odaklanmaktadır. Akkuyu NGS projesi, bu bağlamda Türkiye'nin Rusya ile geliştirdiği önemli bir stratejik ortaklığı temsil etmektedir. Bu proje kapsamında Rusya; teknik bilgi, mühendislik desteği ve finansman sağlayarak Türkiye'nin nükleer enerji kapasitesini artırmaya katkıda bulunmaktadır. Bunun yanı sıra Türk mühendis ve teknisyenlerin yurt dışında eğitim alması, uzmanlık seviyesini artırarak uzun vadeli bilgi transferine olanak tanımaktadır.

UAEA, Türkiye'nin nükleer enerji projelerinde önemli bir rol oynamaktadır.[9] Türkiye, UAEA ile düzenli iş birliği içinde çalışarak projelerini uluslararası güvenlik ve çevre standartlarına uygun bir şekilde yürütmektedir. Bu iş birliği yalnızca teknik denetim ve düzenlemelerle sınırlı kalmamakta, aynı zamanda nükleer enerjinin barışçıl kullanımına olan bağlılığın pekiştirilmesine de katkı sağlamaktadır. UAEA ile yürütülen projeler, Türkiye'nin nükleer enerji konusundaki uluslararası güvenilirliğini artırmaktadır.

Türkiye'nin nükleer enerji projelerinde uluslararası iş birliğini güçlendirmesi, küresel enerji güvenliği çerçevesinde de değerlendirilmektedir. Enerji arz güvenliği, ülkeler arası dayanışmayı gerektiren bir konudur ve Türkiye, nükleer enerji projelerini bu dayanışmanın bir aracı olarak kullanmaktadır. Türkiye'nin bölgesel enerji projelerine katkısı yalnızca kendi enerji ihtiyaçlarını karşılamayı değil, aynı zamanda çevre ülkelerle karşılıklı bağımlılığa dayalı bir enerji ağı oluşturmayı da hedeflemektedir.

Türkiye'nin Nükleer Enerji Politikalarının Ekonomik ve Sosyal Etkileri

Türkiye'nin nükleer enerji politikaları yalnızca enerji arz güvenliği ve ekonomik kalkınma açısından değil, aynı zamanda sosyal etkileriyle de dikkat çekmektedir. Nükleer enerji projelerinin ekonomik

büyümeyi teşvik etmesi, istihdam yaratması ve teknoloji transferine olanak sağlaması bu politikaların olumlu yanlarını oluştururken halkın nükleer enerjiye karşı algısı ve sosyal kabul düzeyi ise önemli bir zorluk olarak ortaya çıkmaktadır.

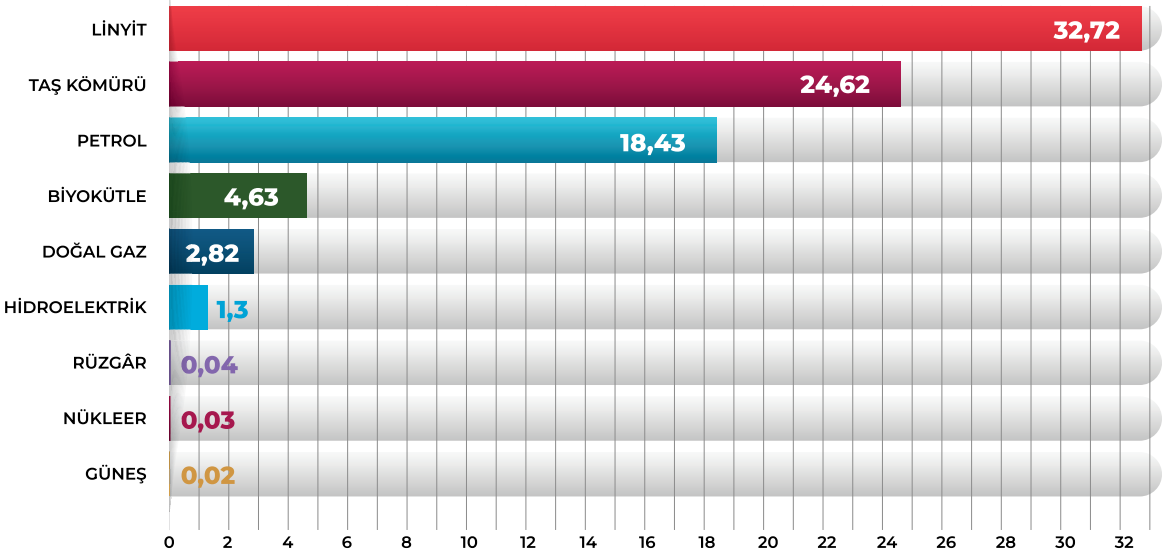
Nükleer enerji, enerji üretim maliyetlerini düşürerek Türkiye'nin ekonomik büyümesine katkıda bulunabilir. Akkuyu NGS'nin tamamlanması, Türkiye'nin yıllık enerji ithalat maliyetlerini azaltarak ekonomik kalkınmayı destekleyecektir. Enerji arz güvenliği sağlandığında, sanayi ve hizmet sektörlerindeki enerji maliyetleri de düşecektir.

Nükleer enerji projeleri, yüksek sermaye yatırımları gerektirir ve bu projeler hem yerli hem de uluslararası yatırımcıları çekebilir. Akkuyu NGS'nin toplam maliyetinin yaklaşık 22 milyar doların üzerinde olması, bu projelerin ekonomik boyutunu ve yaratacağı finansal hareketliliği göstermektedir.[10] Nükleer enerji projeleri, yerli sanayinin gelişimini destekler. Türkiye, Akkuyu NGS projesinde kullanılan ekipmanların ve malzemelerin bir kısmını yerli üretimle karşılayarak sanayi altyapısını güçlendirmeyi hedeflemektedir. Bu, yerli üreticiler için yeni fırsatlar yaratmaktadır.

Nükleer enerji projeleri hem inşaat hem de işletme aşamalarında binlerce kişiye istihdam sağlar. Akkuyu NGS'de yaklaşık 4.000 kişinin doğrudan istihdam edilmesi planlanmaktadır.[11] Bu hem teknik hem de idari kadrolar için yeni iş imkânları anlamına gelir. Türkiye, nükleer enerji projeleriyle teknik kapasitesini artırmayı ve uzmanlaşmış bir iş gücü yaratmayı hedeflemektedir. Rusya ile yapılan anlaşmalar çerçevesinde, Türk mühendisler ve teknisyenler yurt dışında eğitim alarak projelere dâhil edilmektedir. Bu, teknik bilgi birikimini artırmaktadır.

Nükleer enerjiye yönelik halkın algısı, Çernobil ve Fukuşima gibi kazalar nedeniyle genellikle olumsuzdur. Fakat nükleer enerji kazalarının ölüm oranları, diğer enerji üretim yöntemlerine kıyasla oldukça düşüktür (bk. Grafik 1). Çernobil kazası, şimdiye kadar en ciddi nükleer kaza olarak kabul edilse de doğrudan radyasyona bağlı ölümler sınırlıdır. Dünya Sağlık Örgütü (DSÖ) ve Birleşmiş Milletler (BM) verileri, bu kazadan kaynaklanan ölümlerin varsayıldığı kadar yüksek olmadığını göstermektedir.[12] Fukuşima kazasında, üç reaktörün erimesine rağmen radyasyona bağlı hiçbir ölüm kaydedilmemiştir. Bunun yerine, geniş çaplı ve gereksiz tahliyeler sonucunda birçok kişinin hayatını kaybettiği tahmin edilmektedir.[13] Bu, kazaların değil, yanlış yönetim ve panik kararlarının sonuçlarını vurgulamaktadır. Araştırmalar düşük seviyelerde radyasyonun ciddi bir sağlık riski oluşturmadığını göstermektedir. Colorado gibi doğal radyasyon seviyelerinin yüksek olduğu bölgelerde yaşayan insanlar, daha düşük radyasyon seviyelerine sahip bölgelere kıyasla daha yüksek kanser oranları sergilememektedir.[14] Bu durum, radyasyona karşı duyulan korkunun çoğunlukla yanlış algılara dayandığını ortaya koymaktadır.

Grafik 1: Enerji Santrallerinde TWh Başına Ölüm Oranları[15,16,17]



Türkiye, nükleer enerjiye yönelik yanlış algıyı değiştirmek için kamuoyunu bilinçlendirme kampanyaları düzenlemekte ve nükleer enerjinin avantajlarını anlatmaktadır. Halkın projelere katılımı ve şeffaflık, güvenin artırılmasında kritik bir rol oynamaktadır. Nükleer enerji projeleri, radyasyon güvenliği ve atık yönetimi gibi konularda toplumsal endişelere yol açabilir. Türkiye, bu endişeleri gidermek için UAEA standartlarına uygun güvenlik protokollerini uygulamakta ve atık yönetimi konusunda uluslararası uygulamaları benimsemektedir.

Türkiye'nin Jeopolitik Konumu ve Nükleer Enerjinin Bu Konuma Katkıları

Türkiye'nin jeopolitik konumu; Asya, Avrupa ve Orta Doğu'yu birbirine bağlayan stratejik bir kesişim noktasında yer alması nedeniyle büyük bir öneme sahiptir. Enerji arz ve transit yollarının merkezinde yer alan Türkiye, bu avantajını enerji politikalarında güçlendirmeyi ve bölgesel güç dengesinde belirleyici bir rol oynamayı hedeflemektedir. Nükleer enerji, Türkiye'nin jeopolitik avantajlarını artırarak enerji güvenliği, ekonomik kalkınma ve uluslararası etkisini artırma hedeflerinde kritik bir araç olarak öne çıkmaktadır.

Türkiye, dünya enerji rezervlerinin büyük bir kısmını barındıran Orta Doğu, Hazar ve Rusya bölgelerinin Avrupa'ya açılan kapısıdır. Doğal gaz ve petrol boru hatlarının geçiş noktası olan Türkiye, bu konumuyla enerji ticaretinde önemli bir rol üstlenmektedir. Türkiye'nin jeopolitik konumu yalnızca enerji kaynaklarının taşınması açısından değil, aynı zamanda Asya ve Avrupa arasında enerji iş birliği projelerinde köprü görevi görmesi açısından da önemlidir. Nükleer enerji, Türkiye'nin bu rolünü daha etkin bir şekilde yerine getirmesine olanak tanır.

Doğu Akdeniz, enerji rezervleri ve jeopolitik konumu nedeniyle artan bir stratejik öneme sahiptir. Türkiye, bu bölgede enerji kaynaklarına erişim sağlamak ve enerji güvenliğini artırmak için etkin bir rol oynamaktadır. Türkiye, nükleer enerjiyi yenilenebilir enerji kaynaklarıyla entegre ederek Orta Doğu ve Doğu Akdeniz'deki enerji politikalarında etkisini artırabilir.

BÖLÜM 2

NÜKLEER TESİSLERİN MİLLÎ GÜVENLİK ÜZERİNDEKİ ETKİLERİ

Nükleer Tesislerin Emniyeti ve Korunması

Nükleer enerji tesisleri, ulusal enerji arz güvenliğini sağlamanın yanı sıra stratejik bir önem taşır. Ancak bu kritik altyapılar, fiziksel ve siber tehditler dâhil olmak üzere geniş bir yelpazede risklerle karşı karşıyadır. Bu nedenle nükleer tesislerin emniyeti ve korunması hem ulusal hem de uluslararası düzeyde sıkı güvenlik protokollerini ve düzenlemeleri gerektirir.

Fiziksel koruma sistemleri; nükleer tesislerin yetkisiz erişime, sabotaja ve terörist saldırılara karşı korunmasını hedefler. Bu koruma katmanı; fiziksel bariyerler, gözetim sistemleri, erişim kontrol teknolojileri ve güvenlik personelinden oluşur.

- **Çevresel bariyerler ve izleme sistemleri:** Nükleer tesislerin çevresi; yüksek güvenlikli çitler, hendekler ve elektronik algılama sistemleriyle korunur. Çevresel bariyerler, yetkisiz kişilerin tesise fiziksel erişimini zorlaştırmak amacıyla tasarlanmıştır.
- **Erişim kontrol sistemleri:** Fiziksel erişim kontrolleri, yalnızca yetkilendirilmiş personelin belirli alanlara giriş yapmasını sağlamak için biyometrik tarama, manyetik kartlar ve PIN kodları gibi teknolojilerle desteklenir.
- **Silahlı güvenlik personeli ve gözetim:** Fiziksel güvenlik personeli, 7/24 devriye gezerek ve güvenlik kameralarını izleyerek tesisin korunmasını sağlar. Ayrıca güvenlik personelinin düzenli olarak acil durum tatbikatlarına katılması, potansiyel krizlere müdahale kabiliyetini artırır.
- **Radyolojik materyallerin korunması:** Nükleer materyallerin yetkisiz erişim ve kötüye kullanıma karşı korunması, nükleer emniyetin en hassas yönlerinden biridir. UAEA tarafından belirlenen fiziksel koruma önlemleri, radyolojik materyallerin güvenliğini artırmayı hedefler.

Nükleer tesislerin dijitalleşmesi, operasyonel süreçleri daha verimli hâle getirirken siber tehditlere karşı savunmasızlığı artırmıştır. Siber güvenlik, tesislerin dijital altyapısının korunmasını sağlayan önemli bir unsurdur.

- **Ağ segmentasyonu ve izolasyon:** Nükleer tesislerde kullanılan dijital kontrol sistemleri, ağ segmentasyonu ve hava boşluğu (air gap) gibi yöntemlerle izole edilir. Ancak Stuxnet saldırısı, bu yöntemlerin tam anlamıyla güvenlik sağlamayabileceğini göstermiştir. Bu nedenle siber güvenlik önlemleri sürekli olarak güncellenmelidir.
- **Tehdit algılama ve müdahale:** Tehdit algılama sistemleri, ağ trafiğini sürekli izleyerek anormal aktiviteleri tespit eder ve saldırılar başlamadan önce müdahale olanağı sunar.
- **Çalışan eğitimi ve sosyal mühendislik:** Sosyal mühendislik saldırıları, çalışanların bilinçsiz hataları yoluyla nükleer tesislerin güvenliğini tehlikeye atabilir. Bu nedenle personelin düzenli olarak siber güvenlik eğitimleri alması kritik önem taşır.

Nükleer enerji tesisleri, stratejik önemi nedeniyle sabotaj, terör saldırıları ve siber tehditler gibi çeşitli risklere karşı açık hedeflerdir. Bu tür saldırılar yalnızca enerji arz güvenliğini değil, aynı zamanda çevresel ve ulusal güvenliği de tehdit eder. Nükleer santrallerin stratejik hedef olma riski özellikle radyolojik materyallerin yanlış kullanımı ve tesislerin kritik altyapılar arasındaki rolü nedeniyle artmaktadır. Terör örgütleri için nükleer tesisler, sembolik ve stratejik birer hedeftir. Bir nükleer santrale yapılacak saldırı, halk arasında korku yaratma ve devlete zarar verme gibi amaçlar taşıyabilir. Nükleer tesisler özellikle 1980'lerde ve sonrasında artan terörist faaliyetler nedeniyle daha güçlü fiziksel koruma sistemleri gerektiren hedefler hâline gelmiştir. Bu tür tehditler, nükleer tesislerin hem fiziksel hem de dijital güvenlik önlemleriyle korunmasını zorunlu kılmaktadır.

Dijitalleşen dünyada, siber saldırılar nükleer tesislerin stratejik hedef olma riskini artıran başlıca unsurlardan biridir. Siber tehditler yalnızca operasyonel teknolojileri (OT) değil, aynı zamanda bilgi teknolojilerini (BT) de hedef alır. 2010 yılında İran'daki Natanz tesislerine yapılan Stuxnet saldırısı, dijital sistemlerin nasıl bir tehdit oluşturabileceğini açıkça göstermiştir. Zararlı yazılım, santrifüjlerin hızını bozarak fiziksel hasara neden olmuştur.[18] 2019 yılında Hindistan'da Kudankulam Nükleer Tesisine yönelik saldırıda, tesisin idari ağları hedef alınmıştır. Bu saldırı, bilgi güvenliğinin zafiyetlerini ortaya koymuştur.[19]

Nükleer tesisler; depremler, sel baskınları ve fırtınalar gibi doğal afetlere karşı savunmasız kalabilir. Bu durum, tesislerin stratejik hedef olma riskini daha da artırır. 2011 yılında deprem ve tsunami sonrası meydana gelen Fukuşima felaketi, nükleer tesislerin doğal afetlere karşı dayanıklılığını artırma gerekliliğini göstermiştir. Bu olay, aynı zamanda nükleer tesislerin stratejik öneme sahip diğer altyapılarla olan bağlantılarının nasıl etkilendiğini de ortaya koymuştur.[20] Akkuyu NGS, Akdeniz bölgesinde yer alması nedeniyle sismik risklere açıktır. Bu nedenle tesis, depreme dayanıklı modern mühendislik standartlarına uygun olarak inşa edilmiştir.[21]

Nükleer tesislerdeki radyolojik materyaller hem sabotaj hem de yasa dışı ticaret riski taşır. Bu materyallerin yanlış ellere geçmesi, büyük ölçekli güvenlik tehditleri doğurabilir. 1987 yılında Brezilya'da bir tıbbi cihazdan sızan radyolojik materyal (Goiania olayı), halka açık bir alanda ciddi bir kriz yaratmıştır. Bu olay, nükleer materyallerin sıkı bir şekilde korunması gerektiğini göstermiştir.[22] Türkiye, radyolojik materyallerin korunmasında UAEA tarafından belirlenen standartlara uyarak bu tür riskleri minimize etmektedir.[23]

Nükleer Enerjinin Askerî Teknoloji ve Savunma Sanayisi Üzerindeki Etkisi

Nükleer enerji sadece enerji üretimi ile sınırlı bir alan değil, aynı zamanda askerî teknoloji ve savunma sanayisi üzerinde de önemli etkiler yaratan bir güçtür. Nükleer teknolojilerin gelişimi, askerî uygulamalara olan katkılarıyla modern savunma sistemlerinde kritik bir yer edinmiştir. Bu etki, nükleer enerji altyapısının oluşturduğu bilgi birikimi, teknik uzmanlık ve stratejik üstünlük unsurlarından kaynaklanmaktadır.

Nükleer enerji, askerî denizaltılar ve uçak gemileri gibi stratejik araçların güç kaynağı olarak kullanılmaktadır. Nükleer tahrikli denizaltılar, yüksek operasyonel kapasite ve uzun süreli görevler için enerji sağlar. Örneğin, ABD'nin Ohio sınıfı balistik füze denizaltıları, nükleer tahrik sistemleri sayesinde aylarca yakıt ikmali yapmadan görev yapabilir.[24] Nükleer teknoloji, 20. yüzyılın ortalarından itibaren stratejik savunma politikalarının bir parçası olarak kullanılmaktadır. Nükleer silah geliştirme süreçleri, enerji üretimi için kullanılan reaktörlerden elde edilen bilgi birikimine dayanır. Bu bilgi, nükleer mühimmatların üretiminde ve tasarımında kritik bir rol oynar.[25] Nükleer enerji, uzun süreli enerji ihtiyacı olan askerî iletişim ve uzay sistemlerinde de kullanılmaktadır. Özellikle uzay görevlerinde kullanılan radyoizotop termoelektrik jeneratörler, nükleer enerjinin savunma sanayisindeki bir başka stratejik kullanımını oluşturur.[26]

Nükleer enerji tesisleri, askerî teknolojilerin geliştirilmesi için araştırma ve geliştirme merkezleri olarak kullanılabilir. Bu tesislerde geliştirilen ileri düzey teknolojiler, savunma sanayisinde yenilikçi çözümlerin ortaya çıkmasını sağlar. Örneğin lazer teknolojisi, radar sistemleri ve elektromanyetik silahların geliştirilmesi için gereken enerji ve teknik altyapı, nükleer enerji sayesinde sağlanmaktadır.[27] Nükleer enerji projeleri, savunma sanayisine yönelik endüstriyel kapasitenin artırılmasında önemli bir rol oynar. Bu projeler, yüksek hassasiyetli mühendislik süreçleri, malzeme bilimi ve üretim kabiliyetlerini güçlendiren geniş bir bilgi tabanı oluşturur.[28]

Nükleer enerji, uluslararası arenada stratejik bir güç unsuru olarak değerlendirilmektedir. Bu özellikle enerji bağımsızlığı, jeopolitik avantajlar ve askerî caydırıcılık açısından kritik öneme sahiptir. Nükleer enerji, enerji bağımsızlığını artırarak ülkelerin dışa bağımlılığını azaltır. Bu durum, enerji arz güvenliği ile birlikte askerî operasyonlar için sürekli bir enerji kaynağı sağlanmasına da katkıda bulunur.[29] Nükleer enerji altyapısına sahip ülkeler, bu teknolojiyi diplomatik müzakerelerde bir güç unsuru olarak kullanabilir. Özellikle askerî açıdan stratejik konumda olan ülkeler, nükleer enerji yatırımları sayesinde bölgesel etkilerini artırabilir. Nükleer enerji, dolaylı olarak nükleer silah üretim kapasitesi ile ilişkilendirildiğinden askerî caydırıcılık sağlayan bir unsur olarak değerlendirilmektedir. Bu durum, nükleer enerji altyapısına sahip ülkelerin uluslararası sistemde daha fazla söz sahibi olmasını sağlar.

Nükleer Silahlanma Tartışmaları ve Türkiye'nin Duruşu

Nükleer silahlanma, uluslararası güvenlik politikalarının en tartışmalı konularından biridir. Nükleer enerji altyapısına sahip olmak, dolaylı olarak nükleer silah geliştirme kapasitesini de beraberinde getirebilir. Bu durum; nükleer silahsızlanma anlaşmaları, bölgesel istikrar ve ulusal savunma politikaları açısından çeşitli tartışmalara neden olmaktadır. Türkiye, nükleer enerji projeleriyle ilgilense de nükleer silah geliştirme konusunda net bir şekilde uluslararası düzenlemelere bağlı kalmaktadır.

Nükleer silahlar, uluslararası sistemde caydırıcı güç unsurları olarak kabul edilir. Özellikle Soğuk Savaş Dönemi'nde ABD ve Sovyetler Birliği arasında yaşanan silahlanma yarışı, nükleer silahların uluslararası ilişkilerdeki kritik rolünü ortaya koymuştur. Günümüzde nükleer silah sahibi ülkeler, bu teknolojiyi hem askerî hem de diplomatik avantajlar sağlamak için kullanmaktadır.

Uluslararası toplum, nükleer silahlanmayı kontrol altına almak amacıyla çeşitli anlaşmalar imzalamıştır. Bunlardan en önemlisi, 1968 yılında kabul edilen Nükleer Silahların Yayılmasının Önlenmesi Antlaşması'dır (NPT). Bu antlaşma, nükleer silahların yayılmasını önlemeyi ve nükleer enerji kullanımını barışçıl amaçlarla sınırlandırmayı hedefler.[30] Türkiye, NPT'ye taraf olarak nükleer enerji projelerinde barışçıl kullanım ilkesine bağlı kalacağını uluslararası düzeyde taahhüt etmiştir.[31] Akkuyu NGS gibi projeler, yalnızca enerji üretimi ve ekonomik kalkınma hedeflerine odaklanmıştır.

Harita 1: UAEA'ya Göre Türkiye ve Çevre Ülkelerde Bulunan Nükleer Güç ve Araştırma Reaktörleri Sayısı

Not: Bölgemizde NPT'ye taraf olmayan tek ülke İsrail'dir.

Türkiye, bölgesel güvenlik kaygıları nedeniyle nükleer silahlanma tartışmalarında sık sık gündeme gelmektedir. Orta Doğu'daki güvenlik dengeleri ve İran'ın nükleer programı gibi konular, Türkiye'nin nükleer politikalarını etkileyen faktörler arasında yer almaktadır. Orta Doğu, nükleer silahlanma

açısından kritik bir bölge olarak kabul edilmektedir. İsrail'in nükleer kapasiteye sahip olduğu yönündeki iddialar ve İran'ın nükleer programı, bölgedeki güç dengelerini etkileyen önemli faktörlerdir. Ancak Türkiye, bu tartışmalarda uluslararası yükümlülüklerine bağlı kalarak barışçıl nükleer enerjiyi savunan bir pozisyon tercih etmektedir. Türkiye, bölgedeki nükleer silahlanma risklerini azaltmaya yönelik uluslararası çabaları da desteklemektedir.

Türkiye, UAEA ile iş birliği içinde, nükleer enerji projelerini sıkı denetimlere tabi tutmaktadır. Bu iş birliği, nükleer materyallerin barışçıl amaçlarla kullanılmasını ve uluslararası standartlara uygunluğun sağlanmasını garanti altına alır. Nükleer enerji altyapısı, doğrudan nükleer silahlanma amacı taşımamakla birlikte, dolaylı olarak askerî caydırıcılık kapasitesine katkı sağlayabilir. Türkiye, bu kapasiteyi enerji bağımsızlığı ve ulusal güvenlik hedeflerini desteklemek için kullanmayı amaçlamaktadır. Bu durum, nükleer enerjiyi stratejik bir araç hâline getirmektedir.

BÖLÜM 3

NÜKLEER TESİSLER VE SİBER GÜVENLİK

Nükleer Enerji Tesislerine Yönelik Gerçekleşen Siber Saldırılar

Nükleer enerji tesisleri yalnızca fiziksel saldırılara değil, aynı zamanda siber tehditlere karşı da savunmasız kalabilir. Modern nükleer santrallerdeki dijitalleşme, operasyonel süreçleri optimize etse de aynı zamanda tesisleri karmaşık ve koordineli siber saldırılar için bir hedef hâline getirmiştir. Siber saldırılar; tesisin operasyonel teknolojilerini, bilgi sistemlerini ve kritik altyapılarını hedef alarak hem enerji üretiminde aksamalara hem de ulusal güvenlik tehditlerine yol açabilir. Aşağıda farklı ülkelerde gerçekleşen siber saldırı örnekleri listelenmiştir.[32,33,34,35,36]

- **Davis-Besse NGS, ABD (2003):** Ohio eyaletindeki nükleer santral, "Slammer" adlı bir bilgisayar solucanının hedefi olmuştur. Bu zararlı yazılım, santralin güvenlik izleme sistemini yaklaşık 5 saat boyunca devre dışı bırakmıştır. Santral personeli, kurum ağı önündeki güvenlik duvarının koruma sağladığını düşünürken bu olayın gerçekleşmesi şaşkınlığa yol açmıştır. Bu olay, nükleer tesislerin siber güvenlik önlemlerinin önemini ve güvenlik duvarlarının tek başına yeterli olmadığını göstermiştir.

- **Natanz Tesisi, İran (2010):** "Stuxnet" saldırısı, nükleer enerji tesislerine yönelik siber saldırıların en dikkat çekici örneklerinden biridir. İran'ın Natanz Uranyum Zenginleştirme Tesisine yönelik bu saldırıda, santrifüjlerin çalışma hızları manipüle edilerek fiziksel hasar yaratılmıştır. Stuxnet, nükleer tesislerin dijital sistemlerinin nasıl istismar edilebileceğini göstermiş ve bu alandaki güvenlik açıklarını gözler önüne sermiştir.

- **Hydro and Nuclear Power Co., Güney Kore (2014):** Güney Kore'nin 23 nükleer reaktörünü işleten Korea Hydro and Nuclear Power Co., kimliği belirsiz bir grup tarafından hacklendi. Phishing e-postalarıyla başlatılan saldırıda, Gori ve Wolseong nükleer santrallerine ait planlar ve kılavuzlar, radyasyon tahminleri, 10.000 çalışanın kişisel bilgileri ve elektrik akış diyagramları çalınarak X (Twitter) üzerinden sızdırıldı. Bu olay, nükleer tesislerde veri sızıntılarının yarattığı güvenlik sorunlarını ve siber saldırıların karmaşık izlenebilirliğini bir kez daha ortaya koymuştur.

- **Toyama Üniversitesi Hidrojen İzotopu Araştırma Merkezi, Japonya (2016):** Merkez, bir siber saldırıya uğramış ve trityum araştırmaları dâhil olmak üzere 59.000'den fazla dosya çalınmıştır. Saldırganlar, Tokyo Üniversitesi öğrencisi gibi davranarak zararlı yazılım içeren e-postalarla araştırmacılara ulaşmıştır. Çalınan veriler arasında Fukuşima Nükleer Santraline dair araştırmalar ve 1.500 kişinin kişisel bilgileri bulunmaktadır. Bu olay, nükleer araştırma merkezlerine yönelik siber tehditlerin ciddiyetini ve "spear-phishing" yöntemlerinin etkinliğini göstermiştir.

- **Gundremmingen NGS, Almanya (2016):** Santralde, "W32.Ramnit" ve "Conficker" isimli kötü amaçlı yazılımlar tespit edilmiştir. Bu virüsler, nükleer yakıt çubuklarını taşıyan ekipmanlarla

bağlantılı veri görselleştirme sistemi ile 18 adet çıkarılabilir veri cihazında (çoğunlukla USB bellekler) bulunmuştur. Santralin işletmecisi, enfekte sistemlerin internete bağlı olmadığını ve kötü amaçlı yazılımın santralin operasyonel sistemlerini etkilemediğini ya da güvenliğine bir tehdit oluşturmadığını açıklamıştır.

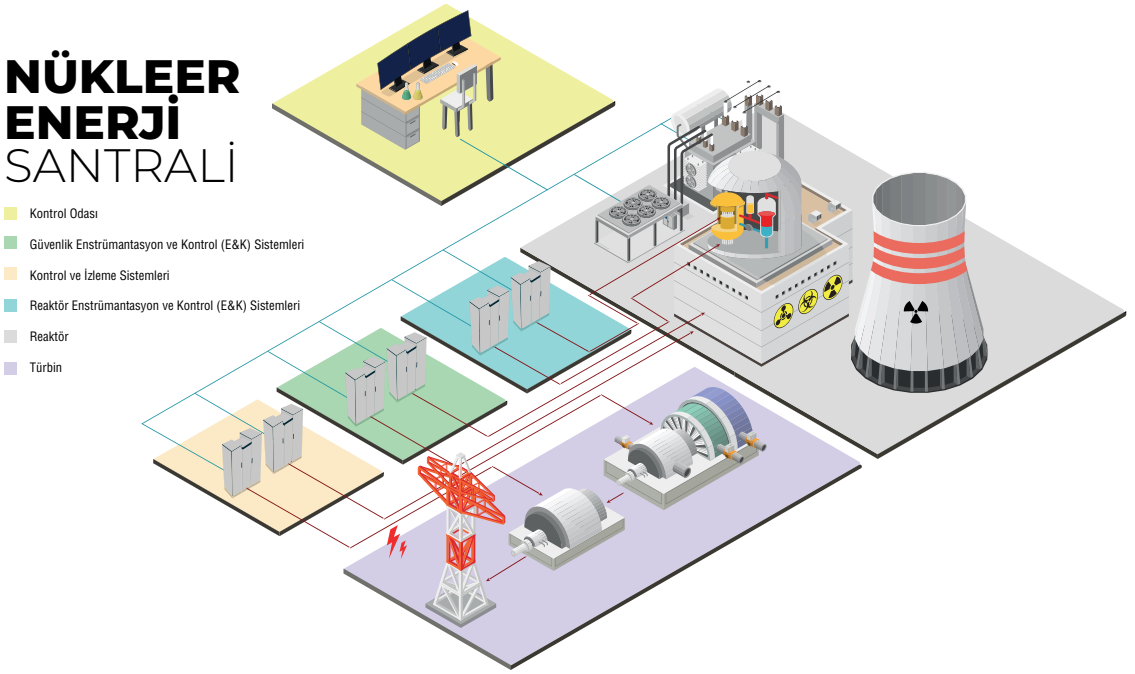
- **Wolf Creek NGS, ABD (2017):** ABD'deki Wolf Creek Nükleer Santrali, 2017 yılında kimliği belirsiz bir grup tarafından siber saldırıya uğramıştır. Bu saldırıda, tesisin operasyonel ağlarına erişim sağlanamasa da bilgi sistemlerine yönelik tehditler artmıştır. Saldırının amacı, tesisin dijital altyapısını test etmek ve potansiyel açıkları tespit etmek olmuştur.

- **Kudankulam NGS, Hindistan (2019):** Hindistan'daki Kudankulam Nükleer Santraline yapılan siber saldırı, tesisin idari ağlarını hedef almıştır. Saldırı sonucunda hassas veriler çalınmış ve tesisin güvenlik önlemleri sorgulanmıştır. Bu saldırı, nükleer tesislerdeki bilgi güvenliği zafiyetlerinin ciddi sonuçlar doğurabileceğini kanıtlamıştır.

Nükleer Güç Santrallerinin Enstrümantasyon ve Kontrol Sistemi

Enstrümantasyon ve kontrol (E&K) sistem mimarisi, tesis işletme personeli ile birlikte bir nükleer santralin "merkezî sinir sistemi" olarak görev yapar. Nükleer güç santralinin E&K sistem mimarisinin işlevi Şekil 1'de özetlendiği gibi süreç (reaktör, ısı taşıma ve enerji dönüşüm sistemleri) ile tesis personeli (işletme ve bakım ekibi) arasında yer alan algılama, iletişim, izleme, gösterim, kontrol ve komut sistemlerini ele alır. Bir tesis parametresini tasarım sınırları içinde tutmak için bu parametreye ilişkin doğru ve güvenilir bilgilere ihtiyaç vardır. Bu bilgi, sensörler kullanılarak yapılan ölçümlerle sağlanır. Parametre türüne (örneğin sıcaklık, basınç, akış hızı, seviye) ve gereksinimler ile kısıtlamalara (örneğin doğruluk, yanıt süresi ve çevresel koşullar) bağlı olarak geniş bir sensör çeşitliliği kullanılabilir. Tesis parametresinin ölçümü, tasarımda belirlenen ayar noktasına göre karşılaştırılır ve bu ayar noktasından sapmaya bağlı olarak uygun aktüatörlerin kontrol edilmesiyle düzeltici eylemler gerçekleştirilir.

Şekil 1: E&K Ana İşlevlerinin Genel Görünümü



Birçok nükleer santralin işletme ömrünün uzatılması amacıyla yeniden lisanslanması, eskiyen veya teknolojik olarak modası geçmiş bileşen ve ekipmanların korunmasını maliyet açısından verimsiz hâle getirebilir. Bu nedenle mevcut analog E&K sistemleri dijital sistemlere dönüştürülmekte ve yeni santrallerde modern dijital E&K teknolojileri devreye alınmaktadır. Bu gelişmiş sistemler, tüm santralin performansını artırarak hem mevcut hem de gelecekteki santrallerin ekonomik verimliliğini ve güvenliğini önemli ölçüde iyileştirmektedir. Ayrıca modern dijital ölçüm ve izleme sistemleri, güvenlik öncelikli bir anlayışla tasarlandığında, fiziksel ve siber güvenliğe de önemli katkılar sağlayabilir.[37]

Dijital E&K sistemlerinin benimsenmesi, aşağıdaki faktörler nedeniyle karmaşıklıklar taşır.[38]

- **Siber güvenlik:** Dijital teknolojinin yaygınlaşması, güvenliği sağlamak için güçlü siber güvenlik önlemlerini gerektirir.
- **Gelişmiş tasarımlar:** Yeni nesil reaktörler (küçük modüler reaktör ve 4. nesil reaktörler) için uyarlanabilir sistemler gereklidir.
- **Tanılama:** Gerçek zamanlı veri işleyerek arıza tespiti ve bakım süreçlerini iyileştiren entegre tanılama araçları önemlidir.

- **Kullanıcı dostu arayüzler:** Artırılmış gerçeklik ve sanal gerçeklik ile desteklenen gelişmiş arayüzler, operatörlerin verimliliğini artırır.
- **Modüler ve ölçeklenebilir sistemler:** Bu sistemler, mevcut santralleri modernize ederken yeni reaktör tasarımlarına uyum sağlayabilir.
- **Düzenleme ve iş birliği:** Uluslararası standartlar ve iş birliği çerçevesinde, düzenlemeler dijitalleşmeye uyum sağlamaktadır.

Nükleer Enerji Altyapısının Siber Tehditlere Karşı Korunması

Nükleer enerji altyapısı yalnızca enerji üretiminde değil, aynı zamanda ulusal güvenlik stratejilerinde de kritik bir rol oynar. Ancak dijitalleşme ve otomasyonun artmasıyla birlikte bu altyapılar, siber tehditlere karşı daha savunmasız hâle gelmiştir. Bu nedenle nükleer enerji tesislerinin siber tehditlere karşı korunması hem operasyonel süreçlerin kesintisiz devamı hem de ulusal güvenliğin sağlanması açısından büyük önem taşır.

Nükleer tesislere yönelik siber saldırılar bağlamında bilgi teknolojileri (BT) ve operasyonel teknolojiler (OT) kavramları kritik bir öneme sahiptir.[39] Her iki kavram, nükleer tesislerin farklı işlevsel alanlarını ifade eder ve saldırılara karşı alınacak koruma önlemlerinin temelini oluşturur. Siber güvenlik bağlamında BT ve OT sistemleri arasındaki farkları anlamak, saldırı risklerini minimize etmek için hayati öneme sahiptir.

BT, nükleer tesislerin yönetimsel ve idari süreçlerini destekleyen dijital altyapıyı ifade eder.[40] Bu sistemler genellikle dış dünyaya açıktır ve çalışan maaş bordrolarından insan kaynakları yönetimine, finansal raporlamadan kurum içi iletişime kadar birçok kritik işlevi yerine getirir. BT sistemleri; e-posta, dosya paylaşımı ve internet bağlantısı gibi özelliklerle organizasyonel verimliliği artırırken aynı zamanda dış tehditlere açık bir hedef hâline gelir. Yazılım güncellemeleri veya uzaktan erişim gibi işlemler sırasında sistemlerin saldırılara karşı savunmasız hâle gelme riski yüksektir.

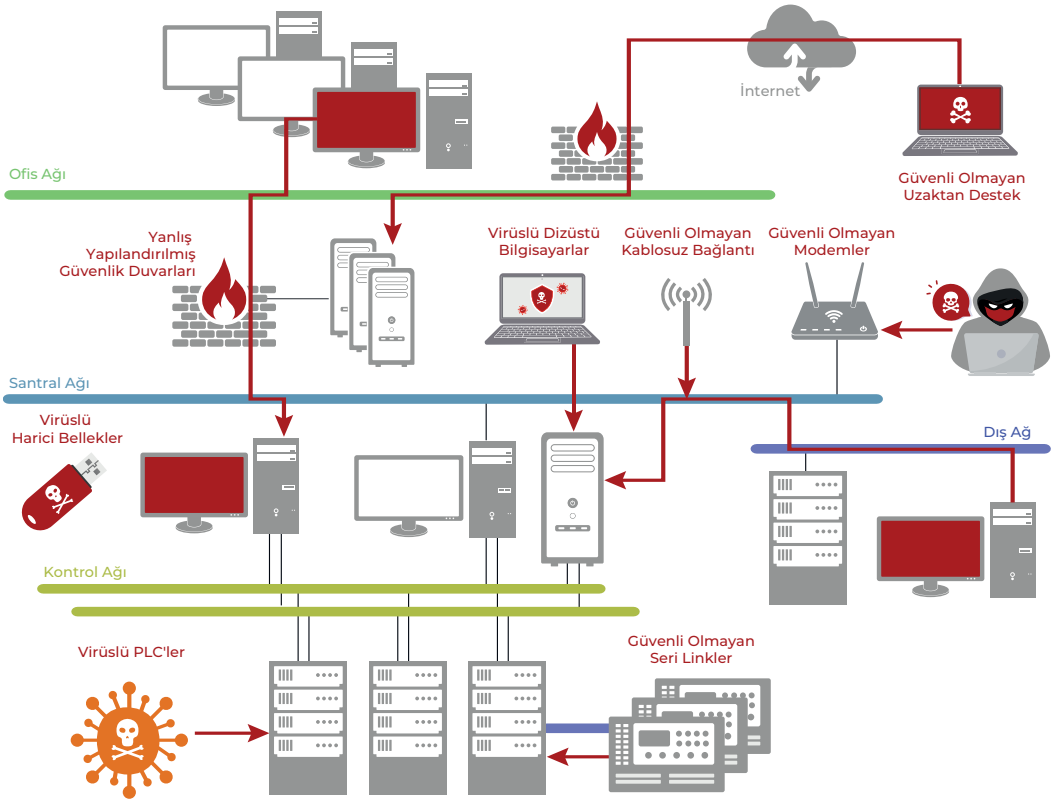
OT, nükleer tesislerin fiziksel işleyişini ve kritik süreçlerini yöneten sistemlerdir.[41] OT altyapısı, reaktörlerin enerji üretiminden güvenlik sistemlerinin işleyişine kadar bir tesisin operasyonel performansını doğrudan etkiler. Bu sistemler, veri toplama ve analiz yoluyla süreç optimizasyonu sağlarken güvenlik sistemleri ani durumlara müdahale ederek tesisin güvenliğini korur. OT sistemleri genellikle internet bağlantısından yalıtılmış bir şekilde çalıştırılır ve "air gap" adı verilen bir güvenlik stratejisi ile BT ağlarından izole edilir. Ancak fiziksel yalıtım, mutlak bir güvenlik sağlamaz; USB cihazları veya tedarik zinciri üzerinden gelen bileşenlerin sisteme dâhil edilmesiyle bu izolasyon aşılabilir.

BT ve OT sistemlerinin farklı rollerine rağmen bu iki sistem arasında zayıf bir bağlantı bulunması bile ciddi güvenlik riskleri oluşturabilir. BT sistemlerinde meydana gelen bir güvenlik ihlali, OT sistemlerine

sıçrayabilir ve fiziksel operasyonları tehlikeye atabilir. BT ve OT sistemlerinin güvenliği, nükleer tesislerin genel güvenliği için birbirini tamamlayan unsurlardır. BT sistemleri, dış tehditlere karşı sıkı koruma gerektirirken OT sistemleri için daha katı fiziksel ve dijital güvenlik önlemleri alınmalıdır. Özellikle BT ve OT sistemleri arasındaki geçiş noktalarının korunması, siber saldırılar karşısında en önemli savunma mekanizmalarından biridir.

Modern nükleer santral altyapıları genellikle Programlanabilir Mantıksal Denetleyiciler (PLC) ve Gözetim Kontrol ve Veri Toplama (SCADA) sistemleri üzerine kuruludur. Bu sistemler, nükleer santraller gibi kritik altyapıların kontrolü ve izlenmesinde kullanılır. Ancak SCADA ve PLC sistemlerinin özellikle dış bağlantılar ve insan hataları nedeniyle ciddi güvenlik açıklarına sahip olduğu bilinmektedir. Şekil 2, SCADA sistemlerinin zayıf noktalarını ve bu zafiyetlerin Stuxnet gibi saldırılarda nasıl kullanıldığını açıklamaktadır. Stuxnet virüsü, İran'ın nükleer programına bağlı şirketlerin ağlarını enfekte ederek Siemens S7-400 PLC'leri hedef almıştır. Bu PLC'ler, uranyum zenginleştirme işlemleri için kullanılan santrifüjleri kontrol etmektedir. USB cihazları yoluyla yayılan virüs, SCADA sistemleri üzerinden PLC'lere bulaşmış ve bu sistemlerdeki kodları manipüle ederek santrifüjlerin kontrol dışı çalışmasına ve kendilerini yok etmelerine neden olmuştur.[42,43]

Şekil 2: Potansiyel Kontrol Sistemi Zafiyetleri[43]



SCADA sistemlerinin açıkları ve Stuxnet'in yayılımı aşağıdaki sebeplerle gerçekleşebilir.

- **İnternet bağlantıları:** SCADA sistemleri genellikle doğrudan internete bağlı olmasa da bağlı oldukları ağların internet erişimi bulunmaktadır. Bu durum, dış tehditlerin sisteme erişmesini kolaylaştırır.

- **İnsan hataları:** Virüs bulaşmış cihazların kullanımı veya iç ağı etkileyebilecek hatalar, sistem güvenliğini tehlikeye atabilir. Stuxnet'in USB cihazları yoluyla yayılması bu duruma örnek teşkil eder.

- **Standartlaştırılmış protokoller:** Modern SCADA sistemleri, eskiden kullanılan özel protokoller yerine TCP/IP gibi standart iletişim dillerini kullanır. Bu, sistemlerin daha geniş bir saldırı yüzeyine sahip olmasına neden olur.

SCADA sistemleri, nükleer enerji altyapısında hayati bir öneme sahiptir ancak mevcut zafiyetler bu altyapının tehditlere açık olmasına yol açmaktadır. Stuxnet saldırısı, bu tür güvenlik açıklarının hem hedefli saldırılar hem de yaygın bulaşma için nasıl kullanılabileceğini ortaya koymuştur.[44] Bu tehditleri azaltmak için SCADA ve PLC sistemlerinin güvenliği artırılmalı, internet bağlantıları minimuma indirilmeli ve çalışan farkındalık eğitimleri düzenlenmelidir.

Nükleer tesislerde kullanılan BT, idari süreçlerin yönetilmesinde ve veri saklama işlemlerinde kritik bir rol oynar. Siber saldırılar, bu sistemler üzerinden hassas verilerin sızdırılmasına veya manipüle edilmesine yol açabilir. Hindistan'daki Kudankulam Nükleer Santraline yapılan saldırı, BT altyapısının nasıl hedef alınabileceğini göstermiştir.[35] Santralin kritik operasyonel ağı, internet bağlantısı olmayan bir "air gap" sistemi ile korunuyordu. Ancak bu güvenlik stratejisi, hedefli saldırılara karşı etkisizdir. Özellikle Stuxnet saldırısında olduğu gibi bu tür sistemler insan hataları veya tedarik zinciri yoluyla dolaylı yoldan ihlal edilebilir. Kudankulam saldırısında Dtrack malware (zararlı yazılım) içeren bir kişisel bilgisayarın idari ağa bağlanması, saldırının başlangıç noktası oldu.[45] Google'ın sahip olduğu VirusTotal tarama platformu, santralin idari ağından önemli miktarda veri çalındığını ortaya koydu. Bu durum, santralin kritik sistemlerine yönelik gelecekte daha hedefli saldırıların zeminini oluşturabilir.[46] Kudankulam saldırısı, OT sistemlerinin doğrudan bir hedef olmasa da BT sistemleri üzerinden elde edilen bilgilerle tehdit edilebileceğini ve bu sistemlerin siber güvenlik stratejilerinin güçlendirilmesi gerektiğini açıkça ortaya koymuştur.[47]

Air gap stratejisi,[36] bir ağın internet ve diğer dış bağlantılardan fiziksel olarak izole edilmesiyle kritik sistemlerin korunmasını amaçlar. Ancak bu yöntem, hedefli ve karmaşık siber saldırılar karşısında ciddi zayıflıklara sahiptir. İlk olarak insan faktörü, bu izolasyonu aşmanın en yaygın yollarından biridir. Çalışanların farkında olmadan zararlı yazılımlarla enfekte olmuş USB bellekler veya cihazlar kullanması, saldırganların air gap'i ihlal etmesini kolaylaştırır. İkinci olarak sistem güncellemeleri ve veri transferleri, air gap'in etkinliğini zayıflatır. Air gap ile izole edilmiş bir ağ bile yazılım güncellemeleri, sistem bakım işlemleri veya analiz verilerinin aktarımı gibi operasyonel gereksinimler nedeniyle dış veri kaynaklarına ihtiyaç duyabilir. Bu süreçlerde kullanılan cihazlar veya transfer yöntemleri, siber

saldırılara açık bir kapı hâline gelir. Örneğin, kritik bir sistemin güncellenmesi sırasında kullanılan harici bir bellek, güvenlik ihlali riskini artırabilir. Son olarak tedarik zinciri güvenliği de air gap sistemlerinin savunmasız noktalarından biridir. Nükleer tesislerde kullanılan donanım ve yazılım bileşenleri genellikle farklı tedarikçilerden temin edilir. Bu tedarik zincirinde yer alan herhangi bir bileşen, zararlı yazılımları barındırma riski taşıyabilir ve bu da izole edilmiş ağlarda bile ihlal olasılığını artırır. Tüm bu faktörler, air gap stratejisinin modern ve sofistike siber tehditler karşısında tek başına yeterli olmadığını göstermektedir. Bu nedenle air gap ile birlikte çok katmanlı siber güvenlik önlemleri uygulanmalı, insan hatası riskini azaltacak otomasyon sistemleri ve tedarik zinciri güvenliği gibi ek koruma mekanizmaları devreye alınmalıdır.

Nisan 2021'de İran'ın Natanz Nükleer Tesisi, uranyum zenginleştirme faaliyetlerini aksatan büyük bir saldırıya maruz kaldı. İran, bu olayı "nükleer terörizm" olarak tanımladı ve saldırının, tesiste elektrik kesintisine neden olan ve ileri düzey santrifüjlere zarar veren bir patlama içerdiğini bildirdi. Saldırı, İran'ın tesiste ileri teknoloji IR-6 santrifüjlerini tanıtmasından kısa bir süre sonra gerçekleşti ve bu durum, İran'ın nükleer kapasitesindeki önemli bir yükseltmeye işaret ediyordu. Bu olay, İran Nükleer Anlaşması (2015 tarihli Kapsamlı Ortak Eylem Planı, KOEP) kapsamında yapılan müzakerelerin sürdüğü bir dönemde yaşandı. İran, başlangıçta saldırıyı bir siber saldırı olarak tanımladıysa da sonrasında bunun 2010'daki Stuxnet saldırısından farklı olarak fiziksel sabotaj içerdiği anlaşıldı. Patlama, tesisin elektrik altyapısına ve santrifüjlere ciddi zarar verdi. Bu yöntem, fiziksel sabotajla birlikte siber istihbarat veya koordinasyonu içeren hibrit taktiklerin kullanımına işaret etmektedir. Bu durum, kritik altyapılara yönelik tehditlerin evrimini ve çeşitliliğini ortaya koymaktadır. Olay, Natanz Nükleer Tesisinin güvenliğinde zafiyetler olduğunu ortaya çıkardı. İran'ın nükleer altyapıyı korumak için yaptığı yatırımlara rağmen saldırganların bu kadar kolay bir şekilde ciddi hasar verebilmesi, güvenlik protokollerinde eksiklikler ve içeriden gelen tehditlere karşı savunma yetersizliğini gündeme getirdi.[48,49]

Natanz saldırısı, nükleer altyapıya yönelik tehditlerin giderek karmaşık hâle geldiğini bir kez daha gösterdi. Stuxnet gibi geleneksel siber saldırılar, sistemleri zararlı yazılımlarla hedef alırken 2021'deki olay, fiziksel sabotajın ve siber unsurların bir arada kullanıldığı hibrit bir stratejiye işaret etmiştir. Bu durum, nükleer tesislerin emniyeti için yalnızca dış tehditlere değil, aynı zamanda iç tehditlere karşı da sıkı önlemler alınması gerektiğini vurgulamıştır. Bu olay, nükleer altyapının modern çatışmalardaki merkezî rolünü ve bu tür olayların uluslararası ilişkiler ile küresel nükleer politikaların gidişatını nasıl etkilediğini ortaya koymaktadır. İran'ın nükleer programını hedef alan bu saldırı, gelecekte nükleer tesislerin emniyetini artırmak için daha kapsamlı ve katmanlı koruma sistemlerinin geliştirilmesi gerektiğini açıkça göstermiştir.

BÖLÜM 4

TÜRKİYE'DE MEVCUT DURUM

Siber tehditlerin artan karmaşıklığı ve nükleer enerji tesislerine yönelik potansiyel riskler, etkili bir siber güvenlik stratejisinin uygulanmasını zorunlu kılmaktadır. Türkiye, nükleer tesislerin korunması için hem ulusal düzeyde düzenlemeler hem de uluslararası standartlara uygun stratejiler benimsemektedir. Bu yaklaşımlar, kritik altyapıların korunması ve siber saldırılara karşı dirençli bir sistem kurulması için tasarlanmıştır. 2024 yılında yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve Eylem Planı[50] ile siber güvenlik alanında kapsamlı bir çerçeve belirlenmiştir. Bu strateji, kritik altyapıların korunmasını ve siber saldırılara hızlı müdahale edilebilmesini hedeflemektedir. Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve USOM, bu stratejinin uygulanmasında önemli roller üstlenmiştir.

Nükleer Düzenleme Kurumunun (NDK) Teşkilat ve Görevleri Hakkında 95 sayılı Cumhurbaşkanlığı Kararnamesi'nin 9'uncu maddesinin birinci fıkrasının (a) bendine istinaden; nükleer santraller için siber güvenliğe ilişkin planlarda yer alması gereken hususları içeren siber güvenlik planı içeriğinin, 11/6/2024 tarihli ve 32573 sayılı Resmî Gazete'de yayımlanan Nükleer Tesislerin ve Nükleer Maddelerin Emniyetine İlişkin Yönetmelik'in 11'inci maddesinin dördüncü fıkrasına dayanılarak "Nükleer Santraller İçin Siber Güvenlik Planı" dokümanı hazırlanmıştır.[51] Türkiye'deki nükleer santrallerin siber güvenliği hem ulusal enerji güvenliğinin bir parçası hem de küresel düzenleyici standartlara uyum sağlamak açısından büyük bir öneme sahiptir. Hazırlanan planda; siber güvenlik stratejilerinin detayları, organizasyon yapıları ve uygulanacak önlemler kapsamlı bir şekilde ele alınmaktadır.

Nükleer santrallerin siber güvenlik organizasyon yapısı, görev ve sorumlulukların net bir şekilde tanımlanmasını gerektirir. Bu doğrultuda Siber Güvenlik Planı; yetkilendirilen kişiler, yükleniciler ve diğer paydaşlar arasında iş bölümü ve koordinasyonun önemine dikkat çekmektedir. Organizasyon şemaları, bilgi akışı mekanizmaları ve raporlama süreçleri detaylandırılarak özellikle siber olaylara müdahale ekiplerinin sektörel Siber Olaylara Müdahale Ekibi (SOME) ve USOM ile ilişkileri tanımlanmaktadır.

Siber güvenlik politikalarının oluşturulmasında, derinliğine savunma ve dereceli yaklaşım gibi ilkeler temel alınmaktadır. Emniyet ve güvenlik kültürü ile uyumlu bir şekilde oluşturulan bu politikalar; nükleer santral yönetimi, çalışanlar ve tedarikçiler tarafından benimsenmelidir. Kritik dijital varlıkların korunması, risk tabanlı bir yaklaşımın benimsenmesi ve "bilmesi gereken" ilkesinin uygulanması bu stratejilerin temel taşlarını oluşturmaktadır.

Planda, dijital varlık yönetimi detaylı bir şekilde ele alınmıştır. Nükleer santrallerdeki kritik dijital varlıkların tanımlanması, sınıflandırılması ve izlenmesi için yöntemler geliştirilmiştir. Kritik sistemlerin konumları, birbirleriyle bağlantıları ve kullanıcı gruplarının yetkilendirilmesi gibi konulara ilişkin prosedürler açıklanmıştır. Ayrıca yapılandırma yönetimi ve sistem sıkılaştırma süreçleri, dijital varlıkların güvenliğinin sağlanması için hayati öneme sahiptir. Yamalar ve güncellemelerin uygulanması, potansiyel tehditlere karşı sistemin dayanıklılığını artırmak için önerilmektedir.

Türkiye, nükleer tesislerde kullanılan donanım ve yazılımları yerli olarak üretmeyi hedeflemektedir. Yerli üretim, tedarik zinciri risklerini azaltır ve daha güvenli bir altyapı sağlar. Tehdit algılama ve risk yönetimi süreçlerinde yapay zekâ ve makine öğrenimi tabanlı teknolojilerin kullanımı, siber tehditlere karşı daha etkili bir savunma sağlar. Türkiye, bu teknolojileri altyapısına entegre etmeyi planlamaktadır.

Nükleer santrallerin siber güvenlik mimarisi, uluslararası standartlara ve kılavuzlara uygun olarak tasarlanmıştır. Derinlemesine savunma yaklaşımı ile her bir ağ seviyesi için farklı koruma önlemleri tanımlanmıştır. Erişim kontrolü, veri güvenliği, taşınabilir cihaz güvenliği ve sistem izleme gibi başlıklar altında gerekli prosedürler ve talimatlar belirtilmiştir. Ağ topolojisi tasarımı, cihazların ağ seviyelerindeki konumlandırılması ve her bir seviyede uygulanan güvenlik önlemleri detaylı bir şekilde açıklanmıştır.

Risk yönetimi, siber güvenlik planlarının merkezinde yer almaktadır. Plan hem santral genelinde hem de spesifik sistemler üzerinde gerçekleştirilen risk değerlendirmesi süreçlerini tanımlamaktadır. Risk değerlendirmeleri sırasında kullanılan standartlar ve çerçeveler, tehditlerin tanımlanması ve önceliklendirilmesi için temel oluşturur. Tedarik zinciri analizleri, sistem güvenlik gereksinimlerinin karşılanmasını sağlamak için sözleşme düzenlemeleriyle desteklenmiştir. Zafiyet yönetimi kapsamında, kritik dijital varlıkların düzenli olarak analiz edilmesi ve raporlanması gerekliliği vurgulanmıştır.

Nükleer santrallerdeki siber olaylara müdahale politikası; olay öncesi hazırlık, tespit ve analiz, kontrol altına alma, kurtarma ve olay sonrası faaliyetler olmak üzere dört aşamadan oluşmaktadır. Olaylara müdahale ekiplerinin organizasyon yapısı, görev ve sorumlulukları ile USOM ve sektörel SOME ile koordinasyonu açıklanmıştır. Olay sonrası öğrenilen derslerin dokümantasyonu ve düzeltici faaliyetlerin uygulanması, gelecekte benzer olayların önlenmesi için kritik bir adımdır.

UAEA, nükleer enerji tesislerinin siber güvenliğini sağlamak için kapsamlı bir çerçeve sunmaktadır. Bu standartlar, operasyonel ve bilgi teknolojilerinin korunmasına yönelik protokolleri içerir. Türkiye, UAEA'nın ilgili rehberlerine uyarak Akkuyu NGS'de bu standartları uygulamaktadır. Türkiye, UAEA ile yaptığı iş birlikleri sayesinde, nükleer santrallerin güvenliğini artırmayı hedeflemektedir. Bu kuruluşların düzenlediği tatbikatlar ve bilgi paylaşımı, Türkiye'nin siber güvenlik kapasitelerini geliştirmesine olanak tanımaktadır. Türkiye, Akkuyu NGS gibi projelerde uluslararası denetim mekanizmalarını benimseyerek global güvenlik standartlarına uyum sağlamaktadır. Bu süreç hem ulusal hem de uluslararası kamuoyunun güvenini artırmaktadır.

Türkiye, nükleer santrallerde çalışan personelin siber güvenlik konusundaki farkındalığını artırmak için düzenli eğitim programları düzenlemektedir. Bu programlar, sosyal mühendislik saldırılarına karşı direnç oluşturmayı ve teknik becerileri geliştirmeyi hedeflemektedir. Türkiye, nükleer enerji sektöründe çalışacak siber güvenlik uzmanlarını yetiştirmek için üniversiteler ve meslek kuruluşlarıyla iş birliği yapmaktadır. NDK, nükleer tesislerde siber güvenliği güçlendirmek amacıyla Offensive Security Certified Professional (OSCP) eğitim programını başarıyla tamamlamıştır.[52] Bu eğitim, etik hacking becerileri ve güvenlik açıklarının tespitine yönelik yetkinlikler kazandırarak

nükleer tesislerin siber tehditlere karşı korunmasında önemli bir katkı sunmaktadır. NDK'nin bu alandaki uzmanlık kapasitesini artırması, nükleer tesislerin gelişmiş siber saldırılara karşı daha dirençli hâle gelmesini sağlamaktadır. Eğitim kapsamında katılımcılar, pratik uygulamalar aracılığıyla güvenlik açıklarını belirlemiş ve sızma testi tekniklerini gerçek dünya senaryolarında deneyimlemiştir. Bu tür girişimler, Türkiye'nin nükleer enerji sektöründe emniyet standartlarını yükseltmekle kalmayıp NDK'nin uluslararası normlara uyum sağlama çabalarını da desteklemektedir. NDK'nin bu yatırımı, nükleer tesislerin siber tehditlere karşı emniyetini sağlama konusundaki kararlılığını ve liderlik hedefini göstermektedir.

BÖLÜM 5

NÜKLEER TESİSLERİ SİBER TEHDİTLERE KARŞI KORUMA STRATEJİLERİ

Nükleer tesislerin siber tehditlere karşı emniyeti, ulusal enerji altyapısının korunması ve küresel nükleer emniyet standartlarının sağlanması açısından kritik öneme sahiptir. Geçmişte yaşanan olaylar, nükleer tesislerin artan dijitalleşme ve siber saldırılara karşı savunmasızlığını açıkça ortaya koymuştur. Bu bağlamda alınması gereken tedbirler ve uygulanabilecek stratejiler Şekil 3'te gösterildiği üzere altı madde hâlinde sıralanabilir.[32,33,36,47,53]

Şekil 3: Nükleer Tesislerde Siber Saldırılara Karşı Alınması Gereken Tedbirler

Siber Güvenlik Kültürünün Geliştirilmesi

Siber güvenlik kültürünün yerleşmesi, nükleer tesislerdeki en kritik savunma katmanlarından birini oluşturur. Teknolojik altyapı ne kadar gelişmiş olursa olsun, insan hataları veya yetersiz farkındalık nedeniyle siber tehditlerin önüne geçmek mümkün olmayabilir. Bu nedenle nükleer emniyet kültürünün tesiste çalışan her birey tarafından benimsenmesi ve uygulanması hayati önem taşır.

Nükleer tesislerde çalışan personelin, siber güvenlik riskleri ve alınması gereken önlemler konusunda kapsamlı bir eğitime tabi tutulması gerekir. Bu eğitimler yalnızca teknik personeli değil, idari ve ope-

rasyonel tüm çalışanları kapsamalıdır. Özellikle USB bellekler gibi harici cihazların kullanımına ilişkin farkındalık artırılmalı; bu cihazların kötü amaçlı yazılımları sisteme taşıyabileceği açıkça belirtilmelidir. Çalışanların sisteme erişim yetkileri, yalnızca görevleriyle doğrudan ilgili olan verilere ulaşmalarını sağlayacak şekilde sınırlandırılmalıdır. Ayrıca yüksek düzeyde erişim gerektiren yetkilerin izlenmesi ve denetlenmesi, içeriden kaynaklanan tehditlerin önlenmesine katkıda bulunur.

Siber güvenlik kültürünü desteklemek için düzenli tatbikatlar yapılmalıdır. Bu tatbikatlar, çalışanların olası bir siber saldırı durumunda nasıl davranacaklarını öğrenmelerini sağlar. Aynı zamanda tesis yönetimine, mevcut güvenlik açıklarını belirleme ve iyileştirme fırsatı sunar. Tatbikatların yanı sıra kurum içinde siber güvenlik konusunda liderlik yapabilecek uzmanlar yetiştirilmelidir. Bu uzmanlar hem çalışanların eğitimine katkı sağlar hem de günlük operasyonlar sırasında siber güvenlik protokollerinin doğru bir şekilde uygulanmasını denetler.

Nükleer tesislerdeki siber güvenlik kültürü, yalnızca çalışanların eğitimiyle sınırlı kalmamalıdır. Siber güvenlik önlemleri ve protokoller, günlük operasyonların doğal bir parçası hâline getirilmelidir. Çalışanlar, herhangi bir ihlal veya şüpheli durum tespit ettiklerinde hızlı bir şekilde ilgili birimlere rapor verebilmelidir. Bu tür bir yaklaşım, proaktif bir savunma hattı oluşturulmasına yardımcı olur.

Teknolojik Güncellemeler ve Sistem İyileştirmeleri

Nükleer tesislerin emniyetini sağlamak için kullanılan teknolojik altyapının güncel ve etkin olması gerekir. Eski veya modası geçmiş sistemler, modern tehditlere karşı ciddi güvenlik açıklarına neden olabilir. Bu nedenle tesislerin teknoloji altyapısını sürekli olarak güncellemesi ve iyileştirmesi kritik öneme sahiptir.

Modernizasyon süreçleri, tesisin hem dijital hem de fiziksel koruma sistemlerini kapsamalıdır. Dijital sistemlerde, eskiyen analog kontrol sistemleri, daha güvenli ve esnek bir şekilde çalışabilen dijital sistemlerle değiştirilmelidir. Dijital sistemler, daha yüksek bir otomasyon seviyesi sunar ve insan hatalarını en aza indirir. Ayrıca dijital altyapıların siber güvenlik özellikleri artırılarak saldırılara karşı daha dayanıklı hâle getirilmelidir. Özellikle siber saldırılara karşı koruma sağlamak için sistemlere düzenli yazılım güncellemeleri yapılmalı ve güvenlik yamaları zamanında uygulanmalıdır.

Fiziksel altyapıda ise güvenlik kameraları, erişim kontrol sistemleri ve izleme cihazları gibi sistemler sürekli olarak denetlenmeli ve güncellenmelidir. Bu sistemlerin, siber güvenlik altyapısıyla entegre bir şekilde çalışması sağlanmalıdır. Örneğin, fiziksel bir erişim ihlali durumunda, dijital sistemlere de otomatik bir uyarı gönderilmelidir. Bu tür entegre çözümler, saldırılara daha hızlı ve etkili bir şekilde yanıt verilmesini sağlar.

Teknolojik iyileştirmeler yalnızca savunma amaçlı değil, aynı zamanda tesisin genel operasyonel verimliliğini artırmak için de kullanılmalıdır. Modern veri analitiği araçları ve yapay zekâ tabanlı çözümler, tesisin enerji üretim süreçlerini optimize edebilir. Ayrıca bu araçlar, sistem performansını izlemek ve potansiyel sorunları erken tespit etmek için kullanılabilir.

Teknolojik güncellemeler yalnızca sistemlerin kendisini değil, aynı zamanda bu sistemlerle çalışan personelin yetkinliklerini de kapsamalıdır. Çalışanlar, yeni teknolojilere uyum sağlayabilmek için düzenli olarak eğitilmelidir. Bu eğitimler hem teknik hem de operasyonel konuları kapsamalıdır.

Aktif Savunma Stratejileri

Statik savunma mekanizmaları, günümüzün dinamik ve karmaşık siber tehditlerine karşı yeterli koruma sağlayamaz. Bu nedenle nükleer tesislerin, tehditleri önceden algılayabilen ve saldırılara hızlı bir şekilde yanıt verebilen aktif savunma stratejileri geliştirmesi gereklidir.

Aktif savunma, siber tehditlerin erken tespiti ve etkili bir şekilde yönetilmesini hedefler. Bu strateji, gerçek zamanlı izleme ve tehdit analizi sistemlerini içerir. Yapay zekâ ve makine öğrenimi tabanlı çözümler, bu süreçte kritik bir rol oynar. Bir tesisin ağında gerçekleşen anormal bir etkinlik, otomatik olarak tespit edilebilir ve ilgili birimlere bildirilir. Bu, potansiyel bir saldırının erken aşamada durdurulmasını sağlar ve sistemin güvenliğini korur. Ayrıca aktif savunma stratejileri kapsamında, nükleer tesislerde hızlı müdahale ekiplerinin oluşturulması önerilir. Bu ekipler, olası bir siber saldırı durumunda, sistemlerin normale döndürülmesi için gerekli tüm adımları hızla atabilir. Ekiplerin düzenli olarak tatbikat yapması ve yeni tehdit senaryolarına hazırlıklı olması, savunma kapasitesini artırır. Bunun yanı sıra olay müdahale planlarının düzenli olarak güncellenmesi ve test edilmesi gerekir.

Dinamik bir savunma stratejisinin bir diğer önemli bileşeni, sürekli tehdit değerlendirme ve risk analizi süreçleridir. Nükleer tesisler, mevcut tehditleri ve potansiyel riskleri değerlendiren düzenli raporlar hazırlamalıdır. Bu raporlar, güvenlik protokollerinin güncellenmesi ve iyileştirilmesi için temel oluşturur.

Uluslararası İş Birliği ve Standartlaşma

Siber tehditler, uluslararası bir boyut taşıdığı için nükleer tesislerin emniyeti yalnızca ulusal düzeyde alınan önlemlerle tam anlamıyla sağlanamaz. Bu nedenle uluslararası iş birliği ve standartlaşma, nükleer tesislerin siber güvenliğini artırmak için kritik bir rol oynar. Ülkeler arasında bilgi paylaşımı, düzenleyici çerçevelerin uyumlaştırılması ve ortak eylem planlarının geliştirilmesi; siber saldırılara karşı daha etkili bir savunma sağlar.

Birçok uluslararası kuruluş, nükleer emniyet standartlarının oluşturulmasında önemli katkılar sağlamaktadır. UAEA, nükleer tesislerin emniyeti konusunda rehber ilkeler belirlemekte ve üye ülkeler arasında iş birliğini teşvik etmektedir. Özellikle siber güvenlik konularında, UAEA gibi kuruluşların yayımladığı standartlar ve yönergeler, ulusal düzeydeki uygulamalara rehberlik edebilir.

Uluslararası iş birliği özellikle siber tehditlere dair bilgi paylaşımı konusunda büyük önem taşır. Ülkeler, karşılaştıkları tehdit türleri ve saldırı yöntemleri hakkında düzenli bilgi alışverişinde bulunmalıdır. Bu bilgi, diğer ülkelerin benzer tehditlere karşı hazırlıklı olmalarını sağlar. Aynı zamanda, ortaklaşa geliştirilen tehdit izleme ve erken uyarı sistemleri, saldırıların tespit edilmesi ve önlenmesinde etkili bir araç olabilir.

Standartlaşma, koruma önlemlerinin her ülkede tutarlı bir şekilde uygulanmasını sağlar. Nükleer tesislerde kullanılan siber güvenlik yazılımlarının belirli standartlara uygun olması, sistemlerin küresel düzeyde daha güvenilir hâle gelmesini sağlar. Ayrıca standartlara uyum, tedarik zinciri güvenliğini de artırır. Ülkeler arasında uyumlu emniyet standartlarının uygulanması, tedarik edilen ekipman ve yazılımların belirli bir koruma seviyesini karşılamasını garanti eder.

Tedarik Zinciri Güvenliği

Nükleer tesislerin emniyeti ve güvenliği yalnızca tesis içindeki sistemlerin değil, kullanılan ekipman ve yazılımların da güvenli olmasına bağlıdır. Tedarik zinciri güvenliği, bu bağlamda kritik bir öneme sahiptir. Nükleer tesislerde kullanılan bileşenlerin büyük bir kısmı, dış tedarikçilerden temin edilir. Ancak tedarik zinciri boyunca herhangi bir zafiyet, tesisin siber güvenliğini riske atabilir.

Tedarik zinciri güvenliğinin sağlanması için ilk adım, tedarikçi firmaların sıkı bir şekilde denetlenmesidir. Her tedarikçi, belirli bir güvenlik standardını karşılamalı ve bu standartlara uygunluğunu düzenli olarak kanıtlamalıdır. Tedarik edilen yazılım ve donanımların güvenlik testlerinden geçirilmesi, zararlı yazılımların sisteme sızmasını önlemek için gereklidir. Özellikle tedarik zinciri kaynaklı Stuxnet gibi tehditler, bu tür kontrollerin önemini vurgulamaktadır.

Tedarik zincirinde kullanılan bileşenlerin kaynaklarının doğrulanması da önemlidir. Tedarik edilen bir cihazın veya yazılımın kimlik bilgileri ve güvenlik sertifikaları dikkatle incelenmelidir. Bu, sahte veya değiştirilmiş bileşenlerin kullanılmasını önler. Ayrıca yazılımların güvenilir bir kaynaktan indirildiğinden ve hiçbir şekilde değiştirilmediğinden emin olunmalıdır.

Tedarik zinciri güvenliğinin artırılmasında iş birliği de önemli bir rol oynar. Ulusal ve uluslararası düzeydeki düzenleyici kuruluşlar, tedarik zinciri güvenliği için standartlar geliştirmeli ve uygulamalara rehberlik etmelidir. Bu standartlar yalnızca bireysel tesislerin değil, tüm sektördeki koruma seviyesinin yükseltilmesini sağlar.

Fiziksel Koruma ve Siber Güvenliğin Entegrasyonu

Fiziksel koruma ve siber güvenlik, nükleer tesislerin genel güvenliğini sağlamak için birbiriyle entegre bir şekilde çalışmalıdır. Her iki güvenlik katmanı da bağımsız olarak güçlü olsa da entegrasyonları, tehditlere karşı çok daha etkili bir savunma mekanizması oluşturur.

Fiziksel koruma önlemleri, tesisin kritik alanlarına erişimi sınırlamayı amaçlar. Bu önlemler; güvenlik kameraları, erişim kontrol sistemleri ve devriye ekipleri gibi yöntemlerle sağlanır. Ancak bu fiziksel önlemler, siber güvenlik sistemleriyle entegre edildiğinde daha etkili hâle gelir. Örneğin, bir güvenlik kamerası tarafından tespit edilen şüpheli bir aktivite, siber güvenlik sistemine otomatik olarak bir uyarı gönderebilir. Bu tür bir entegrasyon, olası tehditlerin daha hızlı tespit edilmesini ve yanıtlanmasını sağlar.

Siber güvenlik sistemleri de fiziksel koruma önlemlerini destekleyebilir. Örneğin, dijital erişim kontrol sistemleri, yalnızca yetkilendirilmiş personelin belirli alanlara giriş yapmasını sağlar. Bu sistemler,

giriş ve çıkış kayıtlarını tutarak olası bir güvenlik ihlali durumunda detaylı bir inceleme yapılmasına olanak tanır. Ayrıca siber güvenlik protokolleri, fiziksel koruma cihazlarının da siber saldırılara karşı korunmasını sağlar. Fiziksel koruma ve siber güvenlik entegrasyonu, hibrit saldırılara karşı da önemli bir koruma sağlar. Hibrit saldırılar hem fiziksel hem de dijital yöntemleri bir arada kullanarak tesislerin güvenliğini tehlikeye atabilir. Bu tür saldırılara karşı, her iki güvenlik katmanının uyumlu bir şekilde çalışması hayati önem taşır.

SONUÇ

SONUÇ

Türkiye'nin nükleer enerji stratejisi sadece enerji arz güvenliğini sağlamak için değil, aynı zamanda ekonomik kalkınma, teknoloji transferi ve uluslararası iş birliği gibi çok boyutlu hedeflere ulaşmak için de önemli bir araçtır. Artan enerji talebi ve çevresel kaygılar, Türkiye'yi nükleer enerji gibi düşük karbonlu ve sürdürülebilir kaynaklara yönlendirmiştir. Ancak bu projelerin başarısı; güvenlik, toplumsal kabul ve uluslararası standartlara uyum gibi unsurların etkin bir şekilde ele alınmasına bağlıdır.

Nükleer tesisler; fiziksel sabotaj, terörizm ve siber saldırılar gibi çeşitli tehditlerle karşı karşıyadır. Geçmişte yaşanan Stuxnet, Kudankulam ve Natanz gibi olaylar, nükleer altyapıların hem fiziksel hem de dijital güvenlik açısından ne kadar hassas olduğunu göstermiştir. Bu bağlamda Türkiye'nin nükleer enerji projelerinde emniyeti bir öncelik hâline getirmesi gerekmektedir. Fiziksel koruma, yetkisiz erişimi önlemek ve tesisin çevresel tehditlere karşı korunmasını sağlamak için temel bir unsurdur. Ancak dijitalleşen dünyada siber güvenlik, nükleer tesislerin korunmasında daha önemli hâle gelmiştir. Dijital kontrol sistemlerinin güvenliği, siber saldırılara karşı dayanıklı bir altyapı oluşturmayı gerektirir.

Tedarik zinciri güvenliği de kritik bir bileşendir. Türkiye'nin nükleer tesislerinde kullanılacak ekipman ve yazılımların güvenilirliği, uluslararası tedarik zincirindeki potansiyel zafiyetlere karşı sıkı denetimlerle sağlanmalıdır. Aynı zamanda UAEA gibi kuruluşlarla iş birliği artırılarak uluslararası standartlara uyumlu bir nükleer emniyet sistemi oluşturulması gerekmektedir.

Türkiye, nükleer enerji projelerinde siber güvenlik konusuna büyük bir titizlikle yaklaşmakta ve ulusal güvenlik stratejileri kapsamında detaylı önlemler almaktadır. Kritik altyapıların korunması için yalnızca ulusal düzeyde düzenlemeler yapmakla kalmayan Türkiye, aynı zamanda UAEA gibi küresel düzenleyici kuruluşların standartlarına sıkı sıkıya bağlıdır. Akkuyu NGS gibi projelerde uygulanan siber güvenlik planları, ulusal ve uluslararası gerekliliklere uygun şekilde hazırlanmış; tehditlerin erken tespiti, hızlı müdahale ve sistem dayanıklılığını artırma hedeflerini gözetmektedir. NDK'nin OSCP gibi uluslararası tanınan eğitim programlarına katılımı ve yerli siber güvenlik kapasitelerini artırmaya yönelik yatırımları, bu alandaki kararlılığını açıkça göstermektedir. Türkiye, nükleer enerji sektöründe siber güvenliği bir öncelik hâline getirerek potansiyel riskleri minimize etmeyi ve güvenilir, sürdürülebilir bir enerji altyapısı oluşturmayı hedeflemektedir. Bu yaklaşım hem ulusal güvenliği güçlendirmekte hem de uluslararası arenada Türkiye'nin bu konudaki yetkinliğini ve güvenilirliğini pekiştirmektedir.

Sonuç olarak nükleer enerji projeleri, Türkiye'nin enerji politikalarında bir dönüm noktasıdır ve bu projelerin sürdürülebilirliği, kapsamlı bir emniyet anlayışıyla doğrudan ilişkilidir. Türkiye hem ulusal hem de uluslararası deneyimlerden faydalanarak nükleer enerji stratejisini daha güvenli ve sürdürülebilir bir şekilde şekillendirebilir. Nükleer enerji, gelecekte Türkiye'nin enerji bağımsızlığı hedeflerine ulaşmasında stratejik bir araç olmaya devam edecektir.

KAYNAKÇA

KAYNAKÇA

1. *Nuclear Power Reactors in the World*. (International Atomic Energy Agency, Vienna, 2024).
2. TEİAŞ. Türkiye Elektrik Üretim-İletim İstatistikleri. https://www.teias.gov.tr/turkiye-elektrik-uretim-iletim-istatistikleri (2023).
3. Polatoğlu, M. G. Nükleer Enerji Politikalari Ekseninde Türkiye'nin İlk Nükleer Güç Santrali: Akkuyu ve İnşa Faaliyetleri. *ÇTTAD* 24, 389–420 (2024).
4. Alparslan Bayraktar. Hedefimiz 2028'de 4 Reaktörün de Devreye Girmesi. https://enerji.gov.tr/haber-detay?id=21352 (2024).
5. Firdevs Yüksel. Sinop projesinde Rosatom ile işbirliğimizi geliştirmek istiyoruz. https://www.aa.com.tr/tr/ekonomi/enerji-ve-tabii-kaynaklar-bakani-bayraktar-sinop-projesinde-rosatom-ile-isbirligimizi-gelistirmek-istiyoruz/3174313 (2024).
6. Fatih Mehmet Kürkçü. Akkuyu Nükleer Güç Santrali'nde 55 Türk mühendis göreve başladı. *Anadolu Ajansı* (2022).
7. Ayşe Böcüoğlu Bodur. TSE, Akkuyu NGS'de 664 milyon dolarlık yerli ürün kullanılmasını sağladı. *Anadolu Ajansı* (2024).
8. Sezgin Pancar & Mustafa Ünal Uysal. Enerji ve Tabii Kaynaklar Bakanı Bayraktar: Akkuyu NGS'deki ilk reaktörü 2025'te deneme üretimine alacağız. *Anadolu Ajansı* (2024).
9. Burak Bir. Türkiye, IAEA in close cooperation on Akkuyu Nuclear Power Plant's construction: Turkish official. *Anadolu Ajansı* (2023).
10. Akkuyu Nükleer Güç Santrali Projesi. https://enerji.gov.tr/neupgm-akkuyu-nukleer-guc-santrali-projesi-en.
11. Nükleer Enerji Türkiye Ekonomisini Canlandırıyor. https://rosatomnewsletter.com/tr/2021/06/28/atom-stimulates-turkish-economy/ (2021).
12. World Health Organization. Chernobyl: the true scale of the accident. https://www.who.int/news/item/05-09-2005-chernobyl-the-true-scale-of-the-accident (2005).
13. Sofia Lotto Persio. 'No One Died From Radiation At Fukushima': IAEA Boss Statement Met With Laughter At COP26. (2024).
14. Jennifer Brown. Colorado has the highest per-capita rate of skin cancer, thanks to sunshine and high elevation. (2019).
15. Markandya, A. & Wilkinson, P. Electricity generation and health. *The Lancet* 370, 979–990 (2007).
16. Sovacool, B. K. *et al.* Balancing Safety with Sustainability: Assessing the Risk of Accidents for Modernlow-carbon Energy Systems. *Journal of Cleaner Production* 112, 3952–3965 (2016).
17. Ritchie, H. What are the safest and cleanest sources of energy? *Our World in Data* (2020).
18. Pickering, S. & Davies, P. Cyber Security of Nuclear Power Plants: US and Global Perspectives. *Georgetown Journal of International Affairs* (2024).
19. Kuru, H. Cyber Terror Threats Against Nuclear Power Plants. *JOLTIDA* 8, 237–244 (2023).

20. *National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements*. (International Atomic Energy Agency, Vienna, 2021).

21. Akkuyu Nükleer A.Ş'den Bilgilendirme. https://akkuyu.com/tr/news/akkuyu-n-kleer-a-den-b-lg-lendrme-2 (2024).

22. *The Radiological Accident in Goiania*. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub815_web.pdf (1988).

23. *Disposal of Radioactive Waste*. (International Atomic Energy Agency, Vienna, 2011).

24. *The U.S. Nuclear Energy Enterprise: A Key National Security Enabler*. https://efifoundation.org/reports/the-u-s-nuclear-energy-enterprise-a-key-national-security-enabler/ (2024).

25. Echols, T. Why Nuclear Energy is a Matter of National Security. *Public Utilities Fortnightly* (2017).

26. Gattie, D. K. & Massey, J. N. K. Twenty-First- Century US Nuclear Power. *Strategic Studies Quarterly* 14, 121–142 (2020).

27. Gattie, D. Competitive Advantage as a National Security Objective for US Civilian Nuclear Power Policy. *Georgetown Journal of International Affairs* (2024).

28. Squassoni, S. *New Nuclear Energy: Assessing the National Security Risks*. https://elliott.gwu.edu/new-nuclear-energy-assessing-national-security-risks (2024).

29. Ichord, R. & Oosterveld, B. *The Value of the US Nuclear Power Complex to US National Security*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-value-of-the-us-nuclear-power-complex-to-us-national-security/ (2019).

30. Firmage, E. B. The Treaty on the Non-Proliferation of Nuclear Weapons. *American Journal of International Law* 63, 711–746 (1969).

31. Arms Control and Disarmament. https://www.mfa.gov.tr/arms-control-and-disarmament.en.mfa.

32. Dias, T., Hakmeh, J. & Messmer, M. Cybersecurity of the Civil Nuclear Sector: Threat Landscape and International Legal Protections in Peacetime and Conflict. *London: Royal Institute of International Affairs* doi:10.55317/9781784136161.

33. Dine, A., Assante, M. & Stoutland, P. *Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities*. https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf (2016).

34. Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say. *The New York Times* (2017).

35. Mallick, M. G. P. *Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call*. https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf (2019).

36. Livingstone, D., Baylon, C. & Brunt, R. *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*. https://www.chathamhouse.org/archive/cyber-security-civil-nuclear-facilities-understanding-risks (2015).

37. Eggers, S. L. Chapter 5 - Cyber risk considerations for nuclear digital I&C systems. in *Risk-Informed Methods and Applications in Nuclear and Energy Engineering* (eds. Smith, C. L., Le Blanc, K. & Mandelli, D.) 55–72 (Academic Press, 2024). doi:10.1016/B978-0-323-91152-8.00003-X.

38. Victor, C. A Clean Energy Powerhouse: The Digital I&C Systems Modernizing Nuclear. *American Nuclear Society* (2024).

39. Zhang, F. & Kelly, K. Overview and Recommendations for Cyber Risk Assessment in Nuclear Power Plants. *Nuclear Technology* 209, 488–502 (2023).

40. Kesler, B. The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010. *Strategic Insights, Spring 2011* (2011).

41. P. Litherland, R. Orr, & R. Piggin. Cyber Security of Operational Technology: Understanding Differences and Achieving Balance Between Nuclear Safety and Nuclear Security. in *11th International Conference on System Safety and Cyber-Security (SSCS 2016)* 1–6 (2016). doi:10.1049/cp.2016.0856.

42. Csanyi, E. How Stuxnet (PLC virus) spreads. *Electrical Engineering Portal*.

43. Byres, E. Air Gaps won't Stop Stuxnet's Children. *Tofino Security* (2012).

44. Poresky, C., Andreades, C., Kendrick, J. & Peterson, P. *Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies*. (2017). doi:10.13140/RG.2.2.34430.69449.

45. Cyber attack on KKNPP. *Press Information Bureau Government of India Department of Atomic Energy* https://pib.gov.in/Pressreleaseshare.aspx?PRID=1592498 (2019).

46. Das, D. An Indian nuclear power plant suffered a cyberattack. *The Washington Post* (2019).

47. R, N. Cybersecurity in Indian Nuclear Facilities. *Electronic Journal of Social and Strategic Studies* 04, 314–338 (2024).

48. Chulov, M. Israel appears to confirm it carried out cyberattack on Iran nuclear facility. *The Guardian* (2021).

49. O'Grady, S. What we know about the Natanz nuclear site attack. *The Washington Post* (2021).

50. *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)*. https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028-66e97803f13ea.pdf (2024).

51. *Nükleer Santraller Için Siber Güvenlik Planı İçeriği*. https://www.ndk.gov.tr/duyurular/nukleer-santraller-tarafindan-sunulmasi-gereken-siber-guvenlik-plani-icerigi (2024).

52. NDK ile Offensive Security Certified Professional (OSCP) Eğitimi. https://www.digitalvizyon.net/biten-egitimler/ndk-ile-offensive-security-certified-professional-oscp-egitimi.

53. Mohan, P., Glantz, C., Landine, G., Gourisetti, S. N. & Motkuri, R. K. Cybersecurity and Nuclear Facilities. in *The Challenges of Nuclear Security: U.S. and Indian Perspectives* (eds. Kapur, S. P., Rajagopalan, R. P. & Wueger, D.) 245–290 (Springer International Publishing, Cham, 2024). doi:10.1007/978-3-031-56814-5_7.

RA-
POR

SİBER GÜVENLİK PERSPEKTİFİNDEN TÜRKİYE'NİN NÜKLEER ENERJİ STRATEJİSİ

ŞUBAT 2025