NÜKLEER TESİSLERİN SİBER GÜVENLİĞİNE GİRİŞ

Doç.Dr. Salih Bıçakcı

Fakülte Üyesi, Uluslararası İlişkiler - Kadir Has Üniversitesi

1. Giriş: Siber Güvenlikte Roller ve Aktörler

Siber güvenlik, nükleer enerji santrallerinin güvenlik sisteminin vazgeçilemez bir unsurudur. Siber güvenlik kültürünün öncelikli bir konu başlığına dönüşmesinin görece yeni bir gündem konusu olduğu akla getirildiğinde, birçok nükleer enerji tesisinin herhangi bir siber saldırı endişesi taşınmadan tasarlandığı söylenebilir.

Internet, ABD Savunma Bakanlığının parlak bir buluşu olarak Gelişmiş Araştırma Projeleri Dairesi Ağı'nın (ARPANET) sivilleştirilmesiyle birlikte ana gündem maddesi haline gelmiştir. 1990'lı yılların başında telefon hatları üzerinden bağlantı kuran modemlerle başlayan sınırlı internet erişimi, 21. yüzyılın başına gelindiğinde hiper bağlantı seviyesine ulaşmıştır. Kişisel bilgisayarlar, mobil telefonlar ve dijital algılayıcılar ağ kapasitesinin artması ve dünyanın günümüzdeki düzeninin kurulmasıyla neticelenmiştir. Bu yeni araçlar aynı zamanda bilgi üretim ve depolama kapasitelerinin de artmasını sağlamıştır.

Bilginin dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın kullanımı ise dünyayı yeni bir çağa taşımıştır. Bu sistemlerin kullanımının kolaylığı ve etkinliği yöneticilerin toplumları daha rahat kontrol edebilmeleri ve daha iyi yönetim becerileri geliştirmelerini sağlamıştır. Bu türde bir kazancın elbette maliyetleri de olmuştur. Altyapının dijital hale gelmesi, bu sistemleri siber tehlike ve hibrit saldırı tehditlerine karşı daha açık ve hassas bir konuma taşımıştır.

Bu çalışma nükleer güç santrallerinin siber güvenliği konusuna ışık tutmayı ve bu çerçevede karar alıcılara yardımcı olmayı amaçlamaktadır. Türkiye'de inşası planlanan nükleer enerji santralleri, enerji altyapısı altında, birer kritik altyapı tesisi olarak kabul edilmektedirler. Fakat her bir nükleer tesisin kendine has ve farklı tehdit ve hassasiyetleri bulunmaktadır ve bunların esnek-dayanıklılığının (*resilience*) sağlanması için özel yöntemlere başvurmak gerekmektedir. Türkiye'nin gelecek nükleer enerji santrallerinin elektrik şebekesine bağlantılarındaki hassasiyetleri, bu ağa bağlı olan diğer enerji şebekeleri açısından da bir tehdit arz etmektedir.

İşletime girecek olan ilk nükleer santral, gelecekte diğer santrallerde de her seviyede ortaya çıkabilecek her türlü uyum sorunlarının anlaşılabilmesi ve aşılabilmesi açısından bir örnek teşkil edecektir. İlgili yasa ve düzenlemelerin hazırlanması, bilişim sistemlerinin uyumluluğu ve paydaşlar arasında iletişimin devamlılığını sağlarken, etkin bir nükleer emniyet kültürünün geliştirilmesine de yardımcı olacaktır. Nükleer enerji tesislerinin korunması,

nükleer emniyet, siber güvenlik, fiziki emniyet, ulaştırma ve depolama güvenliğini de içeren nükleer güvenlik kültürünün oluşturulmasına bağlıdır. Nükleer emniyet kültürünün yönetimi ve başarısı ise farklı seviyelerdeki birimlerin farklılaşan sorumlulukları yüklenmesi ile bağlantılıdır:

Uluslararası Toplum:

- Gerekli düzenlemeleri yapmak ve uluslararası bir uyarı sistemi oluşturmak amacıyla devletler arasında koordinasyonu sağlamak.

Devletler:

- Sorumlulukları dağıtmak amacıyla genel koruma hedeflerini belirlemek,
- Nükleer güvenlik (safety) ve emniyet (security) ile ilgili bilgiyi korumak,
- İlgili birimleri denetlemek ve bunların düzenlemelerle uyumunu incelemek.

Kuruluşlar:

- Nükleer enerji santralinin korunması için gereken emniyet politikalarını uygulamak. Örneğin:
  - Tehdit seviyesinin belirlenmesi,
  - Fiziki emniyet sistemlerinin tasarlanması,
  - Bireysel sistemlerin emniyet önceliklerinin tanımlanması,
  - Hassas bilginin korunması,
  - Raporlama,
  - Kayıt tutma ve loglama (logging),
  - Kötü niyetli girişimlerin saptanması ve bunlara yanıt verilmesi ile ilgili tedbirleri belirlemek.
- Tesis içindeki birimlerin her birinin, emniyet ve diğer ara yüzler de dâhil olmak üzere, görev, sorumluluk ve denetimlerini sağlayacak yapıların oluşturulması.
- Verilen sorumlulukların yerine getirilmesini sağlayacak yeterli finansal, teknik, eğitsel ve insan kaynağının sağlanması ve kontrolü.
- Devam eden süreçleri, gerekli düzenleme ve düzeltmeleri yapmak amacıyla sürekli gözden geçirmek.

Nükleer Güç Tesislerinin Yöneticileri:

- Sorumlulukları belirlemek,
- En iyi uygulamaları tanımlamak ve kontrol etmek,
- Personelin eğitimi yapmak,
- Personeli güvenlik uygulamaları konusunda motive etmek ve operasyon sırasında karşılaşılan anormal durumları rapor etmelerini sağlamaya

teşvik etmek.
- Gerekli süreçleri denetlemek ve gözden geçirmek.

Personel:
- Bilgi güvenliğini amaçlayan katı ve sağduyulu bir yaklaşım geliştirmek,
- İhtiyatlı davranmak,
- Beklenilmeyen ya da acil herhangi bir durum karşısında hazırlıklı olma süresini kısaltmak.

Bu farklı seviyedeki unsurlar arasında yukarıdaki çerçeveye uygun bir görev dağılımı olsa da, "hızla gelişen teknolojik yeniliklerin ortaya çıkarttığı ve toplumsal tepkilerin ivme kazandırdığı gerçek belirsizlikler, tamamen yeni bir küresel risk alanı yaratmaktadır. Tüm bu yeni belirsiz risk teknolojilerinin muhtemel son ürünleriyle aramız bilinmezlikler okyanusuyla ayrılmış durumdadır."[1]

Stuxnet, kritik altyapının işletilmesinde kullanılan bilgisayar sistemlerine yönelik saldırıların en son ve önemli aşamasıdır. SCADA sistemlerinin doğrudan İnternete bağlantılarının olmaması veya başka bir deyişle bir hava boşluğu (air gap) tarafından korundukları için saldırılara karşı dayanıklı olduklarına dair inanışı tamamen tersine çevirmiştir.[2] Nükleer tesislerin siber güvenliği konusu, özellikle Stuxnet saldırısı sonrasında, nükleer emniyetin devamlılığının sağlanabilmesi adına hayati bir konu halini almıştır. Fiziki altyapıyı internet bağlantısından koparmış olmanın tek başına bir çözüm olamayacağı anlaşılmıştır.[3] Teknoloji ile insan gücü arasındaki ilişkilerin doğası değişmiştir. Bu saptama nükleer santrallerde çalışanlar açısından da geçerlidir. Artık nükleer tesis çalışanlarının da akıllı telefonlar ve tabletler vasıtasıyla Internete erişimleri oldukları kabul edilmiştir.[4]

Sosyal medyada görünür olmak her geçen gün biraz daha yükselen bir değer halini almıştır. Bu haliyle akıllı cihazlar birçok insan için sosyalleşmemenin ana aracına dönüşmüştür. İnsanlar internete bağlanmak ve çevrimiçi kalabilmek için farklı yöntemleri denemektedirler. Fakat sosyalleşmeyi sağlayan bu araçlar, başta kritik altyapı unsurları olmak üzere, yüksek güvenlikli alanların siber güvenliği önündeki öncelikli tehditler halini almışlardır. Tam da bu nedenle nükleer enerji santrali çalışanlarının elektronik akıllı araçlarını dolaplarında kilitli halde bırakmalarını beklemek çok zor bir öngörü olarak karşımızda durmaktadır.

Kısacası, siber ve hibrit tehditler, dünyanın değişen siyasi ve ekonomik koşullarıyla birlikte geometrik biçimde artmaktadır. Siber risk hesaplamaları zafiyetler (*vulnerability*), varlıklar (*asset*) ve siber tehdit tahminlerine dayanmaktadır.

2. Zafiyetler (Vulnerabilities)

2.1. Tasarım

Bir nükleer santralin tasarımı, tehdit değerlendirmesi ile birlikte yapılmaktadır. Başka bir deyişle, tehdit algısı santralin tasarım özelliklerini yakından etkilemektedir. Bu ilişkiyi ortaya koyan çalışma Tasarıma Esas Tehdit (*Design Basis Threat - DBT*) olarak adlandırılmaktadır[5]. DBT, bir devletin cari tehdit değerlendirmesine dayanmaktadır. Nükleer enerji tesislerinin korunması konusunda son dönemlerde yapılan tartışmalar, siber DBT'nin nükleer enerji santralinin güvenliğinin ayrılmaz bir parçası olduğunu göstermektedir. İşletmeciler, nükleer enerji santralinin tasarımını, siber DBT'ye ek olarak sınırlı bir bütçeyle güvenliğini devamlı kılacak biçimde yapmak durumundadırlar. Bunun yanı sıra işletmecilerin nükleer enerji santralinin dayanıklılık ve işlevselliği arasındaki ilişkiye de karar vermeleri gerekmektedir. Bir nükleer enerji santralinin tasarımı aşamasında yapılacak bir hata, siber ve fiziki kırılganlığa yol açabilmektedir.

2.2. Donanım

Nükleer enerji santralinin tasarımı aşamasında yapılan tercihler, bu tesislerde kullanılacak donanımı da belirlemektedir. Zamanla, ortaya çıkan yeni ihtiyaçlar ve değişen güvenlik ortamı eski bilişim altyapısının cevap veremeyeceği bir takım yeni sorunların ortaya çıkmasına ve daha önceden düşünülüp hesaplanmamış yeni bir takım zafiyetlere yol açmaktadır. Stuxnet (ayrıca dragonfly, HAVEX, and black energy) en küçük elektronik donanım unsurları ile geride çalışan kod ve sürücülerin dahi, nükleer tesislerin güvenliği açısından ne düzeyde önemli olabildiğini kanıtlamıştır.[6]

İyi tasarlanmış bir sistemin kurulması nükleer güvenlik ve emniyetin sağlanmasının sadece ilk adımını oluşturmaktadır. Bir nükleer enerji santralının herhangi bir temel aksama ile karşılaşılmadan çalışmaya devam etmesi ve bu bağlamda tesisin emniyet ve güvenliğinin sağlanması için donanım sağlayıcıları da önemli bir rol oynamaktadırlar. Bir Rus haber kaynağı 2013 yılında, bir teknisyenin Çin'den ithal edilen ütünün şarj cihazında bir "spy chip" bulduğunu iddia etmiştir. Bu minik elektronik devreler, asıl elektronik araçlara eklenerek 200 metrelik yarıçapa sahip

bir alanda korumasız kablosuz ağ kullanarak, bilgisayara bağlanmakta ve virüs bulaştırmaktır.[7] Bu basit örnek dahi bize nükleer emniyet ve güvenliğin, DBT'ye olduğu kadar, güvenilir sağlayıcılarla iş yapmaya da bağlı olduğunu göstermektedir. Nükleer santrallerin yedek parçalarını güvenilir bir sağlayıcıdan almaları gerekmektedir. Her bir yedek parça için, bu parçanın nükleer enerji santralinde kullanılan donanıma uyumlu olup olmadığını denetleyecek bir doğrulama süreci olmalıdır.

Nükleer enerji santralleri yıllarca faaliyet gösterdikleri için, tesisin işletmecileri sistemin aksamadan çalışmasını sağlamakla ve tesisin ve donanımların eskiyerek kırılganlığa yol açmasının önüne geçecek uzun ömürlü işletim stratejilerini geliştirmekle yükümlüdürler.

Hackerların ve Advanced Persistent Threats (İleri Düzey Kalıcı Tehdit-APT) saldırganlarının çoğunluğunun ihtiyaç duydukları bilgiyi çöp kutularından elde ettikleri gerçeği akılda tutularak, nükleer enerji tesislerinin nükleer atıkların yanısıra geleneksel atık yönetimi sistemlerine yönelik özel güvenlik önlemleri geliştirmeleri şarttır. Hackerların donanımlarını ve özel bilgi seviyelerini geliştirmek ve saldırı planlamak amacıyla nükleer tesisler tarafından geri dönüşüme verilen ya da açık artırmayla satılan donanımları satın aldıkları örnekler bulunmaktadır. Bunun önüne geçilmesi için her bir nükleer enerji santralinin, radyoaktif olmayan malzemenin elden çıkartılmasını sağlayacak, iyi organize edilmiş bir atık yönetimi sistemi kurması gerekmektedir. İşletmeciler, nükleer enerji tesislerinin donanım yedek parçalarının kötücül yazılıma (*malware*) karşı kontrolüne yardımcı olacak işletme yaşam süreci yönetimini (life cycle management programs) kurmalıdırlar. Bu türde imkân ve kabiliyetlerin geliştirilmemesi, nükleer enerji santrallerinin faaliyetlerinin durması anlamına gelmektedir.

2.3. Yazılım

Yüklenecek yazılımın güvenli olup olmadığının kontrolünü yapmaktan nükleer tesisin bilgisayar güvenliği uzmanları sorumludur. Kırılganlık listesinin en üstünde "Zero-day exploits"[8] ve özel iletişim protokolleri[9] (*special communication protocols*) yer almaktadır. Gelişmiş/tecrübeli saldırganlar, yüksek düzeyli güvenliğe sahip nükleer tesislere, daha düşük seviyede bir dirençle karşılaşmak amacıyla az bilinen zafiyetleri kullanarak saldırmayı tercih etmektedirler. Nükleer tesislerin bilgi işlem merkezleri,

zaman zaman sistemlerine entegre edilecek yeni kod yazılmasını talep etmektedirler. Güvenlik ve emniyet ihtiyaçlarını dikkate almadan, fonksiyonel amaçlarla hızlıca yazılmış olan bu kodlar nükleer tesisi risk altında bırakabilmekte, ve bu nedenle kodların ana sisteme yüklenmeden önce mutlaka bir uzmanlar grubu tarafından düzenli biçimde test edilmesi gerekmektedir.

Bir diğer yazılım güvenliği sorunu de varsayılan (default) güvenlik ayarlarının kullanılmasıdır. Bilgi işlem merkezleri yazılımlar için genellikle varsayılan güvenlik ayarlarına güvenmektedirler. Fakat bu ayarların büyük bir çoğunluğu ortalama sistemlere göre tasarlanmış, dolayısıyla nükleer tesisler gibi özel gelişkin sistemlerin ihtiyaçlarını karşılayamamaktadırlar. Her bir nükleer tesisin kendine has özellikleri olması nedeniyle mühendis ve bilişim uzmanlarının tesisin ihtiyaçlarını ve özel koşullarını dikkate alan yazılımları (güvenlik duvarı, ihlalleri saptama sistemleri-IDS ve emniyete ilişkin programlar gibi) kurmaları gerekmektedir.

Nükleer tesislerin siber güvenliğini yüklenici firmalara devretmek de potansiyel bir takım riskler taşımaktadır. Endişeye yol açabilecek ilk başlık entegrasyondur. Bilişim şirketleri her ne kadar yazılımlarının uyumlu ve güvenilir olduğunu savunsalar da, bu yazılımların tesisin sistemine yüklenmesi sırasında beklenilmeyen bir takım sorunlar ile karşılaşabilinilmektedir. Yüklenici firmaların sürece müdahil olmasıyla çıkabilecek ikinci sorun, yüklenici şirketin yükleme sırasında teknik bilgiyi tesisin işletmecileriyle paylaşmamasıdır. Yüklenici firmaların büyük bir çoğunluğu piyasadaki göreceli avantajlı konumlarını koruyabilmek amacıyla deneme sürecinde kod ve programlarıyla ilgili hiç bir bilgiyi paylaşmamaktadırlar. Bu süreçte herhangi bir gözetim mekanizması olmaması nedeniyle de bu gizli kodlar, nükleer tesisin güvenliğine yönelik beklenilmeyen bir takım zafiyetler yaratabilmektedirler. Bu nedenle düzenleyicilerin, tesislerin saldırılara karşı güvenliklerinin sağlanabilmesi amacıyla, işletmecilerin siber ürünlerin test aşamalarını büyük bir dikkatle yürütmelerini sağlayacak süreçleri planlayarak yürütmelerini sağlamaları şiddetle tavsiye edilmektedir.

Yüklenicilerden kaynaklanan potansiyel risk faktörlerinden bir diğeri bu şirketlerin çalışanlarının bakım ve onarım gibi görevlerle sağlayıcı odalarına (*server rooms*) erişimlerinin olmasıdır. Bu nedenle fiziki ve siber güvenlik birimlerinin yüklenici firma çalışanlarının tesisi içinde bulundukları ve yükleme yaptıkları zamanlarda onlara eşlik etmelerinin sağlanması

gerekmektedir. Böylece, tesisin bilgi ve yazılım bütünlüğü daha etkin bir şekilde güvenlik altına alınacaktır. Düzenleyiciler ve bilgi teknolojileri birimleri işletmecilerden ayrıca sistemin güncellemesinde kullanılan yama yönetim sistemlerinin kontrolünü de düzenleyiciye vermelerini talep etmelidirler.

Nükleer tesislerin büyük bir çoğunluğunda statik kodlu kötücül yazılımları yakalamak amacıyla programlanmış anti-virüs programları bulunmaktadır. Anti-virüs programları bu kötücül yazılımları, statik kodlar bir tür örüntü oluşturdukları için kolaylıkla tanımakta ve tanımlamaktadırlar. Fakat kendi kendisini yenileyen (*self-modifying*) kötücül yazılımlar davranış değişikliklerinde bulunarak ya da kod gizleme teknikleriyle dinamik anti-virüs programlarını başarısızlığa uğratabildikleri için IT birimleri için artan bir tehdit haline gelmektedirler. Bu kötücül yazılımlar, yazılımın farklı düzeylerine uyum göstererek gelişmekte ve bilgisayarlara virüs bulaştırmaktadırlar. Anti-virüs programları, kodlama yapılarındaki hızlı ve sürekli değişiklikler nedeniyle bu çok biçimli kötücül yazılımları (*polymorphic malwares*) saptamada zorlanmaktadırlar. Günümüzde bu kötücül yazılım kodlamasının en üst seviyesi evrimsel programlamadır (*evolutionary programming*)[10]. Evrimsel programlama, programcının hedeflerine hizmet eden ve en uygun değişken ve dayanıklı kodları bulmayı amaçlayan evrimsel simülasyon metoduna verilen addır.[11]

2.4. İnsan Sermayesi

Ekipman, donanım ve yazılımlar ancak onları kullanan insanlar kadar zekidirler. Nükleer enerji santrallerinde, başta nükleer hırsızlık olmak üzere, içeriden kaynaklanan tehditler öncelikli zafiyetler arasında kabul edilmektedir. Güvenlik ortamı açısından insan kaynağı konusu, genel olarak, ahlaki değer yargılarının en güvenilir bireylerin davranışlarını dahi etkilemesi ihtimali dikkate alındığında, en sorunlu başlıklardan biri olarak gözükmektedir.[12] Benzer biçimde, siber güvenlik açısından insan kaynağı tehdidi de personelin siber saldırılara suç ortağı olmaları, ya da dışarıdan unsurların çalışanları bilişim sistemlerini kırmak için kullanabilmeleri birer tehdit olarak kabul edilmektedir.[13] Bilişim sistemlerinin ihlali konusunda Uluslararası Atom Enerjisi Kurumu (UAEK) tarafından rapor edilmiş çok az sayıda belge bulunmakla birlikte, siber güvenlik literatüründe

sistemlere yönelik içeriden kaynaklanan tehditlere dair geniş bir literatür bulunmaktadır. [14]

Kasıtsız kötüye kullanım da nükleer enerji santrallerinin çalışmasına olumsuz etki edebilmektedir. Santral yönetimi genelde çalışanlara odaklanmış olmakla birlikte yükleniciler ve tesise dışarıdan gelen diğer çalışanlar da risk yaratabilmektedirler. Stuxnet örneği bize "zorlu hedeflere sızmak için kullanılabilecek bir takım ana yoları işaret etmesi nedeniyle, muhtemel saldırganların varlığına işaret eden kullanışlı bir yol haritası" sağlamaktadır.[15] Saldırganlar, sistemdeki 15 ayrı güvenlik duvarı, üç bilgi diyodu ve sızıntı saptama sistemlerini aşarak doğrudan bir sızma eylemi gerçekleştirmek yerine nükleer enerji santralinin merkezine erişim yetkisine sahip yumuşak hedeflere sızmak gibi daha dolaylı yolları kullanmayı tercih etmişlerdir.[16] Düzenleyiciler bu nedenle sadece işletmeci ve çalışanların değil, yüklenicilerin de geçmişlerini titizlikle ve sistematik bir biçimde kontrol etmelidirler.

Nükleer güç santralinin siber güvenliği aşağıdaki şu dört noktaya odaklanmaktadır:[17]

- Yetkisiz bilgi ulaşımı (gizliliğin kaybı)
  - Kötü niyetli ya da farkında olmayan çalışanlar;
  - Saldırganların dikkatsiz çalışanların ihmalkarlıklarını kullanarak kimlik hırsızlığı yoluyla bilgiye ulaşmaları;
- Yazılım ve donanımın engellenmesi ve bilgi değişikliğine gitme (bütünlüğün kaybı)
  - Bilgiye zarar veren, açığa çıkartan ya da ele geçiren virüs, solucan ve Truva Atları;
  - Saldırganların uzak sistemleri çalıp, bu sayede bilgiye erişim sağlaması;
- Bilgi iletim hatlarının bloke edilmesi ve/veya sistemin kapatılması (mevcudiyetin kaybı)
  - Yangın, su baskını ve deprem gibi felaketlerin elektrik kesintilerine ya da araç ve donanımın kaybına yol açması;
- Bilgi iletişim sistemleri ya da bilgisayarlara yetkisiz erişim/sızma (güvenilirliğin kaybı)
  - Bilgisayarları çalabilen ya da sağlayıcı odalarına, dosya dolaplarına veya ofislere erişim sağlayan saldırganlar;

- Ele geçirdikleri sistemleri kamuya açık ağlarda açık edebilen veya uzaktan sistemlerin hareketlerini kontrol ya da takip edebilen saldırganlar.

Hâlihazırda saldırı pozisyonunda bulunmak savunma yapmaktan daha avantajlı gibi gözükse de, siber alanın kurallarının henüz tam anlamıyla belirlenmediği söylenmelidir. Siber alanda hem savunma hem de saldırı imkân ve kabiliyetleri sürekli biçimde gelişmektedirler. Düzenleyici ve işletmeciler, siber güvenliğin daha bilgisayar ve sistemlerin açma düğmesine basılmadan önce başladığını akıllarında tutmalıdırlar. Bu bağlamda, nükleer emniyet ve güvenlik kâğıt üzerinde sağlanması kolaydır. Sahadaki unsurlar arasında etkin iletişim kanallarının kurulması ve bunların uyum içinde çalışmasının sağlanması zorlu bir mücadeleyi gerektirmektedir.

3.Siber Olaylar

Nükleer enerji tesislerinde SCADA ve endüstriyel kontrol sistemlerinin kullanılıyor olması, siber güvenlik olaylarını ve bilgisayar sorunlarını araştırmacıların dikkatine taşımaktadır. Nükleer enerji tesislerinin yanı sıra, bu kategorideki her türlü bilgi yüksek hassasiyet düzeyindedir. Nükleer enerji santraliyle ilgili bilgilerin yüklü olduğu platformlara yönelik olarak düzenlenmiş saldırı örnekleri bulunmaktadır.[18] Aşağıda örnek olay olarak anlatılan 7 siber olay, bizlere siber aksaklık ve saldırının boyutları ve ciddiyeti hakkında bir fikir verecektir.

3.1. Slammer Solucanı ve David Besse Nükleer Enerji Santralı

Slammer solucanı, son kullanıcı bilgisayarına bulaşmak (*infect*) amacıyla yazılan bir solucan olmadığı için, tipik bir kötücül yazılım olarak kabul edilemez. Slammer solucanı, Microsoft SQL sağlayıcılarını ve Microsoft Data Engine (MSDE) 2000'le çalışan bilgisayarları etkilemeyi amaçlamaktadır. Solucan, bilgisayarın hard diskine yerleşip herhangi bir dosyaya virüs bulaştırmadığı için teknik elemanlar solucanı temizlemek için basitçe sistemi yeniden başlatmaktadırlar. Solucanın esas rolü ağın yükünü artırmak ve bu sayede "buffer overflow" olarak adlandırılan bir hataya yol açarak SQL sağlayıcıları kullanıcılarına görünmez kılmaktır. 24 Ocak 2003'te ABD'de bu şekilde solucanın bulaştırılmış olduğu bilgisayar sayısı en üst seviyeye ulaşmıştır.[19] Bu bilgisayarlar arasında, Ohio'daki David-Besse Nükleer Enerji Santrali'nin bilgisayarları da yer almaktadır.

Araştırmacılar, temizleme sürecinin sonunda, solucanın nükleer santrala First Energy Nuclear isimli bir yüklenicinin ağından ulaştığını saptamışlardır. Solucanın yolunu, lisan sahibinin David-Besse'nin kurumsal ağına bağlanan T1 hattını kullanarak bulduğu anlaşılmıştır. David-Bessa nükleer santralinin güvenlik duvarının aslında Slammer solucanının kullandığı port'u bloke etmek üzere programlanmış olmasına rağmen, David-Besse'nin iş ağı üzerinde bulunan çeşitli geçişlerin varlığı, bu türde bir sonuca neden olmuştur. Microsoft, Slammer solucanının tesisi vurmasından altı ay kadar önce, bu konuda yardımcı olacak ağ yamaları konusundaki bilgiyi yayınlamış olsa da, tesisin bilgisayar mühendisleri bu ağ yamalarını sisteme yüklememişlerdir. Güvenlik odaklı çalışmalar yapan

SecurityFocus web sitesi olayları anlatan zaman çizelgesinin tutanaklarını şöyle yayınlamıştır:

> "Tesis çalışanları saat 16:00'da tesisin ağındaki yavaşlamayı fark ettiler. Saat 16:50'de solucanın sebep olduğu tıkanıklık, tesisin Emniyet Parametreleri Gösterge Sistemi (*Safety Parameter Display System SPDS*) olarak adlandırılan kompüterize edilmiş gösterge panelini çökertti.
>
> SPDS monitörleri; soğutma sistemleri, çekirdek ısı sensörleri ve harici radyasyon sensörleri gibi tesisin en önemli güvenlik göstergeleridir. Bir uzman, bunların çoğunluğunun tesis kapalı durumdayken dahi izlenmesi gereken göstergeler olduğu bilgisini vermektedir. Bir SPDS'nin 8 saatten daha uzun bir süre çalışmaması durumunda Nükleer Düzenleme Komisyonu'nun (Nuclear Regulatory Commission NRC) bilgilendirilmesi gerektirmektedir.
>
> Saat 17:13'de Tesis Süreç Bilgisayarı (*Plant Process Computer*) olarak adlandırılan, daha az önemde bir izleme sistemi daha çöktü. Her iki sistemin de solucandan etkilenmemiş durumda, kullanılmayan analog yedekleri bulunmaktaydı. Fakat danışman kuruluş niteliğindeki March "SPDS ve PPC'nin ulaşılabilir olmaması, işletmeci açısından ağır bir sorumluktur" değerlendirmesini yapmaktadır.
>
> SPDS'nin yeniden çalışır hale getirilmesi 4 saat 50 dakika, PPC'nin ki ise 6 saat 9 dakikayı aldı."[20]

Davis-Besse örneği, nükleer enerji tesislerinin kötücül yazılım saldırılarına karşı korumasız ve Scada sistemlerine yapılan uzaktan izleme bağlantılarının da siber saldırılara karşı artan bir riskle karşı karşıya olduğu gerçeğinin altını açıkça çizmektedir.

3.2. Browns Ferry Nükleer Enerji Santralı

1974 yılında Alabama Athens yakınlarında inşa edilen Browns Ferry Nükleer Enerji Santrali, dünyanın en büyük nükleer enerji santrallerinden biridir. Bu tesiste Ağustos 2006'da yaşanan olay, reaktörlerin kritik unsurlarının da siber saldırıların yarattığı aksaklıklar karşısında zafiyet içinde olduklarını göstermiştir.[21] Tennessee Valley Authority (TVA) işletmecisi, su devridaim pompasının, ağda yaşanan yüksek trafik nedeniyle faaliyetinin durması sonrasında santralin iki reaktöründen

birisini manuel olarak kapatmak zorunda kalmıştır. Devridaim pompaları, reaktöre pompalanan suyun akışını kontrol ettikleri ve kaynar sulu reaktörlerin (*boiling-water reactors*) enerji çıktısını yönettikleri için kritik bir role sahiptirler. NRC raporunda da belirtildiği üzere, "Ruhsat sahibi, olayın ana sebebinin tesisin ICS ağındaki yoğun trafik nedeniyle devridaim pompasının VFD (*variable frequency drive*) kontrolörünün arıza vermesi olduğu kararına varmıştır."[22] Devridaim pompalarının kapatılmasının sonuçları bilinmekle birlikte arızaya neden olan ağdaki yoğun trafiğin nedenini ortaya koyacak mantıklı bir açıklama bulunmamaktadır.

Byres Security isimli şirketin CEO'su Eric Byres, sorunun kontrolörün, tesisin devridaim pompasında yanlış ağ kodları kullanması olduğundan şüphelenmektedir. Byres, "aşırı trafik yaratarak sistemin çökmesine neden olan kod, bilinen bir yazılım hatasıdır (bug)"[23]. Diğer taraftan NRC raporu, şu noktaya dikkat çekmektedir: "ağdaki aşırı yüklenmenin sebebi açıklanamadığı sürece, ne lisans sahibi olan şirketin ne de NRC'nin bunun dışarıdan kaynaklanan bir hizmet dışı bırakma saldırısı (*denial-of-service attack*) olup olmadığını bilmesine imkân yoktur."[24] Bu iddiayı desteklemek için logların ve ilgili verilerin bağımsız denetçilerce incelenmesi gerekmektedir.

3.3. Hatch Nükleer Enerji Santralı

Hatch Nükleer Enerji Santralı olayı, nükleer tesislerdeki ağ bağlantısı sorunlarının altını çizmektedir. Baxley, Georgia yakınlarındaki Hatch Nükleer Enerji Santralı, bir yazılım güncellemesi nedeniyle 48 saatliğine acil bir biçimde zorunlu kapatılmayla karşı karşıya kalmıştır. Nükleer tesisin 2 numaralı ünitesi, Southern Company isimli lisanlı şirketin bir mühendisinin, tesisin idari ağında kullanılan bir yazılımı güncellemesine kadar düzgün bir biçimde çalışmaktaydı. Mühendisin güncelleme sonrasında bilgisayarı yeniden başlatmasıyla (*reboot*) birlikte bilgisayar süreç kontrol ağından (*process control network*) sistem kontrol bilgisi (*diagnostic data*) toplamaya başladı. Bu, kontrol sisteminin eşleme programının tekrar kurulmasını ve sistemin, reaktörün rezervuarındaki su miktarında ani su azalması olarak algılayarak otomatik kapatma sistemini başlatmasına neden oldu.

Southern Company'nin sözcüsü Carrie Phillips, devreye giren acil durum sistemlerinin, nükleer enerji santralının emniyetinin sağlanması için tasarlandığını açıklamıştır. Phillips, güncellemeyi yükleyen mühendisin

yazılımın bu şekilde tasarlandığını bilmediğini ve herhangi bir yeniden başlatma (reboot) durumunda sistemin kendisini tekrar kurduğunu (system reset) ve diğer ağları da buna zorladığını sözlerine eklemiştir.[25] Bu olay enformasyon teknoloji sistemleri endüstriyel kontrol sistemleriyle, gerekli tasarım öncelikleri dikkate alınmadan bağlantılandırıldığında beklenilmeyen sonuçlarla karşılaşılacağını göstermektedir. Hatch olayı bize SCADA sistemlerinin korunmasının, ayrıntılı iş bölümünün olduğu bir müdahale stratejisi gerektirdiğini kanıtlamıştır.

3.4. ABD'deki Nükleer Santrallara Yönelik Kötücül Yazılım Saldırıları

Nükleer enerji santrallarının zafiyetleri kritik bilgi olarak kabul edildiği için bu tesislerde meydana gelen olaylar genellikle kitlesel medyada yer almamaktadır. NRC raporlarına bakıldığında, 2008-2010 döneminde bilgisayarların işleyiş, depolama ve taşınması sırasında çeşitli olayların meydana geldiği anlaşılmaktadır.[26] Stuxnet olayının ortaya çıkması ise nükleer tesislerde kullanılan SCADA/ICS sistemlerine yönelik tehditlere dair algıyı değiştirmiştir. Stuxnet saldırısında virüs bulaştırılmış bir USB'in (*Universal Serial Bus*) kullanılmış olması, bu tür araçlara yönelik bir hassasiyet yaratmıştır.

ABD'de yaşanan benzer tecrübeler USB olarak adlandırılan sürücülerin kritik altyapıya bir tehdit oluşturabileceğini göstermektedir. Ekim 2012'de bir teknisyenin, nükleer enerji santralının ekipmanının planlı bakımı için, santralın çalışmasının durdurulduğu sırada sorunlu bir USB'yi sisteme bağlaması sebebiyle santral, üç hafta boyunca kapalı kalmıştır.[27] Yüklenici firmada çalışan teknisyen bunu, USB'nin virüslü olduğunu bilmeden gerçekleştirmiştir. ABD İç Güvenlik Müsteşarlığı santralın adını ve konumunu belirtmese de, yüklenicinin USB'siyle sisteme yüklenen kötücül yazılımın Mariposa virüsünün değişik bir türü olduğunu açıklamıştır. [28] Mariposa, siber güvenlik listesinde, bir virüsten ziyade virüs bulaştırılmış bilgisayarlardan kişisel bilgi, hesap numarası, kullanıcı adı, şifre ve banka bilgilerini toplayan bir böcek olarak sınıflandırılmıştır. Bu virüslü bilgisayarlar aynı zamanda dağıtık hizmet dışı bırakma saldırısı (distributed denial of service attacks -DDoS) düzenlemek için de kullanılabilmektedirler.

Benzer bir diğer olay, bir çalışanın sorun yaşadığı bir USB sürücüsünü

kontrol etmeleri için IT birimine vermesiyle yaşanmıştır. IT görevlisi USB'yi güncel bir virüs programının yüklü olduğu bir bilgisayara takması sonucunda, USB'de yüklü olduğu anlaşılan üç kötücül yazılımdan birinin gelişmiş bir virüs olduğu anlaşılmıştır.[29] Sonuçları gören IT görevlisi tesisteki çeşitli bilgisayarları kontrol etmiş, bunlara da adı geçen gelişmiş virüsün bulaştırılmış olduğu anlaşılmıştır.

Bu türde örnekler bize, USB sürücülerinin nükleer enerji santrallarının siber güvenliği açısından kritik roller oynayabildiğini göstermektedir. İki araştırmacının BlackHat Konferansı'nda yaptıkları bir sunum, nükleer tesise yönelik olarak bir USB sunucusuyla düzenlenecek bir saldırının sadece kötücül bir yazılımın yüklü olduğu USB sürücüsü aracılığıyla değil, bilgisayarla USB bağlantıları sayesinde iletişim halinde olan yazıcı, tarayıcı gibi diğer bağlantılar aracılığıyla da düzenlenebileceğini göstermiştir.[30]

3.5. Nükleer Enerji Santrallarına Yönelik Uluslararası Sabotaj ve Yetkisiz Erişim (*Break-in*) Girişimleri

Kritik altyapıya yönelik tehditlerin başında, üst düzey hackerların gündelik faaliyetleri arasında yer alan, sistemlerin kontrolünü elde etmek için çeşitli alternatif yollar arama olarak kabul edilebilecek olan, geniş çaplı siber keşif aktiviteleri yer almaktadır. ABD'de yaşanan olaylar arasından seçilen iki farklı örnek, bize devletlerin diğer devletlerin kritik altyapı ve kaynaklarını koruma imkân ve kabiliyetlerini nasıl sınadıklarını göstermektedir.

Bir grup hacker, sistemlerinin nasıl aşılabildiğini test etmek amacıyla Kuzey Amerika'daki çeşitli doğal gaz üreticilerinin sistemlerine saldırmıştır. Bu saldırıların birinde, bir nükleer tesisin yönetiminin haber bülteninin alıcı listesi hackerlar tarafından ele geçirilmiş ve bülten gönderilmeden önce, bu listede yer alan e-posta adreslerine bir casus yazılımın yüklü olduğu e-postalar gönderilmiştir.[31] Bu girişim, Santa Barbara'nın kuzeyindeki Diablo Canyon nükleer enerji santralinin bilgisayar ağına zorla girilmesi başarısıyla neticelenmiştir.

Ağustos 2012'de Çinli bir hacker grubunun bir Amerikan nükleer tesisine sızması bu türde saldırılara örnek teşkil eden bir diğer girişimdir. ABD İç Güvenlik Müsteşarlığı, saldırıya uğrayan bu tesisin ve benzer saldırılarla

karşılaşmış olan diğer tesislerin adlarını, tesisleri ileride yaşanabilecek benzer saldırılardan korumak amacıyla açıklamamıştır. Çinli askeri hackerlar tesisin kıdemli yöneticisinin bilgisayarının kontrolü ele geçirmeyi başarmışlardır. Tesisin olay inceleme ekibi, yaptığı araştırma neticesinde, Çinli hackerların bir Amerikan nükleer reaktörünün güvenlik ve işletim zafiyetlerini tanımlamayı amaçladıkları sonucuna varmıştır.[32]

3.6. Monju Nükleer Enerji Santralı

Japonya'daki Fukui bölgesindeki Tsuruga şehrinde kurulu bulunan Monju nükleer reaktöründe, normal şartlarda tesisin nöbetçi personelinin şirketin gündelik evrak işleri için kullanmakta olduğu bir bilgisayar 2 Ocak 2014 saat 15:00'de, şüpheli bir biçimde, bilinmeyen bir web sitesinden bilgi alıp göndermeye başlamıştır. Yapılan dikkatli ve ayrıntılı inceleme neticesinde virüsün, bilgisayara kayıtlı görüntüleri yeniden oynatmak için yüklenmiş olan bir programın düzenli güncellemesi yüklenirken bulaştığı anlaşılmıştır. Japon Atom Enerjisi Kurumu, virüs bulaşan bilgisayarın, daha sonra düzenlenebilecek saldırılarda kullanılması muhtemel bir takım hassas bilgi, çalışan bilgi formları ve eğitim programına dair loglar içermesine rağmen, sızan bilgilerin tesisin güvenliğine herhangi bir tehdit oluşturmadığını iddia etmiştir. Monju Nükleer Enerji Santrali'nde yaşanan bu olay, tesislerde, tesisin siber saldırılardan korunması amacıyla, olay inceleme ekiplerinin bulundurulmasının ne kadar önemli olduğunu göstermektedir.[33] Bu tesislerde olay inceleme ekiplerinin görevlendirilmesi, nükleer enerji santralı işletmecilerince, ekonomik açıdan maliyetli ve uygulanmaz olarak görüldüğü için bu türde görevler genelde tesis mühendislerine verilmektedir. Fakat olay incelemesi, siber saldırıların anlaşılması ve izlerinin sürülmesi açısından bir takım özel tekniklerin bilinmesini gerektirmektedir.

3.7. ICS ve SCADA Sistemleri Açısından Bir Dönüm Noktası: Stuxnet

Haziran 2010 başında, İran'daki bir güvenlik mühendisi Belarus'ta bulunan anti-virüs yazılımları geliştiren VirusBlokAda'yı telefonla arayıp, Windows işletim sistemi ile çalışan bilgisayarların ekranlarının mavi bir ekran haline dönüşerek donduğu ve bilgisayarların sistemi kendiliğinden yeniden yüklemeye başladığı bilgisini vermiştir. VirusBlokAda'nın sistem

kurtarma teknolojilerinden sorumlu programcısı Sergey Ulasen, İran'daki meslektaşıyla yaptığı ilk değerlendirme sonrasında hatayı saptamış ancak sorunun çözümünü tespit edememiştir. Ulasen'e, sorunun çözümü için derinlemesine inceleme yapmak üzere, sisteme uzaktan erişim yetkisi verilmiştir. Ulasen, ilk incelemeler neticesinde, kötücül yazılımın kendisini Tayvanlı güvenilir bir donanın sağlayıcısı, Realtek Realtek Semiconductor'un gerçek dijital sertifikasına sahip, sıfır-gün zafiyeti[34] kullanmakta olan işletim sistemine bir sürücü olarak tanıttığını fark etmiş, böylece Stuxnet'in en iyi biçimde yamanmış Windows bilgisayarlara dahi bulaşabileceği ve sertifikalarının çalınabileceği açıklığa kavuşmuştur. VirusBlokAda, bu zafiyeti 12 Haziran'da Microsoft'a iletmiş ve saptamalarını daha sonra bir güvenlik forumunda paylaşmıştır. Tanınmış güvenlik bloggerları da güvenlik sektöründe ilgi uyandıran bu bilgileri 15 Temmuz'da Internette paylaşmışlardır. Son dönemde Symantec tarafında yapılan çalışmalar, Stuxnet 0.5'in ilk sürümünün Kasım 2005'den bu yana aktif olduğunu açığa çıkartmıştır. [35]

VirusBlokAda tarafından "Rootkit Tmphider" ismi verilen kötücül yazılım sonradan Symantec tarafından ilk önce "W32 Temphid" olarak adlandırılmış ve takiben "W32 Stuxnet" şeklinde değiştirilmiştir. Stuxnet internette yayılmak üzere tasarlanmamıştır. Aksine, Stuxnet'in virüs bulaştırılmış bir USB vasıtasıyla yerel ağdaki bir Programlanabilir Mantıksal Kontrol Aygıtı'na (Programmable Logic Control - PLC) bulaştırıldığı hedeflenmiştir. Bir USB sürücüsü vasıtasıyla sisteme bulaştırılan bu kötücül yazılım, komuta kontrol servis sağlayıcısına bağlanmak üzere programlanmıştır. Stuxnet, bu sayede saldırıyı düzenleyene hareket serbestliği kazandırmakta ve bulaştırılan bilgisayar vasıtasıyla sisteme daha fazla kötücül kod yüklemesi yapılabilmektedir.

Stuxnet, bir USB sürücüsünün sisteme virüs bulaştırması yoluyla ortaya çıkmaktadır. Stuxnet, dört farklı sıfır gün zafiyetini ve çalınmış dijital sertifikaları kullanmaktadır. Bu sıfır gün zafiyetlerinden biri, virüsün ortak yazıcıyı kullanan Windows yüklü bilgisayarların tamamına yayılmasına yol açan yazıcı belge yönetim sistemindeki (print spooler) bir hatadır. Microsoft bu yamayı kullanmayı, Nisan 2009'da Polonya'da yayınlanan bir güvenlik dergisinin bunu açığa çıkartmasıyla bırakmıştır.[36] Tüm bu ipuçları saldırganların hedeflerinin internete bağlı olmadığını bildiklerini göstermektedir. Symantec'in tersine mühendislik girişimlerinin ortaya çıkarttığı biçimiyle; "Stuxnet'in, Rus matruşka bebekleri gibi şifrelenmiş

tabakalardan oluşan ve tamamı birbirine sarmalanmış 3 ana parçası ve buna bağlı 15 bileşeni vardır. Kötücül yazılım, kötü niyetle yazılmış kodların bulaştırılması yoluyla Simens kontrol sistemlerinin kullanıldığı PLC'leri ele geçirmeyi hedeflemiştir."[37] Endüstriyel kontrol sistemlerinin kullanımı, bu saldırının İran'daki Buşehr ya da Natanz nükleer enerji santrallerini hedeflediği yönündeki spekülatif değerlendirmelerin yapılmasına neden olmuştur. Daha sonra yapılan incelemeler neticesinde, Stuxnet'in Natanz nükleer enerji santrelini hedeflediği anlaşılmıştır.

Yapılan incelemeler, Stuxnet'in işletim kodu hakkında da bir fikir vermektedir. Kötücül yazılım, muhtemelen sistemin nasıl çalıştığını anlamak amacıyla sisteme yerleşerek iki hafta boyunca keşif yapmaktadır. Saldırı, İran'ın uranyum zenginleştirmesi için kullandığı santrifüjlerin dönen motorlarının 1,064Hz olan hızının 15 dakikalığına çok çabuk biçimde ve sessizce 1,410Hz çıkartılmasıyla başlamıştır. Kötücül yazılım, takip eden 27 gün boyunca, hızın 50 dakikalığına 2Hz'e düşürüldüğü diğer saldırı başlatılıncaya kadar sesiz kalmıştır.[38] Saldırının bu rastgele örüntüsü, kötücül yazılımı anti-virüs programlarından da gizlemiştir. Kontrolün yapıldığı monitörlerin kapanması da kötücül yazılımın neden olduğu normal dışı faaliyetin kontrol odasındaki operatör tarafından fark edilmesinin önüne geçmiştir.

Stuxnet sadece İran'daki tesislere saldırı düzenlemede kullanılmamıştır. Stuxnet, Kaspersky Security Network tarafından verilen bilgiye göre, Eylül 2010 sonu itibarıyla dünya çapında yaklaşık 30,000 kurumdaki 100,000'den fazla bilgisayar sistemine bulaşmıştır.[39] Stuxnet'ten sonra ortaya çıkan Flame, Duqu ve Regin gibi benzer kötücül yazılımlar enerjiden bankacılığa birçok sektörü tehdit etmektedir. Bu yazılımlar, Stuxnet'in yazılım mantığıyla dikkatleri çeken düzeyde bir benzerlik taşımaktadırlar.

4. Veri Tabanlı Kontrol ve Gözetleme (The Supervisory Control and Data Acquisition-SCADA) ve İnsan Etkileşimi

Herkesin tahmin ettiği sırdan daha iyi gizlenmiş sır yoktur.
George Bernard Shaw

Ulusal güvenlik, içinde bulunduğumuz 21. yüzyılda, enerji ve kritik altyapıya bağımlı durumdaki ekonomi ile iç içe geçmiş durumdadır. Yüksek elektrik üretimi ve tüketimi devletleri enerji güvenliğine odaklanmaya yönlendirmektedir. Devletlerin çoğunluğu elektrik ihtiyacını karşılamak için farklı enerji kaynaklarını kullanmaktadırlar. Elektrik şebekeleri ve bileşenleri ise neredeyse tamamen bilişim teknolojilerince kontrol edilmektedir. Modern çağın ulusal güvenliği, tarihin hiç bir döneminde olmadığı kadar donanım, yazılım ve insan-makina etkileşimine dayalı hale gelmiştir. Bu bağlamda, çok yönlü, gelişmiş bir siber saldırıyla bir ulusu felce uğratmak mümkün hale gelmiştir.

Devletler, yıkıcı bir siber saldırının hedef olabileceklerinin farkına varır varmaz, siber durumlarını ve bir saldırıya karşı koyabilmek için sahip oldukları imkân ve kabiliyetleri tanımlayan ulusal stratejileri belirlemeye başlamışlardır. Bu ulusal siber stratejileri, belli başlı tehditleri tanımlayarak ilgili kurum ve kuruluşların bu tehditlere karşı nasıl hazırlanacaklarını belirlemektedir. Devletlerin, zihniyet, bilgi ve internetin neden olduğu teknolojik ve yapısal değişikliklerin yarattığı tehditlere karşı dayanıklı duyabilmeleri için, stratejilerini uyumlu hale getirmeleri gerekmektedir.

4.1. İnsan-Makina Etkileşimi

Bilgisayar teknolojileri 1957'ye kadar işlerin geri planda (batch processing) yapılmasına dayanan sınırlı bir kapasiteye sahiptir. Araştırmacıların bilgisayarlara doğrudan ulaşımı yoktur. Bilgisayarlar, yetersiz işlem kapasitelerine ek olarak, fiziki anlamda soğutucularla donatılmış devasa odaları gerektirecek kadar büyüktüler. Modern teknolojinin kullanıldığı

gelişmiş bilgisayarların icadına kadar geçen sürede, bilgisayar kullanımı uzun ve zaman alıcı bir süreçti.

Sonra 1957'de araştırmacıların, uzaktan bağlantı kurmakta bir takım kısıtlamalar olmakla birlikte, servis sağlayıcılarına doğrudan bağlanabilmeleri, bilgisayar teknolojisinde önemli bir dönüm noktası olmuştur. Talepteki artış beraberinde farklı araştırmacıların sınırlı bir zaman aralığında sağlayıcılara doğrudan bağlanmasına imkân tanıyan zaman paylaşımı olgusunu getirmiştir. Bu olgu, bir bilgisayarın işlem gücünün birden fazla kullanıcı tarafından paylaşılması anlamına gelmiştir. Bu süreç, aynı zamanda kullanıcı hesabı kavramının yaratılmasını ve sağlayıcıya ulaşmaya imkân tanıyan yeni yönetim stratejilerinin gelişimini de sağlamıştır. 1960'ların bilgisayar teknolojisi kullanıcı dostu, kullanışlı ve ulaşılabilir olmaktan çok uzaktır. Kullanıcıları birbirine bağlamaya olan ihtiyaç, araştırmacıları yetkilendirilmiş kullanıcıların dosyaları paylaşmalarını sağlayacak bir ağ yaratmaya zorlamıştır.[40] Özellikle Sovyetler ve ABD arasındaki uzay yarışı bilgisayar teknolojisinin gelişimini hızlandırmıştır.

1960'larda üniversiteler kendi bilgisayar kaynaklarını ARPANET üzerinden diğer kullanıcılarla paylaşmaktan kaçınmaktaydılar. Bu durum onları, ağ süreçlerini kontrol eden anabilgisayarın (*mainframe*) kullanılmaya başlamasının hemen öncesinde, arayüz terminalleri adı verilen küçük bilgisayarları kullanmaya zorlamıştır. Anabilgisayar, sadece programların ilk kullanıma hazırlanması ve bilgi dosyalarından sorumluydu. Sonuçta ağların etkileşimi ağdaki çeşitli bilgisayarların bilgi transfer kontrol protokollerinin onaylandığı Network Control Protocol (NCP) kurulmasını sağlamıştır.

Artan sayıda katılımcının ağa girişi, ağda bir takım teknolojik düzenlemelerin yapılmasını beraberinde getirmiştir. E-posta, doğrudan mesajlaşma sistemleri ile Bulletin Board System (BBS) kullanılmaya başlaması ise ağ kullanıcılarının sayısını büyük bir oranda arttırmıştır.[41] Bu türde platformlar, bilgisayara dayalı iletişimin de önünü açmış ve bilgi paylaşımını başlatmışlardır. Hacker grupları ve teknoloji meraklıları çoğunlukla bilgisayara dayalı iletişim platformlarının bu ilk biçimlerini kullanmaktaydılar. 1990'lardan itibaren internet kullanıcılarının sayısındaki büyük artış, insan-makina etkileşimini de çarpıcı biçimde değiştirmiştir. Bu gelişme neticesinde, bilgisayar yoğun iletişimde büyük bir gelişme kat edilmiştir. Dünyanın dört bir tarafındaki hacker ve cracker

grupları, sahip oldukları teknolojik uzmanlığı paylaşmaya başlamışlardır.[42] Bu gruplar aynı zamanda hacker kültürünün ve kapasitesinin gelişmesinde de önemli rol oynamışlardır. Bilgisayarlara izinsiz erişim, ağa ulaşımın mümkün olduğu yerlerde artarak yaşanmaya başlanmıştır. Örneğin Milwaukee'den bir grup genç tarafından kurulan Group 414, Los Alamos Ulusal Laboratuvarı, Sloan-Kettering Kanser Merkezi ve Security Pacific Bankası gibi kurum ve kuruluşlara çeşitli saldırılar düzenlemişlerdir. Legion of Doom isimli bir hacker grubu tarafından başlatılan saldırılar ise idareyi bilgisayar güvenliği konusunda yasa çıkartmak yönünde bir takım önlemler almaya zorlamıştır.

Bilgisayar teknolojisinde otomasyon geliştikçe, rutin süreçler de daha az insani müdahaleyi gerektirir bir biçimde daha da yaygınlaşmıştır. Bilgisayara dayalı ana süreç kontrol teknolojisine Veri Tabanlı Kontrol ve Gözetleme (*The Supervisory Control and Data Acquisition*-SCADA) Sistemi adı verilmektedir. SCADA sistemleri, bilgisayar teknolojilerinin ilk yıllarında, tüm işlemlerin genelde anabilgisayarda yapıldığı fakat izleme sistemlerinin sınırlı bir kapasiteye sahip olduğu yekpare sistemlerdir. Anabilgisayardaki merkezi işlemcilerin (CPU) zamanı yönetme imkân ve kabiliyetlerinin gelişmesiyle birlikte sanayi, dağıtık SCADA sistemlerini kullanmaya başlamıştır.

Dağıtık SCADA sistemleri, kontrol fonksiyonlarını ve tam zamanlı bilgiyi çoğunlukla yerel ağdaki diğer bilgisayarlarla paylaşırlar. Bu tip SCADA sistemleri, sınırlı kontrol görevlerini yekpare sistemlere kıyasla daha etkin bir şekilde yürütürler. Nükleer enerji santrallerinin çoğundaki SCADA sistemleri şu üç unsuru içermektedir:

- Belirli bir noktadaki durumu ölçen sensörler,
- Pompa ve vanalar gibi işletim ekipmanı,
- İşletim ekipmanı ile sensörler arasındaki iletişimi sağlayan yerel işlemciler.[43]

Dört çeşit yerel işlemci bulunmaktadır: Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Unit (IED), ve Process Automation Controller (PAC). Bu işlemcilerin başlıca görevleri ise şunlardır: sensörlerden bilgi toplamak; daha önceden yüklenmiş programlara (internal programmed logic) ya da uzaktan komutlara bağlı olarak işletim ekipmanının açılıp kapanmasını sağlamak; iletişim sensörlerine ve işletim ekipmanına protokollerin bilgisini tanımlamak; acil durum koşullarını

tanımlamak ve yerel işlemciler, işletim ekipmanı ve sensörler arasında kısa mesafeli iletişimi sağlamak. Bu türde iletişim çoğunlukla kısa kablolar ya da kablosuz ağ bağlantısı aracılığıyla yürütülmektedir.

Sunucu bilgisayar ise izleme ve denetlemenin merkezi olarak görev yapmaktadır. Bireysel operatörler her türlü faaliyeti bu anabilgisayar üzerinden izlemekte ve gerekli durumlarda denetimsel faaliyette bulunmaktadırlar. Anabilgisayarların görev ve yetkilerini Ana Terminal Ünitesi'ne (Master Terminal Unit) (MTU) müdahale ederek değiştirmek mümkündür. Uzun erimli iletişim ise kiralanmış iletişim hatları, uydu, mikrodalga, hücresel veri aktarımı (*cellular packet data*) ve frame delay gibi farklı yöntemler kullanılarak, yerel bilgisayarlarla anabilgisayar arasında olmaktadır. Bu türdeki SCADA sistemleri, Ethernet ya da fiber optik bağlantıları kullanan Geniş Alan Ağları (Wide Area Networks) vasıtasıyla haberleşmektedirler.

SCADA sistemleri, farklı süreçleri denetlemek ve operasyonun düzenli biçimde devamlılığını sağlayabilmek amacıyla gerekli düzeltme ve düzenlemeleri yapabilmek için çeşitli Programlanabilir Mantıksal Kontrol Aygıtları'nı (Programmable Logic Controllers - PLC) kullanmaktadırlar. Bu PLC'ler aynı zamanda insani müdahale gerektiğinde operatörü uyarmaktadırlar. SCADA sistemlerine olan artan bağlılık (connectivity), bireysel operatörlerin süreci izlemesi de dâhil olmak üzere sürecin gerçek zamanlı bilgi aracılığıyla izlenmesini ve kontrolünü sağlamaktadır. Ancak, bu türdeki bir bağlılık sistemleri ağ tabanlı saldırılar karşısında zarar görebilir hale getirmektedir. Şebekeye bağlı olarak çalışan bu SCADA sistemleri, insan-makina etkileşimini farklı bir düzeye taşımaktadırlar. Bu sistemler, herhangi bir acil durumda kritik altyapının korunması açısından insan müdahalesinin önem ve rolünün altını çizmektedirler.

İnsan kullanıcılar, nükleer enerji santralleri gibi kritik tesislerin işlevlerini yerine getirebilmeleri açısından, vazgeçilmez unsurlar arasındadır. Nükleer enerji santrallerinde çalışan bireyler, bir kazanın önlenmesi ya da herhangi bir aksaklığın fark edilmesi açısından emniyet zincirinin ilk aşamasını oluşturmaktadırlar. Kontrol odasında görev yapan operatör, tesisin görev tanımı yapılmış göstergelerini kontrol etmek ve gerektiğinde sürecin devamlılığını sağlayacak düzeltmelerin yapılmasını sağlamak durumundadır. Bu bağlamda insan-makine etkileşimi sürecinde iki temel sorunla karşılaşılmaktadır: insan merkezli ve anabilgisayar arayüzü merkezli (*hosting computer interface-centered*).

SCADA sistemlerinin yürüttüğü denetleme ve iletişimi sağlayan yazılım, gerekli bilgiyi sağlamak ve bir sorun oluşması halinde görevli operatörü uyaracak alarmı başlatmak için tasarlanmıştır. SCADA sistemlerinin erken dönem arayüz tasarımları, ilkel ve bireysel operatörlerin bilişsel ve psikolojik farkındalık seviyesine odaklanmamıştır. Bu arayüzlerin en büyük sorunu, herhangi bir hareketi ya da animasyonu içermeyen statik bir tasarıma sahip olmalarıdır. Arayüzde yetersiz grafikler yer almış ve bunlar ancak bir alarm durumunda tetiklendiğinde değişiklik göstermiştir. Ancak, bu alarmlar tehdidin düzeyine göre farklılık göstermemiştir. Bazı durumlarda alarm mesajının boyutu, operatörün ekranda yer alan diğer bilgiyi görmesinin önüne geçmiştir. Monitör ve klavye gibi destek donanımı da operatörün bilgiyi kolaylıkla kavramasını ve en az çabayla en hızlı biçimde yanıt vermesini sağlayacak biçimde tasarlanmamıştır.

Eski arayüz tasarımlarında bilgi üç ya da dört ayrı monitöre yansıtılmıştır. Operatörlerin ilettikleri sorunların başında yetersiz ekran alanı gelmiştir. Modern nükleer enerji santrallerinde kullanılan arayüz, operatörün, sürecin tamamını 40 inçten daha büyük geniş ve yüksek çözünürlüklü ekranlarda izlemesine imkân tanıyan bir biçimde tasarlanmalıdır. Bu monitörlerin satın alınması aşamasında, ekran üzerine uzmanlaşmış donanım uzmanlarının monitörleri belirlemesi gerekmektedir.[44] Geniş ekranlı monitörler, hataların izlenmesinde takım çalışmasını da mümkün kılarak, operatörlerin durum farkındalığını da arttırmaktadır. Anabilgisayarın arayüzü ise bir siber saldırı düzenlenmesi halinde ortaya çıkabilecek aykırılıkları yakalamada kritik role sahiptir. [45]

4.2. İnsan Kaynaklı Sorunlar

Statik bir izleme sürecini yürütmek, yüksek düzeyde dikkat ve özen gerektirmektedir. Bu herhangi bir çalışan için devamlılığı hiç de kolay olmayan bir durumdur. Bu kişisel bir sorun olmaktan ziyade, insan doğasını ilgilendiren bilişsel ve fiziksel bir kapasite konusudur. Farklı SCADA sistemleri farklı arayüzler kullanmaktadır. Operatörler bu yeni arayüzlere uyum sağlamak için zamana ihtiyaç duyarlar. Arayüzler, bu konuda verilen eğitimin erken aşamalarında çalışanların kafalarını çeşitli uyarı, mesaj ve bilgiler ile karıştırırlar. Uyum sürecinin tamamlanmasını takiben, çalışanlarda statik arayüz tasarımına alışmanın ve can sıkıcı tekrarların yarattığı dar odaklılığın (*tunnel vision*) oluşması ciddi bir risk olarak karşımıza çıkmaktadır.[46] Operatör olmak, başlangıçta dinamik bir

görev olarak görülürken, zamanla sıklıkla verilen alarmlar rutin uyarılara dönüşmekte ve günlük görevlerin yerine getirilmesi gereken tepki süresini aşmaktadır. Bu konuda hazırlanmış olan bir rapora göre, "her bir çalışan için her bir saatte yönetilebilecek azami alarm sayısı yaklaşık 12'dir ve bunun gündelik ortalaması ise 300 civarındadır. Bilgi akışındaki artış ve alarmların sıklığı, operatörde çoğunlukla kafa karışıklığına neden olmakta ve bu durumda gerçek alarmlar yüzlerce yanlış alarm arasında atlanabilmektedir."[47]

Operatörler, kontrol odasında diğer çalışanların sürece karışmaları ya da telefon aramaları gibi dikkat dağıtan çok sayıda olaydan da bahsetmektedirler. Kontrol odalarının sessiz ve sakin ortamlar olması, operatörlerin tüm dikkatlerini monitör ekranlarına vermelerinin sağlanması açısından kritik önemdedir. Sonuç olarak, kontrol odasında yetkisiz personelin varlığı tesisin güvenliğini tehlikeye düşürür.

Nükleer enerji santrallerinin güvenliğinin izlenmesinde, operatörün karşılaştığı arayüz eldeki tek imkân olduğu sürece, operatör ve onun anabilgisayarı kazaların ve güvenlik ihlallerinin önlenmesi açısından kritik bir role sahiptir. Fakat çoğu arayüz tasarımdan kaynaklanan, kendine has güvenlik sorunlarına neden olabilmektedir. Arayüzlerin birçoğu gerekli bilgiyi operatörlere 2D grafik tasarımlar şeklinde iletmek üzere tasarlanmıştır. Bu arayüz tasarımlarının ana odağında işlevsellik, kullanılabilirlik ve görünebilirlik yer almaktadır. Muntazam ve etkileşimli tasarımlar, operatörün dikkatini desteklemek açısından hayati öneme haizdir. Sonuç olarak, söz konusu arayüz siber savunma açısından bir cephe hattına dönüşmektedir. Arayüz aynı zamanda bir sistemin sıra dışı olaylara karşı savunucusu olarak da faaliyet gösterir.

İstikrarlı bir güvenlik sistemi kurulabilmesinin ardında yatan temel prensip, güvenliğin devlet tarafından, kurumsal ayrıntıların da kurumlar tarafından belirlendiği yazılı düzenlemeler ile sağlanan, titizlikle hazırlanmış, gayet açık bir güvenlik politikasının uygulanmasıdır. Bir güvenlik politikasının kesin ve açık bir biçimde ifade edilmesi, yöneticilere iş bölümünün kolay anlaşılabilir olmasında ve ölçülebilir ve kendi kendini yenileyebilen bir sistem kurmalarında yardımcı olmaktadır. Enerji santrallerinde yerel ağa bağlı birçok bilgisayar ve elektronik araç, güç santrallerinin fiziksel güvenliğini sağlar. Fakat ağ bağlı olmaları bu sistemleri aynı zamanda özellikle siber saldırılara açık hale getirmektedir. Bu nedenle fiziki ve siber güvenlik alanlarının yöneticileri arasında güçlü

bir iletişim ve işbirliği olmalıdır. Bu yöneticilerin ayrıntılara hâkim ve muhtemel tehditlere karşı hazırlıklı olabilmeleri için, her biri diğerinin alanıyla ilgili temel bilgilerle donanmış olmalıdır.

Güvenlik, tehditlerin değişen doğasına bağlı olarak düzenli biçimde ele alınan, sürekli gelişen bir döngü olarak kabul edilmek zorundadır. Nükleer enerji santrallerindeki geleneksel güvenlik yaklaşımı, fiziki ve siber güvenlik sektörlerinin belirlediği sınırlarla uyum içindedir. Uluslararası toplum, hibrit tehditlerin hâkim olduğu bu çağda esneklik, uyumluluk ve işbirliğini sağlayan akıllı güvenlik politikaları uygulamalıdır. Türkiye'de inşa edilecek yeni tesisin fiziki ve siber güvenliğinden sorumlu yöneticiler şu noktalara dikkat etmek durumundadırlar:

- Türkiye'de ve uluslararası alanda hâkim olan yasal ve düzenleyici şartları anlamak,
- Güvenliği kurumsal kültürün bir parçası haline getirmek ve bunun tüm paydaşlarca bu şekilde algılanması konusunda ısrarcı olmak,
- Etkin risk değerlendirme programlarını geliştirmek,
- Riskli bilginin yönetimini amaçlayan bütüncül yönetim programları geliştirmek,
- Güvenlik stratejilerinin ve potansiyel güvenlik ihlalleri ile insan faktörünün etkilerini kıymetlendirmek,
- Acil durum yönetim politikalarını geliştirmek,
- Bilgi teminatı ve güvenliği yönetiminde kalite kontrolünü sağlamak ve geliştirmek,
- Acil durumlar için alternatif iletişim teknolojilerini geliştirmek,
- Tesisin güvenlik seviyesini güncellemek amacıyla yeni teknolojileri takip etmek.

Nükleer enerji santrali işletmeye açıldığı gün sorunsuz ve güvenle çalışmasını sağlayacak en son teknoloji le donanmış olacaktır. Fakat yeni teknolojinin olması bir nükleer enerji santrali hangi sıklıkta teknolojisini yenilemelidir sorusunu gündeme taşımaktadır. Tesis yöneticileri ve devlet yetkilileri düzenli biçimde yeni gelişen teknolojileri ele almalı ve tesisin hâlihazırdaki durumunu güvenlik perspektifiyle değerlendirmelidirler. Tesisin güvenlik sisteminin korunması ve geliştirilmesi en az güvenlik politikasının yazılması kadar kritiktir.[48]

Nükleer enerji santrallerine özel olarak hazırlanmış olan teknolojik

koruma, bu araçlara olan bağımlılığı insan kaynağının aleyhine olacak bir biçimde arttırmaktadır. Fakat tesis personeli tesisin planlama, güncelleme ve bakımı açısından kritik öneme sahiptir. En güvenilir sistemler dahi yetersiz eğitim ve gerekli bakım personelinin olmaması nedeniyle güvenlik ihlalleriyle karşı karşıya kalabilmektedir. Sürekli eğitim ve nükleer enerji santrallerinin birbirinden farklılaşan güvenlik sistemlerinin koordinasyonu, nükleer emniyetin devamlılığı açısından hayati konulardır. Nükleer tesislere yönelik saldırıların varlığı, çevre güvenliğinden sorumlu görevlilerin, siber güvenlik yöneticilerinin ve SCADA mühendislerinin koordinasyon içinde hareket etmelerini gerektirmektedir. Bu türde karmaşık bir ortamda yöneticilerin, acil bir durumun kaotik bir ortama dönüşmesinin önüne geçebilmek için, iş bölümlerini açıkça tanımlamaları ve uygulamaları gerekmektedir.

Bir diğer önemli kritik güvenlik konusu ise bilginin yayılması (*dissemination*) ile ilgilidir. Çalışanların güvenlik politikalarını ve güvenlikle ilgili yönergelerde yapılan düzenlemeleri nadiren okudukları bilinen bir gerçektir. Çalışanları bu teknik bilgiyi ve siyasa belgelerini izlemeye motive etmek ve bilginin yayılımı konusunda dikkatli olmaya yönlendirmek bir sorun olarak önümüzde durmaktadır. Yöneticinin, bir güvenlik kültürü oluşturduktan sonra personelini bu konuda motive etmeyi sağlayacak yolları bulması gerekmektedir.

Türkiye örneğinde, dil konusu bir diğer engel olarak belirmektedir. Tesislerin işletmecisi durumundaki şirketler (Akkuyu'da Ruslar ve Sinop'ta Japon ve Fransızlar) herhangi bir yanlış anlamanın önüne geçmek ve acil durum senaryolarına karşı hazırlıklı olabilmek amacıyla teknik ve siyasa belgelerinin tamamını aynı zamanda Türkçe olarak da hazırlamak durumundadırlar.

4.3. Güvenlik Seviyeleri ve Güvenlik Kontrolü/Yetkilendirmesi (*Clearance*)

Nükleer enerji santrallerinin siber korumasının etkinliği, çevre güvenliğinin de dikkate alınmasını gerektirmektedir. Fiziki güvenlik, nükleer enerji santralleri güvenlik duvarlarını ve sızma detektörlerini fiziksel suncular üzerinden sağladıkları için, siber güvenliğin ayrılmaz bir parçasını teşkil etmektedir. Bir saldırının ilk adımı, bunlara ulaşılmasıdır. Fiber optik kablolar ve açıktaki diğer bağlantılar kötü amaçlı saldırılara karşı

korunmalıdır. Bazı durumlarda bir makas Trojan virüsünden daha tehlikeli olabilmektedir. Bu nedenle elektrik şebekesi ile bağlantıyı sağlayan bilgisayar sistemleri ile kablo ve bağlantıların korunması, bunların yüksek risk varlıkları sınıfında değerlendirilmesini gerektimektedir. Enerji santralinin bilgisayarları da güvenlik yetkilendirme seviyelerine göre sınıflandırılmalıdırlar. Düşük seviyedeki bilgisayarların yüksek güvenlikli olanlarla bağlantısına izin verilmemelidir. Bu güvenlik protokolleri güvenlik kurallarına uyulmadığı varsayımı ile rutin aralıklarda kontrol edilmelidir.

Tüm bu güvenlik önlemleri, güvenlik bölgesinin girişinde yapılan aramalar aracılığıyla elektromanyetik kapasiteye sahip her türlü donanımın kontrol edilmesini de içermelidir. Saha yöneticilerinin, elektromanyetik araçların kapsama alanının genişliğini de dikkate alarak, bu türdeki cihazların tesise giriş ve kullanımını nasıl sınırlandıracaklarına karar vermeleri gerekmektedir. Stuxnet, mobil telefon, USB, NFC, radyo frekanslı chipler, harici hard diskler, dizüstü bilgisayarlar, mikro işlemci kullanan diğer araçlar ile bluetooth ve kablosuz internet bağlantısına sahip diğer tüm taşınabilir araçların kötücül yazılımların transferine imkân verdiğini göstermiştir. Bu türde araçların tesise girişi sınırlandırılmalı ve kontrole bağlanmalıdır. Tesis çalışanlarının arama yapan güvenlik görevlileriyle olan kişisel ilişki ve dostluklarını bu türde manyetik araçları tesisin korumalı bölgesine sokmak için kullanmayı denedikleri örnekler bulunmaktadır. Ziyaretçilerin tamamının da arama süreçlerine tabi olmaları ve yanlarındaki elektromanyetik cihazları, kullanımlarına tahsisi edilen özel dolaplara bırakmaları sağlanmalıdır. Girişte yer alan kontrol noktasında mobil telefonların kullanımı yakın takibin (*tailgating*) engellenmesi amacıyla izin verilmemelidir.[49] Ayrıca, ziyaretçilerden toplanan elektromanyetik cihazlar, tesisin ağına muhtemel bir sızmanın önüne geçebilmesi amacıyla, tesisin önceden belirlenen güvenli bir bölgesinde yer alan Faraday Kafesi'nin içinde tutulmalıdır. Arama, tesisten herhangi bir manyetik cihazın çıkarılmadığından emin olabilmek amacıyla ayrılırken de tekrarlanmalıdır.

Bir nükleer tesisin bilgisayar ve ağ sistemleri bir diğer güvenlik endişesidir. Nükleer enerji santralleri zaman zaman donanım değişikliği ve bakıma ihtiyaç duyarlar. Düzenleyici, işletmecinin donanım destek sistemlerini nasıl tasarlayacağını organize etmelidir. Her bir yeni donanım test edilmelidir ve bu test ulusal yetkililerce test yatağında gözlenmelidir. Bu sürecin zaman aldığı akılda tutularak, düzenleyicinin işletmeciyi, tesis çalışmaya başlamadan önce yedek parçaların depolanmasını öngören bir donanım yönetim sistemi kurması yönünde teşvik etmesi gerekmektedir. Bu türde bir girişim, tesis

yönetiminin, herhangi bir arıza ile karşılaşılması durumunda hiç vakit kaybetmeden gerekli parçayı değiştirebilmesine imkân tanıyacaktır.

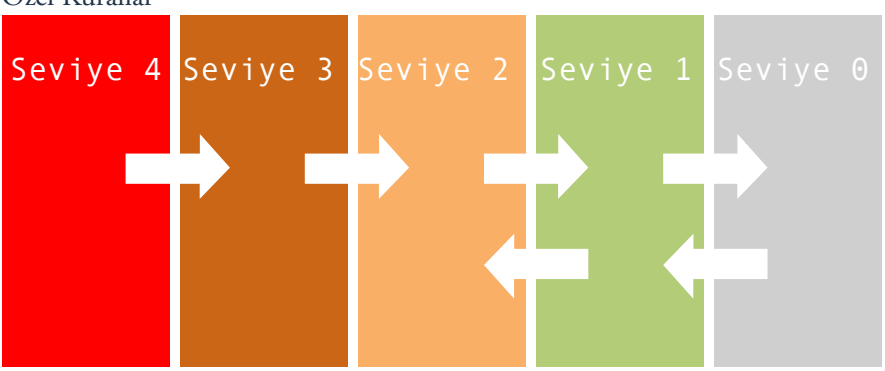
Ayrıca, yüklenicilerin sabıka kaydı sorgulaması yapılmalıdır. Güvenlikten ziyade işlevsellik ve dayanıklılıkları dikkate alınarak tasarlanan ısıtma, havalandırma ve soğutma gibi sistemler, nükleer enerji santrallerinin en az güvenli unsurları olarak kabul edilmelidir. Bu sistemler günümüzde yerel ağa bağlı IP tabanlı uygulamalara dönüşmüşlerdir. Yükleniciler bu sistemlere, sistemlerin yazılımlarını yükseltmek ve gerekli yamaları yapabilmek için tesisin dışından bağlanmaktadırlar. Bu sunucuların zafiyetleri bir anda tesis açısından sistemik risklere dönüşmektedir. Isıtma ve soğutma (HVAC) sistemlerine sızılması, kolaylıkla bir siber saldırı düzenlemesine imkân tanıyabilecektir. Nükleer enerji santrallerinin düzenleyici ve işletmecilerini, HVAC sistemlerinin her seviyedeki güvenliğine özel bir hassasiyet göstermelidir. [50]

4.4. Güvenlik Bölgeleri

Siber ve fiziki güvenlik personeli, nükleer tesisin güvenlik bölgelerine ayrılması görevini daha tesisin inşası başlamadan önce ortaklaşa çalışarak yerine getirmelidirler. En bilinen uygulama, Seviye 4'ten (yüksek güvenlik) Seviye 1'e (düşük güvenlik) derecelendirmeyi öngören bir yaklaşımdır. İşletmeci, çevresel faktörlerin ışığında, temel güvenlik önlemlerini de dikkate alarak bir güvenlik tasarımı yapmalıdır.

Nükleer enerji santrallerinin işletmecileri farklı güvenlik seviyesi modelleri uygulamaktadırlar.[51] Siber güvenlik mimarisinde de bir kısmı, Seviye 1'den başlayarak ilerleyen seviyeleri öngören farklı yaklaşımları tercih etmektedirler. Bazı örneklerde ise bu seviyelendirme Seviye 4'ten başlayarak Seviye 0'a doğru tasarlanmıştır.

Özel Kurallar



4.4.1. Seviye 4 (Hayati Bölge – Kontrol ve Emniyet Sistemi):

Seviye 4'teki dijital ekipmanlar, iletişim özellikleri bakımından mutlak koruma altına alınmalıdır. Bu seviyedeki herhangi bir ihlal, nükleer enerji santralini tehlikeye düşürmektedir. Bu seviyede herhangi bir ağ bilgi trafiğine izin verilmemelidir. İşletmeci, sistemin tasarımına bağlı olarak, dışarıyla sadece tek yönlü iletişime izin verebilir. Fakat tek yönlü iletişim bile bir takım güvenilirlik ve bütünlük sorunlarına yol açabilmektedir.[52] İşletmeciler ekonomik fizibilite, pratiklik ve üretime bir an önce başlamak gibi nedenlerle bir takım istisnalar yapmak eğilimindedirler. UAEK, işletmecileri, güvenlik odaklı çözümler geliştirme ve istisnaları olay temelli olarak değerlendirme yönünde teşvik etmektedir. Gereksiz uygulama, hizmet ve protokollerin tamamı engellenmelidir. UAEK ayrıca şu noktalarda da tavsiyelerde bulunmaktadır[53]:

- Uzaktan bakım ve onarıma hiç bir koşulda izin verilemez.
- Sistemlere fiziki erişim sıkı biçimde kontrol altında tutulmalıdır.
- Sistemlere erişimi izin verilen personel sayısı asgari sayı ile sınırlanmalıdır.
- Bilgisayar sistemlerinde yapılacak onaylı bakımlar için iki kişi kuralı uygulanmalıdır.
- Tüm faaliyetler kayıt altına alınmalı ve takip edilmelidir.
- Sisteme girilecek her türlü bilgi, her bir duruma göre gözden geçirilmeli ve doğrulanmalıdır.
- Tüm bakım ve onarım faaliyetleri; donanım bakımı, güncellemeler ve yazılım bakımı da dâhil olmak üzere çok katı kurumsal ve idari prosedürler belirlenmeli ve uygulanmalıdır.[54]

4.4.2. Seviye 3 (Korumalı Alan – Bilgi Edinme Ağı):

- Sadece Seviye 3'ten Seviye 2'ye ya da dışarıya doğru tek yönlü bilgi akışına imkân tanıyan ağ sistemlerine izin verilmelidir.
- Ters yönde (içeriye doğru) sadece gerekli alındı mesajlarının ve kontrollü sinyal mesajlarının iletimine izin verilebilir (örneğin TCP/IP).
- Uzaktan bakım erişimine, sadece olay temelli olarak ve belirlenmiş bir

süre için izin verilebilir. Bu türde durumlarda tesis, çok iyi tanımlanmış önlemlerle korunmalı ve sözleşmeli kullanıcılar belirlemiş güvenlik planına uymalıdır.

- Sisteme erişimine izin verilen kişi sayısı asgaride tutulmalı ve kullanıcı ve idari personel arasında bir farklılaştırmaya gidilmelidir.
- Sistemlere fiziki erişim çok dikkatli bir biçimde kontrol edilmelidir.
- Sistemlerin bütünlüğü ve ulaşılabilirliğini sağlayacak her türlü akılcı önlem alınmalıdır.
- Sistemdeki uygulamalarla ilgili zafiyet değerlendirmeleri tesis ya da süreçlerde bir takım istikrarsızlıklara yol açabilir. Bu nedenle bu değerlendirmelerin deney yatağı veya yedek sistemler üzerinde ya da fabrika kabul testleri veya uzun süreli olarak planlanan kapatmalar sırasında yapılması düşünülmelidir.

4.4.3. Seviye 2 (Mülkiyet Sahibi Kontrollü Saha – Tesis Yerel Alan Ağı):

Seviye 2 koruma önlemleri, genel güvenlik önlemlerine ek olarak, orta seviyedeki siber tehditlere yönelik olarak kontrol odasından yöneltilen faaliyetleri gerektirmeyen, gerçek zamanlı sistemlerin yönetimi için alınması gereken önlemleri içermektedir. Erişim kontrol ve iletişimini filtreleyen özelliklere sahip bir güvenlik duvarı, ihtiyaç duyulmayan gereksiz bilgi akışını engellemek için farklı güvenlik seviyeleri arasındaki iletişimi ayrıştırmaya yardımcı olacaktır. Bu türde koruma önlemleri şu başlıkları içermektedir:

- Seviye 2'deki sistemlere internet erişimine izin verilemez.
- Anahtar kaynaklara ulaşan loglama ve denetleme yolları izlenmelidir. Bilgi teknoloji personeli, herhangi bir değiştirme girişimine karşı bu log ve denetlemeleri düzenli aralıklarla kontrol etmelidir.
- Bu seviyenin güvenliğinin sağlanması amacıyla, Seviye 3'ten gelecek her türlü kontrolsüz bilgi akışının engellenerek sadece tanımlı ve sınırlı faaliyete izin verilecek emniyet geçişleri uygulamaya konulmalıdır.
- Sistemlere fiziki erişim çok dikkatli bir biçimde kontrol edilmelidir.
- Uzaktan bakım ve onarıma, olay temelli olarak ve sadece siber güvenlik görevlilerinin onayı sonrasında izin verilebilir. Bu türdeki istisnalar periyodik olarak kontrol edilmeli ve erişim sonlandırılmalıdır. Erişimin

gerekmesi durumunda ise uzaktan erişim bilgisayarı ve kullanıcı tanımlanmış olan siber güvenlik politikasına uymalıdır.

- Sistemin faaliyetine erişimi olan kullanıcılar kati surette, zorunlu erişim kontrol mekanizmaları tarafından ve "bilinmesi gereken" prensip çerçevesinde kontrol edilmelidir. Bu prensibin her türlü istisnası mutlaka yöneticiler ile siber güvenlik görevlileri arasında değerlendirilmelidir. Bilgisayar ve ağ erişim kanalları her türlü yetkisiz erişime karşı korunmalıdır.[55]

4.4.4. Seviye 1 (Kurumsal Erişim Alanı – Geniş Ağ Alanı):

Bu seviyede, teknik bilgi koruma sistemi ve işletme faaliyet yönetimi (örneğin çalışma izinleri, iş göreve emirleri, etiketleme, evrak yönetimi gibi), iş yönetim sistemleri tesisin kapalı ağına bağlıdır. Süreç kontrol ağları ile iş yönetim ağları arasındaki bağlantı, genel güvenlik önlemlerine ek olarak, özel bir dikkat ve ayrımı gerektirmektedir. UAEK'nin Seviye 1 için öngördüğü sınırlamalar şu şekilde tanımlanmaktadır[56]:

- Sistemde değişiklik yapma yetkisi, sadece onaylanmış ve yetkin kullanıcılara tanınmalıdır. Bu kullanıcılar ve konumları, insan kaynakları ve siber güvenlik birimi tarafından periyodik aralıklarla incelenmelidir. Etkin olmayan kullanıcı hesapları mümkün olduğunca çabuk silinmelidir.
- Seviye 1'de kullanıcılara, uygun koruma önlemleri alındıktan sonra, internete erişim yetkisi verilebilir. Bu sistemler düzenli biçimde kontrol edilmeli ve sistem kullanıcıları kimlik hırsızlığı saldırılarına (*phishing attacks*) karşı uyarılmış olmalıdır.
- Bu seviyenin sözleşmeli yüklenici şirketlerden ve siteye bağlı ağlardan kaynaklanacak kontrol dışı faaliyetlerden korunması ve kontrol altındaki idari dosyaların indirilmesi, kara listeye alınmış web sayfalarının engellenmesi gibi özel faaliyetlere izin verilmesi için güvenlik geçitleri kurulmalıdır.
- Bu sistemlere fiziki bağlantı ve erişim kontrol altında olmalıdır. Bu sistemlere her türlü erişim kayıt edilmelidir. Siber güvenlik görevlileri, beklenmedik faaliyetlere karşı bu logları periyodik olarak incelemelidirler.
- Uzaktan bakım ve koruma erişimine kontrollü bir biçimde izin

verilebilir. Erişime yetkili uzaktan erişim bilgisayarı ve kullanıcı, sözleşmede de tanımlanmış olan siber güvenlik politikasına uymalı ve bu durum kontrol edilmelidir.

- Kullanıcıların erişimine açık olan sistem faaliyetleri, erişim kontrol araçlarınca sürekli kontrol edilmelidir. Bu prensibe istisna teşkil edecek herhangi bir durum, dikkatle çalışılmalı ve her türlü araç vasıtasıyla koruma sağlanmalıdır. Siber güvenlik görevlileri bu istisnaları düzenli biçimde denetlemeli ve etkin olmayanlar mutlaka sonlandırılmalıdır.

4.4.5. Seviye 0 (Kamusal Erişime Açık Alan):

Seviye 0, ofis otomasyon sistemleri, sistem yenileme sürücüleri ve yama yönetimi ile anti-virüs sürücüleri gibi teknik kontrol ve işletim ile doğrudan bağlantısı olmayan sistemlerin yüklü olduğu alandır. Bu sistemler düşük seviyeli siber tehditlerin söz konusu olduğu sistemlerdir. Seviye 0 önlemleri, tesise özel önlemlerin dışında şu önlemleri içermektedir:

- Sistemde gerekli düzeltme ve bakımları yapma izni, sadece işinin ehli ve yetkilendirilmiş kullanıcılara verilebilir. Bu kullanıcıların listesi periyodik olarak gözden geçirilmelidir. Etkin olmayan kullanıcı hesapları siber güvenlik görevlilerince sonlandırılmalıdır.
- Bu seviyedeki kullanıcılara, uygun koruma önlemleri alındıktan sonra, internete erişim yetkisi verilebilir. Erişim, gereksiz iletişimin kesilebilmesi amacıyla bir güvenlik duvarı sistemi tarafından kontrol edilmelidir. Bu seviyedeki sistem kullanıcıları kimlik hırsızlığı saldırılarına (phishing attacks) karşı uyarılmış olmalıdır.
- Uzaktan erişime, gerekli kontrollerin yapılabilmesi amacıyla kontrollü bir biçimde izin verilebilir. Siber güvenlik görevlileri kontrolleri denetlemeli ve herhangi ihlal olayında erişimi engellemelidirler.

Bir nükleer enerji santralinin yerleşim sahasında, siber güvenlik alanları fiziki güvenlik ile bağlantılıdır. Siber ve fiziki güvenlik birimlerinin yöneticileri, koşulların uygun olması durumunda, tesisi hibrit tehditlere karşı korunaklı kılacak yeni güvenlik planlarını hazırlamalıdırlar.

Fakat işletmecinin sağlam bir siber güvenlik politikası oluşturabilmek için tesise özel kuralları da belirlemesi, bu kuralları yürürlüğe koyması ve herhangi bir ihlalden şüphelenmesi durumunda, ilgili birimleri uyarması

da gerekmektedir. UAEK, bu türde kuralların örneklerine Bilgisayar Acil Durum El Kitabı'nda yer vermektedir[57]:

- Tüm kullanıcılar siber güvenlik işletim süreçlerini anlamak ve bunlara uymak zorundadırlar.
- Sisteme erişim için sadece kurallara uygun biçimde yetkilendirilmiş, tecrübeli ve gerektiğinde güvenlik kontrolünden geçmiş personele izin verilmelidir.
- Kullanıcılara sistemde sadece kendi işlerini yapmak için gereken seviyedeki fonksiyonlara erişim izni verilmelidir.
- Bilişim uygulamaları, uygun erişim kontrollerine ve kullanıcı kimlik denetlemesine sahip olmalıdır.
- Uygulama ve sistemden kaynaklanan zafiyetler denetlenmeli ve gerekli önlemler alınmalıdır.
- Sistem zafiyet değerlendirmeleri periyodik olarak yapılmalıdır.
- Bilgisayar ve ağ güvenlik unsurları, kesinlikle, sızma tespit sistemleri ve sızma önleme sistemleriyle korunmalı ve sanal özel ağ sağlayıcıları da mutlaka kayıt ve takip edilmelidir.
- Uygun yedekleme ve telafi süreçleri periyodik olarak kontrol edilmelidir.
- Çeşitli unsur ve sistemlere fiziksel erişim, bunların gördükleri fonksiyona bağlı olarak, mutlaka sınırlandırılmalıdır.

5. Siber Güvenlik ve Nükleer Enerji: Türkiye Örneği

5.1. Organizasyon

Bir düzenleyici olarak Türkiye'nin hem nükleer enerji santrali hem de bunun fiziki ve siber güvenliğinin sağlanması konularında sınırlı deneyimi olduğu aşikâr bir gerçektir. İran'ın nükleer enerji santraline yönelik Stuxnet saldırısı benzeri tehdit ve saldırılar, Ankara'nın endişesini arttırmaktadır. Afet ve Acil Durum Yönetimi Başkanlığı'nın (AFAD) hazırladığı Kritik Altyapı (KA) Koruma Raporu'na göre nükleer enerji alanında başta Enerji ve Tabii Kaynaklar Bakanlığı, Türk Atom Enerjisi Kurumu, AFAD, Enerji Piyasası Denetleme Kurulu (EPDK) gibi pek çok kontrol kurumu söz konusudur.[58] Nükleer enerji santrali lisansı alma sürecinde ve sonrasında bu bakanlık, kurum ve kuruluşların farklı yetki alanları ve sorumlulukları bulunmaktadır.

Nükleer enerji santrali projesinin organizasyonu, planlaması ve yürütmesinden Enerji Bakanlığı sorumludur. EPDK, projenin elektrik üretimi ve satışına ait yasal düzenleme sürecini yönetmektedir. TAEK, Türkiye'de tesislerin nükleer güvenliği konusunda lisans vermek için yetkili olan kurumdur. AFAD ise santrallerin acil durum hazırlığını kontrol etmektedir. Bu kurum ve kuruluşların yanı sıra İçişleri Bakanlığı, tesislerin dış güvenliğini sağlamakla mükellef ve acil durumlarda santrallerin özel güvenliğini koordine etme sorumluluğunu taşımaktadır. İçişleri Bakanlığı'nın, oldukça hassas olan bu tesislerin korunmasını sağlamak için iyi eğitilmiş, bilinçli ve kapsamlı güvenlik anlayışına sahip olan özel güvenliğin yasal arka planını hazırlama sorumluluğu da bulunmaktadır.

Türkiye'deki nükleer enerji santrallerinin siber güvenliklerini ilgilendirebilecek en büyük sorun, gerekli ve yeterli kanun ve düzenlemelerin olmayışıdır. KA korumasına yönelik olarak hazırlanmış olan mevcut kanun ve düzenlemeler, nükleer enerji santrallerine özel durumlara gereken cevabı vermemektedir. Şu anda Türkiye'de, siber güvenlik alanında faaliyet göstermek amacıyla düzenlenmiş TİB bünyesinde görev yapan bir Siber Olaylara Müdahele Ekibi (SOME) olmakla birlikte, nükleer tesislerin siber güvenliğinin daha karmaşık ve uzmanlaşmış teknik bilgi ve özel ilgiyi gerektirdiği belirtilmelidir.

Akkuyu'nun ön lisans verme işlemi, nükleer enerji santralinin inşası için gereken lisansı verme yetkisine sahip olan EPDK tarafından 25 Haziran 2015'te tamamlanmıştır. Ön lisans verme işlemi, lisans vermenin risklerini azaltmak ve lisans verme işleminin sonuçlarını daha öngörülebilir kılmak için bir dönüm noktası olarak kabul edilmektedir. Ancak Akkuyu santrali özelinde açık kaynaklarda, güvenlik başta olmak üzere, lisanslama süreciyle ilgili olarak yukarıda bahsi geçen konular hakkında sınırlı bilgi bulunmaktadır. Bu bağlamda akıllara gelen en önemli soru, siber güvenlikle ilgili tasarım ve planların ön lisans aşamasında dikkate alınıp alınmadığıdır. EPDK ya da TAEK, ROSATOM'un siber güvenlik tasarım ve planlarını tesisin yüksek ve düşük güvenlik seviyesindeki alanları için de gözden geçirmeli ve analiz etmelidir. Tasarım planları ayrıca ısıtma ve soğutma (HVAC) hizmetlerinin uygulanması ile üçüncü tarafların siber güvenlik yaklaşımları hakkında da ipuçları vermelidir. Akkuyu ve ROSATOM, HVAC altyapısının koruyucu bakımını organize etmeyi nasıl planlamaktadır? HVAC sunucularının siber güvenliğinden kim sorumludur? Üçüncü taraf taşeronların altyapı koruyucu bakımına uzaktan erişim hakkı var mıdır? Üçüncü taraf taşeronlar sunucularını ve altyapılarını nasıl güncelleştirmektedirler? Lisans verme süreci öncesinde bu türde bir dizi soru, hala cevaplanmayı beklemektedir.

Amerika'daki NRC'nin Türkiye'deki karşılığı olarak TAEK kabul edilmektedir. İdarenin de konuya bu çerçeveden baktığının işareti, TAEK'in nükleer enerji santralinin güvenliğinin denetlenmesi yetkisini almış olmasıdır. Ancak TAEK'in bu tesislerin siber güvenliği konusunu nasıl ele aldığı ya da planları nasıl kontrol edeceği konusu henüz açıklığa kavuşmuş değildir. HVAC sistemleri ve üçüncü taraf yüklenicilerle ilgili olarak, yukardaki sorulara benzer sorular ile TAEK'in Akkuyu santraliyle olan bağlantısı gündemde yerini korumaktadır.

Akkuyu nükleer enerji santralinin operasyon merkezinin en az üç bağlantısının olduğu gerçeği, konuyu bir üst düzeyde daha karmaşık hale getirmektedir: birincisi Akkuyu Anonim Şirketi, ikincisi ROSATOM Anonim Şirketi, üçüncüsü ise elektrik şebekesidir. Bu bağlantılar karmaşık bir dalga (*cascade*) etkisi yaratma potansiyeli/tehdidi taşımaktadır. Şirketler için yerel ağları (LAN) kontrol etmek çok daha kolay olacaktır. Fakat, "ulusal elektrik şebekesi ağının zafiyetlerinden doğacak güvenlik sorunlarının yönetimini kim ve nasıl yapacaktır?" sorusu hala cevaplanması gereken bir soru olarak gündemdeki yerini korumaktadır.

5.2. Bilgi Paylaşımı, Güvenlik İzleme ve Vakaları Yönetme

ABD ve AB'nin var olan nükleer enerji santralleri konusunda her türlü bilgiyi, güvenlik zafiyeti oluşturmadan paylaştıkları bir sistemleri bulunmaktadır. Nükleer enerji santralleri, herhangi bir siber ya da fiziki güvenlik ihlal girişimi ya da olayını, hazır durumdaki yetkililere rapor etmek durumundadırlar. Bu yetkili ise, diğer ilgili birimleri olaydan haberdar etmek ve tüm santralleri benzer tehdit ve acil durumlara karşı uyarmakla yükümlüdür.

Çok kritik olan bu türde bir sistemin eksikliği gerçekten de tüm operasyonları tehlikeye atmaktadır. Öte yandan nükleer enerji santrallerine yönelik siber olayların seyrekliği, bu konuda bir gizlilik olması nedeniyle gerek operatörler gerekse düzenleyiciler arasında nükleer tesislerin güvenliği konusunda yanlış bir özgüven algısı oluşturmuştur. Genel olarak nükleer tesis operatörlerinin, özellikle bu algı nedeniyle siber güvenlik alanında, diğer sektörlerle olan ilişkilerini daha sınırlı bir işbirliğ düzeyinde tuttukları gözlemlenmektedir. Oysa, ortak donanım kullanımı aracılığıyla muhtemel tehditlere karşı tüm endüstriyel kontrol sistemlerini kapsayan daha verimli bir işbirliği alanı yaratılması mümkündür.

Nükleer siber güvenliğin en temel önceliği, güvenliği ve muhtemel tehditleri sürekli biçimde izlemektir. Bu görev sadece nükleer enerji santraline odaklanmayıp, siber uzayda derin bir istihbarat yapabilmeyi ve bu bağlamda bir tür veri madenciliği becerisine sahip olmayı da gerektirmektedir. Türkiye'nin sahte kimlikler yaratmak ve uluslararası hacker gruplarıyla ve diğer organize suç birimleriyle iletişim kurmak anlamında sınırlı bir siber istihbarat becerisine sahip olduğu görülmektedir. Türkiye'de Milli İstihbarat Teşkilatı (MİT) ve Emniyet Genel Müdürlüğü'nün istihbarat birimleri siber uzaydan istihbarat amaçlı veri toplamaktadırlar. Bu istihbaratın kalitesinin yüksek olduğu kabul edilse bile, bu istihbaratın Akkuyu'da inşa edilecek nükleer enerji santralinin güvenliğinden sorumlu olacak birimlerle ne düzeyde ve ne hızda paylaşılabileceği sorusu akılları meşgul etmektedir. Bu nedenle, nükleer santral yönetimi bilgi akışını düzenli olarak sağlayabilecek özel bir siber istihbarat şirketinin/biriminin varlığına ihtiyaç duyabilecektir.

Nükleer tesisin siber güvenlik alanı, bu bakış açısıyla, tüm yazılım, iletişim ve kritik dijital varlıkların dijital korunması ve, tüm altyapının ve

gerekli iletişim donanımının, ya da santralin işlevselliğini etkileyebilecek diğer aygıtların, bir fiziki güvenlik ekibi tarafından korunması olarak iki ana koldan oluşmaktadır. Bu ikilinin ikincisi durumundaki fiziki koruma görevi, İçişleri Bakanlığı'nın koordinasyonu çerçevesinde faaliyet gösterecek olan özel güvenliğin sorumluluğunda olacaktır. Bununla birlikte tarafların, en üst düzeyde bir korumanın sağlanabilmesi için, fiber optik hatların sağlayıcıları dâhil olmak üzere altyapıyla ilgili diğer birimlerin tamamıyla iletişim içinde olması gerekmektedir. Fiziki koruma birimi, kolluk kuvvetleriyle uyum içinde çalışmayı öngören ve bunun ayrıntılarını içeren bir işbirliği ve iletişim planı hazırlamalıdır. Kolluk güçleri de, santralin fiziki güvenliğiyle ilgili kritik ve stratejik iletişimi tasarlamalıdır. Özel güvenlik şirketleri ve çalışanlarının saldırılar karşısında silah kullanma yetkilerini ve bunun derecesini belirleyen özel yasal düzenlemeler ise bir an önce hazırlanmalıdır. Nükleer enerji santrallerinin korunmasında reaksiyon süresinin saldırıların sebep olabileceği olası trajedileri önlemede kritik bir öneme sahip olduğu akılda tutulmalıdır.

Hem fiziki hem de siber tehditleri içeren hibrit tehditlerin artışıyla birlikte, fiziki güvenlik ekipleri ve siber güvenlik ekiplerinin yakın bir işbirliği içinde çalışmaları zorunluluğu doğmuştur. Bu iki grubun işbirliği en azından iki noktada açıkça örtüşmektedir; öncelikle, bütün sunucuların kullandığı CCTV sistemlerinin, herhangi bir düşmanca saldırıya karşı korunması gerekmektedir. İkinci olarak, siber güvenlik altyapısı fiziki saldırı ve ihlaller karşısında zarar görebilir konumdadır. Fiziki güvenlik ekibinin saldırılar karşısında aygıtları doğru biçimde koruyabilmek için siber güvenlik ve bilgisayar altyapısını en azından temel düzeyde tanımak ve bilmek zorunlulukları bulunmaktadır.

Fiziki koruma ekibinin birincil önceliği, yürüttükleri görevin tanımı gereği her türlü tehdit karşısında tesis içi güvenliği sağlamaktır. Çalışanlar ve güvenlik ekibi arasındaki kişisel ilişki ve bağların özellikle vardiya değişimleri sırasındaki güvenlik kontrollerinin karakterini değiştirme ihtimali bulunmaktadır. Bu nedenle fiziki güvenlik ekibinin yönetim kademeleri, bu türde şartlara hazırlıklı olmalıdır. Güvenlik görevlilerinin özellikle tanıdıklar ve bilindik diğer çalışanlar karşısında temel kuralların gereğince uygulanmasından kaçınmalarının önüne geçilmeli, amiyane tabirle gevşeme gibi her türlü olası insani faktörlere karşı dikkatli olmalıdır. Bu çerçevede örneğin kontrol noktalarında ikişer kişilik ekipler oluşturulması bu türde hataların yaşanmasını engelleyerek ve birebir duygusal yakınlığı azaltacaktır.

Başarılı uygulama örneklerine bakıldığında, nükleer enerji santrallerinin çoğunluğunda çalışanların acil durumlarda yüklenecekleri rolün belirlenmiş olduğu ayrıntılı bir vaka müdahale planı bulunmaktadır. Çalışanlar farklı tatbikat senaryolarına dayalı olarak rollerini öğrenir ve uygularlar. Tatbikatlar, bir kaza durumunda yapılması gereken her türlü hazırlığı ve uygulamayı, tekrarlaması alışıldık pratiklere döktükleri için önem taşımaktadırlar. Ancak, gerçek olaylarda korku, zaman ve risk gibi baskıların insanların muhakeme ve karar verme sürecini oldukça etkilediği ve aksamalara yol açtığı bilinmektedir.[59] En deneyimli personelin dahi, gerçek bir acil durum sırasında durgunluk ve donma davranışı sergileyebildiğini ve görevinin gereklerini yerine getiremediği durumları gözlemlemek mümkündür. Bu türde durumların önüne geçilebilmesi için, siber güvenlik ekibinin farklı durumlarda nasıl davranacağını öğreten yol haritaları geliştirilmelidir.

Unutulmaması gereken nokta, nükleer enerji santrallerindeki vakalara yanıt vermenin bireysel bir faaliyet olmadığıdır. Tesis yönetimi, tesise özel, şirkete ait ve ulusal düzeyde planları harekete geçirmek için ilgili birimlere haber vermelidir. Tesis, ulusal boyutlarla kıyaslandığında daha küçük bir birim olduğu için, idaresi daha büyük bir vaka ya da vakalar zinciriyle karşılaşıldığı taktirde daha kapsamlı müdahale planları hazırlamalıdır. Bu planlar ilgili tarafların tamamıyla paylaşılmalı ve güncel halde tutulmalıdır. Bu bağlamda, Türkiye özelinde AFAD, TAEK, Enerji Bakanlığı, İçişleri Bakanlığı, TİB, ICS-SOME (eğer varsa), ile Başbakanlığın ilgili birimlerinin koordinasyon içinde, ve gereken mevzuatı da oluşturarak, kapsamlı bir acil durum hazırlık planı geliştirmesi gerekmektedir. Bu plan ve mevzuat ışığında kurulacak bir kriz yönetimi merkezinin de doğru yerde ve krize doğru zamanda müdahale edebilecek şekilde oluşturulması gerekmektedir. Bu muhtemel planın tasarlanmasında ayrıntıların ROSATOM ve AREVA gibi ilgili paydaşlarla da paylaşılması önemlidir. Taraflar arasında doğrudan görüşme hatları yaratılmalıdır. Plan, acil durumdan önce, karar verilmesi daha kolay olacak olan hedefleri önem sırasına göre tanımlamalıdır. İdare, özellikle siber acil durumlarda tesisi korumak için ne yapılması gerektiğine karar vermelidir. Bu büyük plan, ulusal ekibin çözüm konusunda yetersiz kalması ve yardıma ihtiyaç duyması halinde acilen başvurulacak uluslararası üst düzey bir ICS-SOME ekibi seçeneğini de kapsamalıdır. AFAD bu acil durum hazırlık planını en az ayda bir test etmeli ve yeni çalışanları kodlara uygun davranmaya sevk etmelidir. Hazırlıklarından emin olmak için AFAD, nükleer enerji santrali ve kriz yönetimi yetkilisine yönelik bir siber saldırı için üçüncü bir taraf saldırı denetimcisi (*penetration tester*) de kullanmalıdır.

Yönetim, tesisin işletim sorumluluğunu üstlenmiş teknoloji mühendisleri ile siber güvenlik personeli arasında ayrışmalara sebep olabilecek bir takım iletişim sorunları yaşayabileceğini de göz önünde bulundurmalıdır. Sorunlar, çoğunlukla siber güvenlik personelinin tesis dışında olmasından kaynaklanır. Yönetim her iki grubun çalışma uyum ve bütünlüğünü sağlayarak çalışanların tamamının tesisin bekası açısından vazgeçilmez olduğunu onlara ifade etmelidir.

Nükleer tesisler de dâhil olmak üzere, özel sektör girişimlerinin neredeyse tamamında güvenlik yatırımlarının düzeyi risk ve sonuç arasındaki ikilemi yansıtmaktadır. Bu durum iki etmene bağlıdır: (1) risk çevresi hakkında bilinenler ve (2) rekabet içindeki bir pazarda, ya da kaynak eksikliği içeresindeyken ekonomik açıdan, kabul edilebilir ve sürdürülebilir olana. Türkiye'deki düzenleyici de bu dengeyi dikkate almalıdır. Bir nükleer enerji santralinin inşasına lisans verilmeden önce riski en aza indirmek adına düzenleyicinin santrali tasarım sorunları açısından da kontrol etmesi gerekmektedir. Siber güvenlik bakış açısından gerekli yazılımın denetlenmesi, güvenliği sağlamak ve olası tehditleri engellemek açısından kritik bir önem taşımaktadır. Nükleer enerji santrali çalışırken, güvenlik yazılımı uzun vadede bir takım yama ve güncellemelere ihtiyaç duymaktadır. Ancak, yanlış yazılım güncellemeleri saldırganların en çok kullandığı yöntemlerden biridir. Dolayısıyla, bilgi teknoloji ekibi programların yamalama sürecini düzenlemeli ve, nükleer enerji santrali siber sistemi uygulamaya koymadan önce, ayrıntılı testler yapmalıdır. İşletmeci, donanımın eskimesini önlemek amacıyla neredeyse başlangıçtan itibaren bir yenileme yönetimi planı oluşturmak zorundadır. Düzenleyici ise, tesisin güvenliğini sağlamak için işletmeci şirketi belirli aralıklarla donanım ve yazılımı yenilemeye zorlamalıdır. İşletmecinin teknolojik gelişmeye ayak uydurması güç ve maliyetli olabilmektedir. Bazen tesisin tasarımı bazen de ekonomik sebepler, işletmecinin yenileme yapmasını engelleyebilmektedirler. Ancak günden güne eskiyen sistemler, santralin nükleer güvenliğini tehlikeye atacaktır.

Türkiye'de, Akkuyu da dâhil olmak üzere, tüm nükleer enerji santralleri, ürettikleri elektriği aktarabilmek için elektrik şebekesiyle bağlantılı olmak zorundadırlar. Bu da elektrik şebekesinin tüm zafiyetlerinin nükleer enerji santralini de kolayca etkileyeceği anlamına gelmektedir. Türkiye'nin elektrik dağıtım sisteminde yakın zamanda yaşanan kesinti sırasında medyada çeşitli fikirler dile getirilmiştir. Bazı araştırmacılar

İran'ı siber saldırılarla suçlarken, diğerleri az sayıdaki elektrik santralinin arızalanmasının tüm elektrik şebekesini etkilediğini iddia etmiştir. Her neden kaynaklı olursa olsun bu olay, elektrik şebekesinin diğer kurumlarla bağlantılı olmasından dolayı bir dalga etkisinin mümkün olduğunu göstermiştir.[60] Akkuyu ve diğer nükleer enerji santralleri saldırılara karşı dayanıklı olarak kabul edilse bile, elektrik şebekesini hedef alan siber saldıralardan etkileneceklerdir. Bu nedenle nükleer santraller sadece fiziki etkilere değil aynı zamanda istenmeyen dijital etkilere karşı da güçlendirilmelidir.

Son olarak, yüksek irtifa elektro manyetik sinyal (EMS) saldırıları, kritik altyapılar için nükleer enerji santralleri de dâhil olmak üzere en etkili saldırılardan biri olarak görülmektedir. Bir EMS, yüklü partiküllerin hızlarının ani artışından kaynaklı aşırı yoğun bir elektro manyetik enerji patlamasıdır. Bu yıldırım benzeri sinyal, elektrik akımı hatlarından geçer, enerji hatları ve sigorta ve elektrik akımı hatlarına aşırı yükleme yaparak onlara zarar verir. Bu geniş bant, yüksek şiddetli (*amplitude*) EMS akımı, hassas elektronik aletlerle birlikte çalışınca, kritik altyapılara geniş çaplı ve uzun süreli zarar verme kapasitesine sahiptir.

Nükleer enerji santrallerinin SCADA sistemleri de EMS saldırılarına karşı savunmasızdır. ABD'deki Komisyon, EMS tehdidinin boyutunu değerlendirebilmek için farklı test ortamlarında denemeler yapmıştır. Yapılan denemeler sonucunda, test edilen sistemlerin tamamının EMS'ye maruz kaldıklarında çalışamaz hale geldikleri anlaşılmıştır.[61] Bu saldırı türü için EMS cihazı yapmanın, ya da temin etmenin, sanıldığından daha kolay olduğunu söyleyebiliriz. SCADA sistemlerinin fazla sayıda olması ve onlara karşı olan fazla bağımlılık, bir EMS vakası sonrasında, bu sistemlerin çalışmasına sistematik bir tehdit oluşturmaktadır. Ayrıca, çok fazla sayıda sistemi yeniden yükleme, onarma ya da değiştirme ihtiyacı, ülkenin böylesi bir saldırıyı atlatma sürecini de sekteye uğratacaktır. Dolayısıyla Ankara işletmecileri, bu tür saldırılardan korunmak için gerekli tedbirler almaya ve EMS saldırılarını olası saldırı senaryoları arasına eklemeye zorlamalıdır.

6. Sonuç

Stuxnet saldırısı sonrasında kritik altyapıların ve ana kaynakların korunması uluslararası arenada daha çok tartışılır hale gelmiştir. Uluslararası organizasyonlar kritik altyapılar için siber güvenliğin önemini vurgulayarak, durumsal farkındalığı arttırmaya odaklanmıştır. Bütün kritik altyapılar arasında nükleer enerji tesislerinin siber güvenliği istisnai bir yere sahiptir. Endüstriyel kontrol sistemlerinin güvenlik yaklaşımıyla tasarlanmaması, nükleer enerji tesislerinin düzenleyicilerine ve işletmecilerine siber güvenliğe azami dikkat göstermek için, politikalar oluşturmak ve etkili bir siber güvenlik kültürü inşa etmek zorunluluğu getirmektedir. Bu araştırmada sıralanan güvenlik olaylarının da gösterdiği gibi, hiçbir ülkenin nükleer tesisi siber saldırılara karşı tamamen korunmuş değildir. Ülkelerin nükleer faaliyetlerinin düzenleyici kurumları risk yönetimi, titiz bir koordinasyon ve stratejik iletişim vurgusuyla gerekli yasamayı tamamlamalı ve nükleer enerji tesislerinin çalışmasını kontrol edecek politikalar belirlenmesini sağlamalıdır.

Bütün bu önlemlere rağmen her gün yeni zafiyetleri kullanan yeni saldırı biçimleri görülmektedir. Uluslararası Atom Enerji Kurumu üyelerini yönlendirecek, bir bilgisayar güvenliği yol haritası oluşturmak için çalışmaktadır. Ulus devletler bu adımları takip ederek kritik altyapıları ve ana kaynakları koruyacak esas aktörlerdir. Türkiye'deki nükleer enerji tesisi yap – sahip ol – işlet modeliyle benzerlerinden daha farklı bir yere sahiptir. Projeyi üstlenen Rus ROSATOM firması ile Türk Akkuyu Nükleer AŞ, Türk yasa ve yönergelerinin nükleer tesisler için ihtiyaç ve beklentilerini karşılamak için teknik uzman yetiştirmekte, planlama yapmakta ve raporlar hazırlamaktadır. Her iki firmanın yüzleşeceği ilk büyük problem beşeri sermayedir. Böyle bir tesiste siber güvenlik ekibinin her iki toplumun güvenlik kültürleri hakkında bilgi sahibi olmasının yanı sıra iki dili de konuşabilmesi zorunludur. Nükleer enerji tesisi siber güvenliği, bilişim teknoloji altyapısı bilgisinin yanı sıra endüstriyel kontrol sistemleri hakkında derinlemesine bir uzmanlık gerektirmektedir. Şu anda Türk nükleer enerji tesisleri için nükleer mühendis yetiştirmek adına dikkati çeken bir gayret olmasına rağmen, bu konuda siber güvenlik uzmanlarının yetiştirildiğine dair herhangi bir bilgi bulunmamaktadır.

Problemin ikinci kısmı iki boyutludur. Birincisi, Ankara nükleer tesisin altyapısının en uygun şekilde hazırlanması için gereken yasama

ve yönetmelikleri çıkarmaya çalışmaktadır. Bütün devlet kurumları problemlerin çözümü için kendi mikro perspektiflerini ortaya koymakta ve kendi ilgi alanlarını seviyesinde düzenlemeler için gereken çabayı göstermektedir. Fakat bütün bu mikro yaklaşımlarını birleştirerek makro planı oluşturacak, koordinasyon yeteneğine sahip yetkili bir merci tam anlamıyla tanımlanmamıştır. İkinci olarak, Türkiye'de endüstriyel kontrol sistemlerine odaklı, sektördeki özel ve kamu kurumlarını koordine edebilecek bir siber güvenlik kurumu da bulunmamaktadır. Türkiye'nin bulunduğu coğrafi bölgedeki güncel politik sorunlar ve siber saldırıların uluslararası hukuk açısından belirsizliği göz önüne alındığında Türkiye kendi savunma ve saldırı amaçlı siber güvenlik kapasitesini geliştirmek zorundadır. Ankara'nın ısrarlı bir şekilde gerekli kurumlar arasında koordinasyona ve stratejik iletişime odaklanması gerekmektedir.

1- Joshua Yates, "Interview with Ulrich Beck",The Hedgehoc Review, 5:3, Güz 2003, s.97.

2- Mordechai Guri, Matan Monitz, Yisroel Mirski, Yuval Yelovici. "Bitwhisper: Covert Signalling Channel Between air-gapped computers using Thermal manipulations". http://arxiv.org/pdf/1503.07919v1.pdf;

3- Kim Zetter, "Researchers hack air gapped computer with simple cell phone". Wired, 27 Haziran 2015, http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/ (Erişim Tarihi 29 Haziran 2015)

4- Kim Zetter, "How attackers can use radio signals and mobile phones to steal the protected data". Wired, 03 Kasım 2014, http://www.wired.com/2014/11/airhopper-hack/ (Erişim Tarihi 01 Temmuz 2015)

5- DBT nükleer, radyoaktif madde ya da ilgili tesislerin fiziksel güvenliğinin tasarlanıp, değerlendirilmesi amacıyla yapılan, radyoaktif madde hırsızlığı ya da sabotaj gibi kötücül faaliyetlere teşebbüs edebilecek iç veya dış saldırganların nitelik ve özelliklerinin tanımıdır. Daha fazla detay için bkz; "Development, use and maintenance of the design basis threat: implementing guide". Viyana: International Atomic Energy Agency, 2009.

6- Benzer eğilimleri Havex, Dragonfly ve Blackenergy kötücül yazılımlarında da görmekteyiz.

7- Russia: Hidden chips 'launch spam attacks from irons, BBC News, 28 Ekim 2013, http://www.bbc.com/news/blogs-news-from-elsewhere-24707337

8- "Sıfır-gün istismarı şeklinde kullanılan bu kısaltma bir yazılımın keşfi anında ortaya çıkan zafiyeti anlatmaktadır. Bu nedenle sıfır-gün saldırıları, güvenlik topluluğu ya da yazılımın satıcısı henüz zafiyetin varlığının farkına varmadan ya da bu çerçevede koruma için gereken yamaları eklemeden gerçekleşir. Bu nedenle de bu türdeki kötü niyetli kullanımlar crackerların sistemde azami hasarı yaratmalarına imkân tanımaktadır." Bkz. Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, s. 371.

9- Sözel İletişim Protokolleri iletişimi kontrol etmek için hazırlanmışlardır. Yerleşik sistemlerde bilgi değişiminin nasıl yapılacağının kurallarını belirleyen programlardır.

10- David B. Fogel, "What is evolutionary computing?" Spectrum IEEE, 37(2), 2000, ss. 26-32.

11- David B. Fogel – Lawrence J. Fogel, "An Introduction to Evolutionary Programming", Artificial Evolution, Springer: Volume 1063 of the series Lecture Notes in Computer Science, 2005, s. 21.

12- WINS, Human Reliability as factor in nuclear security, World Institute for Nuclear Security, 2012, s. 3.

13- "İç tehdit kavramı tesislere, taşıma faaliyetlerine ya da hassas bilgisayarlara ve

iletişim sistemlerine erişim yetkisine sahip, yetkisini ve güvenilir pozisyonunun yetkilendirilmediği amaçlar için kullanan kişileri (çalışan ya da yüklenici) tanımlamaktadır." Wins, "Managing Internal Threats (Rev. 1.0)", World Institute of Nuclear Security, 2010, s.3.

14- IAEA, Preventive and Protective Measures against Insider Threats, Viyana, 2008.

15- Ralph Langner, "To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve", Kasım 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (Erişim tarihi 19 Kasım 2015)

16- Ralph Langer, "Stuxnet's Secret Twin". Foreign Policy, 19 Kasım 2013, http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack (Erişim tarihi 26 Ağustos 2014)

17- IAEA, Computer security at nuclear facilities : reference manual ,Viyana, 2011, ss. 39-40.

18- Matt Paulson, "Cyber-Terrorism Struck the Nuclear Regulation Commission Three Times in Three Years", 19 Ağustos 2014, http://it.tmcnet.com/topics/it/articles/2014/08/19/386959-cyber-terrorism-struck-nuclear-regulation-commission-three-times.htm

19- W32/Slammer, http://www.f-secure.com/v-descs/mssqlm.shtml

20- Kevin Poulsen, "Slammer worm crashed Ohio nuke plant network", SecurityFocus, 2003, http://www.securityfocus.com/news/6767

21- United States Nuclear Regulatory Commission, "Effects of Ethernet-Based, non-safety related controls on the safe and continued operation of nuclear power stations", http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf

22- A.g.e.

23- Robert McMillan, "Nuclear Plant Shutdown by Network Trouble", PCWorld, 2007, http://www.pcworld.com/article/132118/article.html

24- Robert Lemos, "Data Storm blamed or nuclear - plant shutdown", Security Focus, 2007, http://www.securityfocus.com/news/11465

25- Brian Krebs, "Cyber Incident Blamed for Nuclear Power Plant Shutdown", Washington Post, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html

26- Daha fazla detay için bkz; http://www.nrc.gov/reading-rm/doc-collections/event-status/event/

27- Reuters, "Malicious Virus Shuttered US Power Plant", Ocak 2013, http://www.voanews.com/content/us-power-plant-computer-virus/1585452.html

28- Industrial Control Systems Cyber Emergency Response Team, "ICS-CERT

Monitor", Ekim/Kasım/Aralık 2012, http://ics-cert.us-cert.gov/monitors/ICS-MM201212

29- A.g.e.

30- Karsten Nohl, Sascha Krissler, Jakob Lell, "Bad USB. On accessories that turn evil". https://srlabs.de/blog/wp- content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf

31- Michael Riley - Dune Lawrence, "Hackers linked to China's Army seen from EU to D.C.", Bloomberg, Haziran 2012, http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine- candor.html

32- Michael Riley - Eric Englaman, "Why congress hacked up a bill to stop hackers", Bloomberg, Kasım 2012, http://www.businessweek.com/articles/2012-11-15/why-congress-hacked-up-a-bill-to-stop-hackers

33- "Monju power plant facility PC infected with virus", Japan Today, 7 Ocak 2014, http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus

34- Sıfır gün zafiyeti, yaygın olarak kullanılan yazılımlarda bulunan ve yazılım sahibi firmanın da bilmediği zayıflıklara işaret etmektedir. Bu zayıflıklar tesbit edebilen hacker grupları bu sayede bu yazılımın kullanıldığı bilgisayar sistemlerinin kontrolünü ele geçirebilmektedirler.

35- Geoff McDonald, Liam Murchu, Stephen Dolerty, Eric Chien, "Stuxnet 0,5 The missing link", 6 Şubat 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

36- Kim Zetter, "How digital detectives deciphered Stuxnet, the most menacing malware in history." Arstechnica, 11 Haziran 2011, http://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most- menacing-malware-in-history/3/

37- Ralph Langner, "To kill a centrifuge A technical Analysis of what Stuxnet's Cretors tried to achieve", Kasım 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

38- Nicolas Falliere, "Exploring Stuxnet's PLC Infection Process" Symantec, 22 Eylül 2010, http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

39- "US - Israeli computer super-worm hit Russian nuclear plant Kaspersky" Reuter, 12 Kasım 2013, http://rt.com/usa/kaspersky-russia-nuclear-plants-612/

40- Salih Bıçakcı, 21yy Siber Güvenlik, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2013.

41- Bir Bulletin Board System'i, kullanıcıların terminal program kullanarak sisteme bağlanmaları ve giriş yapmalarını sağlayan bir bilgisayar sistemi yürütme yazılımıdır.

42- Crackerlar (genel kavram): Başkalarının bilgisayar sistemlerine yetkisiz bir biçimde girerek yazılımın kopyalama koruma hükümlerini kırmak, internet sitelerini ele geçirmek, web sitelerini bilinçli olarak tahrif eden ve kimlik ya da para çalmak amacıyla kodları ele geçiren gruplardır. Bu kişiler tanımlamak içim zaman zaman "ağ hackerları" ya da "ağ koşucuları" da denilmektedir. Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, s. 73.

43- Mini S. Thomas – John D. McDonald, Power System SCADA and Smart Grids, Boca Raton: CRC Press, 2015.

44- Erica Harefors, "Use of large screen displays in nuclear control room" Yayınlanmamış mezuniyet tezi, Institute Energiteknikk, Uppsala Universitet, 2008. http://www.utn.uu.se/sts/cms/filarea/0804_härefors.pdf

45- Bir diğer siber saldırı kategorisi de semantik saldırılardır. Bu türde saldırılar, hileli yönlendirme, bilgiyi değiştirme ve kandırma gibi karar alma süreçlerine zarar verebilecek yöntemlerle sisteme ve bilgiye olan güveni yıkmayı ve amaçlamaktadır.

46- Tünel Görüşü, sadece tek bir şeyi düşünerek diğer her şeyi göz ardı etme eğilimine verilen addır. http://www.merriam-webster.com/dictionary/tunnel%20 vision (Erişim tarihi 27 Ağustos 2014)

47- Dileep Buddaraju, "Performance of control room operators in alarm management", Yayınlanmamış yüksek lisans tezi, Lousiana State University, 2008, s. 2.

48- Bilgisayar sistemleri, güvenlik planlaması sırasında, bilgi bütünlüğünü güçlendirmek amacıyla çok seviyeli güvenlik stratejilerinin ihtiyaçlarını karşılayacak biçimde tasarlanmalıdır.

49- Tailgating: "Bu yakınınızdaki kapalı kapıları kontrol ederek fırsat bulduğunuzda kullanma yöntemiyle düzenlenen saldırılara verilen addır. Prensip olarak yeterince kolay gözükmekle birlikte uygulamada başarılı bir saldırı düzenlemek için bir miktar ön hesaplamaların yapılmasını gerektirmektedir. İhlalci, aktive edilmiş herhangi bir yanıltıcı kullanmadan yakınındaki bir kapı kilidini açamaz. Bilinen en klasik yöntem koridorda, kapının yakınında bir yerlerde telefonla 'konuşmak' ve yanınızdan geçen birisinin kapıyı açmasıyla konuşmayı bitirmektir. Sonrasında onu takip edersiniz. Sadece, bir telefon çağrısına cevap vermek için dışarı çıkmışsınız ve sonra da içeriye geri dönmüşsünüz izlemini vermeniz yeterlidir." Will Allsopp, Unauthorised Access: Physical Penetration Testing for IT Security Teams, Wiley: Sussex, 2009, s. 34.

50- Steve Huff, "Access HVAC Systems via Big Security Holes". Observer, http:// observer.com/2012/12/hackers-in- the-vents-cyber-intruders-could-access-hvac-systems-via-big-security-holes/ (Erişim tarihi 11 Mart 2015)

51- Güvenlik seviyeleri modeli, bir kritik altyapı tesisinin güvenliğini sağlamak amacıyla güvenlik önlemlerinin derecelendirilerek uygulanmasına verilen addır. Ayrıntılı bilgi için bkz. IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Viyana: 2011, ss. 29 – 35.

52- George Kamis, "Resolving the Critical Infrastructure Cybersecurity Puzzle", Signal AFCEA, March 2014, http://www.afcea.org/content/?q=resolving-critical-infrastructure-cybersecurity-puzzle (Erişim tarihi 29 Aralık 2015)

53- IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, ss. 29 – 35.

54- A.g.e., s. 32.

55- Majed Al Breiki, "Cyber Security Design Methodology for Nuclear Power Control and Protection Systems", http://www.automation.com/pdf_articles/Cyber_Security_Design_Methodology.pdf (Erişim tarihi 5 Ekim 2015)

56- IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, s. 31.

57- IAEA, "Computer Security at Nuclear Facilities –Reference Manual", Nuclear Security Series, Vienna: 2011, s. 33.

58- AFAD, 2014 – 2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, Eylül 2014, s. 4, https://www.afad.gov.tr/Dokuman/TR/123-20141010111330-kritikaltyapi-son.pdf (19 Eylül 2015'de erişildi)

59- Kenneth R. Hammond, Judgments under Stress, Oxford University Press: New York, 2000; Judgment and Decision making at work, S. Highhouse, Reeshad S. Dalal, E. Salas (eds.), Routledge: New York, 2014.

60- TEİAŞ – ENTSOE, "Report on Blackout in Turkey on 31st March 2015", 21 Eylül 2015, https://www.entsoe.eu/Documents/SOC %20documents/Regional_Groups_Continental_Europe/20150921_Black_Out_Report_v10_w.pdf (Erişim tarihi 21 Ekim 2015)

61- "Report to the Commission to Assess the threat to the United States from Electromagnetic Pulse Attack, Critical National Infrastructures", Nisan 2008, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf (Erişim tarihi 15 Eylül 2015)