ULUSLARARASI ÇERÇEVEDE SİBER GÜVENLİK VE NÜKLEER ENERJİ

Doç.Dr. Ahmet Han

Rektör Danışmanı ve Fakülte Üyesi-
Kadir Has Üniversitesi

Yönetim Kurulu Üyesi- EDAM

Prof.Dr. Mitat Çelikpala

Dekan, Sosyal Bilimler Yüksek Okulu-
Kadir Has Üniversitesi

1. Giriş

Enerji kaynak çeşitliliğine nükleeri de eklemek isteyen Türkiye'nin 2023 hedefi üç nükleer santrale sahip olmak ve elektrik ihtiyacının %20'sini bu nükleer tesislerden sağlamaktır. Yüzde 20'lik bu hedef, günümüzde ABD'de elektrik üretiminde nükleer santrallerin sahip olduğu paya eşittir.[1] Açıkça görüldüğü üzere bu oldukça iddialı bir hedeftir. Bu bağlamda söz konusu tesislerinin siber güvenliğinin sağlanması özel önem atfedilmesi gereken bir alan olarak belirginleşmektedir. Bu çalışma nükleer tesislerin siber güvenlik meselesinin uluslararası boyutuna odaklanarak, Türkiye örneği açısından önemli kabul edilebilecek uluslararası gelişmeleri tartışacaktır.

2. Siber Uzay, Siber Saldırı, Siber Suç: Kavramsal bir Giriş

Siber uzay, alan ve zaman sınırlamasının söz konusu olmadığı, görece bilinemez bir düzlem olarak belirginleşmektedir. Farklı kaynaklarda farklı biçimlerde tanımlanan bu alan için "bilginin depolanması, düzenlenmesi ve iletilmesi amacıyla kullanılan, dijital ağlarca yönetilen, ağların kendi alanlarında gerçekleştirdikleri işlemlerin de dâhil olduğu dijital faaliyetlerin yer aldığı her türlü ağ" tanımı örnek bir tanım olarak sunulabilir.[2] Bu haliyle siber uzay, "internetin yanı sıra, altyapıyı ve hizmetleri destekleyen diğer bilgi sistemlerini de içerir."[3] Bilgi bu alanda dolaşır. Çoğu zaman ağı kimin ya da neyin kontrol ettiğini, niyetini, kapasitesini ve hedefini bilmek neredeyse mümkün değildir. Son dönemde kritik altyapılardaki ağ sistemlerine sağlanan hizmetin kalite ve etkinliğinde gelişme kaydedilmiş olsa da, bu sistemleri kullanan kurum ve kuruluşların, sistemlerin güvenliğinin devamlılığını sağlamak için yüklendikleri maliyetler çok yükselmiştir.

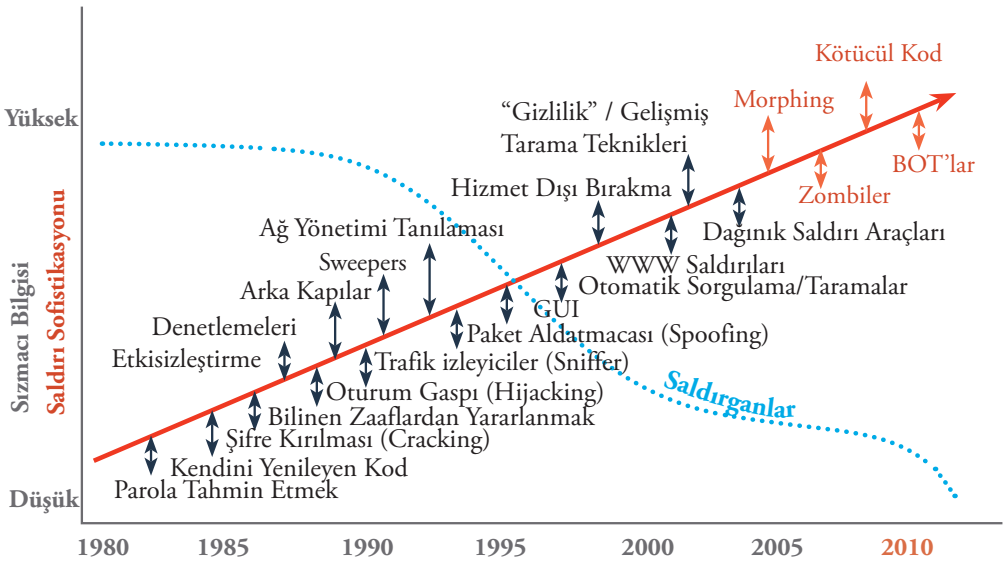
Devletlerin ve çeşitli uluslararası kuruluşların siber uzayda işleyen sistemlerin güvenliğini tehdit eden siber saldırıları tanımlamaya çalıştıkları görülmektedir. ABD Savunma Bakanlığı, siber saldırıyı "bilgisayar veya bilgisayar bağlantılı ağ ve sistemleri kullanarak hasımlarının siber sistemlerini, varlıklarını ve bunların işleyişini aksatmayı ve/veya tamamen yok etmeyi amaçlayan düşmanca eylem"[4] şeklinde tanımlamaktadır.

Bakanlık bu tanımda, altyapıyı bozma ya da yok etme ibaresine de yer vererek, siber saldırı teşebbüslerini yalnızca bilgisayar sistemlerine ve verilere yönelik olanlarla sınırlamamaktadır. NATO'nun Talinn El Kitabı'ndaki 30 numaralı kuralda siber saldırı, "ister taarruzi, ister müdafi olsun kişilerin yaralanmasına veya ölümüne ya da nesnelerin zarar görmesine veya yok olmasına yol açması beklenen bir siber operasyon" şeklinde tanımlanmaktadır.[5] Bu türde saldırılar, "güvenliğin bilgi ortamındaki standart hedefleri"[6] sayılan, bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine zarar vermeyi hedeflemektedir. Bu bağlamda gizlilik, "bilginin gizli tutulmasıdır." Bütünlük, bilginin "uygunsuz biçimde bozulmadığı ya da yetkisiz kişilerce değiştirilmediğinden" emin olmak demektir ki bu bilginin güvenilir olduğu anlamına da gelmektedir. Erişilebilirlik ise "sistemin beklentilere uygun bir biçimde kullanılabilmesi" anlamına gelmektedir."[7] Bu saldırılar, tanımları gereği devlet faaliyetlerinin ve kritik altyapıların neredeyse tamamını ilgilendirmektedir. Tanımların ortak kaygıları birarada değerlendirildiğinde; siber saldırı, doğrudan bilgi sistem ve teknolojilerine ve/veya kritik altyapı unsurlarına, stratejik hedefler gözeterek, sızma anlamına gelmektedir. Saldırganlar bunu yaparken karmaşık yöntemler kullanırlar ve bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine zarar vermeyi hedeflerler.

Genelde siyasi amaçlar güden bu saldırıların yanı sıra suç odaklı saldırılar da söz konusu olabilmektedir. Bilgi sistemleri ve teknolojileri açısından ciddi sorunlar yaratmak bağlamında, "geleneksel suçların bir tür uzantısı durumundaki siber suçlar, geleneksel suçlardan farklı olarak, bilgisayar sistemlerince yaratılmış fiziki olmayan siber uzayda işlenmektedir."[8] Bu alanı etkin biçimde kullanan siber suçluların, iletişim için gerekli ağ bağlantısına sahip oldukları sürece dünyanın herhangi bir yerinden, dünyanın herhangi bir yerindeki bilgisayar sistemine erişme imkânları vardır.[9] Bu yeni sınırsız ve görece belirsiz alanda, zaman, konum ve fiziksel sınırlamalar gibi kavramlar anlamlarını yitirmektedir. Siber suçlular, uzmanlık ve sofistikasyonun nerdeyse her şey anlamına geldiği siber uzayda, sahip oldukları uzmanlığı dijital dünyanın bilinmezliği ya da uluslararası boyutu ile birleştirerek diğer siber suçlularla işbirliğine gitmekte ve siber çeteler olarak adlandırılabilecek türde yapılar yaratmaktadırlar. Bu bağlamda, "siber savaş aktörlerinin" de siber suçluların kullandığı araç ve yöntemleri kullandığını söylemek yanlış olmayacaktır.

Siber alanın doğası gereği bu türde saldırıların, "nükleer alan da dâhil" olmak üzere "engellenmesi, kontrolsüz biçimde yayılmasının önlenmesi ve kritik altyapı açısından çok sayıda tehlikeye neden olmasının önüne geçilmesi" zordur.[10] Şekil 1'de altı çizildiği üzere, sofistike saldırı sayısında devamlı bir artış görülmektedir ve saldırganların daha sofistike saldırı düzenleyebilmek için ihtiyaç duydukları bilgi seviyesi azalmaktadır. Bu bağlamda, siber saldırganların sofistikasyon eşiğinin bilgi derinliği azaldıkça, risk sürekli biçimde evrilip artmaktadır. Bu gerçekliğin yarattığı yeni ortam, bilgisayar güvenliği programlarının çok fazla tür ve sayıda muhtemel saldırı senaryolarını kapsayan değerlendirme seviyelerine ulaşmasını gerektirmektedir.[11] Siber saldırganların motivasyon, çıkar ve yetenekleri hakkındaki belirsizlik arttıkça bilişim sistemlerinin maruz kalabilecekleri zafiyetlerin kamusal görünürlüğü de artmaktadır.

Şekil 1. Saldırgan Görünüşlerine (Profil) Bağlı Olarak Tehditlerin Artan Karmaşıklığı



2.1. Canavarın Doğası: Siber Saldırganlar

Siber saldırganları, hedefledikleri kurum ve kuruluşlar karşısındaki konumlarına göre sınıflandırmak mümkündür. Bu bağlamda, en azından kâğıt üzerinde karşımıza iki ana grup çıkmaktadır: iç ve dış saldırı/saldırganlar. İçeriden kaynaklanan saldırılar, basitçe, bilişim sistemlerine erişim yetkisi çalıştıkları kurum tarafından verilen, hâlihazırda o kurumda çalışan ya da erişime yetkili olan yüklenici firmalarda görev yapan kişilerin düzenledikleri saldırılardır. Dışarıdan kaynaklanan saldırılar ise kurum dışındaki kişi ve kurumlarca düzenlenen saldırılardır.

Carnegie Mellon Üniversitesi, Yazılım Mühendisliği Enstitüsü'ne (Software Engineering Institute) bağlı olarak faaliyet gösteren Bilgisayar Acil Durum Hazırlık Timi'nin (the Computer Emergency Readiness Team-CERT) düzenli olarak tekrarladığı anketlere göre, 2010'dan bugüne gerçekleştirilen siber saldırıların yaklaşık yüzde 30'u içerideki aktörlerce yapılmıştır.[12] Aynı araştırmanın sonuçlarına göz atıldığında karşımıza çıkan bir diğer önemli sonuç, tesisin içinden düzenlenen saldırıların dışarıdan düzenlenen saldırılara oranla, saldırılan kuruma yüzde 46 oranında daha fazla maliyete yol açtığıdır.[13] Bu anket bilgisinden elde edilen sonuçlar daha ayrıntılı bir biçimde incelendiğinde, araştırmaya katılan kuruluşların yüzde 43'ünün hangi türde saldırının daha fazla maliyete yol açtığını, hatta saldırının içeriden mi yoksa dışarıdan mı olduğunu belirleme yeteneğine sahip olmadığını göstermektedir.[14]

Açıkçası bir saldırıya içeriden unsurların dâhil olması, saldırının başarı ihtimalini arttırmaktadır. İçeride bulunan unsurların yarattığı risk, nükleer tesisler de dâhil olmak üzere, tüm kurum ve kuruluşlar açısından önemli bir başlıktır. Tehdidi zamanında saptamak oldukça zordur. Ayrıca, uygun biçimde tasarlanmış emniyet/güvenlik kültürünün olmaması durumunda dâhili unsurların, farkında olmadan haricilerin kullandıkları birer araca dönüşme ihtimalleri de söz konusudur. Bu nedenle, ağırlıklı olarak güvenlik sisteminin sadece bir unsuruna odaklanmış, tek boyutlu ve tek katmanlı güvenlik düzenlemelerine bel bağlanmamalıdır. Daha da önemlisi, başlangıçta güvenilir çalışanlar olan tesis personeli, inşaat işçileri ve bakım görevlileri zamanla kendi istekleriyle ya da zorla taraf değiştirebilirler. Bu bağlamda, diğer faktörlerin yanında kurumsal kültür ve çalışan memnuniyeti gibi konular, zamanla belirleyici etkenlere

dönüşebilmektedir. Gerçekte ise "tehditler farklı ve karmaşık şekillerde ortaya çıkmaktadır" ve risklerin ve sistemlerin "mümkün olduğunca gerçekçi biçimde" düzenli olarak değerlendirilmesi ve denenmesi büyük önem arz etmektedir.[15]

Aşağıdaki tablolar[16] nükleer güç santralleri tesislerine karşı başlıca iç ve dış tehditleri, saldırganların kaynakları, siber saldırılar için ihtiyaç duydukları zaman, araçları ve niyetleri de dâhil olmak üzere sıralamaktadır.

Tablo 1. İçeriden Kaynaklanan Tehditler

Saldırgan	Kaynak	Zaman	Araç	Saik
Gizli ajan	Kolaylaştırılmış 'sosyal mühendislik'. Belirli seviyede sisteme erişim. Sistem belgeleme ve uzmanlığı mevcuttur.	Değişken ama genelde çok uzun saatler ayıramazlar.	Var olan erişim, programlama ve sistem mimarisi bilgisi. - Mevcut şifreleri bilme ihtimali. - Özel olarak yaratılmış arka kapıları ve veya Trojan'ları yerleştirme ihtimali. - Muhtemel dışarıdan uzmanlık yardımı.	İş bilgisi, teknolojik sır, personel bilgisi hırsızlığı. Mali kazanç (rakiplere bilgi satmak). Şantaj.
Garezli çalışan/ kullanıcı	Orta/Güçlü kaynaklar. Belirli seviyede sisteme erişim. Belli iş ve faaliyet sistemlerinde sistem belgeleme ve uzmanlığı mevcuttur.	Değişken ama genelde çok uzun saatler ayıramazlar.	Var olan erişim, programlama ve sistem mimarisi bilgisi. Mevcut şifreleri bilme ihtimali. Amatörce araç ve kod yerleştirme yetisi (eğer belli bilgisayar yetenekleri varsa daha özenle hazırlanmış olabilir).	İntikam, kaos, zarar vermek. Şirket bilgisi hırsızlığı. İşveren/ başka çalışanı utandırma. Kamu nezdinde imajı ya da güveni zedeleme.

Tablo 2. Harici Tehditler

Saldırgan	Kaynak	Zaman	Araç	Saik
Keyif için hacker	Farklılaşmış ama genelde sınırlı yetenekler. Sistem hakkında kamu bilgisinin ötesinde kısıtlı bilgi.	Zamanı boldur ama sabırsızdır.	Genel olarak erişilebilen kodlar ve araçlar. Bir miktar araç geliştirme yeteneği olabilir.	Eğlence, statü. Fırsat bulup hedef almak. Erişimi kolay hedeflerden yararlanmak.
Nükleer güce militanca karşıt kişi	Kısıtlı kaynaklar ama gizli kanallar tarafından mali olarak gizlice desteklenebilir. Siber camianın araçlarına erişim. Sistem hakkında kamu bilgisinin ötesinde kısıtlı bilgi.	Saldırılar önceden bilinen belli etkinliklere yöneltilebilir (örneğin kutlamalar, seçimler). Bolca zaman, sabırlı ve motivasyon sahibi.	Bilgisayar yetenekleri mevcut. Hacker camiasından yardım alması mümkün. 'Sosyal mühendislik'.	Dünyayı kurtarma inancına sahip. Kamu görüşünü belli meselelerde değiştirmek. Şirket faaliyetlerini aksatmak.
Garezli çalışan/ kullanıcı (artık çalışmayan)	Eğer daha büyük bir grup insanla bir arada değilse kısıtlı kaynaklar. Hala sistem belgelerine sahip olabilir. Düzenlenmemiş eski erişimini kullanabilir. Tesis çalışanlarıyla muhtemel bağlantılar.	İlintili kişilere bağlı olarak farklılık gösteren.	Var olan şifreleri bilme ihtimali. Kontrol edilmeyen eski erişimini kullanılabilir. Çalıştığı dönemde sistemde arka kapılar yaratabilir. 'Sosyal mühendislik'.	İntikam, kaos, zarar vermek. İş bilgisi hırsızlığı. İşveren/başka çalışanı utandırma. Kamu nezdinde imajı ya da güveni zedeleme.
Organize suç	Güçlü kaynaklar. Siber uzmanlığın kullanılması.	Farklılık gösteren ama kısa vadeli.	Kodlar, evde yapılmış araçlar. "Kiralık hacker" tutabilir. Eski ya da mevcut çalışanları kullanabilir. 'Sosyal mühendislik'.	Şantaj. Nükleer madde hırsızlığı. Haraç (mali kazanç) Şirketlerin mali ve algı korkularından yararlanmak. Satılık bilgi (teknik, iş ile ilgili ve kişisel).

Saldırgan	Kaynak	Zaman	Araç	Saik
Ulus devlet	Güçlü kaynaklar ve uzmanlık. İstihbarat toplama faaliyetleri. Sistem üzerinde eğitim/uzmanlık sahibi olma ihtimali.	Farklılık gösteren.	Eğitimli siber uzmanlardan oluşan ekipler. Gelişmiş araçlar. Eski ya da mevcut çalışanları kullanabilir. 'Sosyal mühendislik'.	İstihbarat toplama. Sonra alınacak eylemler için erişim noktaları açmak. Teknoloji hırsızlığı.
Terörist	Farklı yetenekler. Sistem üzerinde eğitim/uzmanlık sahibi olma ihtimali.	Bolca zaman, çok sabırlı.	Kodlar, evde yapılmış araçlar. "Kiralık hacker" tutabilir. Eski ya da mevcut çalışanları kullanabilir. 'Sosyal mühendislik'.	İstihbarat toplama. Sonra alınacak eylemler için erişim noktaları açmak. Kaos. İntikam. Kamu görüşünü etkileme (korku).

Siber saldırıların sınıflandırılmasında başvurulan bir diğer yaklaşım, saldırganların niyetlerine bakmaktır. Bu türde bir sınıflandırmada karşımıza hackerlardan suçlulara kadar uzanan geniş bir yelpaze çıkmaktadır.[17] Hackerlar, "can sıkıntısı ve entellektüel meydan okuma arzusundan esinlenerek kısıtlanmış bilgiyi elde etmeyi amaçlamaktadırlar." Vandallar, "mümkün olan en büyük hasarı vermeyi amaçlamaktadırlar". Suçlular ise, "ekonomik kazanç duygusuyla, amaçlarına ulaşmak için aralarında casusluk ve yolsuzluğun da olduğu her türlü taktiği kullanmaktadırlar."[18] Muhtemel saldırganların niyetlerini öngörmek, olası hedeflerini tespit etmek ve buna uygun önlemler almak açısından elzemdir.

Siyasi karar alıcılar üzerinde etki yaratmayı amaçlayan toplumsal eylemciler ve teröristler de interneti gittikçe artan bir biçimde kullanmaktadırlar. Bu grupların, siber uzayı gerçek bir savaş alanına dönüştürmek için gerekli olan araçların yanı sıra, teknik ve kurumsal yöntemler edindikleri ve kritik altyapıya gerçek bir tehdit oluşturdukları görülmektedir. Bu türde faaliyetlere yönelen grupların siyasi hedeflerine tam anlamıyla ulaşmaları çok mümkün görünmemekle birlikte, idareye ait bilgisayarlara erişimin bir tür güç verdiği ve medyanın ilgisini çektiği bir gerçektir.

3. Nükleer Enerji Santralleri ve Kritik Enerji Altyapıları

Kritik altyapı, bağımsız çeşitli tesislerin birbirleriyle bağlantısını sağlayan ve işlevleriyle toplumun devamlılığına katkı sağlayan, fiziki ve/veya kurumsal asli sistemlerdir. Amerikan Anavatan Güvenliği Bakanlığı'nın değerlendirmesiyle, kritik altyapılar, "ulusun ekonomik, güvenlik ve sağlık sektörlerinin omurgası olarak kabul edilen fiziki ya da sanal varlık, sistem ve ağlardır. Bunlar, Birleşik Devletler için o kadar hayati bir konuma sahiptirler ki, zarar görmeleri ya da çalışamaz hale gelmeleri halinde ülkenin güvenliği, ulusal ekonomik güvenliği, ulusal kamu sağlığı ve emniyeti ya da bunların birkaçı üzerinde zafiyet yaşanmaktadır."[19] Başbakanlık Afet ve Acil Durum Yönetim Başkanlığı (AFAD) da, kritik altyapıyı, bu tanıma benzer bir biçimde tanımlamaktadır: "İşlevini kısmen veya tamamen yerine getiremediğinde, çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür."[20]

Bir altyapının ne kadar kritik olduğunu üç unsur belirlemektedir: kritik altyapının sembolik önemi, bu altyapıya olan bağımlılık ve karmaşık bağımlılıklar.[21] Halkın, idarenin kritik altyapı üzerindeki hâkimiyetine olan inancı, sembolik olduğu kadar hayati önem taşımaktadır. Kritik altyapıya bir hasar gelmesi halinde zarar görecek tek şey idarenin çalışma kabiliyeti olmayacaktır. Bundan daha önemli olan, vatandaşların idareye hatta rejime olan güvenlerinin kaybolması ihtimalidir. Bu altyapılar birbirleriyle bağlantılı ve ilintilidirler. Herhangi bir unsurda yaşanan zarar ya da aksama, zincirleme ya da kelebek etkisiyle, diğer unsurlarda da bir takım kapsamlı aksamaların yaşanmasına neden olabilir.

Nükleer tesislerde kullanılan mesleki uzmanlık, finansal ve teknolojik bilgi, bilimsel ve fikri haklar gibi bileşenler, bilişim sistemleri aracılığıyla, program, veri tabanı gibi biçimlerde bir araya gelmektedir. Bundan ötürü nükleer santraller yalnızca fiziksel kritik altyapılar olmanın ötesinde, çalışmak için sağlıklı işleyen bilişim sistemlerinin varlığına muhtaçtırlar. Bilişim sisteminde meydana gelebilecek herhangi bir hasar geniş kapsamlı olabilir, hatta fiziksel hasarlara da yol açabilir. Bu nedenle tesisin fiziki güvenliği ile siber/bilgisayar güvenliği planları birbirini tamamlayacak şekilde tasarlanmalıdır

Nükleer tesis ve altyapılara yönelik, "kötü niyetli olmayan" saldırıları da içeren ve strateji, siyaset ve suç boyutlarını dikkate alan kapsamlı bir tanımlama, ABD Nükleer Düzenleme Komisyonu'nca hazırlanan Nükleer Tesisler için Siber Güvenlik Programları (*Cyber Security Programs for Nuclear Facilities*) başlıklı Düzenleyici El Kitabı 5.71'de yer almaktadır:

> "Bilgisayar, iletişim sistemleri ya da ağlarına yönelik fiziki ya da mantıki (elektronik ya da dijital) tehditler şu şekillerde karşımıza çıkabilmektedir: (1) lisans sahibine ait tesislerin içinden ya da dışından kaynaklananlar, (2) dâhili ve harici unsurları barındıranlar, (3) fiziki ve mantıki tehditleri içerenler, (4) tabiatı itibariyle doğrudan veya dolaylı olanlar, (5) kötü niyetli olan ve olmayan tehdit unsurlarınca gerçekleştirilenler ve (6) kritik dijital unsurlarda veya kritik sistemlerde doğrudan ya da dolaylı biçimde olumsuz etki ya da sonuçlar yaratabilecek potansiyele sahip olanlar. Bir siber saldırı bunlardan birini ya da birkaçını içerecek şekilde gerçekleştirilebilir."[22]

Her ne kadar nükleer tesisler hâlihazırda siber saldırıların hedefi olsa da, bilgi alışverişi ve en iyi uygulama örneklerinin paylaşılması gibi konularda küresel ölçekli koordinasyon ve işbirliği adına atılan adımların sınırlı olduğu görülmektedir.[23] Ülkelerin ve özel sektöre mensup tesis işletmecilerinin büyük bir çoğunluğu bu konuyu "hassas bilgi" kategorisinde ele almakta ve bu türde saldırılara ilişkin bilgi ve deneyimleri paylaşmaktan kaçınmaktadırlar.[24] Sofistikasyonun gittikçe arttığı uluslararası ortamda, hacktivistler, içeriden kaynaklanan tehditler, suçlular, devletler ve Suriye'den Irak'a uzanan geniş bir alanda etkin olan DAEŞ gibi terörist yapılanmaların, siber saldırı düzenleyebilme yönünde imkân ve kabiliyetlerini arttırdıkları görülmektedir. 2014 yılında sadece ABD'de gerçekleştirilen siber saldırıların yaklaşık %35'inin kritik enerji altyapısını hedeflediği ve bunun da %2'sinin nükleer tesislere yönelik olarak gerçekleştirildiği akla getirildiğinde, durumun aciliyet kazandığı anlaşılmaktadır. Bu saldırıların %55'inin "gelişmiş kalıcı tehditler" (*advanced persistent threats*) olduğu ve sofistike aktörlerce" gerçekleştirildiğinin altı çizilmelidir.[25]

Hasım olarak nitelenen unsurların kritik altyapıları, özellikle de kritik enerji altyapıları ve buna bağlı enerji şebekeleri "doğal hedefler" olarak tanımlanmaktadır.[26] Nükleer enerji tesisleri de bu bağlamda "meşru" hedefler olarak görülebilirler; üstelik günümüzde düşman olarak nitelenebilecek aktör sayısında geçmişe kıyasla ciddi bir artış söz

konusudur. Özellikle de dijital dünyanın yarattığı ağa bağlılık, kötücül niyetlerin gerçekleştirilmesine imkân tanımaktadır.

Nükleer enerji santrali işletmecilerinin, enerji sektöründe yer alan diğer paydaşlara kıyasla siber saldırılara karşı daha az hazırlıklı oldukları genel olarak vurgulanan bir unsurdur. Ayrıca, güvenlik meseleleri söz konusu olduğunda, siber dünyanın yeni bir alan olduğu akılda tutulmalıdır. Bu, siber güvenlik alanındaki denetim ve yaptırımların ve yol gösterici konumda olması gereken devlet kurumlarının "bu alanın yenileri" oldukları anlamına gelmektedir. Dolayısıyla henüz bilgi ve tecrübe edinme ve biriktirme aşamasında olan sektörün, güvenlik konusunda kendi başının çaresine bakmak zorunda olduğu söylenebilir.

Nükleer enerji santrallerinin herhangi bir siber saldırı karşısında güvende olup olmadığı sorusuna ilişkin genel varsayım, bu sistemlerin analog olarak çalışan kapalı sistemler oldukları ve bu nedenle, büyük bir endişeye zemin olmadığıdır. Bu yaklaşımı benimseyen ABD Nükleer Düzenleme Kurulu (NRC) Backgrounder on Cyber Security başlıklı raporunda şu değerlendirmeyi yapmaktadır:

> "Nükleer enerji santrallerinin gözlem, işletim, kontrol ve korunmasında dijital ve analog sistemler kullanılmaktadır. Santralin emniyet, güvenlik ve acil durum yönetimiyle bağlantılı görevlerin yerine getirilmesinde kullanılan 'kritik dijital varlıklar' internete bağlı değillerdir. Bu ayrım, siber tehditlerden korunmayı sağlamaktadır. Buna ek olarak tüm enerji reaktörlerinin lisans sahipleri NRC'nin siber güvenlik kurallarına uygun bir siber güvenlik planını uygulamak durumundadırlar."[27]

Benzer biçimde, Amerikan nükleer enerji sektörünün siyasa belirleyici kurumu konumundaki Amerikan Nükleer Enerji Enstitüsü (NEI), siber güvenlik alanının NRC tarafından çok sıkı biçimde düzenlendiğini ve bu nedenle de ek bir düzenlemeye ihtiyaç bulunmadığını varsaymaktadır.[28]

Aslında ABD nükleer enerji sektörü yeni ortaya çıkan siber tehditlere karşı hazırlıklı olmak konusunda görece hızlı hareket etmiştir. Sektör, dijital unsurları ve sahip olunan bilgiyi, herhangi bir sabotaj ya da kötü amaçlı kullanım girişimine karşı korumak için, 2002 senesinde bir siber güvenlik programı başlatmıştır. NRC, nükleer enerji tesislerinin kontrolünü yapan kritik bilgisayar sistemlerinin "internette bağlı olmadıkları", "nükleer enerji santrallerinin, sistemin elektrik ağında herhangi bir sorun saptaması durumunda santrali otomatik olarak kapatmak üzere tasarlandığı" ve

"katman katman" güvenlik önlemleri ile korunduğunu ve bu nedenlerle güvenli olduklarını savunmuştur. NRC bunun da ötesinde, kendisini sektörün siber güvenliğini sağlayacak bütün girişimlerin koordinasyon makamı olarak görmektedir. Bu sebeple, 2009 yılında ticari reaktörler için uygulanması zorunlu siber güvenlik kuralları belirlemiştir. 11 Eylül saldırılarının yarattığı güvensizlik hissine rağmen NRC, nükleer sektörün güvende olduğunu hissetmektedir. NRC bunda, 2009'da yürürlüğe soktuğu ve işletmeci şirketleri siber güvenlik programı uygulamaya mecbur bırakan kuralların katkısı olduğunu düşünmektedir.

NEI 2014'te NRC'ye siber güvenlik düzenlemesini "radyolojik sabotajları önleyerek kamu sağlığını ve emniyetini güvence altına almak amacıyla" gözden geçirmesi yönünde bir öneride bulunmuştur. Bu öneri, nükleer enerji santrallerinin siber güvenliklerinin merkezi bir biçimde sağlanmasını ve NRC'nin bunu sağlayacak "tek düzenleyici" olmasını içermektedir.[29]

Fakat siber güvenliğin hızla değişen güvenlik ortamı ve gerekleri, bunun gerçekleşmesini imkânsız kılmıştır. Bunun ötesinde son dönemde, nükleer enerji santrallerinin işletmecileri artan biçimde, "süreç kontrol sistemlerinin işletimini sağlamak için açık protokolleri ve standart olarak satılan donanımları kullanmaya ve hatta bunları kimi zaman bütünüyle dikkatsizlikten kaynaklanır şekilde internete bağlamaya [başlamışlardır]."[30]

Bu gelişmenin ilk nedeni; ekipman üreticilerinin artık analog sistem üretimini bırakmış olmalarıdır. İkinci bir sebep ise, yeni yazılımlara dayalı teknolojilerin kullanılmaya başlamasıyla sağlanan süreç optimizasyonu etkisinin sonucunda, iş ağları ve Süreç Kontrol Sistemlerinin kendi aralarında, ve birbirleriyle, internet bağlantıları üzerinden daha fazla iletişim içinde olmalarıdır. Son sebep ise, nükleer enerji santrallerinin modernleşmesiyle, işletim ve güvenlikle ilgili unsurlarının büyük bir çoğunluğunun, bilgisayarla çalışan dijital sistemlere dönüşerek bilişim altyapısına bağımlı hale gelmesidir. Böylelikle, yeni teknolojilerin siber saldırı ihtimalini ve zaafiyetini arttıran biçimde sürece dâhil olması, nükleer güvenliği ciddi bir tehdit altına sokmuştur. Bu nedenle, kritik altyapının fiziki güvenlik önlemlerinin ötesine geçilerek korunması ihtiyacı ortaya çıkmıştır. Söz konusu ihtiyaca cevap vermek amacıyla, çeşitli yazılım temelli sistemler geliştirilerek kullanılmaya başlanmıştır.[31] Bu konuya özel hassasiyet gösteren kurumların başında Uluslararası Atom Enerjisi Kurumu (UAEK) gelmektedir.

4. UAEK'nin Nükleer Enerji Altyapı Güvenliği Yaklaşımı ve Siber Boyutu

UAEK, nükleer altyapı güvenliği ve bunun küresel ölçekteki standardizasyonu konularında faaliyet gösteren en önemli uluslararası kuruluştur. İsabetli biçimde UAEK "bilgisayar güvenliği" ortamını "hızla değişen ve evrimleşen bir senaryo" olarak tanımlamaktadır.[32] UAEK'nin nükleer güvenlikle ilgili GC(55)/RES/10 kararı, nükleer enerji santrallerinin siber güvenliği konusunda artan çekincelere örnektir. Kurum bu kararında "artan siber saldırı tehdidine karşı farkındalığı arttırma girişimlerine ve bunun nükleer güvenliğe olan potansiyel etkilerine"[33] vurgu yapmaktadır. UAEK bu çalışmasında fiziki koruma ve bilgisayar güvenliği önlemlerinin alınmasının, nükleer güvenliğin sağlanması açısından zorunlu olduğunun altını çizmektedir.

UAEK, bu yöndeki çalışmaları teşvik etmek amacıyla, uygulanmakta olan programlardan çıkarılan derslerin temel alındığı, siber güvenlik programlarında dikkate alınması gereken kuralları içeren, nükleer tesislerin siber (bilgisayar) güvenliğine adanmış bir belge yayınlamıştır.[34] Kurum, bu belgede bilişim sistemlerinin güvenliğini "gittikçe daha hayati hale gelen" şeklinde nitelemekte ve "kritik role sahip bilgisayar sistemleri, ağlar ve diğer dijital sistemlerin güvenliğini sağlamak amacıyla programların kurulması ve geliştirilmesini[n]"[35] altını önemle çizmektedir.

Bu belge incelendiğinde, UAEK'nın nükleer enerji santrallerinin siber güvenliğinin sağlanması amacıyla geliştirdiği yaklaşımın derinlemesine savunma (*Defense–in-depth*) olarak adlandırıldığı görülmektedir. Derinlemesine savunma, "esasen bilgisayar sistemini tehlikeye düşürecek saldırı yaşanmasını başarısız kılacak ya da engelleyecek, birbirinden bağımsız biçimde ve art arda çalışan bir seri koruma seviyesinin birleşimidir."[36] Buradaki anlayış, bu çok katmanlı düzey ve güvenlik önlemlerinin birbirleriyle uyum içinde çalışmasının sağlanması yönündedir.

UAEK için bir diğer öncelik verilmesi gereken kavram nükleer güvenlik kültürüdür. Kuruma göre nükleer güvenlik kültürü, "nükleer güvenliği destekleme ve arttırmakla görevli birey, kurum ve kuruluşların özellik, tutum ve davranışlarının bütününe verilen isimdir… Bu türde bir nükleer

güvenlik kültürünün temelinde, dikkate değer bir tehdidin varlığını ve nükleer güvenliğin önemli olduğunu kabul etmek yatmaktadır."[37] Bu yönde bir kültürün şekillendirilmesi ise, "nihayetinde karar alıcılara, düzenleyicilere, yöneticilere ya da çalışan bireylere ve belli bir düzeyde de kamuoyuna bağlıdır. Nükleer güvenlik kültürü kavramı (ve bunun tanıtılması ve geliştirilmesi) uluslararası bir yönlendirmenin sağlanması ile kamu ve özel sektörlerin tamamını kapsayacak bir biçimde ilgili tarafların tamamının farkındalığını artıracak bir bakış açısıyla belirginleşebilir."[38] Bu bağlamda, UAEK nükleer güvenlik ve emniyet anlayışına dayalı olarak kapsamlı bir nükleer güvenlik yönetimi oluşturulması çağrısı yapmakta ve bu türde bir yönetimin oluşturulmasını sağlayacak küresel standartları geliştirmeyi amaçlamaktadır. Kurumun değerlendirmesiyle, "nükleer güvenlik yönetimi; yasama ve düzenleme, istihbarat toplanması, radyoaktif maddeler ile ilintili tesis ve sahalara yönelik tehditlerin değerlendirilmesi, idari sistemler, çeşitli teknik donanım sistemleri, müdahale kapasitesi ve yatıştırma faaliyetleri gibi geniş kapsamlı unsur ve faaliyetleri içermektedir."[39]

Nükleer güvenlik ve siber güvenliğin iç içe geçtiği bu bağlamda, UAEK şu tespitte bulunmaktadır: "Sorumlu devlet kurumları; nükleer tesislerde kullanılan bilgisayar sistemlerinin güvenliğini ilgilendiren güncel saldırı vektörleri ile bilgisayar sistemleri ve bilginin güvenliğine yönelik tehditleri de içerecek biçimde, düzenli tehdit değerlendirmeleri yapmalıdırlar. ...Tesislerin, aktif ve sürekli güncellenen tehdit değerlendirmelerini yapmaya devam etmeleri ve bundan yöneticiler ile işletmecileri de haberdar etmeleri, hayati bir öneme haizdir."[40] Bu tavsiyenin yerine getirilebilmesi için, temel bir "nükleer güvenlik/emniyet kültürü" anlayışı ile eşgüdüm içinde çalışacak bir "bilgisayar güvenlik kültürünün" oluşturulması şarttır. UAEK, güçlü bir güvenlik planının geliştirilebilmesinin ön şartı olarak kapsamlı bir kültürün geliştirilmesi konusuna da böylelikle derinlik kazandırmaktadır.

Ne yazık ki, tehdit ve risklerin bu kadar aleni olduğu bu alanda, farklı paydaşların bu konuda çözüm geliştirmek için bir araya gelmesi çok eskilere dayanmamaktadır. UAEK, bu konuyu ele alan ilk kapsamlı toplantı olan Nükleer Dünyada Bilgisayar Güvenliği Uluslararası Konferansı'nı (*The International Conference on Computer Security in a Nuclear World*) ancak Haziran 2015'te düzenlemiştir.[41] Toplantının bu kadar geç bir tarihte yapılmış olması konunun görece yeni gündeme alındığına işaret etmektedir. Bunun ötesinde, UAEK gibi uluslararası

yapılanmalar, bu alanda herhangi bir yaptırım gücüne de sahip değildirler.

Konferansın düzenleyicisi konumundaki UAEK Başkanı Yukiya Amano konuşmasında, "aklına nükleer tesislere saldırı düzenlenmeyi koymuş suçlu ve teröristlerin yarattığı küresel tehdidin önüne geçmek amacıyla uluslararası düzeyde girişimlerde bulunulması" çağrısı yapmıştır.[42] Toplantı, nükleer enerji santrallerinin yasal düzenleyicileri ile işletmecilerinin temsilcileri, kolluk kuvvetleri, sistem ve güvenlik yüklenicilerinin yanı sıra "92 üye ülke ile 17 bölgesel ve uluslararası kurum ve kuruluştan 650 uzmanın"[43] katımıyla gerçekleşmiştir. Toplantıyı düzenleyen kurum ve kuruluşlar ile katılımcıların çeşitliliği, nükleer altyapının siber güvenliğine yönelik dünya çapındaki tehdit ve risklerin çok boyutlu ve çok uluslu doğasına açıkça işaret etmektedir. Kısacası, dijital sistemlerin ve bilgi ağlarının artan kullanımı ile bilgi teknolojilerine olan bağımlılığın gittikçe derinleşmesi, devletlerin ve toplumların siber saldırıları önemli bir mesele olarak algılamalarını sağlamıştır. Bu bağlamda üzerinde durulması gereken öncelik olarak karşımıza risk ve risk yönetimi kavramları çıkmaktadır.

5. Risk Yönetimi

Küresel olarak nükleer tesisleri hedef alan siber saldırıların yaygın bir olgu olduğu söylenemez. Bununla birlikte nükleer tesislere yönelik bu türden tehditlerin gerçekleşmeleri durumunda ortaya çıkacak riskler oldukça vahim ve toleransı güç cinstendir. Siber ortam bütüncül bir risk alanı oluşturmaktadır. Bu bakımdan "ağ" ortamlarının risk değerlendirmesinde dâhili ve harici ayrımı her zaman bir ölçüde belirsiz ve anlamsız kalmaya mahkûmdur. Buna ek olarak, nükleer bir tesisi hedef alan bir siber saldırı riski, kaynağı, yöntemi, faili bakımından siber ortamın herhangi bir alanına sınırlı veya münhasır, kabul edilemez. Siber risklerin bir bütün olarak görülmesine ve bertaraf edilmesine yönelik uluslararası hukuki düzenlemelerin hayata geçirilmesi ve koordinasyonu için harcanan çabalar bu manada da önemlidir.

Bu bağlamda siber güvenlik alanında bir uluslararası anlaşmanın yapılandırılması teklifi sıklıkla ortaya atılmaktadır. Bu güne kadar söz konusu yönde harcanan çabaların hayata geçirilmesi yönünde atılan adımların en başarılısı 2001 tarihli Avrupa Konseyi, Siber Suçlar Konvansiyonu'dur.[44] Konsey üyesi olmayan ülkeler tarafından da onaylanmış bulunan ve bu alanda uluslararası toplum tarafından benimsenmiş en yaygın metni oluşturan, Konvansiyon, "siber suçlar üzerine oluşturulmuş ulusal hukukların uyumlulaştırlmasını amaçlayan bir uluslararası anlaşmadır."[45] Bu belgenin yapılandırılma, imza ve uygulama aşamalarında da görüldüğü üzere, nükleer tesisleri ilgilendirsin veya ilgilendirmesin, siber risklere yönelik bu türden uluslararası düzenlemelerin karşılaştığı en önemli meydan okumalar, temelde, devletler arasındaki yetkinlik ve öncelik farklılıklarından kaynaklanmaktadır. Ancak, belki bundan daha da önemlisi, nelerin siber ortamda işlenmiş bir siber suç oluşturduğuna veya oluşturmadığına, yönelik tanımlar arasındaki uyuşmazlıklardır. Tüm bu meydan okumalar risk ve tehdidin doğasında içlek bilinmezliği arttıran ve uluslararası işbirliği ve düzenleme çabalarını sorunlu kılan, bir gri alan ortaya çıkarmaktadır. Bu durumun açık yansıması, söz konusu Konvansiyon gibi geniş bir katılımı sağlayan bir belgenin bile, örneğin Rusya tarafından imzalanmamış, ABD tarafından ise bu ülkenin iç hukukundan kaynaklanan nedenlerle çekincelerle imza altına alınmış olmasıdır.[46] Konvansiyon özelde nükleer tesislere bir atıfta bulunmamakla beraber, siber ortamın bütünsel yapısı nedeniyle, bu tesisleri ilgilendiren risklerin önlenmesine yönelik olarak gelecekte

yapılandırılabilecek ve yapılandırılması şart olan, kapsayıcı uluslararası çerçeveye potansiyel katkısı nedeniyle önemlidir.

Uluslararası alanda bir başka girişim ABD Başkanı Barack Obama'nın 2009'da Prag'da yaptığı konuşmayı izleyerek toplanan "Nükleer Güvenlik Zirveleri" idir.[47] İlki 2010 yılında Vaşington'da düzenlenen bu Zirveler başlangıçta temel olarak nükleer silahlar ve bunların yaygınlaşması ile ilgiliyken, önemli ölçüde Stuxnet saldırısının da etkisiyle, 2012'de Seul'de düzenlenen ikincisi nükleer tesisler bağlamında siber güvenliğe atıfta bulunmaktadır. Bu bağlamda Seul bildirgesi UAEK'in belgelerine ve yaklaşımlarına atıfta bulunmakta ve devletleri uluslararası işbirliğini geliştirmeye yönelik çaba harcamaya davet etmekle birlikte, pratikte "ulusal ve tesis düzeyinde önlemleri geliştirip güçlendirilmeye"[48] çağırmaktadır.

Anlaşıldığı üzere, uluslararası çabaların henüz başlangıç aşamasında olması nedeniyle, nükleer tesislere yönelik siber saldırı riskinin değerlendirme, yönetim ve önlenmesinde ülkelerin işletme yönetimi çerçevesinde ve tesislerin yapısına bağlı olarak, yapacakları risk ve tehdit analizlerinin etkinliği öne çıkmaktadır. UAEK bu çerçevede, "[Nükleer] tesislerin, faal ve sürekli tehdit değerlendirmesi yapmalarını" ve bunları düzenli olarak işletme ve yönetim seviyelerine raporlamalarını "hayati" nitelikte bulmaktadır.[49] Bu yapılırken aynı zamanda santral işletmecileri ve resmi kuruluşlar arasında sorumluluk sahalarına ilişkin iş bölümü ve koordinasyonun ortaya konması gerekmektedir. Aynı zamanda tüm bu çabaların kapsamlı bir ortak güvenlik kültürünün oluşturulması önceliği gözetilerek yapılandırılması gerekmektedir.

Bu çerçevede risk yönetimi, tasarım, geliştirme, işletim ve bakım da dâhil olmak üzere, sistemin yaşam döngüsünün her aşamasını ilgilendirir. "Bilgisayar güvenliği bağlamında risk, bir tehdidin, [bilgisayar ve enformasyon teknolojisi altyapısına dâhil] bir varlık (*asset)* ya da varlık kümesinin zafiyetlerini istismar etmesi ve bu şekilde kuruma zarar vermesi anlamına gelmektedir."[50] Bu çerçevede risk değerlendirmesi, "zafiyetlerin belirlenmesi ve bunların istismar edilmesi ihtimalinin saptanması için" gerekli olan kaynakların en etkin biçimde dağılımı ile faaliyetlerin belirlenmesinde yardımcı olur. Bir bütün olarak tehdit ve zafiyetlerin risk bağlamında değerlendirmesi, bilgisayar sistemlerine yönelik olarak düzenlenebilecek saldırıları engellemek ya da sonuçlarını hafifletmek için gereken karşı tedbirlerin alınması için gereken zemini sağlamaktadır.[51]

ABD, kritik altyapının siber güvenliğinin sağlanmasını ve risk yönetimini ele alan genel "Çerçeve"yi Şubat 2013'te oluşturmaya başlamıştır.[52] Türünün ilk örneği olarak kabul edilebilecek bu belge, ABD Başkanı'nın "Kritik Altyapının Siber Güvenliğinin İyileştirilmesi" (*Improving Critical Infrastructure Cybersecurity*) başlıklı Başkanlık Emrine uygun olarak hazırlanmıştır. Söz konusu Başkanlık Emri, "siber risklere yanıt vermek üzere siyasi, ticari ve teknolojik yaklaşımların tamamını kapsayan standart, yöntem, izlek ve süreçler dizgesi"[53] oluşturulması gereğine işaret etmektedir. Bu doğrultuda hazırlanan genel "Çerçeve" belgesi, bir seri standart ve esasları belirlemekle birlikte, risk yönetimini sağlayacak türde "tek tip bir yaklaşım" (*one-size-fits-all approach*) geliştirmemektedir. Tersine her bir yapının, "kendine has risk, farklı tehdit, zafiyet ve risk toleransı" olduğu uyarısı yapılmaktadır. Bu nedenle de ilgililere koordinasyon, bütünleşme ve bilgi paylaşımında bulunma çağrısı yapılmaktadır.[54]

Tıpkı ABD gibi UAEK de, risk yönetimine verdiği önemi şu noktalara dikkat çekerek belirtmiştir:

> "Gerekli destek ve kaynağa dayalı olarak geliştirilen bir bilgisayar güvenlik programı, takiben, bilinen saldırgan profilleri ve saldırı senaryolarına dayalı muhtemel tehditleri anlamaya odaklanmalıdır. Muhtemel ilk adım, bilinir saldırganların, bunların motivasyonlarının ve muhtemel hedeflerinin listelendiği bir saldırgan profil matrisinin hazırlanması olabilir. Bu saldırgan profil matrisi, akla yatkın saldırı senaryolarının yaratılmasında kullanılabilir ve izleyen alt bölümler de sürecin daha ayrıntılı bir biçimde çalışılmasına yardımcı olacaktır. …Tehdit seviyelerini ve buna bağlı olarak bir güvenlik duruşunu geliştirmede yaygın biçimde kullanılan en önemli araç, tasarıma esas tehdittir (*design basis threat-DBT*). Tasarıma esas tehdit, muhtemel hasımların (iç ve/veya dış) nitelik ve özelliklerine dair bir beyandır. DBT, güvenilir istihbari bilgiye dayalıdır fakat cari, gerçek bir tehdide dair bir beyan olmayı hedeflemez."[55]

Stuxnet örneğinin gayet açık bir biçimde gösterdiği gibi, niyetin belirsizliği ve saldırı düzenlemek için gereken imkân ve kabiliyetlerin kolaylığı dikkate alındığında, siber risklerle etkin bir biçimde mücadele edebilmek kolay değildir. Bunun için nükleer tesis işletmecilerinin "devlet destekli kaynaklardan sağlanan kullanılabilir istihbarata ve mali kaynağa ihtiyaç[ları] bulunmaktadır."[56] Bu, bakımdan UAEK ve NRC'nin

önerdiği türde bir siber emniyet ve güvenlik yapılanmasını sağlamak için en etkili yaklaşımı DBT'nin oluşturduğu söylenebilir. Esasen, nükleer altyapının fiziki ve kinetik saldırılara karşı emniyetini sağlamaya yönelik olarak yapılandırılan DBT, siber riskler karşısında etkin bir korumanın sağlanması için de uygun bir şablon sağlamaktadır. Zira olası iç ve/veya dış düşmanların karakteristik özelliklerine, önceliklerine, operasyon biçimlerine ve potansiyellerine odaklıdır. Böylece, güvenlik sisteminin dizaynına temel teşkil eder, performans ölçümüne ve sistemin etkinliğine ilişkin şablon ve kriterleri belirleyerek tedbirler ve ihtiyaçlar arasında bağ kurar. Aşırıya kaçılmasını önleyerek hem gereksiz maliyetlerin önüne geçme imkanı sunar hem de kurumların sorumluluk sınırlarını belirleyerek işleyişe açıklık getirir. Bu türde bir yaklaşım, bilişim sistemlerinin gelişen ve dönüşen gerekleri ve yapısı ile eldeki imkân ve kabiliyetleri de dikkate alarak, sürekli güncellenmelidir. Bu, "nükleer tesislerin faaliyetlerini destekleyen sistem ve ağlarının yapısı, standart bilgisayar sistemlerinin mimarisi, yapılandırması ya da işletim gerekleri ile uyumlu"[57] olmasa da geçerli bir yaklaşımdır.

6. Türkiye için Çıkarımlar

Türkiye'nin inşa etmeyi hedeflediği nükleer santraller, ülkenin enerji politikasında ve elektrik talebini karşılamada oynayacakları hayati rolün yanı sıra, nükleer teknolojiye sahip olmanın yaratacağı riskler ve bu risklerin dayatacağı gereksinimler nedeniyle de önemlidirler. Bu bağlamda Türkiye, nükleer enerjiye geçişin yarattığı bir takım özel tehditlerle karşı karşıyadır. Ülkenin yeni oluşmaya başlayan siber ve nükleer güvenlik anlayışını bir "kültüre" dönüştürebilmesi için; özellikle nükleer ve siber güvenlik gibi konulardaki farklı davranış kalıpları, anlayışları, öncelikleri ve yaklaşımlara sahip uluslararası ortakları olan, Rusya, Fransa ve Japonya ile işbirliği içinde hareket etmelidir. Taraflar arasında hâlihazırda var olan farklılıkların giderilmemesi durumunda, çok karmaşık sorunlarla karşılaşılacağı aşikârdır. Bu nedenle Türkiye, önceden çizdiği bir yol haritası çerçevesinde tarafların yaklaşımlarının koordinasyonu ve uyumlulaştırılması sürecinde etkin bir rol oynamalıdır.

Öte yandan Türkiye'nin durumu, nükleer hedeflerini gerçekleştirmek için seçtiği model nedeniyle daha da karmaşık bir haldedir. Nükleer santrallerinin iki tanesi, nükleer teknolojinin doğrudan ithali yoluyla inşa edilecektir (henüz üçüncü santral konusunda kesinleşmiş bir detay yoktur). Bunlardan ilki olan Akkuyu Nükleer Santrali, 'yap-sahip ol-işlet' (*build-own-operate*-BOO) finans modeline uygun olarak inşa edilecektir. Bu model, nükleer santralin inşası konusunda ülke içerisinde bir çoğunluğu tesisin fiziki emniyet ve güvenliğine odaklanmış olan temel bir takım eleştirilere yol açmıştır.[58] Zira tesisi inşa edecek Rus yüklenici şirket aynı zamanda tesisin ömrü boyunca sahibi olacaktır; bu da Türkiye'nin tesisin işletilmesi konusunda söz hakkını ciddi oranda kısıtlayacaktır.

Türkiye nükleer enerji üretme ihtimali olan bir UAEK üyesi olduğu için, kurumun genel yaklaşımını benimsemeli ve uygulamalıdır. İlk nükleer enerji santralinin 'yap-sahip ol-işlet' modeliyle yapılacak olması nedeniyle, ülkenin UAEK düzenlemelerine uyumu yalnızca tesisin işletim usulleri ve yasal düzenlemeler konularıyla sınırlı olmamalıdır. Türkiye bunun da ötesinde, ülkenin bütün nükleer paydaşlarının UAEK standart ve esaslarına bütünüyle uyumlu ve bağlı şekilde işlemesi için elinden geleni yapmalıdır

7. Sonuç

11 Eylül'de Dünya Ticaret Merkezi'ne düzenlenen saldırılar, ulusal kritik altyapıyı hedefleyecek saldırıların muhtemel etkileri konusundaki endişeleri gündeme getirmiştir. El-Kaide üyesi teröristlerin saldırı öncesinde siber iletişim araçlarını kullanarak dijital planlama yaptıkları bilgisi siber uzayın devletler ile asimetrik güçler arasında yeni bir mücadele alanı olacağı yönündeki genel kaygıları arttırmıştır.

Siber uzayda zaman ve alan fiziki dünyada olduğu gibi simetrik değillerdir. Bu durum aktörlere fiziki dünyanın çok ötesinde stratejik asimetriler yaratma imkânı sağlamaktadır. Simetrik bir dünyada yaşanan çatışmada, rakipler birbirlerini görür ve biri diğerinin belirli bir zaman ve alandaki hareketlerini izleyebilirler. Oysa bir siber saldırı söz konusu olduğunda kurban, saldırganın kimliği, yeri ve gerçek amacı konusunda kolay kolay kesin bir bilgiye sahip olamaz. Hackerlerin mesai algısı olmayabilir ve kurbanlarının mesai saatlerini de hiç önemsemezler. Kısacası siber tehditlerin asimetrik ve esnek doğası, çoğunlukla, simetrik olarak tasarlanmış olan devlet, kamu kurum ve kuruluşları ilişkilerini, bunların hâkim hiyerarşi ve kültürlerini, nükleer enerji santralleri ve kritik altyapı unsurları bağlamında, genellikle, birer dezavantaja dönüştürmektedir.

Günümüzün dijital dünyasında bağlantı ve ağların tamamını kontrol etmek ve korumak neredeyse beyhude bir girişim olarak görünmektedir. Bu konuda en gelişmiş düzenlemelere sahip ülkelerde dahi, nükleer enerji santrallerinin sahipleri ve işletmecileri özellikle raporlama ve kamuoyu ile bilgi paylaşımı konularında yetersiz yasal düzenlemelerle tanımlanan bir ortamda faaliyet göstermektedirler. Bu durum, en iyi uygulamalar olarak nitelenen, ilgili olay ve gelişmelerin bilgisinin toplanması, paylaşılması ve analizine dayalı biçimde endüstriyel standartların geliştirilmesi konusunu da karmaşık bir hale sokmaktadır.[59] İran'ın Natanz'daki tesislerine, İsrail ve ABD tarafından düzenlendiği iddia edilen saldırı,[60] devletlerin siber saldırılarla hasımlarına zarar vermek için kritik altyapıları hedef almasına kuvvetli bir örnek teşkil etmektedir. Bu gerçeklik, sektörün nükleer tesisleri koruması konusunu daha da karmaşıklaştırmış, mevcut riski daha belirgin kılmıştır.

Siber güvenlik alanı, hem kamu hem de özel sektörü ilgilendiren risk ve tehditlerin söz konusu olduğu, yeni ortaya çıkmış bir alandır. Siber güvenlik konusunda sadece 2012 yılında yaklaşık 15 milyar dolar

harcamış olan[61] ve bu konunun önemini en fazla benimsemiş ülke olarak kabul edebileceğimiz ABD'de bile devletle iş yapan yüklenicilerin, "ABD hükümetinin sivil hizmetlerini" sağlamaya imkân verecek bir tür temiz belgesini almalarını mümkün kılan Federal Risk ve Yetkilendirme Yönetimi Programı (*Federal Risk and Authorization Management Program-FedRAMP*), başlıklı bir sertifika programı ilk defa 2013'te uygulamaya sokulabilmiştir.[62] Açıkça söylemek gerekirse, deneyim, bilgi, model ve standartların küresel düzeyde bu derece sınırlı; soru ve sorunların cevaplardan daha fazla sayıda olduğu bir alanda, bilişim teknolojileri bağlamında ikincil bir çevre ülkesi olarak nitelenebilecek olan ve kritik altyapısı ile bilişim teknolojilerinin güvenliğini sağlayacak düzenleme, çerçeve ve kurumları geliştirmeye çalışan Türkiye bakımından ciddi zorluklar ortaya çıkması beklenilirdir. Öte yandan, Türkiye'nin nükleer altyapısı ve güvenlik yaklaşımı henüz 'çizim tahtası" aşamasından uygulama aşamasına geçmektedir. Uluslararası planda en iyi örnekleri ve tecrübeyi ön sıradan takip ederek kendi model ve düzenlemelerini oluşturacak bir Türkiye, nükleer güvenlik kültürünü yapılandırmak noktasında sahip olduğu konumu bir avantaja da çevirebilecektir. Bu bağlamda bürokrasinin bilgi paylaşmaya yönelik, şeffaf ve hesap verebilirlik odaklı bir yaklaşımı benimsemesi ve nükleer santral işletmecilerini de bu yönde davranmaya yöneltmesi hayati önemde görünmektedir.

1- Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Cilt 10, Sayı 1, Bahar 2011, s.18.

2- Bu tanıma, Birleşik Krallık hükümetince hazırlanmış olan iki belgede yer verilmektedir: UK Cabinet Office, Cyber Security Strategy of the United Kingdom, Safety, Security and Resilience in Cyber Space, Norwich, The Stationery Office, 2009, s.7 ve UK Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, London, UK Cabinet Office, 2011. Kaynak için bkz. Melissa E. Hathaway ve Alexander Klimburg, "Preliminary Considerations: On National Cyber Security", Alexander Klimburg (der.), National Cybersecurity: Framework Manual, Tallinn, NATO CCD COE Publications, 2012, fn.35, s.8.

3- A.g.e.

4- Joint Terminology for Cyberspace Operations, s.5.

5- "İster saldırı amaçlı olsun isterse savunma, bir siber operasyonun mantıken, bir kişinin yaralanmasına veya ölümüne ya da bir nesnenin zarar görmesine veya yok olmasına yol açması beklenir." Bkz. Michael N. Schmitt (Der.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambrige University Press, Cambridge, 2013, s.106.

6- P.W. Singer ve Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, s.36.

7- A.g.e. s.34 - 35.

8- Ed Gabrys, "The International Dimensions of Cyber-Crime, Part 1", Information Systems Security, Cilt 11, No.4, s.23.

9- A.g.e.

10- Thalif Deen, "World's Nuclear Facilities Vulnerable to Cyber-Attacks", 17 Ağustos, 2015, http://www.ipsnews.net/2015/08/worlds-nuclear-facilities-vulnerable-to-cyber-attacks/.

11- IAEA, Computer Security at Nuclear Facilities, s.37-8.

12- 2014 US State of Cyber Security Watch Survey, Software Engineering Institute, CERT, Carnegie Mellon University, 2014, s.8, resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_ 298322.pdf.

13- A.g.e., s.6.

14- A.g.e ., s.5-6.

15- Matthew Bunn ve Scott D. Sagan, A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes, Cambridge, MA, American Academy of Arts and Sciences, 2014.

16- A.g.e. ss 40-42

17- A.g.e.

18- Christine Hess Orthmann ve Karem Matison Hess, Criminal Investigation, Clifton Park, Delmar, 2013, s.535.

19- http://www.dhs.gov/what-critical-infrastructure.

20- AFAD, 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, Eylül 2014, Ankara, s.4.

21- Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", Military and Strategic Affairs, Cilt 3, No.2, Kasım 2011, s.62-63.

22- Cyber Security Programs for Nuclear Facilities, RG 5.71, US Nuclear Regulatory Commission, Washington DC, Ocak 2010, s.35.

23- A.g.e.

24- Martin Matishak, "Nation's Nuclear Power Plants Prepare for Cyber Attacks",

25- ICS-CERT Monitor, September 2014 – February 2015, Department of Homeland Security, Washington DC., s.1. APT, " Konusunda uzmanlaşmış koordine ekiplerce, kurumsal kabiliyet, istihbarat, sofistikasyon ve sabrın birleştirilerek uyumlulaştırılması yoluyla düzenlenen, özel hedefi ve belirli amaçları bulunan siber saldırı kampanyası." şeklinde tanımlanmaktadır. Bkz. P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, s.294.

26- James Andrew Lewis, The Electrical Grid as a Target for Cyber Attack, Center for Strategic and International Studies, Washington DC., Mart 2010, s. 1. 27 Ağustos 2010, http://www.nti.org/gsn/article/nations-nuclear-power-plants-prepare-for-cyber-attacks/.

27- Backgrounder on Cyber Security, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security- bg.html.

28- "Siber güvenlik NRC tarafından sıkı bir biçimde düzenlenmektedir dolayısıyla ilaveten başka yasal düzenlemelere ihtiyaç yoktur" Policy Brief, Mart 2014, ttp://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy- Briefs/Cyber-Security-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf

29- "Cyber Security for Nuclear Power Plants", Policy Brief, April 2015, http://www.nei.org/Master-Document- Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit.

30- Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Cilt 10, Sayı 1, 2011, s. 17.

31- André Lochthofen ve Dagmar Sommer, "Implementation of Computer Security at Nuclear Facilities in Germany" Nuclear Energy, Cilt. XXX, s.1-5.

32- IAEA, Computer Security at Nuclear Facilities, s.13.

33- IAEA, GC55/Res/10 Nuclear Security, Genel Konferans tarafından 23 Eylül 2011 tarihinde kabul edilmiştir, Paragraf 17, s. 3

34- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17,

Viyana, 2011.

35- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Viyana, 2011. s. 1

36- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Viyana, 2011. s.13.

37- IAEA, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No.7, Viyana, 2008, s. 19.

38- Age., s.2

39- Age., s.4.

40- IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series no.17, Viyana, 2011. s.13-14.

41- UAEK bu toplantıyı Uluslararası Polis Teşkilatı (INTERPOL), Uluslararası İletişim/Telekom Birliği (ITU), BM Bölgelerarası Suç ve Adalet Araştırma Enstitüsü (The UN Interregional Crime and Justice Research Institute - UNICRI) ve Uluslararası Elektroteknik Komisyonu (The International Electrotechnical Commission - IEC) gibi çeşitli uluslararası yapılanmalarla işbirliği içinde düzenlemiştir.

42- Jeffrey Donovan, "IAEA's Amano Calls for Strengthened Computer Security in a Nuclear World", 1 Haziran 2015, www.iaea.org/newscenter/news/iaea%E2%80%99s-amano-calls-strengthened-computer-security-nuclear- world.

43- A.g.e.

44- Bu belge Budapeşte Konvansiyonu olarak da bilinmektedir. 1 Ocak 2004 tarihinde yürürlüğe girmiştir. Konvansiyon metnine; www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_ budapest_/7_conv_budapest_en.pdf, adresinden çevrimiçi olarak ulaşılabilir Erişim Tarihi: 10 Eylül 2015. Söz konusu Konvansiyon Türkiye tarafından da imzalanmıştır ve 1 Ocak 2015'den bu yana yürürlüktedir.

45- Michael A. Vatis, "The Council of Europe Convention on Cybercrime", Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy Computer Science and Telecommunications Board Division on Engineering and Physical Sciences Policy and Global Affairs DivisionWashington D.C., The National Academies Press, 2010, içerisinde s. 207

46- Anlaşma hakkında bir tartışma için bkz. "Overall assessment: Nascent governance, growing gaps", e Monitor: The Internet, The Council on Foreign relations, Global Governance www.cfr.org/global-governance/global-governance-monitor/p18985?gclid=CjwKEAiApYGyBRCg_jIstuduV8SJABCEzhZYJFEw3x1y11- p_nTMWeBQJJgrY5PSZXF6LTS0sxo5BoCRcTw_wcB#!/internet?cid=ppc-Google-grantGGM _Internet_Gen-102115 Erişim Tarihi: 23 Ekim 2015

47- Bu Zirvelerin sonuncusu 2016 Mart sonunda yine Vaşhington'da yapılacaktır. "Statement by the Press Secretary on the 2016 Nuclear Security Summit", 10 Ağustos 2015,www.whitehouse.gov/the-press-office/2015/08/10/statement- press-secretary-2016-nuclear-security-summit, Erişim Tarihi: 25 Ekim 2015

48- "Seoul Communiqué", 2012 Seoul Nuclear Security Summit, 26 – 27 Mart 2012, Paragraf 12, s. 6. www.un.org/disarmament/content/spotlight/docs/Seoul_Communique.pdf, Erişim Tarihi: 25 Ekim 2015.

49- IAEA, Computer Security at Nuclear Facilities, s.13-14.

50- A.g.e., s.36.

51- A.g.e., s.36.

52- Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 National Institute of Standards and Technology, 12 Şubat 2014, www.nist.gov/cyberframework/upload/ cybersecurity-framework-021214-final.pdf. Erişim tarihi: 23 Ekim 2015

53- "Executive Order of the President of the United States 13636 - Improving Critical Infrastructure Cybersecurity", 12 Şubat 2013, www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Erişim tarihi: 23 Ekim 2015

54- Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 National Institute of Standards and Technology, 12 Şubat 2014, s.2 www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. Erişim tarihi: 23 Ekim 2015

55- IAEA, Computer Security at Nuclear Facilities, s.38-9.

56- Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Cilt 10, Sayı 1, 2011, s.22-23.

57- IAEA, "Design Basis Threat (DBT)", www-ns.iaea.org/security/dbt.asp?s=4 Erişim Tarihi: Ekim 30, 2015.

58- Sinan Ülgen (der.), Türkiye'de Nükleer Enerji ve Emniyeti, EDAM, İstanbul, 2015, http://edam.org.tr/document/NuclearBook3/edam_nukleeremniyet2015_tam.pdf

59- Bu konuda ayrıntılı bilgi için bkz. Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", Strategic Insights, Cilt 10, Sayı 1, 2011

60- Ellen Nakashima ve Jaby Warrick, "Stuxnet was the work of Us and Israeli Experts, Officials Say", Washington Post, Haziran 2, 2012.

61- P.W. Singer ve Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, s.200.

62- P.W. Singer ve Allan Friedman, Cybersecurity and Cyberwar: What everyone needs to know, Oxford, OUP, 2014, s.198.