TÜRKİYE'DE SİBER GÜVENLİK VE NÜKLEER ENERJİ

Ekonomi ve Dış Politika Araştırmalar Merkezi
edam
Ekonomi ve Dış Politika Araştırmalar Merkezi

Ekonomi ve Dış Politika Araştırmalar Merkezi

TÜRKİYE'DE SİBER GÜVENLİK VE NÜKLEER ENERJİ

Editör: Sinan Ülgen, EDAM

Yardımcı Editör: Grace Kim, EDAM

Araştırmacılar:

Doç. Dr. Salih Bıçakcı, Kadir Has Üniversitesi

Prof. Dr. Mitat Çelikpala, Kadir Has Üniversitesi

Doç. Dr. Ahmet Kasım Han, Kadir Has Üniversitesi, EDAM

Yrd. Doç. Dr. Can Kasapoğlu, EDAM

F. Doruk Ergun, EDAM

THE WILLIAM AND FLORA HEWLETT FOUNDATION

Bu araştırma "The William and Flora Hewlett Foundation"dan elde edilen bir hibe ile gerçekleştirilmiştir.

Bu raporda yer alan görüşler tamamen yazarlara aittir ve The William and Flora Hewlett Foundation'ın görüşlerini temsil etmemektedirler.

Hare Sokak No: 16,
Akatlar 34335 Istanbul

Tel: +90 212 352 18 54

Email: info@edam.org.tr

www.edam.org.tr

1. Baskı, İstanbul, Mart 2016

ISBN: 978-9944-0133-8-3

Kapak Tasarımı: Güngör Genç

Baskı: İmak Ofset Basım Yayın Tic. ve San. Ltd. Şti.
Merkez Mh. Atatürk Cad. Göl Sk. No:1 34197 Yenibosna / İstanbul
Tel: 0212 444 62 18 Faks: 0212 656 29 26

TÜRKİYE'DE SİBER GÜVENLİK VE NÜKLEER ENERJİ

edam
Ekonomi ve Dış Politika Araştırmalar Merkezi

EDAM Hakkında

Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM) İstanbul merkezli bağımsız bir düşünce kuruluşudur. EDAM'ın ana çalışma alanları:

- Dış siyaset ve güvenlik,
- Türkiye-AB ilişkileri,
- Enerji ve iklim değişikliği,
- Ekonomi ve küreselleşme,
- Silahların kontrolü ve silahların yayılmasının önlenmesi,
- Siber politikalar programını kapsamaktadır.

EDAM, Türkiye'nin yeni dünya düzeni içinde alacağı yeri belirleyecek politika alanlarına dair görüş oluşturmak suretiyle Türkiye içinde ve dışında karar alma süreçlerine katkıda bulunmayı amaçlamaktadır. EDAM bu çerçevede araştırmalar yapmasının yanı sıra düzenli yuvarlak masa toplantıları ve konferanslar düzenlemektedir. EDAM aynı zamanda çeşitli kuruluşlar ile ortak araştırma ve yayın konularında işbirliği yapmaktadır.

Kurumsal Yapı

EDAM, akademi, sivil toplum, iş dünyası ve medya gibi Türk toplumunun farklı sektörlerinden oluşan bir üye ağını bir araya getirmektedir. Çeşitlilik arz eden bu yapı, farklı öngörü ve bakış açılarının karşılıklı etkileşimine açık, etkin bir platform oluşturmada EDAM'a önemli bir katkı sağlamaktadır.

EDAM'ın Yönetim ve Denetim Kurulu akademi, iş dünyası, sivil toplum ve medya mensuplarından oluşmaktadır. Kurul üyeleri, araştırma projelerinin akademik ve edebi kalitesini temin etmek için, projeleri denetleme görevini üstlenirler. EDAM sürekli bünyesinde çalışan ufak sayıda profesyonel bir ekip istihdam etmekle birlikte, yürüttüğü projelerde proje bazlı araştırma ekipleri kurmak amacıyla seçkin Türk ve uluslararası araştırmacılara da erişmektedir.

EDAM projelerini gerçekleştirmek amacıyla proje bazlı fonlar, kurumsal bağışlar ve ilgili ödeneklere dayanmaktadır ve böylelikle edebi bağımsızlığını korumaktadır. Buna ek olarak, EDAM birçok farklı sivil toplum örgütü ve uluslararası kuruluşlar ile ortak finansman prensibi temelinde ortak proje ve araştırmalar yapmaktadır.

Yazarlar Hakkında

Doç. Dr. Ahmet K. Han Kadir Has Üniversitesi Uluslararası İlişkiler fakültesinde öğretim üyeliği yapmaktadır. Araştırma konuları stratejik düşünce, müzakere ve dış siyaset analizidir. İstanbul Üniversitesi'nde lisans eğitimini Ekonomi ve Uluslararası İlişkiler alanında, yüksek lisansını Politik Tarih ve doktorasını Uluslararası İlişkiler konularında almıştır. Harvard'da Müzakere eğitimi görmüştür. ABD Dışişleri Bakanlığı'ndan ABD Dış Politikası konusunda "Avrupa'nın Genç Liderleri" bursunu alış ve Afganistan'daki NATO/ISAF Operasyonunda 2005 ve 2011'de NATO gözlemciliği yapmıştır. Afganistan, jeostrateji ve enerji politikası, ABD dış siyaseti ve Türkiye dış siyaseti üzerine yayınları vardır. Radikal ve Referans gazetelerinde köşe yazarları yapmıştır.

Doç. Dr. Salih Bıçakcı Kadir Has Üniversitesi Uluslararası İlişkiler Bölümünde öğretim üyesi olarak çalışmaktadır. Lisans eğitimini 1994'te Marmara Üniversitesi Eğitim Fakültesi Tarih bölümünde tamamladıktan sonra Türkiye'ye Göç eden Özbekler üzerine yazdığı yüksek lisans teziyle Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü'ndeki araştırma görevlisi olarak görev yaptı ve yüksek lisans programını 1996'da tamamladı. 1999'da Norveç'teki Bergen Üniversitesi'ndeki Sosyal Bilimler Bilgisayar (Humanities Computing) programını tamamladı. 2004'te İsrail'deki Tel Aviv Üniversitesi'ndeki doktora çalışmalarını tamamladı. Işık Üniversitesi'nde akademik hayatına başlayan Dr. Bıçakcı kimlik, güvenlik ve terörizm konusunda birçok akademik projede yer aldı. Uluslararası ve ulusal üniversitelerde Uluslararası Siyasette Orta Doğu, Uluslararası Güvenlik, Uluslararası İlişkiler Teorisi, Türk Dış Politikası dersleri verdi. Siber güvenlik konusunda NATO Terörle Mücadele Mükemmeliyet Merkezi'nde (COEDAT), NATO Komuta ve Kontrol Mükemmeliyet Merkezi'nde (C2COE) ve NATO Deniz Güvenliği Mükemmeliyet Merkezi'nde (MARSEC COE) sunumlar ve değerlendirmeler yapmıştır. Harp Akademileri'ne bağlı Silahlı Kuvvetler Akademisinde Siber güvenlik ve Orta Doğu Güvenliği konularında dersler vermiştir. Uluslararası güvenlik, siber güvenlik sahasında uluslararası akademik konferanslarda sunumlar yaptı. Aynı konularda farklı akademik dergilerde makaleler yayınladı.

Prof. Dr. Mitat Çelikpala Kadir Has Üniversitesi Uluslararası İlişkiler bölümü profesörüdür ve Avrasya güvenliği, enerji, kritik altyapı güvenliği, Türkiye dış siyaseti ve Kafkasya siyaseti, güvenliği ve tarihi üzerine lisans ve yüksek lisans dersleri vermekte ve bu alanlarda doktora bitirme tezlerine danışmanlık yapmaktadır. Uzmanlık alanları Kafkaslar, Kuzey Kafkasya Diyasporası, Kafkaslar ve Karadeniz bölgelerinde halk ve güvenlik, Türkiye-Rusya ilişkileri, enerji güvenliği ve kritik altyapı korumasıdır. Kadir Has Üniversitesi'nin yanı sıra Bilgi Üniversitesi, Harp Akademisi, Türkiye Ulusal Güvenlik ve askeri akademilerinde Türkiye dış siyaseti, Kafkaslar ve Orta Asya siyaseti, tarihi ve güvenliği ve Türkiye siyasi yapısı ve yaşamı üzerine dersler vermiştir. Ankara'daki NATO Terörizmle Mücadele Mükemmeliyet Merkezi'nde özellikle kritik altyapı güvenliği alanında akademik danışmanlık yapmıştır. Yukarıda bahsedilen alanlarda akademik makaleler ve analizler yayınlamış ve medyada yer almıştır.

Yrd. Doç. Dr. Can Kasapoğlu Harp Calışmaları ve Güvenlik Bilimleri alanlarında akademik faaliyetlerini sürdürmektedir. Dr. Kasapoğlu doktora derecesini 2011 yılında Harp Akademileri Stratejik Araştırmalar Enstitüsü'nden Düşük Yoğunluklu Çatışmalarda Konvansiyonel Kuvvetlerin kullanılmasını incelediği tezi ile yüksek lisans derecesini ise 2008 yılında Kara Harp Okulu Savunma Bilimleri Enstitüsü'nden 1974 öncesi Kıbrıs Türk gayrinizami harp faaliyetlerini incelediği teziyle almıştır. Yrd. Doç. Dr. Can Kasapoğlu, İsrail'in önde gelen düşünce kuruluşlarından BESA Center'da Türk-İsrail ilişkileri ve Orta Doğu'da stratejik konular ile Fransız düşünce kuruluşu FRS bünyesinde Orta Doğu'da stratejik silah sistemlerinin yayılması ve Türkiye'nin uzun menzilli hava ve füze savunma projesi uzerine bilimsel çalışmalarda bulunmuştur. Dr. Kasapoğlu'nun çalışma konuları arasında, kimyasal & biyolojik harp ve füze & füze savunma sistemleri başta olmak üzere stratejik silah sistemleri, melez savaşlar, NATO'nun kolektif savunma ve işbirliğine dayalı güvenlik konuları, Türk-İsrail ilişkileri, küresel ve bölgesel askeri modernizasyon trendleri, jeopolitik ve açık-kaynaklı stratejik istihbarat analizi bulunmaktadır. Yrd. Doç. Dr. Can Kasapoğlu NATO Savunma Koleji, Baltık Savunma Koleji, International Society of Military Sciences gibi askeri bilimler alanında önemli platformlarda konusmacı olarak bulunmus: Girne Amerikan Üniversitesi'nde Harp ve Strateji Teorisi, Küresel Barış ve Güvenlik, Sivil-Asker İlişkileri, Güncel Terörizm Çalısmaları ve Jeopolitik gibi dersler vermiştir. Dr. Kasapoğlu'nun makaleleri sıkça İsrail'in önde gelen yayın organı the Jerusalem Post tarafından yayımlanmaktadır. Hâlihazırda NATO Savunma Koleji'nde misafir akademisyen olarak görev yapmaktadır.

F. Doruk Ergun EDAM'da Türkiye dış politikası ve güvenliği konuları üzerine araştırma görevlisi olarak çalışmaktadır. Doruk Ergun 2012'de EDAM'da çalışmaya başlamadan önce NATO Parlamenter Asamblesi'nin Brüksel'deki uluslararası sekreteryasında araştırma görevlisi olarak çalışmıştır. 2009 senesinde Sabancı Üniversitesi'nin Toplumsal ve Siyasal Bilimler bölümünde lisans derecesini, 2011 senesinde ise George Washington Üniversitesi'nin Uluslararası İlişkiler bölümü altındaki Uluslararası Güvenlik Çalışmaları üzerine yüksek lisans derecesini tamamlamıştır.

İçindekiler

Giriş

EDAM'ın bu çalışması siber güvenlik alanında artan tehditleri, kritik altyapı ve nükleer güç santrallerine odaklanmak suretiyle incelemektir. Bu derlemede, okuyucunun, Türkiye'nin siber güvenlik alanında karşılaştığı güçlükleri anlamasını kolaylaştırmak için yazılmış dört adet birbirini tamamlayan bölüm bulunmaktadır.

Can Kasapoğlu tarafından kaleme alınan birinci bölüm, siber savaş kavramına Askeri Meselelerde Devrim (AMD) olarak nitelendirmek suretiyle bir giriş yapmaktadır. Bölümde mevcut ve olası düşmanların siber alanında gelişen devlet kabiliyetleri belirlenmektedir. Bölüm siber uzayı harbin beşinci alanı olarak analiz etmekte ve ağ-merkezli savaşa odaklanmaktadır. Aynı zamanda Türkiye'nin bakış açısından devlet-dışı tehditler incelenmektedir.

Salih Bıçakcı, Doruk Ergun ve Mitat Çelikpala tarafından yazılan ikinci bölüm Türkiye'de siber güvenliğe odaklanmaktadır. Hâlihazırda siber uzayda faal olan yerel aktörler araştırılmaktadır. Bu aktörlerin arasında Redhack ve Ayyıldız Tim gibi hacker grupları ve Türkiye'nin siber güvenlikten sorumlu olarak atadığı Milli İstihbarat Teşkilatı ve Türk Silahlı Kuvvetleri gibi kurumlarının siber birimleri vardır.

Üçüncü bölümde Ahmet Han ve Mitat Çelikpala siber uzay, siber saldırganlar, siber güvenlik ve bunların kritik altyapılar ve nükleer güç santralleri ile ilişkisini ele almaktadır. Yazıda daha sonra nükleer güç tesislerinin siber güvenliği değerlendirilmekte ve alandaki en gelişmiş kurumsal ve yasal yapıya sahip ülkelerden olan Amerika Birleşik Devletleri ile nükleer güvenlik ve emniyet alanındaki kilit uluslararası kurum olan Uluslararası Atom Enerjisi Kurumu incelenmektedir. Bölüm Türkiye için sonuçlar ve tavsiyeler çıkartarak sonlanmaktadır.

Salih Bıçakcı'nın kaleme aldığı dördüncü ve son bölüm siber güvenlik kavramını ve nükleer güç santralleri ve tesisleri özelindeki yerini netleştirmektedir. Nükleer güç santrallerini etkileyen siber vakalar ve bu altyapıların korunması için uluslararası seviyede alınan çabalar incelenmektedir. Nükleer güç tesislerinin çoğu endüstriyel kontrol ve

veri tabanlı kontrol ve gözetleme (SCADA) sistemleri ile çalıştıklarından, işgücünün SCADA ve bilgisayarlar ile etkileşimi nükleer güç tesislerinin emniyeti ve güvenliği açısından hayati öneme sahiptir. Nükleer güç santrallerinin güvenliğini sağlamanın zorluğu incelendikten sonra, bu bakış açısından Türkiye'nin siber savunma kabiliyetleri değerlendirilmektedir. Ülkenin mevcut kabiliyetlerinin, siber güvenlik dayanıklılığını sağlamak noktasında ne durumda olduğu incelenmektedir. Bölüm, Ankara'nın mevcut siber politikalarını siber güvenlikten ve savunmadan sorumlu kurumları inceleyerek özetlemektedir.

Özgün araştırmalardan oluşan bu derlemenin, bir yandan Türkiye'de henüz şekillenmeye başlanan siber güvenlik, kritik altyapı ve nükleer enerji konularındaki tartışmaya katkıda bulunacağı diğer yandan politika yapıcıların ve kamuoyunun bundan böyle daha fazla gündeminde olacağı düşünülen konulara faydalı bir giriş sağlayacağı ümit edilmektedir.

TÜRKİYE'NİN GELECEKTEKİ SİBER SAVUNMA ORTAMI

Yrd.Doç.Dr. Can Kasapoğlu

Araştırma Görevlisi – EDAM

1. Giriş

Türkiye'nin internet kullanımı sosyal medya, özel sektörün artan gereksinimleri ve devlet ağının nitelikleri dolayısıyla hızla yükselen bir profildedir. Giderek artan söz konusu 'bağlantılılık' durumu *(interconnectedness),* Türkiye'nin kritik milli altyapısının siber ağlara olan bağımlılığı ve siber saldırılar, Türk milli güvenlik ajandasına siber güvenliğin karmaşık gerçekliklerinin girmesine neden olmuştur. Bu bağlamda Ankara, 20 Ekim 2012 itibariyle Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar ile siber güvenlik koordinasyona ilişkin ilk milli hukuki düzenlemesini hazırlamıştır[1]. Ayrıca, Siber Güvenlik Ulusal Eylem Planı da 2013 yılında yürürlüğe girmiştir. Ulusal Eylem Planı siber saldırıların tespit edilmesindeki zorlukların altını çizmiş, hassas bilgilerin ve kritik milli altyapının korunmasına özel bir önem atfetmiştir[2]. Aynı zamanda, Ankara Türk Silahlı Kuvvetleri bünyesinde bir Siber Komutanlık kurmuş ve Türk Hükümeti 2011 yılında ülkenin kurumlar-arası ilk siber tatbikatını icra etmiştir[3].

Yukarıda aktarılan tüm çabalara karşın, siber tehditler Türkiye'nin siber güvenlik önlemlerini aşan bir süratte artmaktadır. Bir NATO üyesi olarak Ankara kendi milli güvenliği bağlamında siber güvenliğini sağlamak zorunda olduğu kadar, ittifakın da siber savunmasına katkıda bulunmak durumundadır. Bu doğrultuda Türkiye'nin ve NATO müttefiklerinin siber harbe ilişkin, taarruz ve müdafaa boyutlarını kapsayacak bir çerçevede, isabetli ve net bir anlayışa sahip olmaları büyük önem arz etmektedir.

Bu noktada, siber harbe ilişkin salt siyasa düzeyinde çözümler üretmeye yönelik bir çalışmanın dahi askeri ve güvenlik alanlarında kavramsallaştırmalara gereksinim duyacağı belirtilmedir. Çünkü öncelikle Batı dünyasının gelişmiş siber güvenlik doktrinleri ve konseptleri ile kıyaslandığında, Türkiye'nin önünde siber tehditlerle mücadelede ve bu bağlamda tehdit algılamasının mükemmelleştirilmesinde gidilecek uzun bir yol olduğu görülmektedir. İkinci olarak, siber harp tartışmalarının ilginç bir şekilde hava gücü *(Air Power)* askeri teorik tartışmaları ile benzeştiği, daha açık bir anlatımla askeri pratiğin teoriyi takip ettiğine ilişkin ciddi emareler bulunduğu gözlemlenmektedir. Bu tartışma çerçevesinde, Washington merkezli düşünce kuruluşu the Center for Strategic and International Studies (CSIS) tarafından hazırlanan bir rapor,

siber terörizm ile 2. Dünya Savaşı dönemi hava gücü teorisi ve pratiği arasındaki mukayeseli analizi şu şekilde açıklamaktadır:

> "Siber terörizm yeni bir teknolojinin stratejik zafiyet yaratmak amacıyla kullanıldığı ilk vaka değildir. Siber harp ve hava gücü teorileri arasında bir eşleşme olduğunu öne sürmek tam anlamıyla isabetli olmasa da, ikisi arasında bir mukayesede yarar görülmektedir. Birinci Dünya Savaşı'na bir tepki olarak Douhet ve Trenchard gibi Avrupalı stratejistler, düşman ileri hatlarının çok gerisine, kritik altyapıya yönelik hava taarruzlarının düşmanın savaşma gücünü akamete uğratacağını savunmuşlardır. Söz konusu teoriler 2. Dünya Savaşı sırasında ABD Silahlı Kuvvetleri ve Britanya Kraliyet Hava Kuvvetleri tarafından denenmiş; bu kapsamda stratejik bombardıman taarruzları elektrik hatları, ulaşım altyapısı ve üretim tesislerini hedef almıştır. İşte siber saldırılara ilişkin literatürün ilk safhaları birçok yönüyle stratejik bombardıman konseptine dair askeri teorik tartışmaları andırmaktadır ve hatta varlığını bu tartışmalara borçludur".[4]

Türkiye'nin muhtemel siber saldırılar karşısındaki zafiyetine ilişkin doğru bir anlayış geliştirmek için, öncelikle gelişen teknolojik trendlerin ve bahse konu trendlere bağlı olarak ortaya çıkan tehdit algılamalarının incelenmesi ve sayılan faktörlerin harbin geleceğini nasıl şekillendirdiğinin kavramsal olarak açıklanması gerekmektedir. Müteakip alt başlık kapsamında analiz edildiği üzere, siber yeteneklerin askeri meselelerde devrim *(Revolution in Military Affairs – RMA)* kapsamında nasıl değerlendirilebileceğine ışık tutulacaktır. Bu çalışma daha sonra mevcut ve potansiyel siber trendler ve tehditler ile bahse konu sahada Türkiye'nin ve NATO'nun göz önünde bulundurması gereken devletlerdeki imkan ve kabiliyetleri inceleyecektir. Daha sonra siber harbin, gelecekte savaşın 'beşinci boyutu' olarak nasıl ele alınabileceği 'ağ merkezli harp' çerçevesinde değerlendirilmektedir. Dördüncü alt başlık kapsamında ise siber güvenlik çerçevesinde devlet-dışı aktörler analiz edilmekte ve Türkiye için genel tehdit değerlendirmesi yapılmaktadır. Son olarak, bu çalışmanın bulguları ve önerileri aktarılmaktadır.

2."Siber-Yıldırım Harbinin" Kavramsallaştırılması: Yeni Askeri Meselelerde Devrim (AMD) Olarak Siber Harp

AMD kavramının kökleri esas olarak Sovyet Genelkurmay Başkanı Mareşal Ogarkov'un ortaya attığı "askeri teknolojik devrim" kavramına dayanmakla birlikte, konseptin evrimi teknolojik gelişmelerin ötesine geçmiştir. AMD, özü itibariyle, muharip yeteneklerde teknoloji, stratejik kültür, teşkilat yapısı, doktrin, eğitim, strateji ve taktik sahalarındaki kırılma düzeyinde ilerlemelere bağlı olarak gelişen büyük ve radikal artış olarak tanımlanabilir. Bu çerçevede, teknolojinin yenilikçi konseptler ve teşkilat adaptasyonu ile birlikte askeri sistemlere uygulanmasını içermektedir[5]. Andrew Krepinevich'in AMD kavramını incelediği "Süvariden Bilgisayara" *(From Cavalry to Computer)* adlı önemli eserinde dikkat çektiği gibi, gelişmiş simülasyonlarda kullanılan bilgisayar-destekli dizaynlar ve etkileri askeri teşkilatların yeteneklerini büyük ölçüde geliştirmektedir[6].

Yukarıda aktarılan çerçeve de göz önünde bulundurulduğunda, siber harbin bir sonraki –ya da hâlihazırdaki– Askeri Meselelerde Devrim olarak ele alınması gerektiği söylenebilir. Bu bağlamda, gelişmiş savaş komuta kontrol ağlarının, muhtemel hedeflerin tespiti, tanımlanması ve izlenmesi amacıyla yönetiminin yanı sıra; istihbarat-gözetleme-keşif sistemlerinin işletilmesi de küresel ortak varlıkların yörüngesel ve siber boyutlarına erişimi gerekli kılmaktadır. Dolayısıyla 'siber silahlanma yarışı' ağ-saldırıları, anti-uydu sistemleri ve yönlendirilmiş enerji silah sistemleri bağlamında ön plana çıkmaya başlamıştır. Esasen, uzay ve siber uzaydaki rekabetin, ki söz konusu alanlar akıllı mühimmatlar açısından da büyük önem taşımaktadır, harp sahasının yönetimi, komuta-kontrol, hedef tespiti gibi konular bakımından gerçek zamanlı bilgi akışı ve mekan ile ilintisi dolayısıyla doğrudan ve kritik etkileri olduğu görülmektedir[7].

Siber harp ile ilintili ancak yalnızca siber harbe indirgenemeyecek olan siber-espiyonaj da siber-teknolojilerdeki gelişmelerin güvenlik araçlarına dönüştürüldüğü, ön plana çıkan alanlardan biridir. Siber-teknolojik ilerlemeler casusluğu, ülke dışına çıkmadan yapılabilen bir etkinlik haline getirdiği gibi, buna bağlı olarak devletleri de kontr-siber espiyonaj faaliyeti

icra etmeye zorlamaktadır. Ayrıca, "kar amacı gütmeyen" siber espiyonaj sektörü halihazırda hassas bilgilerin kamuoyu ile paylaşıldığı bir alan haline gelmektedir[8].

Gelecek harp senaryolarının değerlendirilmesi ve stratejik öngörü geliştirilmesi bağlamında, siber fonksiyonlara ilişkin katı ayırımlar yapılmamasında yarar görülmektedir. Daha açık bir ifadeyle aktarmak gerekir ise, siber harp, sivil-asker ayrımını giderek bulanıklaştırmaktadır. On yıllar süren inovasyon ve deneylerin sonucu olarak siber silahlar ve robot teknolojisinin yeni AMD'nin temel taşlarını oluşturacağı görülmektedir. Tüm bu sayılanlar teknoloji-yoğun varlıklardır ve belirtildiği gibi on yıllarca süren çalışmaların ürünüdürler[9].

Siber harbe ilişkin tarihsel ve siyasa-amaçlı bir çerçeve oluşturmak amacıyla, özellikle enformasyon üstünlüğünün harp sahasındaki kilit rolünün açıklanabilmesi bağlamında, harp tarihinin kullanılması önem arz etmektedir.

Kuşkusuz, yeni muharebeleri icra etmek için kullanılacak yeni imkân ve kabiliyetler kritik üstünlükler kadar kritik zafiyetleri beraberinde getirmiştir. Örneğin, Hannibal'ın savaş filleri harp meydanındaki en ağır ve çetin birlikleri teşkil etmişlerdir. Öte yandan, Zama Muharebesi sırasında Scipio Africanus'un ciritli birlikleri olan *velite* formasyonları kısa mesafeden fillerin görme yeteneklerini hedef alarak, onları takip eden düşman unsurları için bir koruma kalkanı yerine tehdide dönüştürmüştür[10]. Benzer durumu modern orduların enformasyon ve bilgisayar ağlarında da görmek mümkündür. Daha açık bir ifadeyle, modern ordular bilgisayar ağları ve gelişmiş ağ altyapıları ile önemli avantajlar kazansalar da, bahse konu avantajlar potansiyel düşmanlar için aynı zamanda yararlanılacak 'yeni taarruz alanları' açmıştır[11]. Türk Silahlı Kuvvetleri ve NATO bu duruma istisna değildir.

Askeri perspektiften bakıldığında, siber savaşın harp meydanı üzerinde enformasyon üstünlüğü ve kontrole dayandığını söylemek mümkündür. Bu bağlamda, John Arquilla ve David Ronfeldt, 13. yüzyıl Moğol ordularını siber savaşı kavramsallaştırmak için kullanmışlardır. Yazarlara göre, Moğol orduları birçok kez sayısal olarak dezavantajlı olsa da, steplerden gelen komutanlar Moğolistan'ın hafif ve süratli süvarileri sayesinde harp meydanında sistematik enformasyon ve sevk – idare üstünlüğünü kurmaları için sistematik olarak başarıyla kullanmışlardır[12].

Moğol ordularının enformasyon üstünlüğünü harp meydanında muharip başarıya çevirmelerine benzer şekilde, Arquilla ve Ronfeldt, siber savaşı "enformasyona bağlı prensipler ile askeri operasyonları icra etmek ve icra etmeye hazırlanmak" şeklinde tanımlamışlardır. Bu çerçevede, siber harp enformasyon ve muhabere sistemlerinin; düşmanın kendisine ilişkin farkındalığını da oluşturan ve askeri kültürü de içeren "kim olduğuna, nerede olduğuna, ne zaman neler yapabileceğine ve niçin savaştığına ve tehdit sıralamasına" ilişkin verilerin de akamete uğratılmasını içermektedir[13].

Yukarıda atıf verilen Arquilla ve Ronfeldt'in eserini takiben daha kapsamlı birçok analiz ortaya koyulmuş olsa da, söz konusu yazarların çalışmalarının başında Carl von Clausewitz'e atıfla belirttikleri alıntı siber savaşın, harbin geleceğine ilişkin dönüştürücü etkilerini açıklamaktadır: "bilgi, yeteneğe dönüşmelidir"[14]. Bu bağlamda yazarlar, harp meydanına ilişkin en iyi bilgiye sahip olunmasının en az harp meydanına daha fazla insan gücü, teknoloji ve sermaye aktarılması kadar önemli olduğunun altını çizmektedirler[15].

2.1. Yeni AMD'nin Somutlaştırılması ve Görünürlüğü

Siber harp yalnızca teknolojik atılımları değil, aynı zamanda teşkilat, doktrin, konsept ve askeri düşünce alanlarında bir dizi etkin gelişimi de gerektirmektedir. ABD siber savunma harcamaları, Başkan Obama dönemi 2014 bütçesindeki 800 milyon dolar artış ile tarihi bir çıkış göstermiş ve 4,7 milyar dolara ulaşmıştır[16]. Mukayeseli bir örnek vermek gerekirse, ABD'nin 2014 siber savunma bütçesi, Danimarka, Finlandiya ya da Ürdün'ün 2013 yılında tek başlarına savunma bütçelerinden fazladır[17].

Sözü edilen bütçe hareketleri ABD Silahlı Kuvvetleri teşkilat yapısındaki değişiklikleri de beraberinde getirmiştir. 2009 yılında dönemin Savunma Bakanı Robert Gates ABD Stratejik Komutanlığına Siber Komutanlık (USCYBERCOM) kurulması direktifini vermiştir. Söz konusu komutanlık ilk somut operasyonel imkân ve kabiliyetlere 21 Mayıs 2010 itibariyle kavuşmuştur[18]. Yeni Siber Komutanlığın görev tanımı Savunma Bakanlığı'nın özel enformasyon ağının korunması ve operasyonlarının yönetilmesi, planlanması, koordine edilmesi, entegrasyon ve senkronizasyonu ile emir verildiğinde siber-uzayda operasyonların tüm alanlarda icra edilmesi ve ABD ve müttefiklerinin siber-uzayda

hareket serbestisinin sağlanması, olası düşmanların da benzer bir hareket kabiliyetinden mahrum bırakılmasıdır[19].

Benzer şekilde, İsrail Savunma Kuvvetleri Genelkurmay Başkanı General Gadi Eizenkot da İsrail'in siber yeteneklerini konsolide edecek bir birim kurma kararı almıştır[20]. Söz konusu İsrail Siber Komutanlığı kurulmasına ilişkin ilk emareler, Savunma Bakanı Moshe Ya'alon'un 2014 Gazze Savaşı sırasında İsrail'in İran siber saldırıları tarafından hedef alındığını ancak önemli bir zarar verilemediğini belirten açıklamaları sırasında gelmiştir[21].

Estonya, Gürcistan ve Ukrayna'daki siber saldırıların olağan şüphelisi konumunda bulunan Rusya ise siber imkân ve kabiliyetlerini önemli ölçüde arttıran bir diğer devlettir. Bu çerçevede, Moskova'nın, siber harekâtı, mevcut hibrid harp stratejisi ve dış politikasının bir parçası olarak değerlendirdiği görülmektedir. Rusya'nın Ukrayna'daki saldırgan faaliyetleri çerçevesinde siber harbi bir 'koç başı' gibi kullandığı da göz önünde bulundurulduğunda, taarruzi siber yeteneklerin Moskova'nın askeri düşüncesine ve hatta askeri doktrinine entegre edildiği değerlendirilmektedir[22]. Rusya kaynaklı siber harp tehditlerine karşı koymak için NATO 2008 yılında, Estonya-Talin'de Müşterek Siber Savunma Mükemmeliyet Merkezi'ni kurmuştur. Merkezin görevi, NATO, üyeleri ve ortakları arasındaki siber savunma alanında yeteneklerin, işbirliğinin ve bilgi paylaşımının genişletilmesi olarak belirtilmektedir[23]. Ayrıca, 2014 Galler Zirvesi'nin ardından, NATO siber savunma ve güvenliğe daha çok ağırlık vermiş ve bu bağlamda siber savunmayı kolektif savunmanın ana görevlerinden biri olarak değerlendiren bir siyaset benimsemiştir[24].

Çin Halk Cumhuriyeti de siber uzayda yükselen güçlerden biri olarak görülmektedir. Çin'in siber harp programları, diğer aktörlere kıyasla, daha çok taarruzi yeteneklere odaklanmaktadır. Bazı analizlere göre, Çin'in siber yetenekleri, KGB'nin ABD teknolojik üstünlüklerine yönelik en önemli tehditlerinden biri olan endüstriyel espiyonaj yöntemlerine dayanmaktadır[25]. Çin'in siber doktrini ve harp teşkilatı kapsamında esas sorumlu birimin 61398. Birim olduğu değerlendirilmektedir. Söz konusu birim, Çin Genelkurmayı'nın 3. Departmanı'na bağlıdır ve bu departman 'bilgisayar ağları harekatlarını' yürütmekle sorumludur. China Telecom'un bahse konu birim için özel fiber-optik iletişim altyapısı sağladığı ve birimin personel sayısının 'yüzler ve hatta binlerce asker' ile ifade edilebileceği tahmin edilmektedir[26]. Çin Genelkurmayı doğrudan Komünist Parti'nin Merkezi Askeri Komisyonu'na bağlıdır. Bu nedenle, 61398. Birim'in siber

faaliyetleri doğrudan en üst düzey siyasal kontrol altında yürütülmektedir ve komünist idarenin karakterinden ötürü merkezi karar-alma mekanizmalarına tabidir.

61398. Birim'in siber faaliyetlerinin 'Gelişmiş Kalıcı Tehdit' kategorisinde (*Advanced Persistent Threat - APT*) değerlendirilmesi gerektiği öne sürülebilir. 'APT', "güçlü kaynaklar ve iyi eğitimle desteklenmiş düşmanın hassas ekonomik, hususi ya da milli güvenliğe ilişkin verileri birkaç yıl süren sızma harekâtları ile hedef alması faaliyetlerine karşılık gelmektedir. Bahse konu düşmanlar, hedeflerine çoğu konvansiyonel bilgisayar ağ savunma mekanizmalarını akamete uğratmak için tasarlanmış gelişmiş araçlar ve teknikler ile ulaşmaktadırlar"[27]. APT yoluyla potansiyel düşmanların hem endüstri hem de devlet segmentlerinde bilgi toplamayı amaçladıkları da düşünülürse, APT en önemli yükselen tehditlerden biri olarak değerlendirilmelidir[28].

Daha geniş bir perspektiften bakıldığında, Çin Halk Kurtuluş Ordusu'nun (HKO) harp konseptlerinin siber harp, sinyal-istihbaratı, uyduları hedef alan yetenekler, psikolojik harp ve bilgi harekâtlarını giderek daha sistematik biçimde kullanarak geliştiği görülmektedir. HKO'nun askeri jeopolitik perspektifi, elektro-manyetik spektrum, siber-uzay ve uzay tarafından oluşturulan harp sahalarına ve bunların birleşimiyle meydana çıkan nihai bir "sanal harp sahasına" uzanmaktadır[29]. Pratikte, böyle bir askeri yaklaşım müşterek harp konseptleri çerçevesinde bir Çin modeli ortaya koyacak ve elektronik harp, hassas taarruz yetenekleri ve siber harbi kapsayacaktır. Soğuk Savaş dönemi Sovyet konsepti olan 'telsiz ve elektronik harp' anlayışını yeni boyutlara taşıyan Çin askeri stratejistleri, sadece harp sahasına ve taktik angajmanlara odaklanan Sovyet yaklaşımını geliştirerek, HKO'nun 'telsiz ve elektronik harp' anlayışını stratejik seviyeye taşıyabileceğini hesaplamaktadırlar. Bahse konu çabaların merkezinde uzay ve siber-uzayın entegrasyonu bulunmaktadır[30].

Son olarak, İran'ın da siber harp dünyasına gelişen ve iddialı bir aktör olarak girdiği söylenebilir. Diğer birçok otoriter rejim gibi, İran'ın siber adımlarının ilk olarak iç güvenlik odaklı başladığı görülmektedir. 2009 protestolarına müteakip, Tahran ülke içindeki bütün iletişimi gözetlemek için Çin yapımı kapsamlı bir izleme-dinleme sistemi kurmuştur[31]. Daha sonra, Stuxnet'in etkisiyle siber teknolojinin yıkıcı sonuçlarını gören rejim, Dini Lider Ayetullah Ali Hamaney'in onayı ile 2011 yılında Yüksek Siber-uzay Konseyi'ni kurmuştur. Söz konusu birim, hem müdafi hem

de taarruzi siber yeteneklerin yönetiminden sorumludur. Konsey, çeşitli istihbarat ve güvenlik kurumları ile kültür ve haberleşme bakanlıklarını da çalışmalarına dahil etmektedir. İran siber güvenlik mekanizmasında Devrim Muhafızları'nın da önemli bir rol oynadığı görülmektedir. Ayrıca, İran 2012 yılında ilk siber tatbikatını icra etmiştir ve Ruhani'nin devlet başkanlığına gelmesi ile siber operasyonlar bütçesini 20 milyon dolar arttırmıştır[32].

Stuxnet'in, İran'ın nükleer yeteneklerinin yaklaşık %20'sine zarar vererek göreceli bir başarı göstermesinin ardından, Tahran 'siber savaşçılar' yetiştirmeyi amaçlayan bir programa daha fazla yatırım yapmaya başlamıştır[33]. Söz konusu program ve siber savaşçılar bağlamında aktarılan noktalar önemlidir: "İran'da önemli seviyede bir hacker topluluğu bulunmaktadır. Bahse konu hacker'ların yetenek spektrumu, bilinen açıkları yazılım araçları kullanarak hedef alan amatörlerden, yeni açıklar ve hedef alma araçları üreten üstün hackerlara kadar uzanmaktadır"[34]. İran hacker toplulukları arasında önemli yere sahip olanlara Iran Babol Hackers Security Team, Ashiyane Digital Security Team ve Iran Hackers Sabotage Team örnek verilebilir[35]. Suudi Aramco şirketi ve Katar RasGas şirketine yönelik siber saldırılar, İran'ın bu alanda özellikle Körfez Bölgesi kritik enerji varlıklarına yönelik taarruzi yeteneklerinin boyutunu göstermesi bakımından önem arz etmektedir. Benzer şekilde, bahse konu saldırılar sırasında bazı ABD bankalarının da hizmet dışı bırakma saldırılarına maruz kaldığı bilinmektedir[36].

Yukarıda aktarılan bilgiler ışığında, Türkiye'nin ve NATO'nun 21. yüzyılda daha ciddi siber meydan okumalar ile karşılaşacağı değerlendirilmektedir. Yukarıda değinilen bütün yetenekler, devlet düzeyindeki aktörlerin siber imkân ve kabiliyetlerinin yanı sıra, yeni güvenlik tehditlerinin çerçevesinde siber vekalet savaşları tehditlerine de dönüştürülebilir. Devlet düzeyindeki aktörler özellikle '*false flag*' tarzı operasyonlara yönelebilirler, hackerlardan yararlanabilirler ve üçüncü devletleri siber operasyonlar için kullanabilirler. Bu karmaşık tehdit ortamı, Türkiye'nin milli güvenliğine ve NATO'nun işbirliğine dayalı güvenlik ve kolektif savunma prensiplerine yeni tehditler teşkil edecektir. Siber çalışmalar, aktör-temelindeki değerlendirmeler kadar, siber harp konseptine, savaşın beşinci boyutu olarak odaklanmalı ve etkilerinin ağ merkezli harp ortamına nasıl aktarıldığını incelemelidir; bunun Türkiye ve NATO müttefiklerinin siber tehdit hesaplarını daha iyi anlamasını sağlayacağı düşünülmektedir.

3. Savaşın Beşinci Boyutunu Kavramsallaştırmak: Siber-uzay ve Ağ Merkezli Harp

Siber harp sahasının yer aldığı bilgi sistemleri çevresi fiziksel, sinaptik ve semantik olmak üzere üç katmandan oluşur. Siber taarruzi yetenekler ve ağ merkezli harekâta yönelik destek operasyonları söz konusu üç katmanda icra edilmektedir. Fiziksel katman bilgisayarlar, donanım unsurları, kablolar ve radyo frekansı, elektronik sinyaller ve fotonlar gibi öğelerden oluşur[37].

Fiziksel katmanın, özellikle mevcut akıllı mühimmatlar, özel kuvvetler operasyonları ve 'görünmezlik teknolojisine' (*stealth*) ilişkin imkân ve kabiliyetler göz önünde bulundurulduğunda, kinetik askeri saldırılara açık olduğu görülmektedir. Sözdizimsel katman ise fiziksel sistem içinde dolaşan, bilgi sistemlerini aktive eden ve görevler veren emirlerden oluşur[38]. Söz konusu katman hacker saldırılarına açıktır ve bilgi sistemlerini korumak üzere siber savunma yetenekleri gerektirmektedir. Son olarak, semantik katman bilgi içeriğine 'anlam katılan' bölümdür ve bu nedenle aldatma ve şaşırtmacalara yönelik faaliyetlere karşı hassastır[39]. Bu bağlamda, mevcut askeri trendlerin 'kesin ve açık olmayan savaşların' ipuçlarını verdiği bu çerçevede 'savaşan tarafların kimliği ve savaşın bizatihi kendisinin' belirsizlikler taşıyabileceği görülmektedir. Özellikle teknoloji ve askeri teşkilatlardaki değişimler bahse konu trendlerin önünü açmaktadır. Belirtilen nedenlerle bu çalışma siber harbin geleceğin ağ merkezli harekatında oynayacağı rolü de irdeleyen bir paradigma üzerine kurulmuştur[40].

Siber savaşa ilişkin harp sahası kategorizasyonu karar vericilere geleceğin siber operasyonları ve operasyonların icra edileceği 'topografyaya' ilişkin önemli fikirler verebilecektir. Siber-uzay savaşın yeni bir sahası olarak algılansa da, enformasyon sistemlerinin fiziksel katmanı halen deniz-hava-kara kuvvetleri gibi 'geleneksel' güçlerin müdahalelerini gerektirmektedir. Ayrıca, sinaptik ve semantik katmanlarda icra edilen siber operasyonlar, düşman hacker faaliyetleri kinetik olmayan metotlar ve aldatmaya yönelik psikolojik harekat ile entegre edilebileceği için birbirine bağımlıdır. Bu nedenle siber-uzayda yeni nesil 'müşterek harekât' konseptleri, yani aynı anda fiziksel, sözdizimsel ve semantik katmanlarda icra edilen operasyonlar, müdafi ve taarruzi siber harekât anlayışında ciddi değişikliklere neden olabilir.

Çok katmanlı yapısının dışında, siber uzayı harbin beşinci ve yeni boyutu olarak algılamak, söz konusu zeminin savaşın diğer dört boyutundan izole biçimde düşünüldüğü anlamına gelmemelidir. Aksine, bu çalışma, siber uzayın ve siber savaşın gelecek ağ-merkezli harekât ortamında savaşın diğer boyutları ile birlikte önemli bir rol oynayacağını değerlendirmektedir. 2012 yılında Liles ve meslektaşları tarafından yapılan bir çalışmada vurgulandığı üzere, askeri prensiplerin siber harbe uygulanması:

> "…dijital bilgi teknolojilerinin katmanlı olarak silahlı kuvvetlerin silah platformlarına uyarlanması anlamına gelmektedir. Bu, ulus-devlet düzeyindeki aktörlere düşmana karşı önemli bir bilgi üstünlüğü sağlayacaktır. Siber-uzaydaki yeteneklerin karasal platformlara katmanlı olarak yayılması, özü itibariyle, deniz kuvvetlerine bağlı platformların kara kuvvetleri unsurlarını desteklemesinden çok da farklı değildir. Bu çerçevede bir diğer örnek uzaydaki unsurların askeri faaliyetleri olabilir. Örneğin keşif uyduları savaşın tüm doğal boyutlarını (hava-kara-deniz) desteklemektedir ve siber boyut da hâlihazırda komuta-kontrol sistemlerine benzer destekler sunmaktadır"[41].

Ağ merkezli harp yeteneklerinin gelişmesi, siber varlıklara operasyonel ve taktik imkân ve kabiliyetler kazandırılması bağlamında önemli avantajlar sağlayacaktır. Ağ merkezli harekâtın ve ağ merkezli harbin başarılı bir şekilde icra edilmesi düşman üzerinde enformasyon üstünlüğü kurulmasına, bahse konu enformasyon üstünlüğü de karar vericiler, muharip aktörler ve sensörler arasında güçlü bir bağlantı kurarak harp gücünü teşkil etme kapasitesine bağlıdır[42]. Askeri bir bakış açısıyla, belirtilen yaklaşım zaman, harp sahası ve konuşlandırılan kuvvet arasındaki korelasyonu ciddi biçimde değişikliklere uğratabilecek niteliktedir. Daha açık bir anlatımla, ağ merkezli harekât sayesinde, geniş harp sahalarına yayılmış kuvvetler artık daha etkin muhabere imkânları ile daha iyi senkronize olabilmektedirler[43].

Son olarak, ağ merkezli harekâtın hem teknolojik trendler hem de askeri düşünce bağlamındaki anti-tezinin platform-merkezli yaklaşım olduğu vurgulanmalıdır. ABD Kara Kuvvetlerinden Albay Alvin Bailey'in görüşleri doğrultusunda platform-merkezli harp anlayışının kısıtlılıkları aşağıda aktarılmaktadır:

> "ABD Kara Kuvvetleri dünyanın en çok korkulan, sofistike ve ölümcül zırhlı araçlarına sahiptir. Abrams Tankı ve Bradley Zırhlı Muharebe Aracı çöl koşullarında dahi yüksek hızlarda intikal ederek düşmanlara korku salmaktadır. Bahse konu platformların görevleri o kadar başarılı olmuştur

> ki, düşmanlar açık çöl arazisinde dahi ABD zırhlı birliklerine karşı koymaktan kaçınmışlardır. Öte yandan, Kara Kuvvetlerinin yıllar boyunca platform-merkezli harbi başarıyla icra etmesine karşı bu anlayışa dayanmak gelecekteki harekât ortamı için bazı zorluklar da ortaya koyabilir. Bu büyük platformları hızla konuşlandırmak kolay değildir. ABD Kara Kuvvetleri henüz bu platformları tüm kuvvet çapında modern teknoloji sağlayarak otomatize edebilmiş değildir. Veritabanından bilgi alarak aktarma faaliyeti farklı sistemler arasında enformasyon paylaşımına dayanmaktadır. Son olarak, bant genişliğinde hâlihazırda var olan kısıtlamalar mevcut teknoloji kullanılarak yapılan bilgi paylaşımını sınırlamaktadır. Belirtilen hususlar günümüzdeki platform merkezli harp yaklaşımı yerine alternatif konseptler arayışını da gerekli kılmaktadır".[44]

Dolayısıyla, Türkiye ve müttefikleri yeterli taarruzi ve müdafi siber yetenekler geliştirmedikleri sürece Türkiye'nin ağ merkezli harekât konseptleri gelecekte akamete uğratılabilir ve 'kazara platform merkezli' bir düzeye indirgenebilir.

4. Stratejik Silahlar olarak Siber Silahlar: Türk ve NATO Siber Güvenliği için İmkan ve Kabiliyet Odaklı Yeni bir Modeli Düşünmek

Siber silahlara ilişkin bir diğer tartışma konusu da bu unsurların stratejik silahlar kategorisinde değerlendirilip değerlendirilemeyeceğidir. Siber silahların doğasının ve karakteristik özelliklerinin iyi anlaşılması Türkiye ve müttefikleri için hayati önemdedir. Stratejik silahların karmaşık karakteristik nitelikleri üst düzeyde yıkıcı kapasiteyi ve psikolojik olarak terör-korku etkisini ve dehşet dengesi oluşturabilecek unsurları içermektedir.

Tabanksy'e göre siber harbi anlarken kullanılacak doğru yöntem klasik olarak yeni bir silah sistemine yaklaşımımıza benzer olmalıdır. Siber harbin karakteristik özelliklerini ölçmek ve kavramsallaştırabilmek için analistlerin, menzil, yıkıcı etki ve (silahın) kullanımı durumunda siyasi maliyet ve kısıtlılıklara odaklanmaları gerekmektedir[45]. Ayrıca, ilk darbe (*first strike*) avantajı da siber harp kapsamında açık biçimde görünmektedir. Bu kapsamda, siber teknolojinin komuta-kontrol sistemlerine uygulanmasının sonuçları açısından taarruz müdafaadan daha cazip bir seçenek olarak ortaya çıkmakta ve düşmanın misilleme yeteneklerini sınırlandırmaktadır[46]. Kritik milli altyapı, finans ve bankacılık sistemleri, hassas iletişim sistemleri, internet kullanımı gibi geniş bir hedef spektrumunun bulunması da siber silahları konvansiyonel silahlardan daha korkutucu kılabilmektedir.

Yukarıda açıklanan metodolojiye ek olarak, Center for Strategic and Budgetary Assessments (CSBA) adlı ABD merkezli düşünce kuruluşunun konuyla ilgili raporu siber silahlar ve siber harbe ilişkin aşağıdaki değerlendirmeleri vermektedir:

> "Nükleer silahlar ve siber silahların paylaştığı önemli bir özellik de her iki kategorinin taarruzu avantajlı kılarak ön plana çıkarmasıdır. Daha farklı bir ifadeyle, diğer tüm kaynakların eşit kabul edildiği bir varsayımda, taarruzi yeteneklere yatırım yapan taraf avantajlı olacaktır. Nükleer yarış bağlamında, ABD Silahlı Kuvvetleri dünyanın teknolojik olarak en sofistike gücü olarak kabul edilse de, nükleer yeteneklere sahip balistik

füzelere karşı etkili bir savunma mekanizmasını yarım yüzyıldan beri milyarlarca dolar harcamasına karşın henüz tam olarak geliştirmiş değildir. Benzer şekilde, taarruzi siber yetenekler geliştirmek için kurgulanacak harcamalar siber savunma altyapısı için yeterli olacak bütçeden çok daha azdır. Durum tam tersi olsa idi, siber ekonomik harp, siber suçlar ve siber espiyonaj bugünkü düzeylerde sorun oluşturmayacaktı"[47].

Öte yandan, siber silahları tam anlamıyla 'stratejik silah sistemleri' olarak kategorize etmek henüz mümkün görünmemektedir. Peki, bu durumda söz konusu teknolojinin askerileşmesini ve silah haline dönüşmesini nasıl formüle etmek gerekmektedir? 2012 yılında Royal United Services Institute (RUSI) tarafından yayımlanan bir çalışma yüksek potansiyele sahip siber silahların 'anti-radyasyon füzelerine' ve 'at ve unut' karakterli hassas güdümlü silahlara benzetilmesi gerektiğini önermektedir. Söz konusu silahlar, spesifik hedeflerin hazırlanarak sistemlerine yüklenmesine gereksinim duymaktadırlar[48]. Teknik bir perspektif ile ifade etmek gerekirse, gelişmiş anti-radyasyon füzeleri düşmanın entegre hava savunma sistemlerini coğrafi lokasyona bağlı sistemler, aktif yaklaşma güdümlü sistemleri ve ağ-entegre komünikasyon sistemleri vasıtasıyla imha etmek üzere dizayn edilirler[49]. Askeri planlamada, anti-radyasyon füzeleri, düşman hava savunma sistemlerinin imhası görevlerinde kullanılır ve böylece daha geniş hava saldırıları için gerekli zemini hazırlarlar.

Spektrumun bir ucunda, siber silahlar 'kötücül yazılım' (*malware*) unsurlarına dayanmaktadır ve her ne kadar sistemleri etkileme kapasitesine sahip olsalar da, bu unsurlar ciddi zararlar verebilecek şekilde sızma yeteneklerine sahip değildir. Öte sızma, spektrumun yüksek potansiyelli diğer ucunda korunmuş sistemlere otonom penetrasyon yeteneklerine ve ciddi zarar verme kapasitesine sahip gelişmiş kötücül yazılım unsurları bulunmaktadır[50]. Dolayısıyla, siber silahlar düşmanı muharebeden önce felç etme fonksiyonları dolayısıyla anti-radyasyon füzeleri ile benzerlik göstermektedirler.

Öte yandan siber harp yetenekleri savaşan taraflara, stratejik ve taktik hedefleri uzak mesafeden ve genel harekât için operasyonel riskleri minimize edecek şekilde imha etme imkânı vermektedir. Söz konusu avantaj, siber taarruzun belirsizliğine dayanmaktadır ki, bu belirsizlik saldırıya maruz kalan taraf için saldırıyı, bizatihi kendi sisteminden kaynaklanan teknik arızalardan ayırma zorunluluğu ortaya çıkarmakta ve olaylar ile sonuçlar arasında bağlantı kurmayı zorlaştırmaktadır[51].

Askeri istihbarat perspektifinden bakıldığında, siber saldırıların tespiti ve kimlik saptaması biyolojik harp ile benzerlikler göstermektedir. Siber saldırının başında, en kritik öncelik düşman faaliyetinin tespit edilmesi, tanımlanması ve gerekli önlemlerin alınmasıdır[52]. Biyolojik silah programlarında olduğu gibi, siber silah programlarını gizlemek kolaydır ve taarruzi yetenekler çift-kullanımlı teknolojilerin gelişmesi ile doğrudan ilintilidir. İlk askeri istihbarat tespitleri kullanılan biyolojik harp ajanına göre değişebileceği gibi, aynı prensip siber-ajan için de geçerlidir. Ayrıca, özel sektörün ve birey düzeyinde oyuncuların da dâhil olmasıyla, siber harp sahasında 'savaşan tarafları' kesin netlik ile belirlemek giderek daha da zorlaşmaktadır.

Sonuç olarak, biyolojik silahların yayılmasının önlenmesine ilişkin hususlar gibi, siber silahlar ve siber harp de devlet düzeyinde ve devlet dışı aktörlerin faaliyetlerinin izlenmesi için benzer gelişmiş askeri istihbarat yeteneklerini gerektirmektedir. Biyolojik harp ve siber harp için gerekli olan istihbarat ihtiyaçları geniş bir spektrumda imkan-kabiliyet ve niyetler ile ilgilenmektedir. Yine söz konusu istihbarat çalışması, bireyler için ticari olarak ulaşımı mümkün araçları, küçük radikal grupları ve birey-düzeyinde radikalleri de izlemekle yükümlüdür.

5. Türkiye için Devlet Dışı Tehdit Analizi: Değişken bir Siber Güvenlik Ortamı

Orta Doğu'da devlet Weber'in tanımladığı anlamda bir düşüş yaşarken, devlet-dışı silahlı gruplar siber operasyonlara giderek daha büyük ilgi duymaktadırlar ve bu durum siber-uzaydaki çatışmaya bir yayılma etkisi kazandırmaktadır. Bu çerçevede, Suriye Elektronik Ordusu (SEO) dikkat çekicidir. Bu grubun icra ettiği siber operasyonların merkezi Dubai'dir ve grubun bir bölümü de halen Suriye'de bulunmaktadır. Beşşar Esad'ın kuzeni Rami Makhlouf tarafından finanse edilen grup, Suriye diktatörü Beşşar el Esad tarafından 'sanal gerçeklikte gerçek bir ordu' olarak tanımlanmaktadır[53]. IHS Jane's adlı askeri kaynağa göre, SEO'nun temel yöntemi özel hazırlanmış ve gönderilmiş emailler üzerinden alıcıyı bazı linklere yönlendirmek ve SEO'nun ele geçirdiği ya da vandalize ettiği sitelere çekmektir[54]. Grubun siber operasyon sabıkası The Washington Post, UNICEF, ABD Kara Kuvvetleri web-sitesi, Le Monde, International Business Times ve Reuters gibi önemli hedefleri içermektedir[55]. Grubun yeni gönüllüler aradığı ve sızdırdığı bazı bilgileri yayımladığı bir internet sitesi de bulunmaktadır[56].

Açık kaynaklı istihbarat bilgileri de SEO'nun Baas rejimi adına bir siber vekalet savaşı yürüttüğünü doğrulamaktadır. The New York Times'a göre, "eğer araştırmacılar Esad rejiminin bu grup ile yakın bağlarını doğrular ise, devletler [rejime] yanıt vermeyi tercih edebilirler zira bu [grup tarafından düzenlenen] saldırıların somut sonuçları bulunmaktadır." Örneğin SEO, The Associated Press'in Twitter hesabını ele geçirerek Beyaz Saray'da patlamalar olduğuna ilişkin sahte haberler yayarak borsaya ciddi zarar verebilmiştir[57].

Suriye Bilgisayar Topluluğu'nun (SBT) Bassel el Esad tarafından kurulduğu ve daha sonra Beşşar el Esad'ın bu topluluğun başkanlığını yürüttüğü bilinmektedir. SEO'nun nüvesini SBT teşkil etmektedir[58]. Ayrıca, Rami Makhlouf'un grup ile bağları da dikkat çekicidir. Beşşar al Esad'ın annesi Anise el Esad'ın mensup olduğu Makhlouf ailesi her zaman rejimin kilit pozisyonlarında etkili olmuştur. Örneğin, Rami Makhlouf'un kardeşi, Hafız Makhlouf, Suriye'nin oldukça kötü bir namı olan Genel Güvenlik Direktörlüğü'nün iç güvenlik biriminin başkanlığını yürütmüştür. Dahası, Başkanlık Muhafızlarından 105. Tugay Komutanı Tuğgeneral Talal Makhlouf gibi bahse konu aileye mensup generaller de rejimin askeri yapısında önemli yer tutmakta ve hatta özel olarak savaş suçları ve insanlığa karşı işlenen suçlar iddiaları ile anılmaktadırlar[59]. Belirtilen karanlık aile geçmişi ile Rami Makhlouf, Baas rejiminin finansal dinamosu olarak görülmektedir ve yabancı yatırımcılar ile Suriye firmaları arasında köprü olduğu düşünülmektedir[60].

Bu noktada, SBT'nin rolü ve evrimini incelemekte yarar görülmektedir. Beşşar el Esad SBT'nin başkanlığını 1990'lı yıllarda üstlenmiştir. Proje Beşşar'ın 1994'te bir trafik kazasında vefat eden kardeşi Basel tarafından 1989 yılında oluşturulmuştur. SBT projesinin iki amacı bulunmaktadır. Bunlardan ilki çerçevesinde, kontrollü ve tedrici olarak artan bir tempoda rejimin imaj çalışmasının yapılması ve bilgisayar teknolojileri ile internetin rejimin kontrolünde ülkeye girmesi amaçlanmıştır.[61] Diğer yandan ise, kinetik olmayan bir hareket tarzı ile enformasyon harbi ve psikolojik harekât yöntemleri kullanılarak internette Baas rejimi karşıtı propaganda ile mücadele edilmesi hedeflenmiştir[62].

SBT'nin SEO ile bağları, SBT'nin iç savaş koşullarında siber harp gibi bir misyonu olduğunu ve Suriye iç savaşının harbin beşinci boyutu olan siber-uzaya taşındığını göstermesi bakımından önemlidir. Bu çalışma, Suriye Baas rejiminin iç savaş dâhilinde siber harekât ortamında geliştirdiği yüksek deneyimin ve mevcut siber yeteneklerinin, rejimin ayakta kalması durumunda, daha tehditkâr boyutlara varabileceğini değerlendirmektedir. Ayrıca, rejimin müttefiklerinin, özellikle Çin ve İran'ın siber harp yeteneklerinin de rejimin siber harp imkân ve kabiliyetine kritik katkılar yapabileceği düşünülmektedir.

SEO ve SBT'nin yanı sıra, IŞİD bağlantılı Siber-Halifelik Türkiye'nin dikkat etmesi gereken bir diğer aktördür. Grubun en ses getirici siber operasyonu, 8 Nisan 2015 tarihinde Fransız TV5 Monde Televizyonu'nun hacklenmesi ve 'Je suis IS' mesajının yayımlanmasıdır[63]. Daha tehditkâr biçimde, Siber-Halifeliğin anti-IŞİD operasyonlarda yer alan Fransız askerlerinin kişisel kimlik bilgilerini yayımlamış olması da kritiktir[64]. Son olarak, grubun 2015 yılı başlarında ABD Merkez Komutanlığı'nın resmi Twitter hesabını hacklemiş olması da önemlidir[65].

IŞİD'in siber-uzayda geliştirdiği imkân ve kabiliyet ve varlık ciddiye alınmalıdır. Hoffman ve Schweitzer tarafından Nisan 2015 tarihli çalışmalarında belirtildiği gibi:

> "Siber-uzayın cihatçı bir örgüt tarafından kullanılması yeni olmasa da, IŞİD interneti ve özellikle sosyal medyayı diğer terör örgütlerinden oldukça yoğun biçimde kullanmaktadır. Örgütün teknolojik yeteneklerinin yanı sıra, siber-cihat özelliklerinin IŞİD'i herhangi bir köktendinci İslamcı örgütten, Batı ve İslam dünyasında küresel bir markaya dönüştürdüğü görülmektedir. Örgütün Orta Doğu'da ve küresel ölçekte etki alanı oluşturma çabalarının bir parçası olarak, IŞİD Dabık adlı periyodik yayınında propaganda çalışmaları yapmakta ve YouTube, Twitter ve diğer web platformlarında yüksek kalitede görsel yayınlar hazırlamaktadır. Ayrıca, örgüt sosyal ağları kendi gereksinimleri ve hedefleri doğrultusunda daha önce görülmeyen bir

> ölçekte kullanmaktadır. IŞİD Twitter, Facebook, Tumblr ve Instagram'ı etkin biçimde kullanmaktadır ve ABD yetkililerinin ifade ettikleri gibi örgütün mensupları ve destekçileri günde ortalama 90,000 tweet atmaktadırlar. Son yapılan araştırmalarda, IŞİD destekçilerinin 200 – 500 kadarı her gün aktif olarak kullanılan toplam 46,000 Twitter hesabına sahip oldukları belirtilmektedir ve örgüt propagandası bu hesaplar aracılığıyla yayılmaktadır. …Sosyal medya kullanımının yanı sıra, IŞİD'in siber-cihat faaliyetleri web sitelerine saldırıları da içermektedir"[66].

Siber-Halifeliğin faaliyetleri Türkiye açısından özellikle gençlik arasında radikal fikirlerin yayılması bağlamında kritik tehditler oluşturmaktadır, zira Türkiye'de internet kullanımı diğer Orta Doğu ülkelerine göre çok daha yüksektir. Ayrıca, Türkiye'nin IŞİD kaynaklı siber saldırılara maruz kalması, söz konusu saldırıların resmi internet siteleri ile ana akım medyaya yönelik olması da muhtemeldir.

5.1. 2008 Boru Hattı Saldırısı ve 2015 Elektrik Kesintileri: Türkiye için Siber Alarm mı?

Türkiye'ye yönelik siber saldırılar ve faaliyetler çerçevesinde, bu çalışma iki örnek vaka analizine yer verecektir. Bunlardan ilki 2008 yılında Bakü-Tiflis-Ceyhan petrol boru hattında yaşanan patlamalar ve ikincisi de 2015 yılında Türkiye'deki genel elektrik kesintisidir. Erzincan yakınlarında meydana gelen ilk örnek olay kapsamında, Türkiye'deki boru hatlarının her zaman terörist saldırılara karşı kırılgan bir yapıları olduğu belirtilmelidir. 1987 ile 2010 yılları arasında Türkiye'deki boru hatlarına yönelik 59 sabotaj olmuş, söz konusu 59 sabotajın 19'u 2007 ile 2010 yılları arasında gerçekleştirilmiştir[67].

2008 yılında yaşanan saldırıyı ise 'her zamanki saldırılardan biri' olarak tanımlamak mümkün değildir. Bazı kaynakların belirttikleri üzere, "soruşturmanın gizliliğinden ötürü isimlerinin açıklanmasını istemeyen dört kişinin ifadelerine göre, hackerlar alarmları kapatmışlar, iletişimi kesmişler ve borulardaki ham petrolün basıncını yükseltmişlerdir. 30 Ağustos 2008 tarihinde kullanılan esas silah bir 'klavyedir' ve basıncı değiştirerek büyük bir patlamaya neden olmuştur".[68] Bahse konu saldırı Rusya'nın 2008 yılında Gürcistan'da icra ettiği harekât ile aynı döneme rastlamıştır ve bu nedenle şüphe çekmektedir, zira BTC hattı Moskova'nın Avrasya coğrafyasındaki enerji bağlamındaki jeostratejik çıkarlarına ters düşmektedir[69]. Gerçekten de ilgili olayda boru hattı tesislerine yönelik jammer kullanımı, alarm sistemleri ve iletişimin kesilmesi ve uydu sistemleri ile bağlantının kesilmesine yönelik çabalar tespit edildiği bazı kaynaklarca doğrulanmaktadır[70].

Hackerların ilgili olayda güvenlik kamerası kayıtlarını sildiği anlaşılmaktadır. Ancak olay yerini gören kızıl ötesi bir kamera söz konusu tesis yakınında bulunan ve dizüstü bilgisayarlar taşıyan iki kişinin görüntülerini kaydetmiştir[71]. Rusya – Gürcistan Savaşı öncesinde Ankara – Tiflis ilişkileri oldukça yakın bir profildeydi ve Türk yönetimi Gürcistan'ın NATO üyeliğini desteklemiştir. Bu bağlamda, 2008 Rusya – Gürcistan Savaşı sırasında bazı Rus yetkililerin, Ankara'yı, Gürcistan'ı cesaretlendirmek ve askeri destek vermekle suçlaması da dikkat çekicidir[72].

İncelemeye alacağımız ikinci ses getirici siber saldırı iddiası 31 Mart 2015 tarihinde Türkiye'nin 81 ilinin 44'ünü etkileyen elektrik kesintileri ile ilgilidir. Bu olayda siber saldırı ihtimali bizzat Başbakan Ahmet Davutoğlu tarafından dile getirilmiştir ve bazı medya kaynakları saldırının arkasında İran olabileceğini belirtmişlerdir. Bu çerçevede İran'ın söz konusu saldırıyı Cumhurbaşkanı Erdoğan'ın Tahran'ı bölgesel hegemonya kurmakla suçlaması ve Yemen'de Körfez ülkelerinin yürüttüğü operasyonlara destek vermesine cevaben gerçekleştirdiği de söylenmiştir[73]. Gün boyu süren kesintilerin 298 organize sanayi bölgesinde üretimi durdurduğu ve yaklaşık 700 milyon dolara mal olduğu tahmin edilmektedir[74]. Bazı uzmanlar daha kötümser tahminlerde bulunarak zararın 1 milyar doları bulabileceğini öne sürmüşlerdir[75]. Elektriğini doğrudan İran'dan alan Van'ın kesintilerden etkilenmemesi dikkat çekici olsa da[76], henüz teyit edilebilen ve saldırıların failinin İran olduğunu kesin biçimde doğrulayan verilere, kamuya açık kaynaklar ile ulaşmak mümkün olmamıştır.

2010 yılında CSIS adlı ABD merkezli düşünce kuruluşu için kaleme aldığı raporda, James Andrew Lewis elektrik hatlarının siber saldırılara maruz kalabileceğini açık ifadelerle belirtmiştir. Lewis'e göre:

> "Elektrik güç sistemleri her zaman askeri ve gayrinizami unsurlar için yüksek öncelikli hedefler olmuştur. Zira iletim hatlarının havaya uçurulması ya da sistemin kapatılması ve güç santrallerinin hedef alınması gayrinizami unsurlar için her zaman kolay ve ucuz olmuştur. Bu gerilla harbinin normal akışı içinde değerlendirilmelidir. Düzenli ordular da benzer şekilde enerji santrallerini ya da hidroelektrik tesislerini hedef almayı, bir bombardıman operasyonu çerçevesinde planlamaktadırlar. … Idaho Ulusal Laboratuvarlarında gerçekleştirilen Aurora testleri büyük jeneratörlerin kendilerini imha etmelerine ya da zarar vermelerine neden olabilecek uzaktan müdahalelerin mümkün olduğu kanıtlamıştır. Araştırmacılar jeneratörlerin operasyonel döngülerini uzaktan değiştirebilmişlerdir. İlgili kayıtlar jeneratörün sarsıldığını ve dumanlar çıkararak çalışmayı durdurduğunu göstermektedir. … Yine belirlenemeyen yabancı kaynakların elektrik ağlarına yönelik bilgisayar ağı tabanlı müdahalelerine ilişkin kanıtlar mevcuttur. Bazı elektrik şirketleri her ay kaynağı belirlenemeyen benzer

binlerce girişim rapor etmektedirler ancak birçok kez bunun bir askeri keşif faaliyeti mi yoksa siber suç mu olduğunu tam olarak tespit edememekteyiz. Ayrıca elektrik hatlarına yönelik ağ altyapısını hedef alan keşif ve siber saldırı girişimleri ve potansiyel zafiyetleri anlamak için bu çerçevede yapılan çalışmaların olduğu da bilinmektedir[77].

Stratejik olarak elektrik hatları yüksek değerli hedeflerdir zira düşmana doğrudan ve dolaylı zarar verebilme kapasitesine sahiptirler. Askeri bir perspektiften bakıldığında, bir elektrik iletim hattına maksimum zarar yüksek irtifada nükleer patlama ya da siber harp yoluyla verilebilir. Rusya, Çin, İran ve Kuzey Kore gibi devletler kritik milli altyapı hedefleri bağlamında elektrik hatlarına saldırmayı da değerlendirdiklerinin sinyallerini vermişlerdir[78].

5.2. Türkiye'nin Siber Yeteneklerini Geliştirme Çabaları

2015 yılında yaşanan kesintilerin siber saldırı olma ihtimali 2008 boru hattı patlamaları kadar ciddiye alınmamıştır. Öte yandan ilgili kesinti bir siber saldırı sonucu gerçekleşmiş olmasa da bir uyandırma-zili olarak işlev görebilmeli ve günlük bir milyar dolar zarara neden olabilecek ve Türkiye'de günlük hayatı felce uğratacak olası bir siber saldırıya ilişkin, yıkıcı etkileri bağlamında, dikkat çekmelidir. Nitekim Türkiye'de resmi internet ağlarına ve web sitelerine yönelik siber saldırılar Mayıs 2015'ten sonra tedrici olarak gözlemlenmiştir. Belirtilen saldırılar yaklaşık 12 'siber taarruz çıkış hattından' eş zamanlı olarak kurgulanmıştır.

Bakü-Tiflis-Ceyhan petrol boru hattına yönelik 2008 saldırısı Türk karar vericiler için çok değerli dersler içermektedir. Öncelikle, söz konusu saldırı siber taarruzun kinetik etkilerini göstermesi bağlamında önemlidir. İkincisi, bahse konu saldırı bölgesel güvenlik konuları, enerji jeopolitiği ve askeri-siyasi rekabet arasındaki bağlantıyı göstermiştir. Üçüncü olarak, bu siber saldırı kritik milli altyapının zafiyetine ve savaşın beşinci boyutundaki tehditlere dikkat çekmiştir.

BTC saldırısına cevaben, Ankara siber savunma kapasitesini yükseltmeyi hedeflemiştir. Bu çerçevede, 2010 yılında Milli Güvenlik Kurulu konuyu gündemine almış, 2012 yılında da TSK bünyesinde Siber Komutanlık kurulmuştur[79]. 2011 yılında Türkiye ilk milli Siber Güvenlik Tatbikatı'nı icra etmiş, tatbikat kapsamında senaryolar ve kırmızı-takımlar tarafından gerçekleştirilen yıkıcı faaliyetler yer almıştır[80]. Dört yıl sonra Türkiye'nin Kırmızı Kitap olarak bilinen ve Türk Devletinin kurumları için stratejik rehberlik ve doktrin kaynağı olan Milli Güvenlik Siyaset Belgesi, siber güvenliği de esas konuları arasına almıştır[81].

6. Sonuç ve Öneriler

Askeri bir perspektiften bakıldığında, yüksek profilli bir siber silahın, nükleer silah, biyolojik silah, zaman ayarlı bomba, anti-radyasyon füzesi, özel kuvvetler ve bir Orta Çağ kılıcının karakteristik niteliklerini aynı anda taşıdığı söylenebilir. Yüksek profilli bir siber silah bir ölçüde nükleer silah karakteristiği taşır zira kritik milli altyapıyı ciddi biçimde zarar verecek şekilde hedef alabilir; aynı zamanda bir ölçüde biyolojik silahları andırır zira siber saldırının tespit edilmesi ve saldırganın kimliğinin belirlenmesi özel istihbari çalışma gerektirmektedir. Bir boyutuyla anti-radyasyon füzelerine benzemektedir zira sinyalleri izleyerek hedefine varabilir ve daha müteakip saldırılar için zemin hazırlar. Bir ölçüde zaman ayarlı bir bombayı anımsatmaktadır zira saldırı anı ile etki zamanı arasındaki boşluk saldırgan tarafından dizayn edilebilir. Özel ve gizli operasyon unsurları olmaları nedeniyle, siber silahlar bir ölçüde de özel kuvvetler harekâtlarını andırmaktadır. Son olarak, caydırıcılık bağlamında siber silahların bir Orta Çağ şövalyesinin kılıcına benzetilmesi mümkündür zira kılıcı kalkan ile caydırmak olası değildir.

Belirtilen askeri değerlendirmeler ışığında, siber harbin karmaşık bir fenomen olduğu ve savaşı, teknolojik ilerlemenin ötesinde bir değişime zorladığı söylenebilir. Siber harbin içerdiği teknolojik ilerlemeler ve imkânlar, gerek kinetik gerekse kinetik olmayan etkileri ve yetenekleri ile orantılı olarak, yeni doktrinler, teşkilat yapıları, konseptler, stratejik ve taktik yaklaşımlar, taarruzi ve müdafi hareket tarzları ve daha da önemlisi, yeni bir savaşçı sınıfı oluşturmaktadır. Öte yandan, siber harp savaşlar için yeni bir boyutu da tanımlamaktadır. Daha önce belirtildiği üzere, savaşın boyutları birbirleri ile ilintilidir ve çatışma trendleri giderek müşterek harekât konseptlerini ön plana çıkarmaktadır. Bu durum da, hava-kara harekatı, hava-deniz harekatı gibi hususlar, kara, hava ve deniz kuvvetleri unsurlarını giderek daha entegre biçimde çalışmaya itmektedir ve ağ merkezli harekatı da teşvik etmektedir. Son yüzyılda uzayın da bu karmaşık resme dahil olması önem arz etmektedir ve mevcut askeri harekat ortamlarında uzay-tabanlı yetenekler vazgeçilmez bir önem kazanmıştır.

Günümüz itibariyle, füze savunma ya da kıtalararası balistik füze operasyonları gibi karmaşık görevler uzay-tabanlı sistemler olmadan yapılamazlar. Topçu sistemleri, ana muharebe tankları, hatta modern piyade dahi GPS-tabanlı sistemlerden ve taktik istihbarat ağlarından

doğrudan harekât alanında yararlanmaktadırlar.

Siber bağımlılıkta ve ileri elektronik teknoloji altyapısında yaşanan hızlı değişimler siber-uzayın harbin diğer boyutları ile daha güçlü entegre olmasını sağlamaktadır. Bu bağlamda, ağ merkezli harekât konseptleri komuta-kontrol-komünikasyon-bilgisayar-istihbarat-keşif-gözetleme (C4ISR) altyapısı ve hassas güdümlü silahlar bağlamında giderek daha çok bilgisayarlara bağımlı olmaktadır. Bu şartlar altında, siber silahlar düşmanı felce uğratma ve komuta-kontrol altyapılarını körleştirme yetenekleri dolayısıyla önem kazanmaktadır. Ayrıca, elektronik harp, hava kuvvetleri başta olmak üzere birçok askeri kuvvetin ve birliğin faaliyetlerinde giderek artan bir yer tutmaktadır ve siber harp ile daha yakın ilişki geliştirmektedir. Benzer bir durum enformasyon operasyonları ve psikolojik harp için de söylenebilir.

Sonuç olarak, siber harp, harbin yeni bir boyutu ve askeri teknolojik gelişmelerin bir tezahürü olarak ortaya çıkmaktadır. Bu nedenle, Askeri Meselelerde Devrim teorisinin de gerektirdiği şekilde, adaptasyon kapasitesi yalnızca savunmaya ilişkin bir zorunluluk olarak değil, aynı zamanda devlet ve devlet dışı aktörler için taarruzi avantaj kazanılacak bir işlev olarak önem kazanmaktadır. Türkiye 21. yüzyılın karmaşık siber tehdit ortamında bir istisna değildir. Türk ekonomisinin büyümesi enerji altyapısına, elektrik üretimine ve hidro-stratejik öneme sahip barajlara doğrudan bağımlıdır. Türkiye bir enerji geçiş merkezi olmak ya da İstanbul'u bir havayolu ulaşımı merkezi haline getirmek gibi stratejik hedeflerini izlemeyi sürdürmektedir. Türkiye'nin devlet ve özel sektör alanlarındaki veri tabanlarının büyük bölümü, finans ve bankacılık faaliyetlerinin önemli kısmı ve enformasyon akışı dijital ortamda yer almaktadır. Bu nedenle siber güvenlik Türk güvenlik ortamının kritik bir parçasıdır.

Bu çalışma aşağıda paylaşılan önerileri Türk karar vericilerin dikkatlerine sunmaktadır:

- TSK bünyesinde bir Siber Komutanlık kurulması takdirle desteklenmektedir. Türk Siber Komutanlığı ile NATO bünyesindeki Cooperative Cyber Defense Center of Excellence, US CYBERCOM ve diğer müttefik teşkilatlar arasındaki işbirliğinin derinleştirilerek geliştirilmesinde yarar mütalaa edilmektedir.

- 2011 yılında icra edilen ve birçok kurumun katıldığı siber tatbikat takdirle desteklenmektedir. Siber tehditler ile mücadelede kurumlar arası eşgüdüm ve işbirliği hayati önemdedir. Türk Siber Komutanlığı ile ilgili açık kaynaklı bilgiler sürekli ve sistematik kırmızı-takım çalışmasının ve sızma testlerinin eksikliğini göstermektedir. Bu nedenle düzenli olarak siber tatbikatlar düzenlenmesi ve etkili kırmızı takım aktivitesi tavsiye edilmektedir.

- Güvenliğe yönelik yeni meydan okumalar ışığında, Ankara'nın, kritik milli altyapıya yönelik stratejik hesaplarını, siber espiyonaj, ağ merkezli harp, psikolojik harp, enformasyon harbi, elektronik harp ve sinyal istihbaratı gibi alanları da dikkate alarak, siber harp kapsamındaki kinetik ve kinetik olmayan etkiler bağlamında gözden geçirmesinde fayda mütalaa edilmektedir. Böyle bir dönüşüm için farklı disiplinlerden gelecek uzmanlar tarafından oluşturulacak bir komisyon oluşturulmasında yarar görülmektedir. Böyle bir komisyon, MGK Genel Sekreterliği bünyesinde oluşturulabilir ve siber güvenliğe ilişkin tartışmaları devletin zirvesine taşıyabilir. Ayrıca MGK'nın anayasal olarak iki ayda bir toplanması konunun fikri takibi açısından da süreklilik sağlayacaktır.

- Askeri teorik ve doktriner perspektifle, yalnızca siber savunmaya yatırım yapmanın 'tek kanatla uçmak' anlamına geldiği vurgulanmalıdır. Bu nedenle, siber taarruzi faaliyetler için gerekli yasal çerçeve ve yetenekler bağlamında, NATO imkân ve kabiliyetleri ile uyumlu çalışmaların yapılması önem arz etmektedir.

- Bu çalışma, Silahlı Kuvvetler, kolluk güçleri, iç güvenlik istihbaratı, Dışişleri ve yargı makamlarını kapsayacak kurumlar-arası bir yapının kurulmasında yarar görmektedir. Ayrıca, TSK bünyesindeki Siber Komutanlığın seviyesinin yükseltilmesi de ilerleyen yıllar için değerlendirilebilecek bir husustur.

- Siber güvenlik çok disiplinli bir sahada yükselen bir ihtisas alanına karşılık gelmektedir. Bu nedenle, Türk güvenlik güçleri için akademik dünya, düşünce kuruluşları ve özel sektörün de dâhil olduğu yeni eğitim programları oluşturulması yararlı olacaktır.

- Özel sektör ve devlet güvenlik birimleri siber savunma ve güvenliğe yönelik bütüncül bir yaklaşımın vazgeçilmez aktörleridir. Özel sektörün

siber zafiyetleri, birer 'siber taarruz çıkış' hattı olarak olası düşmanların planlarına hizmet edebilir. Ayrıca, dijital sistemlerin karşılıklı bağımlılığı gereği ve bilginin hızlı akışı nedeniyle, güvenlik açıkları yıkıcı siber espiyonaj faaliyetleri için daha karmaşık olanaklar sunabilir. Dahası, Türkiye özel sektör ve devlet arasında siber güvenlik alanında işbirliği için net bir organizasyon modeline veya doktrine sahip değildir. Belirtilen nedenlerle bu çalışma, Türkiye için siber güvenliğe ve savunmaya, hem teşkilat yapılanması hem de kültürel boyutlarda, daha bütünsel ve geniş kapsamlı bir yaklaşımın geliştirilmesini önemle tavsiye etmektedir.

- Nihayet Türkiye'nin siber savunma ve siber saldırı yeteneklerinin geliştirilmesinde NATO'nun bu alandaki potansiyel yöneliminin de önem taşıyacağı açıktır. 2016 yılındaki Varşova Zirvesi öncesinde NATO liderlerinin siber konusu ile ilgili önemli bir karar arifesinde oldukları bilinmektedir. Söz konusu Zirve NATO'nun siber yeteneklerinin geliştirilmesi açısından bir dönüm noktası olabilir. Bu bağlamda NATO içinde süren tartışma, siberin, aynı kara, hava ve deniz gibi ilave bir operasyonel alan olarak tanımlanması ile ilgilidir. Siber alanın bu tanıma kavuşması ile NATO içinde, aynen nükleer alanda olduğu gibi, mevcut siber savunma ve siber saldırı yeteneklerin paylaşılması söz konusu olacak, NATO ittifak halinde ülkelerin siber savunmalarına yardımcı olmakla mükellef olacak ama aynı zamanda ülkelerin tamamlayıcı siber yetenekler geliştirmeleri hususunda da bir rol üstlenecek ve bununla ilgili bir yol haritası çıkaracaktır.

- Türkiye, NATO'nun bu daha iddialı siber doktrinine yönelmesini savunan müttefik ülkeler arasındadır. Buna karşılık, ABD gibi kısmen kendi mevcut yeteneklerini açıklamak ve bunları bu aşamada diğer NATO müttefiklerine destek vermek için kullanmak istemeyen ülkeler olduğu gibi, Fransa gibi siber güvenlik konusunda NATO yerine AB'nin öncü rol üstlenmesini isteyen ülkeler de bulunmaktadır. Ancak Türkiye'nin Aralık ayı içinde karşılaştığı siber saldırı gibi örneklerin de önümüzdeki dönemde artması muhtemel olduğundan, NATO liderlerinin, 2016 Varşova Zirvesinde İttifakın siber doktrinini, bu alandaki görev ve yeteneklerini güçlendirme yönünde karar almaları beklenmektedir. Böylesine bir karar Türkiye'nin de siber alanda yeni adımlar atmasını ve yeteneklerini geliştirme yönünde daha tutarlı bir iradeye sahip olmasını beraberinde getirecektir.

1- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, SOME-Sektörel Kurulum ve Yönetim Rehberi, 2014.

2- Türkiye'nin Siber Güvenlik Ulusal Eylem Planı, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1- 1.pdf, Erişim tarihi: 7 Temmuz 2015.

3- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Erişim tarihi: 29 Haziran 2015.

4- James A, Lewis., Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats, CSIS, 2002. s.2.

5- Steven Metz ve James Kievit., Strategy and Revolution in Military Affairs: From Theory to Policy, US Army SSI, 1995, ss. 2-3.

6- Andrew Krepinevich., "Cavalry to computer; the pattern of military revolutions." The National Interest n37 (Fall 1994 n37): 30(13). General Reference Center Gold. Thomson Gale. University of Florida. 19 Kasım 2006.

7- Barry D. Watts, The Maturing Revolution in Military Affairs, CSBA, 2011, ss.15-20.

8- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, ss.28-29.

9- Paul J Springer., Thinking about Military History in an Age of Drones, Hackers, and IEDs, Air Command and Staff College, http://www.fpri.org/docs/springer1.pdf, Erişim tarihi: 7 Temmuz 2015.

10- Roma hafif piyadesi için bkz: Adam, O. Anders., Roman Light Infantry and the Art of Combat, Cardiff University, 2011.

11- James A. Lewis., The Role of Offensive Cyber Operations in NATO's Collective Defense, The Tallinn Papers, CCDCOE, 2015, s.3.

12- John Arquilla and David Ronfeldt. "Cyber War is Coming" in In Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC 1997, s.24

13- A.g.e. s.30

14- A.g.e.

15- A.g.e. s.23.

16- Jennifer, J. Li and Lindsay Daugherty, Training Cyber Warriors, RAND, 2015, s..xi.

17- Detaylı savunma harcamaları için bkz: IISS, Military Balance 2014.

18- US Cyber Command Fact Sheet, 25 Mayıs 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED %20replaces%20May%2021%20Fact%20Sheet.pdf, Erişim tarihi: 29 Haziran 2015.

19- A.g.e.

20- http://www.al-monitor.com/pulse/originals/2015/06/israel-idf-cyber-intelligence-new-unit-eisenkot-war- future.html, Erişim tarihi: 29 Haziran 2015.

21- http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/24/israel-target-for-iranian- hezbollah-cyber-attacks/29210755/, Erişim tarihi: 29 Haziran 2015.

22- Joel Mullish. "Russia's Growing Reliance on Cyber Warfare Setting Dangerous Precedent for Future Foreign Policy", INSS, http://www.inss.org.il/uploadImages/systemFiles/Russia's%20growing%20reliance%20on %20cyber%20warfare%20setting%20dangerous%20precedent%20for%20future%20foreign%20policy.pdf, Erişim tarihi: 29 Haziran 2015.

23- NATO CCDCOE, https://ccdcoe.org/, Erişim tarihi: 29 Haziran 2015.

24- NATO, Cyber Security, http://www.nato.int/cps/en/natohq/topics_78170.htm, Erişim tarihi: 29 Haziran 2015.

25- Magnus Hjortdal., "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", Journal of Strategic Studies, Cilt: 4 No: 2, Yaz 2011.

26- Detaylı bilgi için bkz: Mandiant, APT1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, Erişim tarihi: 28 Temmuz 2015.

27- Eric, M. Hutchins v.d. Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven- Defense.pdf, Erişim tarihi: 29 Temmuz 2015.

28- A.g.e.

29- Larry M. Wortzel., The Chinese People's Liberation Army and Information Warfare, US Army SSI, 2014, pp.1-8.

30- A.g.e. ss.12-13.

31- Ilan Berman., The Iranian Cyber Threat Revisited, ABD Temsilciler Meclisi, Siber Güvenlik, Altyapı Koruması ve Güvenlik Teknolojileri Yurtiçi Güvenlik Alt-Komitesi önünde sunulan bildirge, 2013, s.2.

32- James Andrew Lewis., Cybersecurity and Stability in the Gulf, CSIS, Ocak 2014.

33- Executive Cyber Intelligence, INSS-CSFI, Nisan 1, 2015.

34- Jason, P. Patterson and Matthew, N. Smith., Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran, Naval Postgraduate School, 2005, s.44.

35- A.g.e, ss.44-50.

36- James Andrew Lewis., Cybersecurity and Stability in the Gulf, CSIS, Ocak 2014.

37- Craig Stallard., At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force, School of Advanced Air and Space Studies, Maxwell Air Force Base, 2011, ss.35-36.

38- A.g.e.

39- A.g.e.

40- Martin, C. Libicki., "The Specter of Non-Obvious Warfare", Strategic Studies Quarterly, Güz 2012.

41- Samuel Liles. vd. "Applying Traditional Military Principles to Cyber Warfare", 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012, s.171.

42- Jeffrey R. Witsken., Network-Centric Warfare: Implications for Operational Design, School of Advanced Military Studies-US Army Command and General Staff College, 2002, s.3.

43- A.g.e. ss.17-18.

44- Alvin L. Bailey., The Implications of Network Centric Warfare, US Army War College, 2004, ss.2-3.

45- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Cilt: 3 No: 1, Mayıs 2011.

46- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, s.25.

47- Andrew F. Krepinevich., Cyber Warfare: A Nuclear Option, CSBA, 2012, s.66.

48- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, Şubat/ Mart 2012, Cilt: 157 No: 1, s.6.

49- Austin Miller. Advanced Anti-Radiation Guided Missile: Strengthening DEAD Capability in the Fleet, 43rd Annual Systems: Gun and Missile Systems Conference and Exhibition, Nisan 21-24 2008 Brief.

50- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, Şubat/ Mart 2012, Vol: 157 No: 1, s.8.

51- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Cilt: 3 No: 1, Mayıs 2011.

52- Mehmet Nesip Ogun and Adem Kaya., "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri, Yıl: 9 Sayı: 18, s. 147.

53- Jane's Intelligence Review, Middle East Conflict Spills into Cyberspace, 2015, ss.3-4.

54- A.g.e.

55- http://sea.sy/index/en, Erişim tarihi: 28 Haziran 2015.

56- A.g.e.

57- http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=1, Erişim tarihi: 28 Haziran 2015.

58- A.g.e.

59- Human Rights Watch, By All Means Necessary: Individual and Command Responsibility for Crimes Against Humanity in Syria, 2011, s.87.

60- Jeremy M Sharp., Unrest in Syria and U.S. Sanctions Against the Assad

Regime, Congressional Research Service, 2011, s.4.

61- 1990'lı yılların ortalarında Suriye'de her 1000 kişi başına 2 bilgisayar düştüğü ve 1997'de 400 Suriyeliden oluşan pilot bir grubun internete erişimine izin verildiği belirtilmelidir.

62- John B Alterman., New Media New Politics: From Satellite Television to the Internet in the Arab World, Washington Institute for Near East Policy, 1998, ss.40-41.

63- http://rt.com/news/248073-islamic-state-hackers-french-tv/, Erişim tarihi: 28 Haziran 2015.

64- A.g.e.

65- http://rt.com/usa/221927-central-command-hackedcybercaliphate/, Erişim tarihi: 28 Haziran 2015.

66- Adam Hoffman and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)", Strategic Assessment, Cilt: 18 No: 1, Nisan 2015, s.73

67- USAK, Kritik Enerji Altyapı Güvenliği Sonuç Raporu, No: 4, 2011.

68- http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new- cyberwar, Erişim tarihi: 29 Haziran 2015.

69- A.g.e.

70- http://www.milliyet.com.tr/siber-savasin-miladi/dunya/detay/1982549/default.htm, Erişim tarihi: 29 Haziran 2015

71- A.g.e.

72- http://www.hurriyet.com.tr/dunya/9623756.asp, Erişim tarihi: 29 Haziran 2015.

73- http://www.dailysabah.com/diplomacy/2015/04/28/iran-allegedly-behind-nationwide-power-outage, Erişim tarihi: 29 Haziran 2015.

74- http://www.hurriyet.com.tr/ekonomi/28611619.asp, Erişim tarihi: 29 Haziran 2015.

75- EDAM, Elektrik Altyapısı ve Siber Güvenlik, 2015. http://www.edam.org.tr/tr/IcerikFiles?id=1028, Erişim tarihi: 3 Ağustos 2015.

76- http://www.hurriyet.com.tr/gundem/28604226.asp, Erişim tarihi: 29 Haziran 2015.

77- James A. Lewis., The Electrical Grid as a Target for Cyber Attack, CSIS, 2010.

78- Cynthia E. Ayers and Kenneth D. Chrosniak., Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency, US Army War College Center for Strategic Leadership and Development, Issue Paper, Cilt 1- 13, 2013.

79- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Erişim tarihi: 29 Haziran 2015.

80- Bilgi Teknolojileri ve İletişim Kurumu, http://www.tk.gov.tr/sayfa.php?ID=28, Erişim tarihi: 29 Haziran 2015.

81- http://www.haberler.com/tsk-siber-savunma-komutanligi-ndan-hacker-atagi-7035427-haberi/, Erişim tarihi: 29 Haziran 2015.

TÜRKİYE'DE SİBER GÜVENLİK

Doç. Dr. Salih Bıçakcı

Fakülte Üyesi, Uluslararası İlişkiler-
Kadir Has Üniversitesi

F.Doruk Ergun

Araştırma Görevlisi – EDAM

Prof.Dr. Mitat Çelikpala

Dekan, Sosyal Bilimler Yüksek Okulu-
Kadir Has Üniversitesi

1. Giriş

Siber alanın doğuşu hem kullanıcılar hem de ulus devletlerin güvenlik kurumları için pek çok güvenlik riskini beraberinde getirmiştir. Siber alanı kullanarak saldırı düzenleyen kişiler, mali kurumları hedef alarak, ulusal sırlara erişip sızdırarak ve İran'ın nükleer tesislerini hedef alan Stuxnet solucanının da aralarında bulunduğu birçok örnekte görüldüğü gibi, ulusal altyapılara saldırıp kinetik bir saldırının gerçekleştirebileceği boyutta fiziksel hasarlar vererek, ciddi boyutta zarara yol açabilirler. Siber saldırıları kimin yaptığını belirlemek oldukça zordur, çünkü saldırganlar nadiren arkalarında iz bırakırlar ve hatta kendi konumlarını gizlemek için çabalarlar. Çoğu durumda siber saldırganların pahalı ya da nadir bulunan araçlara ihtiyacı olmaz. Hatta kamunun bilişim teknolojilerine erişiminin kolaylaşması ve bilişim teknolojilerinin hem kamu kurumlarının hem de özel kuruluşların işletilmesindeki rolünün git gide artması güvenlik zaaflarını daha da arttırmaktadır. Dağınık servis dışı bırakma (DDoS) saldırıları gibi birkaç istisna dışında, siber saldırılar, hedef sistemde ve siber güvenlik önlemlerinde var olan açıklardan yararlanarak yapılır;[1] müdafaa eden taraf bu açıkların ve dolayısıyla saldırının nereden gelebileceğinin farkında olmadığından, siber saldırılara karşı savunma daha da zordur. Ayrıca siber saldırganları öngörmek, silahsızlandırmak ve caydırmak daha zordur, bu da siber alanda taarruzun müdafaaya nazaran daha fazla avantajı olmasını sağlar.

Bu sıkıntılara rağmen, ulus devletler siber tehditlerle kendi kaynaklarıyla başa çıkmaya mecburdurlar. Dolayısıyla ulusların siber tehditlere ne kadar açık olduğunun ilk belirteci, ülkenin kendi kabiliyetleri ve siber güvenlik algısıdır. Bundan ötürü bu bölüm Türkiye'de siber güvenlik politikalarında ve mevzuatındaki gelişmelerin kronolojisini ve ülkenin siber güvenlik kabiliyetlerini inceleyerek başlamaktadır.

Bir ülkenin varlıklarına yöneltilen siber saldırılar, ülkenin kendi sınırları içinden doğmak zorunda değildirler. Ancak Türkiye ilginç bir vaka oluşturmaktadır, zira 2013 itibariyle Türkiye vatandaşlarının yalnızca yüzde 46'sının internet erişimi varken[2] (bu Türkiye'yi dünyada 97. sıraya koymaktadır), Türkiye geçmişte dünyadaki siber saldırıların üçüncü büyük çıkış noktası olmuştur[3]. Bundan ötürü bu makalede ikinci olarak Türkiye'de hâlihazırda faal olan siber saldırganların, geçmişteki saldırıları, niyetleri ve mümkün olduğu durumlarda kabiliyetleri incelenecektir.

2.Türk Devletinin Kabiliyet ve Araçları

2.1. Bilgisayarla İşlenen Suçlar Üzerine Mevzuat

Mühim ulusal güvenlik meseleleri haline gelmeden önce, siber saldırılar ekseriyetle asayiş ve hukukun uygulamasını ilgilendiren meselelerdi. Dolayısıyla ordular sibere, kara, hava, deniz ve uzaydan sonra yeni bir savaş sahası olarak ilgi duymaya başlamadan önce, ulus devletler ilk olarak siber uzayın hukuka aykırı suç işlemek için kullanılmasına odaklanmıştır. Bu eğilim Türkiye'de de görülmüştür. Siber suçların Türk Ceza Kanunu'nda ilk yer alışı, 6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile olmuştur. Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında bir bab eklenmiş ve bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiştir[4].

Bilahare, Eylül 2004'te yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile tanım genişletilerek siber suç kavramı da ceza kanununa eklenmiştir. Burada "Bilişim Alanında Suçlar" başlığını taşıyan 10. Bölümde üç grup faaliyet bilişim suçu olarak tanımlanmaktadır: 243. maddede 'Bilişim sistemine girme'; 244. maddede sistemi engelleme, bozma, verileri yok etme veya değiştirme ile 245. maddede banka veya kredi kartlarının kötüye kullanılması[5].

Bu konu ile ilgili diğer maddelerde de bilgisayar ve iletişim cihazları gibi bilgisayar sistemlerini kullanarak (sadece bunlar yoluyla değil) işlenen, kişisel hayata karşı suçlar, iletişimin yasal olmayan biçimlerde engellenmesi, hırsızlık, yolsuzluk, kumar oynatma, sahtecilik ve kalpazanlık gibi suçlar başlıkları altında yer almıştır[6]. Takiben 3713 sayılı Terörle Mücadele Kanununda 2006'da yapılan değişiklikle siber suça terör bağlamında da yer verilmektedir. Değişiklikte "Aşağıdaki suçlar 1'inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır"[7] denilerek Türk Caza Kanundan ilgili bir takım maddeler listelenmektedir.

Bu maddeler, 243 ve 244. maddelere belirtilen bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme maddelerine ek olarak bilgisayar sistemlerini kullanarak işlenebilecek suçların listesini içermektedir[8]. Terörle Mücadele Kanununun ikinci maddesine göre "Terör örgütüne mensup olmasa dahi örgüt adına suç işleyenler de terör suçlusu" sayılmaktadır.

Bu esnada, kamu kurumları, Ankara'nın siber uzayda mevcudiyetinin ulusal güvenlik bakış açısının ötesinde, kamu hizmetlerinin sağlanması ve internet kullanımının düzenlenmesi gibi alanlarda nasıl olacağı konusunda aktif olarak politika üretmeye başlamıştır. 2011 senesinde yerini Kalkınma Bakanlığı almadan önce Devlet Planlama Teşkilatı konuyla ilgili bazı belgeler yayınlamıştır. Bunların arasında "e-Türkiye İnisiyatifi Eylem Planı 2002", e-Dönüşüm Türkiye Projesi ve Kısa Dönem Eylem Planı (2003-2004)" ve "e-Dönüşüm Türkiye Projesi 2005 Eylem Planı" vardır.[9] 2005 senesinde Devlet Planlama Teşkilatı "Bilişim Toplumu Stratejisi" isimli bir çalışma başlatmış ve 2006-2010 dönemini kapsayan bir strateji belgesi ve eylem planı yayınlamıştır; bu planların ana temalarından birisi ise güvenlik ve kişisel bilgilerin mahremiyeti olmuştur[10]. Eylem planı, siber güvenlik tehditlerini sürekli olarak takip etmesi, uyarılar yayınlaması, alınacak tedbirler konusunda bilgilendirme ve koordinasyon sağlaması amacıyla Bilgisayar Olaylarına Acil Müdahale Merkezi (SOME, İngilizce *CERT*) kurulacağını belirtmiştir. Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) altındaki Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nü (UEKAE) bu işin sorumlu kurumu olarak atamıştır[11]. 2006-2010 belgeleri bunun yanı sıra Kişisel Verilerin Korunması Kanun Tasarısı'nın 2006 sonuna kadar onanacağı ve ulusal güvenlik ile ilgili verilerin korunması ve devletin veri güvenliği sistemlerinin iyileştirilmesi için ek mevzuatların yürürlüğe konulacağını belirtmiştir.

Bu çabalara rağmen Meclis'e ilk olarak 2008 tarihinde sunulan Kişisel Verilerin Korunması Kanunu Tasarısı[12] hala onanmayı beklemektedir. Planlanan Bilgi Toplumu Genel Müdürlüğü'nu kuracak ve internet üzerinden e-Devlet portalından kamu hizmetlerinin sağlanmasını denetleyecek e-Devlet ve Bilgi Toplumu Kanun Tasarısı da 2009 senesinin Ağustos ayından beri Meclis'te onanmayı beklemektedir[13].

Bununla birlikte 1990'ların sonunda ve 2000'lerin ilk yarısında, Milli Savunma Bakanlığı'nın koordinasyonluğunda, Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı adıyla bir başka kanun

yazımı çalışmasında daha bulunulmuştur. Başbakanlık tarafından yapılan E-Türkiye İnisiyatifi Eylem Planı'na göre yasanın esasen 2003 ortasında tamamlanması ve onanması planlanmıştır[14]. Kanun taslağı Başbakanlık altında, ülkenin bilgi güvenliği politikalarını yönetmekle sorumlu ve Başbakan, Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu Genel Sekreteri, Genel Kurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Milli İstihbarat Teşkilatı (MİT) Müsteşarı ve TÜBİTAK'ın oluşturacağı bir Ulusal Bilgi Güvenliği Üst Kurulu'nun kurulmasını öngörmüştür[15]. Üst Kurul'un ayrıca tehditlerin değerlendirilmesi, ülkenin bilgi güvenliği politikalarının tayin edilmesi ve uygulanması ile ulusal bilgi güvenliği yönetmeliğinde yapılması önerilen değişikliklerin değerlendirilmesinden de sorumlu olması planlanmıştır.

Bu kanun aynı zamanda Ulusal Bilgi Güvenliği Kurumu Başkanlığı'nın da kurulmasını tasarlamıştır. Başkanlığın beş ana hizmet biriminin olması düşünülmüştür, bunlar: Plan Program ve Koordinasyon, Bilgi Güvenliği, Kriptoloji, Bilgi Destek ile Denetleme ve Bilgilendirme Daire Başkanlıklarıdır. Her bir Daire Başkanlığı'nın, tehditlerin belirlenmesinden, ülkenin bilgi güvenliği mimarisinin oluşturulmasına, kripto sistemlerde kullanılabilecek yazılım ve donanımların tasdik edilmesinden, bilgi güvenliği araçlarının ithalat ve ihracat lisanslarının sağlanmasına kadar değişen birçok görevi olması düşünülmüştür. Kuruma, Uluslararası İlişkiler ve Hukuk Müşavirliği ile Ulusal Bilgisayar Güvenliği Merkezi Müdürlüğü'nün destek sağlanması tasarlanmıştır. Ancak bu kanun daha sonra son taslak üzerinde uzlaşma sağlanamaması nedeniyle rafa kaldırılmıştır[16].

2.2. Türkiye'nin Siber Güvenlik Mimarisinin Kurumsallaştırılması

Bu gelişmelere paralel olarak, ülkede siber alandaki politikaların yürütülmesinden sorumlu kurumların kurulması adına adımlar atılmıştır. Bekleneceği üzere, konuya adanmış kurumların kurulması ülkenin siyaset üretme çabalarını hızlandırmış, internet üzerine mevzuatını zenginleştirmiş ve ülkenin kabiliyetlerini geliştirmiştir. Genel itibariyle bu kurumlar siber güvenliğin asayiş ve hukuki boyutuna odaklanmışlar ve siber savaş boyutunu Türk ordusuna bırakmışlardır. Bunun ana istisnasını araştırma kurumları oluşturmuştur; bu kurumlar Türkiye siber güvenlik mimarisinin her boyutunda, güvenilir yerli yazılım ve donanımların geliştirilmesinde çalışmakta ve dolayısıyla orduyla yakın bir ilişki içerisinde faaliyet göstermeye devam etmektedir.

2.2.1. Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve Telekomünikasyon İletişim Başkanlığı (TİB)

2000 senesinin Ocak ayında kurulan Telekomünikasyon Kurumu, 2008 senesinin Kasım ayında Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) dönüştürülmüştür. BTK telekomünikasyon sektörünün düzenleyici kurumu olarak görev yapmaktadır ve yetkilendirme, denetleme, ihtilaf çözümü, tüketici haklarının korunması, sektör rekabetinin düzenlenmesi, teknik yönergeler yayınlamak ve spektrum yönetimi ve izlenmesinden sorumludur. Bunların yanı sıra kurum bilgi teknolojilerinden sorumlu otoritedir ve bu görevi Telekomünikasyon İletişim Başkanlığı (TİB) vasıtasıyla yerine getirmektedir. 2005 senesinde kurulan TİB doğrudan BTK Başkanı'na rapor vermekte ve olağan personelinin yanı sıra Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı'nın ilgili birimlerinden birer temsilci barındırmaktadır.

TİB büyük oranda internetin de arasında bulunduğu telekomünikasyon araçları vasıtasıyla yapılan iletişimin ve sinyal bilgisinin takibi, gözetlenmesi, değerlendirilmesi ve kayıt edilmesiyle sorumludur. TİB aynı zamanda internet hizmetinin "emniyet" boyutuyla ilgili olarak içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının denetlenmesiyle de ilgilenmektedir. Bundan ötürü TİB internete erişim özgürlüğü/internet sansürü ve kullanıcı mahremiyeti/ağ gözetlenmesi tartışmalarının tam ortasında yer alan ve tartışmaya yol açan bir kurum olmuştur. TİB bunların yanı sıra internet hizmetlerinin izlenmesi, perdelenmesi ve filtre edilmesi için yapılacak yazılım ve donanımlara ilişkin asgari kriterleri belirlemekle sorumludur. Ulusal siber güvenlik mimarisinin bir parçası olan TİB, içerik, erişim ve yer sağlayıcıları ile diğer kurumların siber saldırıları tespit etmesi ve engellemesi için eşgüdüm de sağlamaktadır.[17]

2.2.2. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

Türkiye'de elektronik ve kriptoloji araştırmaları yürüten sivil araştırma kurumlarının kökenleri Orta Doğu Teknik Üniversitesi'nde 1968 senesinde kurulan Elektronik Araştırma Ünitesi'ne dayanmaktadır. Başlangıçta beş kişiden oluşan birim, Marmara Bilimsel ve Endüstriyel

Araştırma Enstitüsü'ne (daha sonra Marmara Araştırma Enstitüsü olarak adlandırılmıştır) bağlanmıştır ve ülkenin ilk milli kripto cihazı olan MİLON-1'i[18] Türk Silahlı Kuvvetleri'nin (TSK) ödüllendirdiği bir proje ile üretmiştir.

Ünite 1991 senesinde Elektronik ve Yarıiletken Teknolojileri Bölümü olarak adlandırılmış, 1995'te ise adı yine değişerek Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) halini almıştır. Bölüm Milli Savunma Bakanlığı ile Kriptoanaliz Test ve Dizayn Merkezi'nin kurulması için 1994 senesinde bir sözleşme imzalamış ve merkezi 1997 senesinde faaliyete geçirmiştir[19].

Aynı sene Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) bünyesinde Ağ Güvenliği Grubu kurulmuştur. Grup, Microsoft ve açık kaynak kodlu işletim sistemleri (OS), e-posta sunucuları, veri tabanları ve bunların güvenlik açıkları ile sızma tespit sistemleri üzerinde çalışmıştır. Bir sene sonra UEKAE doğrudan TÜBİTAK'a bağlanmıştır. TÜBİTAK 2000 senesinde Milli Savunma Bakanlığı ile 2001 senesinde tamamlanacak Ortak Kriter Test Merkezi'nin kurulması için bir sözleşme imzalamıştır. Merkez daha sonra Ortak Kriter değerlendirme, haberleşme güvenliği (COMSEC), Yan Kanal Analizi (Side Channel Analysis) ve Tersine Mühendislik (Reverse Engineering) alanında yetkinlik kazanmıştır[20]. 2006 senesinde UEKAE, GÖKTÜRK uydu projesinin güvenliğini sağlama sorumluluğunu üstlenmiştir[21].

2006-2010 Eylem Planı uyarınca, TÜBİTAK 2007 senesinde dört kamu kurumuna Bilgi Güvenliği Yönetim Sistemini kurmuş ve farklı etkinliklerde kamu kurumları ve özel kuruluşlar için bilgi teknolojileri güvenliği günleri düzenlemeye başlamıştır. Yine 2007 senesinde, TÜBİTAK UEKAE kendi ürünleri ile NATO tatbikatlarına katılmaya başlamıştır. Bunun yanı sıra bu dönemde TÜBİTAK UEKAE kurumsal Siber Olaylara Müdahale Ekipleri (SOME) arasında ortak SOME tatbikatları düzenlenmesini koordine etmeye başlamıştır. TÜBİTAK, Türkiye'de akreditasyona sahip iki SOME'den biri olan ve araştırma ve eğitim amacıyla işletilen ULAK-CSIRT'e ev sahipliği yapmaktadır[22]. Diğer SOME devlet tarafından işletilen TR-SOME'dir. 2007 senesinde ULAK-CSIRT NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability – NCIRC) ile NCIRC ağına erişim, zararlı kod analizi, güvenlik açıkları veritabanı, uyarı/ikaz ve çalışan değişimi gibi konuları içeren bir anlaşma memorandumu imzalamıştır[23].

2010'da TÜBİTAK UEKAE ile (aslen Marmara Araştırma Merkezi altında yer alan) Bilişim Teknolojileri Enstitüsü (BTE), Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) adıyla birleştirilmiştir. Aynı sene Türkiye resmi olarak "Ortak Kriter" (ISO 15408) alanında "Sertifika Üreticisi" ülke olmuştur ve TÜBİTAK BİLGEM OKTEM (Ortak Kriter test merkezi) tarafından bilişim teknolojileri alanında sağlanan sertifikalar uluslararası geçerlilik kazanmıştır[24]. 2012 senesinde TÜBİTAK BİLGEM'de üç enstitü daha kurulmuştur, bunlar, Yazılım Teknolojileri Araştırma Enstitüsü (YTE), Siber Güvenlik Enstitüsü (SGE) ve İleri Teknoloji Araştırma Enstitüsü'dür (İLTAREN). Ertesi sene TÜBİTAK BİLGEM NATO ile bir AR-GE (araştırma ve geliştirme) anlaşması, havacılık ve elektronik üzerine yoğunlaşan ve bir devlet şirketi olan HAVELSAN (Hava Elektronik Sanayi) ile de İşbirliği Mutabakatı imzalamıştır[25]. Yine 2013 senesinde BTE Türkiye'nin ilk Gerçek Zamanlı İşletim Sistemini (GİS) tasarlamış ve üretmiştir.

TÜBİTAK Ekim 2012'ye kadar siber güvenlikten sorumlu kurum olmuştur ve bu yetkisini 2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devretmiştir[26]. TÜBİTAK şu anda milli kripto çözümlerinin yüzde 70'e yakınını sağlamaktadır[27]. TÜBİTAK, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDH) ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile birlikte, 81 ilde 164 farklı noktadan trafik toplayan ülkenin bal küpü (honeypot) siber tehdit tespit sistemini işletmektedir[28]. Görünürde sistemin bir parçası olan ama aslında tecrit edilmiş ve gözlem altında tutulan verilerin saldırganları açığa çıkartmak ve engellemek için yem olarak sunulduğu bal küpü sistemi, TİB'in yetkisi altında kurulmuştur.

Günümüze kadar Türkiye'de üç adet ulusal siber güvenlik tatbikatı olmuştur; biri 2008'de TR-BOME, diğerleri ise 2011 ve 2013'te TÜBİTAK ile BTK tarafından düzenlenmiştir. 2011 ulusal tatbikatı 41 tane kamu, özel ve devlet dışı kuruluştan 200'e yakın personelin katılımıyla gerçekleştirilmiştir. Katılımcılar arasında bilişim teknolojileri alanında çalışanların yanı sıra, finans, eğitim, sağlık, hukuk ve savunma sektörlerinden de katılımcılar olmuştur. 2013'te yapılan tatbikata 20'si gözlemci olmak üzere 61 tane kurum katılmıştır. Bu tatbikatta denenen senaryoların arasında log analizi, port taraması, DDoS, WEB güvenliği taraması, WEB uygulama testi, sosyal mühendislik ve bir "bayrağı ele geçir" yarışması olmuştur[29].

2.2.3. Müdahale Kabiliyeti Oluşturulması

Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 2009 senesinin Mayıs ayında yayınlanan bir rapor[30], yukarıda değinilen taslak yasaların onanmasının yanı sıra, ülkenin siber güvenlik mevzuatını güçlendirmek için belli adımlar atması gerektiğini belirtmiştir. Bunların arasında; siber saldırıların nasıl inceleneceğine dair yönetmeliklere duyulan ihtiyaç, delillerin nasıl toplanacağının düzenlenmesi ve devletlerle bu konuya dair prosedürler ile güvenlik güçlerinin ve yargının siber alandaki yetkilerinin netleştirilmesi vardır. Raporda ayrıca hem güvenlik güçleri hem de yargıda teknik uzmanların yetersizliğine değinilmekte ve siber alandaki acil durumlara dair gerçekçi ve uygulanabilir planlara olan ihtiyacın altı çizilmektedir.

Bu sıkıntıların çoğu hala giderilmemiş olsa da geçtiğimiz birkaç sene içerisinde Ankara'nın siber güvenlik kabiliyetlerini arttırma çabaları ivme kazanmıştır. Örneğin Ulusal Güvenlik Siyaset Belgesi, diğer adıyla Kırmızı Kitap'a siber güvenlik başlığı Ekim 2010 ayında eklenmiştir[31]. Ertesi sene Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı (Şubat 2013'te Siber Suçlarla Mücadele Daire Başkanlığı olarak yeniden adlandırılmıştır) kurulmuştur.

Haziran 2012'de düzenlenen Siber Güvenlik Strateji Çalıştayı'ndan sonra, Bilgi Güvenliği Derneği tarafından kaleme alınan bir tavsiye belgesi yayınlanmıştır. Belgede şu adımların atılması çağrısında bulunulmuştur[32]:

- Ulusal Siber Güvenlik Strateji Belgesinin yayınlanması.
- Ulusal Siber Güvenlik Kurulu oluşturulması.
- Siber güvenlik alanında farkındalığın arttırılması ve siber güvenlik kültürünün yaygınlaştırılması.
- Kişisel ve kurumsal verilerin korunması için daha sıkı tedbir alınması.
- Uluslararası işbirliğinin güçlendirilmesi (belgede AB, ENISA, Avrupa Konseyi, BM, NATO ve AGİT sıralanmaktadır).
- Ulusal siber güvenlik Ar-Ge politikasının oluşturulması ve milli teknolojilerin geliştirilmesinin özendirilmesi.
- Üniversitelerde konu üzerine yürütülen bilimsel çalışmaların arttırılması için adımlar atılması.
- Beşeri sermayenin yetiştirilmesi (bir diğer deyişle ulusal siber güvenlik uzmanlarının yetiştirilmesi).

- Kurumların ve güvenlik birimlerinin siber güvenlik kabiliyetlerinin geliştirilmesine yönelik adımlar atılması.
- Kurumlara siber güvenlik sızma testleri yapacak bağımsız merkezlerin kurulması.
- Yasal mevzuatın düzenlenmesi.

Belgede, aynı zamanda kritik altyapılardaki ve kamu ve özel kurumlardaki SOME'ler arasında koordinasyon sağlanması ve eğitim verilmesi için bir Türkiye Ulusal Siber Olaylara Müdahale Ekibinin (TC-SOME) kurulması gerektiği savunulmaktadır. Bununla birlikte merkezi bir ulusal siber tehdit ve korunmasızlık inceleme laboratuvarı kurulması ve bu laboratuvarda zararlı yazılımların incelenmesi ve yerli ve yabancı donanımların tasnifi ve derecelendirilmesinin yapılması önerilmektedir. Belgede ithal edilen donanımlarda bulunabilecek arka kapılara, yerleştirilmiş kötücül yazılımlara ve diğer güvenlik açıklarına değinilmekte ve ulusal donanım, ulusal bir işletim sistemi (OS), arama motoru ve internet tarayıcılarının geliştirilmesi çağrısında bulunmaktadır[33]. Ayrıca Savunma Sanayii Müsteşarlığı altında siber güvenlik alanında Ar-Ge yapmak ve koordinasyon sağlamak amacıyla bir Siber Güvenlik Mükemmeliyet Ağı kurulması önerilmektedir.

Bilgi Güvenliği Derneği'nin taslak belgesi ulusal kritik altyapı konusuna güçlü bir vurgu yapan ilk raporlardan[34] birisi olmuştur. Raporda kritik altyapılar şu şekilde tanımlanmıştır: "zarar görmesi veya yok olması toplumsal düzenin ve kamu hizmetlerinin devamlılığının sağlanmasında güçlük yaratacak; işlevlerini kısmen veya tamamen yerine getiremediğinde vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik faaliyetler veya hükümetin etkin ve verimli işleyişine olumsuz etki edecek yapıdır"[35]. Rapor aşağıda listelenen sektörlere ait yapıları kritik altyapı olarak değerlendirmektedir; bilişim, enerji, mali işler, sağlık, gıda, su, ulaşım, savunma, kamu güvenliği ve nükleer, biyolojik, kimyasal tesisler. Raporda aynı zamanda, kritik altyapıya sahip tüm kurumların her sene düzenlenen ulusal siber güvenlik tatbikatlarına katılmasının gerektiği ve 2013 sonuna kadar kritik altyapı işleten tüm kamu kurumu ve özel kuruluşlarının bünyesindeki bilişim teknolojisi altyapılarının 2013 sonuna kadar Bilgi Güvenliği Yönetim Sistemi standardına (TS ISO/IEC 27001) uyumlu hale gelmesinin gerektiği belirtilmektedir.

2.2.4. Siber Güvenlik Kurulu

Raporun çizdiği rotada atılan ilk adım 20 Ekim 2012 tarihinde 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin" Bakanlar Kurulu Kararı ile atılmıştır. Bu karar "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla"[36] Siber Güvenlik Kurulu'nu kurmuştur. Ulaştırma, Denizcilik ve Haberleşme (UDH) Bakanı'nın başkanlığını yaptığı Kurul, Dışişleri, İçişleri, Milli Savunma, UDH Bakanlıkları müsteşarlarının yanı sıra, Kamu Düzeni ve Güvenliği Müsteşarı, MİT Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, BTK Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ve UDH tarafından belirlenen bakanlık ve kamu kurumu üst düzey yöneticilerinden oluşmaktadır.

2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na aşağıdaki görevler verilmiştir[37]:

- Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak.
- Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak.
- Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik altyapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak.
- Ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmalar yapmak.
- Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak.
- Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini

planlamak, koordine etmek ve yürütmek.

- Bu Karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapmak.
- Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek.
- Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek.
- Siber Güvenlik Kurulunun sekretarya hizmetini yürütmek.

Ertesi sene Siber Güvenlik Kurulu ülkenin ilk Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı[38] yayınlamıştır ve plan 2013/4890 sayılı 25 Mart 2013 tarihli Bakanlar Kurulu Kararı ile yürürlüğe girmiştir. Eylem planında kritik altyapılar şu şekilde tanımlanmaktadır:

"İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- Can kaybına,
- Büyük ölçekli ekonomik zarara,
- Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına,

yol açabilecek bilişim sistemlerini barındıran altyapılar"[39].

Eylem planında çoğu kritik hizmet ve altyapının internet bağlantısı olması ve faaliyetlerini sürdürmek için bilişim sistemlerine bağlı olmalarından ötürü kritik altyapıların siber tehditlere açık olduklarını belirtilmektedir. Ayrıca Türkiye'deki güvenlik zaaflarının, siber uzayın tabiatında bulunan sistemle ilgili güvenlik açıklarının yanı sıra, toplum genelinde, kurumlarda ve yüksek düzeyli yöneticiler arasında siber güvenlik hakkındaki bilgisizlikten kaynaklandığına dikkat çekilmektedir. Eylem planı bunların yanı sıra, bilişim sistemleri altyapısı, uzmanları ve koordinasyon eksikliğine ve ulusal ve uluslararası mevzuatın yetersizliğine değinmektedir.

2013-2014 eylem planı, 2012'de gerçekleştirilen çalıştayın tavsiye raporunun üstüne ilave tavsiyeler eklemiş ve toplamda 29 adet eylemin gerçekleştirilmesi için planlama yapmıştır. Bu iddialı eylem planları pek çok paydaşı kapsamaktadır; bunların arasında bakanlıklar, araştırma kurumları, özel sektör ve ülkenin siber güvenliğini korumakla görevli kurumlar bulunmaktadır. Kritik altyapılar eylem planında ekseriyetle vurgulanmıştır. 5 numaralı eylem, kritik altyapılarda yürütülecek bilgi güvenliği programına değinmektedir ve siber saldırıların doğrudan hedefi

olabilecek kritik altyapıları belirleme ve belirlenecek bir kritik altyapının sektörel risk analizinin yapılması görevlerini TÜBİTAK'a vermektedir. Ayrıca kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar, sektörel risk analizi yöntemlerinin ve sektörel acil eylem planlarının gereksinimlerinin belirlenmesi, yıllık risk analizi raporlama çalışmalarının yapılması ile sektörel iş sürekliliği planlarının gereksinimlerinin ve sektörel güvenlik önlemlerinin belirlenmesi ve uygulanmasından mesul olmuştur[40]. Bununla birlikte 10 numaralı yazılım güvenliği programının yürütülmesi eylemi ile TÜBİTAK, kritik altyapılarda kullanılmak üzere geliştirilen yazılımlar için güvenlik yazılım geliştirme temel kuralları dokümanının yayımlanması ve "kritik altyapılar için geliştirilen yazılımların güvenlik değerlendirmeleri kapsamında ilgili kurumların bünyesinde gerekli teknik isterlerin uygulanması ve kontrolüne yönelik fizibilitenin hazırlanarak Siber Güvenlik Kuruluna sunulmasından"[41] sorumlu tutulmuştur.

Kritik altyapıyı güçlendirmenin yanı sıra, bazı eylem maddeleri, vakaların olası etkilerinin en aza indirilmesi ve dirençliliğin geliştirilmesi üzerinedir. 16 numaralı eylem ile UDH veri sızmasını tespite yönelik test altyapısı geliştirilmesi ve uygulamaya alınmasından ve 14 numaralı eylem ile iş sürekliliği ve veri yedekleme sistemleri kurulmasından sorumlu tutulmuştur. Ayrıca TÜBİTAK ve Türk Standardları Enstitüsü ile siber güvenlik alanındaki ürünlerin ve hizmet sağlayıcıların sertifikalandırılmasından sorumludur.

Eylem planının en büyük önceliklerinden biri ülkenin beşeri sermayesinin geliştirilmesidir. En az 9 adet eylem, siber güvenlik alanında bilgilendirme ve yetkinlik kazandırılması üzerinedir. Örneğin, bu eylem maddeleri, farkındalığın artırılması, bilişim sistemleri uzmanları yetiştirilmesi, siber güvenlik tatbikatları ve etkinlikleri düzenlenmesi, konu üzerine verilen derslerin ve bölümlerin artırılması gibi eylemleri içermektedir. Bununla birlikte 11 numaralı eylemle BTK'ya siber tehditlerin tespit edilmesi, izlenmesi ve önlenmesi için mekanizmalar geliştirmesi görevi verilmiştir; buna tehditlerin tespit edilmesi amacıyla bir bal küpü sisteminin geliştirilmesi de dâhildir.

Bir diğer vurgu, üniversitelerde Ar-Ge laboratuarları kurulması, proje teşviği sistemlerinde siber güvenliğin öncelikli konular arasına eklenmesi, kamu kurumları, özel kuruluşlar, devlet dışı kurumlar, üniversiteler ve bilişim uzmanları ile siber güvenlik alanında milli ürünler ve çözümler yaratılması için düzenli faaliyetlerde bulunulması gibi yöntemlerle siber

güvenlik alanında milli teknolojilerin geliştirilmesi üzerinedir. Strateji belgesinde aynı zamanda ulusal mevzuattaki yetersizliğe değinilmekte ve Adalet Bakanlığı ve ilgili bakanlıklara ihtiyaç duyulan düzenlemelerin belirlenmesi için çağrıda bulunulmaktadır. Ayrıca Türk Dil Kurumu'na siber güvenlik terimler sözlüğü yaratma görevi verilmiştir.

2.2.5. Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın bir getirisi de tehditlerin fark edilmesi ve uyarıların geliştirilip paylaşılması amacıyla kurulan bir Siber Olaylara Müdahale Merkezi kurulması olmuştur. Strateji belgesi, TİB'in denetimi altında "ülkemizi etkileyebilecek tehditlere karşı 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi[nin] (USOM)" ve USOM'un koordinasyonunda çalışacak sektörel "Siber Olaylara Müdahale Ekipleri[nin] (SOME)"[42] kurulması çağrısını yapmıştır. USOM ayrıca kritik altyapı sektörleri ve kamu kurumları için sektörel SOME'ler kurmakla ve bunlara eğitim ve koordinasyon sağlamakla görevlidir.

11 Kasım 2013 tarihinde, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği yayınlamıştır[43]. Tebliğe göre bakanlıklar kendi kurumsal SOME'lerini ihtiyaç doğrultusunda, alt birimlerini ve ilgili kurumları kapsayacak şekilde kurmalıdırlar. Diğer tüm kamu kurumları, alt kuruluşlar, bakanlıkların ilgili birimleri ile özel kurum ve kuruluşlar kendi kurumsal SOME'lerini kurabilirler. Hedef, kritik altyapı işleten firmalara ve kendi bilişim teknolojileri birimleri olan bütün bakanlıklara ve diğer kamu kurumlarına birer kurumsal SOME kurmaktır. Ocak 2015 itibariyle 720 personelle işletilen 245 kurumsal SOME kurulmuştur[44]. Kurumsal SOME'lerin kurulmasını koordine etme görevi UDH'ye verilmiştir.

Siber Güvenlik Kurumu tarafından belirlenecek kritik sektörlerin sektörel SOME'leri olması mecbur kılınmıştır. Düzenleyici ve denetleyici kurumların sektörel SOME'leri BTK tarafından koordine edilmektedir. Şu ana kadar 6 adet kritik sektör belirlenmiştir; bunlar, bankacılık ve finans, ulaştırma, enerji, kritik kamu hizmetleri, su yönetimi ve elektronik haberleşmedir[45]. Kritik altyapı işleten kamu ve özel kuruluşların sektörel

SOME'ler altında çalışacak kurumsal SOME'ler açma yükümlülüğü vardır.

Bütün SOME'lerin 7/24 esasıyla çalışması ve kanun dışı olabilecek her faaliyeti yargı birimlerine ve USOM'a anında haber vermesi gerekmektedir. SOME'ler, siber saldırılara karşı gerekli tedbirleri almak, müdahale ve olay kayıt sistemleri kurmak ve kurumlarının bilgi güvenliğini sağlamakla yükümlüdürler. Eğer bir olay müdahale yeteneklerinin ötesindeyse sektörel SOME'lere ve/veya USOM'a yardım için başvurabilirler. Ayrıca USOM, SOME'lere eğitim vermekle yükümlüdür ve gerekli görmesi halinde kurumsal ve sektörel SOME'lerle doğrudan çalışabilir. Uluslararası kurumlarla veya uluslararası denk birimlerle işbirliği USOM tarafından yürütülür. Halihazırdaki kurumsal yapısına göre USOM şu konularla ilgilenen 5 birimden oluşmaktadır; siber olay raporlaması ve iletişim, zararlı yazılım analizi, kurumlar arası işbirliği, yazılım geliştirilmesi ve uluslararası iletişim[46]. Kurum 2014 başı ile 2015 senesinin Ocak ayı arasında kamu kurumlarını ve özel sektörü hedef alan 1500'den fazla olay tespit etmiştir.

Birçok açıdan bakıldığında, USOM Türkiye'deki kritik altyapının korunmasının asli kurumu olmak ve siber güvenlik krizlerinin yönetimini üstlenmek için iyi bir aday konumundadır. Ancak USOM, diğer kamu kurum ve kuruluşlarını yönlendirmek için gerekli koordinasyon yetkisiyle donatılmamış durumdadır. Oysa ülke çapında gelişebilecek siber güvenlik krizlerinin çoğunluğunun yönetimi kapsamlı bir iletişim, işbirliği, koordinasyon ve yeni politika uygulamalarını gerekli kılmaktadır. Ulusal SOME'nin de böyle bir görevi yerine getirebilmek üzere tasarlanmadığı görülmektedir.

Diğer yandan, enerji dağıtımı, su işleme, ulaştırma, kimyasal, yönetim, savunma ve gıda süreçlerini de içeren kritik altyapının çoğunluğu, endüstriyel süreçlerin önemli bir parçası olan endüstriyel kontrol sistemleri (SCADA dâhil) üzerinde çalışmaktadır. Bu Endüstriyel Kontrol Sistemlerini güvenlik altına almak, içinde sektörel farklılıkları görebilmeyi de gerektiren özel bir uzmanlığı zorunlu kılmaktadır. Bu türdeki bir özel uzmanlık ihtiyacı pek çok devleti Endüstriyel Kontrol Sistemleri Siber Olaylara Müdahale Timleri (EKS–SOME) kurmaya zorlamaktadır. Türkiye, kritik altyapı korunmasına odaklanabilecek bir EKS–SOME'ye sahip değildir.

2.2.6. Afet ve Acil Durum Yönetim Başkanlığı (AFAD)

Öte yandan, Türkiye'de Siber Kriz Yönetimi ve Kritik Altyapı Koruması görevi 5902 sayılı kanunla Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı'na (AFAD) verilmiştir. Kanunda AFAD'ın görevi afetlerle, hem afet esnasında hem de sonrasında mücadele eden kurum ve kuruluşlar arasında koordinasyonu sağlamak ve bunu düzenleyecek politikaları geliştirmek şeklinde tanımlanmaktadır. AFAD bu çerçevede bir eylem planı hazırlayarak afetleri başlıca iki gruba ayırmıştır: doğal afetler ve teknolojik afetler. Kritik altyapı koruma ve siber güvenlik konuları, bu bağlamda teknolojik afetler kategorisinde yer almaktadır. AFAD, Kritik Altyapı Koruma Planı çerçevesinde aralarında çeşitli bakanlıkların da bulunduğu 12 kurum ve kuruluşu bu sürecin kilit üyeleri olarak belirlemiştir. Bunlar: İçişleri, Çevre ve Şehircilik, Enerji ve Tabi Kaynaklar, Sağlık, Ulaştırma, Denizcilik ve Haberleşme ile Bilim, Sanayi ve Teknoloji bakanlıkları ve Enerji Piyasası Düzenleme Kurumu, Türkiye Atom Enerjisi Kurumu, TÜBİTAK, Jandarma Genel Komutanlığı, Kamu Düzeni ve Güvenliği Müsteşarlığı ve Hacettepe Üniversitesi'dir. AFAD, koruma sürecinin temel aşamalarını tanımlamak için Eylül 2014'te 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'ni yayınlamıştır. Belgede gereksinimler ve bunların gerçekleştirilmesi için öngörülen eylemler belirlenmiştir. Tanımlanan gereksinimler şunlardır:[47]

- Yetkili (sorumlu) otoritelerin belirlenmesi.
- Yetkili koordinasyon otoritesinin belirlenmesi, iş bölümü bazında kritik altyapı sektörleri (KAS) belirlemekte kullanılacak kıstasların tespit edilmesi.
- Avrupa Birliği Direktifi ile uyumlaştırılması ile ilgili taslak yönetmelik hazırlanması ve kapsam, büyüklük ve zaman etkisi faktörlerinin göz önünde bulundurularak kritik altyapılarının belirlenmesi ve koruyucu tedbirlerin arttırılması.
- Kritik altyapıların etkin korunması, ulusal seviyede veya AB seviyesinde bütün ilgili paydaşlar arasında iletişim, koordinasyon ve işbirliği.
- KAS'larla ilgili işletmeci güvenlik planı yapılması.
- Güvenlik irtibat görevlisi atamak.
- Eğitim programı oluşturulması ve uygulanması.
- Ulusal düzeydeki kritik altyapıların korunması amacı ile Kritik Altyapı

Koruma Planı hazırlanması.

- En iyi uygulamaların ve anlık tehdit ve alarmların güvenli bir şekilde paylaşımı yoluyla, uygun koruma tedbirlerinin geliştirilmesini teşvik edebilecek AB Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) çalışmalarına entegrasyon.
- Raporlama.

Yol Haritası Belgesi'nde, yerine getirilmesi planlanan görevler için 2016 en yakın, 2018 ise en uzak tarihler olarak belirlenmiştir. Yol Haritası AFAD'ın herhangi bir siber güvenlik krizini nasıl yöneteceğine açıklık getirilmemektedir.

2.3. Silahlı Kuvvetlerin Siber Güvenlik Mekanizmaları

Türkiye'de kamu kurum ve kuruluşları ile özel sektör unsurlarına yönelik olarak özellikle Estonya ve sonrasında Gürcistan'a karşı gerçekleştirilen siber saldırı fırtınası sonrasında artan siber saldırılar, idareyi, siber saldırıları bir tehdit olarak tanımlama yönünde adım atmaya zorlamış ve süreç sonunda da ulusal siber güvenlik stratejisini inşa etmenin yolunu açmıştır. Milli Güvenlik Kurulu da siber güvenliği bir tehdit olarak tanımlayarak tehdidi "Kırmızı Kitap" olarak adlandırılan askeri strateji belgesine eklemiştir. Bu sırada NATO 17 Mayıs 2010'da siber güvenliği üye ülkelere yönelik bir tehdit olarak tanımlayan yeni strateji belgesini açıklamıştır. [48]

Türkiye'nin siber ordusu olarak bilinen Siber Savunma Komutanlığı'nın oluşturulması kararı da bu dönem denk gelmektedir. Ülkeyi siber saldırılara karşı savunmayı amaçlayan Komutanlık, Savunma Bakanlığı, TÜBİTAK ve Orta Doğu Teknik Üniversitesi işbirliğinde Genelkurmay Başkanlığı bünyesinde görev yapacak özel bir birimi şeklinde planlanmıştır.

Takip eden dönemde, Siber Güvenlik Kurulu'nun kurulmasıyla birlikte Türk Silahlı Kuvvetleri (TSK) de Haziran 2012'de Siber Savunma Merkezi Başkanlığını kurmaya karar vermiştir. Bu yapılanma, bir siber komutanlık olmaktan çok uzak olmakla birlikte, TSK'ya destek olan bir SOME merkezi niteliğinde olması nedeniyle iyi bir başlangıç olarak kabul edilebilir. TSK 2013'te, Ulusal Siber Güvenlik Stratejisi'nin ilanını takiben de Siber Savunma Komutanlığı'nın kuruluşunu ilan etmiş ve görevlerini

şöyle tanımlamıştır;

1. TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunması sağlamak.
2. Siber olaylara 7/24 esasına göre müdahale etmek.
3. Ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak etmek.
4. TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütmek.
5. TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapmak.

Muhabere ve Elektronik Bilgi Sistemleri (MEBS) Destek Komutanlığı, Haziran 2012'de TSK Siber Savunma Merkezi Başkanlığı'nın kurulmasıyla takviye edilmiştir. Daha sonra Başkanlık Ağustos 2013'te MEBS ve Siber Savunma Komutanlığı olarak yeniden düzenlenmiştir.[49] MEBS ve Siber Savunma Komutanlığı'nın yaklaşık 30 personel ile faaliyet gösterdiği, albaylık seviyesinde komuta edildiği, 7/24 usulüne göre çalıştığı ve temel olarak siber saldırılara yanıt verdiği ve TSK ağ ve sistemlerini test ettiği basında yer almıştır. [50]

TSK'nın siber komuta konusunda küresel yaklaşımdan çok daha farklı bir yaklaşıma sahip olduğu anlaşılmaktadır. Sonrasında basına yansıyan haberlere bakıldığında, Komutanlığın, TSK'nın altyapısını korumak amacıyla istihbarat topladığı da anlaşılmaktadır.[51] Siber Savunma Komutanlığı'nın bir üyesinin değerlendirmeleri ışığında, TSK'nın, siber güvenlik yönetimini üç katman halinde yapılandırdığı anlaşılmaktadır. Bu hiyerarşinin en üst aşamasında politika ve karar alma süreçlerinden sorumlu olan TSK Siber Savunma Yönetim Kurulu bulunmaktadır. İkinci seviyede yer alan TSK Siber Savunma Komutanlığı ise üçüncü seviyedeki Genelkurmay Başkanlığı ile kara, hava ve deniz kuvvet komutanlıkları ve Sahil Güvenlik Komutanlığı ve Jandarma Genel Komutanlığı siber birimlerini yönetmektedir.

TSK'nın yürüttüğü askeri siber operasyonların temel sorunu asimetrik saldırılara simetrik ve hiyerarşik bir yapıyla karşılık verilmeye çalışılmasıdır. TSK, kara, deniz ve hava merkezli angajman stratejilerine odaklı bir yapılanma olması nedeniyle çeşitli sorunlarla karşı karşıya kalmaktadır. Bunun önüne geçilerek daha güçlü bir duruş sergilenebilmesi için TSK'nın hibrit tehditlere dinamik biçimde cevap verebilecek yeni bir

yapılanmayı tasarlaması ve bununla uyumlu yeni stratejiler geliştirmesi gerekmektedir. Bu bağlamda TSK Siber Savunma Komutanlığı'nın sorumluluklarının ve ulusal siber güvenlik yapılanması içindeki rolünün açık bir biçimde tanımlanmamış olması da sorun yaratmaktadır. Bu muğlaklığın yanı sıra, TSK'nın yüklenicilerin oynadıkları rolü ve sosyal mühendisliği hafife aldığı da söylenebilir. Oysa hackerların, yükleniciler üzerinden TSK'nın kullandığı yazılım ve donanım hakkında bir takım bilgi ve referanslara ulaşması mümkün olabilir.TSK'nin personel yönetimi politikasının da, Siber Savunma Komutanlığı'nda deneyim kazanmaya engel teşkil edebileceği görülmektedir. Tecrübeli siber güvenlik personelini komutanlıkta tutmak için, TSK personel yönetimi politikasını ve de özel sektörle rekabet edebilmek için sağladığı maaş ve imkanları gözden geçirmelidir. TSK, uzun vadede, genç ve parlak beyinleri kendi hizmetine nasıl çekebileceğini düşünmelidir.

Bunun yanı sıra TSK 2014'te Siber Güvenlik konusunda bir Proje Tanımlama Dokümanı hazırlamış ve bu belge Milli Savunma Bakanlığı tarafından onaylanmıştır. Bu belgeye göre, TSK, Siber Komutanlığı için sadece milli yazılım ve donanım tedarik edecek ancak bu yazılım ve donanım NATO ile ortak tatbikatlarda kullanılmaya uygun olacaktır[52]. Siber Komutanlık, Türkiye'nin NATO'nun 17-21 Kasım 2014 tarihleri arasında düzenlediği Siber Koalisyon 2014 tatbikatına katılımını koordine etmiş ve tatbikatta yer almıştır[53]. Söz konusu belgede ayrıca Muhaberat ve Siber Güvenlik Komutanlığı'nın personel sayısının 80'e çıkartılarak genişletileceği de belirtilmiştir[54].

2.4. Emniyet Genel Müdürlüğü'nün (EGM) Siber Güvenlik Yapısı

Emniyet Genel Müdürlüğü (EGM) ilk Bilgisayar Suçları ve Bilgi Güvenliği Kurulu'nu Nisan 1998'de kurmuştur. Bu kurul, bilişim suçlarının kapsamının belirlenmesi, ulusal ve uluslararası mevzuatın incelenmesi, bilişim teknolojilerinin kullanılmasıyla işlenecek suçların çeşitleri ve araçları arasındaki farklılıkları belirlenmesi ve EGM'deki birimlerin görevlendirilmesi amacıyla Mart 1999'da kurulan Bilgi Suçları Çalışma Grubu'na ön ayak olmuştur[55]. Ancak EGM bu grup kurulmadan önce de siber suçlarla mücadele etmekteydi – buna 1997'de ülkenin ilk blog yazısı yargılaması da dahildir. Bu davada sanığın bir blog sayfasında polis şiddetini eleştirmesi başka bir şahıs tarafından polise ihbar edilmiş

ve sonrasında sanık terörle mücadele ekipleri tarafından tutuklanmıştır[56]. Sanık Türk Ceza Kanunu'nun 159/1 sayılı "devletin emniyet muhafaza kuvvetlerini alenen tahkir ve tezyif" suçlamasıyla yargılanmış ve mahkum edilmiştir.

2011 senesinde EGM siber suçlarla mücadeleye odaklanan, Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nı kurmuştur (birim Şubat 2013'te Siber Suçlarla Mücadele Daire Başkanlığı olarak yeniden adlandırılmıştır). Yakın dönemde bu birimin adı, Hacking Team isimli bir İtalyan firmasıyla kanun dışı telefon dinleme ve takip yapılması için anlaştığı iddiasıyla Türk medyasında yer bulmuştur.[57] Raporlara göre, EGM firmayla ilk olarak 2011'de iletişime geçmiş ve yıllar içerisinde sözleşmesini yenilemeye devam etmiştir. Sözleşmenin son yenilenmesi 2015 senesinin Şubat ayında olmuştur.[58] İddialara göre EGM şu ana kadar firmaya 440.000 Euro ödemiş ve karşılığında donanım, eğitim ve uzaktan kontrol ve veri enjeksiyonu yazılımı almıştır.

2.5. İstihbarat ve İstihbarata Karşı Koyma

Siber uzayın muğlaklığı güvenlik kavramlarını da etkilemektedir. Siber espiyonaj, siber casusluk ve siber istihbarat gibi kavramlar benzer anlamları nedeniyle sıklıkla birbirinin yerine kullanılmaktadır. Aslında, bunların tamamı benzer saldırı yöntemleri ve benzer teknolojilere bağlıdırlar. Ancak, siber saldırının failinin bir devlet mi yoksa bir örgüt mü olduğunu bulmak zorlu bir meseledir. Devletler siber uzayın belirsizliğini ya da sahipsizliğini kendi çıkarları için kullanmaktadırlar. Siber istihbaratın en temel özelliği, siber güvenlik tehditlerine yanıt verebilmek amacıyla çeşitli siber araçlarla bilgi toplamaktır.

Milli İstihbarat Teşkilatı (MİT), Türkiye'deki siber güvenlik tehditlerinin gerçekleşmeden engellenmesi için gerekli istihbaratı toplamaktan sorumlu birimlerden biridir. MİT'e bu alanda yetkiler veren 6532 sayılı "Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun" 26 Nisan 2014'te yürürlüğe girmiştir. Bu yeni yasa MİT'in görev ve sorumluluklarını şu şekilde yeniden tanımlamaktadır:

> "Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı

usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak."[59]

Yapılan kanun değişikliğinin, MİT'in kurumsal altyapısında nasıl bir değişiklik yarattığına dair açık bir bilgi olmamakla birlikte, son dönemlerde Teşkilat tarafından verilen iş ilanları iş bölümünde meydana gelen değişiklikler hakkında bazı ipuçları vermektedir. MİT'in iş ilanları sitesinden şu alanlarda çalışmak üzere uzmanlar arandığı anlaşılmaktadır: Sinyal Analizi ve Uygulamaları, Şifreleme ve Kripto Analizi, Siber Faaliyetler,[60] Uydu İletişimi, Coğrafi Bilgi Sistemleri (GIS), İşitsel-Görsel Data İşleme, Telekomünikasyon Sistemleri, Yazılım Geliştirme, İletişim Yazılımı Geliştirme, Donanım Geliştirme, Mobil Uygulama Geliştirme, Sistem Yönetimi, Ağ Yönetimi, Veri tabanı Yönetimi, Bilgi Güvenliği ve Internet Teknolojileri, Sistem Analizi, Mekanik Sistem Tasarlama, Sistem Desteği ve Eğitimi, Veri İşleme. Tüm bu uzmanlık talepleri MİT'in kurumsal yapısının siber istihbarat çerçevesi kurmak yönünde yeniden yapılandırıldığına işaret etmektedir.

6532 sayılı kanun değişikliğinden sonra, dönemin Başbakanı Tayyip Erdoğan yaptığı açıklamada TİB'in yeniden yapılandırılacağını ve bu görevin de MİT'e verildiğini belirtmiştir. Nitekim TİB'in başına MİT'in desteğiyle eski bir MİT çalışanı olan Ahmet Cemalettin Çelik başkan olarak atanmıştır. Bu son atama TİB ile MİT'in siber izleme de dâhil olmak üzere siber güvenlik konularında yakın işbirliği içinde faaliyet gösterdiklerine dair açık bir ipucu vermektedir. Ancak, bu yakın işbirliğinin, Türkiye'de siber güvenlik farkındalığını artırdığı ve gerçek anlamda siber savunma faaliyetini beraberinde getirdiği söylenemez.

2.6. Yakın Dönemdeki Gelişmeler

2013 senesinin sonunda Türkiye sızdırılan tapeler ve telefon konuşmalarıyla ortaya çıkan bir yolsuzluk skandalıyla sarsılmıştır. Müteakip aylarda pek çok sayıda ses kaydı yayınlanmıştır, ki bunların arasında Dışişleri Bakanlığı'nda yapılan oldukça hassas ve yüksek seviyeli bir toplantıdan alınan kayıtlar da bulunmaktadır ve bu kayıtların menşeinin araştırıldığı soruşturmalar 2014 senesinin başında TÜBİTAK ve BİLGEM'e uzanmıştır. Aralarında TÜBİTAK Başkan Yardımcısı ve BİLGEM Başkanı Hasan Palaz'ın da bulunduğu TÜBİTAK çalışanlarının

kayda değer bir kısmı görevlerini kaybetmiştir. Palaz, soruşturmaya dair yazdığı kitabında, 2014'ün ilk çeyreğinde TÜBİTAK idari personelinin yüzde 80'inin işten atıldığı ya da siyasi sebeplerle istifa etmeye zorlandığını iddia etmektedir.[61] 2015'e gelindiğinde, bu sayı 1000'den fazla bilim adamı ve araştırmaya erişmiştir. Bir diğer deyişle, TÜBİTAK çalışanlarının dörtte biri işlerinden ayrılmıştır. Palaz, bunun TÜBİTAK'ta ciddi bir kabiliyet ve uzmanlık kaybına yol açtığını savunmaktadır. Nitekim 2015 senesinin Mart ayında, BİLGEM yasadışı bir örgütün yargılandığı bir davada delil olarak sunulan ve kuruma analiz etmesi talebiyle iletilen dört sabit diski, kurumda, "dijital analiz incelemesi yapabilecek personel ekibinde son altı ay içerisinde yaşanan yoğun değişim sebebi ile söz konusu [talebe] yönelik uygun ve ehliyetli personel [bulunmadığı]" gerekçesiyle geri çevirmiştir.[62]

6 Şubat 2014 tarihinde Meclis 6518 sayılı torba yasayı onamıştır.[63] Yasayla, 4 Mayıs 2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"[64] üzerinde bazı değişiklikler yapılmıştır. Yeni torba yasa ile TİB, ulusal siber güvenlik faaliyetleri çerçevesinde içerik, yer ve hizmet sağlayıcılar ile diğer ilgili kurum ve kuruluşlar arasında siber saldırıların tespit edilmesi ve önlenmesi konusunda koordinasyon sağlamakla görevlendirilmiştir. Torba yasa ayrıca, 5 Kasım 2008 tarihli, 5809 sayılı Elektronik Haberleşme Kanunu'nda da değişiklikler yapmıştır.[65] Bu değişikliklerle birlikte, BTK'ya "siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirme"[66] sorumlulukları verilmiştir. Torba yasanın 106. maddesiyle Siber Güvenlik Kurulu siber güvenlik üzerine politikaların, stratejilerin ve eylem planlarının onaylanmasıyla görevlendirilmiştir. Siber Güvenlik Kurulu bu politikaların, stratejilerin ve eylem planlarının ülke çapında etkin bir biçimde uygulanması için gerekli kararları almak, kritik altyapıların belirlenmesi konusundaki tavsiyelerde son kararı vermek, siber güvenlik konusundaki düzenlemelerin bir kısmından veya tamamından muaf olacak kurum ve kuruluşları belirlemek ve yasa tarafından belirlenen diğer görevleri yerine getirmekle sorumlu tutulmuştur. Değişiklik ile Siber Güvenlik Kurulu'nun çalışma usul ve esasları Başbakanlık tarafından yayınlanacak yönetmeliklerle belirlenecektir.

Zaman içerisinde TİB'in siber güvenlik alanında yetkileri ve sorumlulukları da artmıştır. 2015 senesinin Mart ayında kabul edilen bir değişiklik TİB'e "yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Başbakanlık veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi"[67] hallerinde "internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi" kararını vermek yetkisini sağlamıştır. Bu süreçte TİB, içerik çıkarılması veya bir sayfaya erişimin engellenmesi kararını verdikten sonra, ilgili erişim, içerik ve alan sağlayıcıyı bilgilendirir ve sağlayıcıların da dört saat içerisinde talebi yerine getirmeleri gerekmektedir. Kanuna göre TİB'in kararının yerine getirilmemesi 50.000 ila 500.000 TL (19,000-190,000$) idari para cezasıyla cezalandırılır.

TİB'in aynı zamanda karar aldıktan sonra onay için 24 saat içerisinde sulh ceza mahkemesine başvurması gerekir; hâkimin ise kararını TİB'in başvurusunu aldıktan sonra 48 saat içerisinde vermesi gerekir. Hâkim TİB'in kararını onaylamazsa engelleme otomatik olarak kaldırılır. Diğer yandan eğer hâkim TİB'in içerik veya internet sayfalarına erişim engelleme kararını onaylarsa, içerik, hizmet ve erişim sağlayıcılarının "suçların faillerine ulaşmak için gerekli olan bilgiler[i]" hâkim kararı üzerine adli mercilere sunması gerekir; aksi takdirde para cezasıyla karşı karşıya kalırlar.[68] Erişim sağlayıcılarının TİB'in kararlarına uymak için gerekli tüm yazılım ve donanımı kendileri tedarik etmesi gerekir ve erişimin engellendiği yayınlara alternatif erişim yöntemlerine karşı önleyici tedbirler almaları gerekir.[69] Kanun, Erişim Sağlayıcıları Birliği'nin (ESB) kurulmasını sağlamıştır. Bu birliğe katılım TİB'in kararlarına ve kanuna uyumu sağlamak için mecbur kılınmıştır. Birlik üyelerinin TİB'in kararlarına uymak için gerekli tüm yazılım ve donanımı tedarik etmeleri zorunludur. Özetle 2015'te yapılan değişikliklerle TİB içeriğe ve internet sayfalarına erişimi hızlıca sağlama yetkisi kazanmış ve kararlarına uyulmasını sağlamak için güçlü mali ve yasal caydırıcılar elde etmiştir.

3. Devlet Dışı Aktörler: Yerli Hacker Grupları ve Saikleri

Türkiye menşeli hackerlar uluslararası siber saldırılarda da rol oynamaktadırlar. Ancak bu grupların profilleri hakkında gelecekte kaynak olarak kullanılabilecek hiçbir araştırma yoktur. Türk hackerların kabiliyetlerinin anlaşılması, ülke içinden kaynaklanan tehditlerin anlaşılabilmesi için elzemdir. Son yıllarda devletler, alışılagelmiş internet altyapısını değiştirerek, bağlanabilirliğin kısıtlanması ve intranet bağlantıların kullanılmasına imkan verilmesi fikirlerine destek vermeye başlamışlardır.

Aşağıdaki özellikler Türkiye'deki tipik bir hackerı betimlemektedir:

- 14-45 yaşlar arasında ama ekseriyetle 18-25 yaş aralığındadırlar.
- Çoğunlukla lise ya da üniversite mezunudur ancak hepsi bilgisayar bilimi mezunu değildir.
- Yeni hackerlar kabiliyetlerini hacker forumlarından öğrenerek elde ederler ve çoğunlukla basit hackleme araçları kullanırlar.
- %92'si erkek, %8'i kadındır.
- Çoğunlukla orta veya düşük gelir seviyeli ailelerden gelirler.
- Sosyal Mühendislik[70] ve Ters Mühendislik[71] saldırılarını tercih ederler.
- Ufak bir grup uydu verisi takibi, istihbarat gibi konularla ilgilenmektedir[72].

Türkiye'de internetin sivilleşmesiyle birlikte birkaç hacker grubu ortaya çıkmaya başlamıştır. Bu bölümde bu gruplardan yedi tanesine odaklanılacaktır: Ayyıldız, RedHack, B3yaz Hacker, Turk Hack Team, Cyber Warrior (Akıncılar), Türk Güvenliği ve PKK Hack Team.

3.1. Ayyıldız Tim

İnternet sitelerine göre Ayyıldız Tim 2002 yılında kurulmuştur. Grup hedeflerini yedi maddede sıralamıştır:

"1- Türkiye Cumhuriyeti Devletine, Tüm Kamu Kurum ve Kuruluşlarına yönelebilecek her türlü saldırıyı bertaraf etmek.

2- Türkiye karşıtı, Satanist, Pornografik, Anayasal düzeni değiştirmeye yönelik yayın yapan sitelerin, sistemlerin yayınlarını durdurmak.

3- Faydalı yayın yapan sitelere ve sistemlere gereken teknik desteği vermek.
4- Gov.tr,pol.tr,edu.tr,bel.tr gibi Türkiye Cumhuriyeti Devletini İnternette Temsil eden sistemleri korumak.
5- Karşı propaganda faaliyetleri yürüterek Türkiye Cumhuriyet Devletinin Manevi şahsını dünya milletleri arasında hak ettiği yere getirmek.
6- Gereken hallerde(Yönetim Kurulu Kararı)Ülkemize yönelen sözlü, yazılı ve fiili saldırılara şiddetle cevap vermek.
7- Kamuoyunun bilinçlenmesi adına İnformation admin eli ile yazılı açıklamalar yapmak."[73]

Ayyıldız Tim'in crackleme faaliyetlerine dair Zone-H[74] internet sitesinde 13.579 tane bildirim vardır. Zone-H tarafından kayıt altına alınan tahrif edilmiş sitelerden birisinde Ayyıldız Tim kendilerini aşağıdaki not ile Türkiye'nin Siber Ordusu ilan etmiştir:

"Biz Türkiye'nin sanal ordusuyuz.

Vatanımız için düşmanlar ile soğukta, karda, kışta nasıl savaşıyorsak sanal alemde de vatanımız uğruna savaşırız.

Asla yorulmaz. Asla pes etmeyiz. Birbirimizi destekler, iyi gününde kötü gününde hep bir oluruz.

Dinimize ve Türklüğe karşı kötü fikirlere sahip olan tüm devletlere sanal savaş açacağız.

Bu kötü fikirlere devam edecekseniz sanal savaşa hazır olun! Kimseden korkmayız!

Gerektiği yerde gereken cevabı veririz!

AYYILDIZ TiM
TURKiYE'NiN SiBER ORDUSU"[75]

Bu satırlarda ve ilkelerinde görüleceği gibi Ayyıldız, çoğunlukla devlet hedefleriyle işbirliği yapan ya da paralel bir hatta çalışan kendi ifadesiyle vatansever bir hacker grubudur.[76] Ancak Ayyıldız Tim'in altı üyesi site sahiplerine şantaj yaptıkları gerekçesiyle tutuklanmıştır. Ayyıldız Tim bu şahısların üyeliğini inkar etmiştir. Ancak grubun eylemleri ve suç unsuru teşkil eden faaliyetlerle bağlantılarına dair bazı şüpheler vardır.[77] Bu şüphelerin yanı sıra Ayyıldız Tim saldırılarında çoğunlukla devletçi bir duruş sergilemiştir. Özellikle Anonymous'un Türkiye'ye yakın dönemde

kitle halinde yaptığı saldırılara karşı Ayyıldız Tim'in Türkiye'yi savunması da, bu grubun Türkiye'nin gelecekte kurulacak nükleer tesisinin siber güvenliğine bir tehdit teşkil etmeyeceğini göstermektedir.[78]

3.2. RedHack

RedHack Türkiye'deki en bilinen hacker gruplarından biridir. Röportajlarının birisinde grubun lideri, RedHack'in 1997 senesinin Mayıs ayında kurulduğunu iddia etmiştir.[79] RedHack ideolojisini, eşit, adil ve sömürünün olmadığı bir dünya için hacklemeyi kullanmak olarak açıklamıştır.[80] RedHack aynı zamanda konumunu "[faşist] düzene kurşun atan her örgütün emrinde"[81] olarak belirtmiştir.

Zone-H internet sitesinde 2008'den başlayarak RedHack'e atfedilmiş bazı tahrif kayıtları mevcuttur.[82] Hack grubu, Ankara Emniyet Müdürlüğü'nün internet sitesine yaptıkları ilk saldırıdan ve ardından Türk kamuoyuna yaydıkları gizli belgelerle üstüne daha çok ilgi çekmeye başlamıştır.[83] Grup 2013'de Gezi Parkı protestolarının ardından, devlet kurumlarına yaptıkları şiddetli saldırılardan sonra popülerlik kazanmıştır.[84] Başka bir saldırıdan sonra RedHack Ankara Emniyet Müdürlüğü'nde görev yapan polis memurlarının email hesap ve şifre bilgilerini yayınlamıştır. RedHack, bu saldırıların yanı sıra Emniyet Genel Müdürlüğü, Türk Futbol Federasyonu, Milli İstihbarat Teşkilatı, Türk Telekom, Hava Kuvvetleri Komutanlığı, Türk Hava Yolları, Yüksek Eğitim Kurumu ve Dışişleri Bakanlığı'nın sitelerini tahrif etmiş ve elde ettiği diplomatik görev mensuplarının kimlik bilgileri ve devlet kurumları arasındaki gizli iletişimler gibi gizli belgeleri yayınlamıştır.[85]

RedHack'in uluslararası hacker gruplarıyla işbirliği yapma kapasitesi vardır. 2013 senesinde RedHack ve Anonymous birlikte çalışarak İsrail İstihbarat Servisi'ne (MOSSAD) bir saldırı düzenlemişlerdir.[86]

3.3. B3yaz Hacker

Bu hacker grubu, beyaz hackerlara, yani çevrimiçi sistemleri daha güvenilir hale getirmek için üreticilere güvenlik açıklarını bildiren zararsız hackerlara bir referans olarak, isminde beyaz kelimesini farklı bir yazılışıyla kullanmıştır. Grup, B3yaz Hacker'ın internet sayfasında kadrolarının Pentest[87] taleplerine hazır olduğunu ilan etmiştir. Bu, Türkiye'de bir hacker

grubunun gerçek bir Pentest hizmeti için hackleme kabiliyetlerini sunduğu tek örneği teşkil etmektedir. Sızma testleri güvene dayalı olduğu için, firmalar, firmanın hassas bilgilerini koruma garantisi verebilecek güvenilir özel güvenlik firmalarını tutmayı tercih ederler.

B3yaz Hacker'ın saldırıları iki gruba ayrılabilir. İlk saldırı grubu internet sitelerine güvenlik açıklarını bildirmek için yapılanlardır. İkinci olarak ise grubun değer yargılarına aykırı içerik paylaşan internet sitelerine yapılan saldırılar vardır. Zone-H'de, B3yaz.org, B3yaz, B3yazHacker adları altında kayıtlar vardır; bunlar, çoğu 2015 senesinde farklı internet sitelerine yapılmış olan toplam 540 adet tahriften oluşmaktadır. B3yaz Hacker grubunun kabiliyetleri incelendikten sonra, B3yaz Hacker'ın Türkiye'nin kritik altyapısı ve nükleer enerji tesisleri açısından bir tehdit olarak değerlendirilemeyeceğini söylemek mümkündür.

3.4. Turk Hack Team

Turk Hack Team Türkiye'deki en teşekküllü ve iyi bilinen hacker gruplarından biridir. Turk Hack Team 2002'de kurulmuştur.[88] İnternet sitesi diğer hacker gruplara kıyasla en düzenli internet sitelerinden biridir; tarihçeden videolara, eğitimden e-kitaplara kadar birçok bölümü vardır. İnternet sitesinin tasarımı, Turk Hack Team yönetiminin bir topluluk kurup bunları internet sitesi aracılığıyla eğitmeyi hedeflediklerini göstermektedir. Son on yıl boyunca grup milliyetçi çizgisini korumuştur ancak artık dini imalara da yer vermektedir. Üyeleri grubu "Vatanını seven Müslümanlar" olarak tanımlamaktadırlar.

Grubun ilan ettiği hedefleri aşağıdakilerden oluşmaktadır:

> "1. Dilimize, dinimize, ülkemize, inançlarımıza, örflerimize, adetlerimize, toplum ahlakına ve bunlar gibi değerlere, aykırı yayın yapan sitelerin hayatına son vermektir.
> 2. Hack'in zevk için değil misyon için yapılacağını aşılamaktır.
> 3. Doğru, dürüst, ahlaklı ve yararlı yayın yapan sitelere yardımcı olmak ve onlara çıkar gözetmeden destek olmaktır.
> 4. Turk Hack Team Türk Vatanı için çalışır
> 5. Bu misyonu kabul eden Turk Hack Team üyelerine sorunları ile yardım için hiç bir şart gözetilmeyecektir."[89]

Turk Hack Team faal olan en büyük botnetlerden birisini kontrol

ettiklerini iddia etmektedir. Zone-H internet sitesinde Turk Hack Team'in farklı yazılışlarıyla birçok kaydı vardır, bu da kabiliyetlerini tam olarak anlamayı güçleştirmektedir. Ancak yakın dönemde Turk Hack Team'in lideri Zorrokin'in, Papa'nın Ermeni meselesi hakkındaki açıklamasından sonra Kutsal Makam'ın internet sitesine yaptığı saldırı, grubun yetkinliği ve potansiyeli hakkında bazı fikirler vermektedir.[90] Grubun son saldırısı 7 Haziran 2015 Türkiye genel seçimlerinden hemen önce New York Times gazetesinde Türk cumhurbaşkanının eleştirildiği bir makalenin yayınlanmasının ardından gazeteye yapılan saldırı olmuştur. Saldırı homedelivery.nytimes.com, es.nytimes.com, blog.nytimes.com, app.nytimes.com, register.nytimes.com adreslerini durdurmuş ve hosting sunucusuna zarar vermiştir.[91] Bu saldırının akabinde Turk Hack Team yine Türkiye cumhurbaşkanını eleştiren The Guardian gazetesine saldırmış ve gazetenin internet sitesini ve sunucusunu kısıtlı olarak kesintiye uğratmıştır.[92] Tüm bu saldırılar grubun kabiliyetleri konusunda ipuçları vermektedir. Bu grubun hükümet yanlısı eğilimleri, Türkiye'nin planlanan nükleer enerji tesislerine muhtemel bir tehdit unsuru olmayacağını göstermektedir.

3.5. Cyber Warrior (Akıncılar)

Cyber Warrior, diğer adıyla Akıncılar[93], 1999'da illegal-port adıyla kurulmuş bir gruptur. Daha sonra grubu Cyber Warrior olarak yeniden yapılandırmışlardır. Grubun hiyerarşisi ordu hiyerarşisiyle aynıdır. Eskiden yaptığı bir gönüllü toplama çağrısında grup kendisini bir kardeşlik yolu olarak tanımlamıştır.[94]

Üyelerinde aranan özelliklerini şöyle sıralamışlardır[95]:

- Din, örf, adet, ananelerimize sadık.
- Türk Milliyetçileri.
- Birlik üyeleri arasında bir kardeş bağı sağlayacak kişiler.
- Birlikteki kişiler başka bir oyuncuya küfür, argo söz, ağır laf sarf etmeyecektir. Birliğimizden birine yapılmış hakaret hepimize yapılmış sayılır.

Cyber Warrior internet sitesi, grubun Türkiye İnternet yasasının (No. 5651[96]) hazırlanması sürecinde aktif olduğunu iddia etmektedir, bu da Türk karar vericilere veya siyasi elite yakın oldukları anlamına gelebilir.

Türkiye'nin siber güvenlik yasasının (5651) ardından grup, görevlerini İnternet yasasına uygun olarak yeniden şekillendirmiştir:

- "TIM'in başlıca Amaç/Görevleri; İnternet üzerinden İnanç ve Ahlaki değerlerimize saldırı yapan, Saf beyinleri bulandırmaya yönelik içerikler bulunduran, Satanist ve Pornografik içerikli yayınlarla mücadeledir. Türkiye Aleyhtarı Yayınlar, Toplum ve kamu vicdanını Olumsuz Etkileyen Durumlar da (Bu Misyon'un Genel Prensibi Doğrultusunda) Misyon Kapsamındadır.
- TIM'in Genel Prensibine (Misyon'a) Uygun Yayın Yapan kurum, Site/ Grup ve Oluşumlara Güvenlik ve Diğer Teknik Detaylar Hakkında, Herhangi Bir Menfaat Gözetmeksizin Güvenlik Desteği Saglanır.
- Bizim değerlerimize saldırmadığı sürece hiç bir yayın mücadele kapsamına girmez."[97]

Grup aynı zamanda internet sitelerinin kurum bölümünde görevlerini detaylandırmıştır:

- "Cyber Warrior TIM'in hiç bir şekilde herhangi bir dernek, kurum, örgüt, parti, siyasal ya da ideolojik görüş ile bağı yoktur.
- TIM'e Kabul Edilen üye; Grup içinde Bilgi ve Uzmanlık Alanına Göre; Görev Organizasyonu' nda Görev Almak Üzere; Sorumlulukları ve Görev Tanımı Belirlenir ve Gruba Dahil Edilir."[98]

Cyber Warrior üyeleri bazı çevrimiçi forumlarda Türkiye'deki hiçbir internet sitesine saldırmadıklarını iddia etmişlerdir.[99] Cyber Warrior'ın davranış biçimindeki bu değişiklik, grubun Türk polisiyle farklı seviyelerde bağlantıları olduğu iddiasıyla örtüşmektedir.[100] Zone-H'te grubun 7895 tahrif kaydı vardır. Cyber Warrior mensupları diğer ülkelerin yanı sıra, İsrail, Mısır, Avusturya ve Ermenistan'a saldırmışlardır.[101]

Erişilebilen tüm kanıtlar grubun devletle güçlü ilişkileri olduğunu göstermektedir.[102] HP Siber Güvenlik Araştırmaları Siber Risk Raporu 2015 aşağıdaki kanıtlara dayanarak onları devlet destekli hacker grubu olarak sınıflandırmıştır:

> "Cyber Warrior ekibi tehdit aktör grubunun bir parçası olan Akıncılar hacker ekibinin üyeleri Türk polisi tarafından RedHack ve Türk veya İslami ideallere tehdit olarak algılanan diğer birimlere yaptıkları saldırılardan dolayı methedilmiştir. Akıncılar'ın bazı aktörleri Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği'nin yönetim

> kadrosundadır ve bu kurum gov.tr ve pol.tr domainlerine ücretsiz bilgi güvenliği yardımı yapmış ve devlet kurumlarına hassas bilgiler aktarmışlardır.Nisan 2012'de, grubun yöneticisi Gökhan Şanlı'nın da aralarında bulunduğu Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği temsilcileri, Beyaz Saray'ın Türkiye'deki dengi olan Çankaya Köşkü'nde düzenlenen, Türkiye'deki bazı internet sitelerine erişimin durdurulması ve entellektüel mülkiyet hakları üzerine bir toplantıya katılmıştır. Doktoray rumuzunu kullanan Şanlı, Cyber Warrior forumlarını yönetmektedir. Dogukan rumuzunu kullanan ve artık rahmetli olan Halit Uygur, Cyber Warrior TİM'de ve aynı zamanda İstanbul'daki Milli Eğitim Bakanlığı'nda kilit rol oynayan bir figürdü."[103]

Cyber Warrior grubunun faaliyetleri, Türkiye'nin nükleer enerji santrallerine bir tehdit olarak değerlendirilmeyeceklerini göstermektedir.[104] Ancak siyasi havadaki bir değişiklik, konumlarını ve davranışlarını değiştirebilir. Türk hükümetinin beklenmeyen saldırıları önlemek için grubun faaliyetlerini takip etmesi sağduyulu olacaktır.

3.6. Türk Güvenliği

Türk Güvenliği 2006 senesinde bilinen bir hacker ve grubun şimdiki lideri olan Agd_Scorp tarafından kurulmuştur. Türk Güvenliği fuse.microsoft.com, The Register[105] ve Vodafone'a yapılan saldırılar sonrası uluslararası olarak tanınmışlardır. The Guardian grubun faaliyetlerini şu şekilde tarif etmiştir:

> "Pazar gecesi bir Türk hacker grubu aralarında the Telegraph, UPS, Betfair, Vodafone, National Geographic, bilgisayar yapımcısı Acer ve teknoloji haberleri sitesi Register'a trafiği saptırmış ve farkında olmayan kullanıcıları şifreleri, e-posta hesapları ve diğer bilgilerinin çalınması riskine sokmuşlardır."[106]

The Guardian, saldırıdan sonra grupla röportaj yapmış, bu da grubun uluslararası ününü arttırmıştır.[107] Araştırma yapıldığı sürede Türk Güvenliği'nin internet sitesi faal olmamakla birlikte, Agd_Scorp'un Pastebin[108] internet sitesinde yaklaşımını kısaca netleştirdiği bir manifestosuna erişilmiştir:

> "Uğrunda savaşman gereken şey özgürlüktür. Dünya beni tanımayabilir. Ancak yeraltında kişiler benim kim olduğumu bilir ve bazıları yaptığım işleri bilir.

> Hep internette büyük kurumları hacklemeyi hayal etmiştim. Kısa bir süre sonra hayallerim gerçek oldu.
>
> Google, Microsoft, MSN, NATO, Nintendo, Sony, NASA, Kaspersky, Avast, AOL, Pentagon, TrendMicro, CocaCola, Peugeot, UNESCO, .mil domain'lerini, Yahoo, Playstation Network, UPS, National Geographic, Telegraph, The Register, spam.org, resellerclub.com, eNom ve hatta fbijobs.gov & interpol.com'u hackledim."[109]

Zone-H, Türk Güvenliği'nin 225 adet[110], Agd_Scorp'un da 424[111] tahrifini kaydetmiştir. Grup başlangıçta büyük oranda SQL enjeksiyon teknikleri[112] kullanmıştır ancak yeteneklerini ve yöntemlerini geliştirmiştir. Türk Güvenliği'nin ideolojisi net olmadığından hamlelerini öngörmek zordur; ancak bir durumda grup Suriye Elektronik Ordusu'nun (SEA) Türk hükümeti sitelerine yaptıkları phishing saldırılarına karşılık vermiştir. SEA aynı zamanda kendi internet sitesinde bazı Türk resmi belgelerini sızdırmıştır ve Türk Güvenliği yanıt olarak SEA'nın internet sitesini hackleyerek Kur'an'dan bazı ayetleri içeren bir mesaj bırakmıştır.[113] Türk Güvenliği'nin SEA'nın internet sitesine yaptığı saldırı ve bıraktığı mesaj, milliyetçi eğilimlerini kanıtlamıştır. Milliyetçi bir grup olduğundan Türk Güvenliği Türkiye'nin nükleer siber güvenliğine bir tehdit teşkil etmeyecektir.

3.7. PKK Hack Team

PKK Hack Team, Partiya Karkerên Kurdistanê (PKK) olarak da bilinen Kürdistan İşçi Partisi'nin bir koludur. PKK 1980'ler ve 1990'lar sürecinde yoğunlukla Kürt milliyetçisi bir hareket olmadan önce Marksist-Leninist bir örgüt olarak kurulmuştur. PKK Hack Team'in çevrimiçi faaliyetleri konusunda kısıtlı bilgi mevcuttur. Faaliyetlerine dair en eski haber, iki hackerın 2.307 devlet ve devlet dışı internet sitesini tahrif edip kendi imzalarını bıraktıkları 2006 senesine uzanmaktadır.[114] Polis, PKK destekçisi iki hacker tutuklamıştır. 2008 senesinde PKK'lı hackerlardan birisi Türk polisi tarafından Diyarbakır'da rutin bir arama yapılırken yakalanmıştır. Polis, hacker'ı taşıdığı ve çalıntı olduğu düşünülen dizüstü bilgisayar nedeniyle durdurmuş, ancak sonrasında şifrelenmiş gizli bilgiler, belgeler, pasaportlar, Poison Ivy isimli kötücül yazılım kodu ve Genelkurmay, Milli İstihbarat ve Jandarma'ya ait video kayıtları bulmuştur. Hacker'ın evininin buna müteakiben aranması sonucu polis

924 CD-ROM, 57 DVD, 22 sabit disk ve iki dizüstü bilgisayar ele geçirmiştir. Soruşturma bu bilgileri PKK genel merkezine taşıyan PKK'lı kuryenin tutuklanmasıyla sonuçlanmıştır.

Soruşturma esnasında, hacker, bütün bu bilgileri porno sitelerine kendi kötücül yazılımını yerleştirip, bu açıktan faydalanarak istihbarat servisi ve ordu mensuplarının bilgisayarlarına sızması sonucunda elde ettiğini itiraf etmiştir.[115] Hacker'ın becerileri ve PKK Hack Team'in örgütsel yetenekleri kolluk kuvvetlerinin dikkatini çekmiştir. 2011'de kolluk kuvvetleri PKK'lı hackerları tutuklamak amacıyla, Şanlıurfa, Hakkari, Batman ve Gaziantep'te operasyonlar düzenlemiştir.

PKK Hack Team'in Zone-H internet sitesinde iki farklı kaydı vardır. Zone-H sitesine göre bir tanesinde PKK Hack Team'in 279 adet tahrif[116], diğerinde de 241 adet tahrifi vardır.[117] Haziran 2015 seçimlerinden önce Türkiye'nin doğusunda HÜDAPAR ve PKK arasında artan gerilim[118], siber uzaydaki çatışmayı da arttırmıştır.[119] Bu çatışmalar yeni bir hacker örgütünü, T.A.K.'yi (Teyrenbazên Azadiya Kurdistan – Kürdistan Özgürlük Şahinleri) ortaya çıkartmıştır.[120] Bu grup çoğunlukla Twitter hesaplarını hedef almış ve düşük bir profil sergilemiştir.[121] Özetle, tüm PKK yanlısı hacker grupları nükleer enerji tesislerine tehdit teşkil ederler. Saldırı düzenlemek için başka hacker gruplarıyla ortak çalışabilirler. Dahası, PKK ve PKK Hack Team melez kabiliyetlerini kullanarak tesislere daha fazla zarar verebilirler. Kritik altyapıyı felç etmek için hem kinetik hem de siber saldırılar kullanma becerisine sahip tek örgüttürler. Dolayısıyla hem kamunun hem de özel sektörün grubu yakından takip etmesi gereklidir.

4. Sonuç: Ankara'nın Geleceğe Dair Planları

Türk siber suç dünyasının aslında çeşitli aktörlerin yoğun faaliyetleri nedeniyle adeta istila altında olduğu söylenebilir. Sadece 2014 yılının dördüncü çeyreğinde 199 farklı ülke ya da bölgeden kaynaklanan siber saldırılar söz konusu olmuştur. Türkiye'ye yönelik olarak düzenlenen siber saldırıların düzenlendiği ülkelerin başında Çin, ABD, Tayvan ve Rusya gelmektedir.[122]

Sonuçta, Türkiye'nin artan düzeyde bir siber suç dalgasına maruz kaldığı anlaşılmaktadır.[123] Türkiye, işlenen siber suçların sayısı bağlamında dünyadaki en fazla saldırıya uğrayan 20 ülke arasında 9. sıradadır. Türkiye, kötü niyetli bilgisayar faaliyeti bağlamında, küresel toplamın yaklaşık yüzde 3'ünü tecrübe etmektedir. Kötücül kod bağlamında ise 15. sıradadır. Saldırıların kaynaklandığı ülke sıralamasında 12. sırada yer alan Türkiye, zombie spam'da 5. ve phishing internet siteleri sunucularında da 24. sıradadır.[124] Türkiye, bu konuda hazırlanan bir raporda yapılan değerlendirmeye göre, dağıtılmış hizmet dışı bırakma saldırıları bağlamında 2014 yılının ikinci çeyreğinde 8. sırada yer almaktadır.[125] Bu bilgi ve rakamlar, sonuç olarak, Türkiye'nin gerçekleşen siber saldırılar bağlamında ciddiye alınması gereken bir düzeyde tehdit altında olduğunu göstermektedir. "Aşağı yukarı aynı nüfus büyüklüğüne ve nerdeyse iki kat daha fazla internet kullanıcısına sahip durumdaki Almanya'dan her bir 1.000 kullanıcı başına 37 kat daha fazla Sality ve 1.6 kat daha fazla Zeus Gameover virüsü bulaşması ile karşıya kalmaktadır."[126]

Elimizdeki bilgiler, siber suçluların "ilk önce en zayıf hedeflere yöneldiklerini" göstermektedir.[127] Hedef seçimi yapan muhtemel bir saldırgan için, öncelik, belirli bir ülkenin ya da o ülkedeki belirli bir sektörün güvenlik seviyesi olmaktadır. Bu bağlamda, saldırgan, girişiminin hem düşük maliyetli olmasını, hem de bu girişimin finansal, siyasi ya da farklı biçimlerde beklentileri karşılayacak geri dönüşlerinin olmasını hedeflemektedir. Bu beklentiler, açıkçası, daha güçlü ve etkin güvenliğe sahip hedeflere kıyasla zayıflarda daha yüksek oranda karşılanabilmektedir.

Böyle bir ortamda, ülkenin siber güvenlik programının önümüzdeki beş yıl için bir yol haritasını çıkarmaya çalışan Kalkınma Bakanlığı, 2014-2018 için "Bilgi Toplumu Stratejisi ve Eylem Planı" isimli bir taslak

plan yayınlamıştır. Planda Türkiye'nin siber güvenlik kabiliyetlerinin geliştirilmesi için beş iddialı eylem sıralanmıştır.[128] Bunlardan ilk ikisi, 2015 senesinin sonuna kadar 2000'lerin başından beri tartışılan Ulusal Bilgi Güvenliği Kanunu'nun çıkarılması ve Kişisel Verilerin Korunması Mevzuatı'nın onaylanması çağrısını yapmaktadır. Üçüncü önerilen eylem, 2016'da Siber Suçla Mücadele Stratejisi ve Eylem Planı'nın oluşturulmasıdır. Bu hedefle görevlendirilen kurumlar, Emniyet Genel Müdürlüğü, Adalet Bakanlığı, İçişleri Bakanlığı, Dışişleri Bakanlığı, Jandarma Genel Komutanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı[129] ve Telekomünikasyon İletişim Başkanlığı olmuştur. Dördüncü eylem, internetin güvenli kullanımı alanında en iyi uygulama kuralları konusunda farkındalığın arttırılmasıdır. Taslak belgede son olarak yer verilen eylem ise, 2015 sonuna kadar bilişim suçları konusunda uzmanlaşmış mahkemelerin kurulmasıdır.

Türkiye zaman içerisinde siber uzaydaki mevcudiyetini ve kabiliyetlerini geliştirmiş olsa da, bu bütün alanlarda aynı seviyede olmamıştır; bunun neticesinde bazı alanlarda büyük aşamalar kaydedilse de diğer alanlarda beklenen ilerleme kaydedilememiştir. Yine de, son birkaç senede siber güvenlik ile ilgilenen devlet kurumlarının sayısı artmıştır ve Türk güvenlik güçleri siber tehditlerle mücadeleye ek bir vurgu yapmıştır. Ayrıca bazı meselelerin siyasallaştırılması Türkiye'nin siber alandaki kabiliyetlerini geliştirme arzusunu zorlaştıran bir etken olmuştur; önemli taslak yasaların çıkartılamaması ve TÜBİTAK'ta ciddi boyutta beşeri sermayenin kaybedilmesi buna örnek teşkil etmektedir. Bunların neticesinde Türkiye siber güvenlik alanındaki hazırlıkları itibariyle, belli başlı müttefikleri ve hatta hasım devletlerin gerisinde kalmaya devam etmektedir.

Türkiye'de faaliyet gösteren hacker ve cracker grupları hakkında açık kaynak bilgi kısıtlıdır. Türkiye'nin nükleer tesislerine yönelik olarak tehdit oluşturabilecek unsurlar arasında nükleer karşıtı gruplar ve kurumlar ile yalnız kurt olarak nitelenen siber suçlulara dönüşebilecek bireyler yer almaktadır. Bunlar arasında Redhack gibi yerel hacker grupları ve siyasal hedeflere sahip PKK uzantısı PKK Hack Team gibi terörist yapılanmalar yer almaktadır. Bu bağlamda Türk siber suç dünyası ile ilgili olarak dikkati çeken ilgi çekici bir nokta, siyasal otorite ve devlet yapılanmalarıyla mesafe ve ilişkilerine bağlı olarak, devlet açısından kabul gören ya da kabul görmeyen faaliyetlerde bulunan rakip grupların çeşitliliğidir. Bunun en bilinen ve güzel örneği, kendisini Marksist sosyalist bir grup

olarak tanımlayan Redhack grubu ile kendisini "devlet yanlısı" olarak tanımlayarak görevinin Türkiye'nin kamu kurum ve kuruluşlarını ve devletin çıkarlarını savunmak olduğunu belirten Avustralya kaynaklı Ayyıldız Team arasındaki rekabettir.

Bu türde bir ayrımlaşma Türkiye'nin kritik altyapısını savunmakla görevli kurum ve kuruluşlar açısından kabul edilebilir bir durum değildir. Farklı isimler altında da olsa siber "operasyonlarla" meşgul olan bu tür grupların öncelik, niyet ve güdülerinin zamana ve gelişmelere bağlı olarak değişiklik gösterdiği gerçeği göz önüne alındığında, bu grupları siyasi öncelikleri ve duruşları bağlamında sınıflandırmak ve buna göre muamele etmek açıkça siber güvenlik zafiyetlerinin artmasına neden olacaktır. Ayrıca, farklı suç ya da terör ağlarının zaman zaman benzeşen çıkarlara bağlı olarak geçici bir takım ortaklıklara gidebildiği örnekler de bulunmaktadır. Bu bağlamda, rakip devletlerin bu türde yapıları desteklemeleri ya da bu grupların kimlikleri ardına gizlenerek doğrudan düşmanca siber saldıralar düzenlemeleri ihtimali de Türkiye'nin tehdit görünümünü daha da karmaşıklaştırmaktadır. Son olarak, nükleer enerji santrallerinin uluslararası ortaklarla birlikte girişilen projeler olduğu dikkate alındığında, Türkiye'nin ortaklarının zafiyetlerini/çıkarlarını hedefleyen siber saldırıların gerçekleştirilmesi ihtimali de göz ardı edilmemelidir.

1- Libicki, M. C. (2009) "Cyberdeterrence and Cyberwar" Rand Corporation

2- International Telecommunications Union (Geneva) (2014) "Percentage of Individuals Using the Internet 2000-2013", http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls, Erişim tarihi: 9 Kasım 2015.

3- Bloomberg (2013, Nisan 23) "Top Ten Hacking Countries"

4- TBMM "3765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun", Kanun No. 3756 Kabul Tarihi 6.6.1991 (Resmi Gazete ile yayımı: 14.6.1991, Sayı: 20901) http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf ayrıca bakınız: http://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d18/c061/b127/tbmm180611270516.pdf, Erişim tarihi: 16 Temmuz 2014.

5- Türk Ceza Kanunu (2004, Eylül 26) Kanun no. 5237

6- Dokurer, S. (2002) "Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri" EGM Bilgi İşlem Daire Başkanlığı Bilişim Suçları Büro Amirliği, http://bilisimsurasi.org.tr/dosyalar/17.doc, Erişim tarihi: 23 Eylül 2014.

7- 15 Temmuz 2003'te yapılan değişiklikler ile terörün tanımı üzerine olan birinci madde şu şekildedir: "Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir."

8- Bunların arasında 113 sayılı kamu kurumu faaliyetlerinin engellenmesi, 142 sayılı nitelikli hırsızlık (bu maddenin 142.2.e bandında bilişim sistemlerinin kullanılmasına özellikle atıfta bulunulmaktadır), 151 ve 152 sayılı mala zarar verme ve mala zarar vermenin nitelikli halleri, 170 sayılı genel güvenliğin kasten tehlikeye sokulması, 213 sayılı halk arasında korku ve panik yaratmak amacıyla tehdit, ve belki de, 172 sayılı radyasyon yayma ve 173 sayılı atom enerjisi ile patlamaya sebebiyet verme vardır.

9- Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" International Journal of Information Security Science Cilt.1, Sayı. 4

10- T.C. Resmi Gazete, (2006, Temmuz 28) No: 26242, "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)", http://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm, Erişim tarihi: 16 Temmuz 2014.

11- A.g.e.

12- T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü (2008, 22 April) "Kişisel Verilerin Korunması Kanunu Tasarısı", http://www2.tbmm.gov.tr/d23/1/1-

0576.pdf, Erişim tarihi: 18 Temmuz 2014.

13- T.C. Bakanlığı, http://www.basbakanlik.gov.tr/Handlers/FileHandler.ashx?FileId=1167, Erişim tarihi: 21 Haziran 2014.

14- T.C. Başbakanlık (2002, Ağustos) "e-Türkiye Girişimi Eylem Planı (TASLAK)"

15- Aksakal, A. (1999) "Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı" Türk Kütüphaneciliği Dergisi Cilt. 13 Sayı. 4 ss. 438-457

16- Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı (2010, Mayıs) "Kritik Altyapıların Korunması"

17- Kanun No. 5651 Madde 10.6 (6 Şubat 2014 tarihinde yapılan düzenleme - 6518/95) Aşağıdaki adresten erişilebilir: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

18- TÜBİTAK-BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü internet sayfası, "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

19- TÜBİTAK-BİLGEM internet sayfası, "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://bilgem.tubitak.gov.tr/en/kurumsal/history

20- TÜBİTAK Siber Güvenlik Enstitüsü internet sayfası, "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce

21- TÜBİTAK-BİLGEM internet sayfası "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://bilgem.tubitak.gov.tr/en/kurumsal/history

22- Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" International Journal of Information Security Science Cilt.1, Sayı. 4

23- A.g.e.

24- TÜBİTAK-BİLGEM internet sayfası "Tarihçe". 16 Temmuz 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://bilgem.tubitak.gov.tr/en/kurumsal/history

25- A.g.e.

26- Şentürk, H. vd. (2012), "Cyber Security Analysis of Turkey" International Journal of Information Security Science Cilt.1, Sayı. 4

27- Bekdil, B. E. (2013, Aralık 1) "Cybersecurity an Emerging Market in Turkey" Defense News

28- 30 Ocak 2015 tarihinde USOM ve TÜBİTAK tarafından Ankara'da yapılan Kurumsal SOME etkinliği sunumu, 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.usom.gov.tr/faydali-dokuman/15.html

29- Bilişim Dergisi "2. Ulusal Siber Güvenlik Tatbikatı Yapıldı" Sayı 151 ss:148-151 http://www.bilisimdergisi.org/s151/

30- Raporda Kurumun resmi görüşlerine yer verilmediğini belirten bir açıklama bulunmaktadır. Bkz. Unver, M. vd. (2009, Mayıs) "Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler" Bilgi Teknolojileri ve İletişim Kurumu

31- Sabah (2010, Ekim 28) "Kırmızı Kitap'a MGK'dan vize"

32- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (2012, Haziran) "Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için"

33- Bu yönde bir teşebbüs Linux temelli bir işletim sistemi olan ve TÜBİTAK UEKAE tarafından geliştirilip, ilk olarak Aralık 2005'te yayınlanan Pardus projesi olmuştur. European Commission ISA Joinup (2008, Kasım 27) "A new kid on the block: The Turkish Pardus Linux Distribution". Pardus kullanıcıları arasında Milli Savunma Bakanlığı (Pardus'e geçerek 2 milyon dolar tasarruf edildiği belirtilmektedir) ve Sosyal Güvenlik Kurumu vardır. NTVMSNBC (2009, Nisan 14) "MSB, Pardus ile 2 milyon dolar tasarruf etti" NTVMSNBC (2009, Nisan 13) "SGK, Pardus'a göç etmeye hazırlanıyor".

Proje 2011'de, iddia edildiğine göre TÜBİTAK'taki siyasi değişimler sonucunda işgücünde büyük kayıplar olması sebebiyle, durmuştur. www.shiftdelete.net (2012, Şubat 01) "Yerli Pardus'ta Sona Doğru" 9 Eylül 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://shiftdelete.net/yerli-pardusta-sona-dogru-34654?p=1 2 sene boyunca hiç yeni sürüm yayınlanmamasından sonra işletim sisteminin 2013 sürümü yayınlanmıştır. Ağustos 2014'te hükümetinin programından bahseden Başbakan Ahmet Davutoğlu Pardus projesine açıkça değinmiş ve hükümetin amacının Pardus'ü kamu kurumları ve özel kuruluşlara yaymak olduğunu belirtmiştir. Pardus Portal internet sayfası (2014, Ağustos) "PARDUS 62. Hükümet Programında Yerini Aldı!" 9 Eylül 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://www.pardus.org.tr/pardus-hukumet-programinda

34- BTK çalışanları tarafından Mayıs 2010'da kaleme alınan daha eski bir raporda kritik ulusal altyapı (KUA) konusunda uluslararası tanımlamalar ve mevzuat incelenmiş ve Türkiye'de KUA konusunda atılan adımların noksanlığına dikkat çekilmiştir. Bkz. Ünver, M. vd. (2010, Mayıs) "Kritik Altyapıların Korunması" Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı

35- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği (2012, Haziran) "Ulusal Siber Güvenlik Stratejisi: 2023'ün siber uzayında güçlü ve önder bir Türkiye için" ss.11-12

36- Bakanlar Kurulu Kararı 2012/3842 20 Ekim 2012 tarihli 28447 sayılı Resmi Gazete'de yayınlanmıştır.

37- Bakanlar Kurulu Kararı 2012/3842 #5.1 20 Ekim 2012 tarihli 28447 sayılı Resmi Gazete'de yayınlanmıştır.

38- Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"

39- Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.3

40- Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.15

41- Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.18

42- Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve İletişim Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" s.8

43- Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 11 Kasım 2013 tarihli 28818 sayılı Resmi Gazete'de yayınlanmıştır.

44- USOM ve TÜBİTAK tarafından 30 Ocak 2015 tarihinde Ankara'da düzenlenen Kurumsal SOME Etkinliği sunumu. 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.usom.gov.tr/faydali-dokuman/15.html

45- BTK internet sayfası "USOM-SOME" 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usomsome.php

46- A.g.e

47- T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı (2014, Eylül) "2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi" 30 Kasım 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.afad.gov.tr/Dokuman/TR/123-20141010111330-kritikaltyapi-son.pdf

48- NATO, "Joint Press Conference with NATO secretary General Anders Fogh Rasmussen and Madeleine Albright, Chair of the Group of Experts", 17.05.2010, http://www.nato.int/cps/en/natolive/opinions_63696.htm (29 Temmuz 2015 tarihinde erişilmiştir)

49- Sabah (2013, Aralık 2) "TSK'dan siber savunma atağı"

50- Radikal (2013, Ocak 21) "TSK'da Siber Savunma Merkezi Başkanlığı kuruldu"

51- Emre Soncan, "Security Units patrolling online against cyber attacks and crises", Today's Zaman, 24.02.2013, http://www.todayszaman.com/national_security-units-patrolling-online-against-cyber-attacks-and-crimes_307094.html (3 Ağustos 2015 tarihinde erişilmiştir)

52- Radikal (2014, Mayıs 27) "TSK'da siber ordu için önemli adım"

53- USOM ve TÜBİTAK tarafından 30 Ocak 2015 tarihinde Ankara'da düzenlenen Kurumsal SOME Etkinliği sunumu. 14 Nisan 2015 tarihinde aşağıdaki bağlantıdan erişilmiştir: https://www.usom.gov.tr/faydali-dokuman/15.html

54- Haber7.com (2013, Aralık 5) "TSK'ya Siber Savunma Komutanlığı" 26 Ağustos 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: http://www.haber7.com/guncel/haber/1102379-tskya-siber-savunma-komutanligi

55- Türkiye Bilişim Şurası internet sayfası (2002, Şubat 19) "Bilişim Suçları Çalışma Grubu" 15 Eylül 2014 tarihinde aşağıdaki bağlantıdan erişilmiştir: www.bilisimsurasi.org.tr/dosyalar/9.doc

56- "İlkiz, F. (2001, Aralık 05) "İnternet Ortamındaki Yayınlarda İki Olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar Üzerine Görüşler" Türkiye Bilişim Şurası internet sayfasından 20 Eylül 2014tarihinde aşağıdaki bağlantıdan erişilmiştir: www.bilisimsurasi.org.tr/dosyalar/45.doc

57- Radikal (2015, Temmuz 12) "'Hacker skandalı'nda ilginç ortaklık MHP kasetlerine kadar uzandı"

58- Hürriyet (2015, Temmuz 9) "Polise faturalı hackerlık hizmeti

59- Resmi Gazete, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanunu, no. 6532", No 28983, 17 Nisan 2014, http://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm (23 Temmuz 2014 tarihinde erişilmiştir)

60- Bu Milli İstihbarat Teşkilatı'nın talep ettiği tuhaf bir uzmanlık alanıdır. Başlığı alan hakkında net bir tanım sağlamamaktadır.

61- Palaz, H. (2015, Mart) "Ömrümü Yedin Bay Böcek!" Cinius Yayınları ss.184-185

62- Radikal (2015, Mart 08) "TÜBİTAK'ta dijital analiz yapacak eleman kalmamış!"

63- "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun", 19 Şubat 2014 tarihli 28918 sayılı Resmi Gazete

64- 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 04 Mayıs 2007

65- 5809 sayılı Elektronik Haberleşme Kanunu 05 Kasım 2008, 10 Kasım 2008 tarihli 27050 sayılı Resmi Gazete

66- "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" Madde 103, 19 Şubat 2014 tarihli 28918 sayılı Resmi Gazete

67- 5651 Sayılı Kanun Madde 8/A (27 Mart 2015 tarihinde yapılan değişiklik – 6639/29) Aşağıdaki bağlantıdan erişilebilir: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

68- 5651 Sayılı Kanun Madde 10 (2007, Mayıs 4) 23 Mayıs 2007 tarihli 26530 sayılı Resmi Gazete

69- 5651 Sayılı Kanun Madde 6/Ç (6 Şubat 2014 tarihinde yapılan değişiklik – 6518/89) Aşağıdaki bağlantıdan erişilebilir: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

70- "Sosyal Mühendislik: Crackerların, normalde kapalı olan bir ağa erişim sağlamak amacıyla ağa erişimi olan kişileri kandırmak için sosyal bir durum tasarladıkları ya da "mühendisliğini yaptıkları" ya da kişileri aslında var olmayan bir gerçekliğe inandırdıkları aldatmaya dayalı süreç. Bilgisayar sistemlerini kırmak için crackerlar sıklıkla gelişmiş sosyal mühendislik yeteneklerini kullanırlar. Sosyal mühendislik vakalarının iyi bir derlemesine Kevin Mitnick'in The Art of Deception kitabında erişilebilir." Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, s. 293.

71- "Ters mühendislik: Bir bilgisayar sisteminin parçalarının ve parçalarının birbirleri arasındaki ilişkilerinin belirlenebilmesi için analiz edilmesini içermektedir. Ters mühendislik sıklıkla bir sistemin uzun süre kullanılabilirliğini sağlamak için yeniden tasarlanmasını sağlamak amacıyla ya da orijinal tasarıma erişim olmadan bir sistemin taklitlerini üretebilmek için yapılır. Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, s. 269.

72- Ufuk Eriş, "Türkiye'de Kırıcı (Hacker) Kültürü", Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora tezi, Kasım 2009, ss. 141-200.

73- Ayyıldız Tim Misyonu, http://www.ayyildiz.org/navigasyon.php?id=22 (21 Ağustos 2015 tarihinde erişilmiştir)

74- Zone-H tahrif edilmiş internet sitelerinin arşivini tutan ünlü sitelerden biridir. Site yönetimi sahte kayıtları önlemek için tahriflerin gerçek olup olmadığını kontrol etmektedir. Hackerların tahriflerine dair kanıtı Zone-H internet sitesine iletmektedir. Böylelikle eylem geçmişlerini ve namlarını arttırmaktadırlar. Daha fazla bilgi için bkz; http:// http://www.Zone-H.org/

75- Ayyıldız Tim, "http://www.simos1.gr", Zone-H, http://www.Zone-H.org/mirror/id/13249689, 15 Mart 2011.

76- Ayyıldız – Tim, Görünmeyen Kahramanlar (Sanal Alemin Askerleri), Ankara, 2008, s. 16.

77- Elvan Ezber, "Ayyıldız Tim'e Polisten Çete Baskını". Radikal, 12 Ağustos 2011, http://www.radikal.com.tr/turkiye/Ayyıldız_time_polisten_cete_baskini-1059754; Elvan Ezber, "Ayyıldız Tim: Bekir K. ile bağlantımız yok". Radikal, 14 Ağustos 2011,

78- Gamze Akkuş, "Anonymous resmi hedefe saldırdı. Ayyıldız Tim karşı atakla cevap verdi". Hürriyet, 10 Haziran 2011, http://www.hurriyet.com.tr/ekonomi/17996737.asp

79- "Kızılhack hedefimiz ezenler", Atılım, 21 Eylül 2006, http://web.archive.org/web/20100507133839/http://www.atilim.org/atilim/modules.php?name=Guncel&file=article&sid=16899 (3 Mayıs 2015 tarihinde erişilmiştir)

80- A.g.e.

81- A.g.e.

82- Daha fazla detay için bkz. "RedHack Defacements", Zone-H, http://www.Zone- H.org/archive/notifier=RedHack/page=1 (2 Mayıs 2015 tarihinde erişilmiştir)

83- Serkan Ocak, "Ankara Emniyeti Çökertildi", Radikal, 28 Şubat 2012, http://www.radikal.com.tr/turkiye/ankara_emniyeti_cokertildi-1080108 (3 Mayıs 2015 tarihinde erişilmiştir)

84- "RedHack Emniyeti hackledi mi?", Milliyet, 05 Eylül 2013, http://www.milliyet.com.tr/RedHack-emniyet-i- hackledi-mi-/gundem/detay/1759446/default.htm (Accessed on 5 May 2015)

85- Tahriflerin kronolojisiyle ilgili daha fazla bilgi için bkz; Burak Polat, Cemile Tokgöz Bakıroğlu, Mira Elif Demirhan Sayın. "Hacktivism in Turkey: The Case of RedHack", Mediterranean Journal of Social Sciences, Vol 4, Ekim 2013.

86- Yiğit Turak, "RedHack özelinde Siber olaylar ve Siber Suçlar", İstanbul Bilgi University, Unpublished Course Project for Cyber Crimes and its Practice in Turkish Law, http://www.yigitturak.com/wp-content/uploads/RedHack- Özelinde-Siber-Olaylar-ve-Siber-Suçlar.pdf (11 Mayıs 2015 tarihinde erişilmiştir)

87- Pentest İngilizce sızma testinin (penetration testing) kısa yazılışıdır. "Sızma Testi (genel terim): Güvenlik açıklarının ve crackerların bunları ne ölçüde kendi avantajlarına kullanabileceğinin araştırıldığı ve belirlendiği süreç. Bir kuruma ait, bilgisayarların, ağ birimlerinin ve uygulamalarının da içinde bulunduğu bilişim sistemlerinin güvenlik vaziyetinin değerlendirilmesi için kritik önem teşkil eden bir araçtır. Webster's New World Hacker Dictionary, Indianapolis: Wiley Publishing, 2006, s. 243.

88- http://pastebin.com/mFFw5DqS (3 Ekim 2015 tarihinde erişilmiştir)

89- Bkz. http://www.turkhackteam.org/misyon.html (12 Haziran 2015 tarihinde erişilmiştir)

90- "Vatikan'a Turk Hack Team saldırdı", Aydınlık, 15 Nisan 2015, http://www.aydinlikgazete.com/bilimteknoloji/vatikan-a-turk-hack-team-saldirdi-h67740.html (15 Mayıs 2015 tarihinde erişilmiştir)

91- "New York Times hacklendi", Sabah, 28 Mayıs 2015, http://www.sabah.com.tr/gundem/2015/05/28/new-york-times- hacklendi (6 Haziran 2015 tarihinde erişilmiştir)

92- "Türk Hackerlardan Müdahale", Milliyet, 05 Haziran 2015, http://www.milliyet.com.tr/turk-hackerlardan-the- guardian-gazetesine-istanbul-yerelhaber-824596/ (11 Haziran 2015 tarihinde erişilmiştir). Ayrıca bkz; http://www.turkhackteam.org/basin-duyurusu/1139755-guardian-operasyonu-ulusal-basinda.html

93- Osmanlı İmparatorluğu'nda düşmanı ön saldırılarıyla şaşırtan ve düşman topraklarında keşif görevi yapan özel bir askeri birlik.

94- http://board.tr.gladiatus.gameforge.com/index.php?page=Thread&threadID=8202

95- A.g.e

96- "Türk hükümeti 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu Mayıs 2007'de yürürlüğe koymuştur. Bu yasanın kabulu YouTube'dan erişilebilen ve Türkiye Cumhuriyeti'nin kurucusu Mustafa Kemal Atatürk'ü tahrif eden videolara dair kaygıların, internette çocuk pornografisi ve müstehcen içeriklerin erişilebilirliğine ve intihar ya da çocuklar için zararlı olabilecek ya da uygun olmayabilecek maddelere dair bilgi veren internet sitelerine dair artan kaygıların ardından gelmiştir." Yaman Akdeniz, (2010, Ocak 11) Report of the OSCE Representative on Freedom the Media on Turkey and Internet Censorshiphttp://ec.europa.eu/enlargement/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censor ship.pdf (10 Kasım 2015 tarihinde erişilmiştir)

97- http://www.cyber-warrior.org/Misyon.asp

98- A.g.e.

99- "Cyber Warrior'u ekol yapan etkenler nelerdir?", haberseyret.com, 26 Ocak 2014, http://haberseyret.com/haber/5319/cyber-warrioru-ekol-yapan-etkenler-nelerdir (1 Haziran 2015'te erişilmiştir)

100- "En makbul milliyetçi 'hacker' olan milliyetçi", Agos, 18 Haziran 2012, http://www.agos.com.tr/tr/yazi/1714/en- makbul-milliyetci-hacker-olan-milliyetci (29 Mayıs 2015'te erişilmiştir)

101- "İsrail Sitelerini Hackleyen Türk Hacker", http://www.dailymotion.com/video/xdk8lp_israil-sitelerini-hackleyen- turk-ha_tech (11 Haziran 2015'te erişilmiştir)

102- "Cyber Warrior Röportaj 1. Bölüm", http://www.cyber-warrior.org/Forum/haberseyret-ile-Cyber-warrior-hk- roportaj_510091,0.cwx (02 Haziran 2015'te erişilmiştir); "Cyber Warrior Röportaj 2. Bölüm", http://www.cyber- warrior.org/Forum/haberseyret-ile-cyber-warrior-hk-roportaj-2-bolum_510137,0.cwx (02 Haziran 2015'te erişilmiştir)

103- HP Security Research, "Cyber Risk Report 2015", s.11, http://www.asial.com.au/documents/item/113 (11 Haziran 2015 tarihinde erişilmiştir)

104- Daha fazla detay için bkz; Cyber-Warrior'un basın sözcüsü XY: Emniyet'in 5 katı iş yapıyoruz", http://psikologdoctor.blogcu.com/unlu-turk-hackerdan-muthis-aciklamalar/2454785 (7 Haziran 2015 tarihinde erişilmiştir)

105- İngiliz menşeli ve iyi bilinen, teknoloji üzerine bir internet sitesi

106- Charles Arthur, "Turkish hacker group diverts users away from high-

profile websites", The Guardian, 05 Eylül 2011, http://www.theguardian.com/technology/2011/sep/05/turkish-hacker-group-diverts-users. (07 Haziran 2015 tarihinde erişilmiştir)

107- Charles Arthur, "Interviewed: the Turkish hackers whose DNS attack hit the Telegraph", The Guardian, 05 Eylül 2011

108- Pastebin çevrimiçi bir metin deposudur.

109- Agd_Scorp, "Scorp's Manifesto", Pastebin, 11 Eylül 2012, http://pastebin.com/TsqZpx5H (12 Haziran 2015 tarihinde erişilmiştir)

110- Turk Guvenligi, Zone-H, http://Zone-H.org/archive/notifier=TurkGuvenligi.info/page=1 (09 Haziran 2015 tarihinde erişilmiştir)

111- Agd_Scorp, Zone-H, http://Zone-H.org/archive/notifier=Agd_Scorp (09 Haziran 2015 tarihinde erişilmiştir)

112- SQL enjeksiyonu, kötü niyetli kullanıcıların SQL platform kullanan bir internet sitesine sitenin veritabanını kontrol etmek için SQL komutları enjekte ettikleri bir tekniktir.

113- http://www.Zone-H.org/mirror/id/21545300

114- "PKK'lı hacker'lar 2307 siteyi çökertti", Radikal, 27 Aralık 2006, http://www.radikal.com.tr/turkiye/pkkli_hackerlar_2307_siteyi_cokertti-801430 (29 Haziran 2015 tarihinde erişilmiştir)

115- "Porno meraklısı istihbaratçılar PKK'nın hacker'ına çalışmışlar", Radikal, 27 Kasım 2008, http://www.radikal.com.tr/turkiye/porno_meraklisi_istihbaratcilar_pkknin_hackerina_calismis-910264; "PKK'lı hacker'ın pişmanlığına Yargıtay'dan onay", Radikal, 23 Şubat 2011, http://www.radikal.com.tr/turkiye/pkkli_hackerin_pismanligina_yargitaydan_onay-1040911 (29 Haziran 2015 tarihinde erişilmiştir)

116- http://www.Zone-H.org/archive/notifier=pkkhackteam (21 Eylül 2015 tarihinde erişilmiştir)

117- http://www.Zone-H.org/archive/notifier=Pkk%20Hack%20Team (21 Eylül 2015 tarihinde erişilmiştir)

118- Türkiye Hizbullah'ı ve ortağı Hür Dava Partisi (HÜDAPAR), IŞİD'in Suriye sınırının diğer yakasındaki Kobane'yi kuşatmasına karşı Türkiye çapında 7 Ekim'de yapılan protestolar sırasında PKK ile bazı çatışmalara girmiştir. İki taraf arasındaki gecenin en kanlı çatışması Güneydoğu'daki Diyarbakır'da en azından 10 kişinin ölümüne sebep olmuştur. Daha fazla detay için bkz, Metin Gürcan, "Kurd vs. Kurd: internal clashes continue in Turkey", AlMonitor, 09 Ekim 2014, http://www.al-monitor.com/pulse/originals/2014/10/turkey-syria-kurds-kobani-pkk-kurdo-islamists.html# (11 Kasım 2015'te erişilmiştir) Daha fazla okumak için: http://www.al-monitor.com/pulse/originals/2014/10/turkey-syria- kurds-kobani-pkk-kurdo-islamists.html#ixzz3rZvyedSY

119- "Hüdapar yöneticisinin hesabına hack", Özgür Gelecek, 11 Şubat 2015,

http://www.ozgurgelecek.net/guncel- haberler/13494-2015-02-11-16-01-45.html (30 Haziran 2015'te erişilmiştir)

120- https://twitter.com/tak_hacktim

121- "PKK yandaşı hackerlar Sözcü gazetesinin twitter hesabını hackledi", Mynethaber, 02 Şubat 2015, http://www.mynet.com/teknoloji/pkk-yandasi-hackerlar-sozcu-gazetesinin-twitter-hesabini-hackledi-1687883-1; "PKK'lı hackerlar belediyenin hesabını hackledi", Cumhuriyet, 05 Şubat 2015, http://www.cumhuriyet.com.tr/haber/turkiye/207781/PKK_li_hackerler_belediyenin_hesabini_hack_ledi.html (30 Haziran 2015'te erişilmiştir)

122- "The Most Hacker-Active Countries", InfoSec Institute, 5 Ağustos 2015, resources.infosecinstitute.com/ the-most- hacker-active-countries-part-i/.

123- Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2, 2013, s.135 – 158.

124- Bilgi için bkz. www.enigmasoftware.com/top-20-countries-the-most-cybercrime/.

125- Akamai, Q2 2015 State of the Internet – Security Report, www.stateoftheinternet.com/resources-cloud-security- 2015-q2-web-security-report.html.

126- Stefan Frei, Cyber Crime Threat Intelligence – Turkey, CSIS White Paper – Temmuz 2014,Kopenhag, 2014, www.csis.dk/downloads/Paper_-_Cyber_Threats_Turkey.pdf.

127- A.g.e.

128- T.C. Kalkınma Bakanlığı (2014, May) "2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı (Taslak)" Aşağıdaki bağlantıdan erişilebilir: http://bilgitoplumustratejisi.org/tr/doc/8a94819842e4657b01464d5025b80002

129- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı da 2014-2018 için bir stratejik plan yayınlamıştır. Bu plan 2013- 2014 Eylem Planı'nda belirlenen hedefleri tekrar teyit etmiş, ancak onların ötesine geçememiştir. Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Stratejik Planı 2014-2018

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.

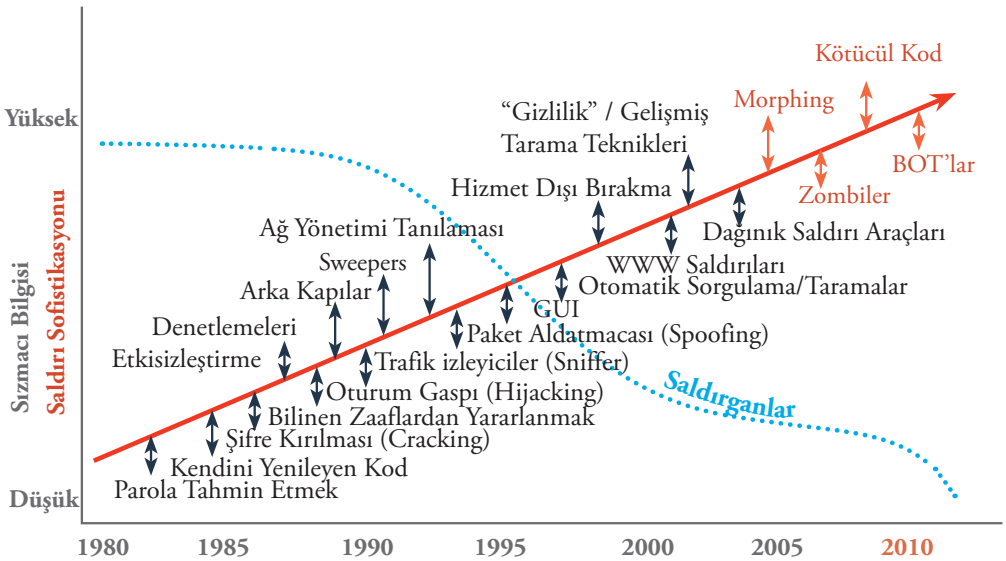
Devletlerin ve çeşitli uluslararası kuruluşların siber uzayda işleyen sistemlerin güvenliğini tehdit eden siber saldırıları tanımlamaya çalıştıkları görülmektedir. ABD Savunma Bakanlığı, siber saldırıyı "bilgisayar veya bilgisayar bağlantılı ağ ve sistemleri kullanarak hasımlarının siber sistemlerini, 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.

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.

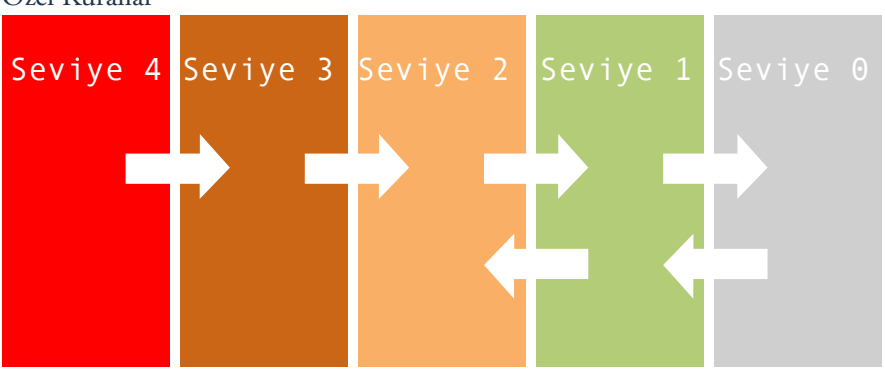
Ayrıca, yüklenicilerin sabıka kaydı sorgulaması yapılmalıdır. Güvenlikten ziyade işlevsellik ve dayanıklılıkları dikkate alınarak tasarlanan ısıtma, havalandırma ve soğutma gibi sistemler, nükleer enerji santrallerinin en az güvenli unsurları olarak kabul edilmelidir. Bu sistemler günümüzde yerel ağa 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)

Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM) İstanbul merkezli bağımsız bir düşünce kuruluşudur. EDAM'ın ana çalışma alanları:

- Dış siyaset ve güvenlik,
- Türkiye-AB ilişkileri,
- Enerji ve iklim değişikliği,
- Ekonomi ve küreselleşme,
- Silahların kontrolü ve silahların yayılmasının önlenmesi,
- Siber politikalar programını kapsamaktadır.

EDAM, Türkiye'nin yeni dünya düzeni içinde alacağı yeri belirleyecek politika alanlarına dair görüş oluşturmak suretiyle Türkiye içinde ve dışında karar alma süreçlerine katkıda bulunmayı amaçlamaktadır. EDAM bu çerçevede araştırmalar yapmasının yanı sıra düzenli yuvarlak masa toplantıları ve konferanslar düzenlemektedir. EDAM aynı zamanda çeşitli kuruluşlar ile ortak araştırma ve yayın konularında işbirliği yapmaktadır.

TÜRKİYE'DE SİBER GÜVENLİK VE NÜKLEER ENERJİ

ISBN : 978-9944-0133-8-3

Ekonomi ve Dış Politika Araştırmalar Merkezi

Hare Sokak No:16,
Akatlar, 34335 Istanbul
Tel : +90 212-352 1854
Email : info@edam.org.tr
www.edam.org.tr