Güvenlik Bilimleri Dergisi, Mayıs 2021,Cilt:10 Sayı:1, 151-174 *DOI:10.28956/gbd.941801*

SİBER GÜVENLİK KAPSAMINDA ENERJİ SİSTEMLERİ GÜVENLİĞİNİN DEĞERLENDİRİLMESİ

Hakan AYDIN[*], Mehmet Ali BARIŞKAN[**], Ali ÇETİNKAYA[***]

Öz

Günümüzde enerji sistemlerinde Bilgi ve İletişim Teknolojilerine (BİT) ve özellikle de İnternete olan artan oranlardaki bağımlılık, bu sistemlerde siber güvenliğin sağlanmasını zorunlu hale getirmiştir. Enerji sistemlerinde kullanılan bilişim teknolojilerinde meydana gelebilecek siber güvenlik olayları; enerji hizmetlerinin durmasına, aksamasına, büyük ölçekli ekonomik zarar görülmesine, kamu düzeninin bozulmasına, can kaybı yaşanmasına ve hatta ülkelerin ulusal güvenliğinin tehlikeye düşmesine neden olma risklerini içermektedir. Bu araştırmanın amacı; enerji sistemlerinde siber güvenlik kavramlarının genel çerçevesini çizmek, enerji sistemlerine yönelik yaşanmış siber saldırıları araştırmak, bu çerçevede SCADA ile yönetilen kritik altyapılarda, özellikle de enerji sistemleri altyapılarında, siber güvenliğin önemini ortaya koymak ve bu konuya ilişkin mevcut farkındalığın artırılmasına yönelik öneriler getirmek olarak belirlenmiştir. Araştırmada betimleme yöntemi kullanılmıştır. Araştırmada elde edilen bilgiler, enerji sistemlerinde siber güvenliğin sağlanmasının hayati derecede öneme sahip olduğu yönündedir. Çalışmada getirilen öneriler arasında, özellikle Türkiye'de enerji sektöründe ulusal siber güvenlik testlerinden geçirilmiş ve ulusal sertifikasyona sahip akredite yerli güvenlik danışman şirketleri tarafından tasarlanmış ve test edilmiş milli siber güvenlik bilgi teknolojileri ve ürünleri kullanılması hususuna özellikle vurgu yapılmıştır.

***Anahtar Kelimeler**: Enerji Sistemleri, Siber Güvenlik, SCADA Sistemleri, Kritik Altyapılar.*

EVALUATION OF THE SECURITY OF ENERGY SYSTEMS UNDER THE SCOPE OF CYBERSECURITY

Abstract

That the dependency on Information and Communication Technologies (ICT) and increasingly on the Internet has made it essential to ensure cyber security in these systems. Cyber security vulnerabilities that may occur in information technologies used in energy systems carries the risks of stopping or failing of energy services, large-scale economic damage, disruption of public order, loss of life and even endangering the national security of the countries. The aim of this research is to outline cyber security concepts in energy systems, to investigate cyber attacks against energy systems, to reveal the importance of cyber security in critical infrastructures, especially the critical energy infrastructure managed by SCADA, and finally to increase current awareness. Descriptive method was employed in the research. The information obtained from the research shows that ensuring cyber security in energy systems is of vital importance. Among the suggestions made by the research, the importance of using national cyber security information technology products that have been subjected to national cyber security tests and developed and tested by national security institutions that both have accreditation and certification in the energy sector in Turkey was particularly emphasized.

***Keywords:** Energy Systems, Cyber Security, SCADA Systems, Critical Infrastructures*

[*]Dr. Öğr. Üyesi, İstanbul Gelişim Üniversitesi, Bilgisayar Mühendisliği Bölümü, haaydin@gelisim.edu.tr, https://orcid.org/0000-0002-0122-8512.

[**]Araş. Görevlisi, İstanbul Gelişim Üniversitesi, Bilgisayar Mühendisliği Bölümü, mabariskan@gelisim.edu.tr, https://orcid.org/0000-0002-8039-2686.

[***]Araştırmacı, İstanbul Gelişim Üniversitesi, Teknoloji Transfer Ofisi Uygulama ve Araştırma Mrk., Lisans Öğr. Kocaeli Üniversitesi alcetinkaya@gelisim.edu.tr, https://orcid.org/0000-0003-4535-3953.

Makale Geliş Tarihi: 06.07.2020 Makale Kabul Tarihi: 24.12.2020

GİRİŞ

Günümüzde enerji sistemlerinde Bilgi ve İletişim Teknolojilerine (BİT) ve özellikle de İnternete olan artan oranlardaki bağımlılık, bu sistemleri siber saldırı ve tehditler ile karşı karşıya bırakmıştır. Enerji sistemleri, petrol boru hatlarından elektrik iletim ve dağıtım hatlarına, doğalgaz depolama tesislerinden basınç regülasyonu ve pompa istasyonlarına, nükleer, fosil yakıt ve su barajları ve santral tesislerinden bilgisayar destekli kritik tesislere kadar siber tehdit ve saldırıların hedefi altındadır. Siber alan, bilgi teknolojilerinde yaşanan gelişmelerle birlikte özellikle harp alanında daha aktif olarak kullanılmaktadır (Dedemen, 2016: 1).

Ülkeler enerji sistemlerine yönelik siber olaylara karşı hazırlıklı halde olmak, bu olaylardan olabilecek en az hasara uğrayarak çıkmak, siber güvenlik risklerini yönetilebilir ve kabul edilebilir düzeylerde tutmayı amaçlamaktadır. Bunun için başta SCADA (Supervising Control and Data Acquisition: Veri Tabanlı Kontrol ve Gözetleme) sistemleri olmak üzere enerji sistemlerinde siber güvenliği sağlamak maksadıyla çalışmalar yapmakta, bu hususlara siber güvenlik strateji ve politikalarında önem vermektedirler. Endüstriyel Kontrol Sistemleri (EKS), endüstriyel süreçleri desteklemek için tasarlanmış komuta ve kontrol sistemleridir. Bu sistemler, gaz ve elektrik dağıtımı, su arıtma, petrol rafinajı veya demiryolu taşımacılığı gibi çeşitli süreçlerin ve işlemlerin izlenmesinden ve kontrol edilmesinden sorumludur.

EKS'nin en büyük alt grubu SCADA sistemleridir (Enisa, 2016; Yılmaz ve Gönen, 2018). SCADA öncelikle, uzaktaki donanıma üst düzey komutlarla sınırlı olan denetim rolündeki dağıtılmış bir sistemdir. SCADA sistemleri coğrafi olarak dağınık uzak terminal ünitelerinden olaya dayalı verileri elde etmek ve bu verileri bir merkezi insan makine arayüzü konsolunda sunmak üzere tasarlanmıştır. Bir SCADA kontrol merkezi, alarmların izlenmesi ve durum verilerinin işlenmesi dâhil olmak üzere uzun mesafeli iletişim ağları üzerinden alan siteleri için merkezi izleme ve kontrol gerçekleştirir. Diğer bir ifadeyle, SCADA sistemleri, bir sistemin gözetim ve denetimini sağlayan ve sistemleri uzaktan ve otomatik olarak denetlemek, yönetmek ve izlemek için tasarlanmış bir EKS türüdür.

Uzak istasyonlardan alınan bilgilere dayanarak otomatikleştirilmiş veya operatör tarafından yönetilen denetim komutları, genellikle saha cihazları olarak adlandırılan uzak istasyon kontrol cihazlarına aktarılabilir (Campbell, 2015) Kontrol sistemleri, merkezi olmayan çeşitli operasyonları izlemek ve kontrol etmek için kullanılan SCADA sistemlerini içermekte olup, bu da esas olarak onu işleten kişinin fiziksel olarak hemen yanında durmadığı anlamına gelmektedir (Teixeira,

2018; Hopkins ve Kalaimannan, 2019). Enerji güvenliği kavramı günlük yaşantı içerisinde "bireysel güvenlik", "bilgi güvenliği", "özel güvenlik", "ulusal güvenlik", " küresel güvenlik", "gıda güvenliği", "fiziki güvenlik", "iş güvenliği", "şirket güvenliği", "çevre güvenliği", "iletişim güvenliği" gibi kavramlar yanında sıkça duyulmakta ve önemli bir yer kaplamaktadır (Çıtak, 2019). Günümüzde enerji sistemleri de tıpkı diğer bilişim sistemleri gibi siber saldırı ve tehdit altında olduklarından dolayı enerji sistemlerinin bilgi güvenliği konusu önemini korumaktadır.

Çalışmanın ilk bölümünde konunun kavramsal bir çerçevesi çizilerek özellikle enerji sistemlerinin bilgi güvenliğine yönelik temel tanım ve açıklamalara yer verilmiş, müteakiben enerji sistemlerinde siber güvenliğin analizinden yola çıkarak enerji sistemlerinde siber güvenliğin önemi araştırılmıştır. Devam eden bölümde siber tehdit ve saldırılar sonrası meydana gelebilecek olumsuz olaylar ve örnekler üzerinden enerji sistemlerine yönelik saldırı örnekleri ile Türkiye'de enerji sistemlerinde siber güvenliğin sağlanması çalışmaları siber güvenlik bakış açısıyla incelenmiştir. Son bölümde ise elde edilen bilgiler doğrultusunda sonuç ve öneriler getirilmiş ve özellikle milli siber güvenlik sertifikasyonuna sahip yazılım ve donanım siber güvenlik ürünlerinin ve uygulamalarının kullanımı üzerinde durulmuştur.

Çalışmanın Metodolojisi

Araştırmanın temel amacı; enerji sistemlerinde siber uzay, siber savunma, siber saldırı, siber savaş, siber terörizm ve siber güvenlik kavramlarının genel çerçevesini çizmek, enerji sistemlerine yönelik yaşanmış siber saldırıları araştırmak, bu çerçevede SCADA (Supervising Control and Data Acquisition: Veri Tabanlı Kontrol ve Gözetleme) ile yönetilen kritik altyapılarda, özellikle de enerji sistemleri altyapılarında, siber güvenliğin önemini ortaya koymak ve bu konuya ilişkin mevcut farkındalığın artırılmasına yönelik öneriler getirmektir.

Araştırmada betimleme yöntemi kullanılmıştır. Kaptan (1995, s. 59) bu yöntemi, olayların, grupların, kurumların vb. çeşitli alanların ne olduğu ve bu sırada gerçekleşen eylemleri daha iyi anlayabilme, aktarabilme adına aralarındaki ilişkinin açıklandığı bir unsur olarak görmektedir. Bu kapsamda nitel bir araştırma yöntemi benimsenerek araştırma yapılmıştır.

Araştırmanın amacı kapsamında aşağıdaki sorulara yanıt aranmıştır:

- Enerji sistemlerinde siber uzay, siber savunma, siber saldırı, siber savaş, siber terörizm ve siber güvenlik kavramlarının genel çerçevesi neleri kapsamaktadır?

- Enerji sistemlerine yönelik geçmişte yaşanmış siber saldırılar ve sonuçları nasıl değerlendirilebilir?
- Türkiye'de enerji sistemlerinde siber güvenliğin sağlanması çalışmaları hangileridir?
- Enerji sistemlerinde siber güvenliğin sağlanmasına ilişkin olarak elde edilen sonuçlar kapsamında hangi öneriler getirilebilir?

Araştırma kapsamında özellikle enerji altyapılarında siber güvenliğin önemi konusunda var olan koşullar, sorunlar tanımlanmaya, elde edilen sonuçlar kapsamında öneriler getirilmeye çalışılmıştır. Çalışmada getirilen öneriler arasında, özellikle Türkiye'de enerji sektöründe ulusal siber güvenlik testlerinden geçirilmiş ve ulusal sertifikasyona sahip akredite yerli güvenlik danışman şirketleri tarafından tasarlanmış ve test edilmiş milli siber güvenlik bilgi teknolojileri ve ürünleri kullanılması hususuna özellikle vurgu yapılmıştır.

1. ENERJİ SİSTEMLERİNDE SİBER GÜVENLİĞİN ÖNEMİ

Siber güvenlik uygulamalarında "gizlilik", "bütünlük" ve "erişilebilirlik" kavramları temeli oluşturmaktadır. Bu kavramlardan gizlilik ilkesi, bir bilgi ve sisteme yetkili kişilerin erişebilmesidir. Bütünlük ilkesi bilginin hiçbir değişikliğe uğratılmamış, bir bölümü veya tamamı bozulmamış ve yok edilmemiş olmasıdır. Erişilebilirlik ilkesi ise bir bilgiye ihtiyaç duyan kullanıcının istediği bilgiye anında ulaşabilmesini ifade etmektedir (ISACA, 2017).

Siber güvenlik, siber ortamı oluşturan bilişim sistemlerinin karşılaşılabilecek saldırılara karşı korunması, söz konusu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin kavramlarını oluşturan bölümlerin güvenliğinin garanti altına alınması, bunların tespit edilmesi (Takaoğlu ve Çağdaş, 2019), tepki mekanizmalarının devreye alınması ve sistemlerin yaşanan saldırı olayı öncesindeki haline geri döndürülmesini içeren kavramdır (2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016). Enerji sistemleri bağlamında bilgi güvenliği günümüzde bir bilgi güvenliği problemidir. Enerji sistemlerinde siber güvenliğin ilk kavramı olan gizlilik ilkesi, bilgiye yalnız ve yalnız bu sektördeki siber uzay aktörlerinden üretim, iletim, dağıtım şirket personeli ve abonelerin kendileriyle ilgili bilgiye ulaşması, başkaca hiç kimsenin ulaşamaması demektir. Enerji sektöründe bütünlük ilkesi; gerilim, frekans, elektrik gücü, yük akışı, teknik bilgilerle faturalandırma mali bilgilerin değiştirilememesi, bozulamaması ve yok edilememesini temsil eder. Enerji sektöründe erişilebilirlik ilkesi bu sektördeki siber uzay aktörlerinin istedikleri anda, yetki hiyerarşisi içerisinde doğru bilgiye erişilebilmesi hususlarını kapsamaktadır.

Enerji sistemlerinde kullanılan bilişim sistemleri tıpkı diğer bilgisayar sistemleri gibi siber saldırı ve tehditlerle karşı karşıyadır (Modeff, 2013; Weed, vd., 2017). Pek çok alana hitap eden bir kavram olarak güvenlik kavramı "enerji güvenliği" alanında da önemli bir yer kaplamaktadır (Çıtak, 2019). Enerji sistemlerinde BİT ve özellikle internet kullanımı sistemin güvenlik risklerinin ve belirsizliklerin oluşması durumunu beraberinde getirmektedir. İnternet kullanımı siber uzaydaki tüm bileşenlerin birbiriyle bağlantılı olması durumunu beraberinde getirmektedir.

Günümüzde petrol boru hatlarından elektrik iletim ve dağıtım hatlarına, doğalgaz depolama tesislerinden basınç regülasyonu ve pompa istasyonlarına, nükleer, fosil yakıt ve su barajları ve santral tesislerinden bilgisayar destekli kritik tesislere kadar enerji sektörünün siber güvenlik kapsamında siber tehdit ve saldırıların hedefi olduğu yadsınamaz bir gerçektir. Yayınlanan raporlara göre 2014 yılında 317 milyon, 2015 yılında ise 431 milyon yeni zararlı yazılım internette dolaşıma verilmiştir (Çiftçi, 2013). Enerji güvenliği ekonomik, toplumsal, siyasi ve jeopolitik risklerin yönetilebilmesi için ana unsur olma özelliğine sahiptir (Lewis, 2002; Özev, 2017). Enerji güvenliği kavramını ifade etmek için enerji ve güvenliğe ağırlık veren iki farklı yaklaşımdan birincisi olan enerjiye olan yaklaşımda enerji kaynaklarının bulunabilirliği, erişilebilirliği ve kabul edilebilirliği kavramlarını içine alırken, ikinci yaklaşım olan güvenliğe yönelik yaklaşımda ise tesislerin her türlü saldırıya karşı fiziki olarak korunması ağırlık yaklaşımdır (Gençtürk, 2012).

Enerji sistemlerinde siber güvenliğin öneminin ortaya konabilmesi maksadıyla öncelikle enerji sistemlerinde siber uzay, siber savunma, siber saldırı, siber savaş, siber terörizm ve siber güvenlik kavramları açıklanmıştır. Siber uzay, siber ortam veya siber alan olarak da isimlendirilmektedir. Bu kavram bütün dünyaya ve uzaya yayılmış durumda olan bilişim sistemlerinden ve bu sistemleri birbirine bağlayan ağlardan meydana gelen ortamı ifade etmektedir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2012; Executive Office of the President, 2016). Ülkelerin silahlı kuvvetleri, istihbarat örgütleri, diğer yasal yetkiye sahip otoriteler, özel sektör, bireysel olarak ya da grup halinde suça karışmış kişiler siber uzayda faaliyet gösteren başlıca aktörlerdir (Çiftçi, 2013). Bu ortam ağ sistemleri ve fiziksel alt yapı ile bilginin depolanması ve değiştirilmesi için kullanılan elektronik ve elektromanyetik bir alandır (Meral, 2008).

Bu bağlamda enerji sistemlerinde siber uzay; kamu ve/veya özel elektrik üretim şirketlerini, iletim sistemini işleten gerilim ve frekansı uluslararası standartlarda tutmakla görevli iletim şirketi ile kamu ve/veya özel sektöre ait alçak ve orta gerilim elektrik dağıtım şebekelerini yöneterek abonelere enerji tedariki yapan

elektrik dağıtım şirketlerini, aboneleri ve enerji sektöründe bilişim teknolojilerini gerçekleştiren kişiler veya tüzel kişilikleri kapsamaktadır (Akıllı ve Özaslan, 2017; Kurnaz ve Karatepe, 2019; İşbilen ve Konar, 2020).

Siber savunma, siber ortamın siber saldırı ve siber terörizme uğramasına karşı önlem almak için uygulanan güvenlik yöntemleri olarak tanımlanabilir (Meral, 2008; ISACA, 2017). Siber savunma; siber ortamda yapılabilecek saldırılar, yanlış kullanım veya zararlı yazılımlar nedeniyle ortaya çıkacak olumsuz etkilerin önlenmesi ve sistemlerin bekasının sağlanması için alınan tedbirler ve yürütülen faaliyetlerdir (Çiftçi, 2013).

Enerji sistemlerinde siber savunma; siber uzayda yer alan enerji sistemlerine yönelik siber saldırılara karşı bu sistemleri korumak için uygulanan siber güvenliğin alınmasına yönelik tedbirleri ve yürütülen faaliyetleri kapsamaktadır.

Siber saldırı, siber ortamda yer alan bilgileri istismar etmek, bozmak, değiştirmek, sistemlere erişimi engellemek ya da zarar vermek amacıyla siber ortamda gerçekleştirilen faaliyetlerdir (Çiftçi, 2013). Siber tehditler bir ülkenin stratejik olarak büyük önem taşıyan haberleşme ve bilgisayar sistemlerine, enerji kaynağı, enerjinin ulaşım ağları, askeri komuta ve kontrol sistemlerini zarara uğratacak büyüklükte etkiye neden olan, asimetrik bir harp çeşidi olarak görülmektedir (Mudrinich, 2012; Aslay, 2017).

Enerji sistemlerinde siber saldırılar siber uzayda yer alan enerji üretim tesislerinin üretimini durdurmak, azaltmak veya çoğaltmak suretiyle frekans ve gerilim stabilitesini ortadan kaldırarak sistem çökmelerine, iletim sistemlerinde yanlış manevralar yaptırmak suretiyle istenmeyen yük akışlarına ve enerji inkitalarına, mal (yangın, infilak vb.) ve can kayıplarına neden olabilecek, abonelerin sayaç okuma, tarifelendirme ve fatura ödeme işlemlerinde yanlış işlem yapılarak maddi kayıplara yol açabilecek enerji sistemlerine yönelik siber ortamda gerçekleştirilen faaliyetlerdir.

Siber savaş, elektronik ağlarda bilgisayar sistemlerinde iletişim ağlarında ve bilgi depolama araçlarında gerçekleşen savaş biçimidir (Boyd, 2009; Johnson, 2015). Bir diğer değişle devletlerin birbirine karşı yürüttüğü siber saldırı faaliyetleridir (Çiftçi, 2013). Bu tanımda dikkat çeken hususlardan birincisi siber savaşın devletlerarasında cereyan etmesidir. İkinci husus ise amacın hasar vermek ve sistemlerde kesinti yapmak olduğudur. Siber savaş aynı zamanda bilgisayarlar ve bu sistemlerde saklanan bilgilere karşı siyasi, sosyal veya ekonomik alanlara karşı girişilen ve kanuna uygun olamayan saldırılar veya tehditlerdir (Meral, 2008).

Siber savaş devletlerarasında siyasi, sosyal veya ekonomik alanlarda elektronik ortamda yer alan bilgilere yönelik olarak cereyan eden kanunsuz saldırılar veya tehditler olarak tanımlanabilir.

Siber terörizm ise kritik milli altyapıları (enerji, ulaştırma, elektronik haberleşme, su yönetimi, bankacılık ve finans ile kamu hizmetleri gibi) devre dışı bırakma ya da bir devleti boyun eğdirme veya sivil toplumu korkutma maksadıyla bilgisayar ağı araçlarının kullanılmasıdır (Çiftçi, 2013). Terörizm saldırılarının amaçları arasında internet ortamı ve bilgisayar sistemleri üzerinden hedef olarak belirlenmiş sistemleri bozmak ve mevcut teknoloji aracılığıyla enerji sistemleri gibi kritik altyapılara zarar vermek bulunmaktadır (Zanini ve Edwards, vd., 2001).

Günümüzde SCADA sistemlerinin kullanıldığı nükleer enerji santralleri gibi büyük öneme taşıyan altyapılar sürekli siber teröristlerin ana hedefleri arasındadır. Bu alanlara saldırı düzenleyen siber teröristler, toplum üzerinde geleneksel terörizmden daha büyük etki yaratmasını amaçlamaktadır (Hardy ve Williams, 2014). Teröristler artık daha az maliyet gerektiren imkânları kullanarak kritik değeri olan bilgisayar sistemlerine zararlı yazılımlar yerleştirilerek bir ülkenin askeri, siyasi ve ekonomik kaynaklarını kilit duruma getirebilir ve zarar verebilirler (Hawks, 2010; Söğüt vd., 2020). Siber terörizm ise kritik milli altyapıları (enerji, ulaştırma, elektronik haberleşme, su yönetimi, bankacılık ve finans ile kamu hizmetleri gibi) devre dışı bırakma ya da bir devleti boyun eğdirme veya sivil toplumu korkutma maksadıyla bilgisayar ağı araçlarının kullanılmasıdır (Çifçi, 2017, s.9). Siber terörizm bilgisayar ağı araçlarının kritik ulusal altyapılarının yani enerji, ulaşım ve hükümet operasyonları gibi altyapıların kapatılması ve bir hükümeti veya sivil nüfusu zorlamak veya yıldırmak için kullanılmasıdır. Siber terörizm geleneksel terörizmle karşılaştırıldığına geleneksel terörizme göre daha küçük boyutta fiziksel eğitim, psikolojik destek ve küçük oranda ölüm riski ve seyahat riski gerektirir. Bu durumlar da terör örgütlerinin takipçilerinin işe alıp tutmalarını kolaylaştırır (Erendor, 2016).

Günümüzde toplumların enerjiye olan bağımlılığı gittikçe arttığından siber savaş unsurları arasında enerji sistemlerine müdahale veya saldırı ilk ala gelen unsurlar arasındadır. Teröristler artık daha az maliyetli imkânlar ile kritik öneme sahip bilgisayar sistemlerine virüs göndererek bir ülkenin ya da kıtanın askeri, siyasi ve ekonomik kaynaklarını felce uğratabilirler (Hawks, 2010). Bu bağlamda enerji sektöründeki siber uzayda yer alan aktörler siber savaş ve siber terörizm tehdidi ile kritik seviyede karşıyadır.

Kritik altyapılar stratejik öneme sahip altyapının üzerinde işlem yaptığı bilginin gizliliği, bütünlüğü veya erişilebilirliği zarar gördüğünde, can ve/veya mal kaybı yaşanmasına, büyük miktarlarda ekonomik zarara, ulusal güvenlikte açıkların meydana gelmesine veya kamu düzeninin hasar görmesine neden olabilecek bilişim veya endüstriyel kontrol sistemlerini içeren sistemlerdir (Homeland Security, 2012; Irmak ve Erkek, 2018; Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı, 2019; Şimşek ve Özen, 2019). Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir (Güntay, 2017). Kritik altyapılar arasında; barajlar, su tutma ve sulama sistemleri, elektrik üretme ve dağıtım sistemleri, petrol tesisleri, gaz sistemleri ve fabrikalar, ulusal enerji sistemleri, ulaşım sistemleri, e-devlet uygulamaları, telekomünikasyon sistemleri, ulusal finansal sistemler, ulusal savunma altyapıları, internet omurgası, stratejik sanayi tesislerinin işletim sistemleri, sanayi ve teknoloji sırlarını barındıran sistemler sayılabilir.

Stratejik öneme sahip altyapılar, temelinde bilgi sistemleri ve/veya bilgi sistemleri ile çalışan sistemlerden meydana gelmektedir. Stratejik öneme sahip altyapılar ve bilgi teknolojileri birçok açıdan, büyük oranda kesişmektedir (Kara ve Çelikkol, 2011). Enerji sistemlerini de kapsayan, kurumsal ağa ve internet ortamına operasyonel gerekçelerle bağlanabilen stratejik öneme sahip altyapılar temelinde bilgi sistemleri ve/veya bilgi sistemlerini kullanarak çalışırlar. Ayrıca siber saldırılara ataklarına açık halde ve korunmasızdırlar (Türkiye Bilişim Derneği, 2020). Elektrik üretimi yapan ve dağıtımını gerçekleştiren sistemler bir ülke için stratejik öneme sahip altyapılardan biridir (Kara ve Çelikkol, 2011; Küçüksille, vd., 2013).

Kaspersky ICS CERT (2020)'de stratejik öneme sahip altyapı endüstriyel otomasyon sistemlerine güvenli uzaktan erişim sağlanmasına ilişkin standartlar ve alınması gereken güvenlik tedbirleri belirtilmiştir. ABD, enerji sektörü bilgi güvenliğini kritik altyapıların bilgi güvenliğinin sağlanması kapsamında ele almaktadır (Modeff, 2013; Kaspersky ICS CERT, 2020). ABD'de enerji sistemleri kritik altyapı olarak belirlenen sektörler arasındadır (Mudrinich, 2012). ABD'de ilk defa 11 Eylül saldırıları sonrasında 13010 sayılı kanun hükmünde kararname ile kritik altyapı terimine yer verilmiş ve kritik altyapının korunmasından sorumlu bir komisyon kurulmuştur (Usak, 2011; Kolevar, 2007). Rusya Federasyonu'nun kritik altyapılarının siber saldırılardan etkilenmemesi ve hasar görmesinin önlenmesi

konularından sorumlu kurumu Rus Federal Güvenlik Servisi (FSB)'dir (Meral, 2015).

Kritik altyapılar; Türkiye tarafından "işlediği 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" olarak tanımlanmaktadır. Türkiye'de ise 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca "enerji" sektörü kritik altyapı sektörleri arasında değerlendirilmektedir (2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016). Görüldüğü gibi AB, ABD, Rusya Federasyonu ve Türkiye kritik altyapı mevzuatında tarif edilen kritik altyapıların tanımı içerisinde enerji sektörü en önde gelen sektörlerden birisidir. Siber saldırıların sektörel dağılımı incelendiğinde, enerji sektörüne yapılan saldırıların ilk sırada olduğu ayrıca, enerji altyapısının Endüstriyel Kontrol Sistemleri / Merkezi Denetim ve Veri Toplama Sistemleri üzerinden çalışmalarını devam ettiren kritik tesislerin saldırıya maruz kalma açısından ilgili sektörler arasında birinci sırada olduğu görülmektedir (Meral, 2015). Enerji sektörüne yapılabilecek bir siber saldırı durumunda abonelerin can ve mal güvenliği, ekonomik refahı azalmakta veya yok olmakta ve bir kamu hizmeti niteliğindeki enerjinin etkin ve verimli işleyişi bozularak hayatı durdurma noktasına kadar getirebilir. Bu durum araştırılan ülkeler tarafından kritik altyapılar kapsamında değerlendirilen enerji sistemlerindeki siber güvenliğin önemini ön plana çıkarmaktadır.

Enerji sistemlerinde bilgi güvenliği konusunda göz önünde bulundurulması gereken SCADA sistemlerinin bilgi güvenliğidir. Kritik altyapıların yönetiminde, hizmet sağlamak için coğrafi anlamda geniş alana yayılmış sistemdir. Bu sistemi oluşturan bileşenlerin merkezi olarak izlenmesi ve kontrol edilmesi için kullanılan sistemler olan SCADA sistemlerini kullanmaktadır (Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı, 2019). SCADA sistemlerinin bilgi teknolojilerine olan bağımlılığı ciddi güvenlik risklerini de beraberinde getirmektedir. Günümüz siber güvenlik endişelerini karşılayacak seviyede tasarlanmamış, basit, kriptosuz ve düşük hızda olan SCADA sistemleri kullanıldıkları enerji sistemlerini siber saldırılara hedef yapmaktadır (Kaspersky ICS CERT., 2019). Kritik üretim tesislerine karşı gerçekleştirilen saldırıların amaçlarından biri istihbarat sağlamak ve hedef hakkında bilgi toplamaktır. Ayrıca saldırılar çoğu zaman internet bağlantısına erişim imkânı sağlayan SCADA üniteleri üzerinden, çalışanların maksatlı veya maksatsız zafiyetler nedeniyle yazılım ve donanımların zayıf yönleri üzerinden gerçekleştirilmektedir (Meral, 2015). Enerji güvenliği ekonomik, toplumsal, siyasi ve jeopolitik risklerin

yönetilebilmesi için en temel maddi unsur olma özelliğini korumaktadır Modern dönemlerde enerji güvenliği olmaksızın askeri, siyasi, stratejik ve ekonomik alanların ötesinde çevre, su ve gıda gibi enerji ile doğrudan ilgi kurmakta güçlük çektiğimiz alanlarda bile güvenlikten söz etmek mümkün değildir (Özev, 2017). Dünyadaki gelişmelerle birlikte ülkemizde de enerji sistemlerinin altyapısının yönetilmesi ve izlenmesi büyük oranda BİT teknolojileri ile birlikte çalışan SCADA sistemleri ile gerçekleştirilmektedir (Kara ve Çelikkol, 2011). EKS kritik altyapılar kapsamında enerji sektöründe kullanılmakta olup güvenlik açısından hassas sistemlerdir (McGurk, 2008).

Bir ülkenin enerji sistemlerinde kullanılan bilişim teknolojilerinde meydana gelebilecek siber güvenlik olayları enerji hizmetlerinin durmasına, aksamasına, büyük ölçekli ekonomik zarar görülmesine, kamu düzeninin hasar almasına, can kaybının yaşanmasına ve hatta ülkelerin ulusal güvenliğinin hasar görmesine neden olma risklerini içermektedir. Elektrik sisteminde meydana gelebilecek kesintiler sonucu oluşacak zafiyet ve riskler milli güvenlik açısından da riskler taşımaktadır. Enerji sistemlerinde ve özellikle de SCADA sistemlerine yönelik meydana gelebilecek siber güvenlik olayları neticesinde;

- Ülkelerde mevcut rafineler ve nükleer santraller atom bombasına dönüştürülebilir.
- Doğalgaz enerji iletim sistemlerinde basınç artışı oluşturmak suretiyle doğal gaz boruları havaya uçurulabilir.
- Baraj kapakları açtırılarak şehirler ve tarım arazileri su altında bırakılabilir.
- SCADA altyapısında kritik bir işletme, fabrika veya merkezin elektrik tedarikini yapan fiderinde açma/kapama veya kısa devre yapılabilir. Bunun sonucunda enerji inkıtaları, hammadde yarı mamul veya mamul madde kayıpları ve hasarları, yangın ve sektöre bağlı olarak infilaklar yapılabilir.
- Özellikle kritik şehirleri besleyen ana indirici trafo merkezlerinde transformatörlerin çeşitli yollarla devre dışı bırakılması kısa devresi neticesinde arızalandırılması ya da trafo yağının yanarak yangına neden olması neticesinde şehirlerin elektriksiz bırakılarak karanlığa gömülmesi ve büyük üretim kayıplarına neden olunabilir.
- Enerji sistemlerine yönelik siber saldırılar neticesinde dünya çapında kaoslar oluşturulabilir, ülke güvenlikleri tehlikeye atılabilir, sağlık, ulaşım, haberleşme

hizmetleri gibi hayati faaliyetler sekteye uğratılabilir, ülkeler enerji sistemlerine yönelik tehditlere karşı savunmasız hale getirilebilir.

- Kamu düzeni bozulabilir ve hatta ulusal güvenlik ihlaline neden olabilir.

Türkiye'de kamu kurumlarının kullanımında olan siber güvenlik araçlarının %97'si yabancı menşeli olup %3'ü yerli ve/veya milli kaynaklarla üretilmiştir (Afyonluoğlu, 2018). Bu durum enerji sistemlerinde siber güvenlik bağlamında yerli ve milli bilişim sistemlerinin kullanılmasının önemini ortaya koymaktadır. Yerli ürün ve teknoloji eksikliği ulusal ölçekte siber güvenlik zafiyeti meydana getirmektedir. Bu yüzden öncelikle kritik altyapılar olması ile birlikte güvenlik sertifikası ile tescillenmiş yerli siber güvenlik teknolojisi, çözümü ve ürünlerinin yaygın olarak kullanılmasını desteklemek üzere gerekli teşvik ve zorunlulukların getirilmesi gereklidir (Türkiye Bilişim Derneği, 2020).

Uluslararası ortaklarla birlikte girişilen projelerden olan nükleer enerji santralleri göz önüne alındığında, projeyi Türkiye ile birlikte yürüten ortakların zafiyetlerini veya çıkarlarını hedef alan siber saldırıların oluşması halinde ülkemizin de zarar görmesi ihtimali göz önünde bulundurulmalıdır Türk ekonomisinin büyüme göstermesi enerji altyapısının, elektrik üretiminin ve hidro-stratejik öneme sahip barajların gelişimine doğrudan bağımlı olması ve Türkiye'nin enerji geçiş merkezi haline getirilmesi gibi stratejik hedeflerin izlemesi sürdürdüğünden siber güvenlik ortamı kritik bir parçadır (Han ve Çelikpala, 2016).

2. ENERJİ SİSTEMLERİNE YÖNELİK SALDIRI ÖRNEKLERİ

Siber saldırıların sektörel dağılımına bakıldığında enerji sektörüne yapılan saldırıların ilk sırada bulunduğunu ve enerji altyapısında ICS/SCADA sistemlerin barındırarak faaliyetlerini devam ettiren kritik tesislerin saldırıya maruz kalma kalma durumunu en fazla olan sektörler arasında birinci sırada olduğu görülmektedir (Kaspersky ICS CERT, 2020). Enerji sitemlerine yönelik en önemli ve bilinen siber saldırı örneği olarak "Stuxnet" yazılımı gösterilmektedir. Stuxnet ile yapılan bir saldırıda birinci aşamada hedef tesisin SCADA sistemine bağlı olarak çalışan ve sistemin yönetilmesini sağlayan programlanabilir mantıksal denetleyicileri (PLC) kontrolünü ele geçirmiştir. Daha sonraki aşamada kontrol için kullanılan SCADA cihazları ile 100 milisaniyede aralıklarla komut göndererek santrifüjlere enerji sağlayan elektrik akım frekanslarında dalgalanmalar meydana getirmiştir. Bu yöntemle genel sürecin kesintiye uğramasına neden olmuştur. Stuxnet siber güvenlik açıklıklarını kullanarak İran'da bulunan nükleer tesislere yönelik zarar vermeye yönelik faaliyetlerini, mevcut imkân ve gelişerek sürekli

güncellenme halinde olan bütün güvenlik önlemlerine rağmen devam ettirmiştir. Stuxnet yöntemiyle devlet kurumlarından bağımsız kişi ve kişiler tarafından yürütülen siber saldırılar; artık sistemler üzerinde büyük oranda fiziksel hasar verebilecek, etkili siber silahlar oluşmasının yolunu açılmıştır (Meral, 2015). SCADA protokollerinden Modbus protokolüne yönelik Command Injection, Reconnaissance and DoS (Denial of Service) gibi kategorilerde çeşitli ataklar gerçekleştirilmiş ve en doğru sınıflandırma oranının Random Tree algoritması ile sağlandığı görülmüştür (Söğüt ve Erdem, 2020).

2010 yılından önce bilgisayar virüsleri aracılığıyla küçük ölçekte karıştırma, bozma, veri kaybı gibi olaylar yaşanan SCADA sistemlerinde, stuxnet yöntemi kullanılarak bir devletin ulusal kritik altyapılarına sızma girişimiyle karşılaşılmıştır. Halihazırda elektrik dağıtım yönetim sistemleri ve SCADA sistemleri de internete bağımlı olmayan yazılımlar olmasına karşın Stuxnet örneğinde olduğu gibi siber savaş ve siber terörizmin etkisi altında olduğu bir gerçektir. Tablo 1 üzerinde SCADA sistemlerine yönelik gerçekleştirilen ve kayıt altına alınmış olan saldırılar verilmiştir (Çiftçi, 2013; Kaspersky ICS CERT, 2020).

Tablo-1. SCADA Sistemlerine Yönelik Saldırılar

Yıl	Olay Tanımı	Olay Yeri
2000	Hırsızlık ve alarm sistemlerine saldırı.	Avustralya
2000	Gazprom petrol boru hattına saldırı.	Rusya
2001	Atık su sistemine saldırı.	Avustralya
2003	Nükleer santrale saldırı.	Amerika
2003	Hidroelektrik santralin kilitlenmesi.	Türkiye
2003	Yazılım firmalarına düzenlenen saldırı.	Amerika
2004	Demiryolu hatlarının kapanması.	Amerika
2008	Nükleer santrale saldırı.	Amerika
2009	Nükleer tesislerinin Stuxnet solucanından etkilenmesi.	İran
2010	Stuxnet ile SCADA saldırısı.	İran
2012	SCADA sisteminin IP adreslerine saldırı.	Rusya
2014	SCADA sistemine saldırı.	Finlandiya
2015	Elektrik şebekesine saldırı.	Ukrayna
2015	Elektrik şebekesine saldırı.	Türkiye
2016	Elektrik kesintisi.	Ukrayna
2016	Nükleer tesislerin santrallerine yapılan saldırı.	Almanya
2019	Elektrik santrali SCADA sistemi saldırısı.	Amerika
2020	Rüzgâr türbinleri SCADA sistemlerine saldırısı.	Azerbaycan

Tablo 1'de verilen örnek olaylar SCADA sistemlerinin BİT sistemleri ile bütünleşmesi birçok kolaylık ve esnekliği getirse de siber güvenlik açısından önemli riskleri de birlikte getirdiğini göstermektedir. Söz konusu risklerin ortadan kaldırılması veya olası etkilerinin en aza indirgenmesi için yönetimsel, teknik ve yasal boyutta düzenlemeler yapılması şarttır. Enerji sistemlerinin kesintisiz olarak, güvenli ve belirli bir kalitede hizmet vermesinde SCADA sistemlerinin siber güvenliği konusu büyük önem taşımaktadır.

2.1. Yaşanmış Büyük Ölçekli Elektrik Kesintileri

Elektrik sistemleri altyapısı, domino taşı etkisine sahip olması nedeniyle kritik altyapılar arasında ayrıca üzerinde durulması gereken bir konudur. Çünkü hayati öneme haiz olan ve kritik olduğu değerlendirilen altyapıların neredeyse tamamı elektriğin olmaması durumunda hizmetlerini sürdüremezler. Diğer kritik altyapıların yanında elektrik altyapısının önemi ayrı önem taşımaktadır. Çünkü elektrik depolanamaz ve uzun süreli ikame edilemezken diğer enerji kaynakları için bu durumlar yaşanmamaktadır. Elektrik sistemlerinin bir sorunla karşılaşması halinde diğer altyapı hizmetlerinde de aksamalar meydana gelmektedir.

Bir siber saldırı durumunda, gözlem ve kontrol görevlerini yerine getiren SCADA/ICS sistemlerinde üzerinden yaşanan aksaklıklarla birlikte kesinti yaşanan elektrik altyapısında olayın uzun süre yaşanmasına ve büyük ölçekli hasarlara yol açmaktadır. Tablo 2'de dünya tarihinde meydana gelmiş olan etki alanı ve sonuçlarına göz önüne alınarak değerlendirildiğine etkili olduğu ifade edilen büyük çaplı elektrik kesintileri verilmiştir (Meral, 2015).

Tablo-2. Büyük Çaplı Elektrik Kesintileri

Kesinti Yeri	Tarihi	İnsan Sayısı (milyon)	Süre (saat)
Brezilya	11 Mart 1999	97	4
Hindistan	02 Ocak 2001	230	12
ABD - Kanada	14 Ağustos 2003	50	4-7
İtalya	28 Eylül 2003	56	18
Java - Bali	18 Ağustos 2005	100	11
Brezilya - Paraguay	10-11 Kasım 2009	87	7
Hindistan	30-31 Temmuz 2012	350-680	6-14
Bangladeş	01 Kasım 2014	150	10-12
Pakistan	26 Ocak 2015	140	12
Türkiye	31 Mart 2015	70	3 - 10
Ukrayna	23 Aralık 2015	1	6

2003 ABD ve Kanada Elektrik Kesintisi sonucunda;

- Otomobil ve motor üretim tesislerinden General Motors ve Ford gibi büyük şirketleri de içeren en az 70 adedinin faaliyetleri kesinti boyunca durdurulmuş ve bu süre sırasında neredeyse 100.000 çalışan işine gidememiştir.

- 8 adet petrol rafinerisi yaşanan kesinti yüzünden etkilenmiştir. Bazı eyaletlerde bu yüzden meydana gelen üretim kaybı yakıt tedariki sorununa yol açmıştır.

- Yaşanan kesinti dolayı su altyapısında etkilemiştir. Bu durum su kesintilerinin de yaşanmasına yol açmıştır.

- Elektrikli toplu taşıma sistemlerinden metro ve tren seferleri durmuştur. Yaşanan aksaklık nedeniyle yüksek binaların asansörlerinde ve toplu taşıma sistemlerinde mahsur kalmışlardır.

- Demir-çelik fabrikalarında üretim faaliyetleri durmuş ve bazı fabrikalarda kesintiden sonra erimiş haldeki çeliği soğutmak için kullanılan sistemler çalışmadığından dolayı yangınlar meydana gelmiş, büyük çapta hasara neden olmuştur.

- Özellikle Ontario eyaletinde birbirine yakınn bölgelerde bulunan kimyasal-petrokimyasal tesislerde kesinti nedeniyle çalışma süreçlerinde aksaklıklar yaşamıştır. Büyük çaplı bölgede çevrenin zarar görmesine yol açan bu aksaklıklar ayrıca saat başı on ile yirmi milyon dolar arasında maddi zarara neden olmuştur.

- Büyük şehirlerde trafik ışıklarının çalışmaması nedeniyle karayolu ulaşım sistemleri durmuştur.

- Günlük ihtiyaçların karşılandığı ilaç şirketleri, restoranlar, marketler ve esnaflar gerçekleştirdikleri üretim veya sağladıkları hizmetlerini durdurmak durumunda kalmıştır. Gıda depolama ve gıda tedarikçileri büyük zarara uğramışlardır.

- Telefon altyapısı elektrik kaynağına ihtiyaç duyduğu için kesintinin başlaması ile birlikte sabit telefonlar kullanılamamıştır. Mobil telefonlarda yaşanan yoğunlukdan dolayı kullanılamamıştır.

31 Mart 2015 tarihi sabah saatlerinde Türkiye'de meydana gelen elektrik kesintisinin nedeni henüz tam olarak belirlenememiştir (Meral, 2015). Söz konusu kesinti sonrası Türkiye'de;

- Şehirlerde toplu taşımada kullanılan elektrik ile çalışan araçların seferlerinde iptaller oluşmuştur. İptaller nedeniyle trafik yoğunluğu yaşanmıştır.

- Kara yolları üzerinde gerçekleşen kesinti nedeniyle trafik ışıklarının devre dışı kalması trafik karmaşası gerçekleşmiştir.

- Hastane hizmetlerinden acil servis ve yoğun bakım üniteleri dışında kalan bölümlerde sağlık hizmeti verilmemiştir.

- Okullar ve devlet kurumlarının birçoğunda hizmetlerde aksama yaşanmış ve personeller evlerine dönmek durumunda kalmıştır.

- Üretim sektörlerinde vardiyalar durdurulmuştur.

3. TÜRKİYE'DE ENERJİ SİSTEMLERİNDE SİBER GÜVENLİĞİN SAĞLANMASI ÇALIŞMALARI

Türkiye'nin siber güvenlik alanında kurumsallaşması kapsamında; İçişleri Bakanlığı bünyesinde oluşturulan Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı (JGK) Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü, BTK, MİT Başkanlığı, Afet ve Acil Durum Yönetimi (AFAD) Başkanlığı, TSK Siber Savunma Komutanlığı, TÜBİTAK, Savunma Teknolojileri Mühendislik, Hava Elektronik Sanayii (HAVELSAN) ve Askeri Elektronik Sanayii (ASELSAN) ve Siber Güvenlik Kurulu (SGK) yer almaktadır. 2012'de Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu tarafından Ulusal Siber güvenlik ile ilgili politika, strateji ve eylem planlarını oluşturmak ve kritik altyapıların belirlenmesinde teklifleri karara bağlamak için Siber Güvenlik Kurulu oluşturulmuştur. Bu Kurul 2013 yılında Türkiye'nin ilk Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı yayımlamıştır.

Ülkemizde 2020 yılında Ankara'da teknoloji altyapısı ile tamamlanan Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile ulusal ve uluslararası tehditlerin belirlenmesi, yapılacak muhtemel saldırı ve olayların etkilerini azaltılması için kurulmuştur. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında (2012) Türkiye'de Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri (SOME) oluşturulması için karar alınmıştır. Türkiye'de kritik altyapıların korunması amacıyla siber güvenlik kapsamında katkı sağlayan önemli adım "2013–2014 Eylem Planı"dır. Söz konusu plan ile "Ulusal Siber Olaylara Müdahale Merkezi" (USOM) ve "Siber Olaylara Müdahale Ekipleri" (SOME) kurulması öngörülmüştür. Böylelikle Türkiye'de enerji sektöründe de kamu kurumları ile özel kuruluşlar SOME'lerini kurmaya başlamışlardır. Halen Türkiye'de enerji sektörünün sektörel SOME'si olarak Enerji Piyasası Düzenleme Kurumu'dur.

Günümüzde Türkiye'de enerji dağıtım, iletim, üretim ve rafineri alt sektörlerinde faaliyet gösteren SOME'lerin sayısı her geçen gün artmaktadır.

2016 yılında Türkiye Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) tarafından Enerji Piyasası Düzenleme Kurumunun görev alanına giren konuları da içere"2016-2019 Ulusal Siber Güvenlik Strateji Belgesi" yayımlanmıştır. Türkiye'nin bu eylem planında 2013-2014 Eylem Planında olduğu gibi siber güvenlik riskleri ve göz önünde bulundurulması gereken ilkeler açıklanmıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında (2016) kritik altyapıların kullandığı bilişim sistemlerine karşı gerçekleştirilecek saldırılar sonucunda enerji, ulaştırma, vb. kritik öneme sahip hizmetlerde kesinti yaşanması konusu siber güvenlik riskleri arasında tanımlanmıştır. Türkiye'de kritik altyapılara ait bilişim sistemlerinin siber güvenlik sorumluluğu TÜBİTAK'a verilmiştir. Türkiye "2016-2019 Ulusal Siber Güvenlik Strateji Belgesinde" enerji sistemlerinin siber güvenliğine ilişkin hususlar Tablo 3'de sunulmuştur.

Tablo-3. 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi

S.Nu.	Enerji Sistemleri ile İlişkilendirme
1.	Kritik Altyapılar: 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma" ve "Bankacılık ve Finans" sektörlerini, ifade eder.
2.	Siber Güvenlik Riskleri: Kritik altyapıların kullandığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırılar sonucunda enerji, ulaştırma, vb. kritik hizmetlerin kesintiye uğraması.

Tablo 3'de yer alan hususlar incelendiğinde; Türkiye'de enerji sistemlerinin siber güvenliğinin kritik altyapılar ile ilişkilendirildiği görülmektedir. Söz konusu strateji belgesinde yer alan önemli bir belirleme enerji sistemlerinin kullanımında olan bilişim sistemlerine karşı gerçekleştirilecek faaliyetini durdurma gibi hedef odaklı saldırılar sonucunda enerji hizmetlerinin kesintiye uğrayabileceğine ilişkin yapılan vurgudur. Burada enerji sistemlerinin siber güvenliğinin, ulusal siber güvenlik politikasının doğal bir parçası olarak görüldüğü söylenebilir.

Türkiye'de 2017 yılında "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği" Resmi Gazatede çıkan bir karar ile yayınlanmış ve uygulamaya alınmıştır. Bu Yönetmeliğin amacı; kritik enerji altyapılarında kullanılan endüstriyel kontrol sistemlerinin (EKS) bilişim

süreçlerinin izlenmesi, sistem sürekliliğinin sağlanması ile siber güvenliğinin sağlanmasına ilişkin usul ve esasları düzenlemektir. 2017 yılında ayrıca siber savunma faaliyetlerini bir birimden yönlendirmek, siber olayların takibi, analizi ve değerlendirmelerini yapmak, siber güvenlik standartlarını belirlemek ve kullanılan sistemlerin zafiyet analizlerini yapmak için Siber Savunma Harekat Merkezi kurulmuştur. Bu merkezde 2020 yılı ilk çeyreğinde milli olarak geliştirilen yazılımlar kullanılmaya başlanmıştır.

Türkiye'de siber güvenlik ürünlerinde yerli ve/veya milli ürün kullanılması hususu enerji sistemlerinin güvenliğinin sağlanmasında dikkate alınması gereken bir konudur (Afyonluoğlu, 2018). Siber güvenlik tatbikatları Türkiye'de Siber güvenlik alanında yapılan önemli çalışmalar arasındadır. Günümüzdeki teknolojik gelişmelere rağmen enerji altyapıları için SCADA ve kontrol sistemlerine yönelik olarak Stuxnet siber saldırısına benzeyen siber saldırılar yapılabilir.

Türkiye'nin ulusal güvenliği açısından enerji sistemlerinin siber güvenliği; ekonomik, toplumsal, siyasi ve jeopolitik risklerin yönetilebilmesi için ana unsurlardan birisidir. Türk ekonomisinin büyüme sağlaması enerji altyapısına, elektrik üretimine ve hidro-stratejik önemi bulunan barajlara doğrudan bağımlıdır. Bu durumla birlikte Türkiye'yi enerji kaynaklarının aktarım merkezi haline getirmek gibi stratejik hedefler sürdürüldüğü için enerji altyapılarında siber güvenlik ortamının geliştirilmesi kritik öneme sahiptir (Han ve Çelikpala, 2016). Enerji santrallarına veya elektrik dağıtım şebekelerine düzenlenebilecek Stuxnet benzeri siber saldırılar bir ülkenin tamamının günlerce elektriksiz bırakılması ve çok büyük bir ekonomik zarar verilmesi mümkün gözükmektedir. Enerji sistemlerine yönelik yapılabilecek siber saldırılar bir ülkenin askeri gücünüzü de sekteye uğratabilir. Gelişmiş ülkelerde olduğu gibi güvenlik testlerinden geçirilmiş ve ulusal sertifikasyona sahip milli SCADA ve siber güvenlik ürünlerine sahip olunması durumunun Türkiye'nin enerji güvenliğine etkisi büyük olacaktır.

SONUÇ ve ÖNERİLER

İçinde bulunduğumuz bilgi çağında enerji sistemlerine olan bağımlılık giderek artmıştır. Bu durum enerji sistemlerinin bilgi güvenliği olgusunun önemini de arttırmıştır. Enerji sistemlerinin bilgi güvenliği günümüzde devletlerin ulusal güvenliklerini sağlayabilmek adına öne çıkan bir konu haline gelmiştir. Çünkü siber saldırıların sektörel dağılımına bakıldığında enerji sektörüne yapılan saldırıların ilk sırada bulunduğu görülmektedir. Enerji sistemlerine yönelik olası siber tehdit ve saldırılar dünya ülkelerinin enerji hizmetlerinin durmasına, aksamasına, büyük ölçekli ekonomik zarar görülmesine, kamu düzeninin hasar

almasına, can kaybının yaşanmasına ve hatta ülkelerin ulusal güvenliğinin hasar görmesine neden olabilmektedir. Ülkelerin enerji sistemlerine yönelik siber tehdit ve saldırılardan zarar görmemek için kısa, orta ve uzun vadede stratejik seviye dâhil başta farkındalık olmak üzere teknolojik çalışmalarda dâhil çalışmalar yaparak enerji sistemlerinin siber güvenliğine yönelik gerekli siber güvenlik tedbirlerini almaları gerektiği ortadadır. İçinde bulunduğumuz bilgi çağında enerji sistemlerine yönelik bilgi güvenliğini anlamlandıramayan ve gerekli tedbirleri almayan ülkelerin enerji sistemleri kritik altyapıları ciddi siber güvenlik risk, saldırı ve tehditlere maruz kalacak, enerji sistemleri bilgi güvenliğine yönelik gerekli hassasiyeti gösteren ve tedbirleri alarak uygulama geçiren ülkeler ise maruz kaldıkları tehditleri en aza indirmeyi başarabileceklerdir.

Enerji siber güvenlik kavramı enerji sistemlerine yönelik gerekli önlemler alınmadığında büyük ölçekte zararlara neden olacak nitelikte bir güvenlik bileşenidir. Enerji sistemlerinde siber güvenliğin sağlanmasına yönelik alınacak siber güvenlik tedbirlerinin hayati derecede öneme sahip olduğu, enerji sistemlerinin siber güvenliğinin bir ulusal güvenlik politikası olarak değerlendirilmesi gerektiği ortaya çıkmıştır. Ayrıca mümkün olan her alanda ve aşamada siber güvenlik eğitimleri ve bu alanlarda farkındalık yaratılmasını sağlayacak organizasyonların gerçekleştirilmesi gerekliliği ortaya çıkmaktadır. Sektörde bulunan kuruluşların ve kurumların birbirleri ile bilgi paylaşımı ve iş birliği sağlaması ihtiyacının önem kazandığı ortadadır. Bu durumu enerji sistemlerine yönelik yaşanan siber saldırılar doğrulamaktadır. Ülkelerin enerji sistemlerine olan bağımlılığı kapsamında gelecekte enerji sistemlerine yönelik siber tehdit ve saldırıların daha yoğun şekilde gözlemleneceğini kestirmek güç değildir.

Siber güvenlik kapsamında enerji sistemleri güvenliğinin değerlendirilmesine yönelik yapılan bu çalışmada aşağıdaki sonuçlara ulaşılmıştır.

- Enerji sistemlerinde BİT ve özellikle de internetin yaygın olarak kullanımı siber güvenlik risk ve belirsizlikleri de beraberinde getirmektedir.

- Enerji sistemlerine ve özellikle de SCADA sistemlerine yönelik araştırılan siber saldırılar bu sistemlerin siber tehdit ve saldırıların odağı haline geldiğini ortaya koymaktadır.

- Enerji sistemlerinin siber güvenliğinin sağlanmasına yönelik alınacak siber güvenlik tedbirleri hayati derecede öneme sahiptir.

- Araştırılan ülkelerin enerji sistemleri siber güvenliğini kritik altyapılar kapsamında değerlendirdikleri görülmektedir. Bu ülkeler enerji sistemlerine yönelik siber güvenlik saldırı ve tehdit risklerini yönetilebilir ve kabul edilebilir düzeylerde tutmak maksadıyla stratejik seviyede çalışmalar yapmaktadırlar.

- Türkiye'nin de incelenen ülkelere benzer şekilde enerji sistemlerinde siber güvenliğin sağlanmasına yönelik stratejik seviyede çalışmalar yaptığı görülmektedir. Türkiye "2016-2019 Ulusal Siber Güvenlik Strateji Belgesi" Türkiye'de yapılmış Siber Güvenlik alanında en önemli çalışmalardan birisidir. Bu belgede Türkiye'de enerji sistemlerinin siber güvenliğinin kritik altyapılar ile ilişkilendirildiği görülmektedir. Bu belgede enerji sistemlerinin siber güvenliği ulusal siber güvenlik politikasının doğal bir parçası olarak ele alınmaktadır.

Ulaşılan bu sonuçlara dayanarak Türkiye'de enerji sistemlerinin siber güvenliği konusunda aşağıdaki öneriler getirilebilir.

- Elektrik Dağıtım Yönetim Sistemi'nde şebekeye ve abonelere ait "büyük bilgi" yığınlarının depolanması ABD, Çin gibi belli başlı ülkelerde yapılmakta olup, siber güvenlik tehdidi açısından bu yığınların da lokalleştirilmesi, depolama şekli ve yönetilmesi siber güvenlik tehditleri arasında çözülmesi gereken bir problemdir.

- Tek bir siber saldırı yöntemi ile tüm ülke şebekesinin arz güvenliğinin tehlikeye düşebileceği dikkate alınarak enerji sistemlerinin siber güvenliğine ilişkin yaklaşım genel bir ulusal güvenlik politikası gibi değerlendirilmelidir.

- Hem kamu hem de özel sektörde enerji sistemlerine yönelik aktörlerin (dağıtım şirketleri vb.) enerji sistemlerinin bilgi güvenliği konusunda farkındalığın artırılmasına yönelik gerekli çalışmalar yapılmalıdır.

- Enerji sektörüne yönelik siber tehdit ve saldırılara karşı gerekli siber savunma tedbirleri proaktif tedbirlerle alınmalı, bu konuda tatbikatlar planlanmalı ve yapılmalıdır.

- Kritik enerji altyapılarının siber saldırı ataklarından korunması için çalışmalar tüm enerji sektörünü barındıran bütüncül bir bakış açısıyla değerlendirilmeli ve takibi sağlanmalıdır.

- Enerji sektöründe SCADA sistemlerinde kullanılan yazılımların kaynak kodları ürün güvenlik sertifikasyonları ile birlikte tedarikçi firmalardan temin edilmeli, bu sistemlerin farklı güvenlik seviyesine sahip ağlar bazında birbirinden ayrıştırılarak çalıştırılması, bu sistemlere yönelik gerçekleşen zafiyet ve saldırılar takip edilmeli, gereken yazılım yamaları ve önlemlerin zamanında alınması sağlanmalıdır.

- Özellikle en başta yabancı firmalardan tedarik edilen enerji dağıtımında kullanılan bilişim ve otomasyon-kontrol yazılımlarının periyodik yazılım güvenliği testleri bu konuda yetkin yerli ve milli yazılım şirketlerine yaptırılmalıdır.

- Enerji sistemlerine ilişkin gerekli hususları içerecek hususları kapsayan siber güvenlik strateji ve politikaları, genel bir ulusal güvenlik politikası gibi değerlendirilmelidir.

- Özel sektörün enerji sistemlerinde başta milli SCADA Sistemlerinin geliştirilmesi olmak üzere AR-GE çalışmaları yapması teşvik edilmelidir.

- Kamu ve özel sektör iş birliğinde yerli siber güvenlik ekosistemi oluşturulmalıdır. Bu bağlamda siber güvenlik testlerinden geçirilmiş ve ulusal sertifikasyona sahip milli siber güvenlik bilgi teknoloji ve ürünleri (SCADA vb.) kullanılmalıdır. Bu durumu teşvik edecek politika ve stratejiler geliştirilmelidir.

- Enerji sektöründe ulusal siber güvenlik testlerinden geçirilmiş ve ülkemiz sertifikasyonuna sahip akredite yerli güvenlik danışman şirketleri tarafından tasarlanmış ve test edilmiş milli siber güvenlik bilgi teknolojileri ve ürünleri kullanılmalıdır.

KAYNAKÇA

Afyonluoğlu, M. (2018). Siber Güvenlik ve Kamu Kurumları için Milli Sertifikasyon Mekanizması. Erişim tarihi: 11 Mayıs 2020, https://afyonluoglu.org/PublicWebFiles/Reports/20180121-Siber%20G%C3%BCvenlik%20ve%20Milli%20Sertifikasyon%20Mekanizmas%C4%B1.pdf

Akıllı, H., & Kızılboğa Özaslan, R. (2017). Su kayıplarının önlenmesinde teknoloji kullanımı: Büyükşehir Belediyelerinde SCADA uygulaması. Suleyman Demirel University Journal of Faculty of Economics & Administrative Sciences, 22.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi.

Boyd, B. L. (2009). Cyber warfare: Armageddon in a Teacup?. Army Command and General Staff Coll Fort Leavenworth KS.

Çıtak, E. (2019). Silahsız Savaş Sahası: Yeni Savaş Anlayışında İstihbaratın Yeri. Güvenlik Bilimleri Dergisi, 8(2), 191-213.

Çiftçi, H. (2013). Her Yönüyle Siber Savaş. TÜBİTAK.

Dedemen, F. (2016). Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi. Güvenlik Bilimleri Dergisi, 5(1), 141-176.

Denizcilik, U., & Bakanlığı, H. (2012). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.

Erendor, M. E. (2016). Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu. Cyberpolitik Journal, 1(1), 114-134.

Executive Office of the President. (2016). National Electric Grid Security and Resilience Action Plan, Executive Office of the President, Erişim tarihi: 10.05.2020, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf

Gençtürk, T. (2012). Enerji Güvenliği Nedir? Ulusal ve Uluslararası Boyutta Enerji Güvenliği Sorunu. Başkent Üniversitesi Stratejik Araştırmalar Merkezi Raporu.

Güntay, V. (2017). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. Güvenlik Bilimleri Dergisi, 6(2), 81-108.

HM Government. (2016). National Cyber Security Strategy 2016-2021.

Han, A. & Çelikpala, M. (2016). Uluslararası Çerçevede Siber Güvenlik ve Nükleer Enerji. Ekonomi ve Dış Politika Araştırmalar Merkezi. Erişim tarihi: 01.05.2020, https://edam.org.tr/wp-content/uploads/2017/10/edam_siber_guvenlik_raporu.pdf

Hardy, K., & Williams, G. (2014). What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism. In Cyberterrorism (pp. 1-23). Springer, New York, NY.

Hawks, B. B. (2010). Cyber terror: The borderless danger.

Homeland Security. (2012). National Protection and Programs Directorate Office of Infrastructure Protection Strategic Plan: 2012–2016.

Hopkins, S., & Kalaimannan, E. (2019). Towards establishing a security engineered SCADA framework. Journal of Cyber Security Technology, 3(1), 47-59.

Irmak, E., & Erkek, İ. Endüstriyel Kontrol Sistemleri ve SCADA Uygulamalarının Siber Güvenliği: Modbus TCP Protokolü Örneği. Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 6(1), 1-16.

ISACA, C. (2017). Cybersecurity Fundamentals. Study Guide.

İşbilen, F., & Konar, M. (2020). Uçak Sistemlerinin SCADA İle Modellenmesi. Avrupa Bilim ve Teknoloji Dergisi, (18), 338-346.

Johnson, T. A. (Ed.). (2015). Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. CRC Press.

Kaptan, S. (1995). Bilimsel araştırma teknikleri ve istatistik teknikleri. Rehber Yayınevi.

Kara, M., & Çelikkol, S. (2011). Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği. IV. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara.

Kaspersky ICS CERT. (2020). Overview of recommendations on organizing secure remote work for critical infrastructure and other facilities, Erişim Tarihi: 30.04.2020, https://ics-cert.kaspersky.com/reports/2020/04/30/secure-remote-work-for-critical-infrastructure/

Kolevar, K. M. (2007). Energy Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan (Redacted).

Kurnaz, S., & Karatepe, S. (2019). Kamusal Kritik Tesislerin Güvenliği Kapsamında Türkiye'deki Hava Alanlarının Siber Güvenliği. ASSAM Uluslararası Hakemli Dergi, 119-129.

Küçüksille, U. E. Genç, N. S. & Karabulut, E. Y., (2013). Dünyada Siber Güvenlik Stratejileri ve Bir Siber Güvenlik Stratejisinin Oluşumu. 1 st International Symposium on Digital Forensics and Security.

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: Center for Strategic & International Studies.

Meral, M. (2015). Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi. Harp Akademileri Stratejik Araştırmalar Enstitüsü Savunma Kaynakları Yönetimi Ana Bilim Dalı, İstanbul, 54-73.

McGurk, S. P. (2008). Industrial control systems security: Protecting the critical infrastructure. In a Presentation by tge US Department of Homeland Security. Available Online: https://csrc. nist. gov/CSRC/media/Events/ISPAB-DECEMBER-2008-MEETING/documents/ICSsecurity_ISPAB-dec2008_SPMcGurk. pdf (Accessed on: 09/18/2018).

Mudrinich, E. M. (2012). Cyber 3.0: The department of defense strategy for operating in cyberspace and the attribution problem. AFL Rev., 68, 167.

Özev, M. H. (2017). Küresel denklemde Türkiye'nin enerji güvenliği. Seta.

Söğüt, E., & Erdem, O. A. (2020). Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi. Politeknik Dergisi, 23(2), 557-566.

Şimşek, M. A., & Özen, F. Realization of A Building Automation System Using PLC and SCADA. International Journal of Engineering and Innovative Research, 1(1), 28-34.

Takaoğlu, M., & Çağdaş, Ö. Z. E. R. (2019). Saldırı Tespit Sistemlerine Makine Öğrenme Etkisi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 3(1), 11-22.

Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. Future Internet, 10(8), 76.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK). (2019). Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı. Erişim tarihi: 25.05.2020, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kritik-

bilgi-sistem-altyapilari-i-c-in-asgari-gu-venlik-o-nlemleri-6445b90e-b2ad-4e5e-9c13-6ae19ba10e37.pdf

Türkiye Bilişim Derneği. (2020). 3. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi Sonuç Raporu. Ankara.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. Erişim tarihi: 20.05.2020, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

Uygulamalarının Siber Güvenliği: MODBUS TCP Protokolü Örneği. Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 6(1), 1-16.

Usak, (2011). Kritik Enerji Altyapı Güvenliği Projesi Sonuç Raporu. Ankara: Uluslararası Stratejik Araştırmalar Kurumu.

Weed, S. A. (2017). US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure. Air University Press, Air Force Research Institute.

Yılmaz, E. N., & Gönen, S. (2018). Attack detection/prevention system against cyber attack in industrial control systems. Computers & Security, 77, 94-105.

Zanini, M., & Edwards, S. J. (2001). The networking of terror in the information age. Networks and netwars: The future of terror, crime, and militancy, 32.