ARAŞTIRMA

Geliş Tarihi: 18.12.2020
Kabul Tarihi: 12.01.2021

TÜRKİYE'DE KRİTİK ALTYAPI VE KRİTİK ALTYAPIYA YÖNELİK TEHDİTLER

Critical Infrastructure In Turkey And Threats For Critical Infrastructure

Abdullah GENCO*

Özet

Kritik altyapı ülkelerin her türlü faaliyetlerini yürütebilmeleri ve gündelik yaşamın gereklerinin sağlanmasında kullanılan hayati öneme sahip sistemlerin internet hatları vasıtasıyla koordine edildiği bir sistemler sistemidir. Kritik altyapı kavramı ortaya atıldığı 1997 yılından itibaren kabul görmüş ve kritik altyapı kurma imkanına sahip olan birçok ülkede kurulmaya başlamıştır. Sadece ulusal değil bölgesel ve küresel anlamda öneme sahip olan kritik altyapılar hem uluslararası işbirliğinin hem de savaş ve tehdit algılarının da değişmesine sebep olmuştur. İletişim ve bilgi teknolojisinin gelişimi yeni bir siber dünya yaratmış ve kritik altyapılar bu siber dünyada tehditlere karşı korunması gereken en önemli sistemler olarak öne çıkmışlardır. Bu çalışmada literatür taraması ile elde edilen bilgiler ile kritik altyapı kavramının ortaya çıkışı, ABD, AB ve Türkiye'de kritik altyapılar, kritik altyapılara yönelik tehditler ve alınması gereken önlemler ele alınmıştır.

Anahtar Kelimeler: *Kritik Altyapı, Siber Saldırı, Bilgi Teknolojisi SCADA*

Abstract

Critical infrastructure is a system of systems in which the vital systems used for the countries to carry out all kinds of activities and to meet the requirements of daily life are coordinated through internet lines. Since 1997, when the critical infrastructure concept was introduced, it has been accepted and started to be established in many countries that have the opportunity to establish critical infrastructure. Critical infrastructures, which are important not only nationally but also regionally and globally, have caused changes in both international cooperation and perceptions of war and threat. The development of communication and information technology has created a new cyber world and critical infrastructures have emerged as the most important systems that must be protected against threats in this cyber world. The emergence of this study, the concept of critical infrastructure with information obtained through literature, US, EU and critical infrastructure in Turkey, threats and measures to be taken against critical infrastructure are discussed.

Keywords: *Critical Infrastructure, Cyber Attack, Information Technology, SCADA*

*Abdullah GENCO, Araştırma Görevlisi, , Hacettepe Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, agenco@hacettepe.edu.tr

1. Giriş

Bilgi iletişim teknolojilerinin gelişme hızı 20. yüzyılın ikinci yarısıyla birlikte artmış; 21. yüzyılın başlarından itibaren de bu gelişim zirve noktasına ulaşmıştır. Bu gelişimin etkileri bireysel ve kamusal hayatın neredeyse her alanında etkisini hissettirmektedir. Bireylerin tek tek ve toplumun bütünün faydalandığı bu teknolojinin sağladığı kolaylıklar için günlük kullanıma ait ulaşım, iletişim ve haberleşme alanından örnekler vermek mümkündür. Tüm hizmetlerin sunumunda kritik altyapı kavramı da gelişen teknolojinin bir sonucu olarak hayatımıza girmiştir.

Canlılara benzer olarak toplumlar ve devletler de varlıklarını sürdürebilmek için enerjiye ihtiyaç duymaktadırlar. Sadece enerjinin varlığı değil enerjinin kaynağından tüketiciye ulaştırılmasındaki süreklilik de çok önemlidir. Enerji kaynakları coğrafi olarak eşit dağılmadığından bu kaynakların kullanıcılara -oluşturulacak ağlar vasıtasıyla- kesintisiz bir biçimde ulaştırılması için güçlü sistemlere gereksinim duyulmaktadır. Enerji kaynaklarına ek olarak toplumun düzeni, vatandaşların refahı ve kamu güvenliğinin sağlanabilmesi için sağlık, güvenlik, ulaşım, finans gibi hizmetlerin aksamaması da önem arz etmektedir. Hayati değeri olan enerji kaynakları ve hizmetlerin aktarılmasında sürekliliği sağlamak için oluşturulan altyapıların tek tek işletilmesi, kontrolü, güvenliğinin sağlanması hem zor hem de oldukça maliyetlidir. Maliyetleri azaltabilmek, altyapıların güvenliğini ve kontrolünü sağlayabilmek ve ağlardaki sorunları en aza indirebilmek adına kritik altyapı adı altında sistemlerin sistemi olarak nitelenebilecek bir işletim ve kontrol yapısı oluşturulmuştur. Kritik altyapıların kurulması ve işletilmesi Supervisory Control And Data Acquisition (SCADA) olarak da adlandırılan kontrol sistemi ile geniş alana yayılmış ağların ve altyapıların tek merkezden bilgisayar temelli cihazlar kullanarak yönetilmesi ile mümkün olmaktadır (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014).

2. Kritik Altyapı

Kontrol edilebilmesi ve devamlılığı için internet hatlarına bağlı olması gereken kritik altyapılar özellikle internetin gelişmesi, yaygınlaşması ve ağların güçlenmesi ile kurulmuşlardır. Kritik altyapı kavramı ilk kez dönemin ABD Başkanı Bill Clinton (1993-2001) tarafından 1996 yılında imzalanan bir kararnamede gündeme gelmiştir. Bu kararname gereğince kritik altyapıların korunmasına dair ilke ve esasların belirlenmesi için bir komisyon oluşturulmuştur. Bu komisyon tarafından 1997'de ABD'de kritik altyapılarla ilgili bir rapor hazırlanmıştır (President's Commission on Critical Infrastructure Protection, 1997). Her ne kadar tanım konusunda kesin bir uzlaşı sağlanamamış olsa da kritik altyapı, AFAD'ın hazırlayıp yayınladığı Açıklamalı Afet Yönetimi Terimleri Sözlüğünde şöyle karşılık bulmaktadır: *"İşlevlerini kısmen veya tamamen yerine getir(e)mediğinde toplumsal düzenin sürdürülebilirliğinin veya kamu hizmetlerinin sunumunun olumsuz etkileneceği, ulaşım, haberleşme, enerji, su finans gibi sektörleri kapsayan ağ, varlık, sistem ve yapılar bütünü"* (AFAD, 2014).

Kritik altyapılar, barındırdığı bilginin özelliği ve ulaşılabilirliği bozulduğunda, can ve mal kaybına, büyük ve telafi edilemez ekonomik zarara, kişisel ve ulusal güvenlik zafiyetine ve kamu düzeninin bozulmasına sebep olabilecek alt sistemleri içeren kompleks ve büyük sistemlerdir. Avrupa Birliği tarafından 2004 yılında yukarıdaki tanımlama temel alınarak kritik altyapıya dahil olabilecek sektörler 9 başlık altında kategorize edilmiştir.

Bu sektörler şunlardır:

1. Enerji kurulumları ve ağları
2. Bilgi ve İletişim teknolojileri ile bağlantılı yapılar.
3. Finansman hizmetleri
4. Sağlık hizmetleri ve ilişkili yapılar
5. Gıdanın kendisi, yapıları ve ağları
6. Suyla ilgili altyapılar
7. Ulaşım araçları ve ağları
8. Nükleer, kimyasal, biyolojik maddeler gibi tehlike arz eden maddelerin üretimi, saklanması ve nakliyesi
9. Hükümete ait değerli varlıklar ve işlevler (EU COM, 2004).

Yukarıda sıralanan listeden de anlaşılabileceği üzere kritik altyapı kavramı sadece enerji ağlarını değil birçok ürün ve hizmetin sunulmasını ve tedarik edilmesini sağlayan alt yapıları da bünyesinde barındırmaktadır.

3. ABD VE AB'de Kritik Altyapı

Kritik altyapı özellikle gelişen bilgi ve iletişim teknolojisiyle birlikte birçok ülkede kurulan, devlet ve toplum için hayati öneme sahip ağların yönetildiği sistemlerin sistemidir. Dünyada birçok ülke kritik altyapılarını oluşturmakta ve geliştirmektedir. Burada Avrupa Birliği ve Amerika Birleşik Devletleri'nde kritik altyapıya mevcut yaklaşımın nasıl olduğuna değinilmektedir.

Kritik altyapı kavramının çıkış noktası olan ABD'de toplumun refahı ve yaşam destek sistemlerinin sürekliliği için önemli olan yapılara yönelik tehditlerin belirlenmesi ve tedbirlerin alınması öncelikli bir konumdadır. Bununla ilgili olarak da 1997 yılında bir rapor yayınlanmıştır. Bu raporun ardından 1998'de kritik altyapının refah ve ulusal güvenlik açısından önemi vurgulanmıştır. Ulusal çıkar ve hedefler, kritik altyapıya dahil olan sistemlerin listesi, kurumlardan beklenen adımlar, kritik altyapı için gerekli yapılanmalar ve ulusal koordinasyon birimlerinin tanımlandığı *"Başkanlık Karar Direktifi"* yayınlanmıştır. Bu direktif başta güvenlikle ilgili olmak üzere tüm kamu kurumlarına ve kritik altyapı ile ilgisi bulunan tüm özel sektör kuruluşlarına gönderilmiştir (US PDD, 1998). ABD'de kritik altyapılar kimya sektöründen nükleer enerji ile ilgili tüm birimlere, kamu binalarının düzenli ve sürekli çalışmasından su ve atık su sistemlerine kadar 16 farklı başlık altında toplanmıştır (DHS, 2019).

Kritik altyapıların güvenliğinin sağlanması ile ilgili Avrupa Birliği tarafından atılan ilk adım ise Avrupa Komisyonu'nun 20 Ekim 2004 tarihinde yayınladığı "Terörle Mücadele için Kritik Altyapı Korunması" başlıklı rapordur. Bu rapor Avrupa Konseyi ve Avrupa Parlamentosu'na gönderilmiştir (EU COM, 2004). Bu raporda, kritik altyapılar tanımlanmış, tehditler belirlenmiş ve tedbirlerle ilgili önerilerde bulunulmuştur. Bu raporun neticesinde, "Kritik Altyapıların Korunması için Avrupa Programı-EPCIP" başlıklı bir program başlatılmıştır (EPCIP, 2004). 17 Kasım 2005 tarihinde de Avrupa Komisyonu tarafından EPCIP'in kurulmasına dair politika ilkelerinin yer aldığı belge yayınlanmıştır .(COM, 2005)EPCIP'in tamamlanması ise 2007 yılının Nisan ayında, Avrupa Konseyi'nin yaptığı duyuruyla olmuştur. Bu duyuruya göre üye ülkeler kendi sınırları içerisindeki kritik altyapıyı korumakla sorumluydular. Avrupa Komisyonu konuyla ilgili çalışmalarına Avrupa'daki kritik altyapıların belirlenmesi, tehditlere ve saldırılara karşı korunması ile ilgili prosedür geliştirerek devam etmiştir.

Avrupa Konseyi'nin 2008/114/EC kodlu direktifi de prosedür geliştirme çalışmalarının sonucu olarak yayınlanmıştır (THE COUNCIL OF THE EUROPEAN UNION, 2018). Bu direktifte kritik altyapı içerisinde enerji ve taşımacılık alanlarına ağırlık verilmiş olsa da bilgi ve iletişim teknolojilerine de yer verilmiştir. Avrupa Birliği'nde kritik altyapıların korunması ile ilgili yayınlanan son belge de 30 Mart 2009'da Avrupa Komisyonu tarafından hazırlanan "Avrupa'yı büyük ölçekli siber saldırılara ve bozulmalara karşı korumak: hazırlıklı olma, güvenlik ve dayanıklılığı artırma" raporu olmuştur (COM, 2009). Avrupa Birliği bünyesinde kritik altyapı ile ilgili 2004 yılından den beri yapılan tüm toplantı ve çalışmaların önemli bir ayağını da güvenlik önlemleri oluşturmaktadır. Zira kritik altyapıya yöneltilecek bir terör saldırısının telafi edilemez ölçüde zarara yol açması olasıdır.

4. Türkiye'de Kritik Altyapı

Türkiye'nin enerji tüketimi artan nüfusu ve ekonomik büyüme hızıyla doğru orantılı olarak artmaktadır. İş kollarında çeşitliliğin artması, sanayi, ulaşım ve turizm gibi sürekli faaliyet gösteren sektörlerin iş kapasitelerinin yükselmesi Türkiye'de teknoloji kapasitesinin artmasıyla da daha büyük ve kesintisiz bir enerji altyapısına ihtiyaç duyulmaktadır (Ak, 2019). Böylesine geniş çaplı bir enerji ihtiyacı kritik altyapının oluşturulmasını Türkiye için zorunlu hale getirmiştir. Jeopolitik konumundan ötürü birçok enerji hattının da ana geçiş güzergahı olan Türkiye'de kritik altyapıların zarar görmesi Türkiye dışında birçok ülkeyi de hem ekonomik açıdan hem yaşam kalitesi açısından olumsuz etkileyecektir (AFAD, 2014). Türkiye'de kritik altyapılar Siber Güvenlik Kurulu'nun 20.06.2013 tarih ve 2 sayılı kararına göre elektronik haberleşme, enerji, bankacılık ve finans, kritik kamu hizmetleri, ulaştırma ve su yönetimi olarak belirlenmiştir (Resmi Gazete, 2013). Türkiye'nin kritik altyapılara ilişkin özel bir stratejik planı bulunmasa da kamu kurumlarının toplam bilgi varlığının risk düzeylerini tanımlamak, analizini yapmak ve önlem almak gibi aşamalardan oluşan bilgi güvenliği yönetim sistemi ISO/IEC 27001 standardizasyonu kullanımının zorunlu hale getirilmesi, sızma testlerinin belirli aralıkla yapılması, sistem odalarında bulunması gereken asgari kriterlerin belirlenmesi gibi kritik altyapıyla bağlantılı genel hedeflere 2016-2019 Siber Güvenlik Stratejisi'nde yer verilmiştir (UAB, 2016).

İkincil mevzuatta da Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği'nde "Kritik enerji altyapılarında kullanılan endüstriyel kontrol sistemlerinin (EKS) bilişim süreçlerinin izlenmesi, sistem sürekliliğinin sağlanması ile siber güvenliğinin sağlanmasına ilişkin usul ve esaslar" düzenlenmiştir (Resmi Gazete, 2017).

Bunlara ek olarak TÜBİTAK tarafından hazırlanan "Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı" Türkiye'de kritik altyapıyı tanımlayıp kategorize etmektedir. Ayrıca bünyesinde kritik altyapı işleten kurum ve kuruluşları kapsayan bu dokümanda kritik altyapı sistemleri için gerekli olan asgari güvenlik önlemleri belirlenmiştir (TÜBİTAK, 2019).

5. Kritik Altyapıya Yönelik Tehditler

Teknolojinin gelişmesi sağladığı faydaların yanı sıra risk ve tehdit kavramlarına farklı yaklaşımların getirilmesini de zorunlu kılmaktadır. Soğuk Savaş Dönemi'nin ardından bilgi teknolojilerinde yaşanan gelişmeler daha önce askeri alanda kullanılan teknolojinin hızla sivil alanda yayılmasını sağlamıştır. (Bayrak, 2020).Hem risk altında olan ve korunması gereken unsurların değişmesi hem de tehdit oluşturacak silahların farklılaşması devletlerin risk, tehdit ve önlemler konusunda daha derinlikli planlar oluşturmaya mecbur bırakmıştır.

Özellikle kritik altyapılar olarak nitelendirilen sistemlerin önemi bu risk ve tehdit analizlerinin hassasiyetini artırmaktadır. Kritik altyapı içerisinde yer alan sistemler arasında fazla sayıda, karmaşık ilişkiler ve bağımlılıklardan söz etmek mümkündür (Lewis, 2006). Bu yüzden kritik altyapıların tehdide uğraması veya faaliyetlerinin durması durumunda toplum hayatının işleyişinde olumsuz etkiler yaşanacağı, teknoloji, ulaşım, sağlık, ekonomi, güvenlik ve çevre sistemlerindeki dengenin bozulacağı açıktır (Caşın, Nifti, & Gücüyener, 2015). Bu nedenle tehditlerin belirlenmesi ve bunlarla ilgili önlemlerin alınması gerekmektedir. Aksi takdirde kritik altyapıda yaşanacak aksaklıklar hem vatandaş hem de devlet açısından büyük sorunlara yol açacaktır. Kritik altyapıya yönelik tehditlerden bazıları Şekil-1'deki tabloda yer almaktadır.

Şekil-1: Kritik Altyapıya Yönelik Tehditler

Doğal Olaylar	Teknik/İnsan Hataları	Terörizm, Suçlar ve Savaş
Meteorolojik afetler	Sistemsel hatalar	Terörizm
Jeolojik afetler	İhmal ve dikkatsizlik	Sabotaj
Salgın hastalıklar	Kazalar ve acil durumlar	Diğer suçlar
Kozmik olaylar	Organizasyondan kaynaklanan hatalar	Savaşlar

Kaynak: Claudia Bach, Anil K. Gupta, Sreeja S. Nair and Jöm Birkmann, 'Critical Infrastructure and Disaster Risk Education', ss.17

The International Disaster Database (EM-DAT) kayıtlarına göre sanayi devrimi sonrası dönemde, 1900'lu yıllar ile 2014 arasında ciddi sonuçlar doğuran 7825 adet büyük kaza ve teknolojik afet meydana gelmiştir (AFAD, 2014). Oldukça fazla can ve mal kaybına sebep olmakla birlikte bu kaza ve afetler kritik altyapıların korunması ve güvenliğinin sağlanması hususuda da alınması gereken önlemleri uluslararası boyutta olması gerektiğini göstermiştir. Kritik altyapı güvenliği sadece bir devleti ilgilendiren bir konu değildir ve kritik altyapıların korunması uluslararası işbirliği gerektirmektedir (Federal Office for Information Security of Germany, 2004). Özellikle Türkiye gibi birçok kıtalararası enerji hattının geçtiği jeopolitik ve jeostratejik öneme sahip ülkelerde kritik altyapıya yöneltilecek herhangi bir tehlike sadece kritik altyapının bulunduğu ülkede değil o hattan faydalanan tüm ülkelerde kaos ve aksaklıklara neden olacaktır. Japonya'da 11 Mart 2011 tarihinde meydana gelen 9.0 büyüklüğündeki Büyük Doğu Japonya Depremi (Tohoku depremi) ve buna bağlı olarak gerçekleşen tsunaminin Fukuşima Nükleer Elektrik Santralinde yol açtığı nükleer kaza kritik altyapı güvenliğine yönelik jeolojik tehditlere en önemli örneklerden biri olarak gösterilebilir. Ayrıca afet yönetiminin de kritik altyapıların korunmasında önemli bir rolü olduğunu ortaya koymaktadır. 31 Mart 2015 tarihinde Türkiye'nin İstanbul ve Ankara gibi büyükşehirlerinin de dahil olduğu 51 il merkezini ve ilçelerini etkileyen uzun süreli bir elektrik kesintisi yaşanmıştır (NTV, 2015). Avrupa Elektrik İletim Ağı (ENTSO-E) ve Türkiye Elektrik İletim AŞ (TEİAŞ) tarafından hazırlanan raporda elektrik kesintisinin nedeni olarak tam kapasiteyle çalışan santrallerden hatlara aşırı yüklenilmesi gösterilmiştir. Elektrik kesintisine bağlı olarak internet kesintisi de yaşanmış, şehir içi ve şehirlerarası ulaşım sekteye uğramış, madencilik, sanayi, eğitim ve sağlık sektörlerinde aksamalar yaşanmıştır. Bu elektrik kesintisi alınan önlemler ile sadece Türkiye'yi etkilemiş ve komşularında herhangi bir aksaklığa yol açmamıştır (Türkiye Proje Grubu, 2015). Kritik altyapılara yönelik tehditler arasında özellikle siber saldırılara bir başlık açılması gerekmektedir. Kritik altyapıların kurulması ve devamlılığının sağlanması internet altyapısına bağlı olduğundan bu kanal üzerinden gerçekleştirilecek siber saldırılar çok büyük hasarlara sebep olmaktadır.

Siber dünya fiziki özelliklere sahip bir dünya gibi geliştirilmeye, kontrol altında tutulmaya ve savunulmaya ihtiyaç duymaktadır. Kara, hava, deniz ve uzayın yanı sıra siber dünya da yeni bir harekât alanı olarak kabul edilmektedir. Haberleşme sistem ve alt yapıları, ulaşım sistemleri, akıllı şebekeler, barajlar, e-ticaret, e-devlet gibi hizmetleri daimi surette hedef olma potansiyeli taşımaktadırlar (CBDDO, 2018). Acil durum iletişim hatlarının engellenmesi, elektriğin kesilmesi, devlet bilgisayar ağlarının, finansal ağların veya kritik sivil sistemlerin altında yatan bilgi teknolojisinin bozulması, enerji santrallerini ve barajları kontrol eden makineleri devralmak için bilgisayar ağların kullanılması, siber ortamda gizli dosyaların çalınması, yanlış bilgilerin yayılması, verilerin silinmesi gibi işlemlerin hepsini siber terörizm kapsamında değerlendirmek mümkündür (Terzi, 2019). Özellikle kritik altyapıları hedef alan siber silahlar geliştirilmektedir. Advanced Persistent Threat (APT) olarak adlandırılan Stuxnet, DUQU, Flame gibi siber silahlar ülkelerin kritik altyapılarına zarar vermek amacıyla uzun vadeli tehditler barındıran ve siber saldırılarda kullanılmak üzere tasarlanmış tehlikeli yazılımlar bulunmaktadır (KARA, 2013). Bu tür yazılımlar kullanılarak 1982'de Sibirya Doğalgaz Patlaması, 1998'de Ay Işığı Labirenti Operasyonu, 1999'da NATO-Kosova Krizi, 2007'de Estonya Siber Savaşı, 2008'de Gürcistan Krizi ve Tiflis-Ceyhan-Bakü Petrol Boru Hattı Patlaması ve 2010'da İran Nükleer Sistemine Saldırı gerçekleştirilmiştir (Eralp, 2017). Görüldüğü üzere savaş kavramı da yerine konvansiyonel ve silahlı savaşlardan siber dünyadaki yazılım savaşlarına bırakmaktadır. Siber güvenlik alanında çalışmaları da bulunan NATO Güvenlik Danışmanı Rex Hughes "Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır." diyerek bu durumu özetlemiştir (Dizdar Group, 2018). Hatta siber saldırıların bir ülkenin ekonomisine, güvenliğine ve vatandaşların refah ve huzuruna etkisi çok yıkıcı olabilmektedir.

6. Sonuç

Kritik altyapı bünyesinde yer alan ve ileride yer alacak olan tüm sistemlerle insan, toplum, devlet ve uluslararası ilişkiler için gün geçtikçe önemli bir konu olmaktadır. Bir ülkenin kritik altyapısında yaşanan problemlerin küresel anlamda sorunlara yol açabileceği ya da bir sektördeki aksamaların diğer sektörlere de olumsuz etki edebileceği bu sistemin güvenliğini ve sürekliliğini sağlamak kolay olmasa da hayati öneme sahiptir. Sadece tek bir kurumun ya da organizasyonun kritik altyapı ile ilgili çalışmaları yürütmesi mümkün görünmemektedir. Dolayısıyla kritik altyapıların korunması için kamu kurumlarının yanı sıra kritik altyapı yatırımları olan özel işletmeler ile birlikte kurumsal, sektörel, ulusal ve uluslararası boyutta koordineli bir faaliyet yürütülmesi gerekmektedir (Önen & Kurnaz, 2017). Özellikle Kritik altyapının etkilediği ve kritik altyapıdan etkilenen alanlarda tüm birey, kurum, kuruluş ve uluslararası örgütlerin güçlü bir işbirliği içerisinde olması kaçınılmazdır. Hızla gelişen ve yenilenen siber dünyada kritik altyapıların güvenliğini ve sürekliliğini sağlamak ancak kalifiye personel ve kaliteli teçhizat ile mümkündür. Özellikle Türkiye'de siber güvenlik konusuna TÜBİTAK tarafından öncelikli akademik alanlar arasında yer verilmesi gayet olumlu bir yaklaşımdır. Kritik altyapının korunması kadar olası bir arıza durumunda olabildiğince hızlı çözümler bulmak ve uygulamak da çok önemlidir. Koruma ve arızaya müdahale için bu alanda ulusal ve uluslararası mevzuat oluşturulması, tatbikatlar yapılması, alternatif kaynakların hazır bulundurulması, ilgili personelin eğitiminin güncel tutulması gibi birçok öneri sıralanabilir.

Kaynakça

AFAD. (2014). 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi. 12. Ankara: Başbakanlık Afet Acil Durum Yönetimi Başkanlığı.

AFAD. (2014, Kasım). Açıklamalı Afet Yönetimi Terimleri Sözlüğü. 106. Ankara: Başbakanlık Afet Acil Durum Yönetimi Başkanlığı.

Ak, T. (2019). İç Güvenlik Yönetimi Açısından Kritik Altyapılarını Korunması. *Assam Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı*, (s. 42-51).

Bayrak, M. (2020). Abd İle Birleşik Krallık'ın Ab ve Nato Çerçevesinde Siber Alanlarının Tarihsel Analizi. *Cyberpolitik Journal, 5*(9), 22-51.

Caşın, M. H., Nifti, E., & Gücüyener, A. (2015). *Kritik Enerji Altyapı Güvenliği El Kitabı*. Hazar Strateji Enstitüsü. İstanbul: Hazar Strateji Enstitüsü.

CBDDO. (2018). Aralık 26, 2020 tarihinde T.C. Dijital Dönüşüm Ofisi: https://cbddo.gov.tr/siber-gvenlik/ adresinden alındı

COM. (2005). *Green Paper On A European Programme For Critical Infrastructure Protection*. Brussels: COMMISSION OF THE EUROPEAN COMMUNITIES.

COM. (2009, Mart 30). *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* Kasım 17, 2019 tarihinde https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52009DC0149 adresinden alındı

DHS. (2019). *Critical Infrastructure Sectors.* Kasım 19, 2019 tarihinde https://www.dhs.gov/cisa/critical-infrastructure-sectors adresinden alındı

Dizdar Group. (2018). *Dizdar Group*. Mayıs 10, 2020 tarihinde https://www.dizdargroup.com.tr/siber-guvenlik/ adresinden alındı

EPCIP. (2004). *European Programme for Critical Infrastructure Protection.* Kasım 22, 2019 tarihinde http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm adresinden alındı

Eralp, Ö. E. (2017, Kasım 12). *Dünden Bugüne Siber Savaşlar*. Mayıs 25, 2020 tarihinde Bookmark: http://www.bookmark.com.tr/dunden-bugune-siber-savaslar-2/ adresinden alındı

EU COM. (2004). *Critical Infrastructure Protection in the Fight Against Terrorism*. Brüksel: Communication from the Commission to the Council and the European Parliament. Kasım 22, 2020 tarihinde http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1 &year=2004&number=702&language=EN adresinden alındı

Eralp, Ö. E. (2017, Kasım 12). *Dünden Bugüne Siber Savaşlar*. Mayıs 25, 2020 tarihinde Bookmark: http://www.bookmark.com.tr/dunden-bugune-siber-savaslar-2/ adresinden alındı

EU COM. (2004). *Critical Infrastructure Protection in the Fight Against Terrorism*. Brüksel: Communication from the Commission to the Council and the European Parliament. Kasım 22, 2020 tarihinde http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1 &year=2004&number=702&language=EN adresinden alındı

Federal Office for Information Security of Germany. (2004). *Critical Infrastructure Protection: Survey of World-Wide Activities*. Mayıs 22, 2020 tarihinde https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile adresinden alındı

KARA, M. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. 31. İstanbul.

Lewis, T. G. (2006). *Critical Infrastructure Protection In Homeland Security - Defending A Networked Nation*. A John Wiley & Sons, Inc., Publication.

NTV. (2015, Nisan 04). Mayıs 14, 2020 tarihinde www.ntv.com.tr: https://www.ntv.com.tr/turkiye/turkiye-genelinde-elektrik-kesintisi,RhfwqMiNNkOUj5_sO12qJg adresinden alındı

Önen, S., & Kurnaz, S. (2017). Siber Güvenlik Politikalarının Kamu Yönetimine Yansıması. *Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi IV*, (s. 732-752). Malatya.

President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations Protecting America's Infrastructures*. Washington, DC.

Presidential Decision Directive/NSC-63. (1998). 01 10, 2020 tarihinde https://fas.org/irp/offdocs/pdd/pdd-63.htm adresinden alındı

Resmi Gazete. (2013, Haziran 20). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*. Kasım 20, 2019 tarihinde https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm adresinden alındı

Resmi Gazete. (2017, Temmuz 13). *Enerji Sektöründe Kullanılan Endüstriyel Kontrol*. Kasım 20, 2019 tarihinde https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm adresinden alındı

Sektörel SOME Kurulum ve Yönetim Rehberi. (2014). Mayıs 9, 2020 tarihinde Ulusal Siber Olaylarla Mücadele Merkezi (USOM): https://www.usom.gov.tr/dosya/1470335484-Sektorel%20SOME %20Rehberi.pdf adresinden alındı

Terzi, M. (2019). E-government and cyber terrorism: Conceptual framework, theoretical discussions and possible solutions. *Tesam Akademi Dergisi*, 6(1), 213-247.

THE COUNCIL OF THE EUROPEAN UNION. (2018, Aralık 8). COUNCIL DIRECTIVE 2008/114/EC. *Official Journal of the European Union*, s. 75-82.

TÜBİTAK. (2019). *Kritik Altyapı Bilgi Sistemleri için Asgari Güvenlik Önlemleri Dokümanı.* Kasım 18, 2019 tarihinde 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 adresinden alındı

Türkiye Proje Grubu. (2015). *Türkiye 3 art 2015 Sistem Çökmesi Raporu.* European Networks of Transmission System Operators for Electricity. ENTSO-E.

UAB. (2016). *2016-2019 Siber Güvenlik Stratejisi.* T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Stratejik Eylem 4.1: Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması, Ankara.

US PDD. (1998, Mayıs). *Presidential Decision Directive/NSC-63.* Kasım 18, 2019 tarihinde https://fas.org/irp/offdocs/pdd/pdd-63.htm adresinden alındı