KRİTİK ALTYAPILARDA SİBER GÜVENLİK VE AFAD ÜZERİNDEN BİR DEĞERLENDİRME

Kıvanç DEMİRCİ[1]

Özet

Küreselleşmenin getirmiş olduğu yapısal dönüşüm hareketleri güvenlik anlayışındaki değişimleri de beraberinde getirmiştir. Bu dönüşüm hareketleriyle literatürde askeri bir kavram olarak ele alınan güvenlik sosyal, ekonomik, askeri tüm boyutlarıyla ele alınmaya başlamıştır. Teknolojik gelişimin de etkisiyle güvenlik anlayışıyla beraber sınır kavramında da bir dönüşüm yaşanmıştır. Artık sınır kavramını kara, hava ve deniz olarak tanımlamanın yanı sıra siber sınır olarak adlandırılan bir kavram da ortaya çıkmıştır. Bu bağlamda çalışmanın temel amacı Afet ve Acil Durum Yönetim Başkanlığı (AFAD) kritik altyapıların korunması konusundaki görev ve sorumluluklarının tespitidir. Çalışmada nitel bir araştırma yöntemi olan döküman taraması yöntemi kullanılmıştır.

Çalışma kapsamında AFAD'ın kritik altyapıların korunması konusunda özel bir öneme sahip kamu kurumu olduğu sonucuna ulaşılmıştır. Özellikle kritik altyapıları belirlenmesi, kurumlar arasındaki koordinasyonun sağlanması ve bu altyapılara yönelik verileri hazırlama görevi AFAD'a verilerek bu yolla siber güvenliğe karşı direnç oluşturmak amaçlandığı tespit edilmiştir. AFAD'ın son dönemde kamu hizmetlerinin dijitalleşmesine önem vermiş olduğu görülmektedir. Bu durum kritik altyapılara yönelik risk ve tehditleri arttıran gelişmelerin başında gelmektedir.

Anahtar Kelimeler: AFAD, Güvenlik, Kritik Altyapılar, Siber Güvenlik, Siber Sınır.

JEL Kodları: J28, K32.

CYBER SECURITY IN CRITICAL INFRASTRUCTURE AND AN EVALUATION BY AFAD

Abstract

Structural transformation movements brought about by globalization have brought about changes in the understanding of security. With these transformation movements, security, which is considered as a military concept in the literature, has begun to be discussed with all its social, economic and military dimensions. With the effect of technological development, there has been a transformation in the concept of border along with the understanding of security. Now, in addition to defining the border concept as land, air and sea, a concept called cyber border has emerged. In this context, the main purpose of the study is to determine the duties and responsibilities of the Disaster and Emergency Management Presidency in the protection of critical infrastructures.

Within the scope of the study, it was concluded that AFAD is a public institution with a special importance in the protection of critical infrastructures. In particular, it has been determined that AFAD is given the task of identifying critical infrastructures, ensuring coordination between institutions, and preparing data for these infrastructures, in order to create resistance against cyber security in this way. It is seen that AFAD has recently given to the digitalization of public services. In this case, it is one of the developments that increase the risks and threats to critical infrastructures.

Keywords: AFAD, Security, Critical Infrastructures, Cyber Security, Cyber Frontier.

JEL Codes: J28, K32.

1. GİRİŞ

Fiziksel veya sanal olsun bir devletin devamı için önemli olan hizmetlerin kesintisi kamu güvenliği üzerinde tehdit oluşturuyorsa bu hizmetlerin yürütüldüğü altyapılar kritik altyapı olarak tanımlanabilir. Literatürde bilgi iletişim teknolojileri, su ve enerji kaynakları, kimya, uzay ve nükleer endüstrisi, sivil idare, mali sistemler ile halk sağlığı hizmetlerinin kritik altyapılar içerisinde değerlendirildiği görülmektedir (Alcaraz & Zeadally, 2015).

Kritik altyapı terimi ve bu altyapılara karşı tehditler 1990'lı yılların ortalarında çalışılmaya başlanmıştır. Dijital Pearl Harbor olarak sistematize edilen bu saldırı tehditleri baraj suları ve temel gıdalara zehir karıştırılması, yolcu uçaklarının rotalarını kaybettirilerek birbirine çarptırılması vb. olaylar olarak tahmin edilmekteydi. Ancak zaman içerisinde tehditler fiziksel ortamdan sanal ortamlara taşınarak kritik

[1] Arş, Gör., Bitlis Eren Üniversitesi, Bitlis, Türkiye, kivancdemirci4@gmail.com, ORCID ID: orcid.org/ 0000-0001-6598-6673

Araştırma Makalesi (Research Article)

Makale Gönderilme Tarihi (Received Date): 05.09.2021
Makale Kabul Tarihi (Acceptance Date): 05.11.2021

altyapıları kontrol eden sistemlere doğru yöneldi. Fiziksel tehditlerin sanal tehditlere yönelmesinin temel nedeni ise kritik altyapı sistemlerinin karmaşıklığından dolayı kontrol edilmesinin güçlüğünden ve kullanılacak bir yazılımın birbirine bağlı karmaşık sistemlere vereceği zararın yüksek olması düşüncesinden kaynaklanmaktadır (Lewis, 2006: 1).

Ülke örnekleri incelendiğinde bu tehditlerin önemli kısmı ulusal güvenlik kurum ve kuruluşları tarafından bertaraf edilmeye çalışıldığı görülmektedir (Ani, Watson, Nurse, Cook, & Maple, 2019).

Türkiye'de kritik altyapılara karşı siber tehditlerin önlenmesi amacıyla çeşitli düzenlemeler yürürlüğe girmiş çeşitli kurum ve kuruluşlar yetkilendirilmiştir. Buna göre 22.12.1981 tarihinde yürürlüğe giren 2565 sayılı Askeri Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu'nun 1. maddesiyle yurt savunmasında kritik önem sahip bölgelerin korunması amaçlanmıştır (2565 sk. md.1). Kanun kapsamında askeri güvenlik bölgelerinin oluşturulması ve kaldırılmasında Genelkurmay Başkanlığı yetkilendirilmiştir. Cumhurbaşkanına ise özel güvenlik bölgelerinin oluşturulması konusunda yetki, görev ve sorumluluk verilmiştir (2565 sk. md.3).

Kritik altyapıların zarar görebilirliği konusunda özel öneme sahip elektronik haberleşme, altyapı ve şebekelerinin korunma usulleri 5.11.2008 tarihinde yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu ile düzenlenmiştir. Kanun kapsamında Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı'na çeşitli görev ve sorumluluklar verilmiştir. Bakanlık; milli güvenlik politikalarına uygun olarak şebeke-altyapı hizmetlerinin kurulması ve güvenliğinin tesis edilmesine yönelik politikaların geliştirilmesi, doğal afet ve olağanüstü durumlarda elektronik haberleşmenin aksamaması için gerekli önlemlerin alınması, ulusal siber güvenliğin sağlanması için usul ve esasların belirlenmesi ve ilgili faaliyetlerin koordinasyonunun sağlanması konularında yetkili kılınmıştır. Ayrıca ulusal entegre kamu sistemlerine yönelik plan, politika ve stratejiler geliştirmek, e-devlet verilerinin transferleri konusunda gerekli altyapıların kurulmasını sağlamak ve bu faaliyetlere yönelik usul ve esasları belirlemek bakanlığın diğer görev ve sorumlulukları arasında yer almaktadır (5809 sk. md. 5).

10.07.2018 tarihinde yürürlüğe giren 1 numaralı Cumhurbaşkanlığı Kararnamesi'nde de kritik altyapıların korunmasına yönelik hükümler bulunmaktadır. İlgili mevzuatta dijital dönüşüm ofisine konuyla ilgili çeşitli görev ve sorumluluklar verildiği görülmektedir. Buna göre kararnamenin 527/B maddesinde ofis; kritik altyapıların belirlenmesine ilişkin çalışmalar gerçekleştirmek, kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek, bilgi güvenliği yönetim sistemleri kurmak, işletmek ve teknik standartlarla ilgili usul esasları belirleyerek ilgili çalışmaları yürütmek konularında yetkilendirilmiştir (Turan, 2018: 74). Dijital Dönüşüm Ofisi hizmet birimleri arasında yer alan Siber Güvenlik Dairesi Başkanlığı ise Cumhurbaşkanlığı tarafından belirlenen kurumlar için siber güvenlik stratejileri geliştirmek, bilgi güvenliğini destekleyici nitelikte çalışmalar yapmak, kamu-özel-sivil paydaşlarla birlikte ulusal siber güvenlik ekosisteminin oluşturulmasına destek sağlamak ve siber güvenlikle ilgili eylem planlarının uygulanmasına yönelik pratikleri takip etme konularında yetkili kılınmıştır (Cumhurbaşkanlığı, 2021).

Yine 1 numaralı Cumhurbaşkanlığı Kararnamesiyle oluşturulan Güvenlik ve Dış Politikalar Kurulu'na da siber güvenlikle ilgili politika ve strateji önerileri geliştirme görevi verilmiştir (1 Nolu CBK, md. 26).

Sanayi ve Teknoloji Bakanlığı da kararname kapsamında yetkilendirilen kurumların başında gelmektedir. Bakanlık siber saldırıların önceden tespit edilerek kritik altyapıların güvenliğinin sağlanması, siber güvenlik konusunda toplumsal farkındalığın arttırılması, kritik sektörlerin yerli siber altyapı donanımlarıyla korunmasının sağlanması, e-ticaretin gelişmesinden hareketle veri güvenliği standartlarının oluşturulması konularında yetkili kurum olarak kabul edilmiştir (Sanayi ve Teknoloji Bakanlığı, 2019).

İçişleri Bakanlığı Güvenlik ve Acil Durumlar Koordinasyon Merkezine (GAMER) 24.10.2019 tarihinde yürürlüğe giren *Güvenlik ve Acil Durumlar Koordinasyon Merkezi Teşkilat, Görev, Yetki, Çalışma Usul ve Esasları Hakkındaki Yönetmeliğin* GAMER'in görevleri başlıklı 13. maddesinde kritik altyapıların güvenliğini sağlayan kurumlar arasında koordinasyon görevi verilmiştir (30928 sk. md.13).

Bu çalışmada yukarıda verilen kurumlarla birlikte koordineli bir şekilde çalışan ve Türkiye'de kritik altyapıların korunması konusunda temel sorumlu kurumların başında gelen Afet ve Acil Durum Yönetim Başkanlığı (AFAD)'nın bu konudaki görev ve sorumluluklarını vurgulamak amaçlanmıştır.

Çalışmada nitel bir araştırma yöntemi olan doküman analizi yöntemine başvurulmuştur. Çalışmanın temel sınırlılığı ise AFAD'ın güncel kaynak ve mevzuat hükümleri çerçevesinde değerlendirme yapılması mülakat yöntemine başvurulmamasıdır.

Çalışmanın kavramsal çerçeve başlıklı birinci bölümünde güvenlik, siber güvenlik, kritik altyapı ve siber uzay kavramları üzerinde durulmuştur. İkinci bölümde Kritik Altyapılara Yönelik Gerçekleştirilen Siber Saldırı Yazılımları ve Örnekleri anlatılmış olup son bölümde ise AFAD'ın kritik altyapıların korunması konusundaki değerlendirmesine yer verilmiştir.

2. KAVRAMSAL ÇERÇEVE

2.1. Güvenlik Kavramı

İngilizce dilinde security, Latince'de securus kelimesinden türeyen güvenlik (Birdişli, 2011:151) insanlık tarihi kadar eski olsa da bilimsel anlamda ele alınışı açısından oldukça yeni bir kavramdır. Soğuk savaş öncesi dönemde sadece askeri ve ulusal güvenlik gibi dar anlamda tanımlanan güvenlik kavramı soğuk savaş sonrası dönemde ise uluslararası güvenlik boyutuyla çok yönlü olarak incelenmeye başlanmıştır (Birdişli, 2010: 234).

Birinci ve İkinci Dünya Savaşları arasında daha çok savunma, egemenlik, milli çıkar anlamlarında kullanılan güvenlik (Brauch, 2008: 4) soğuk savaş sonrası dönemde çok yönlü olarak incelenerek literatürde ilgi alanlarına göre değişik şekillerde tanımlanmıştır. Bu değişimin temel nedeni soğuk savaş sonrası dönemde askeri kaynaklı tehditlerin azalması buna paralel olarak askeri olmayan tehditlerin artmaya başlamasıdır. Diğer bir neden ise dünyada güvenliğe yönelik oluşan tehditlerin asker kaynaklı güvenlikten çevrenin ve doğanın tahrip edilmesi, etnik gerilimler, yumuşak güç kullanarak siyasi baskı, ekonomik savaş gibi birçok nedenden kaynaklanabilmesidir (Aksu & Turhan, 2012: 70).

Yeni güvenlik yaklaşımı üzerinde çalışmakta olan araştırmacılar uluslararası sistemde bir değer değişim süreci yaşanmakta ve yeni değerler hem bireysel hem de küresel anlamda ulus-devletin merkeziyetçiliğinin yerini almaya başladığını iddia etmektedir. Yani bireysel olarak, insan hakları ve ihtiyaçlarına küresel anlamda ise, demokrasi ve serbest piyasanın yayılması, insanlığın refahına yönelik tehditler bağlamında hastalıklar, kirlilik, uyuşturucu gibi diğer insanlık için ortak olan ulus-aşırı tehditlere odaklanmışlardır (Ağır, 2015: 106).

Bu birikimlerin getirmiş olduğu kazanımlarla birlikte güvenlik objektif ve sübjektif olarak 2 şekilde tanımlanmaya başlanmıştır. Objektif güvenlik sahip olunan değerlere yönelik bir saldırı olmaması anlamına gelmekteyken; sübjektif güvenlik ise bu değerlere yönelik saldırı olmayacağı düşüncesine sahip olunmasıdır (Buzan, 1991: 17).

Tanımdan da görüldüğü üzere güvenlik korku halinde olmamak ve zarara uğramamak anlamına gelmektedir Günümüzde insan faktörü birçok alanda güvenlik içinde olma arayışından dolayı devlet endeksli güvenlik anlayışından bahsedilememektedir.

2.2. Kritik Altyapı

Kritik altyapı, ABD'nin 2001 yılında yürürlüğe girmiş olan Vatanseverlik Yasası içerisinde tanımlanan bir kavramdır. Buna göre kritik altyapı; yetersizliği, eksikliği, duraklaması veya durdurulması halinde milli güvenliğe zayıflatıcı etkisi olacak sanal varlıklar olarak tanımlanmıştır (GPO, 2001).

Avrupa Birliği tarafından 2006 yılında kritik altyapıların güvenlik açıklarını azaltmak için başlatmış olduğu Kritik Altyapıların Korunmasına Yönelik Avrupa Programında ABD'de yapılan tanıma benzer tanımın yapıldığı görülmektedir. Zarar görmesi halinde devlet güvenliğini sekteye uğratan servis, şebeke ve ağlar, kritik altyapılar olarak tanımlanmıştır (EU, 2006).

Uygulama örnekleri incelendiğinde ise ABD'de 16 temel kritik altyapının olduğu görülmektedir. Kimya, iletişim, baraj, ticari, kritik imalat, savunma sanayi, acil hizmetler, enerji, finansal hizmetler, gıda ve tarım, bilgi teknolojileri, ulaşım gibi altyapılar ciddi öneme sahip tesisler olarak sıralanmaktadır (CİSA, 2021). Avrupa Birliği'nde ise iletişim ve navigasyon altyapısı, uzay tesisleri, yerleşim alanlarının saldırılara karşı korunması ABD programından farklılaşan başlıklar olarak karşımıza çıkmaktadır (EU, 2021).

Türkiye'de Ulaştırma ve Altyapı Bakanlığı tarafından 2020 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planında ise kritik altyapılar; işlediği verilerin sistematik bütünlüğü bozulduğunda kamu, kişi ve ekonomik güvenliği sekteye uğratacak bilişim altyapıları olarak tanımlanmıştır. Yine aynı eylem planında bu altyapılar finans, ulaştırma, kritik kamu hizmet sektörleri, enerji ve haberleşme olarak sıralanmıştır (Ulaştırma ve Altyapı Bakanlığı, 2020).

Kritik altyapıların güvenliğinin sağlanması amacıyla üç temel boyut oldukça önemlidir. Kritik altyapılarda yer alan sistemsel sorunların tespit edilip bu eksikliklerin giderilmesi teknik boyutu ifade etmektedir. Sistemin güvenlik açığı yaratabilecek altyapısı detaylı bir şekilde incelenerek risk haritalarının çıkartılmasına önem verilmelidir. Bu aşamada riskler tanımlanarak, bu riskler analiz edilip yönetilmesi gerekmektedir. Teknik boyut içerisinde üzerinde durulması gereken bir diğer husus ise teknik açıklıkların önlenmesi hususudur. Kritik altyapılarda yer alan diğer bir önemli durum ise teknik açıklığın etkin bir şekilde yönetilmesidir. Sistemde bulunan teknik altyapısal açıklıkların giderilerek uygulanacak programların belirlenmesi güvenliğin sağlanması açısından oldukça önemlidir. Teknik boyutun ardından gelen kurumsal boyut ise kurum ve kuruluşların siber güvenlik politikalarını oluşturmasını içermektedir. Bu bağlamda kurumlardaki personelin siber altyapı konusunda çalıştığı alana uygun bilgi birikimine ve farkındalığa sahip olması gerekmektedir. Personele belirli aralıklarla düzenli eğitimler verilecek etkin siber savunma mekanizmalarının oluşturulması oldukça önemlidir.

Üçüncü boyutta yer alan ulusal ve uluslararası iş birliği boyutunda ise ulusal ve uluslararası kurumlar kritik altyapılarının güvenliğini sağlamak adına gereken iş birliğine başvurmaları hedeflenmektedir. Ülke içindeki her kurumun siber güvenlik politikaları bulunmaktadır ancak bu politikaların üstünde bir politika geliştirilmesi gerekmektedir. Ülkelerin bu politikaları belirlenmesinden önce ilk olarak yapmaları gereken kritik altyapılarını tespit ederek hedef ve stratejilerini oluşturmaları gerekmektedir (Semiz, Göztepe, & Kılıç, 2013).

2.3. Siber Güvenlik

Amerikalı Matematikçi ve Felsefeci Norbert Wiener Sibernetik kavramını kullanarak insan ve hayvan sistemleri üzerine iletişim eksenli çalışmalar gerçekleştirmiştir (Wiener, 1948: 5). Sibernetik kavramının "siber" ön ekinden gelen ve günümüzde ise daha çok elektronik kontrol sistemlerini niteleyen bir kavram olarak siber güvenlik, son zamanlarda üzerinde önemle durulan konulardan biri olmuştur (Göçoğlu, 2018: 1).

Siber güvenlik teknolojik gelişmelerin etkisiyle internetin yaygınlaşması sonucunda yaşanılan hızlı dijitalleşme sonucunda ortaya çıkan bir kavramdır. 1991 yılında internetin sivil kullanıma açılması sanal ortamı etkilemiş dijital üretimi teşvik etmiştir. Bu üretim süreci sonucunda siber alanların güvenliği artık sadece kurumların değil kişilerinde talep ettiği olgu konumuna gelmiştir. Günümüzde de sıkça kullanılan bir kavram olan siber güvenlik en temel tanımıyla siber alanlarda meydana gelecek tehditlerin önlenmesi anlamına gelmektedir (Bıçakçı, 2019: 2).

Bir diğer tanımda siber güvenlik siber alanlarda meydana gelecek riskleri öngörüp bu risklere karşı önlem alma girişimleri olarak ifade edilmiştir. Diğer bir tanımda ise siber uzayda yetkisiz kabul edilen birey ve sistemlerin zararlı etkilerinden kurtulma yöntemi olarak da tanımlanmaktadır (Sağıroğlu, 2018: 24).

Uluslararası Telekomünikasyon Birliği siber güvenliği, *siber ortamda, organizasyon ve kullanıcıların varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetimi yaklaşımları, eylemler, eğitim, uygulamalar, altyapı ve teknolojilerin bütünü* olarak tanımlamaktadır (ITU-T, 2014).

Bu yeni güvenlik anlayışının siber güvenlik boyutu, tüm güvenlik unsurlarının belirli verilere sahip olması nedeniyle kapsayıcılık açısından en üst düzeyde yer almaktadır. Küresel güvenlik açısından ele alınan unsurlar uzay boşluğunda teknolojik unsurlar ile birbirlerine yakınlaştığı ölçüde siber tehditlere maruz kalabilecektir (Güntay, 2017: 17)

Siber güvenliğin bu kadar üzerinde durulmasının diğer bir nedeni ise birçok terörist atakların siber yolları tercih etmesi olmuştur. Bu noktada da ülkeler kendi kurum ve kuruluşlarının ve kritik altyapılarının güvenliğini sağlamak adına siber güvenlik konusunda politika geliştirmekte ve farkındalık

çalışmaları yapmaktadır. Nitekim bu kritik altyapılar iletişim, su, enerji, gıda üretim gibi endüstriyel kontrol sistemlerinin güvenliğini de içeren bir alan haline gelmiştir (Göçoğlu, 2018: 1).

2.4. Siber Uzay

Siber uzay siber güvenlik açısından kilit kavramlar arasında yer almaktadır. 1982 yılında bilim kurgu yazarı olan William Gibson, Burning Chrome adlı eserinde siber alanı tanımlamak amacıyla siber uzay kavramını kullanmıştır. Bundan iki yıl sonra ise kavramı daha detaylı bir şekilde tanımlayarak birçok birey tarafından her gün kullanılan bir halüsinasyon, tanımlanamayan bir kargaşa olarak tanımlamıştır (Bıçakçı, 2014: 106).

Günümüzde, çok çeşitli siber uzay tanımlarının da yapıldığı görülmektedir. Bu tanımlardan bir tanesi de 11 Eylül sonrasında, Amerika Birleşik Devletleri'nin Ulusal Siber Savunma Stratejisinde yer almaktadır. Bu belgede siber uzay ülkelerin kritik altyapılarını kontrol eden ve sistemin birbiriyle bağlantılı ögelerinin yer aldığı bir sinir sistemi olarak tanımlanmıştır (Klimburg & Mirtl, 2012: 9).

Türkiye'nin 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Plan'ında ise siber uzay; "*Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam"* olarak tanımlanmıştır. Soğuk Savaş'ın ardından güvenliğin anlamının genişlemesi ve dönüşüme uğraması sonrasında artık sadece askeri ve politik güvenlikten bahsedilememekte, bunun yanında ekonomik güvenlik, çevre güvenliği, sağlık güvenliği, gıda güvenliği gibi konular da ele alınmaktadır. Bu noktada ileride üzerinde ayrıntılı şekilde durulacak olan güvenliğin siber boyutu da önem arz etmektedir

Siber uzay için ekranın arkasındaki dünya şeklinde bir tanım yapılabilir. Ancak özellikle 1960'lardan sonra bu dünya internet teknolojilerinin gelişmesine de bağlı olarak daha da gelişmiştir (Klimburg & Mirtl, 2012). Bilgi ve iletişim teknolojileri günümüzde sivilleşmekle birlikte devletler bunları, e-devlet, internet teknolojileri ve internet bankacılığı gibi kullanabilmekte ve vatandaşlar da bu anlamda teşvik edilebilmektedir. Teknolojik gelişmelerin etkisiyle siber uzayın genişlemiş, bu genişlemenin etkisiyle ortaya çıkacak olan bir sorunun yalnızca yazılım, bilgisayar veya ağ mühendislerince çözülecek bir problem olmadığı anlaşılmıştır (Bıçakçı, 2014). Kara, deniz, hava ve uzayın aksine siber uzay, zamanla değişebilen bileşenlere sahip bir insan yapısıdır.

3. KRİTİK ALTYAPILARA YÖNELİK GERÇEKLEŞTİRİLEN SİBER SALDIRI YAZILIMLARI VE ÖRNEKLERİ

Kritik altyapılara yapılan saldırılar devletlerin üzerinde önemle durması gereken konuların başında gelmektedir. Geçmişte yaşanmış olan siber saldırıların incelenmesi gelecekte yaşanabilecek siber saldırılar açısından farkındalık yaratmak açısından önemlidir.

Uluslararası ve ulusal literatür incelendiğinde siber güvenlik açıklarının genelde insan eylemleri sonucunda ortaya çıktığı görülmektedir. Bu eylemler her ne kadar sanal mecralarda meydana gelmiş olsalar da bireyleri ve kurumları ciddi bir şekilde etkilemektedir. Siber saldırı devletlerin veya kurumların kritik altyapılarına verileri çalma, değiştirme, bozma, kötücül yazılımlarla zarar verme, hizmet dışı bırakma, gizli bilgileri açığa çıkartma gibi planlı ve koordineli saldırıları ifade eden bir kavram olarak tanımlanmaktadır (Çakmak & Demir, 2009: 29-31). Siber tehditlerin ortaya çıkmasında ise temel olarak üç boyutun etkili olduğu görülmektedir. Bu boyutlar donanımsal ve yazılımsal hatalar ile internet tasarımındaki eksiklikler olarak sınıflandırılmaktadır (Clarke, Richard, & Knake, 2010: 78-85).

Kritik altyapılara gerçekleştirilen siber saldırılarda bu altyapıların kontrol noktalarının güvenliği büyük bir önem arz etmektedir. Veri toplama ve kontrol sistemlerinden bir tanesi olan ve ağa bağlı bilgisayarların iletişimine ve kontrolüne olanak sağlayan Supervisory Control and Data Acquisition (SCADA) doğalgaz ve su gibi kritik sistemlerin kontrol edilmesinde kullanılmaktadır (Daneels & Salter, 1999). Stuxnet'de SCADA sistemlerine saldırmak üzere oluşturulmuş zararlı bir yazılımdır. 2010 yılının Haziran ayında keşfedilen ve İran'ın yüksek düzeyde korunan nükleer tesislerinin arızalanmasına neden olan dünya üzerinde en zararlı yazılımların başında gelmektedir. Literatürde bu saldırının ABD tarafından gerçekleştirildiğine inanılsa da bu durum henüz kanıtlanamamış olup ABD tarafından da konuyla ilgili açıklama yapılmamıştır (Çelik, 2013: 144-147).

Duqu ise, Stuxnet'in tespitinden bir yıl sonra keşfedilen bir diğer zararlı yazılımdır. Duqu zarar verme şekli açısından Stuxnet ile benzerlik göstermektedir. Bu iki zararlı yazılımın en temel ortak özelliği kritik altyapıların kontrol sistemlerini hedef almalarıdır Nüfuz etmiş olduğu elektronik cihazlarda *dq* adlı bir kaynak kodu oluşturduğu için bu isimle anılmaktadır (Rid & Mcburney, 2012: 11; Çahmutoğlu, 2020: 9).

Stuxnet yazılımından daha karmaşık kodlar içeren Flame ise Ortadoğu ülkelerini hedef alan bir virüstür. Etkisi altına almış olduğu bilgisayardan yıllarca veri akışı sağlamıştır. Yerleştiği bilgisayarlarda ve akıllı telefonlarda bluetooth özelliğini açarak, veri toplayabilen bu yazılım özellikle İran'ın petrol ve gaz şirketlerine sızmıştır (Bencsáth, Pek, Buttyan, & Feleghazi, 2012).

Tarihte siber kaynaklar aracılığıyla meydana gelen ilk saldırı ABD ile Sovyetler arasındaki soğuk savaş döneminde Sibirya'da gerçekleştirilmiştir. ABD tarafından Sovyetlere ait doğalgaz tesisini idare eden yazılım içerisine virüs yerleştirilerek sistemin yapısı bozulmuş, boru hatlarının patlaması sağlanmıştır (Sertçelik, 2015: 31).

İsrail'in Gazze kentine yapmış olduğu saldırıları arttırması üzerine Anonymous adlı hacktivist grup İsrail'e karşı "OpIsrael" adını verdikleri saldırılara başlamışlardır. 07.04.2013 tarihinde Redhack grubuyla birlikte saldırılara başlayan grup yaklaşık olarak 40.000 Facebook, 5.000 Twitter ve 30.000 İsrail banka hesabına siber saldırı düzenlemiştir. Bu saldırılara sonucunda İsrail'e 3 milyar dolar zarar verildiği bildirilmiştir. İsrail hükümeti her ne kadar saldırıların amacına ulaşmadığını iddia etmiş olsa da bu durum ülkenin siber saldırılara açık olduğunun bir göstergesidir (The Atlantic, 2013).

Yine 2011 yılının Şubat ayında McAfee güvenlik şirketi başkan yardımcısı Dmitri Alperovitch Çin tarafından organize edilen siber saldırıların tespit edildiğini iddia etmiştir. Çin tarafından en az beş batılı ülkenin petrol ve doğalgaz şirketlerinin altyapılarının hedef alındığı ve bu saldırılar sonucunda ise Çin devletinin önemli bilgiler ele geçirdiği iddia edilmektedir (Keizer, 2011; Knapp, 2011: 41).

Türkiye'de de son dönemde yoğun olarak siber saldırıların gerçekleştiği görülmektedir. 09.07.2021 tarihi itibariyle Türkiye'ye yönelik toplam 1.6 milyon siber saldırı gerçekleşmiştir. Bu oranın 2020 yılına göre %81 artış gösterdiği görülmektedir. Zamansal olarak incelendiğinde ise her üç dakikada bir Türkiye'de siber saldırı olduğu görülmektedir (Hürriyet, 2021). Nitekim son dönemde MNG kargo, Akbank, Sinoz kozmetik gibi ciddi sayıda insanın yararlandığı firmalara veri transferi amacıyla çeşitli siber saldırılar gerçekleştirilmiştir (NTV, 2021).

Bu örnekler dünya genelinde gerçekleşen siber saldırılardan aslında sadece birkaçıdır. Bu noktada her ülkenin siber güvenliği sağlamak noktasında kritik altyapılara gelecek herhangi bir saldırıya karşı kurum ve kuruluşlarıyla hazır olması önem arz etmektedir. Çalışmada bu açıdan Türkiye'de önemli bir kurum olan AFAD'ın çalışmalarına, mevzuatına, uygulamalarına yer verilerek bir değerlendirme yapılacaktır.

4. KRİTİK ALTYAPILARA SALDIRI BAĞLAMINDA AFET VE ACİL DURUM YÖNETİMİ BAŞKANLIĞI'NIN DEĞERLENDİRİLMESİ

Bu başlık altında kritik altyapıların korunması konusunda AFAD'ın mevzuat ve kurumsal raporlar açısından değerlendirilecektir.

4.1. Mevzuat Yönünden Değerlendirme

Dünya genelindeki afetlerin sayısının ve vermiş olduğu yıkıcı etkilerin artmasıyla birlikte önem kazanan afet yönetimi; doğal, teknolojik veya insan kaynaklı yıkıcı olayların, riskli alan ve konuların tespitini sağlayan planlamadan kontrole kadar olan süreçleri kapsayan disiplinlerarası bir çalışmadır (Karaman, 2017: 2,3). Bu bağlamda kamu kurum ve kuruluşlarının paydaşlarla birlikte etkin ve verimli işbirliği büyük önem taşımaktadır.

Siber güvenlik ile doğrudan bağlantılı ilk hukuki düzenleme ulusal siber güvenlik çalışmalarının yürütülmesine ilişkin 2012 yılındaki bakanlar kurulu kararıdır. Bu kararın amacı bilgi teknolojilerinin güvenliğini sağlayarak kritik altyapıları yönetilmesinde gerçek ve tüzel kişilerin sorumluluklarını belirlemektir. Bu düzenlemeyle birlikte Türkiye'de ilk siber güvenlik kurulu kurulmuştur. Bu kurulda İçişleri, Dışişleri, Ulaştırma ve Altyapı Bakanlıklarının yanı sıra Millî İstihbarat Teşkilâtı, Genelkurmay Başkanlığı gibi güvenlik açısından kritik öneme sahip kurumlarda bulunmaktadır (RG, 2012).

2013 yılında da Bakanlar Kurulu kararıyla bağlantılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ yürürlüğe girmiştir. Bu tebliğin amacı siber olaylara müdahale eden ekibin görev ve sorumluklarının belirlenerek hizmette etkinlik ve verimliliğin sağlanmasıdır. Tebliğ içerisinde ayrıca Ulusal Siber Olaylara Müdahale Merkezinin görev sorumlulukları, yapısı ve diğer kurumlarla olan ilişkisi hükme bağlanmıştır (RG, 2013).

4 numaralı Cumhurbaşkanlığı kararnamesinin 30. maddesinde ise afet ve acil durumlarda kurum ve kuruluşlar arasındaki koordinasyonun sağlanması görevi AFAD'a verilmiştir. Siber saldırı eylemlerinin de teknolojik bir afet olduğu düşünüldüğünde AFAD'ın bu konudaki önemi oldukça açıktır. 4 numaralı kararnamenin 35. maddesine göre başkanlığın merkez teşkilatı 13 adet hizmet biriminden oluşmaktadır. Bu hizmet birimleri içerisinde kritik altyapıların güvenliğini sağlayan başkanlık Bilgi ve Haberleşme Dairesi Başkanlığı'dır. İlgili kararnamede başkanlığın bilişim altyapısının gelişimini izlemek, bilgi işlem konusunda ilgili kamu kurum ve kuruluşlarıyla işbirliğinde bulunmak, afet ve acil durumlarla mücadele amacıyla coğrafi bilişim sistemlerinin kurulmasını sağlamak, başkanlığın bilişim altyapısının bakımı, gelişimi ve güncellenmesi faaliyetlerini yürütmek bunlarla ilgili güvenlik tedbirlerini almak ve e-devlet uygulamalarının başkanlık ile ilgili faaliyetlerini gerçekleştirmek başkanlığın temel görevleri arasında sayılmıştır.

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı tarafından hazırlanan 2019-2023 yılları arasını kapsayan 11. Kalkınma Planında siber güvenliğe yönelik düzenlemelerin ve kurumsal altyapının güçlendirileceği üzerinde durulmuştur. Planda kurumlararası koordinasyona da özel bir önem verildiği görülmektedir. Ayrıca ihtiyaç duyulan alanlarda da siber güvenlik standartlarının oluşturulacağı hüküm altına alınmıştır.

Yukarıda görüldüğü üzere AFAD, mevzuat bakımından kritik altyapıların korunup kurumlararası eşgüdümün sağlanması, bilişim altyapısının izlenmesi, kamu kurum ve kuruluşları arasında iletişimin sağlanması ve kritik altyapıların güncel tutulması konusunda yetkili kılınmıştır (Cumhurbaşkanlığı, 2019).

4.2. Kurumsal Raporların Değerlendirilmesi

Bu başlık içerisinde AFAD'ın kritik altyapıların korunmasına yönelik 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, 2019-2023 AFAD Stratejik Planı, Türkiye Afet Müdahale Planı ve 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı üzerinde durulmuştur.

4.2.1. 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi

AFAD tarafından 2014 yılında yürürlüğe giren 2014-2023 yılları arasını kapsayan belgede kritik altyapıların korunmasıyla ilgili yol haritası hazırlanmıştır. Bu yol haritası içerisinde teknolojik afetler konusundaki çalışmaların desteklenmesi, teknolojik afetlerin önlenmesi konusundaki kurumlararası işbirliğinin geliştirilmesi, siber risk ve saldırıların önlenmesi amacıyla araştırma projelerinin desteklenmesi, kritik altyapıları belirleyecek kurumlar arasındaki koordinasyonun sağlanması ve bu altyapılara yönelik verileri hazırlama görevi AFAD'a verilmiştir. Belgede ayrıca kritik altyapı konusundaki yetkili kurumlar belirlenerek AFAD ile işbirliği içerisindeki roller ve sorumlulukları belirlenmiştir.

Yol haritası belgesinde kritik altyapıların korunması çerçevesi alt başlığında kritik altyapı sektörleri üzerinde de durulmuştur. Enerji, ulaştırma altyapı, barajlar, finans, sağlık, tarım, kültür turizm, kritik kamu ve ticari üretim sektörlerinin kritik öneme sahip olduğu vurgulanmıştır. Burada AFAD'a tesis, sektör ve koordinasyon konusunda da çeşitli görev ve sorumluluklar verildiği görülmektedir (AFAD, 2014).

4.2.2. AFAD 2019-2023 Stratejik Planı

2013-2017 yıllarını kapsayan AFAD Stratejik Planı'nda siber güvenlikle ilgili doğrudan bir hüküm olmasa da bilişim altyapısının güçlendirilmesine yönelik stratejilerin belirlendiği görülmektedir. Bilişim altyapısının güçlendirilmesi ve bilgi güvenliğinin sağlanması kapsamında çeşitli plan projeler gerçekleştirilmesi hedeflenmiştir. Bu projelerin ilki Kurumsal Kaynak Planlama Sistemi (ERP) Projesidir. Bu proje kapsamında kurumsal faaliyetleri ilgilendiren iş ve işlemlerin elektronik ortama

aktarılması amaçlanmaktadır. Bilişim Güvenliği Yönetim Sistemi Projesinde, bilgi ve veri güvenliği farkındalığı oluşturmak amacıyla danışmanlık hizmeti sağlamak; Bilişim Sistemleri ve Ağ Altyapısının Güçlendirilmesi Projesinde ise ağ sistemlerinin altyapısını güçlendirmek amaçlanmıştır (AFAD, 2012).

2019 yılında uygulanmasına başlanan AFAD Stratejik Planı'nda ise kritik altyapıların korunmasına yönelik hedeflerin yer aldığı görülmektedir. Planda siber saldırılar risk olarak tanımlanmış olup siber saldırılara karşı etkin tedbirlerin alınması temel ihtiyaç listesinde sayılmıştır. Buna göre dünya genelinde ve Türkiye'de artış gösteren afet olaylarına karşı 2030 yılına kadar kritik altyapıların dirençliliğini arttırmak, kritik tesislerde meydana gelecek kriz durumlarında uygulanacak özel müdahale planlarının etkinliğinin arttırmak, kritik altyapı sektörlerinin belirlenerek 2023 yılına kadar 10 sektörde metodolojik planlar oluşturmak planda belirlenen temel hedef ve stratejiler arasında yer almaktadır (AFAD, 2019).

4.2.3. Türkiye Afet Müdahale Planı

Türkiye'de yaşanma ihtimali olan her türlü afete karşı görev alacak kurum ve kuruluşların görev ve yetkilerini kapsayan afet müdahale planında da kritik altyapıların korunması ve siber saldırıların önlenmesine ilişkin başlıklar bulunmaktadır. Plan hükümet tesisleri, sağlık gibi kritik altyapıların saldırılara uğrama ihtimalinden hareketle il afet ve acil durum kurullarına kritik tesislerde meydana gelme ihtimali olan riskleri önleme çalışmaları yapma sorumluluğu verilmiştir. Afet müdahale planı kapsamında oluşturulan alt hizmet gruplarının da kritik tesislerin korunması konusunda ilgi alanlarına göre çeşitli görevleri bulunmaktadır. Örneğin altyapı hizmet grubunun altyapı ile ilgili önemli tesislerin acil durumlarda hızlı bir şekilde devreye girmesini sağlama görevi bulunmaktayken; enerji hizmet grubunun ise enerji kaynaklarının hızlı bir şekilde deveye girmesi görevi bulunmaktadır (AFAD, 2013).

Planda da görüldüğü üzere kritik altyapıların korunması konusunda çok paydaşlı bir sistemin benimsendiği bu konudaki koordinasyon işinin AFAD'a bırakıldığı görülmektedir.

4.2.4. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Ulaştırma ve Altyapı Bakanlığı tarafından 2020-2023 yılları arasını kapsayan eylem planında AFAD ile ilgili doğrudan bir hüküm olmasa da AFAD'ın görev ve yetkilerinin şekillenmesinde önemli bir yol haritası olmaktadır. Bu planda sekiz temel stratejik hedef belirlenmiştir. Kritik altyapıların korunması, yeni dönem teknolojik yapılanmaların güvenliğinin sağlanması, siber suçlarla mücadele edilmesi, uluslararası iş birliğinin geliştirilmesi ve organik siber güvenlik ağı projesi konuyla bağlantılı hedeflerin arasında yer almaktadır. Planda Covid-19 dönemiyle bağlantılı siber güvenliğin önemine vurgu yapılmış olup kritik altyapıların güvenliğinin önemi vurgulanmıştır. Siber güvenliğin ulusal güvenliğin önemli bir parçası olduğu vurgulanmış dijitalleşmenin modern dünyanın parçası olduğu üzerinden paydaşların katılımıyla ortak bir güvenlik politika belirlenmesi zorunluluğu vurgulanmıştır. Bu bağlamda kritik altyapıların güvenliği ve siber savunmanın ana konusunun güvenlik olmasına rağmen literatürde görev ve sorumluluğun AFAD'a verildiği görülmektedir. 2018 yılı Cumhurbaşkanlığı hükümet sistemi değişiklikleri de göz önüne alındığında AFAD'ın İçişleri Bakanlığı'na bağlanması iç güvenliğin koordine edilmesi konusunda daha yetkilendirilmesine yol açtığını ifade eden çalışmalar bulunmaktadır (Ak, 2019: 48).

SONUÇ

Kritik altyapıların korunması gelecekte yaşanabilme ihtimali olan bir siber saldırıya karşı hazırlıklı olunması adına oldukça önemlidir. Ülkelerin siber saldırılara karşı mücadele etmesi için bu altyapıların belirlenmesi ve bu altyapılara yönelik bir savunma mekanizması oluşturulması büyük önem taşımaktadır. Sadece ülke düzeyinde değil tüm ülkelerin ortak hareket ettiği sınır ötesi iş birliğinin de sağlanması siber suçlara yönelik bir caydırıcılığın ortak hedef olarak belirlenmesi önemli bir faktördür.

Kurum ve kuruluşlarıyla ülkelerin kritik altyapılarına saldırılar noktasında hazır bulunması gerekir. Bu anlamda Türkiye'de AFAD önemli sorumlu bir kurumdur. AFAD'ın çalışmalarında genel olarak doğal afet ağırlıklı çalışmalar olduğu görülse de siber tehditlere yönelik olarak da farkındalık çalışmaları yaptıkları ve personellerine bu konularda çeşitli eğitimler verdikleri görülmektedir. Özellikle Kritik Altyapıların Korunmasına Yönelik Yol Haritası Belgesi siber alanların güvenliğinde yol gösterici olması açısından önemlidir. Bunun yanı sıra özellikle Bütünleşik İkaz ve Alarm Sistemi afetlere yönelik olarak

vatandaşların bilgilenmesini sağlaması açısından önemli bir adımdır. 3. Uluslararası Afet ve Dirençlilik Kongresinde (Resilience, 2021) edinilen bilgiden hareketle mesajla uyarı sisteminin etkili olmadığı ifade edilmiştir. Bu noktada çalışmaların devam ettirilmesi ve çözüm sağlanması önemli görülmektedir. AFAD'ın siber tehditlere yönelik çalışmalarının devam etmesinin yanı sıra Sanayi ve Teknoloji Bakanlığı, Dijital Dönüşüm Ofisi, Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı ve üniversitelerin konuda ortak çalışmalar yapması gelecekte gerçekleşebilecek bir siber saldırıya karşı hazırlıklı olunması adına kayda değer bir konudur.

KAYNAKÇA

AFAD. (2012). *2013 – 2017 Stratejik planı*. http://www.sp.gov.tr/upload/xSPStratejikPlan/files/9hMG-G+afadsp2013-2017.pdf adresinden alındı.

AFAD. (2013). *Türkiye afet müdahale planı*. https://www.afad.gov.tr/kurumlar/afad.gov.tr/2419/files/Afet_Mud_Pl_ResmiG_20122013.pdf adresinden alındı

AFAD. (2014, 09). *Kritik altyapıların korunması yol haritası belgesi*. https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-2023-AFAD-Kritik%20Altyap%C4%B1larin%20Korunmasi%20Yol%20Haritasi.pdf adresinden alındı

AFAD. (2019). *Afet ve acil durum*. afad.gov.tr/kurumlar/afad.gov.tr/e_Kutuphane/Planlar/AFAD-2019_2023-STRATEJIK-PLAN.pdf adresinden alındı

Ağır, B. S. (2015). Güvenlik kavramını yeniden düşünmek: Küreselleşme, kimlik ve değişen güvenlik anlayışı. *Güvenlik Stratejileri, 11*(22), 97-131.

Ak, T. (2019). İç güvenlik yönetimi açısından kritik altyapılarını korunması. *ASSAM Uluslararası Hakemli Dergi,* 42 - 51.

Aksu, M., & Turhan, F. (2012). Yeni tehditler, güvenliğin genişleme boyutları ve insani güvenlik. *Uluslararası Alanya İşletme Fakültesi Dergisi*, *4*(2), 69-80.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66.

Ani, U. D., Watson, J. D., Nurse, J. R., Cook, A., & Maple, C. (2019). A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modeling landscape. PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT, (s. 1-16).

Bencsáth, B., Pek, G., Buttyan, L., & Feleghazi, M. (2012). The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet, 4*(4), 971-1003.

Bıçakçı, S. (2014). Nato'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler, 10*(40), 100-130.

Bıçakçı, S. (2019). Siber güvenlik ve savunma. *Güvenlik Yazıları*, 1-8.

Birdişli, F. (2010). Eleştirel güvenlik çalışmaları kapsamında Frankfurt okulu ve soğuk savaş sonrası güvenlik sorunlarına eleştirel bir yaklaşım: Galler ekolü. *Güvenlik Stratejileri*, (20), 229-255.

Birdişli, F. (2011). Ulusal güvenlik kavramının tarihsel ve düşünsel temelleri. *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *1*(31), 149-169.

Brauch, H. G. (2008). Güvenliğin yeniden kavramlaştırılması: Barış, güvenlik, kalkınma ve çevre kavramsal dörtlüsü. *Uluslararası İlişkiler*, 1-47.

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-cold war*. New York: Prentice Hall Harvester Wheatsheaf.

CİSA. (2021). *Critical infrastructure sectors*. https://www.cisa.gov/critical-infrastructure-sectors adresinden alındı

Clarke, R. K., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins Publishers.

Cumhurbaşkanlığı. (2019, 07). *On birinci kalkınma planı*. https://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf adresinden alındı

Cumhurbaşkanlığı. (2021). *Siber güvenlik dairesi başkanlığı*. https://cbddo.gov.tr/hizmet-birimlerimiz/siber-guvenlik-dairesi-baskanligi/ adresinden alındı.

Çahmutoğlu, E. (2020). Siber uzayda güç ve siber silah teknolojilerinin küresel etkisi. *Analytical Politics*, 63-79.

Çakmak, H., & Demir, C. K. (2009). *Siber dünyadaki tehdit ve kavramlar*. H. Çakmak, & T. Altunok içinde, Suç - Terör - Savaş Üçgeninde Siber Dünya (s. 23-55). İstanbul: Platin Yayınları.

Çelik, Ş. (2013). Stuxnet saldırısı ve Abd'nin siber savaş stratejisi: Uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 15*(1), 137-175.

Daneels, A., & Salter, W. (1999). *What is scada*. International Conference on Accelerator and Large Experimental Physics Control Systems, (s. 339-343). Trieste.

EU. (2006, 12 12). *European programme for critical infrastructure protection*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33260 adresinden alındı

EU. (2021). *Critical infrastructure protection*. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection adresinden alındı

Göçoğlu, V. (2018). *Türkiye'nin siber güvenlik politikalarının kamu politikası analizi çerçevesinde değerlendirilmesi*. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp adresinden alındı

GPO. (2001). *USA PATRIOT ACT*. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf adresinden alındı

Güntay, V. (2017). *Siber uzay ve güvenlik politikası üzerine teorik bir yaklaşım*. *Cyberpolitik Journal, 2*(4), 9-22.

Hürriyet. (2021, 07 09). *Türkiye'de 1.6 milyon siber saldırı gerçekleşti*. https://www.hurriyet.com.tr/sosyal/tekno/turkiyede-1-6-milyon-siber-saldiri-gerceklesti-41711458 adresinden alındı

ITU-T. (2014). A *cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies*. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1208-201401-I!!PDF-E&type=items adresinden alındı

Karaman, Z. T. (2017). *Afet yönetimine giriş ve Türkiye'de örgütlenme*. Z. T. Karaman içinde, Bütünleşik Afet Yönetimi (s. 1-38). İzmir: Birleşik Matbaa.

Keizer, G. (2011). *Sloppy' Chinese hackers scored data-theft coup with 'Night Dragon'*. https://www.computerworld.com/article/2513128/-sloppy--chinese-hackers-scored-data-theft-coup-with--night-dragon-.html adresinden alındı

Klimburg, A., & Mirtl, P. (2012). *Cyberspace and governance - A Primer*. https://www.ssoar.info/ssoar/handle/document/43560 adresinden alındı

Knapp, E. (2011). *Industrial Network Security*. Elsevier Inc.

Lewis, J. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*, 1-12.

NTV. (2021, 08 27). *Sinoz Kozmetik'e siber saldırı.* https://www.ntv.com.tr/turkiye/sinoz-kozmetike-siber-saldiri,0ZEz9NEv80eTvvmUgHaA4g adresinden alındı

Resilience. (2021). *3. Uluslararası Afet ve Dirençlilik Kongresi*. https://www.afad.gov.tr/3-uluslararasi-afet-ve-direnclilik-kongresi-afad-ev-sahipliginde-gerceklestirilecek adresinden alındı.

RG. (2012, 06 11). *Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar*. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf adresinden alındı

RG. (2013, 11 11). *Siber olaylara müdahale ekiplerinin kuruluş, görev ve çalışmalarına dair usul ve esaslar hakkında tebliğ*. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19004&MevzuatTur=9&MevzuatTertip=5 adresinden alındı

Rid, T., & Mcburney, P. (2012). Cyber weapons. *Rusi Journal, 157*(1), 6-13.

Sağıroğlu, Ş. (2018). *Siber güvenlik ve savunma: Önem, tanımlar, unsurlar ve önlemler*. Ş. Sağıroğlu, & M. Alkan içinde, Siber Güvenlik ve Savunma (s. 21-45). Ankara: Grafik Matbaacılık.

Sanayi ve Teknoloji Bakanlığı. (2019). *Sanayi ve Teknoloji Zirvesi Belgesi*. https://www.sanayi.gov.tr/assets/pdf/SanayiStratejiBelgesi2023.pdf adresinden alındı.

Semiz, İ., Göztepe, K., & Kılıç, R. (2013). *Kritik altyapıların siber güvenliğinin sağlanmasında üçlü boyut yaklaşımı*. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (s. 32-35). Ankara: Proceedings.

Sertçelik, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi, 2*(3), 25-42.

The Atlantic . (2013, 04 08). *Anonymous tits Israel with a massive cyber attack, Israel attacks back*. https://www.theatlantic.com/international/archive/2013/04/anonymous-hits-israel-massive-cyber-attack-israel-attacks-back/316538/ adresinden alındı

Turan, M. (2018). Türkiye'nin Yeni Yönetim Düzeni: Cumhurbaşkanlığı Hükümet Sistemi. Social Sciences Research Journal, 7(3), 42-91.

Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal siber güvenlik stratejisi ve eylem planı.* https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf adresinden alındı

Wiener, N. (1948). Cybernetics or control and communication in the animal and the machine. Paris: Cambridge MIT Press.