***İÇ GÜVENLİK YÖNETİMİ AÇISINDAN KRİTİK ALTYAPILARINI* KORUNMASI**

 ***Tarık AK[[1]](#footnote-1)\****

 **Öz**

 Kritik altyapılar, modern toplumun yaşamı için vazgeçilmezdir. Kritik altyapılar, toplumsal refahın ve ekonomik gelişmişliğin işareti olarak görülür. Hayatın her yönünü destekleyen kritik altyapıların korunması, kamu düzeni ve güvenliğin sağlanması açısından da zorunluluktur. Bu kapsamda çalışma, kritik altyapıların korunmasıyla ilgili olarak dünyada yaşanan gelişmeler ve bu konuda iç güvenlik açısından Türkiye’de yapılması gerekenlerin tespit edilmesini hedeflemektedir. Çalışma, literatür taraması yapılarak teorik bir zeminde yürütülmüştür. Çalışma’da ilk olarak kritik altyapı güvenliğinin ne olduğu irdelenecek, müteakiben ABD, AB ve BM açısından odaklandıkları konular vurgulanacaktır. Son olarak ise; iç güvenlik açısından kritik altyapıların korunması usulü belirtilecek ve Türkiye bağlamında değerlendirmeler yapılacaktır. Dünyada, kritik altyapıların korunmasıyla ilgili olarak afet yardım ve acil yönetim ihtiyaçları yanında terör olayları ve internet yoluyla müdahalelere de odaklanıldığı görülmektedir. Türkiye’de ise daha çok kritik altyapıların korunamaması durumunda meydana gelecek çevresel ve insani etkiler vurgulanmıştır. Bunun nedeni kritik altyapıların korunmasının Türkiye’de literatüre AB’ye uyum süreci kapsamında çevre temelli etkileri bağlamında girmiş olmasıdır. Türkiye tüm kritik altyapılara yönelik farklı tehditleri ve tedbirleri kapsayan bir iç güvenlik yaklaşımına sahip olmalıdır.

 **Anahtar Kelimeler:** İç güvenlik, Anayurt güvenliği, İç güvenlik yönetimi, Kritik altyapı

**PROTECTION OF CRITICAL INFRASTRUCTURES IN TERMS OF**

**INTERNAL SECURITY ADMINISTRATION**

 **Abstract**

 Critical infrastructures are indispensable for the life of modern society. Critical infrastructures are seen as a sign of social welfare and economic development. The protection of critical infrastructures that support all aspects of life is a necessity in terms of public order and security. This study, within this framework, aims to determine developments in the world related to the protection of critical infrastructures and identify what to do in Turkey on this issue in terms of internal security. This study has been carried out in a theoretical foundation by reviewing the literature. In this study, the first step will be followed by examining what the critical infrastructure security is. Aftermath, the issues that United States, the EU and the UN focused on will be emphasized. Finally, procedures on the protection of critical infrastructures for internal security will be indicated and it will be evaluate in the context of Turkey. Concerning the protection of critical infrastructures in the world, it is seen that there is a focus on the need for disaster relief and emergency management as well as terror events and interventions on the internet. In Turkey, the environmental and human impact will occur in case of lack of protection of critical infrastructure are highlighted. The reason is that subject of protection of critical infrastructure entered literature in Turkey by EU harmonization process which is based on environmental impact issues. Turkey should have a different approach involving internal security threats and measures for all critical infrastructure.

 **Key Words:** Internal security, Homeland security, Internal security administration, Critical infrastructure.

**GİRİŞ**

 Kritik altyapılar, modern toplumun yaşamı için vazgeçilmezdir. Kritik altyapıların varlığı, toplumsal refahın ve ekonomik gelişmişliğin göstergesi olarak ortaya çıkar, gelecek kuşaklara miras bırakılan medeniyetlerin beşeri alanını karşılar. Özellikle bir ülkenin insanları kendilerini teknoloji odaklı bir toplum olarak görüyorsa ve birlikte yaşama ölçüsünü sanayileşme olarak belirlediyse, kritik altyapıların önemi daha da anlamlı hale gelmektedir. Genel olarak altyapıların kritikliği, altyapının yakın çevresi, tüm ülke hatta sınırdaş ülkeleri olmak üzere bu tesisten faydalanan ya da etkilenenlerin hayatta kalmasını, refahını ve yaşam tarzını koruma derecesine göre belirlenir. Kritik altyapıların tehdit edilmesi durumunda çalışmaması veya kaybı neticesinde insanların hayatına ve yaşam tarzına doğrudan olumsuz etki edebileceği, ülkelerin hali hazırda yürütülen sağlık, çevre, teknoloji, ekonomi, siyaset ve ulusal güvenlik sistemlerindeki dengeyi bozabileceği bir gerçektir (Caşın, 2015:10). Bu nedenle hayatın her yönünü destekleyen kritik altyapıların korunması, kamu düzeni ve güvenliğin sağlanması açısından da vazgeçilmezdir. Vatandaşların yaşamına, yaşam tarzına, toplumunun birlikteliğine ve birlikte yaşama arzusuna yönelen her türlü saldırı ve tehditlere karşı önlem almaya karşılık gelen iç güvenlik, altyapıların kullanılabilirliğinin devamını sağlamak için bir seçenek değil zorunluluk olarak görülmektedir (AK, 2018:75; US PCCIP, 1997: vii).

 Kritik altyapı kavramı, ilk olarak 1996 yılında Amerika Birleşik Devletleri (ABD)’nde imzalanan kanun hükmünde kararnamede kullanılmıştır. Dönemin ABD Başkanı kritik altyapıların korunmasına ilişkin esasların belirlenmesi için bir komisyon oluşturmuş, bu komisyon bir yıl sonra ABD’de kritik altyapılarla ilgili içinde tespit ve öneriler bulunan bir rapor hazırlamıştır (Karanacak, 2011; US PCCIP, 1997:6). ABD için kritik altyapılar, çalışmaması veya çökmesi durumunda ulusal savunma ve ekonomik güvenliğini zayıflatma etkisine sahip olan yerlerdir. 1997 yılında bu yerleri; **(ı)** Telekomünikasyon. **(ıı)** Elektrik güç kaynakları, gaz ve petrol depolama ve üretim üniteleri. **(ııı)** Bankacılık ve finans kurumları. **(ıv)** Ulaştırma birim ve unsurları. **(v)** Suyun tedarik edildiği birimler. **(vı)** Acil tıbbi müdahale birimleri, genel kolluk, yangın ve arama kurtarma ünitelerini içine alan acil hizmet birimleri. **(vıı)** Devlet hizmet ve kurumları olarak göstermiştir (US PCCIP, 1997: A-1/B-1).

 *“Kritik altyapı”* kavramı, tanım olarak Türkiye’de Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) tarafından hazırlanan “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”nde *“İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür”* şeklinde tanımlanmıştır (AFAD, 2014a: 4). Yine AFAD’a ait Açıklamalı Afet Yönetimi Terimleri Sözlüğü’nde *“İşlevlerini kısmen veya tamamen yerine getiremediğinde toplumsal düzenin sürdürülebilirliğinin veya kamu hizmetlerinin sunumunun olumsuz etkileneceği ulaşım, haberleşme, enerji, su, finans gibi sektörleri kapsayan ağ, varlık, sistem ve yapılar bütünü”* olarak tanımlanmıştır (AFAD, 2014b: 106). Benzer tanımlamalar dünyada birçok ülke ve kuruluş tarafından yapılmakla birlikte, 1990’lı yıllardan itibaren tartışılan bu kavrama ilişkin tanımlama çeşitliliği göze çarpmaktadır (AFAD, 2014a: 14; Tüney & Gücüyener, 2015). Avrupa Birliği (AB), kritik altyapılar kavramını *“bozulduğunda veya tahrip edildiğinde üyesi devletlerin vatandaşlarının sağlığı, emniyeti, güvenliği ve ekonomik refahı veya hükümetlerin etkin işleyişi üzerinde ciddi bir etkisi olacak olan fiziksel ve bilgi teknoloji tesisleri, ağları, hizmetleri ve varlıkları”* olarak tanımlamaktadır. AB, 2004 yılında ilk kez bu tanımlamaya uyan dokuz sektör belirlemiştir. Bunlar; **(ı)** Enerji kurulumları ve ağları. (Elektrik enerjisi, petrol ve gaz üretimi, depolama tesisleri ve rafineriler, iletim ve dağıtım sistemleri) **(ıı)** İletişim ve bilgi teknolojilerinin kendisi ve altyapıları. (İnternet dâhil telekomünikasyon, yayın sistemleri, yazılım, donanım ve ağlar) **(ııı)** Finansman hizmetleri. (Bankacılık, menkul kıymetler ve yatırım) **(ıv)** Sağlık hizmetlerinin kendisi ve yapıları. (Hastaneler, sağlık ve kan sağlama tesisleri, laboratuvarlar ve eczacılık ürünleri, arama kurtarma, acil durum hizmetleri) **(v)** Gıdanın kendisi, yapıları ve ağları. (Gıda güvenliği, üretim araçları, toptan dağıtım ve gıda endüstrisi) **(vı)** Suyla ilgili altyapılar. (Barajlar, depolama, arıtma ve ağlar) **(vıı)** Ulaşım araçları ve ağları. (Havaalanları, limanlar, demiryolu ve toplu taşıma ağları, trafik kontrol sistemleri) **(vııı)** Kimyasal, biyolojik, radyolojik ve nükleer maddeler gibi tehlikeli malların üretimi, depolanması ve taşınması. **(ıx)** Hükümete ait değerli varlıklar ve işlevler. (Kritik hizmetler, tesisler, bilgi ağları, ulusal önemde alanlar ve anıtlar) AB’nin vurguladığı kritik unsurlara bakıldığında altyapı özelliği dışında birçok temel ürün veya hizmetin sunumu ile onu destekleyen ağların ve tedarik zincirlerinin olduğu görülebilir (EU COM702(F1), 2004: 3-4). Birleşmiş Milletler ise; kritik altyapıları, su gibi yaşamsal ürünlerin tedariklerinin sağlanması, enerji, ulaşım hizmetleri olarak değerlendirirken, altyapıların korunmasını bu tesislerin fiziki ve internet yoluyla terör saldırılarına maruz kalmasını önlemek olarak tanımlamıştır. Bu tesisler; iletişim, acil durum hizmetleri, enerji, barajlar, finans, gıda, kamu hizmetleri, sanayi, sağlık, ulaştırma, doğal gaz, radyo ve televizyon gibi kamu ile iletişim araçları, bilgi teknolojileri, ticari tesisler, kimya ve nükleer sektörler ile suyla ilişkili tedarik ve ikmal tesisleridir (UN CTED, 2017: 2-4).

**1. AB AÇISINDAN KRİTİK ALTYAPILAR**

 AB, kritik altyapılara yönelik terör ve siber saldırıları iç güvenlik stratejileri içerisine dâhil etmiştir (European Commission, 2014:7 EU COUNCIL, 2015, 7; EU COUNCIL, 2016: 25/42). AB’nin kritik altyapıların korunması ile ilgili ilk adımları, 2004 yılında Madrid’de tren ağlarına ve sonraki yılda Londra'da metro istasyonuna yapılan terör saldırıları[[2]](#footnote-2) sonrasında olmuştur. Benzer saldırıların Avrupa çapında önlenmesi, bu saldırılara karşı hazırlıklı olunması ve gerçekleşmesi durumunda gereken tepkilerin gösterilmesi maksadıyla başlatılmıştır. Avrupa’da altyapılara yönelik beliren terör saldırı riskleri, 2004 Haziran ayında Avrupa Konseyi’nden gelen talep doğrultusunda Avrupa Komisyonu tarafından 20 Ekim 2004’de *“Terörle Mücadele için Kritik Altyapı Korunması”* başlıklı bir belge hazırlanmasıyla sonuçlanmıştır. Bu belgede; kritik altyapıların tanımı yapılmış, kritik altyapılara yapılacak fiziki ve siber terör saldırılarının birçok insanın hayatının kaybetmesiyle sonuçlanacağı, bu bakımdan AB’nin tepkisinin hızlı, koordineli ve verimli olması gerektiği hususu vurgulanmıştır. AB ülkelerin sanayileşme, kentleşmeyle birlikte kritik altyapı ve bilgi teknolojileri başta olmak üzere her alanda birbirine bağımlı hale geldiği bilindiğinden bunların tahrip edilme durumlarına karşılık savunmasız kalınmaması için hazırlık yapılmasının zaruriyeti ortaya konmuştur. Bu nedenle 2005 yılına kadar ülkelerin kritik tesislerinin belirlemeleri gerektiği ifade edilmiştir. Ayrıca ülkelerin çok sayıda ve farklı özellikte kritik altyapıları göz önünde bulundurulduğunda öncelikle, ülkelerin sınırları aşan altyapıların korunmasına yönelik çabalarını yoğunlaştırması gerektiği belirtilmiş, diğer ulusal altyapı tesislerinin de güvenliğinin ortak bir yaklaşımla üye ülkelerce sağlanması istenmiştir (EU COM702(F1), 2004:4; EU COM576, 2005: 2; AFAD, 2014a: 17). AB tarafından 2005 yılında ise “*Kritik Altyapıların Korunması için Avrupa Programı (KAKAP)”* programı açılmış, ayrıca *“Kritik Altyapılar Uyarı Bilgi Ağı”* kurulmuştur. Bu belge, kritik altyapıların terör saldırıları öncelikli olmak üzere doğal afetleri de içerecek şekilde bir korunma kapasitesi oluşturulmasını ve kritik altyapılarda zayıf noktaların azaltılması hususuna odaklanmıştır. 2006 yılındaki programa ilişkin tebliğ ile üye ülkelerin mevzuatları uyumlaştırılarak 2013 yılına kadar kritik altyapıların korunması hususunda risklerin azaltılması ve önlemlerin geliştirilmesi istenmiştir. 2008 yılında nihai çerçeve olarak *“Avrupa Kritik Altyapılarının Belirlenmesi ve Koruyucu Tedbirlerin Artırılması”* direktifi yayınlanmıştır. Bu direktifte genel bir zorunluluk yaratılmamakla birlikte kritik alt yapılar enerji ve ulaşım olarak ikiye ayrılmıştır. **(ı)** Enerji alanındaki altyapılar elektriğin kullanımıyla ilgili doğalgaz, elektrik üretim ve iletim tesisleri ve altyapısı, petrol üretim, rafine, işleme, depolama tesisleri ve dağıtım boru hatları, sıvılaştırılmış doğalgaz terminalleridir. **(ıı)** Ulaştırma alanında altyapılar ise hava, demiryolu ve karayolu taşımacılığı, iç sularda taşımacılık, okyanus ve kısa mesafe deniz yolu taşımacılığı ile limanlardır (EU COUNCIL DIRECTIVE/114/EC, 2008: L345/81). Direktif, Avrupa kritik altyapıların korunması sorumluluğunu öncelikli üye devletlere ve bu tür altyapıların sahiplerine veya işletmecilere vermiştir. Direktif, bilgi ve iletişim teknolojilerini göz ardı etmeyen ancak enerji ve taşımacılık sektörlerine ağırlık veren bir direktif olarak yayınlanmıştır. Direktifin uygulamaya geçmesi ve işlerliğinin denetimi için en geç 2012 yılı Ocak ayı belirlenmiştir. 2009 yılı Stockholm Programı ise, Avrupa Kritik Altyapıların korunmasının önemini vurgulamış ve özellikle kırılganlıkların belirlenmesi üzerine dikkat çekilmiştir. 2011 yılında Avrupa Birliği İç Güvenlik Stratejisi *“5 Adımda Daha Güvenli Avrupa”* ile altyapıların korunmasının dayanışma yoluyla olacağını belirtmiştir. Lizbon Antlaşması ve İç Güvenlik Stratejilerinin yürürlüğe girmesi ise, KAKAP faaliyetlerini desteklemiştir (EU COM576, 2005:2; EU COUNCIL DIRECTIVE/114/EC, 2008; Karanacak, 2011; AFAD, 2014a: 17).

**2. BM AÇISINDAN KRİTİK ALTYAPILAR**

Birleşmiş Milletler (BM) Güvenlik Konseyi, 2001 yılından itibaren kritik altyapılara ilişkin uygulamaları ve kırılganlıkları belirlemek, terör saldırılarına karşı korumak maksadıyla ülkeleri önlemler almaya çağırmıştır (UN Security Council, 2001). 2004 yılında da, bu tür saldırılara hızlı yanıt vermenin önemini vurgulamıştır (UN Security Council, 2004). Güvenlik Konseyi Terörle Mücadele Komitesi ise 2014 yılında *“Turizmde Kritik Altyapının Korunması”* ve 2015 yılında *“Terörist Olaylar Sonrası Acil Müdahalenin Güçlendirilmesi”* konularında iki toplantı düzenlemiştir. 2016 yılında Güvenlik Konseyi tarafından üye devletlerin sorumluluklarına ilişkin görüşlerin sunulduğu ve Ukrayna heyeti tarafından başlatılan *“Terörist Saldırılara Karşı Kritik Altyapının Korunması”* konulu bir toplantı icra edilmiştir. *“Hassas Hedefler, İnternet ve Turizm Güvenliğinde Kritik Altyapının Korunması”* konulu bir Çalışma Grubu da oluşturulmuştur. Güvenlik Konseyi 2017 yılında kritik altyapılara olabilecek terör saldırılarına karşı kırılganlık ve yeteneklerin değerlendirmelerini isteyen bir karar yayınlamış, Terörle Mücadele Komitesi tarafından *“Terörist Saldırılara Karşı Fiziki Altyapıların Korunması”* adıyla bir rapor hazırlanmıştır (2341, 2017; UN CTED, 2017: 1). 2018 yılında ise *“Terörist Saldırılara Karşı Kritik Altyapının Korunması: İyi Uygulamaların İncelemesi”* adıyla ülkeler tarafından kritik altyapıların korunmasına katkı yapan uygulamalar dile getirilmiştir (UN CTED & UNOCT, 2018: 6).

**3. ABD AÇISINDAN KRİTİK ALTYAPILAR**

 Kritik altyapı kavramı, ABD Başkanlığı tarafından 1996 yılında konuya ilişkin komisyon oluşturulmasına ilişkin kararnamesinden bir yıl sonra *“Kritik Altyapıların Korunması Hakkında Raporu”*nda ayrıntılı olarak açıklanmıştır. Bu raporda tanımlamalar ve durum tespitleri yapılmış, alınması gereken önlemler sıralanmıştır. Raporda toplumda yaşam destek sistemleri ve refahın teminatı olarak görülen bu yapıların incelenmesine, kırılganlıklarının tespitine ve gelecekte de korunması için strateji önerilerinin oluşturulmasına yer verilmiştir (US PCCIP, 1997). Bu raporu müteakip 1998 yılında *“Başkanlık Karar Direktifi”* yayınlanmış; direktif, ABD’de kritik altyapıları işleten sektörlere ve güvenlikle ilgili çalışan tüm kamu kurumlarına gönderilmiştir. Direktifte, kritik altyapıların toplum refahı ve ülkenin ulusal güvenliği açısından önemi tekrar vurgulanarak ulusal hedefler, kritik altyapıların listesi, kurumların gerçekleştirmesi gereken adımlar, koordinasyon ile ilgili hususlar, yeni yapılanmalar ve ulusal koordinatör birimleri tanımlanmıştır (US PDD, 1998; Karanacak, 2011). ABD günümüzde kritik altyapıları; kimya sektörü, ticari alanların korunması, iletişim, kritik üretim tesisleri, barajlar, savunma sanayi ve üretim alanları, finansal hizmetler, acil servis hizmetleri, enerji, gıda ve tarım, halk sağlığı ve bakımı, bilgi teknolojileri, nükleer reaktör-malzeme ve atıkları, kamu binaları ve alanları, ulaşım sistemleri, su ve atık su sistemleri olarak tanımlamıştır (DHS, 2019).

**4. KRİTİK ALTYAPILARIN KORUNMASI**

 Kritik altyapıların korunması, özellikle 11 Eylül 2001 yılında ABD’de gerçekleşen terör saldırıları sonrasında ülkelerin üzerinde daha yoğun bir şekilde düşündüğü, önemine ilişkin farkındalığın her geçen gün arttığı bir kavram olmuştur (AFAD, 2014a: 12). Bu süreçte kritik altyapıların korunmasının hem ulusal hem de iç güvenlik açısından elzem olduğunun anlaşıldığı, bu kapsamda ülkelerin iç güvenlik stratejileri içerisinde buna yer ayırdığı görülmektedir (US PDD, 1998; European Commission, 2014:7 EU COUNCIL, 2015, 7; EU COUNCIL, 2016: 25/42). Ülkelerin altyapılara yönelik terör eylemleri veya doğal afet gibi çeşitli müdahalelerden korunması, altyapıların çalışmaması durumunda da acil müdahale edilerek işler hale getirilme esaslarını içeren stratejilerin oluşturulmasının önemi açıktır. Kuşkusuz önceki yıllarda da altyapıların önemi biliniyor, korunmaları için asgari standartlar geliştiriliyordu.[[3]](#footnote-3) Ulaşım, iletişim, enerji, iş sağlığı ve güvenliği ile halk sağlığı sektörlerinin işlemesi için öngörülen düzenlemeler buna örnek tedbirler içerisindedir. Ancak kritik altyapılara ilişkin tanımlamalar ve planlamaların geliştirilmesi, bu tesislere karşı tedbirlerin daha fazla iyileşmesine katkı sağlamıştır (EU COM702(F1), 2004: 3-4). Devletlerin, iç güvenliğinin sağlanması ile kritik altyapıların korunması arasında üç husus ilişkilendirilebilir.

 - İlki; kritik altyapıların işleyişini bozacak fiziki ve siber tehditlere yönelik güvenliğin sağlanması faaliyetidir.

 - İkincisi; kritik altyapılarda sistemin kendisinden veya doğal afetlerden kaynaklanan bozulma, çalışmama gibi durumlarda ortaya çıkabilecek çevresel, toplumsal, ekonomik ve siyasal etkilerine karşı hazırlıklı olmak, bu maksatla koordinasyon ve iş güvenliği plan ve eylemlerinin oluşturulmasıdır.

 - Üçüncüsü; kritik altyapıların güvenliğini ve işlerliğini sağlamada yer alan kolluk kuvvetleri, itfaiye, arama kurtarma ve tıbbi birimlerin de bir kritik altyapı hizmeti olarak değerlendirilmesidir. Kritik altyapılara müdahale edecek bu birimlerin varlığı ve işlevinin devamını sağlayacak tedbirler alınmalıdır (US PCCIP, 1997:B-1).

 İç güvenlik birimlerinin kritik altyapıların korunmasına ilişkin olarak belirleyeceği yöntem şu şekilde açıklanabilir.

 **(ı) Kritik altyapılarda tehdidin tespiti:** Kritik altyapıların korunması bir tehdidin varlığının kabul edilmesiyle başlar. Bu tehditler genel olarak fiziksel nitelikte olup bunlar günümüzde uzun menzilli silahlar, terörist saldırılar ve siber müdahaleler şeklinde sıralanır. Geçmiş yıllarda işletme, tesis ve fabrika sahipleri çoğunlukla kendilerini tesis dışından gelebilecek herhangi bir düşman bombardımanı veya füze saldırısı tehdidi altında görmüyordu. Benzer tehditler ortaya çıkması durumunda ise devletin ulusal güvenlik birimlerinin bu tür tehlikeleri ülkeye ulaşmadan sonlandırabileceği görüşü hâkimdi. Ancak günümüzde tehditlerin terörizm ve internet yoluyla yapılan saldırılar başta olmak üzere çeşitlenmesi, bu saldırıların altyapıların kendisinden başlayarak devletlerin ulusal güvenlik düzeyindeki birimlerine kadar ulaşabilmesi, tehditlerin kaynaklarının ise bireyden başlayarak bir örgüt veya ülkeye kadar uzanabilmesi iç güvenliğin kritik altyapılar bağlamında önemini göstermiştir (US PCCIP, 1997: 3-20). Bu bağlamda kritik altyapıların korunmasının amacı, dışarıdan bir müdahaleyle gerçekleşen fiziksel ve internet yoluyla oluşan saldırıların önlenmesidir. Bu kapsamda internet saldırılarını örnek vermek gerekirse, örneğin barajlar, enerji üretim ve nakil tesislerine sahiptir ve bilgi teknolojileri tarafından kontrol edilerek izlenmektedir. Telekomünikasyon gibi kritik altyapılar ise bizatihi bilgi ve iletişim teknolojilerinin kendisidir. İnternet yoluyla yapılan bir saldırı; (ı) barajlarda olduğu gibi kritik altyapıları destekleyen bilgi ve iletişim teknolojilerine veya (ıı) kritik altyapı olarak tanımlanan telekomünikasyon, ekonomi, finans gibi devlet fonksiyonlarını yerine getiren bilgi ve iletişim teknolojilerinin kendisine yönelik olabilmektedir (Karanacak, 2011).

 **(ıı) Kritik altyapılarda önem boyutunun derecelendirilmesi:** Bir altyapının kritikliği, kaybında ya da kullanılamaması durumunda etkilediği insanlar ve bölgesel alanın genişliğiyle ölçülebilir. Kritikliğin önemi; (ı) Etkilenen nüfusun miktarı ile yaşam kaybı, tıbbi hastalık, ciddi yaralanma, tahliye bağlamında halka etkisi. (ıı) Ekonomik açıdan Gayri Safi Yurt İçi Hâsıla (GSYİH)’ya etkisi, ekonomik kaybın önemi. (ııı) Çevresel etkisi. (ıv) Coğrafi faktörlere göre konumu. (v) Diğer kritik altyapı unsurları arasında karşılıklı bağımlılığı ve ilişkisi. (vı) Devletin kapasitesi ve kabiliyetine yönelik politik etkisidir. (vıı) Altyapıların (hemen veya 24-48 saat, bir hafta gibi) belirlenen bir zaman içerisinde çalışır duruma gelmesi altyapının önem derecesini belirler (EU COM702(F1), 2004: 5). Ayrıca, kritik altyapının önemi ve durumunun zamana, teknolojiye ve cazibesine göre dönemsel olarak değişebileceği unutulmamalıdır (US PCCIP, 1997: 21-23).

 **(ııı) Kritik altyapılarda koruma tedbirlerinin alınması:** Altyapıların korunmasına ilişkin çalışmalar, öngörülen riskleri tanımlamak, ölçmek, kontrol etmek ve kabul edilebilir bir değere uygun olarak belirli bir seviyeye azaltmak için yapılan güvenliğin yönetilmesidir. Herhangi bir tehdit, risk ya da zayıf noktaların tespit edilmesi, hafifletilmesi veya bertaraf edilmesidir. Bu sayede koruma tedbiri kritik altyapıların işlevselliğinin, sürekliliğinin ve bütünlüğünün devamını sağlamayı amaçlayan tüm faaliyetleri kapsar (EU COM702(F1), 2004: 5). Burada unutulmaması gereken tespit edilen tüm kritik altyapıların eşit olarak ve riskleri tamamen ortadan kaldırabilecek bir tedbirin imkânsızlığının bilinmesi, bunun yerine risk düzeylerine uygun olarak etkin ve verimli tedbirlerin alınmasıdır.

 Kritik altyapıların korunma yöntemi, iç güvenlik açısından hem dışarıdan tehditlerin ve müdahalelerin engellenmesi, hem de uygun ve doğru çalışması için uygulanacak iş güvenliği tedbirlerinin koordinasyonunu kapsar. Bu yaklaşım dışarıdan tehditlere maruz kalınmasını önlediği gibi, diğer taraftan altyapının iş güvenliğine uygun çalıştırılmaması veya afetler gibi nedenler neticesinde iş göremez duruma geldiğinde çevre ve insanlara olumsuz ekonomik, çevresel, siyasal etki yapmaması açısından da önemlidir. Ayrıca, kritik altyapıların korunmasında gelişen teknoloji ve farklılaşan ihtiyaçlarla birlikte yeni zorlukların yeni koruma usulleri gerektirdiği de bilinmelidir (US PCCIP, 1997: 21-23).

 **(ııı) Kritik altyapıların korunmasına ilişkin işbirliği:** Kritik altyapıların korunması çoklu aktörleri içermektedir. Altyapıların sahipliği ülkenin ideolojilerine ve tercihine göre değişebilmekle birlikte ya kamu ya da özel sektördür. Ancak genellikle bu aktörlere uluslararası özel şirketler hatta diğer devletlerde katılabilir. Korunmasında tesisin sahipleri, operatörleri, devlet yetkilileri arasında tutarlı ve işbirliğine dayalı bir ortaklık gerekmektedir. Tesislerde, tedarik zincirlerinde, bilgi teknolojilerinde ve iletişim ağlarında riski yönetme sorumluluğu öncelikle tesislerin sahiplerine ve operatörlerine aittir. Ancak, altyapının sahipleri, operatörleri, meslek örgütlenmeleri, sanayi birlikleri ve devlet bu sürece aktif katılmalıdır. Altyapının güvenliğine ilişkin katkılar ve istihbarat bilgileri, kolluk kuvvetleri ve diğer yetkili birimler tarafından sağlanmalıdır. Kamu ve özel sektör paydaşları, terör saldırıları ve benzer risklere karşı altyapı sistemlerini koruma veya acil müdahalede bulunmada yardımcı olmak için uyarılar, tavsiyeler ve bilgilendirmeler yapmalıdır. En iyi güvenlik yönetimi planları ve uygulanması zorunlu olan kanunların bile gereken zamanda uygulanmadığında değersizleşebileceği bilinmelidir. Tecrübelerden yararlanmak, bağımsız denetimlerin icrası güvenlik gereksinimlerinin doğru uygulanmasını sağlamaya katkı sağlayacaktır (EU COM702(F1), 2004: 4-8).

**5. TÜRKİYE BAĞLAMINDA KRİTİK ALTYAPILARIN KORUNMASI**

 Türkiye’nin her geçen gün teknolojik kapasitesi artmaktadır. Yaşanan mekânlar ve işgücü, daha kapsamlı ekonomik ve teknolojik altyapıları ve ihtiyaçları ortaya çıkarmaktadır. Hatta Türkiye gibi jeopolitik önemi olan ülkelerde, barajlar, petrol-doğalgaz boru hatları gibi kritik altyapıların maruz kalabileceği tehditler ve ortaya çıkabilecek afetler sadece Türkiye değil çevre ülkeleri de olumsuz etkileyebilir (AFAD, 2014a: 12). Şimdilik, Türkiye’de ABD ve AB örneğinde olduğu gibi iç güvenlik açısından kritik altyapıların korunmasına ilişkin bütünsel bir yaklaşım hâkim olmamakla ve bir strateji belgesi henüz hazırlanmamakla birlikte, devlet teşkilatlanması içerisinde bakanlıkların kendi görev alanları içerisinde hali hazırda bu faaliyetlerin yürütüldüğü görülmektedir. Nitekim;

 (ı) Kritik alt yapıların fiziki korunması hususunda, kolluk kuvvetleri tarafından 1981 yılı ve 2565 sayılı *“Askeri Yasak Bölgeler ve Güvenlik Bölgeleri Kanunu”* kapsamında yurt savunması, toplum hayatı ve ekonomisine yönelik olumsuz sonuçlar doğurabilecek yer ve tesisler için güvenlik bölgeleri oluşturularak güvenlikleri sağlanmaktadır. Türkiye’de kurulacak iki adet nükleer santral ile İstanbul Havaalanının denizden güvenliği dâhil olmak üzere doğu bölgelerinde bulunan barajlar özel koruma tedbirleri kapsamında, diğer kritik baraj ve hidroelektrik santralleri gibi tesisler emniyet ve asayiş hizmetleri çerçevesinde korunmaktadır.

 (ıı) İnternet güvenliğine ilişkin olarak ise; 2008 yılı Elektronik Haberleşme Kanunu ve 20/10/2012 tarihli 28447 sayılı Resmi Gazetede yayınlanan *“Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı”* kapsamında faaliyetler yürütülmektedir. Ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarının hazırlanması ve koordinasyonu için Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Bilgi Teknolojileri ve İletişim Kurumu yetkilendirilmiş, internet güvenlik faaliyetleri bu kurum tarafından oluşturulmuştur.

 (ııı) Kritik altyapılarda afet risklerine karşı korunma ile yaşanabilecek afetlerin ve acil durumların yönetiminde 2009 yılında kurulan Afet ve Acil Durum Yönetimi Başkanlığı yetkili ve koordinatör kılınmıştır.

 Türkiye’de kritik altyapıların korunmasına ilişkin süreç, 1999 yılında AB’ye aday ülke olma sürecinde başlatılan ve tam üyelik müzakerelerinde uyum mevzuatı kapsamında çevre başlığı altında yürütülen çalışmalarla başlamıştır. Kritik altyapıların korunması, teknolojik afetler başlığı altında ele alınmış, teknolojik afetlerinde doğal afetlerin tetiklenmesi sonucunda veya insan kaynaklı bir kaza, terör veya sabotajdan kaynaklanabilecek durumlar karşısında olabileceği değerlendirilmiştir. Kritik altyapıların korunmasının güvenlik boyutu da bulunmasına rağmen literatür Türkiye’de daha çok afet ve acil durum yönetimi ile özdeşlemiş, bu işlemler için AFAD sorumlu kılınmıştır.[[4]](#footnote-4) AFAD’ın Cumhurbaşkanlığı Hükümet Sistemi ile ilgili yapılan düzenlemeler kapsamında 2018 yılında İçişleri Bakanlığına bağlanması kritik altyapıların iç güvenlik bağlamında koordine görevinin daha da artırılmasına vesile olacağı açıktır.[[5]](#footnote-5) AFAD, devlet teşkilatlanması içerisinde bir şemsiye kuruluş olarak afet ve acil durumun niteliği ve büyüklüğüne göre Milli Savunma Bakanlığı, Dışişleri, Sağlık, Ulaştırma ve Altyapı gibi diğer bakanlıklar ve sivil toplum kuruluşlarıyla işbirliği içerisinde faaliyetlerini yürütmektedir. Ayrıca, AFAD bünyesinde öneri ve politikaların belirlenmesi için Afet ve Acil Durum Danışma Kurulu oluşturulmuştur.[[6]](#footnote-6) AFAD’ın kuruluşuna ilişkin 5902 sayılı kanun kapsamında; (ı) Doğal, teknolojik ve insan kaynaklı afetler ile acil durumlara ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması. (ıı) Olayların meydana gelmesinden önce hazırlıkların yapılması ve zararların azaltılması. (ııı) Olay sırasında yapılacak müdahale ve olay sonrasında gerçekleştirilecek iyileştirme çalışmalarını yürütmekten sorumlu kılınmıştır. Ayrıca, kurum ve kuruluşlar arasında koordinasyonun sağlanmasından ve bu konularda politikaların üretilmesinden ve uygulanmasından da yetkilidir[[7]](#footnote-7) (AFAD, 2014a: 12-20; AFAD, 2019).

 AFAD’ın kuruluş amacı Türkiye’de karşılaşılan her türlü doğal, insani ve teknolojik felakete karşı *“Bütünleşik Afet Yönetimi”* anlayışına geçilmesi açısından önemli olmuştur. Önceden devlet tarafından öngörülen *“Kriz Yönetimi”* yaklaşımı bütünsel bir yaklaşımla *“Risk Yönetimi”*ne evrilmiştir. *“Bütünleşik Afet Yönetimi Sistemi”* olarak adlandırılan bu model; (ı) Afet ve acil durumların sebep olduğu zararların önlenmesi maksadıyla tehlike ve risklerin önceden tespiti. (ıı) Afet olmadan önce meydana gelebilecek zararların önlenmesi veya en aza indirecek tedbirlerin alınması. (ııı) Etkin müdahale ve koordinasyonun sağlanması ve afet sonrasında iyileştirme çalışmalarının bir bütünlük içerisinde yürütülmesine katkı sağlamayı öngörmektedir (AFAD, 2014: 20). AFAD, Türkiye’de kritik altyapıların afetlerden korunması maksadıyla 2014 yılında bir yol haritası yayınlanmıştır. Bu belgenin amacı, kritik altyapılara ilişkin hizmetlerin yürütülmesinde ulusal mevzuat, uluslararası sözleşmeler ve AB mevzuatı ile farklı ülkelerdeki koordinasyon ve uygulamaların dikkate alınması, kısa ve uzun vadeli hedeflerin belirlenmesi ve uygulanması için eylem planlarının hazırlanmasıdır (AFAD, 2014a: 12). AFAD’ın kritik altyapılara ilişkin yol haritası belgesi yayınlaması ve diğer bakanlık ve kurumlarla ilgili işbirliği alanlarını belirlemesinin önemi açıktır.

 İnternet güvenliği ile ilgili olarak mevzuat açısından ise, 2008 yılı 5809 sayılı Elektronik ve Haberleşme Kanunu’na eklenen Ek 1.madde ile *“Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir”* denilmektedir. Söz konusu Kanun ile işaret edilen 2012 yılı 3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu kararı gereğince Siber Güvenlik Kurulu oluşturulmuştur.[[8]](#footnote-8) Siber Güvenlik Kurulu, ilk toplantısında *“Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı”* hazırlamış, bu belge 20 Haziran 2013 tarihinde *“Bakanlar Kurulu Kararı”* olarak yayımlanmıştır. Bu belgede kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına karar verilmiştir. Bu kapsamda, Söz konusu eylem planı bünyesinde *Ulusal Siber Olaylara Müdahale Merkezi (USOM)* kurulmuş, *Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri (SOME)* oluşturulmuştur (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2013: 18-19). Kurumsal SOME’ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri almak veya aldırılması için yönlendirmek, karşı müdahale için mekanizma geliştirmek, kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmalar yapmakla yükümlü kılınmıştır. Kurumsal SOME’ler, siber saldırıların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunmaktadır (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, 2014: 6-10; BTK, 2019).

**SONUÇ**

 Kritik altyapılar, toplumsal hayat için refahın temeli, beşeri varlığın devamı için ulusal güvenliğin teminatı ve gelecek kuşaklar için üzerinde yaşayacağı kültürel ve ekonomik mirastır. Bu nedenle kritik altyapıların güvenliği ve devamlılığının sağlanması için bütünsel bir bakış açısı gereklilik değil zorunluluk olarak görülmelidir.

 Dünyada iç güvenlik bağlamında kritik altyapılarla ilgili olarak, afet yardım ve acil yönetim ihtiyaçlarından ayrı olarak dışarından terör olayları ve internet yoluyla müdahalelere de odaklanıldığı görülmektedir. Kritik altyapıların hem dışarıdan gelecek terör ve internet ortamlı tehditlere hem de afet ve acil yönetim bağlamında risk odaklı değerlendirmelere hazırlıklı olması kuşkusuz zor bir iştir. Görevi sürekli temel ürün ve hizmet akışını üretmek ve dağıtmak olan çoğunlukla özel sektöre ait sistem ve süreçlere sahip ağ yapılarının sürdürülebilirliği için işbirliğine gerek duyulmalıdır. Altyapıların devlet yanında mülkiyeti veya işletmesi özel şahıslara da ait olabileceğinden bu işbirliği kamu ve özel sektörün ortak bir sorumluluğudur. Ayrıca, kritik altyapı güvenliğinin yalnızca ulusal bir konu olmadığından uluslararası işbirliğinin gerekliliği ve önemi de bilinmelidir. İç güvenlik yönetimi açısından belirlenecek temel stratejiler içerisinde;

 - İçişleri Bakanlığı tarafından ülkedeki kritik altyapıların fiziki korunmasına karşı ulusal bir stratejinin belirlenmesi ve yönetimi,

 - İçişleri Bakanlığının bağlı birimi olan AFAD tarafından kritik altyapıların tespiti ve afetlerde müdahalelere ilişkin gerekli önlemlerin alınması,[[9]](#footnote-9)

 - İçişleri Bakanlığı, Sağlık Bakanlığı ve yerel yönetimlerin sorumluluğundan bulunan kolluk, ilk yardım, itfaiye teşkilatlarının icra ettiği görevlerin niteliği dikkate alınarak bunların da bir kritik altyapı hizmet birimleri olarak değerlendirilmesi ve buna yönelik korunmalarına ilişkin planlamaların ve önlemlerin geliştirilmesi gerekmektedir.

 Türkiye’de iç güvenlik açısından kritik altyapıların korunmasına ilişkin bütünsel bir yaklaşım ve bir strateji belgesi henüz hazırlanmamıştır. Hali hazırda ise kritik altyapıların korunmasına ilişkin işlemler, devlet teşkilatlanması bünyesinde farklı bakanlıklarda yürütülmektedir. Bunun nedenlerine bakıldığında kritik altyapı konusunun AB uyum süreci bağlamında afet kaynaklı insani ve çevresel etkinin azaltılması olarak anlaşıldığı görülmektedir. Bu yaklaşımın altyapıların sürdürülebilirliği ve işlerliğini sağlayan iş güvenliği ve afetlere hazırlık çalışmaları açısından önemi açıktır. Ancak bu çalışmalara ilave olarak terör eylemleri ve internet müdahaleleri gibi farklı boyutta tehditlerin de ilave edildiği bütünsel bir yaklaşımla oluşturulmuş bir iç güvenlik stratejisine ulaşılmasının daha faydalı olacağı değerlendirilmektedir.

**KAYNAKÇA**

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

AFAD (2014b). *Açıklamalı Afet Yönetimi Terimleri Sözlüğü*. Ankara: Başbakanlık Afet Acil Durum Yönetimi Başkanlığı.

AFAD (2019). 15.02.2019 tarihinde https://www.afad.gov.tr/tr/2211/AFAD-Hakkinda ve https:// www.afad.gov.tr/tr/2505/Afet-ve-Acil-Durum-Danisma -Kurulu adresinden alınmıştır.

Ak, T. (2018). *Dünyada İç güvenlik Yaklaşımının Değişimi ve İç Güvenlik Yönetimine Etkisi*. Van Yüzüncü Yıl Üniversitesi İİBF Dergisi,(6), 74-93.

BBC (2017). 15.02.2019 tarihinde https://www.bbc.com/turkce/haberler-dunya-39354709 adresinden alınmıştır.

BTK (2019). *USOM ve Kurumsal Siber Olaylara Müdahale Ekibi*, Bilgi Teknolojileri ve İletişim Kurumu.25.02.2019 tarihinde https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi adresinden alınmıştır.

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

DHS (2019). *Critical Infrastructure Sectors*. 15.02.2019 tarihinde https://www.dhs.gov/cisa/critical-infrastructure-sectors adresinden alınmıştır.

EU COM702(F1) (2004). *Critical Infrastructure Protection in the Fight Against Terrorism*, Brussels: Communication from the Commission to the Council and the European Parliament. 14.02.2019 tarihinde http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1 &year=2004&number=702&language=EN adresinden alınmıştır.

EU COM576 (2005). *Green Paper on a European Programme for Crtıcıcal Infrasturacture Protection*, Brussels: Commission of the European Communities, 14.02.2019 tarihinde http://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-576-EN-F1-1.Pdf adresinden alınmıştır.

EU COUNCIL DIRECTIVE/114/EC (2008). *On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*, 15.02.2019 tarihinde https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008: 345:0075:0082:EN:PDF adresinden alınmıştır.

EU COUNCIL (2015). *Draft Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020*, 9798/15. 10 June 2015.

EU COUNCIL (2016). *Renewed European Union Internal Security Strategy Implementation*, Brussels, 8587/16. 13 May 2016.

EUROPEAN COMMISSION (2014). *Communication from the Commisison to the European Parliament and the Council, The final implementation report of the EU Internal Security Strategy 2010-2014*,20.6.2014, COM(2014) 365 final, Brussels.

Karanacak, B. (2011). *Kritik Altyapılar ve Kritik Altyapıların Korunması*, Siber Savunma Sempozyumu, 24-25 Mayıs 2011, İstanbul.

SABAH (2004). 1502.2019 tarihinde http://arsiv.sabah.com.tr/2004/03/12/gnd101.html adresinden alınmıştır.

UN Security Council (2001). *Resolution 1373 (2001)*,28 September 2001.

UN Security Council (2001). *Resolution 1566 (2004)*, 8 October 2004.

UN CTED (2017). *Protection of Critical Infrastructure against Terrorist Attacks*, UN Security Council Counter Terrorism Committee Executive Directorate Trends Report.

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, 25.02.2019 tarihinde https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü (2014). *Kurumsal SOME Kurulum ve Yönetim Rehberi*. Ankara: T.C. Ulaştırma. Denizcilik ve Haberleşme Bakanlığı.

Tüney, S. & Gücüyener, A. (2015). *Kritik Altyapı Güvenliği, Teknolojik Afetler ve Türkiye’nin 2023 Stratejisi*, Kritik Altyapıları Koruma Programı, 21.02.2019 tarihinde https://www. afad.gov.tr/tr/2629/Makaleler adresinden alınmıştır.

UN CTED & UNOCT (2018). *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Counter Terrorism Committee Executive Directorate & United Nation Office of Counter Terrorism.

US PCCIP (1997). *Critical Foundations Protecting America’s Infrastructures*.The Report of the President’s Commission on Critical Infrastructure Protection President’s Commission on Critical Infrastructure Protection, Washington, DC: White House.

US PDD (1998). *Critical Infrastructure Protection*, Residential Decision Directive/NSC-63, May 22, 1998, Washington: The White House, 13.02.2019 tarihinde [https://fas.org/irp/offdocs/ pdd/pdd63.htm](https://fas.org/irp/offdocs/%20pdd/pdd63.htm) adresinden alınmıştır.

4 sayılı Cumhurbaşkanlığı Kararnamesi (2018). *Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar İle Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi*, 15/7/2018 tarihli ve 30479 sayılı kararname, 25.02.2019 tarihinde http:// www.mevzuat.gov.tr/MevzuatMetin/19.5.4.pdf adresinden alınmıştır.

1. \* Dr., Jandarma ve Sahil Güvenlik Akademisi, Güvenlik Bilimleri Enstitüsü, aktrkak@gmail.com [↑](#footnote-ref-1)
2. 11 Mart 2004 tarihinde İspanya'nın başkenti Madrid'de banliyö tren ağında insanları hedef alan terör saldırısıdır. Saldırılar sonucunda 192 kişi ölmüş, 2050 kişi yaralanmıştır. 2005 yılının temmuz ayında Londra’da şehrin ulaşım sistemine de teröristler tarafından insanları hedef alan patlamalar gerçekleştirilmiş, otobüs durağı, metro istasyonu gibi alanlarda 52 kişi ölmüştür (SABAH, 2004; BBC 2017). [↑](#footnote-ref-2)
3. AB bünyesinde, nükleer malzemelerin uygun kullanımını kontrol etmek için EURATOM Antlaşması çerçevesinde yapılan denetimler, havacılık ve denizcilik sektörlerini içeren uluslararası taşımacılık mevzuatları altyapıların korunmasına ilişkin örnekler arasında sayılabilir (EU COM702(F1), 2004: 7). [↑](#footnote-ref-3)
4. AFAD’ın kuruluş seyri şu şekilde gerçekleşmiştir. Önceleri İçişleri Bakanlığı’na bağlı Sivil Savunma Genel Müdürlüğü, Bayındırlık ve İskân Bakanlığı’na bağlı Afet İşleri Genel Müdürlüğü ve Başbakanlık’a bağlı Türkiye Acil Durum Yönetimi Genel Müdürlüğü’nün kapatılarak 2009 yılında 5902 sayılı kanun ile Başbakanlık’a bağlı koordinatör kuruluş olarak oluşturulmuştur. Farklı bakanlıklardaki yetki ve sorumlulukların tek bir çatı altında toplanması ile oluşan AFAD, Cumhurbaşkanlığı Hükümet Sistemi ile ilgili yapılan düzenlemeler kapsamında 15 Temmuz 2018 tarihinde yayınlanan 4 numaralı Cumhurbaşkanlığı Kararnamesi ile İçişleri Bakanlığına bağlanmıştır (AFAD, 2019). [↑](#footnote-ref-4)
5. AFAD, hali hazırda illerde doğrudan valiye bağlı İl Afet ve Acil Durum Müdürlükleri ve 11 ilde bulunan Afet ve Acil Durum Arama ve Kurtarma Birlik Müdürlükleri vasıtasıyla çalışmalarını yürütmektedir (AFAD, 2019). [↑](#footnote-ref-5)
6. Afet ve Acil Durum Danışma Kurulu; Dışişleri Bakanlığı, İçişleri Bakanlığı, Boğaziçi Üniversitesi Kandilli Rasathanesi ve Deprem Araştırma Enstitüsü, Maden Tetkik ve Arama Genel Müdürlüğü, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Türkiye Kızılay Derneği temsilcileri, Yükseköğretim Kurulu tarafından bildirilen en az on üniversite öğretim üyesi ve sivil toplum kuruluşları üyelerinden oluşmaktadır (AFAD, 2019). [↑](#footnote-ref-6)
7. 15.07.2018 tarihli 4 sayılı “Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar İle Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi”nde 51.madde “Koordinasyon ve İşbirliği” bölümünde “(1) Başkanlık, görevleriyle ilgili konularda kamu kurum ve kuruluşları, üniversiteler, yerel yönetimler, Türkiye Kızılay Derneği ve konu ile ilgili diğer sivil toplum kuruluşları, özel sektör ve uluslararası kuruluşlar ile işbirliği ve koordinasyonu sağlamakla yetkilidir. (2) Çeşitli kamu kurum ve kuruluşları tarafından üretilen ve afet ve acil durum yönetiminin her safhasında kullanılabilecek sayısal ve sayısal olmayan her türlü veri ve envanter bilgisi Başkanlıkla bedelsiz olarak paylaşılır. Verinin gerektirdiği önem derecesine uygun olarak bilgi güvenliğinin gerekleri yerine getirilir.” hususuna yer verilmiştir. [↑](#footnote-ref-7)
8. Siber Güvenlik Kurulu, 2012 yılı itibariyle Ulaştırma, Denizcilik ve Haberleşme Bakanı’nın başkanlığında, Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır (BTK, 2019). [↑](#footnote-ref-8)
9. Buna internet üzerinden tehdit ve müdahalelere maruz kalan enerji üretim ve dağıtım sistemleri, su ve kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesini sağlayan SCADA (Supervisory Control And Data Acquisition/ Denetimsel Kontrol ve Veri Toplama) sistemleri ve teknolojileri de dâhildir. [↑](#footnote-ref-9)