



T.C.
BAŞBAKANLIK
Afet ve Acil Durum Yönetimi Başkanlığı



2014-2023

Kritik Altyapıların Korunması Yol Haritası Belgesi

Bu belge, **Planlama ve Zarar Azaltma Dairesi Başkanlığı**
Teknolojik Afetler Risk Azaltma Çalışma Grubu tarafından,
AB mevzuatı ve uluslararası belgeler incelenerek, ilgili kurum ve kuruluşların destek ve çalışmalarıyla hazırlanmıştır.
Raporun kendisi resmi bir AB belgesi değildir ve AB politikasını temsil etmemektedir.

Eylül, 2014



KISALTMALAR

AB:	Avrupa Birliđi
ABD:	Amerika Birleşik Devletleri
AFAD:	Afet ve Acil Durum Yönetimi Başkanlığı
AKA:	Avrupa Kritik Altyapılar (European Critical Infrastructures) (ECI)
ERNICIP:	Kritik Altyapıların Korunması İçin Avrupa Birliđi Referans Ađı (European Reference Network for CIP)
EM-DAT:	Uluslararası Afet Veritabanı (The International Disaster Database)
İGP:	İşletmecisi Güvenlik Planı (Operator Security Plan) (OSP)
KAKAP:	Kritik Altyapıların Korunması İçin Avrupa Programı (European Programme for Critical Infrastructure Protection) (EPCIP)
KAS:	Kritik Altyapı Sektörleri
KAUBA:	Kritik Altyapı Uyarı Bilgi Ađı (Critical Infrastructure Warning Information Network) (CIWIN)
KOMİSYON:	Avrupa Birliđi Komisyonu
KONSEY:	Avrupa Birliđi Konseyi
PARLEMENTO:	Avrupa Birliđi Parlamento
UKA:	Ulusal Kritik Altyapı (National Critical Infrastructure) (NCI)





TANIMLAR

Kritik Altyapı:	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.
Avrupa Kritik Altyapıları (AKA):	Bozulması ya da yıkılması neticesinde en az iki üye devleti etkileyebilecek kritik altyapılardır.
Risk Analizi:	Kritik altyapının bozulmasının ya da yıkımının olası etkileri ile zayıf noktalarını değerlendirebilmek için ilgili tehdit senaryolarının göz önünde bulundurulmasıdır.
Koruma:	Herhangi bir tehdit, risk ya da zayıf noktanın tespit edilmesi, hafifletilmesi ve nötralize edilmesi için, kritik altyapıların işlevselliğini, sürekliliğini ve bütünlüğünü sağlamayı amaçlayan tüm faaliyetler anlamına gelmektedir.
AKA Sahipleri/ İşletmecileri:	AKA olarak belirlenmiş belirli bir varlık, sistem ya da ilgili her türlü öğenin günlük işletimi ile bunlara yapılacak yatırımlardan sorumlu olan kişi ya da işletmeler anlamına gelmektedir.
Güvenlik İrtibat Görevlisi :	Kritik altyapı sahibi/işletmecisi ile devlet otoritesi arasında güvenlikle ilgili konularda irtibat noktası görevi görecek kişidir.
Kritik Altyapı Koruma Avrupa Programı (KAKAP):	2004 yılında çıkarılan Tebliğ'e istinaden 2006 yılında ortaya konulan, net olarak Avrupa'da "Kritik Altyapı" kavramını tanımlayan, 11 adet Kritik Altyapı Sektörünü belirleyen ve öncelikli olarak "Ulaştırma ve Enerji Sektörleri" üzerine yoğunlaşılması gerektiği ifade edilen programdır.
Kritik Altyapı Uyarı Bilgi Ağı (KAUBA):	Kritik altyapıların korunması konusunda bilgi alışverişini sağlayan bir forum olup, üye ülkelere ve Komisyona kritik altyapılara yönelik anlık riskler ve tehditler üzerine uyarılar yollama imkânı sağlayan ağıdır.
İşletmeci Güvenlik Planı :	İşletme içerisinde bulunan önemli varlıkların tanımları, risk analizi, alınacak tedbirleri ve prosedürleri, önceliklendirme değerlerini kapsayan plandır.



BAKAN SUNUŞU

Prof.Dr. Numan KURTULMUŞ
Başbakan Yardımcısı



İnsanoğlu tarih öncesi zamanlarda, doğa ve işleyişi hakkında çok az bilgiye sahipti. Doğayı kendi imkânları ile bir ölçüde kontrol etmeye çalıştı. Deprem, fırtına, heyelan gibi doğal afetler insanın mantıksal anlama ötesinde bir olguydu. Zaman geçtikçe zihinsel olarak gelişen insan doğal afetleri tanımayı, ondan korunmayı ve afetin zararlarını azaltmayı öğrendi. Böylece teknolojiyi üreten insan kendisinin neden olduğu insan kaynaklı ve teknolojik afet kavramını ortaya çıkardı.

Son 50 yılda dünya üzerinde 2 milyon kişi doğal ve insan kaynaklı afetlerle hayatını kaybetmiştir. Dünyada olduğu gibi ülkemizde de doğal afetlerin sıklıkla yaşandığı bir ülke olması ve teknolojiyle birlikte gelişen sanayi ile insan kaynaklı, teknolojik afetlerin ne derece üzerine düşünülmesi gerektiği konusu ortaya çıkmıştır.

Devlet politikası olarak her alanda olduğu gibi ülkemizin afet yönetimindeki eksikliklerini ve aksaklıklarını iyi etüt ederek afet yönetimi alanında başarılı bir model ve sistem geliştirdik. Kamudaki acil eylem planı çerçevesinde afet yönetimini ülkemizin yapısına ve çağımızın gereklerine göre yeniden şekillendirdik. Afetlerin daha etkin ve tek elden

yönetilmesi için kurduğumuz Başbakanlık AFAD, afet ve acil durumlara ilgili güncel gelişmeleri ve gelecek eğilimleri değerlendirerek, kamu imkânlarının daha profesyonel kullanımı için çalışmaktadır. Bu sebeple afete hazırlık ve mücadele, çok yönlü koordinasyon ve bütün kurumların aktif katılımı gerekmektedir.

Başbakanlık AFAD, afet ve acil durumlara politikalar üretmekte, afet yönetimi konusunda ülkemizin uluslararası alanda öncü olması için çalışmalar yürütmektedir. AFAD, bütünlükten oluşan afet yönetim sisteminin yerleştirilmesi ve geliştirilmesi çalışmaları kapsamında, afet ve acil durumlara ilgili birçok yeni düzenleme yapmış, çok sayıda proje üretmiş ve üretmeye de devam etmektedir. “Kriz Yönetimi” anlayışından “Risk Yönetimi” anlayışına geçen, afet öncesi hazırlık, planlama ve risk azaltma çalışmaları, eğitim ve bilinçlendirme faaliyetleri, erken uyarı ve kesintisiz haberleşme projeleri ile afetin zararlarını en aza indirmeye çalışan bir ülkeyiz artık. Türkiye’deki afet ve acil duruma ilgili koordinasyon birçok ülkede örnek alınan, birçok ülkeye destek verdiğimiz bir seviyeye ulaşmıştır.

Bu çerçevede, Başbakanlık AFAD'ın koordinatörlüğünde ülke düzeyinde 2014-2023 Teknolojik Afetler Yol Haritası Belgeleri hazırlanarak yayımlanmıştır.

Belgelerin hazırlanmasında emeği geçen ve bu faaliyetlerde görev alan başta AFAD çalışanları olmak üzere, destekleriyle tüm kamu

kurum ve kuruluşlarına içtenlikle teşekkür eder, bugüne kadar olduğu gibi bundan sonraki dönemlerde de başarılı çalışmalarının devam etmesini temenni ederim.

Prof.Dr. Numan KURTULMUŞ
Başbakan Yardımcısı



ÖNSÖZ

Ülkemizde afet ve acil durumların etkin bir şekilde yönetilmesi amacıyla, 5902 sayılı Kanun gereği Başkanlığımızın kurulması ile Bütünleşik Afet Yönetim Sistemine geçilmiş, bu kapsamda afet ve acil durumlar ile sivil savunma hizmetlerinin tek bir merkezden düzenlenmesi, koordine edilmesi, denetlenmesi ve bu hizmetlere ilişkin eğitimlerin standartlarının belirlenmesi hedeflenmiştir.

Küreselleşen dünyamızda artık doğal afetler kadar, insan kaynaklı afetlerin sayısı ve şiddeti de giderek artmaktadır. Ülkemizde sanayinin hızla gelişmesi ve tehlikeli maddelere olan talebin artması neticesinde bu maddelerin üretimleri yaygınlaşmakta ve teknolojik afetler sonucunda çevreyi ve insan hayatını tehdit etme riski her geçen gün artmaktadır. Diğer yandan petrol-doğal gaz boru hatları, önemli tesisler ve ulaşım gibi kritik altyapılara sahip olunması teknolojik afetlere karşı daha duyarlı olmamızı zorunlu kılmaktadır.

Ulaşım, endüstriyel, maden, kimyasal, radyolojik ve nükleer kazalar, biyolojik olaylar, iklim değişikliği, kritik altyapı ve siber tehlikeler, petrol sızıntıları sonucu denizlerin kirlenmesi gibi teknolojik afetler konusunda da çalışmalar yürütmekte ve kapasitemizi her geçen gün geliştirmekteyiz.

Dr. Fuat OKTAY
AFAD Başkanı



Gelişen teknoloji ile birlikte, tehdit senaryoları da değişmiştir. Siber tehlikeler, günümüzde doğal afetler kadar ses getirmeye başlamıştır. Özellikler Kritik altyapılara gerçekleştirilecek siber saldırılar ülke genelinde büyük afetlere neden olabilmektedir. AFAD Başkanlığı olarak, bu konuda ülkemizde oluşabilecek tüm tehdit ve tehlikeler göz önüne alarak kritik altyapı, varlık ve tesisleri belirleyip, risk analizini yaparak, önceliklendirme çalışmalarımız sürmektedir.

Afetlerin ve afet yönetiminin artık sadece yerel olmadığı, uluslararası boyutunun da önemli olduğundan hareketle; işbirliği çalışmalarına, yardımlaşmaya, bilgi ve tecrübe paylaşımına ağırlık vermekteyiz.

Teknolojik afetlere yönelik tehdit ve tehlikelere karşı toplumsal farkındalığın artırılması, afetlere dirençli bir toplumun oluşturulması, gerekli tedbirlerin alınması ve yapılacak müdahale çalışmalarının etkin bir şekilde yürütülmesi için ülke düzeyinde kamu kurum ve kuruluşları ve sivil toplum kuruluşları; yerel düzeyde ise İl Afet ve Acil Durum Müdürlükleri arasında koordinasyonu sağlamak ve teknolojinin getirdiği yenilikleri afet yönetim sistemimize entegre etmek Başkanlığımızın öncelikli görevleri arasında yer almaktadır.

AFAD olarak, afet yönetiminin bütün safhalarını tek tek el almakta, uygulamaya geçirdiğimiz entegre afet yönetim sistemi ile de enerji ve mesaimizin çoğunu afet öncesi planlama, hazırlık ve risk azaltma çalışmalarına yoğunlaştırmaktayız. Ülkemizin ortak gücünü, ortak aklını ve ortak vicdanını harekete geçirerek afetleri tek elden yönetmekteyiz.

AFAD çalışanları ve ilgili kuruluşların katılımlarıyla birlikte, yoğun çalışmalar sonucu hazırladığımız 2014-2023 Teknolojik

Afetler Yol Haritası Belgeleri ile ülkemizin uzun vadede ulaşmayı hedeflediği konumunu göstermek amaçlanmıştır. Bu belgelerin oluşturulmasında emeği geçen tüm personelimize ve bu konuda katkı veren kurum ve kuruluşlarımıza teşekkür eder, bu süreçte ilgilerini ve desteklerini esirgemeyen Başbakan Yardımcımız Sayın Prof. Dr. Numan KURTULMUŞ'a şükranlarımı sunarım.

Dr. Fuat OKTAY
AFAD Başkanı





İÇİNDEKİLER

KISALTMALAR	2
TANIMLAR	4
BAKAN SUNUŞU	6
ÖNSÖZ	8
YÖNETİCİ ÖZETİ	12
1. GİRİŞ - DURUM ANALİZİ	14
1.1. AB Politikası	17
1.2. Türkiye Politikası	20
1.3. Metodoloji	26
2. AB MEVZUATI	28
2.1. Yetkili Otoritenin Belirlenmesi ve İş Bölümü; Sektör Bazında AKA'ları Belirlemekte Kullanılacak Kıstasların Tespit Edilmesi	28
2.2. Kritik Altyapıların Etkin Korunması Ulusal Seviyede veya AB Seviyesinde Bütün İlgili Paydaşlar Arasında İletişim, Koordinasyon ve İşbirliğinin Sağlanması	29
2.3. AKA'larla İlgili İşletmeciler Güvenlik Planı Yapılması	30
2.4. Güvenlik İrtibat Görevlisi Atanması	30
2.5. KAKAP Çalışmalarını Koordine Edecek Bir Kurum Belirlenmesi	30
2.6. AB Çapında "Kritik Altyapı Koruma İletişim Grubu" İrtibat Noktaları İle Koordinasyon	31
2.7. Ulusal Kritik Altyapıların Korumak Amacıyla Kritik Altyapı Koruma Planı	31
2.8. Kritik Altyapıların Etkin Korunması Ulusal Seviyede veya AB Seviyesinde Bütün İlgili Paydaşlar Arasında İletişim, Koordinasyon ve İşbirliği	32
2.9. En İyi Uygulamaların, Anlık Tehdit ve Alarmların Güvenli Bir Şekilde Paylaşımı Yoluyla Uygun Koruma Tedbirlerinin Geliştirilmesini Teşvik Edebilecek Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) Çalışmalarına Entegrasyon	32
3. ÜLKEMİZDEKİ MEVCUT DURUM	34
3.1. Devlet Politikası	36
3.1.1. Mevzuat	36
3.1.2. Projeler	36
3.2. Görev ve Sorumluluklar	37
3.3. Uygulama Çerçevesi ve Detayları	41
4. GEREKSİNİMLER VE EYLEMLER	42
KATKIDA BULUNANLAR	46
KAYNAKLAR	50





YÖNETİCİ ÖZETİ

Teknolojik afetler, insan faaliyetleri ya da doğal afetlerin tetiklenmesi sonucunda oluşan endüstriyel, maden, ulaşım ve taşımacılık, nükleer ve radyolojik, deniz kirliliğine neden olan kazalar, büyük yangınlar, biyolojik olaylar, kritik altyapılar ve siber tehditler ile çevresel tehlikeler gibi can ve mal kaybına, hastalıklara, sosyal, ekonomik ve çevresel bozulmalara neden olan afet ya da acil durumlar olarak tanımlanmaktadır.

Son yıllarda teknolojinin gelişmesi, hızlı nüfus artışı, gelişmişlik düzeyi, çevre kirliliği, çarpık kentleşmeye bağlı olarak teknolojik afetlerin sayısı ve sıklığı dünya genelinde olduğu gibi ülkemizde de artış göstermiştir. **Uluslararası afet ve acil durumlar veritabanı (EM-DAT – The International Disaster Database)** bilgilerine göre **1900 ile 2014 arasında dünya üzerinde 7825 adet teknolojik afet veya büyük kaza** kaydedilmiş ve birçok can ve mal kaybı meydana gelmiştir.

“**Kritik altyapıların korunması**”, özellikle 11 Eylül 2001 yılında ABD’deki ikiz kulelere yapılan saldırı sonrasında ülkelerin üzerinde daha yoğun bir şekilde düşündüğü, öneminin her geçen gün daha da arttığı bir kavram olmuştur. Dünya genelinde, özellikle ABD ve Avrupa olmak üzere, kritik altyapılarını belirleme ve bu altyapıların her türlü tehdit ve tehlikeye karşı korunması için önemli adımlar atılmıştır. Kritik altyapıların korunması sadece ulusal bir konu olmayıp, uluslararası alanda da çalışılması gereken çoklu bir disiplindir. Türkiye gibi jeostratejik önemi olan bir ülkenin kritik altyapılarından birinin işlevsiz kalması halinde sadece ülke içerisinde değil, Türkiye’ye bağımlı ülkelerde de kaosa neden olabilecek durumlar meydana gelebilir. Örneğin ülkemizden geçen petrol-doğalgaz boru hatlarının maruz ka-

EM-DAT Verilerine Göre
1900 ile 2014 arasında
7825 ADET
TEKNOLOJİK AFET
ve KAZA Kaydedilmiştir.

lacağı çevresel, fiziksel veya siber bir tehlike karşısında sadece ülkemiz değil, ülkemiz üzerinden enerji ithalatı yapan tüm ülkeler bu durumdan etkilenecektir.

5902 sayılı kanun gereğince; afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması ve olayların meydana gelmesinden önce hazırlık ve zarar azaltma, olay sırasında yapılacak müdahale ve olay sonrasında gerçekleştirilecek iyileştirme çalışmalarını yürüten kurum ve kuruluşlar arasında koordinasyonun sağlanmasından ve bu konularda politikaların üretilmesinden, uygulanmasından AFAD sorumlu kılınmıştır.

AFAD’ın yukarıda sayılan yetki ve görevleri kapsamında, kurum ve kuruluşların koordinasyonu ve teknolojik afetlerin etkin yönetimi amacıyla “Kritik Altyapıların Korunması Yol Haritası Belgesi” hazırlaması ihtiyacı ortaya çıkmış ve bu belge sadece AFAD tarafından değil aynı zamanda diğer kurum, kuruluşlar ve Türkiye çapındaki faydalanıcı grupların yetkililerinin de katılımıyla hazırlanmıştır.

Kritik Altyapıların Korunması Yol Haritası Belgesi ile AFAD’ın yasal olarak tanımlanmış görevleri göz önünde bulundurularak, Kritik Altyapılara ilişkin hizmetlerin yürütülmesinde ulusal mevzuat, uluslararası sözleşmeler ve ilgili AB mevzuatı ile farklı ülkelerdeki koordinasyon ve uygulamalar dikkate alınarak kısa ve uzun vadeli hedeflerin belirlenmesi ve bu hedeflerin uygulanması için eylem planlarını hazırlamak ve ulusal öncelikleri belirlemek amaçlanmıştır.

5902 Sayılı Kanun Geređi;

kurum ve kuruluşların koordinasyonu
ve teknolojik afetlerin etkin yönetiminden
AFAD sorumlu kılınmıştır.



1. GİRİŞ - DURUM ANALİZİ

“Kritik Altyapı” kavramı ülkelerin öncelikleri ve tehdit algılamalarına ya da teknolojik alanda yaşanan gelişmelere ve zamana bağlı olarak farklı şekillerde tanımlanmaktadır. Bu durumun temel nedenlerinin başında kritik altyapı tanımlamasının dinamik bir süreçte yürütülmek zorunda olması gelmektedir.

Kritik altyapı kavramı ilk olarak, başta ABD olmak üzere gelişmiş batılı ülkelerde telaffuz edilmiştir. ABD Başkanı tarafından Ekim 1996’da imzalanan kanun hükmünde kararname ile Başkan’ın “Kritik Altyapının Korunmasından Sorumlu Komisyonu” kurulmuş ve kritik altyapı tanımı ilk defa bu komisyonca yapılmıştır.

Sonrasında meydana gelen terör/sabotaj, kaza ve yaşanan doğal/insan kaynaklı afetler birçok ülke ile bölgesel ve küresel kuruluşu, güvenlik kavramını gözden geçirmeye zorlamıştır. ABD’de yaşanan 11 Eylül saldırıları ve Katrina Kasırgası, 2004 yılında İspanya’da yolcu trenlerine yapılan terör saldırıları ve 2006 yılında İngiltere’de yaşanan terör saldırıları, 2007 yılında Estonya’da ve 2008 yılında Gürcistan’da meydana gelen siber saldırılar bu durum için öne çıkan örneklerdir. İnsan kaynaklı veya doğal afetler, terör/sabotaj ve diğer olaylar ülkelerin güvenliği ve vatandaşların refahı açısından kritik altyapıların belirlenmesi ve korunmasının gerekliliği konusunda ciddi bir görüş birliğinin oluşmasına yol açmıştır.

Avrupa Birliği, kritik altyapıların korunması konusunu sistematik bir biçimde ilk defa 2004 yılında gündemine almıştır. Komisyon, Konsey’den gelen talep doğrultusunda “Terörizmle Mücadelede Kritik Altyapının Korunması” başlıklı bir tebliğ yayınlamıştır. 11 sayfalık belgede, kritik altyapının tanımı yapılmış ve terörizmle mücadelede altyapı unsurlarının korunması için yapılması gereken çalışmalar özetlenmiştir. Bu belgenin ışığında 2006 yılında hazırlanan “Kritik Altyapıların Korunması İçin Avrupa Programı” (KAKAP) başlıklı programda kritik altyapı, “işlevsiz kalması veya hasar görmesi durumunda üye ülkelerin ve vatandaşlarının sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak fiziksel ve teknolojik sistemler” olarak tanımlanmıştır. Bu kapsamda AB bünyesinde bulunan kritik altyapı, tesis ve varlıkların detaylı bir listesi hazırlanmıştır.

12 Aralık 2006 yılında yayımlanan “Kritik Altyapının Korunması İçin Avrupa Programı” Tebliği ile 11 ayrı sektör tanımlanarak, üye ülkelerin, sahip olduğu kritik altyapılarının bu sektörler bazında her türlü saldırı, terör, sabotaj ve kazaya karşı korunması için yapılması gerekenleri belirlemiş ve ülkelerin kendi mevzuatlarını bu süreçte uyumlaştırmaları gerektiğini belirtilmiştir.

Nihai çerçeveyi çizen son düzenleme 8 Aralık 2008 tarihli 114 sayılı “Avrupa Kritik Altyapılarının Belirlenmesi ve Koruyucu Tedbirlerin Arttırılması” başlıklı direktiftir.



1. GİRİŞ - DURUM ANALİZİ

2012 Yılı İtibari İle
Ülkemizde Kullanılan **Kredi Kartı ve Banka Kartı Sayısı 130 Milyondur.**
9.3 Milyon İnsan Aktif Olarak İnternet Bankacılığı Kullanmakta ve
Yaklaşık 1,5 Trilyon TL lik İşlem Yapılmaktadır.



1. GİRİŞ - DURUM ANALİZİ

- Avrupa Kritik Altyapıların(AKA) tanımlanması, belirlenmesi ve korunmasına yönelik önlemler geliştirmek.

2007 tarihinde Konsey, Avrupa'daki kritik altyapıların ve bu altyapıların korunmalarını geliştirme ihtiyacının tanımlanması ve belirlenmesi için bir Avrupa prosedürü geliştirmek adına Komisyon'un yaptığı çalışmalarını memnuniyetle karşılarken ulusal sınırlar içerisinde kritik altyapıların korunması için gerekli düzenlemeleri yönetme konusunun tamamen üye devletlerin sorumluluğunda olduğu gerçeğini vurgulayan sonuçlara varmıştır.

2008 yılında "Avrupa Kritik Altyapılarının Belirlenmesi ve Koruyucu Tedbirlerin Arttırılması" direktifi yayınlanmış ve son yasal düzenleme olarak kayda geçmiştir. Bu direktif ile de Avrupa Kritik Altyapıların korunması sorumluluğu öncelikle ve tamamen üye devletlere ve bu tür altyapıların sahiplerine/işletmecilerine düşmektedir.

Direktifin uygulamaya geçmesi ve işlerliğinin teftiş edilmesi için en geç tarih 2012 yılı Ocak Ayı olarak belirlenmiştir.

2009 yılında Stockholm Programı ile Avrupa Kritik Altyapıların korunmasının önemi vurgulanmış ve özellikle açıklıklarının belirlenmesi üzerine dikkat çekilmiştir. Ayrıca Stockholm Programı, konunun öneminin yüksek olduğunu, gerekli önlemlerin alınması ve ulaştırma ve

enerjinin yanısıra, bilgi ve iletişim teknolojileri ile kritik kamu hizmetlerin de dikkate alınması gerektiği hususlarında Konsey, Komisyon ve Avrupa Parlamentosunu davet etmiştir.

2011 yılında Avrupa Birliği İç Güvenlik Stratejisi "5 adımda daha güvenli Avrupa" ile altyapıların korunmasını dayanışma yoluyla olacağıın altını çizmiştir. Lizbon Antlaşması ve İç Güvenlik Stratejilerinin yürürlüğe girmesi ile KAKAP daha da önemli bir hale gelmiştir.

Direktifin uygulanması ve işlerliğinin teftiş 2011 yılında başlamış ve 2012 yılında net sonuçlar alınmıştır. Birçok toplantı, seminer vb. etkinlikler gerçekleştirilmiştir. Örnek olarak, Komisyon tarafından 15 Şubat 2012 tarihinde elektrik şebekeleri ağının korunması üzerine bir organizasyon yapılmıştır. 14-16 mart 2012 tarihinde Brüksel'de üye devletlerin kontak kişileri biraraya gelmiştir. Ayrıca 2008 yılındaki direktifin uygulanma sonuçlarını görmek adına 24-26 Nisan 2012 tarihinde 7. çalıştay yapılmıştır. Bu çalıştay sonucunda tartışılan konulardan biri de "Kritik Altyapıların Risk Değerlendirmesi" ile ilgilidir.

Avrupa Birliği, ABD ve Kanada uzmanlarının biraraya geldiği 3 adet seminer yapılmıştır. 3. Semineri takiben 2008 yılındaki direktifin de yazıldığından öte politikalar yapmanın gerektiği ortaya çıkmıştır. Direktifin etki değerlendirilmesi 2012 Eylül Ayında bitirilmiştir.

Son olarak “2012 yılı Komisyon Çalışma Programı” kasım ayında yeni kritik altyapı korunma paketini tasarlamıştır. Yeni paket ile, yeniden şekillenen AB’nin “Kritik Altyapıların Korunması Çerçevesi” önerilmiştir.

2008/114 sayılı direktif, tüm üye ülkeler tarafından, hukuki düzenlemelerini, kendilerine göre adapte ederek uygulamaya koyulmuştur.

KAUBA 2012 yılında yapılmaya başlamış ve 2013 Ocak ayında uygulamaya başlamıştır. Daha ilk aylarında çok iyi sonuçlar gözlemlenmiştir.

AB Bünyesinde Hazırlanan Projeler

Avrupa Birliği bünyesinde 2007-2012 yılları arasında “Terörizm ve Diğer Güvenlik ile İlgili Riskleri Önleme, Hazırlık ve Sonuç Yönetimi” başlığı altında kritik altyapı güvenliği ve kriz yönetimini adres gösteren 100 farklı proje yapılmıştır. Bunlardan bazıları;

- Kritik Altyapı Güvenliği Konusunda Politika Yapıcılar İçin İyi Örnekler
- Kritik Bilgi ve İletişim Teknolojileri Altyapı Koruma Simülasyon Modelleri
- Etkin Kritik Altyapı Korunması ve En İyi Uygulamaların Geliştirilmesi
- ERNCIP Projesi(Kritik Altyapıların Korunması İçin Avrupa Birliği Referans Ağı)

Bu projelerden en iyilerinden biri denilebilecek “ERNCIP Projesi” 4 yıllık bir projedir.

FP7 Güvenlik Çerçevesinde 40’tan fazla kritik altyapıların korunması ile ilgili proje fonlanmıştır. Projeler de kritik altyapılar, siber tehditler dahil olmak üzere tüm tehdit ve tehlikeler göz önüne alınmaktadır. Yine risk değerlendirme ve risk yönetimi başlığı altında da birçok kritik altyapıyı kapsayan proje yapılmıştır.

Son olarak , KAKAP kapsamında yeni pilot proje hazırlanmıştır ve bu pilot projede Avrupa Birliği boyutunda 4 kritik altyapı belirlenmiştir. Eurocontrol, Galileo, Elektrik İletim Şebekesi ve Gaz İletim Ağı’nın korunmasının optimize edilmesi ve güçlendirilmesidir.

AB İle İlgili Yasal Mevzuatlar;

- “Terörizmle Mücadelede Kritik Altyapının Korunması” (EU COM702/2004)
- COM (2005) / 576 sayılı Avrupa Komisyonu Tebliği
- “Kritik Altyapının Korunması İçin Avrupa Programı Direktifi” (EU COM786/2006) (EPCIP),
- “Avrupa Kritik Altyapılarının Belirlenmesi ve Koruyucu Tedbirlerin Arttırılması” 8 Aralık 2008 (2008/114/EC)

1. GİRİŞ - DURUM ANALİZİ

1.2 Türkiye Politikası

Konsey, Aralık 1999'da Helsinki'de gerçekleşen toplantıda Türkiye'nin, diğer aday ülkelere uygulanan kriterler temel alınarak Avrupa Birliği'ne (AB) katılacağı öngörülen bir aday ülke olduğunu onaylamıştır. AB'ye üyeliğin bir ön koşulu olarak aday ülkeler mevzuatlarını, AB müktesebatı tarafından içerilen AB mevzuatının bütününe etkili kılmak için, AB mevzuatına uygun şekilde düzenlemek zorundadırlar.

Uyumlaştırma süreci diye adlandırılan bu süreç, sadece ilgili tüm AB gereklerinin ulusal mevzuata tam olarak yansıtılmasını değil ayrıca ulusal mevzuatı yönetmek için yeterli bütçeye sahip uygun kurumsal yapıların kurulmasını ve kanunlarla tam uyumu sağlamak için gerekli kontrol ve cezaların konulmasını gerektirmektedir. Ek olarak, AB mevzuatının tam olarak uygulanması zorunlu teknik standartları karşılayan yeni veya güncellenmiş tesisler için harcama yapılmasını da gerektirebilmektedir.

Uyumlaştırma süreci, müktesebatın diğer bölümlerinde olduğu gibi çevre başlığı altında yer alan sivil korunma başlığı için de uygulanmaktadır. Kritik altyapıların korunması ve güvenlik önlemlerinin artırılması da sivil korunma başlığı altındadır.

Kritik altyapıların korunması, teknolojik afetler başlığı altında ele alınmalıdır. Teknolojik afetler, doğal afetlerin tetiklemesi sonucu oluşabileceği gibi, insan kaynaklı bir kaza, terör veya sabotajdan da kaynaklanabilir.

Kritik altyapıların korunması, hem güvenlik hem de afet ve acil durum yönetimini birleştiren bir durumdur. Afet ve acil durumlarda ülkemizde afet yönetiminin tek elden koordine edilmesi için Afet ve Acil Durum Yönetimi Başkanlığı 2009 yılında 5902 sayılı yasa ile kurulmuştur.

Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun (5902); afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması ve olayların meydana gelmesinden önce hazırlık ve zarar azaltma, olay sırasında yapılacak müdahale ve olay sonrasında gerçekleştirilecek iyileştirme çalışmalarını yürüten kurum ve kuruluşlar arasında koordinasyon sağlanması ve bu konularda politikaların üretilmesi ve uygulanması hususlarını kapsar.

10. Kalkınma Planı kapsamında;

- Afet risklerinin azaltılmasına yönelik uygulama mekanizmaları güçlendirilecek, afetlere hazırlık ve afet sonrası müdahalede özel önem arz eden hastane, okul, yurt gibi ortak kullanım mekânları ile enerji, ulaştırma, su ve haberleşme gibi kritik altyapıların güçlendirilmesine öncelik verilecektir,
- Afetlere karşı daha etkin mücadele etmek üzere kamu kurum ve kuruluşları arasında hızlı, güvenli ve etkin bir veri paylaşımını sağlayacak afet bilgi yönetim sistemi kurulacak, etkin ve kesintisiz haberleşme temin edilebilmesi için iletişim altyapısı daha da güçlendirilecektir,
- Bina ve altyapı tesislerinin afetlere daha dayanıklı olarak inşa edilmesi sağlanacak ve inşaatların denetimi bağımsız, ehil ve yetkili kişi ve kurumlar aracılığıyla güçlendirilecektir,

Maddeleri ile de ülkemizde kritik altyapı korunmasının önemi vurgulanmıştır.

Kritik Altyapıların Korunması İlgili Yol Haritası Belgesinin Amacı;

- Afetin neden olduğu zararların en aza indirgenmesi amacıyla, doğal ve teknolojik afetlerde bütünlük bir yaklaşımla sivil korunmadan sorumlu olanların hazırlığı ve afet durumunda müdahale konusunda ulusal, bölgesel ve yerel seviyedeki çalışmaları desteklemek,
- Teknolojik afet konusunda sivil korunmayla ilgili AB mevzuatına göre uygulamalar yapabilecek şekilde hukuksal, kurumsal ve teknik çalışmalar yapmayı ve bu mevzuatın özellikle yetkili kurum ve kuruluşlar arasındaki işbirliğiyle ilgili olarak uygulanmasını koordine etmek,
- İnsanların, çevrenin ve malın daha iyi korunmasını sağlamak için, AB sivil korunma

2013 Yılında Topkapı Sarayını

3 Milyon 397 Binden Fazla Turist

Ziyaret Etmiştir.





1. GİRİŞ - DURUM ANALİZİ

İstanbul'da
1 Yılda Raylı Sistemler İle
363,95 Milyon İnsan
Taşınmaktadır.

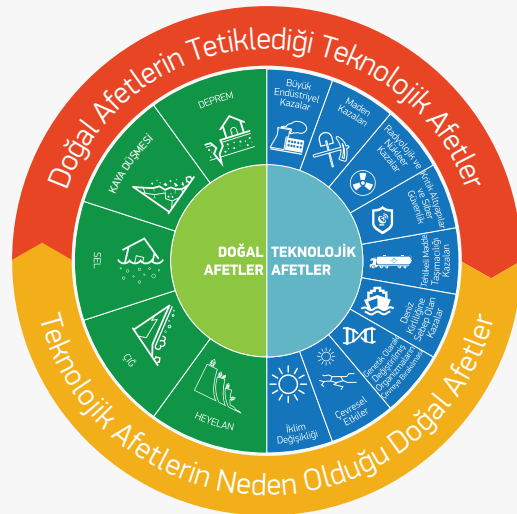


mevzuatı, topluluğun sivil korunma müdahaleleri mekanizması ve sivil korunmanın mali araçları ile ilgili çalışmaları başlatarak, müzakereler için gerekli hazırlıkları yapmak,

- Kritik altyapıların korunması için sivil korunma araştırması alanındaki işbirliğinin güçlendirilmesi, risklerin ve zararların azaltılması konusunda araştırma projelerinin hazırlanmasını teşvik etmek,
- Afet izleme ve bilgilendirmesi amacıyla, erken uyarı sistemlerindeki rolleri belirlemek,
- Ülke düzeyinde uygulanacak afet ve acil durum çalışmalarına yönelik risk yönetimi ve zarar azaltma planlarını hazırlatabilmek, risk değerlendirme sonucunda, zararın ortaya çıkma olasılığını azaltma, ortadan kaldırma veya şiddetini azaltmaya yönelik faaliyetlerin ulusal boyutta uygulanmasını yönlendirmek,
- Ülkemizde bulunan ulusal kritik altyapıları belirleyecek kurum ve kuruluşların koordinasyonunu yapmak,
- Ülkemizde ve komşu ülkelerimizde bulunan ve tahrip olması halinde uluslararası ilişkilerimizi etkileyecek sınır ötesi güce sahip kritik altyapıları belirlemek, korunmasına yönelik politikalar üretmek,
- Kritik Altyapılar Uyarı Bilgi Ağı'na(KAUBA) yönelik verileri hazırlamak.


“Kritik Altyapıların Korunması ile İlgili Yol Haritası Belgesi” hazırlıklarında analizi yapılan AB Müktesebatı, Uluslararası sözleşmeler ve farklı ülkelerdeki koordinasyon ve uygulamalar dikkate alınarak teknolojik afet ile ilgili hususların uygulanması ile ilgili genel gereksinimlere yönelik olarak kurum ve kuruluşların görev ve sorumlulukları aşağıda özetle verilmiştir.

Şekil-1 Afetlerin sınıflandırılması ve aralarındaki ilişki



1. GİRİŞ - DURUM ANALİZİ

Tablo 1. Yetkili Kurumların Genel Rol ve Sorumlulukları Tablosu

YETKİLİ KURUMLAR	ROLLER VE SORUMLULUKLAR
	<ul style="list-style-type: none"> • Teknolojik afetler ile ilgili tüm kurum ve kuruluşlarla koordinasyonu sağlamak, öngörülen görev sorumlulukların yerine getirilmesinde destek vermek • Afet ve acil durumlarda kararlara ve uygulamaya destek vererek fon kullanılmasını sağlamak, • Harici eylem planlarını yapmak, risk haritalarını hazırlamak, kaza sırasında müdahale ve sonrasında iyileştirme çalışmalarında bulunmak, • Kritik altyapı unsurlarında, afet ve acil durumlar ile güvenlik ile ilgili "Kurumsal Hazırlık Planları" nın oluşturulmasını koordine etmek, • Eğitim ve tatbikatları koordine etmek, • Kritik altyapıları kapsam, büyüklük ve zaman etkisi faktörlerini göz önünde bulundurarak belirlemek ve koruyucu tedbirleri arttırmak; Direktifin uyumlaştırılması ile ilgili taslak yönetmelik hazırlamak, • Yetkili otoritenin belirlenmesi ve iş bölümü sektör bazında Kritik Altyapı Sektörleri (KAS) belirlemede kullanılacak kıstasları tespit etmek, • Kritik altyapıların etkin korunması ulusal seviyede veya AB seviyesinde bütün ilgili paydaşlar arasında iletişim, koordinasyon ve işbirliği sağlamak, • KAS ile ilgili İşletmeciler Güvenlik Planı (İGP) yapmak, • Ulusal düzeydeki kritik altyapıların korunması amacı ile proje hazırlamak, • En iyi uygulamaların ve anlık tehdit ve alarmların güvenli bir şekilde paylaşımı yoluyla uygun koruma tedbirlerinin geliştirilmesini teşvik edebilecek AB Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) çalışmalarına entegrasyonu sağlamak, • Dünyada ki en iyi uygulamaları izlemek, ve buna yönelik ilgili diğer yabancı kurumlarla işbirliği yapmak

YETKİLİ KURUMLAR	ROLLER VE SORUMLULUKLAR
	<ul style="list-style-type: none">• AB çevre müktesebatının uyumlaştırılması da dahil olmak üzere, Türkiye'deki çevre politikalarının geliştirilmesi ve uygulanması için bir genel koordinasyon yapmak, kapsamındaki kritik altyapı unsurlarını belirlemek ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Büyük endüstriyel kazalar, maden kazaları konusunda tesisleri denetlemek.
	<ul style="list-style-type: none">• Kritik sağlık altyapı unsurlarını belirlemek ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik kamu hizmetlerini belirlemek, ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik enerji altyapı unsurlarını belirlemek, ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik finans altyapı unsurlarını belirlemek ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik ulaştırma altyapılarını belirlemek ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik öneme haiz kültür varlıklarını, tesisleri belirlemek ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik su kaynaklarını, barajları ve büyük ormanları belirlemek ve gerekli önlemleri almak, aldırarak.
	<ul style="list-style-type: none">• Kritik öneme haiz büyük sanayi tesislerini belirlemek, gerekli güvenlik önlemlerini almak, aldırarak.
	<ul style="list-style-type: none">• Büyük ölçekli üretim yapan tesisleri, kritik öneme haiz limanları ve büyük ticari tesisleri belirlemek, gerekli güvenlik tedbirlerini almak, aldırarak.
	<ul style="list-style-type: none">• Kritik tarım ve hayvancılık arazilerini belirlemek, gerekli önlemleri almak, aldırarak.



1. GİRİŞ - DURUM ANALİZİ

1.3 Metodoloji

Avrupa Birliği ilgili direktifi uyumlaştırılması sürecinde, kritik altyapıların ve kapsamının belirlenmesi;

Kapsam, kritik altyapının kaybı veya müsait olmaması durumunda etkilenecek alanın genişliğini,

Büyüklik ise Hiç, Az, Orta veya Büyük olarak sınıflandırılacak etki büyüklüğünü ifade etmektedir. Büyüklik değeri bulunurken;

- Kamu etkisi (hükümete olan güven)
- Fiziksel etki (etkilenen nüfus büyüklüğü, can kaybı vb.),
- Ekonomik etki,
- Çevresel etki,
- Diğer altyapı elemanlarıyla bağıllık,

gibi etkenlerin dikkate alınması gerekli görülmüştür. Zaman etkisi, kritik altyapının zarar görmesinden faaliyete geçeceği zamana kadar geçen süreyi ifade etmektedir.





Toplam kullanılan
44 Milyar m³ suyun
32 milyar m³'ü
DSİ sulamalarında kullanılmaktadır.



2. AB MEVZUATI

Parlamento ve Konseyin 8 Aralık 2008 tarihli ve 114 sayılı “Avrupa Kritik Altyapılarının Belirlenmesi ve Koruyucu Tedbirlerin Arttırılması” üzerine olan direktif enerji ve ulaşım sektörlerine odaklanmış olmakla birlikte toplamda onbir (11) adet sektörü içermektedir. Direktife göre Avrupa kritik altyapılarını koruma sorumluluğu bu altyapıların bulunduğu ülkelere ve bunların işletmecilerine verilmiştir.

2.1 Yetkili Otoritenin Belirlenmesi ve İş Bölümü; Sektör Bazında AKA'ları Belirlemekte Kullanılacak Kıstasların Tespit Edilmesi

Sektör bazında belirlenecek olan kurumun yerine getireceği görevler sırasıyla;

- KAKAP çalışmalarını izlemek, koordine etmek ve denetlemek,
- Kritik altyapı işletmecileri ve sahipleri, diğer üye ülkeler ile bağlı olduğu üye ülke arasında iletişimi sağlamak,
- KAKAP'ların belirlenmesinde görev almak,
- Kendi yetki alanı içerisindeki bir altyapıyı kritik olarak belirlemek,
- Belirli altyapı sektörleri arasında bağımlılıkları belirlemek,
- KAKAP ve sektöre özel kritik altyapı ko-

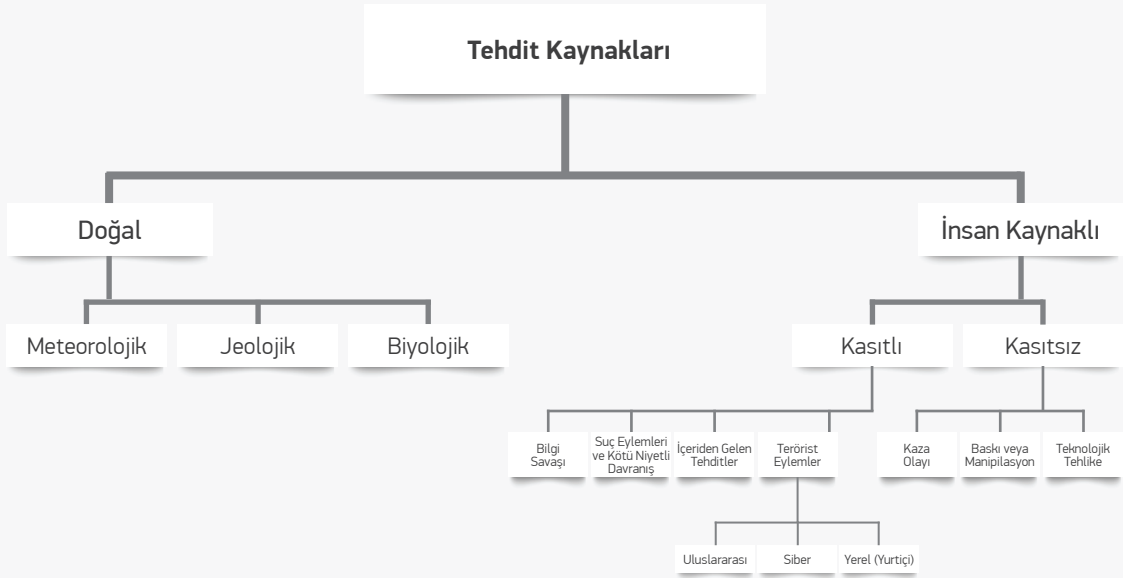
ruma programlarının detaylandırılmasında görev almak.

Kritik altyapıların korunması sırasında kullanılan güvenlik yönetimi yaklaşımı, riskleri anlamaya ve bu riskleri makul bir maliyete ve kabul edilebilir bir seviyeye çekmeyi hedeflemektedir.

1. Taslak bir AKA listesi aşağıdakileri içerir;
 - a. İşletmeci güvenlik planlarının içermesi gereken asgari içerik,
 - b. Önemli varlıkların tespiti,
 - c. Büyük tehdit senaryoları,
 - d. Her bir varlığın zafiyetine ve potansiyel etkiye dayalı risk analizi,
 - e. Karşı tedbirler ve prosedürlerin tespiti, seçimi ve önceliklendirilmesi
2. Kritik altyapılarla ilgili konularda işbirliği ve koordinasyonu sağlamak için kritik altyapı sahipleri/işletmecileri tarafından Kritik Altyapı Koruma İrtibat Görevlisi atanacaktır.
3. Kritik altyapılarını koruma sorumluluğu bu altyapıların bulunduğu ülkelere ve bunların işletmecilerine verilmiştir

Güvenlik İrtibat Görevlisi, AKA'nın sahibi/işletmecisi ve ilgili üye ülke otoritesi arasında güvenlikle ilgili konularda irtibat noktası olarak işleyecektir.

Şekil-2 Tehdit Kaynakları



2.2 Kritik Altyapıların Etkin Korunması, Ulusal Seviyede veya AB seviyesinde Bütün İlgili Paydaşlar Arasında İletişim, Koordinasyon ve İşbirliğinin Sağlanması,

Ortak kritik altyapı koruma prensipleri kullanılmalıdır. Bu prensipler ;

- Genel kabul gören kılavuzlar/standartlar, ortak tanımlar,
- Kritik altyapı öncelik alanları,
- Çalışmalarda rol alan paydaşların sorumlulukların tanımları,
- Kararlaştırılmış performans ölçütleri,
- Farklı sektörlerdeki altyapıları karşılaştıran ve önceliklendiren yöntemler

çerçevenin ana elemanlarından bazılarıdır.

Kritik altyapıların korunması öncelikle

bir ulusal sorumluluktur. Sahiplerin ve işletmecilerin kendi varlıklarını koruma konusunda kendi kararlarını vermeleri ve planlarını yapmaları konusundaki yükümlülükleri ve sorumluluklarının değişmemesi esas alınacaktır.

Kritik altyapıları korumayla ilgili bilgi paylaşımı güven ve gizlilik ortamında yürütülmelidir. Ulusal seviyede kritik altyapı koruma bilgileri gizli olmalı ve sadece bilmesi gerekenlere erişim hakkı verilmesi gereklidir.

AB'nin kritik altyapıları koruma çabalarının, ortak bir KAKAP çerçevesinde (ortak hedefler, yöntemler vb.) en iyi uygulamaların ve uyum izleme mekanizmalarının paylaşımıyla güçlendirilmesi önerilmektedir.



Her bir üye devlet, bölgesinde yer alan AKA olarak belirlenmiş altyapının

Güvenlik İrtibat Yetkilisine

ya da eşdeğerine sahip olup olmadığını değerlendirecektir.

2. AB MEVZUATI

2.3 AKA'larla İlgili İşletmeci Güvenlik Planı Yapılması,

İşletmeci Güvenlik Planı prosedürü, AKA'nın kritik altyapı varlıklarını ve bu altyapıların korunmaları için ne gibi çözümlerinin olduğunu belirleyecektir.

Her bir İGP asgari olarak;

- Önemli varlıkların tanımları,
- Ana/büyük tehdit senaryolarına, her bir varlığın açıklığına ve zarar görmesi halinde potansiyel etkiye dayalı olarak risk analizi yapılması,
- Karşı tedbirlerin ve prosedürlerin belirlenmesi, seçilmesi ve önceliklendirilmesini içerecektir.

2.4 Güvenlik İrtibat Görevlisi Atanması,

Güvenlik İrtibat Yetkilisi, AKA sahibi/operatörü ile ilgili üye devlet otoritesi arasında güvenlikle ilgili konularda irtibat noktası görevi görecektir.

- Her bir üye devlet, bölgesinde yer alan AKA olarak belirlenmiş altyapının Güvenlik İrtibat Yetkilisine ya da eşdeğerine sahip olup olmadığını değerlendirecektir. Üye devletin bu tür bir Güvenlik İrtibat Yetkilisinin yürürlükte olduğunu ya da

eşdeğerinin mevcut olduğunu tespit etmesi durumunda, daha başka bir yapılandırma gerekli olmayacaktır.

- Üye devletin, AKA olarak belirlenen altyapıda bir Güvenlik İrtibat Yetkilisinin ya da eşdeğerinin mevcut olmadığını tespit etmesi durumunda, bu tür bir Güvenlik İrtibat Yetkilisinin ya da eşdeğerinin belirlenmesi için gerekli olan her türlü ölçütün hazırlanacağından emin olacaktır.
- Her bir üye devlet, söz konusu AKA ile ilgili belirlenen riskler ve tehditler hakkındaki bilgilerin paylaşılması doğrultusunda, ilgili üye devlet otoritesi ve Güvenlik İrtibat Yetkilisi ya da eşdeğeri arasında uygun bir iletişim mekanizması kuracaktır. Bu iletişim mekanizması, önemli ve gizli bilgilere erişim konusundaki ulusal gereklilikleri ihlal etmeyecektir.

2.5. KAKAP Çalışmalarını Koordine Edecek Bir Kurumun Belirlenmesi,

Belirlenecek olan kurumun yerine getireceği görevler sırasıyla;

- KAKAP çalışmalarını izlemek, koordine etmek ve denetlemek,
- Kritik altyapı işletmecileri ve sahipleri, diğer üye ülkeler ile bağlı olduğu üye ülke arasında iletişimi sağlamak,

- AKA'ların belirlenmesinde rol almak,
- Kendi yetki alanı içerisindeki bir altyapıyı kritik olarak belirlemek,
- Belirli altyapı sektörleri arasında bağımlılıkları belirlemek,
- Ulusal ve sektöre özel kritik altyapı koruma programlarının detaylandırılmasında görev almak.

2.6 AB Çapında "Kritik Altyapı Koruma İletişim Grubu" İrtibat Noktaları İle Kordinasyon,

KAKAP çerçevesinin uygulanmasında kritik altyapı konusunda uzman gruplardan yardım alınacaktır. Kritik altyapı uzman gruplarının; belirgin açıklıkları azaltmak ve/veya ortadan kaldırmak için tedbirlerin geliştirilmesine ve performans ölçütlerinin geliştirilmesine yardım etmek, kritik altyapı bilgi paylaşımını, eğitimi, güven oluşturmayı kolaylaştırmak, sektör ortaklarını kritik altyapı korumaya teşvik etmek amacıyla iş örnekleri geliştirmek ve desteklemek, araştırma ve geliştirme gibi konularda sektöre özel uzmanlık ve tavsiye sağlamak ve benzeri görevleri yerine getirmesi beklenmektedir. Paylaşılan ticari, kişisel veya hassas bilgiler kamuya açıklanmayacaktır.

2.7 Ulusal Kritik Altyapılarını Korumak Amacıyla Kritik Altyapıları Koruma Planı,

Ulusal Kritik Altyapılar (UKA) belirlenirken dikkate alınacak faktörler kapsam ve riskin boyutudur.

Ulusal Kritik Altyapıların korunması kapsamında kritik altyapı sahiplerine ve işletmecilerine;

- a. İlgili üye ülke kritik altyapı koruma kurumuna bir altyapının kritik bir yapıya sahip olabileceği konusunda bilgi vermek,
- b. Bir temsilciyi kendisiyle ilgili üye ülke otoritesi arasında Güvenlik İrtibat Memuru olarak atamak,
- c. İşletmeci Güvenlik Planının kurulması, uygulanması güncellenmesi ve denetlenmesi,
- d. İlgili üye ülke sivil savunma ve kolluk kuvvetleri ile birlikte hazırlanan acil durum planının geliştirilmesinde yer almak görevleri verilmektedir.





2. AB MEVZUATI

2.8 Kritik Altyapıların Etkin Korunması Ulusal Seviyede veya AB Seviyesinde Bütün İlgili Paydaşlar Arasında İletişim, Koordinasyon ve İşbirliği,

Kritik altyapıların korunması öncelikle bir ulusal sorumluluktur. Sahiplerin ve işletmecilerin kendi varlıklarını koruma konusunda kendi kararlarını vermeleri ve planlarını yapmaları konusundaki yükümlülükleri ve sorumluluklarının değişmemesi esas alınacaktır.

Kritik altyapıları korumayla ilgili bilgi paylaşımı güven ve gizlilik ortamında yürütülmelidir şeklinde ifade edilebilir. Ulusal seviyede kritik altyapı koruma bilgileri gizli olmalı ve sadece bilmesi gerekenlere erişim hakkı verilmesi gerekli görülmektedir.

AB'nin kritik altyapıları koruma çabalarının, ortak bir KAKAP çerçevesinde (ortak hedefler, yöntemler vb.) en iyi uygulamaların ve uyum izleme mekanizmalarının paylaşımıyla güçlendirilmesi önerilmektedir.

2.9. En İyi Uygulamaların, Anlık Tehdit ve Alarmların Güvenli Bir Şekilde Paylaşımı Yoluyla Uygun Koruma Tedbirlerinin Geliştirilmesini Teşvik Edebilecek Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) Çalışmalarına Entegrasyon,

Kritik altyapı bilgi paylaşım işlemleri ve bağımlılıkların belirlenmesi ve analizi yapılmalıdır. Paydaşlar, altyapı sahipleri ve işletmecileri, düzenleyici kurumlar, kamu kurum ve kuruluşları, uzmanlar ve özel sektör ile birliklerini içermektedir.

KAUBA, kritik altyapıların korunması konusunda bilgi alışverişini sağlayan bir forum olup, üye ülkelere ve Komisyona kritik altyapılara yönelik anlık riskler ve tehditler üzerine uyarılar yollama imkânı sağlamaktadır. KAUBA, üye ülkelerin işbirliğini kolaylaştıracak bir bilgi sistemi sağlayarak ve AB içinde kritik altyapılar hakkında bilgilerin aranması için hızlı ve verimli bir yol sunarak kritik altyapıların korunmasına ilişkin tedbirlerin geliştirilmesine katkıda bulunacaktır.

KAUBA yapısında yer alan her bir üye ülke bir irtibat noktası olarak görev yapan KAUBA yöneticisi atamalıdır.



3. ÜLKEMİZDEKİ MEVCUT DURUM

Kritik altyapılar ve bu altyapıların korunması konuları ülkemizde ulusal bilgi güvenliği başlığı altında değerlendirilmiştir. Ulusal bilgi güvenliği konusunda ülkemizde yürütülen çalışmaların geçmişi ise gelişmiş ülkelerin bu konu üzerinde çalışmalar yaptığı 1990'ların sonlarına kadar gitmektedir.

1990'ların sonlarından 2006 yılına kadar Milli Savunma Bakanlığı koordinasyonunda ulusal bilgi güvenliği konusundaki hukuki boşluğu gidermek için çalışmalar yapılmıştır. Bu bağlamda, Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı hazırlanmıştır.

Bu kanun tasarısının amacı;

Ulusal güvenliği ilgilendiren bilgilerin korunması, devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve görevlerine ilişkin esas ve usulleri düzenlemek olarak belirlenmiştir. Uzun süre çalışılmasına rağmen mezkûr Kanun Tasarısı üzerinde mutabakat sağlanamamıştır.

TÜBİTAK'ın Kalkınma Bakanlığı 2012 Yatırım Programı içerisinde yer alan “**Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi**” ve UDHB sponsorluğunda hazırlanan raporlar ülkemizdeki Kritik Altyapıların Bilgi Güvenliği konusunda önemli bir adım olmuştur.

Şu ana kadar ortaya çıkan tek yasal düzenleme 20 Ekim 2012 tarihli Resmi Gazetede “**Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı**”dır. Bu önemli kararlar ülkemizin siber güvenliğinin sağlanması konusunda idari, teknik ve hukuki yapıların oluşturulması hız kazanmış, siber güvenliğe ilişkin program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla “**Siber Güvenlik Kurulu**” oluşturulmuştur. Bu kurulun ilk toplantısında “**Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı**” kabul edilmiş ve 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak yayımlanmıştır. Bu eylem planının 5 numaralı maddesinde Siber Güvenlik Kurulu'nca ülkemizin kritik altyapıları bilgi güvenliği kapsamında ilk etapta “Ulaşım, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri” olarak belirlenmiştir.

“1981 yılında kabul edilen 2565 sayılı kanuna ilişkin olarak, 1983 yılında Resmi Gazete de yürürlüğe giren “Askeri Yasak Bölgeler ve

Güvenlik Bölgeleri Yönetmeliği” kritik altyapılardaki bilgi güvenliğinin dışında, fiziksel güvenliğine değinen ilk yasal düzenleme olarak kabul edilebilir.

Ülkemizdeki net ifadeyle kritik altyapıların çevresel tehdit ve tehlikelerine (deprem, sel vb.) karşı korunmasına yönelik bir yasal düzenleme ise maalesef bulunmamaktadır.

Son yıllarda artan terör tehdidi ve yaşanan büyük çaplı felaketler ülkeleri kritik altyapıların korunması ile ilgili politika, strateji, mevzuat, plan ve programlar yapmaya; yapmış olanları da bütüncül bir bakış açısıyla bunları yeniden gözden geçirmeye itmekte-

dir. ABD, Japonya ve AB üyesi ülkeler başta olmak üzere gelişmiş ülkeler, bu çalışmada da belirtildiği üzere, kritik altyapılarını belirlemiş, bu altyapıların korunmasına ilişkin mevzuatlarını hazırlamış ve kritik altyapıların korunması konusunda sorumlu kurum ve kuruluşlarını tespit etmiş olup, bu kurum ve kuruluşlarca kritik altyapıların korunmasına ilişkin planlı ve yoğun çalışmalarını devam ettirmektedirler.





3. ÜLKEMİZDEKİ MEVCUT DURUM

3.1 Devlet Politikası

3.1.1 Mevzuat

5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun; afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması ve olayların meydana gelmesinden önce hazırlık ve zarar azaltma, olay sırasında yapılacak müdahale ve olay sonrasında gerçekleştirilecek iyileştirme çalışmalarını yürüten kurum ve kuruluşlar arasında koordinasyonun sağlanması ve bu konularda politikaların üretilmesi ve uygulanması hususlarını kapsamaktadır. Bu çerçevede konudan sorumlu yukarıda bahsi geçen kurumların ve konu ile ilgisi olan diğer kurumların koordinasyonunda yetkili kurum olarak AFAD görülmektedir.

Kritik altyapılar ve bu altyapıların korunması ile ilgili olarak ülkemizde şu ana kadar yapılmış ve hazırlanmakta olan direk olarak bu konuyu kapsayan bir mevzuat çalışması bulunmamaktadır.

Ülkemizde EPDK(Enerji), BDDK,SPK(Bankacılık ve Finans) ve BTK(Elektronik Haberleşme) olmak üzere düzenleyici kurumlar bulunmakta ve mevzuatlarından kaynaklanan sektörü düzenleme ve koruma yetkileri mevcuttur. Bunun yanı sıra, Ulaştırma, Denizcilik

ve Haberleşme Bakanlığının altındaki Kara, Deniz ve Demiryolları Düzenleme Genel Müdürlüklerinin ve Sivil Havacılık Genel Müdürlüğü'nün de mevzuatlarından kaynaklanan yetkileri bulunmaktadır.

3.1.2 Projeler

Kalkınma Bakanlığı 2012 Yatırım Programı içerisinde yer alan “**Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi**”

AFAD Başkanlığı'nın “Kamu Binalarının Sismik Önceliklendirilmesi Projesi”



3.2 Görev ve Sorumluluklar

Türkiye’de yapılması gereken çalışmalar konusunda aşağıdaki konular öne çıkmaktadır.

- Bireysel, kurumsal ve ulusal güvenliği ilgilendiren ve temel hak ve hürriyetlerle de ilişkilendirilebilecek bu önemli konuda yasal boşluklar ivedilikle giderilmelidir.
- Mevzuat çalışmaları çerçevesinde, kritik altyapılar, bu altyapılardan sorumlu kurum ve kuruluşlar ile bu kurum ve kuruluşların işbirliği ve koordinasyonu hususları netleştirilmelidir.
- Mevzuat çalışmalarının ardından ilgili kurum ve kuruluşlarca ülkemizin idari, hukuki ve teknik kapasitesi ile vatandaş-

larımızın konu ile ilgili farkındalığını artıracak çalışmalara ağırlık verilmelidir.

- Günümüzde tüm dünyada olduğu gibi ülkemizde de kritik altyapıların önemli bir kısmı özel sektör tarafından işletilmektedir. Bu itibarla, karar alma süreçlerine özel sektörün etkin katılımını sağlayacak yeni ve uygun bir kamu-özel sektör işbirliği modeli geliştirilmelidir.
- Kritik altyapıların ülke sınırlarını aşan etkisi göz önüne alınarak uluslararası işbirliği ve koordinasyonun teminine özel önem verilmelidir.

Şekil-4 Afet Yönetimi Döngüsü



- Bütün bakanlıkların kritik altyapı değerlendirilmesi için sorumlu en az 2 personel belirlemesi önerilmektedir.
- AFAD sorumlu personellerin kritik altyapı kavramını net şekilde anlamaları için bir çalıştay düzenlemelidir.

Sorumlu personeller, AFAD'ın müdahale sorumluluğunun olmadığı kapsamlar hariç tutulmak üzere bakanlıkları kapsamında yer alan kritik altyapı listelerini, önceden belirlenen formata uygun olarak hazırlayacak ve bu listeleri afad'a göndermelidir.

- AFAD bu listeleri değerlendirip, son halini vererek bakanlıkları bu nihai listeler hakkında bilgilendirmelidir.
- AFAD, kritik altyapı işletmecileri tarafından uygulanacak risk değerlendirme metodolojisini tarif edecek bir projeye

öncülük yapmalıdır.

- AFAD oluşturulan metodolojinin daha iyi kavranması için bakanlıklardaki sorumlu personellere yönelik bir çalıştay düzenlemelidir.
- Kritik altyapı işletmecileri, risk değerlendirme raporları ve risk uygulama planları hazırlayacak şekilde eğitilmelidir.
- Kritik altyapı rapor ve planları, ulusal koordinasyon ve ulusal ölçekte risk değerlendirmesi afad tarafından yapılması önerilmektedir.
- Söz konusu kritik altyapı listeleri, risk değerlendirme raporları ve risk uygulama planları yılda bir gözden geçirilerek sürdürülebilirliğinin sağlanmalıdır.

Ülkemizdeki Kritik Enerji Altyapıları
Scada ve Dağıtık Kontrol Sistemleri
Tarafından Kontrol Edilmektedir



3. ÜLKEMİZDEKİ MEVCUT DURUM



3.3 Uygulama Çerçevesi ve Detayları

Tablo 2. Kritik Altyapıların Korunması Uygulama Çerçevesi

Kritik Altyapı Sektörleri(KAS)	KAS Belirleme Sorumluluk	KAS Güvenlik Sorumluluk (Sektör Bazında)	KAS Güvenlik Sorumluluk (Tesis Bazında)	KAS Koordinasyon Sorumluluk
Enerji	EPDK, Enerji Bakanlığı, TAEK, AFAD	EPDK	İşletme Sahibi (Özel Sektör)	AFAD
Ulaştırma	UDHB, AFAD	UDHB,	İşletme Sahibi (Özel Sektör)	AFAD
Su Yönetimi/Barajlar	Orman ve Su İşleri Bakanlığı, AFAD	Orman ve Su İşleri Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Haberleşme	BTK, UDHB, AFAD	BTK, UDHB	İşletme Sahibi (Özel Sektör)	AFAD
Bankacılık ve Finans	BDDK,SPK, Hazine Müsteşarlığı, Maliye Bakanlığı, AFAD	BDDK,SPK, Hazine Müsteşarlığı, Maliye Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Kritik Kamu Hizmetleri	İçişleri Bakanlığı, AFAD	İçişleri Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Kritik Üretim/Ticari Tesisler	Bilim, Sanayi , ve Teknoloji Bakanlığı, Gümrük ve Ticaret Bakanlığı, AFAD TOBB	Bilim, Sanayi ve Teknoloji Bakanlığı, TOBB	İşletme Sahibi (Özel Sektör)	AFAD
Sağlık	Sağlık Bakanlığı, AFAD	Sağlık Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Tarım ve Gıda	GTHB, AFAD	GTHB	İşletme Sahibi (Özel Sektör)	AFAD
Kültür ve Turizm	Kültür ve Turizm Bakanlığı, AFAD	Kültür ve Turizm Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD



4. GEREKSİNİMLER VE EYLEMLER

GEREKSİNİM 1

Yetkili (sorumlu) Otoritelerin Belirlenmesi.

Eylem 1.1

Enerji, Ulaştırma, Su Yönetimi ve Barajlar, Haberleşme, Bankacılık ve Finans, Tarım ve Gıda, Kültür ve Turizm, Kritik Üretim/Ticari Servisler, Kritik Kamu Hizmetleri ve Sağlık kritik altyapı tanımının içinde bulunan sektörlerdir. Bu sektörlerden bazılarının denetleyici ve düzenleyici kurumları olmak ile birlikte, bazı sektörleri ise sorumlu bakanlık ve ilgili kamu kurum ve kuruluşları aracılığıyla, yönlendirmek gerekmektedir. Sektör bazında kritik altyapılar belirlenirken doğrudan sorumlu bir kamu kurum veya kuruluşu belirlenecektir.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
İlgili Kamu, Kurum ve Kuruluşları	AFAD	2016	İK

GEREKSİNİM 2

Yetkili koordinasyon otoritesinin belirlenmesi, iş bölümü bazında kritik altyapı sektörleri (KAS) belirlemede kullanılacak kıstasların tespit edilmesi.

Eylem 2.1

- Tüm sektörleri içine alan bir çalışmayı gerekli kılan bu düzenlemenin ulusal boyutta söz sahibi bir kurumsal yapı içinde çözülmesi gerekmektedir. Bu noktada afad konu ile yetkili ve sorumlu çatı kurum olarak görülmektedir. Özellikle;
- Kritik altyapı tesislerinin belirlenmesi için kriterlerin belirlenmesi ve envanterinin çıkarılması,
- Belirli altyapı sektörleri arasında bağımlılıkları belirlenmesi,
- AB çapında "Kritik Altyapı Koruma İletişim Grubu" irtibat noktaları ile koordinasyon
- "Ulusal Kritik Altyapı Koruma Programı'nın" ve sektöre özel kritik altyapı koruma programlarının detaylandırılması gibi çalışmalarını yürütmesi beklenmektedir.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
AFAD	İlgili Kamu, Kurum ve Kuruluşları	2016	İK

GEREK SINİM 3

Avrupa Birliđi Direktifinin uyumlaştırılması ile ilgili taslak yönetmelik hazırlanması ve kapsam, büyüklük ve zaman etkisi faktörlerinin göz önünde bulundurularak kritik altyapıların belirlenmesi ve koruyucu tedbirlerin artırılması.

Eylem 3.1

Avrupa Parlamentosu ve Avrupa Konseyinin 8 Aralık 2008 tarihli ve 114 sayılı “Avrupa Kritik Altyapılarının Belirlenmesi Ve Koruyucu Tedbirlerin Arttırılması” üzerine olan direktifi dikkate alarak kritik altyapılarını korumak amacı ile ilgili direktifin uyumlaştırma çalışmalarını başlatılması gerekmektedir. Bu konuda hukuksal destek kurumsal kapasite geliştirme, eğitim planlama gibi çalışmaları yapmak için bir “Teknik Danışmanlık” projesi yapılması uygun görülmektedir. Ayrıca ülkenin kritik altyapıları ile ilgili çalışmanın yazılımla desteklenerek bilgi güvenliği açısından da gerekli tedbirlerin alınması gerekmektedir.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
İlgili Kamu, Kurum ve Kuruluşları	AFAD	2016	Teknik Danışmanlık projesi yapılması İşbirliği ve Koordinasyon (İK),

GEREK SINİM 4

Kritik altyapıların etkin korunması, ulusal seviyede veya AB seviyesinde bütün ilgili paydaşlar arasında iletişim, koordinasyon ve işbirliği.

Eylem 4.1

Kritik altyapıların korunması öncelikle bir ulusal sorumluluktur. Sahiplerin ve işletmecilerin kendi varlıklarını koruma konusunda kendi kararlarını vermeleri ve planlarını yapmaları konusundaki yükümlülükleri ve sorumlulukları esastır.

Eylem 4.2

Kritik altyapıları korumayla ilgili bilgi paylaşımı güven ve gizlilik ortamında yürütülmelidir. Ulusal seviyede kritik altyapı koruma bilgileri gizli olmalı ve sadece bilmesi gerekenlere erişim hakkı verilmesi gerekli görülmektedir.

Eylem 4.3

AB'nin kritik altyapıları koruma çabalarının, ortak bir Kritik Altyapı Koruma Planı çerçevesinde (ortak hedefler, yöntemler vb.) en iyi uygulamaların ve uyum izleme mekanizmalarının paylaşımıyla güçlendirilmesi önerilmektedir.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
AFAD	İlgili Kamu Kurum ve Kuruluşları, Tüm KAS	2017	İK



4. GEREKSİNİMLER VE EYLEMLER

GEREKSİNİM 5

KAS'lerle ilgili işletmeci güvenlik planı yapılması.

Eylem 5.1

İşletmeci güvenlik planlama prosedürü, kritik altyapı varlıklarını ve bu altyapıların korunmaları için var olan ya da oluşturulan güvenlik çözümlerinin neler olduğunu tanımlayacaktır. Bir İşletmeci Güvenlik Planının ele alması gerektiği minimum içerik,

- Önemli varlıkların tanımları
- Büyük tehdit senaryoları, her bir değer için zayıf noktasını ve olası etkilerini temel alan bir risk analizinin gerçekleştirilmesi
- Karşıt önlemler ve prosedürlerin tanımları,
- Seçimleri ve önem sırasına göre konumlandırılmaları,
- Her daim kullanılabilir olacak olan vazgeçilmez güvenlik yatırımları ve araçlarını belirleyen kalıcı güvenlik ölçütleri. (Bu madde, teknik ölçütler (tespit, erişim kontrol, koruma ve engelleme araçlarının kurulumu), organizasyonel ölçütler (uyarılar ve kriz yönetim prosedürleri), kontrol ve doğrulama ölçütleri, iletişim, farkındalık artırımı ve eğitim, bilgi sistemleri güvenliği gibi genel ölçütlerle ilgili bilgileri kapsayacaktır.)

- Farklı risk ve tehdit seviyelerine göre aktive edilebilecek dereceli güvenlik ölçütleri.

Her bir sektörden sorumlu kamu kurum ve kuruluşu, sorumluluk alanı içerisindeki kritik altyapı olarak belirlenen altyapının İşletmeci Güvenlik Planına sahip olup olmadığını ve yukarıda belirtilen konulara değinen eşdeğer ölçütleri uygulayıp uygulamadığını değerlendirecektir.

GEREKSİNİM 6

Güvenlik İrtibat Görevlisi atamak.

Eylem 6.1

Güvenlik İrtibat Yetkilisi, Kritik Altyapı Sahibi/İşletmecisi ile devlet otoritesi arasında güvenlikle ilgili konularda irtibat noktası görevi görecektir.

Eylem 6.2

Her bir ilgili kamu kurum ve kuruluşu sorumluluk alanında yer alan kritik altyapı olarak belirlenmiş varlık/tesisin Güvenlik İrtibat Yetkilisine ya da eşdeğerine sahip olup olmadığını değerlendirecektir. Bu tür bir Güvenlik İrtibat Yetkilisinin yürürlükte olduğunu ya da eşdeğerinin mevcut olduğunu tespit etmesi durumunda, daha başka bir yapılandırma gerekli olmayacaktır.

Eylem 6.3

Kamu kurum ve kuruluşunun sorumluluğunda bulunan kritik altyapıda, belirlenen bir Güvenlik İrtibat Yetkilisinin ya da eşdeğerinin mevcut olmadığını tespit etmesi durumunda, Güvenlik İrtibat Yetkilisinin belirlenmesi için gerekli olan her türlü düzenlemeyi hazırlayacaktır.

Eylem 6.4

Güvenlik İrtibat Görevlisi ile ilgili devlet otoritesi arasında uygun bir iletişim mekanizması kurulacaktır. Bu iletişim mekanizması; önemli ve gizli bilgilere erişim konusundaki ulusal gereklilikleri ihlal etmeyecektir.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
-----------------	-------------------	--------------------	------------

İlgili Kamu Kurum ve Kuruluşları Tüm KAS İşletmecileri

AFAD

2018

İK

GEREKSİNİM 7

Eğitim programı oluşturulması ve uygulanması.

Eylem 7.1

Yetkili devlet otoritesi, sorumluluğunda bulunan kritik altyapı işletmecisi/sahibine gerekli eğitimleri verecektir.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
-----------------	-------------------	--------------------	------------

İlgili Kamu Kurum ve Kuruluşları Tüm KAS İşletmecileri

AFAD

2017

İK, KG

GEREKSİNİM 8

Ulusal düzeydeki kritik altyapıların korunması amacı ile Kritik Altyapı Koruma Planı hazırlanması.

Eylem 8.1

Kritik altyapıların korunmasıyla ilgili en iyi uygulamalar hakkında gelişmiş ve doğru bilgi ve farkındalık, paydaşlar arası diyalog, kritik altyapı meseleleri hakkında farkındalık artışı ve daha iyi odaklanmış eğitim, araştırma ve geliştirme gibi çalışmalar yapılması gereklidir. İşletmeci Güvenlik Planı çalışmalarının entegre edilerek ulusal düzeyde kritik altyapı koruma planı için çalışmalar yapılmalıdır.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
-----------------	-------------------	--------------------	------------

AFAD

İlgili Kamu Kurum ve Kuruluşları, Tüm KAS İşletmecileri

2018

İK



4. GEREKSİNİMLER VE EYLEMLER

GEREKSİNİM 9

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

Eylem 9.1

KAUBA, kritik altyapıların korunması konusunda bilgi alışverişini sağlayan bir forum olup, üye ülkelere ve Komisyona kritik altyapılara yönelik anlık riskler ve tehditler üzerine uyarılar yollama imkânı sağlamaktadır. KAUBA üye ülkelerin işbirliğini kolaylaştıracak bir bilgi sistemi sağlayarak ve AB içinde kritik altyapılar hakkında bilgilerin aranması için hızlı ve verimli bir yol sunarak kritik altyapıların korunmasına ilişkin tedbirlerin geliştirilmesine katkıda bulunmaktadır.

KAUBA yapısında yer alan her bir üye ülke bir irtibat noktası olarak görev yapan KAUBA yöneticisi atar. Ülkemizde de bu çalışmalara entegre olacak hazırlıkların yapılması gerekmektedir.

GEREKSİNİM 10

Raporlama.

Eylem 10.1

Her bir kamu kurum ve kuruluşu kendi sorumluluğu bünyesinde bulunan kritik altyapı unsurunu belirlemesinin ardından bir yıl içerisinde tekrardan bir değerlendirme yapacaktır. Yapılan bu değerlendirme sonucunda güncel bilgiler AFAD ile paylaşılacaktır.

Sorumlu Kuruluş	İlgili Kuruluşlar	Gerçekleşme Dönemi	Eylem Türü
AFAD, Sektör Düzenleyici Kurumlar	İlgili Bakanlık, Tüm KAS işletmecileri	2018	İK





KATKIDA BULUNANLAR

Yürütücü Ekip Üyeleri

Ad Soyad	Ünvan	Kurum
Mehmet Akif DANACI	Daire Başkanı	AFAD- Planlama ve Zarar Azaltma Dairesi
Mehmet Akif ALKAN	Grup Başkanı	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Ahmet Tayfun Okşin	AFAD Uzman Yardımcısı	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Osman GÜLEŞEN	AFAD Uzman Yardımcısı	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Öznur ÇAĞLAR	AFAD Uzman Yardımcısı	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Betül KURADA	AFAD Uzman Yardımcısı	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Dr. Devrim BAĞLA	Mühendis	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Dr. Evren TANRIVERDİ	Mühendis	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Mehmet Fatih ŞEN	AFAD Uzman Yardımcısı	AFAD- Teknolojik Afetler Risk Azaltma Çalışma Grubu
Sinem YİĞİTER ATAĞAN	AFAD Uzman Yardımcısı	AFAD- KBRN Çalışma Grubu
Yasin GENÇ	AFAD Uzman Yardımcısı	AFAD- KBRN Çalışma Grubu

Katkıda Bulunanlar

Ad Soyad	Ünvan	Kurum
Fikret OTTEKİN	Başuzman Araştırmacı	Siber Güvenlik Enstitüsü
Bilge KARABACAK	Müdür Yardımcısı	Tübitak-Siber Güvenlik Enstitüsü
Bahtiyar BİRCAN	Başuzman Araştırmacı	Tübitak-Siber Güvenlik Enstitüsü
Doç. Dr. Mitat ÇELİKPALA	Akademisyen	Kadir Has Üniversitesi
Didem AKPAK ERGEN	Uzman	Kamu Düzeni ve Güvenliği Müsteşarlığı
Saffet GÜLEP	Daire Başkanı	Emniyet Genel Müdürlüğü
Celil ŞAHİN	Yüzbaşı	Jandarma Genel Komutanlığı
Fahri KOÇAK	Subay	Jandarma Genel Komutanlığı



KAYNAKLAR

1. Communication from the Commission 2006/12/12 “On a European Programme for Critical Infrastructure Protection”
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF>
2. Council Directive 2008/114/EC of 8 December 2008 “On The Identification and Designation of European Critical Infrastructures and the Assessment of The Need To Improve Their Protection” (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=O-J:L:2008:345:0075:0082:EN:PDF>)
3. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
4. Council Decision 2007/124/EC of 12 February 2007, “Establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme ‘Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks”
5. Proposal for a Council Decision of 27 October 2008 on a Critical Infrastructure Warning Information Network (CIWIN) [COM(2008) 676 final
6. Green Paper of 17 November 2005 on a European programme for critical infrastructure protection [COM(2005) 576 final
7. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Preparedness and consequence management in the fight against terrorism [COM(2004) 701

8. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – “Prevention, preparedness and response to terrorist attacks” [COM(2004) 698 final – Official Journal C 14 of 20.1.2005]
9. REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000 “On the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”
10. SWD(2012) 190 final, COMMISSION STAFF WORKING DOCUMENT “On The Review Of The European Programme For Critical Infrastructure Protection (EPCIP)”
11. SWD(2013) 318 final, COMMISSION STAFF WORKING DOCUMENT “On a New Approach to The European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure”



T.C.
BAŞBAKANLIK
Afet ve Acil Durum Yönetimi Başkanlığı