Güvenlik Savunma ve Emniyet
Yönetişimi Akademisi
Security & Defense Governance Academy

BİLGİ NOTU

GUSEYAD | AKADEMİ
GUSEYAD | ACADEMY

Afetlerde Kritik Altyapılı Tesis Yönetiminde Siber Güvenlik

Eylül 2025
İstanbul / TÜRKİYE

www.guseyadakademi.org

Afetlerde Kritik Altyapılı Tesis Yönetiminde Siber Güvenlik

Uzm. **Burak Soner BOZKURTLAR** *

BİLGİ NOTU / EYLÜL 2025

GUSEYAD | AKADEMİ

* İstanbul Üniversitesi Açık ve Uzaktan Eğitim Fakültesi (AUZEF) Acil Yardım ve Afet Yönetimi (AYAY) Lisans Tamamlama Programı / Ders Veren Uzman

Yayın Tarihi: Eylül 2025

GUSEYAD / AKADEMİ

E-Posta: bilgi@guseyadakademi.org

''Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5'inci maddesinin 2'nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir.''

AFETLERDE

KRİTİK ALTYAPILI TESİS YÖNETİMİNDE

SİBER GÜVENLİK

Resim için bkz.: https://guseyadakademi.org/?p=86

Kritik altyapılar çökerse, sadece binalar değil; umutlar, güven ve devlet aklı da enkaz altında kalır.

Burak Soner Bozkurtlar

Giriş

Acil yardım ve afet durumları, sadece fiziksel altyapıyı değil, aynı zamanda **dijital sistemleri** de kesintiye uğratarak, geniş çapta bireysel ve toplumsal travmalara yol açan, çok boyutlu krizlerdir.

Ülke / toplum / kamu kurumu / özel sektör kuruluşları açısından **stratejik öneme sahip** olan "**kritik altyapılı tesisler**", afetler sırasında yalnızca doğal risklerle değil, aynı anda gerçekleşebilecek **siber tehditlerle** de karşı karşıya kalırlar. Bu tesislerde dikkat edilmesi gereken öncelikli husus, **siber dayanaklılığı da kapsayan bir "iş sürekliliği" anlayışının** sağlanmasıdır. Bu ise, yalnızca teknik bilgi değil, aynı zamanda **siber güvenlik olay yönetimi, dijital farkındalık ve kriz anı refleksi** gerektiren, uzmanlık isteyen bir alandır.

Bu bölümde, **acil yardım ve afet durumlarında kritik dijital altyapıların korunması, siber saldırı türleri, olay müdahale süreçleri, yapay zekâ destekli güvenlik çözümleri, sertifikasyon ve regülasyon süreçleri** gibi başlıklar altında, dikkat edilmesi gereken noktalar detaylı şekilde ele alınacaktır.

Çağdaş bir yaklaşım olarak "**siber güvenlik yönetişimi**" kavramı vurgulanacak ve bu yönetişimin bir alt bileşeni olarak "**coğrafi bilgi sistemleri**" nin **"siber farkındalık"** la nasıl entegre çalışabileceği gösterilecektir.

Etkin bir acil yardım ve afet yönetimi için yalnızca fiziksel müdahale değil, "**dijital müdahale kapasitesi" nin** de yüksek olması gerekmektedir. Bu bağlamda **lojistik güvenliği** ve **veri bütünlüğünün korunması**, kritik başarı faktörlerinden biridir.

Burada "**siber afet lojistiği**" kavramı ön plana çıkmaktadır. İşletme lojistiği ile afet lojistiği benzer süreçleri barındırsa da, dijital tehditler nedeniyle bilgiye erişim, veri yönetimi ve iletişim altyapısı konularında daha yoğun zorluklarla karşılaşılması muhtemeldir.

Acil yardım ve afet durumu ortaya çıkmadan önce yapılması gereken dijital hazırlıkların **ne düzeyde stratejik, test edilmiş ve işlevsel olduğu**, kriz anı geldiğinde anlaşılacaktır. Plansız, korumasız ve güncellenmemiş dijital altyapıların, bir felaketi çok daha yıkıcı hale getirebileceği unutulmamalıdır.

Bu süreçte en önemli bileşenlerden biri, fiziksel güvenlik kadar **siber güvenliğin de eş zamanlı olarak tesis edilmesidir.** Etkin bir siber güvenlik sistemi ise, ancak **strateji, mühendislik ve mimari bilgi ile birlikte** hayata geçirilebilir.

Hâlihazırda kullanılmakta olan **bilgi teknolojileri, otonom sistemler, yapay zekâ uygulamaları ve coğrafi bilgi sistemleri**, afet yönetimi süreçlerine entegre edilerek, yalnızca lojistik akışı değil; **afetzedelerin dijital mahremiyeti, veri güvenliği ve iletişim altyapılarının sürekliliğini** de güvence altına alabilir.

Bu faaliyetleri yürüten kamu ve özel sektör paydaşlarının, yalnızca fiziksel güvenlik değil, aynı zamanda **siber güvenlik sertifikasyonu ve dijital altyapı sağlayıcılarının akreditasyonu** gibi niteliksel yeterliliklere sahip olması elzemdir.

Acil yardım ve afet durumlarında kritik dijital altyapının korunmasına örnek olarak, bu bölümde "**nükleer tesislerde siber güvenlik**" konusu özel bir başlık altında değerlendirilecektir.

Son olarak, **siber güvenlik yönetişiminin geleceği**, "***dijital egemenlik***" **politikaları** ve **yerli-milli yazılım çözümleri** çerçevesinde analiz edilerek, bu alanda kamu ve toplumun nasıl daha dirençli hale getirilebileceği tartışmaya açılacaktır.

1. Kritik Altyapıların Tanımı ve Afet Bağlamında Siber Güvenlik Riskleri

Kritik altyapılar, bir ülkenin ulusal güvenliği, ekonomik sürekliliği, kamu sağlığı ve güvenliği açısından **hayati öneme sahip olan sistem ve varlıklar** olarak tanımlanır. Bunlar; enerji, su, haberleşme, ulaşım, sağlık, finans, gıda, kamu güvenliği ve bilgi teknolojileri gibi sektörleri kapsar.

Afet ve acil durumlar sırasında bu altyapıların işlerliğini koruması, hem kurtarma faaliyetlerinin etkinliğini artırır hem de **toplumsal düzenin devamı** açısından belirleyici rol oynar.

Afet Bağlamında Siber Güvenlik Riskleri

Afet zamanlarında fiziksel zararların yanı sıra **siber tehditler** de **büyük bir risk** oluşturmaktadır. Kritik altyapılara yönelik planlı veya rastlantısal siber saldırılar, afet müdahale kapasitesini ciddi şekilde sekteye uğratabilir. Örneğin:

- **Elektrik şebekesinin çökmesi**, hastanelerin ve haberleşme sistemlerinin durmasına yol açabilir.
- **İletişim altyapılarının hedef alınması**, AFAD, UMKE veya itfaiye ekiplerinin koordinasyonunu bozabilir.
- **SCADA sistemlerine yapılan saldırılar**, barajlar veya doğal gaz sistemlerinde zincirleme felaketlere neden olabilir.

Bu riskler, sadece teknolojik bir tehdit değil; aynı zamanda **insani, hukuki ve yönetsel bir zafiyet** alanı oluşturur.

Güncel Örnek

2021 yılında ABD' ndeki **Colonial Pipeline** saldırısı, yalnızca ekonomik değil, aynı zamanda psikolojik bir kriz yaratmıştır. Enerji altyapısına yönelik bu saldırının bir benzerinin, afet sırasında Türkiye' de yaşanması durumunda oluşacak etkiler **çok daha yıkıcı** olacaktır.

Ulusal Güvenlik ve Yönetişim Açısından Önemi

Kritik altyapılara yönelik siber tehditler, sadece kurumlar arası bir mesele değil; **devletin güvenlik refleksi** içinde ele alınması gereken bir meseledir. Bu noktada, ulusal siber güvenlik stratejileri ile **Kamu - Özel İş Birliği (KÖİ)** mekanizmalarının geliştirilmesi, hem müdahale hem de dayanıklılık bakımından hayati rol oynar.

Afetlerde fiziksel dayanıklılığın ötesine geçerek, **siber dayanıklılık kavramı** kritik hale gelmiştir. Bu bağlamda, afet yönetimi planlarının sadece enkaz kaldırmaya değil, **veri yedekleme, SCADA güvenliği, iletişim sürekliliği ve tehdit analizlerine** de entegre edilmesi gerekmektedir.

1.1. Kritik Altyapının Kapsamı, Türleri ve Türkiye' deki Düzenleyici Çerçeve

Kritik altyapılar, toplumların güvenliği, sağlığı, refahı ve ekonomik istikrarı açısından hayati öneme sahip, kesintisiz işleyişi zorunlu sistem ve tesislerdir. Avrupa Birliği başta olmak üzere birçok ülkede kritik altyapı, bozulduğunda veya tahrip edildiğinde geniş çaplı toplumsal, ekonomik ve yönetsel krizlere yol açabilecek fiziksel ve dijital varlıklar olarak tanımlanmaktadır.

Bu kapsamda; "**kritik altyapılar**" genel olarak **aşağıdaki başlıklar altında sınıflandırılmaktadır:**

- **Enerji Sistemleri:** Elektrik üretimi, iletimi ve dağıtımı; petrol ve doğal gaz altyapısı
- **Bilgi ve İletişim Teknolojileri (BİT):** Telekomünikasyon, veri merkezleri ve internet altyapısı
- **Finansal Sistemler:** Bankacılık, borsa ve ödeme sistemleri
- **Ulaşım:** Karayolu, demiryolu, hava ve deniz taşımacılığı altyapısı
- **Su ve Atık Yönetimi:** İçme suyu temini, kanalizasyon ve arıtma sistemleri
- **Sağlık Altyapısı:** Hastaneler, ilaç tedarik zinciri, acil müdahale birimleri
- **Kamu Yönetimi:** Kritik devlet kurumları ve elektronik devlet hizmetleri

Türkiye'de **kritik altyapılar; 20.06.2013 tarihli ve 2 sayılı Siber Güvenlik Kurulu Kararı ile altı sektörde sınıflandırılmıştır:**

1. Elektronik Haberleşme
2. Enerji
3. Bankacılık ve Finans
4. Kritik Kamu Hizmetleri
5. Ulaştırma
6. Su Yönetimi

Bu sektörlerin korunması, **AFAD, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu (BTK)** gibi kurumların koordinasyonunda yürütülmektedir. Ayrıca **TÜBİTAK** tarafından 2019' da yayınlanan kılavuzda kritik altyapılar, işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybı, büyük ölçekli ekonomik zarar veya kamu düzeninin bozulmasına yol açabilecek sistemler olarak tanımlanmıştır.

1.2. Doğal Afetler Sonrası Siber Tehditlerin Artışı ve Risk Senaryoları

Afetlerin ardından fiziksel hasarın yanı sıra dijital sistemlerde de büyük zafiyetler oluşabilmektedir. Kritik altyapılar, özellikle de bilgi ve iletişim sistemlerine bağımlı hale geldikçe, doğal afetler siber saldırılar için "fırsat penceresi" yaratmaktadır.

Afet Sonrası Ortaya Çıkabilecek Siber Tehditler:

- **İletişim altyapısının çökmesi:** Acil müdahale ve koordinasyonun aksaması
- **SCADA sistemlerinin manipülasyonu:** Enerji, su ve ulaşım gibi alanlarda kriz derinleşebilir
- **Veri hırsızlığı ve fidye yazılımları:** E-devlet sistemleri, sağlık bilgileri, yardım kayıtları hedef haline gelebilir
- **Dezenformasyon kampanyaları:** Sosyal medya ve mesajlaşma sistemleri üzerinden panik yaratma girişimleri
- **Kritik hizmetlerin engellenmesi:** Hastaneler, ulaşım merkezleri, elektrik santralleri vb. yerlerin dijital kontrol sistemlerine müdahale

Risk Senaryoları Örnekleri:

- **Deprem sonrası elektrik şebekesini yöneten sistemlere sızılarak kontrol kaybı yaşanması**
- **Sel sonrası su arıtma tesislerinin siber saldırıya uğrayarak içme suyunun kirlenmesi**
- **Afetzedeler için kurulan geçici barınma ve yardım sistemlerine yönelik veri manipülasyonu**

Afet anında güvenlik açıklarının artması, saldırganlara çeşitli istismar alanları sunmaktadır. Bu nedenle, afet yönetim planlarına **siber güvenlik senaryolarının da entegre edilmesi**, sadece fiziksel güvenliği değil; **veri güvenliği, bilgi bütünlüğü ve "*kamu otoritesinin devamlılığı*" açısından da kritik öneme** sahiptir.

Sonuç olarak; kritik altyapıların korunması yalnızca fiziksel önlemlerle sınırlı kalmamalıdır. Afet anlarında ve sonrasında ortaya çıkabilecek siber riskler, çok katmanlı bir güvenlik mimarisi ile değerlendirilmelidir. Bu bağlamda hem **yerli teknolojilerin geliştirilmesi** hem de **ulusal siber güvenlik stratejilerinin afet senaryoları ile entegre edilmesi**, sürdürülebilir güvenlik yönetişimi için kaçınılmazdır.[1]

2. Afet Anında ve Sonrasında Kritik Tesislere Yönelik Siber Saldırı Türleri

2.1. DDoS, SCADA Saldırıları, Fidye Yazılımları ve İç Tehditler

Afet anlarında fiziksel hasarın ötesinde, dijital altyapılar da önemli ölçüde etkilenmektedir. Kritik tesisler bu tür zamanlarda dijital savunmasızlık yaşadıklarında, çok katmanlı saldırı riskiyle karşı karşıya kalmaktadır. Bu kapsamda dört temel siber saldırı türü öne çıkmaktadır:

2.1.1. DDoS (Dağıtık Hizmet Engelleme) Saldırıları

Afet anında en yaygın görülen saldırı türlerinden biridir. Kritik iletişim ve haberleşme altyapılarına yoğun trafik gönderilerek sistemlerin hizmet dışı bırakılması hedeflenir. Acil müdahale sistemleri, afet koordinasyon merkezleri ve yardım kuruluşlarının çevrimiçi altyapıları etkilenebilir.

2.1.2. SCADA ve Endüstriyel Kontrol Sistemlerine Saldırılar

SCADA sistemleri, enerji santralleri, su arıtma tesisleri, nükleer santraller gibi tesislerin kontrol mekanizmalarını yönetir. Afet sonrası fiziksel hasar ve bilgi kargaşası, saldırganlar için bu sistemlere sızmak adına cazip bir fırsat oluşturur. SCADA sistemlerinin uzaktan kontrolüne yönelik saldırılar, zincirleme felaketlere neden olabilir.

2.1.3. Fidye Yazılımları (Ransomware)

Afet sonrası yeniden yapılandırılmaya çalışan sistemler fidye yazılımları için uygun hedefler haline gelir. Kritik verilerin şifrelenmesi ve karşılığında fidye talep edilmesi, kurtarma ve yeniden başlatma süreçlerini felç edebilir.

2.1.4. İç Tehditler

[1] Bu bölümün hazırlanmasında büyük ölçüde aşağıdaki makaleden yararlanılmıştır. Bkz.; ***Tanrıverdi, E., Kurada, B., Şen, M. F., Demirkol Kılıç, E. (2023)***, Türkiye'de Afet Yönetimi Bağlamında Kritik Altyapı Kavramı, Ankara Üniversitesi Çevrebilimleri Dergisi, 10(1), 1-9.

Kurum içinde yer alan, bilgiye doğrudan erişim yetkisi olan kişilerce gerçekleştirilen kasıtlı veya ihmale dayalı eylemler afet sonrası ciddi riskler oluşturabilir. Özellikle bilgi kargaşası dönemlerinde yetki ve denetim zaafları, iç tehditlerin artmasına neden olabilir.

2.2. Örnek Olaylar: Elektrik Kesintisi, Su Arıtma Tesisi Sabotajı

2.2.1. Elektrik Kesintisi: Ukrayna (2015)

Ukrayna' da yaşanan bir siber saldırı sonucunda elektrik şebekesine bağlı üç farklı enerji dağıtım şirketi hedef alınmış, yaklaşık 230.000 kişinin saatlerce elektriksiz kalmasına neden olunmuştur. Saldırı, sosyal mühendislik ile elde edilen kimlik bilgilerinin SCADA sistemlerine sızmak amacıyla kullanılması sonucu gerçekleşmiştir.[2]

2.2.2. Su Arıtma Tesisi Sabotajı: Florida, ABD (2021)

Oldsmar kentinde bir su arıtma tesisine uzaktan sızılıp suya tehlikeli miktarda sodyum hidroksit (kostik soda) eklenmeye çalışılmıştı. Neyse ki bir çalışan ekran hareketlerini fark ederek müdahale etti. Bu olay, SCADA sistemlerinin sızılabilirliğini ve fiziksel zarara dönüşme potansiyelini ortaya koymuştur.[3]

2.2.3. Ransomware: WannaCry Saldırısı (2017)

WannaCry zararlı yazılımı, NHS (Birleşik Krallık Ulusal Sağlık Hizmeti) dahil olmak üzere kritik sağlık altyapısını felç etti. Randevu sistemleri, acil servisler, hasta bilgileri gibi sistemler saatlerce kullanılamaz hale geldi.[4]

2.2.4. Coğrafi Bilgi Sistemleri (CBS) ile Desteklenen Savunma

Yukarıdaki siber tehditlerin konumsal olarak modellenmesi ve senaryolaştırılması, CBS kullanımı ile mümkün hale gelmektedir. CBS, jeo-uzamsal analizler sayesinde:

- Kritik altyapıların etkileşim haritalarını çıkarabilir,
- Riskli bölgelerdeki SCADA sistemlerini coğrafi olarak etiketleyebilir,
- Saldırı öncesi ve sonrası etki analizi yapabilir,

[2] Ukrayna'da elektrik dağıtım sistemi siber saldırıya uğradı - Teknoloji Haberler, 16 Haziran 2025 tarihinde erişildi.

[3] Hack of Florida Water Treatment Plant Exposes Seriousness of U.S. Cyber Threat - Yandex Video aramada çevrimiçi izle, 16 Haziran 2025 tarihinde erişildi.

[4] https://www.drozdogan.com/wanna-cry-virusu-ile-ingiltere-saglik-sistemine-siber-saldiri/, 16 Haziran 2025 tarihinde erişildi.

- Afet anında işleyen sistemlerin dijital ikizlerini sunabilir.

Böylelikle, afet durumlarında siber tehditlerin izlenmesi, yanıtlanması ve riskin azaltılması için coğrafi tabanlı karar destek sistemleri etkili bir çözüm aracı haline gelmektedir.

3. Kritik Altyapı Tesislerinde Siber Dayanıklılık: Olay Müdahale Ve Kriz İletişimi

Afetlerin hemen sonrasında yaşanan kaos ortamı, yalnızca fiziksel hasarlarla sınırlı kalmayıp dijital sistemlerde de ciddi kırılganlıklara neden olmaktadır. Bu bağlamda kritik altyapıların siber dayanıklılığı, yalnızca teknik önlemlerle değil; olay müdahale planları, kriz iletişim sistemleri ve Siber Operasyon Merkezleri (Security Operations Center) / SOM (SOC) 'nin koordinasyonuyla mümkün hale gelmektedir.

3.1. Afet Senaryolarında Olay Müdahale Planlaması ve Siber Operasyon Merkezi / SOM (Security Operations Center / SOC) Desteği

Afet senaryolarında olay müdahale planlaması, kriz anı görev dağılımları ve iletişim sürekliliği esastır. Siber Operasyon Merkezi /SOM (Security Operations Center / SOC), tehdit algılama ve hızlı yanıt verme kapasitesiyle bu süreçte anahtar rol üstlenmektedir.

Siber Operasyon Merkezleri, afet anında devreye girerek;

- Sistem günlüklerini analiz eder,
- Şüpheli trafik ve saldırı örüntülerini belirler,
- Anlık tehdit istihbaratı ile müdahale sürecini yönlendirir,
- Kurumsal iletişim sistemlerini izler ve korur,
- Kritik sistemlerin çevrimdışı yedeklerine geçişi sağlar.

3.2. Siber Afet Tatbikatları ve Haberleşme Kanallarının Korunması

Kurumların siber dayanıklılığı artırması için, doğal afet senaryoları da dahil olmak üzere tatbikatlar düzenlemesi hayati önem taşır. Bu tatbikatlarda şu unsurlar test edilmelidir:

- Kriz senaryolarına göre olay müdahale zaman çizelgesi,
- Kurumsal iletişim kanallarının (VPN, acil iletişim hatları vb.) sürekliliği,
- Kritik verilerin yedeklenme ve yeniden erişim süresi (RTO/RPO),
- SOC personelinin afet anında görev alabilirliği,

- Dış müdahale ekipleriyle koordinasyon kapasitesi.

Tatbikatlar yalnızca teknik personelle sınırlı kalmamalı; yönetim, halkla ilişkiler, hukuk ve insan kaynakları gibi birimlerin de katılımıyla bütüncül bir kriz yönetim kapasitesi geliştirilmelidir.

Afet anında bilgi kirliliği, panik ve yanlış yönlendirme risklerini azaltmak için kriz iletişim planlarının önceden hazırlanması gereklidir. Bu planlar kapsamında:

- Kurum içi ve kurum dışı tüm haberleşme kanalları (acil SMS sistemleri, mobil uygulamalar, e-posta sunucuları) siber saldırılara karşı yedekli ve şifreli hâle getirilmelidir.
- Kritik görevli personelin yalnızca yetkili cihazlarla sisteme erişimi sağlanmalıdır.
- Kriz iletişim sorumluları önceden belirlenip medya ile iletişim noktaları tanımlanmalıdır.

Kritik altyapılarda siber dayanıklılık, yalnızca teknoloji değil; **disiplinler arası iş birliği**, **kriz senaryolarına hazırlık** ve **sürekli tatbikatlarla** sağlanabilir. **Afet sonrası siber kırılganlıkların** önüne geçmek için **kurumlar arası koordinasyonun güçlü tutulması**, **SOM (SOC) 'nin görev başında olması** ve **kriz iletişiminin önceden planlanmış olması** gereklidir. **Türkiye'nin dijital güvenliği**, afet yönetim stratejileriyle **eşgüdüm** içinde geliştirildiğinde, **siber vatanın bekası** ve **stratejik direnci** sağlanmış olur. Bu bütünsel yaklaşım, sadece bugün için değil, gelecekte karşılaşılabilecek hibrit tehditler için de Türkiye'yi **hazır ve güçlü** kılacaktır.

4. Kritik Tesislerde Siber Güvenlik Sertifikasyonu ve Regülasyonlar

Kritik altyapıların siber tehditlere karşı korunması, yalnızca teknik önlemlerle değil; aynı zamanda ulusal ve uluslararası düzeyde kabul görmüş standartlar, kurumsal denetim süreçleri ve yasal çerçevelerle desteklenmektedir. Türkiye 'de bu alanda son dönemde atılan yapısal adımlar, küresel düzeyde artan siber tehditlere karşı daha dirençli bir altyapının kurulmasını hedeflemektedir.

4.1. ISO/IEC 27001, NIS2 Direktifi, Türkiye Ulusal Siber Güvenlik Stratejisi

ISO / IEC 27001 standardı, bilgi güvenliği yönetim sistemi kurmak isteyen kurumlar için küresel ölçekte kabul görmüş bir çerçeve sunmaktadır. Bu standart sayesinde, kurumların bilgi varlıkları tanımlanır, riskler analiz edilir ve önleyici mekanizmalar sistematik şekilde

devreye alınır. Özellikle kritik tesislerde bu sistemlerin uygulanması, iç denetim süreçlerini dijital güvenlik odaklı hale getirir.

Avrupa Birliği' nin yürürlüğe koyduğu NIS2 Direktifi (Network and Information Security), kritik sektörlerde faaliyet gösteren kurumların; risk değerlendirmesi, olay bildirimi ve temel hizmetlerin sürekliliğini sağlama yükümlülüklerini kapsamlı biçimde ele almaktadır. Türkiye gibi AB ile ekonomik ve dijital anlamda entegre ülkelerde, bu standartlara uyum, hem uluslararası itibar hem de teknik hazırlık açısından elzemdir.

Türkiye'de dijital altyapının korunması amacıyla geliştirilen **Ulusal Siber Güvenlik Stratejisi** belgesi, 2020'li yılların başından itibaren belirli aralıklarla güncellenerek kurumlara rehberlik etmektedir. Bu stratejide kamu-özel sektör iş birliğine, yerli teknolojilerin teşvikine ve siber olaylara müdahale ekiplerinin kapasite artırımlarına öncelik verilmiştir.

Bu stratejinin uygulanmasına ivme kazandıran en önemli adımlardan biri de **Siber Güvenlik Başkanlığı** 'nın kurulması olmuştur. Yeni kurulan bu başkanlık, ülke genelinde siber güvenlik politikalarının belirlenmesi, kurumlar arası koordinasyonun sağlanması ve kriz anlarında karar verici yapıların desteklenmesi açısından hayati bir konumdadır.

4.2. Denetim Süreçleri ve Akreditasyon Örnekleri

Kritik tesislerde görev alacak teknik personelin sadece teknik değil; etik bilgiyle de donatılması gereklidir. Bu doğrultuda, **TSE tarafından verilen Beyaz Şapkalı Hacker Eğitimleri** ve bilgi güvenliği uzmanlığı programları, sektöre nitelikli insan kaynağı kazandırmaktadır. Bu eğitimler, kurumların sızma testi, zafiyet analizi ve olay müdahalesi gibi süreçlerde kendi iç kaynaklarını oluşturmasına olanak tanır.

Ayrıca, ulusal düzeyde kurumsal denetim süreçlerinde kullanılmak üzere **TSE, TÜRKAK ve sektörel düzenleyici kurumlar** tarafından belirlenen denetim kriterleri ve akreditasyon süreçleri sayesinde hem özel hem kamu kurumlarının bilgi güvenliği uygulamaları sürekli olarak kontrol altında tutulmaktadır.

Siber tehditlerin giderek karmaşıklaştığı bir çağda, kritik tesislerin korunması için sadece teknik önlemler değil, organizasyonel yapılar, sürdürülebilir sertifikasyon süreçleri ve yerli-yabancı mevzuata uyum sağlayan bir iç denetim kültürü de geliştirilmelidir. Kurumsal direnç, bu üç sütun üzerine inşa edilmelidir:

- Uluslararası standartlarla uyum (örneğin ISO/IEC 27001, NIS2),
- Ulusal strateji ve yönetişim (örneğin Siber Güvenlik Başkanlığı),
- Eğitimli ve sertifikalı insan kaynağı (örneğin TSE Beyaz Şapkalı Hacker programları).

5. Otonom Sistemler ve Yapay Zekâ Tabanlı Siber Güvenlik Çözümleri

Afet anlarında ve sonrasında, veri toplama, müdahale koordinasyonu ve sistem sürekliliği gibi görevler için kullanılan otonom teknolojiler; bir yandan operasyonel avantajlar sağlarken, diğer yandan siber tehditlere açık yeni yüzeyler oluşturmaktadır. ***İnsansız Hava Araçları (İHA)***[5], sensör ağları, uzaktan erişimli kontrol sistemleri ve yapay zekâ tabanlı karar destek sistemleri; modern kriz yönetiminin dijitalleşmesinde temel taşlar haline gelmiştir.

5.1. İHA' lar, Sensörler, Uzaktan Erişimli Sistemlerin Güvenliği

İHA'lar, robotik araçlar ve otonom keşif sistemleri; doğal afet bölgelerinde arama-kurtarma, hasar tespiti, veri aktarımı gibi kritik görevlerde kullanılmaktadır. Ancak bu sistemlerin GPS, LTE/5G, Wi-Fi ve RF protokolleriyle haberleşiyor olması, saldırganların sinyal bozma (jamming), sahte sinyal üretme (spoofing) veya cihaz ele geçirme (hijacking) gibi yöntemlerle müdahale etmesini mümkün kılar.

Benzer şekilde, çevresel veri toplayan sensör ağları ve uzaktan erişimli kontrol sistemleri (örneğin su pompalama istasyonları, enerji anahtarlama panelleri), yetkisiz erişim veya kötü niyetli yazılım yükleme girişimleri karşısında savunmasız kalabilir. Bu tür sistemlerin korunması, sadece ağ güvenliğiyle değil; donanım temelli güvenlik önlemleri, şifreleme teknikleri ve erişim denetimi politikalarıyla mümkün olmaktadır.

Otonom sistemlerde kullanılan yazılımlar büyük ölçüde dış kaynaklı olduğunda, bu sistemler içinde arka kapı (backdoor), izinsiz erişim vektörleri veya algoritmik manipülasyon riskleri barındırabilir. Bu nedenle, özellikle **afete müdahale eden dron sistemleri**, **yazılım tabanlı sensör ağları** ve **karar destek panelleri** gibi yapılar için yerli yazılım geliştirme politikaları teşvik edilmelidir. Türkiye'nin bu alanda atacağı yerli yazılım adımları, yalnızca siber güvenlik değil, **dijital egemenlik** açısından da stratejik önemdedir.

---

[5] İnsansız Hava Araçları (İHA)' nın, yörünge izleme sistemi ile batarya sistemleri geliştikçe, insanların hizmeti için kullanımları da yaygınlaşmıştır. Bunların başında tarım ve hizmet sektörleri, keşif ve kargo hizmetleri gelmektedir. Yaşanan doğal afetlerden (deprem, yangın, sel vb.) sonra keşif, yardım gibi birçok amaç için değişik amaçlı İHA'lar tasarlanmaktadır. Bu konuda daha detaylı bilgi için bkz.; ***ERGUNŞAH Şenol ve KOŞUNALP Selahattin***, **"İnsansız Hava Araçları Tabanlı Çevresel Uygulamalara Genel Bir Bakış"**, Derleme Makalesi, Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2022, 6(1):43-53. (International Journal of Management Information Systems and Computer Science, 2022). https://dergipark.org.tr/tr/download/ article-file/2289392.

Otonom sistemler ve yapay zekâ tabanlı çözümler, klasik güvenlik paradigmalarını dönüştürmektedir.

Bu dönüşüm sürecinde;

- Her bir cihazın benzersiz dijital kimlik ile doğrulanması,
- Sürekli davranış izleme (behavioral analytics) uygulamaları,
- Olay sonrası hızlı yanıt veren otonom sistem güncellemeleri,
- Saldırıdan öğrenen yapay zekâ modellerinin devreye alınması gereklidir.

5.2. Yapay Zekâ ile Tehdit Analizi ve Saldırı Tespit

Geleneksel güvenlik sistemlerinin ötesine geçen yapay zekâ destekli çözümler, büyük veri akışlarından anlamlı tehdit örüntülerini ayıklayabilmektedir. Makine öğrenimi (ML) ve derin öğrenme (DL) algoritmaları sayesinde:

- Anormal ağ davranışları otomatik olarak tespit edilebilir,
- Potansiyel zararlı yazılım aktiviteleri sınıflandırılabilir,
- Olaylara gerçek zamanlı yanıt verilebilir,
- Otonom karar destek sistemleri, sistem yöneticisini alarm ve aksiyon planı ile bilgilendirebilir.

Özellikle olay müdahale merkezlerinde yapay zekâ algoritmalarının kullanılması, Sürekli Operasyon Merkezi / SOM (Security Operations Center / SOC) verimliliğini artırmakta ve insan kaynaklı hataların azaltılmasını sağlamaktadır.[6]

6. Afetlerde Siber Güvenliğin Geleceği: Dijital Egemenlik ve Siber Dayanıklılık Politikaları

[6] Yapay zekâ destekli dronlarla hızlı acil müdahale, gözetim, güvenlik, izleme ve denetim, akıllı çevresel izleme gibi başlıklarda değişik uygulamalar görülmektedir. Bu konuda daha detaylı bilgi için bkz.; ***YAZAR, Doç.Dr. Işıl***, "**Yapay Zeka ve Havacılık Endüstrisindeki Gelişmeler**", Makale, Elektrik Mühendisleri Odası (EMO) Dergisi, S.476, Nisan 2025, s.4-7.

Ayrıca bkz.; https://www.emo.org.tr/ekler/a5e883ecde46adc_ek.pdf?dergi=1357, 17 Haziran 2025 tarihinde erişildi.

Afetler, yalnızca fiziksel sistemleri değil; dijital altyapıları da hedef alan çok boyutlu krizler doğurur. Siber güvenlik, artık yalnızca savunma değil; bir egemenlik meselesi, bir direnç ve sürdürülebilirlik sorunudur. Bu noktada, **dijital egemenlik**, yalnızca teknolojiyi kullanmak değil; onu geliştirmek, yönetmek ve kriz anlarında dışa bağımlı olmadan karar verebilmek anlamına gelmektedir.

6.1. Yerli-Milli Çözümlerin Önemi ve Stratejik Bağımsızlık

Afet dönemlerinde kesintisiz hizmet sunan iletişim altyapıları, veri merkezleri, karar destek yazılımları ve acil müdahale sistemlerinin kontrolü dış kaynaklı olduğunda, dış müdahalelere açık bir güvenlik zaafı oluşur. Bu nedenle;

- **Yerli işletim sistemleri**, **şifreleme protokolleri** ve **ulusal veri merkezleri**,
- **Milli yazılım mühendisliği** ile geliştirilen karar destek ve izleme sistemleri,
- **TÜBİTAK**[7], **ASELSAN**[8], **HAVELSAN**[9] gibi kurumların geliştirdiği afet ve güvenlik çözümleri,

doğal afetlerde kesintisiz dijital hizmetin sağlanması, kritik verinin korunması ve dış manipülasyonların önlenmesi açısından hayati önem taşır.

Dijital egemenlik, yalnızca teknik bir kavram değil; ulusal karar alma süreçlerinin bağımsızlığı, veri yönetiminin kontrolü ve siber savaşlara hazırlık açısından bir güvenlik doktrinidir. Afetlerde kritik sistemlerin dış etkiyle yönlendirilmesini önlemek için:

- **Ulusal siber güvenlik politikaları**, sadece savunma değil, saldırı ve istihbarat yönleriyle de genişletilmelidir.
- **Yerli yapay zekâ sistemleri**, afet senaryolarına göre eğitilmeli, kriz anlarında özerk kararlar alabilecek yetkinlikte olmalıdır.
- **Siber Güvenlik Başkanlığı** gibi yeni kurulan yapılar, sadece düzenleyici değil, aynı zamanda Ar-Ge merkezli dönüşüm odağı haline getirilmelidir.

[7] https://tubitak.gov.tr/tr/haber/turkiyede-bir-ilk-afad-ve-tubitaktan-cig-alaninda-oncu-birligi, 16 Ocak 2025 tarihinde erişildi.

[8] https://tskgv.org.tr/savunmasanayiigundem/aselsan-ve-afad-arasinda-is-birligi-protokolu-imzalandi , 11 Aralık 2024 tarihinde erişildi.

[9] https://tskgv.org.tr/savunmasanayiigundem/havelsan-kiritik-tesis-guvenligi-sistemleri , 15 Mayıs 2025 tarihinde erişildi.

6.2. Kamu-Özel Sektör İş Birliklerinin Güçlendirilmesi

Siber dayanıklılığın arttırılması yalnızca kamu kurumlarının çabalarıyla değil, özel sektörün bilgi birikimi ve altyapısıyla birlikte başarılabilir. Bu bağlamda:

- **Sektör odaklı siber güvenlik kümelenmeleri** kurulmalıdır (enerji, ulaşım, sağlık, finans).
- **Siber güvenlik girişimlerine kamu teşviki**, afet öncesi hazırlık senaryolarında öncelikli alan olarak belirlenmelidir.
- Kamu-özel sektör arasında **veri paylaşımı protokolleri**, şeffaf ve yasal çerçevelerde güncellenmelidir.

Güçlü "**Siber Dayanıklılık Politikaları**" için yapılması gerekenler aşağıdadır,

1. **Siber Dayanıklılık Endeksi** oluşturularak her kurumun afet anı performansı ölçülmeli,
2. **Yerli siber tatbikat simülasyonları**, kurumlararası senaryolarla yaygınlaştırılmalı,
3. **Ulusal veri havuzları**, şifrelenmiş ve dağıtık biçimde yedeklenmeli,
4. **Dijital anayasa** kapsamında veri hakkı, kriz erişimi ve bilgi egemenliği ilkeleri tanımlanmalıdır.

Kaynakça

AFAD (2019), *Türkiye Afet Müdahale Planı (TAMP).* AFAD Yayını, Ankara.

CISA / ICS-CERT (2021). *Advisory: Oldsmar Water Treatment Facility Intrusion.* U.S. Department of Homeland Security, Washington, DC.

E-ISAC & SANS Institute (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Washington, DC.

European Union (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2).* Resmî Gazete, Brüksel.

ISO/IEC 27001:2022 – *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* International Organization for Standardization, Cenevre.

Ergunşah Şenol ve Koşunalp Selahattin, "İnsansız Hava Araçları Tabanlı Çevresel Uygulamalara Genel Bir Bakış", Derleme Makalesi, Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2022, 6(1). (International Journal of Management Information Systems and Computer Science, 2022).

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023.* Ankara.

T.C. Ulaştırma ve Altyapı Bakanlığı (2013). *Siber Güvenlik Kurulu Kararı (No: 2013/2).* Ankara.

Mataracıoğlu, T. & Özkan, S. (2011). "The Modelling of ISO/IEC 27001 Adoption in Turkish Public Organisations." *International Journal of Information Management, 31*(3), 268-275.

NHS Digital (2018). *Lessons Learned Review of the WannaCry Ransomware Cyber Attack.* Londra.

Tanrıverdi, E., Kurada, B., Şen, M. F., Demirkol Kılıç, E. (2023), Türkiye'de Afet Yönetimi Bağlamında Kritik Altyapı Kavramı, Ankara Üni. Çevrebilimleri Dergisi, 10 (1).

Thomas, A. S. & Kopczak, L. R. (2005). *From Logistics to Supply Chain Management: The Path Forward in the Humanitarian Sector.* Fritz Institute.

Yazar, Doç.Dr. Işıl, "Yapay Zeka ve Havacılık Endüstrisindeki Gelişmeler", Makale, Elektrik Mühendisleri Odası (EMO) Dergisi, S.476, Nisan 2025.

İnternet Linkleri

https://www.iso.org/standard/27001.html, 17 Haziran 2025 tarihinde ziyaret edildi.

https://eur-lex.europa.eu/eli/dir/2022/2555/oj, 17 Haziran 2025 tarihinde ziyaret edildi.

https://cbddo.gov.tr/tr/dijital-donusum/ulusal-siber-guvenlik-stratejisi-2020-2023, 17 Haziran 2025 tarihinde ziyaret edildi.

https://www.afad.gov.tr/tamp-turkiye-afet-mudahale-plani, 17 Haziran 2025 tarihinde ziyaret edildi.

https://www.btk.gov.tr/uploads/pages/siber/siber-guvenlik-kurulu-karari-2013-2.pdf, 17 Haziran 2025 tarihinde ziyaret edildi.

https://www.eisac.com/doc/Analysis_of_Cyber_Attack_Ukrainian_Power_Grid.pdf, 17 Haziran 2025 tarihinde ziyaret edildi.

https://www.cisa.gov/news-events/ics-advisories/ics-alert-21-042-01, 17 Haziran 2025 tarihinde ziyaret edildi.

https://england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-of-wannacry-ransomware-cyber-attack.pdf, 17 Haziran 2025 tarihinde ziyaret edildi.

https://arxiv.org/abs/1103.0405, 17 Haziran 2025 tarihinde ziyaret edildi.

https://www.drozdogan.com/wanna-cry-virusu-ile-ingiltere-saglik-sistemine-siber-saldiri/, 16 Haziran 2025 tarihinde erişildi.

https://dergipark.org.tr/tr/download/article-file/2289392,16 Haziran 2025 tarihinde erişildi.

https://www.emo.org.tr/ekler/a5e883ecde46adc_ek.pdf?dergi=1357, 17 Haziran 2025 tarihinde erişildi.

https://tubitak.gov.tr/tr/haber/turkiyede-bir-ilk-afad-ve-tubitaktan-cig-alaninda-oncu-birligi, 16 Ocak 2025 tarihinde erişildi.

https://tskgv.org.tr/savunmasanayiigundem/aselsan-ve-afad-arasinda-is-birligi-protokolu-imzalandi, 11 Aralık 2024 tarihinde erişildi.

https://tskgv.org.tr/savunmasanayiigundem/havelsan-kiritik-tesis-guvenligi-sistemleri, 15 Mayıs 2025 tarihinde erişildi.

Afetlerde Kritik Altyapılı Tesis Yönetiminde Siber Güvenlik

EYLÜL 2025

Güvenlik Savunma ve Emniyet Yönetişimi Akademisi

Security & Defense Governance Academy

GUSEYAD | AKADEMİ

GUSEYAD | ACADEMY

Barbaros Mh. Sırmaperde Sk. Nu.2 A-Blok D.1

Üsküdar / İSTANBUL

Tel: +90 212 906 09 56

Gsm: +90 532 062 72 10

Fax: +90 212 906 09 57

E-Posta: bilgi@guseyadakademi.org