Güvenlik Savunma ve Emniyet Yönetişimi Akademisi

Security & Defense Governance Academy

BİLGİ NOTU

GUSEYAD | AKADEMİ

GUSEYAD | ACADEMY

Acil Yardım ve Afetlerde Siber Güvenlik

Eylül 2025
İstanbul / TÜRKİYE

www.guseyadakademi.org

Acil Yardım ve Afetlerde 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.''

ACİL YARDIM VE AFETLERDE

SİBER GÜVENLİK

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

Bilgi güvenliği, artık sadece veriyi değil; insan hayatını da korur.

Mikko Hyppönen, Siber Güvenlik Uzmanı

Giriş

Afet yönetimi denilince çoğu zaman akıllara fiziki yıkımlar, arama-kurtarma çalışmaları ve sağlık hizmetleri gelir. Ancak günümüzde bu süreçlerin başarısı, büyük ölçüde "***dijital altyapıların işlerliği***" ne bağlıdır. Elektrik şebekeleri, hastane sistemleri, iletişim ağları, trafik yönetim sistemleri ve kamu veritabanları gibi unsurlar; hem afetin öncesinde hazırlık için hem de sonrasında müdahale ve iyileştirme için kritik rol oynamaktadır.

Bu dijital altyapılar, doğal afetler gibi beklenmedik durumlarda siber saldırıların da hedefi hâline gelebilir. Özellikle de deprem, sel veya yangın gibi olaylar yaşanırken, eş zamanlı gerçekleşen "*siber saldırılar afetin yıkıcılığını katlayarak artırabilir*". Bu durum, klasik afet yönetimi anlayışını, "***dijital bir koruma katmanıyla yeniden düşünmeyi zorunlu kılmıştır***".

Siber güvenlik, artık sadece verileri koruma aracı değil; ulusal güvenliğin, hizmet sürekliliğinin ve toplumsal direncin temel bileşeni hâline gelmiştir. *Yapay zekâ destekli analizler, otonom müdahale sistemleri ve akıllı erken uyarı teknolojileri* sayesinde, yalnızca ***siber tehditlere karşı*** değil, ***afet kaynaklı karmaşık krizlere karşı*** da daha hazırlıklı olunabilmektedir.

Bu bölümde; afet süreçlerinde *siber güvenliğin* nasıl ele alınması gerektiğini, *yapay zekâ teknolojilerinin* bu süreçlere nasıl entegre edileceğini ve *dijital bağımlılığın getirdiği riskleri yönetmenin yollarını* ele alacağız. Ayrıca; *veri yedekleme, sosyal medya manipülasyonları, sahte yardım kampanyaları, YZ destekli tatbikatlar ve ulusal dijital egemenlik politikaları* gibi konulara da odaklanacağız.

1. Dijital Bağımlılık ve Afet Anlarında Risk Yönetimi

Günümüz toplumlarında dijital cihazlara ve internet altyapısına duyulan bağımlılık, afet anlarında hayati riskler doğurabilecek düzeye ulaşmıştır. Toplumun büyük bir kısmı iletişim, bilgi edinme, yön bulma ve hatta yardım isteme gibi temel işlevleri yalnızca dijital kanallar üzerinden gerçekleştirmeye alışmıştır. Ancak bu "***dijital bağımlılık***", *afet sırasında altyapıların çökmesi veya siber saldırılara maruz kalması hâlinde, ciddi bilgi ve iletişim yoksunluğu* yaratabilir.

Öne Çıkan Hususlar:

- Dijital bağımlılık, yalnızca sosyal medya kullanımıyla sınırlı değil; harita uygulamaları, çevrimiçi bankacılık, e-devlet servisleri gibi temel hizmetleri de kapsamaktadır.

- Afet anında yaşanabilecek kesintiler; bilgiye ulaşamama, yanlış yönlendirme, yardım çağrılarına ulaşamama gibi çok boyutlu riskler doğurur.
- Özellikle genç nüfus ve kent merkezlerinde yaşayan bireyler, dijital cihazlar aracılığıyla yönlendirme almaya fazlasıyla alışkındır. Fiziksel harita, klasik telsiz iletişimi gibi alternatif yöntemlere dair bilgi eksikliği yaygındır.
- Bu durum, siber dayanıklılık stratejilerinin sadece teknik düzlemde değil, toplumsal alışkanlıklar düzeyinde de ele alınmasını zorunlu kılar.

RİSK SENARYOLARI		
Durum	**Olası Etki**	**Gereken Müdahale**
GSM altyapısının çökmesi	Toplumun %80' inden fazlası yakınlarını arayamaz hale gelir	Alternatif telsiz / tümleşik sistemlerin eğitimi yaygınlaştırılmalı
Navigasyon servislerine erişilememesi	Tahliye rotaları bilinmez, yön kaybı yaşanır	Basılı yön haritaları, tatbikatlarla desteklenmeli
Sosyal medya ve haber ağının devre dışı kalması	Yanlış bilgi yayılımı artar, panik havası oluşur	Afet anı bilgilendirme sistemleri çok kanallı kurgulanmalı

1.1. Akademik Bakış ve Stratejik Öneri

Afet anlarında ***dijital bağımlılığın zarar verici bir kırılganlık alanına dönüşmemesi***, ancak ***çoklu haberleşme kanallarına sahip, dirençli bir toplumsal altyapının kurulmasıyla*** mümkündür. Risk yönetimi stratejilerinde artık yalnızca teknolojik altyapılar değil, **toplumsal teknoloji kullanımı alışkanlıkları da bir tehdit vektörü olarak** değerlendirilmeli; **bilinçlendirme çalışmaları** afet eğitimlerinin ayrılmaz bir parçası olmalıdır.

2. Uyarı Sistemlerinin Güvenliği ve Siber Müdahale Protokolleri

Afet öncesi, anı ve sonrasında devreye giren **erken uyarı sistemleri**; can kaybını azaltmak, halkı bilinçlendirmek ve acil durum ekiplerini koordine etmek adına hayati öneme sahiptir. Ancak bu sistemlerin dijital altyapılara dayanması, **siber saldırı tehdidini doğrudan afet yönetimiyle kesişen bir güvenlik açığı haline getirmiştir**.

Kritik Gerçekler:

- Türkiye'de **AFAD, Kandilli Rasathanesi**, **Meteoroloji Genel Müdürlüğü** gibi kurumlar tarafından SMS ve mobil uygulama üzerinden yapılan erken uyarılar, mobil şebekeye ve merkezi veri tabanlarına bağlıdır.
- **Sahte uyarılar (spoofed alert)**, panik, kitlesel yönlendirme ve kamu düzenini bozma gibi sonuçlar doğurabilir.
- **IoT tabanlı siren sistemleri**, **şehir anons altyapıları**, **akıllı TV / uydu entegrasyonları** da hedef alınabilecek unsurlar arasında yer alır.
- **US-CERT**, Japonya'nın J-Alert sistemi, Avrupa Sivil Koruma Mekanizması gibi örnekler; merkezi ve çok kanallı sistemlerin güvenliğini siber güvenlik protokolleriyle bütünleştirmiştir.[1]

SİSTEM GÜVENLİĞİ ANALİZİ		
Sistem Bileşeni	**Risk Senaryosu**	**Alınması Gereken Önlem**
GSM & SMS Uyarıları	Sahte afet uyarıları gönderilmesi	Mobil imzalı doğrulama ve kamu sertifikasyon altyapısıyla entegre
Belediye Anons Sistemleri	Sesli uyarıların yetkisiz tetiklenmesi	Fiziksel erişim kısıtlamaları + IP filtreleme
Siren Sistemleri (IoT)	Uzaktan erişimle etkisiz hâle getirme	Edge cihazlarda firmware şifre kullanımı ve güvenlik güncellemesi
Web tabanlı acil uyarılar	Sayfa sahteciliği (phishing)	URL imzalama, HTTPS doğrulama ve MFA kontrolleri

Müdahale Protokolleri:

- **Tier-1 Uyarı** (ön uyarı): Yetkilendirilmiş kurum kimliğiyle imzalanmalı; kopyalanamaz yapıda olmalıdır.
- **Tier-2 Uyarı** (anlık siren): Dijital imza + merkezi alarm kontrol onayı ile yürütülmelidir.

[1] Bu konuda detaylı bilgi için bkz.; **Tsunoda, Akaki, 2023**, *Investigating Threats Posed by SMS Origin Spoofing to IoT Devices. Ayrıca;* **EU-Alert** (Cell Broadcast tabanlı) ile **J-Alert** (Japonya) gibi sistemlerde siber güvenlik entegrasyonunun teknik ve düzenleyici standartları incelenmektedir.

- **Tier-3 Uyarı** (tahliye): Sesli anons sistemleri, sosyal medya ve uygulamalarda senkronize edilerek kriz merkezinden canlı kontrol sağlanmalıdır.

Stratejik Yaklaşım:

Uyarı sistemlerinin siber güvenliği sadece bir teknik ihtiyaç değil; **ulusal güvenlik meselesidir**. Afet sırasında paniği önlemenin yolu, yalnızca sistemin hızlı çalışması değil, aynı zamanda **verilen uyarının halk nezdinde doğruluğuna duyulan güven** ile mümkündür. Bu nedenle tüm uyarı sistemleri **siber tehdit analizine tabi tutulmalı**, bu sistemlere ait **SOC (Security Operations Center) izleme modülleri** her zaman aktif olmalıdır.

3. Sosyal Medya Manipülasyonu ve Sahte Yardım Kampanyaları

Afet anlarında sosyal medya, bilgiye erişimin en hızlı, yayılımın en etkili ve duygusal etkileşimin en yoğun yaşandığı mecralardan biri hâline gelir. Ancak bu yoğunluk, sadece faydalı bilgi akışını değil; **yanıltıcı içerikler, sahte yardım kampanyaları ve psikolojik manipülasyonların da** hızla yayılmasına zemin hazırlar.

Afet sonrası paylaşılan her tweet, gönderi veya video; milyonlarca kişiye ulaşarak bir karar zincirini etkileyebilir. İnsanlar **depremzedeler için bağış yaparken dolandırılabilir**, yanlış bilgilerle paniğe kapılabilir ya da devlet kurumlarına yönelik güvensizlik oluşturacak manipülatif içeriklere maruz kalabilir. Bu nedenle sosyal medya, afet yönetiminde bir avantaj olabildiği kadar, **siber güvenliğin kırılgan bir cephesi hâline de gelebilir.**

TEMEL TEHDİT TÜRLERİ		
Manipülasyon	***Amaç***	***Etkisi***
Sahte bağış kampanyaları	Maddi dolandırıcılık	Mağduriyetin artması, güven kaybı
Deepfake içerikler	Algı yönetimi ve itibar zedeleme	Kurumlara güvensizlik oluşturma
Bot hesaplarla bilgi kirliliği	Yönlendirilmiş kamuoyu oluşturma	Afet koordinasyonunun zayıflaması
Gerçek dışı görseller / sahte haber	Panik oluşturma ve güven sarsma	Tahliye, yardım gibi süreçlerde gecikme
Yurt dışı merkezli dezenformasyon	Dijital psikolojik savaş	Toplumsal kırılganlıkları artırma

Siber Güvenlik ve Algı Yönetimi Stratejileri:

- **Teyit Mekanizmaları Kurulmalıdır:** Resmî kurumlar, sosyal medya hesaplarını **anlık teyit araçlarına** (örneğin: @afadbaskanlik teyitli gönderi) dönüştürmelidir.
- **Sahte Kampanya Tespit Sistemleri Geliştirilmelidir:** Bankalar ve sivil toplum kuruluşları, **bağış API' lerini** kullanarak yalnızca doğrulanmış kampanyalara izin vermelidir.
- **Acil Durum Bilgilendirme Botları:** WhatsApp, Telegram gibi platformlarda afet bölgesi hakkında teyitli bilgi sunan kamu botları aktif hale getirilmelidir.
- **Siber Polislik ve Dijital Takip:** EGM Siber Suçlar Daire Başkanlığı, afet anlarında dijital dolandırıcılık şikâyetlerini özel izleme merkezlerinde değerlendirmelidir.
- **Platformlarla İş Birliği:** X (Twitter), Meta, YouTube gibi platformlarla yapılacak anlaşmalarla sahte yardım kampanyaları, otomatik filtrelerle durdurulabilir.

Kritik Değerlendirme:

Afetlerde sosyal medya hem umutların hem de tuzakların hızla yayıldığı bir alandır. Bu nedenle afet yönetimi stratejileri, yalnızca **fiziksel yardım ve lojistik değil; dijital doğruluk ve bilgi güvenliği** süreçlerini de kapsayacak şekilde yeniden yapılandırılmalıdır. Sosyal medya, kriz iletişiminin kontrolsüz bir alanı değil, **siber vatanın kamu diplomasisi cephesi** olarak görülmelidir.

Örneğin; 4 Ekim 2024' te Kuzey Carolina, Asheville'de yaşanan "***Helene Kasırgası***" esnasında kasırgadan etkilenen bölgelerdeki ***sivil savunma faaliyetlerine ilişkin doğrulanmamış raporlar***, afet görevlilerinin güvenlikleri konusunda endişe duymasına neden olmuş, söz konusu faaliyetler kısmen aksamıştır.[2]

Helen Kasırgası örneği, hükümetlerin yanlış bilgiye karşı aktif mücadele etmek zorunda olduklarını ve hatta benzer **sosyal medya dezenformasyonlarına hızlı ve sert bir şekilde müdahale edilmesi gerektiğini** göstermektedir.

4. Mobil Cihaz Güvenliği ve Kitle İletişiminde Veri Bütünlüğü

Afet anlarında mobil cihazlar, sadece bireysel iletişim aracı olmanın ötesine geçerek, **toplumun dijital refleksi** hâline gelir. Vatandaşların konum bildirimleri, sağlık verileri, aile

[2] https://www.rollingstone.com/politics/politics-news/hurricane-helene-response-disrupted-militia-fema-1235133009/ , 14 Temmuz 2025 tarihinde ziyaret edildi.

üyeleriyle iletişimi ve yardım çağrıları; bu küçük ama güçlü cihazlar üzerinden sağlanır. Ancak bu yoğun dijital etkileşim, **kişisel verilerin güvenliği**, **iletilen bilgilerin doğruluğu** ve **sistematik bir siber saldırıya açıklık** gibi kritik sorunları da beraberinde getirir.

Bu nedenle mobil cihazların sadece donanımsal değil; yazılımsal, ağ bağlantısı ve uygulama erişimleri düzeyinde **çok katmanlı güvenliğe** sahip olması gerekmektedir. Aynı zamanda kamuya yapılan afet bilgilendirmelerinde, iletilen her verinin **bütünlüğünün korunması**, yanlış yönlendirme riskinin azaltılması açısından hayati önemdedir.

RİSK ALANLARI VE TEHDİT TÜRLERİ		
Zafiyet Türü	***Açıklama***	***Etkisi***
Uygulama izinlerinin kötüye kullanımı	Afet uygulamaları gereğinden fazla izne sahip olabilir	Kişisel verilerin çalınması, gözetlenme
SMS spoofing ve sahte uyarılar	Sahte mesajlar gerçekmiş gibi görünerek kullanıcıları kandırır	Panik yaratma, dolandırıcılık
Wi-Fi sniffing / ortak ağ riskleri	Yardım noktalarında açık Wi-Fi ağları	Şifre hırsızlığı, MITM saldırıları
Lokasyon servislerinin manipülasyonu	Yanlış konum bildirimleri veya konumun izinsiz takibi	Yardım koordinasyonunun bozulması
OTA saldırıları (Over The Air)	Mobil cihazlara uzaktan kötü amaçlı yazılım yükleme	Cihazın kontrolünü kaybetme

Güvenlik Önerileri ve Stratejik Yaklaşımlar:

- **Mobil Afet Uygulamaları için Minimum Yetki İlkesi**: Gereksiz erişim taleplerinin denetlenmesi ve açık kaynaklı güvenilir yazılımların tercih edilmesi.
- **Kamuya Açık Uyarılar için Kriptografik İmza**: Resmî bilgilendirme mesajlarının dijital olarak imzalanması ve bu sayede SMS sahtekârlıklarının önüne geçilmesi.
- **E-SIM ve GSM Operatör İş Birliği**: Afet bölgelerinde operatörlerin, sinyal analizleri yoluyla yanlış yönlendirme yapan baz istasyonlarını tespit etmesi.

- **Afet Alanı Mobil Cihaz Güvenliği Protokolleri**: EGM, AFAD ve BTK koordinasyonuyla afet sonrası mobil güvenlik rehberlerinin anında yayınlanması.
- **Veri Bütünlüğü için Blockchain Tabanlı Bildirim Sistemleri**: Özellikle yardım dağıtımı, konum koordinasyonu gibi veriler için şeffaf, değiştirilemez kayıt altyapılarının kurulması.

Kritik Değerlendirme:

Afet dönemlerinde hızlı bilgi akışı yaşamsal önem taşırken, bu sürecin **güvenli, şeffaf ve kesintisiz** olması da aynı derecede önemlidir. Mobil cihaz güvenliği, bireysel farkındalıkla değil; ulusal çapta yürütülen koordineli bir "***siber güvenlik stratejisi***" ile sağlanmalıdır. Toplumun güvenle bağlandığı her mobil ağ, "***siber vatanın dijital damarları***" dır. Bu damarlardan yayılanlar kontrol edilmezse, "***bilgi yerine kaos***" yayılır.

5. Kritik Veri Yedekleme Stratejileri ve Kurtarma Senaryoları

Afetlerin yıkıcı etkisi yalnızca fiziksel yapılarla sınırlı değildir; aynı zamanda **veri varlıkları**, yani bir kurumun, kamu otoritesinin veya bir bireyin en değerli dijital kaynakları da tehdit altındadır. *Elektrik kesintileri, donanım arızaları, siber saldırılar ya da iletişim altyapısındaki çöküşler*; veri kayıplarına ve *hizmet sürekliliğinin tamamen bozulmasına neden olabilir.*

Bu sebeple afet öncesi alınan yedekleme önlemleri, yalnızca teknik bir ihtiyaç değil; "***dijital egemenlik, ulusal güvenlik ve afet sonrası toparlanma kapasitesi***" açısından "***kritik bir gereklilik***" tir. Yedekleme stratejileri ve kurtarma planları, proaktif bir güvenlik kültürünün en temel yapı taşlarından biridir.

Kritik Senaryolar ve Kurtarma Yaklaşımları:

1. **Siber Saldırı (Ransomware) Durumu**:
   → İzole yedekleme havuzu (air-gapped backup) sayesinde verinin şifrelenmeden geri yüklenmesi sağlanır.
2. **Fiziksel Yıkım (Deprem, Yangın)**
   → Farklı şehirlerdeki veri merkezleri veya bulut sağlayıcıları üzerinden erişilebilir yedekleme altyapısı kritik rol oynar.
3. **Donanım Arızası ve İletişim Kesintisi**
   → Yerel ağ dışında zamanlanmış yedeklerin dış ortamlarda saklanması gerekir (örn. taşınabilir NAS, dış disk, offline yedekleme).

4. **İç Tehdit Kaynaklı Silme veya Manipülasyon**
   → Geriye dönük değişiklik takibi (audit trail) ve versiyonlu yedekleme yapıları bu tehdide karşı direnç sağlar.

YEDEKLEME STRATEJİLERİ ve UYGULAMA MODELLERİ		
Yedekleme Tipi	**Tanımı**	**Kullanım Alanı**
Tam Yedekleme (Full Backup)	Tüm veri setlerinin eksiksiz kopyalanması	Haftalık veya kritik veriler için önerilir
Artımlı Yedekleme (Incremental)	Sadece son yedeklemeden sonra değişen verilerin kopyalanması	Günlük operasyonel veriler için idealdir
Farklı Yedekleme (Differential)	Son tam yedeklemeden sonra değişen tüm verilerin yedeklenmesi	Kapsamlı ama hızlı geri yükleme gereken durumlar
Anlık Yedekleme (Snapshot)	Sanal sunucular veya veri blokları için sistemin anlık görüntüsünün alınması	Felaket kurtarma (disaster recovery) için uygundur
Hibrid Yedekleme	Bulut + yerel sistemlerin bir arada kullanılması	Esnek ve coğrafi yedekleme için önerilir

Stratejik Yaklaşım: "3-2-1" Kuralı[3]

- **3** kopya veri olmalı,
- **2** farklı ortamda saklanmalı,
- **1** tanesi mutlaka **offline** veya **bulut dışında bir lokasyonda** tutulmalıdır.

Bu strateji, kamu kurumlarından özel sektöre kadar her yapının afet öncesi ve sonrası veri bütünlüğünü sağlaması için temel referans olmalıdır.

Dijital Kurtarma Planları İçin Ulusal Düzeyde Öneriler:

- **Yedekleme Bilgi Bankası**: AFAD, BTK ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından acil durumlarda erişilecek merkezi bir bilgi deposu kurulmalıdır.
- **Veri Sıralama Rehberleri**: Kurumlar kritik, hassas ve önemsiz verileri sınıflandırarak yedekleme önceliklendirmesi yapmalıdır.

[3] https://www.veeam.com/blog/321-backup-rule.html, 14 Temmuz 2025 tarihinde ziyaret edildi.

- **Tatbikatlar ve Gerçek Zamanlı Senaryolar**: Devlet kurumları, yerel yönetimler ve sağlık hizmetleri için yılda en az bir dijital kurtarma tatbikatı zorunlu olmalıdır.
- **Bulut Yedekleme Politikaları**: KVKK ve ulusal dijital egemenlik ilkeleri çerçevesinde, yurtdışı merkezli bulut hizmetlerinin alternatifleri oluşturulmalıdır.

6. Siber Güvenlik Tatbikatları: Afet Senaryoları ile Uyum

Afetler, sadece fiziki sistemleri değil, aynı zamanda dijital altyapıları da çöküşe sürükleyebilir. Bu nedenle afet yönetim planlarının yalnızca kurtarma ve tahliye adımlarını değil, **siber güvenlik reflekslerini de içermesi** gerekir. Tatbikatlar, bu reflekslerin geliştirilmesi ve kurumların koordineli hareket kabiliyetinin test edilmesi için vazgeçilmezdir.

Siber güvenlik tatbikatları; gerçek dünyaya yakın senaryolarla, ekiplerin teknik ve operasyonel yetkinliklerini ölçmeye yarar. Ancak bu tatbikatların afet senaryolarıyla **entegre ve çok disiplinli** yapılması, kamu-özel sektör-askeri yapıların eş zamanlı savunma gücünü artıracaktır.

Afetlerin karmaşık yapısı, yalnızca IT ekiplerinin değil, **tüm kriz birimlerinin dijital farkındalıkla hareket etmesini** zorunlu kılar.

Uyumlu Tatbikat Modeli: "Karma Kriz Tatbikatları" Yaklaşımı

Karma kriz tatbikatları, afet anlarında **fiziksel krizler ile dijital tehditlerin eş zamanlı test edildiği** hibrit simülasyonlardır.

Bu yaklaşıma göre:

- Afet ve Acil Durum Yönetimi Başkanlığı (AFAD), Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile eş zamanlı senaryo üretir.
- Oyunlaştırılmış senaryolar sayesinde kamu görevlileri ve teknik ekipler "zaman baskısı altında çözüm üretme" pratikleri kazanır.
- Tatbikatlar sadece büyükşehirlerde değil, **kritik tesislerin bulunduğu il ve ilçelere özel olarak** uygulanmalıdır.

Afet Senaryolarına Entegre Siber Tatbikat Başlıkları:

Senaryo Başlığı	Tatbikat İçeriği	Beklenen Kazanım
Elektrik Kesintisi + Ransomware	Kritik bir sağlık tesisi sisteminin çökmesi ve veri şifrelenmesi	Olay müdahale süresi, kriz yönetimi reflekslerinin değerlendirilmesi
Sel Felaketi + DDoS Saldırısı	Belediyenin uyarı sistemi çökertiliyor, sosyal medyada manipülasyon başlatılıyor	Operasyonel koordinasyon, siber-sosyal medya farkındalığı
Deprem Anında Altyapı İletişim Kesintisi	İnternet alt yapısı çöküyor, sistemlere fiziksel erişim sınırlanıyor	Alternatif iletişim yolları, acil plan aktivasyonu
Yönlendirilmiş Sahte Yardım Siteleri	SMS ve sosyal medya üzerinden sahte yardım kampanyaları yayılıyor	Farkındalık, doğrulama mekanizmaları ve ihbar süreçlerinin işlerliği
Bilgi Sızıntısı ve Kamu Panik Senaryosu	AFAD, hastane, valilik gibi kurumların verileri çalınıyor ve yayınlanıyor	Güvenlik duvarlarının test edilmesi, kamu iletişim protokolü tatbiki

Stratejik Öncelikler ve Öneriler:

- **Her kurum yılda en az bir (01) siber afet tatbikatı yapmalı.**
- Tatbikatlar sırasında *iletişim kesilmesi, yanlış bilgi yayılımı ve sosyal medya manipülasyonları* senaryoya dahil edilmeli.
- **Afet simülasyon parkurları**, eğitim kurumlarına entegre edilmeli ve meslek liseleri, üniversiteler bu alana yönlendirilmeli.
- *Yapay zekâ destekli simülasyon platformları* ile tatbikatların *doğruluk, tekrar ve analiz gücü artırılmalı.*
- Tatbikat sonrası raporlama ve "***şeffaf denetim kültürü***" sağlanmalı.

7. Afet Süreçlerinde Siber Vatan Savunması: Politikalar ve Stratejik Uyum

Dijital çağın getirdiği yeni güvenlik paradigmasında, afet süreçleri yalnızca fiziksel değil, aynı zamanda dijital cephelerde de yönetilmesi gereken karmaşık olaylar bütünüdür. "***Siber Vatan***" kavramı bu noktada öne çıkmakta; enerji santrallerinden iletişim altyapılarına, sağlık sistemlerinden lojistik ağlara kadar geniş bir dijital ekosistemin korunması gerekliliğini ifade etmektedir.

Afet anlarında dijital sistemlerin hedef alınması, fiziksel müdahaleyi ve afet yanıt kapasitesini doğrudan sekteye uğratabilir. Bu nedenle, ***siber güvenliğin*** bir güvenlik refleksi değil; "***kurumsal bir strateji ve kamu politikası***" olarak değerlendirilmesi gereklidir. Ulusal Siber Güvenlik Stratejileri (2020–2023 ve sonrası), Ulusal Yapay Zekâ Stratejisi (2021) ve Seferberlik ve Savaş Hâli Yönetmeliği (Karar Sayısı: 8510) gibi mevzuatlar, afet durumlarında siber savunma reflekslerinin nasıl yapılandırılması gerektiğine dair yön gösterici çerçeveler sunmaktadır.

Stratejik uyum açısından, kamu kurumlarının afet öncesinde, sırasında ve sonrasında uygulayacakları ***siber savunma planları***; hem kurumsal dijital refleksleri güçlendirmeli, hem de sektörel bazda koordine edilmelidir. Bunun için;

- **Ulusal siber olaylara müdahale (USOM) birimleri**, afet dönemlerine özgü "***kriz modu***" *prosedürleri* geliştirmelidir.
- **AFAD**, **BTK**, **Siber Güvenlik Başkanlığı** gibi kurumlar arasında *veri paylaşımı ve kriz koordinasyonu için* ***ortak platformlar*** kurulmalıdır.
- **Yerel yönetimler**, kritik tesislere ilişkin ***siber tatbikat zorunlulukları*** ile ***stratejik uyum*** içinde olmalıdır.

Sonuç olarak, afet süreçlerinde "***siber vatan savunması***"; hem *dijital altyapının sürekliliğini sağlamak, hem de ulusal dijital egemenliği güvence altına almak* için hayati önemdedir. Bu bağlamda, *yalnızca teknik müdahale değil*, "***politik kararlılık, stratejik entegrasyon***" ve "***yapay zekâ destekli karar sistemleri ile donatılmış bir yönetişim modeli***" esas alınmalıdır.[4]

[4] *National Oceanic and Atmospheric Administration (NOAA) AI Strategy Report*, 2021, ABD' nde "NOAA / AI" destekli fırtına tahmin sistemleri, ***%92'ye varan isabet oranına ulaşmıştır.*** Bir başka ülkede benzer şekilde, *National Research Institute for Earth Science and Disaster Resilience (NIED)*, (Japonya' da), deprem erken uyarı sistemine AI modülleri entegre ederek ***gerçek zamanlı tahminleme süresini %35 oranında hızlandırmıştır.*** Daha detaylı bilgi için bkz.; ***Nishimoto, K. et al. (2020)***, Development of an Earthquake Early Warning System Using Artificial Intelligence, Earthquake Engineering & Structural Dynamics. - Literatürde

Kaynakça

NIED, National Research Institute for Earth Science and Disaster Resilience.

Nishimoto, K. et al. (2020), Development of an Earthquake Early Warning System Using Artificial Intelligence, Earthquake Engineering & Structural Dynamics.

NOAA, AI Strategy Report, 2021, National Oceanic and Atmospheric Administration.

Tsunoda, Akaki, 2023, Investigating Threats Posed by SMS Origin Spoofing to IoT Devices.

Türkiye Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024–2028), T.C. Ulaştırma ve Altyapı Bakanlığı.

İnternet Linkleri

https://www.rollingstone.com/politics/politics-news/hurricane-helene-response-disrupted-militia-fema-1235133009/, 14 Temmuz 2025 tarihinde ziyaret edildi.

https://www.veeam.com/blog/321-backup-rule.html, 14 Temmuz 2025 tarihinde ziyaret edildi.

https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf, 28 Temmuz 2025 tarihinde ziyaret edildi.

vatan ve siber teknolojiler tanımlarına baktığımızda, teknoloji kullanan her bir bireyin Siber Vatanın birer parçası olduğunu ve hatta özellikle 2000 yılından sonra dünyaya gelen çocukların tamamen siber vatanın birer ferdi olduğunu kolaylıkla ifade edebiliriz (y.n.) – Ayrıca; Türkiye Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024–2028), kritik altyapıların siber koruması, **bağımsız milli güvenlik çözümleri** geliştirilmesi ve **YZ ile desteklenen müdahale kapasitelerinin artırılmasını** hedeflemiştir Bu konuda daha detaylı bilgi ve eylem planını incelemek için bkz.; https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf, 28 Temmuz 2025 tarihinde ziyaret edildi.

Acil Yardım ve Afetlerde 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