Güvenlik Savunma ve Emniyet Yönetişimi Akademisi

Security & Defense Governance Academy

BİLGİ NOTU

GUSEYAD | AKADEMİ

GUSEYAD | ACADEMY

Afetlerde Bilişim ve İletişim Teknolojilerinde Siber Güvenlik

Eylül 2025
İstanbul / TÜRKİYE

www.guseyadakademi.org

Afetlerde Bilişim ve İletişim Teknolojilerinde 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

BİLİŞİM VE İLETİŞİM TEKNOLOJİLERİNDE

SİBER GÜVENLİK

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

Bilgisayar kullanıcısı kadar akıllı, geliştiricisi kadar zekidir.

Burak Soner Bozkurtlar

Giriş

Afet yönetiminin etkinliği, yalnızca *fiziksel müdahale kapasitesiyle* değil; aynı zamanda *bilişim ve iletişim altyapılarının güvenliği* ve *sürekliliğiyle* de doğrudan ilişkilidir. Günümüzde dijital sistemler, afetin her aşamasında (hazırlık, müdahale, iyileştirme) karar alma, veri paylaşımı, erken uyarı, kaynak yönetimi ve halkla iletişim gibi işlevlerde kilit rol oynamaktadır. Ancak bu sistemlerin siber tehditlere karşı korunmaması, afetin yarattığı tahribatı daha da büyütebilir.

Kritik iletişim altyapıları; ***enerji, sağlık, ulaşım, haberleşme ve kamu hizmetleriyle*** doğrudan bağlantılıdır. Bu yapıların herhangi birinde yaşanacak bir kesinti, *zincirleme etkiyle diğer sistemleri de felç edebilir.* Afet anlarında yoğun trafik, altyapı zafiyetleri ve dış kaynaklara bağımlılık gibi nedenlerle iletişim sistemleri çökebilir. Buna ek olarak, kötü niyetli aktörlerin gerçekleştirdiği DDoS saldırıları, veri sızdırma girişimleri, fidye yazılımları ya da sahte bilgi kampanyaları, *zaten hassas durumda olan iletişim ortamını daha da kaotik hâle* getirebilir.

Bu nedenle afet yönetimiyle entegre çalışan bir siber güvenlik stratejisi, yalnızca teknolojik bir tedbir değil; aynı zamanda ulusal güvenlik ve toplumsal dirençlilik açısından da bir zorunluluktur. Dijital egemenliğe dayalı, yerli çözümlerle desteklenen siber güvenlik politikaları sayesinde, kritik bilişim altyapılarının korunması ve hizmet sürekliliğinin sağlanması mümkün olabilir.

Bu bölümde; afet dönemlerinde dijital altyapılara yönelik tehditler, olay müdahale süreçleri, erken uyarı sistemleri, sosyal medya manipülasyonları, yapay zekâ destekli karar mekanizmaları ve ulusal dijital dayanıklılık stratejileri bütüncül bir yaklaşımla ele alınacaktır.

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.

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. Yakın zamanda kurulan *Siber Güvenlik Başkanlığı*'nın da benzer çalışma ve yönergeleri de beklenmektedir.

1. Bilişim ve İletişim Altyapılarının Önemi ve Afet Bağlamında Riskler

Günümüz afet yönetimi süreçlerinde bilişim ve iletişim altyapıları, sadece bilgi paylaşımının sağlandığı teknolojik sistemler değil, aynı zamanda karar alma, kaynak yönlendirme ve kamuoyunu bilgilendirme gibi hayati görevleri üstlenen temel yapılardır. Afet anında kesintiye uğrayan bir iletişim altyapısı, müdahale ve iyileştirme süreçlerinde kaosa yol açabilir.

2023 yılında **Kahramanmaraş merkezli depremlerde**, bölgedeki baz istasyonlarının çökmesi nedeniyle haberleşme altyapısında yaşanan aksaklıklar, hem arama-kurtarma faaliyetlerini hem de yardım koordinasyonunu ciddi ölçüde sekteye uğratmıştır.[1] Benzer şekilde büyük depremlerde, sarsıntıların ardından telefon görüşmelerinin yapılamadığı, SMS ve internet servisleri aşırı yüklenme nedeniyle devre dışı kaldıkları bilinmektedir.

Bu nedenle afetlere dayanıklı, yedekli ve güvenli bilişim altyapılarının oluşturulması; dijital kırılganlıkların tespiti ve giderilmesi büyük önem taşır.

1.1. Kritik Bilişim ve İletişim Sistemlerinin Sınıflandırılması

Kritik bilişim ve iletişim altyapıları, bir ülkenin güvenliği, kamu düzeni, sağlık hizmetleri, finansal sistemleri, enerji ve ulaşım alanlarında sürdürülebilirliği doğrudan etkileyen sistemleri ifade eder. Bu kapsamda, şu alanlar başlıca sınıflandırma başlıklarıdır:

- **Telekomünikasyon Altyapıları** (Baz İstasyonları, Fiber-Optik Hatlar, GSM Şebekeleri)
- **Acil Çağrı Sistemleri** (112, AFAD Sistemleri, Komuta Merkezleri)
- **Veri Merkezleri ve Bulut Sistemleri**
- **Kamuya Ait İletişim Platformları ve Kriz Yönetim Portalları**
- **Kamu Kurumlarına Ait SCADA ve ERP Sistemleri**
- **Radyo, Televizyon, Uydu ve İnternet Yayın Altyapıları**

Avrupa Birliği'nin 2022 yılında güncellediği **NIS2 Direktifi**,[2] bu sistemleri "***kritik dijital altyapı***" başlığı altında değerlendirerek devletlere hem teknik, hem de "***yönetişim temelli***

[1] https://www.haberturk.com/operatorler-yine-sinifta-kaldi-3564007-teknoloji, 15 Temmuz 2025 tarihinde ziyaret edildi.

[2] https://nis2directive.eu/what-is-nis2/, 16 Temmuz 2025 tarihinde ziyaret edildi.

güvenlik yükümlülükleri" getirmiştir. Türkiye' de ise bu sınıflandırmaya ilişkin ilk ciddi adım, 2021 yılında **USOM (*Ulusal Siber Olaylara Müdahale Merkezi*)** tarafından yayımlanan "*Sektörel SOME Yapılanması*" rehberinde atılmıştır.[3]

1.2. Afetlerde Altyapı Zafiyetleri ve Dijital Kırılganlık Alanları

Afet zamanlarında ortaya çıkan zafiyetlerin büyük bir kısmı, dijital sistemlerin afet senaryolarına göre önceden test edilmemesinden kaynaklanmaktadır. Bu kırılganlıklar genel olarak şu başlıklarda toplanabilir:

- **Enerji Bağımlılığı**: İletişim altyapılarının büyük bölümü elektrikle çalıştığı için enerji kesintisi tüm sistemi felç edebilir. Örnek: 2023 depremi sonrası elektrik kesintisi nedeniyle baz istasyonlarının devre dışı kalması.
- **Yedekleme Eksikliği**: Coğrafi olarak dağıtık olmayan veri merkezleri, afet anında tüm bilgi sistemlerinin kaybına neden olabilir. Örnek: 2005' te ABD'de Katrina Kasırgası sonrası birçok yerel kurumun tüm dijital arşivleri zarar görmüştür.
- **Teknolojik Bağımlılık ve Dış Kaynak Riski**: Kritik yazılımlar veya cihazlar, yurt dışı menşeli sistemlere bağlıysa güncelleme, destek ve entegrasyon kriz anında sekteye uğrayabilir.
- **Fiziksel Altyapı Kırılganlığı**: Fiber hatlar, yer altı kablolama sistemleri, enerji panelleri vb. afetlerde doğrudan zarar görebilir.
- **Aşırı Trafik ve Hizmet Reddi**: Afet sırasında yoğunlaşan iletişim trafiği sistemleri kilitleyebilir. Buna DDoS saldırıları da eklendiğinde, kriz büyüyerek sistem dışı kalma süresi uzar.

Bu zafiyetlerin her biri, **siber güvenlik açıklarıyla birleştiğinde**, sadece teknik değil, aynı zamanda **politik ve toplumsal bir güvenlik sorunu** hâline gelir.[4]

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**

[3] Ayrıntılı bilgi için bkz.; https://www.usom.gov.tr/faydali-dokumanlar/sektorel-some-rehberi, 16 Temmuz 2025 tarihinde ziyaret edildi.

[4] Bu bölümün hazırlanmasında büyük ölçüde aşağıdaki makaleden yararlanılmıştır. Detaylı bilgi için Bkz.;https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-2023-AFAD, Kritik%20Altyap%C4%B1lar%20 Korunmasi%20Yol%20Haritasi.pdf

geliştirilmesi hem de **ulusal siber güvenlik stratejilerinin afet senaryoları ile entegre edilmesi**, "***sürdürülebilir güvenlik yönetişimi***" için kaçınılmazdır.[5]

2. Afet Anında ve Sonrasında Görülen Siber Saldırı Türleri

Afet anlarında dijital sistemlere yönelik ***siber saldırılar***, hem doğal krizlerin ***etkisini artırmakta*** hem de müdahale ve iyileştirme süreçlerini ciddi biçimde ***sekteye uğratmaktadır***. Bu dönemlerde sistemlerin fiziksel olarak zarar görmesi, bilgi güvenliği önlemlerinin gevşemesi ve haberleşme trafiğindeki yoğunluk, dijital altyapıları saldırılara karşı savunmasız bırakır.

Özellikle afetin ilk saatlerinde kamu otoritelerine, haberleşme altyapılarına ve yardım platformlarına karşı düzenlenen saldırılar; ***halkta panik yaratmak, kamu güvenini sarsmak ve müdahale süreçlerini sabote etmek amacı*** taşır. Bu saldırıların büyük bir kısmı, ***hizmet reddi, veri ihlali, dolandırıcılık ve dezenformasyon*** şeklinde gerçekleşmektedir.

2.1. DDoS, Fidye Yazılımları, Veri Sızdırma ve Sosyal Mühendislik

DDoS (Dağıtık Hizmet Reddi Saldırıları):

Afet sırasında devlet kurumlarının ve acil müdahale birimlerinin web siteleri, aşırı trafikle işlevsiz hale getirilebilir. Bu saldırılar, müdahale ve bilgilendirme süreçlerini doğrudan etkiler. 2020 yılında Hırvatistan' daki deprem sonrası kamu bilgi portallarına yönelik yapılan ***DDoS saldırıları***, afetle ilgili *resmi bilgilendirme akışını durma noktasına getirmiştir.*

Fidye Yazılımları (Ransomware):

Kritik veri ve sistemlerin şifrelenerek erişilemez hale getirilmesiyle çalışır. Özellikle hastaneler ve belediyeler gibi dijital altyapılara sahip kamu kurumları hedef alınır. 2017'deki ***WannaCry saldırısı***, İngiltere'deki bazı **hastanelerde** *hizmet kesintilerine neden olmuş, ambulans yönlendirme sistemlerini devre dışı bırakmıştır.*

Veri Sızdırma ve Kimlik Avı:

[5] Bu bölümün hazırlanmasında büyük ölçüde aşağıdaki makaleden yararlanılmıştır. Detaylı bilgi için Bkz.; https://tubitak.gov.tr/tubitak_content_files//basin/siber-tatbikat-rapor/siber-tatbikat-rapor.pdf, (International Federation of Red Cross / IFRC), "Data Protection in Humanitarian Action", 2021. BBC News (2018). "Hawaii False Missile Alert: What Really Happened?"

Afet sonrası açılan yardım platformları ve online başvuru formları, saldırganlar tarafından sahte kopyalarla taklit edilerek vatandaşlardan kişisel bilgiler toplanabilir. 2023 Türkiye depremlerinde, ***bazı sahte bağış siteleri*** tespit edilmiş; ***BDDK ve BTK tarafından erişim engelleri*** uygulanmıştır.

Sosyal Mühendislik Saldırıları:

Panik hâlindeki bireylerin güvenlik açıklarını istismar ederek şifre, kimlik bilgisi veya erişim izni elde etmeyi hedefler. Saldırganlar afetle ilgili kurum kimliklerini taklit edebilir.

2.2. Örnek Olaylar: Acil Çağrı Sistemlerine Müdahale, Sahte Uyarı Mesajları

Afet anlarında, doğrudan acil müdahale sistemleri hedef alınabilir. Bu durum sadece teknik değil, aynı zamanda ***toplumsal etkileri olan çok boyutlu bir kriz çıkarabilir.***

Acil Çağrı Sistemlerine Müdahale:

112 gibi entegre çağrı merkezlerinin sunucularına yapılan siber saldırılar ya da bot saldırıları, acil müdahale kapasitesini doğrudan etkileyebilir. 2021 yılında ABD' nde Teksas bölgesinde yaşanan fırtına sırasında, bazı eyaletlerde 911 sistemlerine gelen ***anlık çağrı yoğunluğu bot saldırılarla karışmış ve sistemin çökmesine neden olmuştur.***

Sahte Uyarı Mesajları ve Dezenformasyon:

SMS, e-posta ya da sosyal medya yoluyla ***sahte tahliye uyarıları***, ***yardım bilgileri*** veya ***afet senaryoları*** yayılarak halk yönlendirilebilir. *2018 Hawai' de hatalı gönderilen bir nükleer füze uyarısı mesajı, ülke çapında büyük panik yaratmış;* olayın ardından mesaj güvenliği sistemleri yeniden yapılandırılmıştır.

Bu tür saldırılar sadece teknik birer eylem değil, aynı zamanda psikolojik savaş unsuru olarak da değerlendirilmektedir. *Afet zamanlarında bu tür dijital tehditlere karşı önceden hazırlıklı olmak,* ***hem teknik personel, hem de halk düzeyinde bilinç*** gerektirir.

Saldırı Türü	Etkileri	Önlemler
DDoS Saldırıları	Hizmet kesintisi, web sitelerine erişim engeli	Yük dengeleme, saldırı tespit sistemleri
Fidye Yazılımları	Kritik sistemlerin kilitlenmesi, veri kaybı	Yedekleme, güncel antivirüs ve yazılım yamaları
Veri Sızdırma	Kişisel bilgilerin ifşası, veri bütünlüğünün kaybolması	Veri şifreleme, erişim kontrol politikaları
Sosyal Mühendislik	Kullanıcıların kandırılması, yetkisiz erişim	Farkındalık eğitimi, çok faktörlü kimlik doğrulama
Sahte Uyarı Mesajları	Toplumsal panik, yanlış yönlendirme	Kaynak doğrulama, kriz iletişim protokolleri

3. Erken Uyarı Sistemleri, Sensör Ağları ve Güvenlik Açıkları

Afetlerin erken tespiti ve müdahale planlarının devreye alınabilmesi için geliştirilen ***erken uyarı sistemleri***, günümüzde yoğun biçimde dijital teknolojilere dayanmaktadır. Bu sistemler; sensör ağları, IoT tabanlı veri toplayıcılar, meteorolojik analiz platformları ve yapay zekâ destekli karar destek sistemlerinden oluşmaktadır. Ancak bu teknolojik altyapılar, ***siber güvenlik açıkları*** nedeniyle tehdit altında olabilir.

Afet anında bu sistemlerin hedef alınması; yanlış uyarıların verilmesi, verilerin çarpıtılması ya da sistemin tamamen devre dışı bırakılması gibi sonuçlar doğurabilir. Bu da sadece teknik değil, aynı zamanda ***toplumsal panik ve güven kaybına*** neden olur.

3.1. IoT Tabanlı İzleme Sistemlerinin Güvenliği

Afet izleme ve değerlendirme süreçlerinde kullanılan ***nesnelerin interneti (IoT)*** cihazları; deprem sensörleri, hava durumu izleme istasyonları, gaz kaçak algılayıcıları, su seviyesi ölçüm cihazları gibi unsurları içerir. Bu cihazlar genellikle düşük enerji tüketimi ve hafif protokollerle çalıştığı için, ***şifreleme, kimlik doğrulama ve güncelleme*** gibi temel güvenlik katmanlarından yoksun olabilir.

2019' da Kaliforniya' da kullanılan bazı orman yangını sensörleri, eski şifreleme protokolleri nedeniyle uzaktan manipüle edilmiş ve yangının yönü hakkında hatalı veriler üretilmiştir.[6]

[6] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program, 16 Temmuz 2025 tarihinde ziyaret edildi.

Güvenliği sağlanmamış IoT cihazları üzerinden yapılan saldırılar şunlara yol açabilir:

- Sensör verilerinin manipülasyonu,
- Sistem yöneticilerinin kimlik bilgilerinin çalınması,
- Cihazın uzaktan kontrol edilerek sabote edilmesi,
- Yerel ağlara zararlı yazılım yüklenmesi gibi.

Bu nedenle afet odaklı IoT cihazlarının ***hem yazılım hem donanım düzeyinde sertifikalı ve güncellenebilir sistemlerle desteklenmesi*** gereklidir.

3.2. Yapay Zekâ Destekli Tahmin Modellerine Yönelik Saldırı Senaryoları

Yapay zekâ tabanlı tahmin sistemleri; *deprem tahmini, sel riski analizi, halk hareketliliği takibi* gibi görevlerde ***büyük veri analitiği*** ve ***makine öğrenmesi*** tekniklerini kullanır. Bu sistemler, dış müdahaleye açık veri kaynaklarına (ör. sosyal medya, açık sensör ağları) bağımlı olduğu için ***veri zehirleme (data poisoning)*** gibi saldırı türlerine açık hâle gelir.

Örneğin bir araştırma grubu, hava durumu tahmin algoritmasını eğiten açık kaynaklı büyük veriye sahte rüzgar ölçümleri ekleyerek, YZ modelini kasırga yönünü yanlış tahmin etmeye zorlayabilir.

Bu tür saldırı senaryoları şunları içerebilir:

- Girdi verilerine bilinçli olarak yanıltıcı örnekler eklenmesi (***data poisoning***),
- Eğitim verisinin değiştirilmesi (***model corruption***),
- Tahmin sistemlerinin ***hata paylarının artırılması***,
- Olası risklerin olduğundan ***daha az veya fazla gösterilmesi***,

Yapay zekâ sistemlerinde güvenliğin sağlanabilmesi için, aşağıdaki ***tedbirler*** önerilmektedir:

- Model eğitimi sırasında veri ***doğrulama süreçlerinin güçlendirilmesi***,
- Kritik karar modellerinin ***çok kaynaklı veri ile desteklenmesi***,

YZ kararlarının insan denetimi ile kontrol edilmesi (***human-in-the-loop***),

- ***Açıklanabilir yapay zekâ*** (AYZ) ***prensiplerinin uygulanması,***

Konu	Siber Tehditler	Etkileri	Önlemler
IoT Tabanlı İzleme Sistemleri	Veri Manipülasyonu, kimlik hırsızlığı, cihaz etkileme	Yanlış sensör verisi, ağ güvenliği zafiyeti	Şifreleme, kimlik doğrulama,
YZ Destekli Tahmin Modelleri	Veri zehirleme, model bozulması, hatalı tahmin	Hatalı afet tahmini, karar alma sürecinin manipülasyonu	Veri doğrulama, AYZ kullanımı, insan denetimi,

4. Acil Durum Haberleşme Protokolleri ve Altyapı Koruma Önlemleri

Afet anlarında ilk etkilenen unsurlardan biri iletişim altyapısıdır. GSM baz istasyonları, internet servis sağlayıcıları ve uydu sistemleri yoğun trafik, enerji kesintileri ve fiziksel tahribat nedeniyle işlevsiz hale gelebilir. Bu durumda yalnızca teknoloji değil, aynı zamanda koordinasyon ve kriz iletişimi de sekteye uğrar. Bu nedenle, acil durumlarda iletişim altyapısının **dayanıklılığı** ve **sürdürülebilirliği**, afet yönetiminin temel unsurlarından biri hâline gelmiştir.

Kritik altyapıların koruması sadece teknik önlemlerle değil, aynı zamanda **kurumsal iş birliği, önceden tanımlanmış iletişim protokolleri ve alternatif haberleşme yöntemleri**yle sağlanmalıdır.

4.1. GSM, Uydu ve İnternet Tabanlı Sistemlerde Dayanıklılık

Modern iletişim altyapıları büyük ölçüde GSM, fiber internet ve uydu sistemlerine dayanır. Ancak bu sistemlerin hepsi; ***enerji kesintileri, veri trafiğindeki ani artış, DDoS saldırıları veya fiziksel yıkım*** gibi nedenlerle işlevini yitirebilir.

2023 Kahramanmaraş depremleri sırasında, birçok ilde GSM şebekeleri devre dışı kalmış, mobil iletişim yalnızca SMS ve internet üzerinden zamanlı çalışabilmiştir. Bu durum, afet bölgesine yardımın gecikmesine neden olmuştur.[7]

[7] Bu konuya ilişkin detaylı bir çalışma için bkz.; https://dergipark.org.tr/tr/download/article-file/3120243, 16 Temmuz 2025 tarihinde ziyaret edildi. ***Şen Revşan, Akgül Selma Koç, "WhatsApp Dayanışma Grupları ve***

2022 yılında yaşanan ***Tonga volkanik patlamasında***, ülkenin tek internet çıkış noktası olan denizaltı fiber kablosunun zarar görmesi, adanın dünyayla iletişimini tamamen kesmiştir.[8]

Dayanıklılığı artırmak için öneriler:

- Kritik baz istasyonlarının **yedek enerji kaynaklarıyla** desteklenmesi,
- **Mobil baz istasyonu (COW – Cell on Wheels)** sistemlerinin kullanımı,
- Uydu haberleşmesi için **VSAT sistemlerinin entegrasyonu**,
- Fiber altyapıların **çift yönlü ve yedekli güzergâhlarla** kurulması,
- Telekom şirketlerinin **ortak kriz protokolleri** geliştirmesi.

4.2. Afet Anında Alternatif İletişim Yöntemleri ve Kritik Uygulamalar

İletişim altyapısının devre dışı kaldığı durumlarda ***alternatif haberleşme sistemleri***, afet müdahalesi için kritik rol üstlenir. Bu sistemler, ***çoğunlukla bağımsız çalışan, merkezi bağlantıya ihtiyaç duymayan veya kısa menzilli çözümlerdir.***

Başlıca alternatif yöntemler:

- **Telsiz Sistemleri (VHF/UHF):** Emniyet, sağlık, belediye ve gönüllü kuruluşlar arasında doğrudan iletişim kurmak için yaygın biçimde kullanılır.
- **Mesh Ağ Teknolojileri:** Akıllı telefonlar arasında ağ oluşturup internet olmadan veri paylaşımı sağlar (Örneğin; ***FireChat uygulaması***).
- **Uydu Tabanlı Acil Uygulamalar:** ***Starlink, Inmarsat veya Iridium*** gibi sistemlerle SMS ve internet erişimi sağlanabilir.
- **Bluetooth/BLE tabanlı çözümler:** Kısa mesafeli acil iletişim için geliştirilen özel sistemler (Örneğin; ***Bridgefy***)

2021 Haiti depreminde internetin çökmesinden sonra gönüllüler arasında ***telsiz ağları ve Mesh sistemleri*** ile bilgi paylaşımı yapılmıştır.[9]

İletişim Uygulamaları: 6 Şubat 2023 Kahramanmaraş Depremleri", Araştırma Makalesi / Afet ve Risk Dergisi 6(4), 2023, (1410-1428).

[8] https://www.bbc.com/turkce/haberler-dunya-60087288, 16 Temmuz 2025 tarihinde ziyaret edildi.

[9] ***Yıldız Kürşat (Ed.) (2025), Afet Yönetimi ve Lojistik, Kuramdan Sayısal Modellemeye Dijital Entegrasyon, Bölüm.2 Keskin Büşra Nur, Deprem Lojistiği***, Serüven Yayınevi, Ankara, s.56.

Kritik uygulamalar arasında şunlar yer alır:

- **AFAD Acil Mobil Uygulaması**
- **112 Acil SMS Bildirim Sistemi**
- **e-Devlet Mobil Yardım Başvuru Platformu**
- **Kızılay Acil Kan Bildirim Sistemi**
- **Uydu Destekli Afet Haritalama Sistemleri (Örneğin; Copernicus EMS)**

Yöntem	Kullanım Alanı	Avantajı
Telsiz Sistemleri (VHF / UHF)	Kamu Kurumları, Arama Kurtarma	Bağımsız çalışır, anında haberleşme sağlar.
Mesh Ağ Teknolojileri	İnternet Dışı İletişim, Gönüllü Koordinasyonu	Geniş ağ kurmadan cihazlar arası iletişim sağlar.
Uydu Tabanlı Uygulamalar	İnternetsiz Alanlarda SMS ve Veri Aktarımı	Geniş kapsama alanı ve internet bağımsızlığı imkanı sunar.
Bluetooth / BLE Sistemleri	Kısa Mesafeli Bireysel İletişim	Düşük enerjiyle çalışır, hızlı bağlantı kurar.
Mobil Acil Uygulamalar	Vatandaş Bilgilendirme ve Yardım Başvurusu	Halkla doğrudan etkileşim ve resmi bildirim imkanı sağlar.

5. Sosyal Medya Manipülasyonu, Sahte Kampanyalar ve Bilgi Güvenliği

Afet dönemlerinde sosyal medya, hem halkı bilgilendirme hem de yardım koordinasyonu açısından güçlü bir araç hâline gelir. Ancak bu durum, aynı zamanda dijital manipülasyon, bilgi kirliliği ve siber suçların da hızla artmasına neden olur. Özellikle sosyal medya üzerinden yayılan ***dezenformasyon***, ***sahte yardım kampanyaları*** ve ***kimlik avı saldırıları***, *afetin etkisini psikolojik ve ekonomik boyutlarda derinleştirebilir.*

Bu tehditlerin önlenebilmesi için hem bireysel hem de kurumsal düzeyde ***dijital farkındalık***, ***medya okuryazarlığı*** ve ***güvenli çevrim içi davranış biçimlerinin geliştirilmesi*** büyük önem taşır.

5.1. Afet Döneminde Dezenformasyon ve Dijital Panik Yaratma Taktikleri

Dezenformasyon, afet dönemlerinde halk arasında korku, panik ve güvensizlik yaratmak amacıyla bilinçli olarak yayılan yanıltıcı bilgileri ifade eder. Sosyal medya üzerinden yayılan yanlış bilgiler, resmi yardım ve müdahale ekiplerinin çalışmalarını da sekteye uğratabilir.

2023 Kahramanmaraş depremi sonrası sosyal medyada "***baraj yıkıldı***", "***köprü çöktü***", "***yardımlar durduruldu***" gibi teyit edilmemiş bilgiler hızla yayılmış, *kamuoyunda panik havası yaratmıştır.* ***BTK,*** bu dönemde 150'den fazla ***sahte içerik hakkında işlem*** başlatıldığını açıklamıştır.

Dijital panik yaratma taktikleri şunları içerebilir;

- Sahte görüntü veya ses kayıtları paylaşmak,
- Korku diliyle yazılmış uyarı mesajları yaymak,
- Gerçek hesaplara benzeyen sahte profillerle bilgi yaymak,
- Afet bölgelerinde olmayan kişileri mağdur gibi göstererek halkı yanıltmak.

Çözüm yolları;

- Resmî kurumların teyitli bilgilendirme yapması,
- Sosyal medya platformlarının içerik doğrulama algoritmalarını güçlendirmesi,
- Vatandaşların dijital medya okuryazarlığının artırılması,
- Kriz dönemlerine özel "***Sosyal Medya Kriz Protokolleri***"nin uygulanması.

5.2. Sahte Bağış Siteleri, Kimlik Avı ve Siber Dolandırıcılık Örnekleri

Afet dönemleri, insanların yardım etme duygularının yoğunlaştığı dönemlerdir. Bu da kötü niyetli kişilerin duyguları suistimal ederek ***sahte bağış kampanyaları***, ***kimlik avı e-postaları*** ve ***dolandırıcılık siteleri*** yoluyla vatandaşları hedef almasına zemin hazırlar.

2023 Şubat depremi sonrası "***AFAD Yardım***" adıyla açılan **sahte siteler ve sosyal medya hesapları**, binlerce kişiyi dolandırmaya çalışmış, ***MASAK ve Emniyet Siber Suçlarla Mücadele Dairesi*** eşgüdümünde ***erişim engeli ve gözaltılar*** gerçekleşmiştir.

Sık karşılaşılan yöntemler;

- Gerçek yardım kuruluşlarının ismiyle benzer alan adlarına sahip sahte web siteleri,
- Acil yardım çağrısı gibi görünen e-postalar veya SMS' lerle banka / TCN bilgisi istenmesi,
- E-devlet kopyası gibi görünen ekranlar aracılığıyla vatandaş bilgilerinin çalınması,
- Bağış yapıldığında sistemin "*hata verdiğini*" göstererek tekrar ödeme almaya çalışan sahte arayüzler.

Önlemler;

- Resmî kaynaklara yönlendirme (e-Devlet, AFAD, Kızılay),
- HTTPS sertifikası olmayan sitelere karşı uyarılar,
- Kamu spotları ve görsel bilgilendirme kampanyaları,
- Kamu-özel iş birliği ile dijital bağış kanallarının merkezi olarak yürütülmesi.

6. Mobil Uygulamalar, Konum Tabanlı Servisler ve Yedekleme Politikaları

Afet dönemlerinde ***mobil uygulamalar*** ve ***konum tabanlı servisler***, hem ***bireysel güvenlik*** hem de kriz yönetimi açısından ***stratejik önem*** taşır. Afet bölgelerinde ***yardım koordinasyonu, tahliye yönlendirmeleri*** ve ***bilgi paylaşımı*** çoğunlukla ***mobil cihazlar aracılığıyla*** sağlanır.

Ancak bu uygulamaların yoğun kullanımı, aynı zamanda ***veri mahremiyeti, konum takibi, kimlik sızıntısı*** ve ***dijital manipülasyon*** gibi güvenlik sorunlarını da beraberinde getirir. Ayrıca, afet öncesi ve sonrası süreçlerde **kritik verilerin yedeklenmesi**, *sistemlerin sürekliliği açısından zorunluluktur.*

6.1. Afet Bilgilendirme Uygulamaları ve Veri Mahremiyeti

AFAD, 112 Acil, e-Devlet ve belediyelere ait mobil uygulamalar gibi araçlar, halkı bilgilendirme ve yönlendirme amacıyla yaygın şekilde kullanılmaktadır. Bu uygulamalarda yer alan konum verisi, kullanıcı bilgileri ve sağlık geçmişi gibi hassas bilgiler, saldırganlar için potansiyel hedeftir.

2020 Elazığ depremi sırasında bazı kullanıcıların lokasyon verilerinin üçüncü parti uygulamalar aracılığıyla izinsiz toplandığı iddia edilmiş, KVKK uyarı yayımlamıştır.

Önerilen önlemler;

- Kişisel verilerin anonimleştirilerek işlenmesi,
- Uygulamalarda açık rıza metinlerinin görünür hâle getirilmesi,
- Üçüncü taraf SDK' lara karşı denetim mekanizmalarının uygulanması,
- Uygulama güncellemelerinde siber güvenlik testlerinin zorunlu tutulması.

6.2. Kritik Verilerin Bulut Ortamında Güvenli Yedeklenmesi

Afet sırasında fiziksel sistemlerin zarar görmesi, veri kaybı riskini doğurur. Bu nedenle kamu kurumları, yerel yönetimler ve afet koordinasyon merkezlerinin **bulut tabanlı veri yedekleme sistemlerine** sahip olması hayati önem taşır.

2017 Meksika depreminde yerel afet yönetim merkezinin sunucuları zarar görmüş, ancak yedeklenen bulut verileri sayesinde operasyonlar sürdürülebilmiştir.

Etkin yedekleme stratejileri;

- 3-2-1 kuralı (3 kopya, 2 farklı ortam, 1 bulut yedeği),
- Yedeklerin farklı lokasyonlarda saklanması,
- Şifreleme ve erişim kontrolü uygulanması,
- Otomatik test edilen yedekleme sistemlerinin tercih edilmesi,

7. Kurumsal Tatbikatlar, Farkındalık Eğitimleri ve Siber Dayanıklılık

Afet ve kriz anlarında kurumların dijital varlıklarını, bilgi sistemlerini ve insan kaynaklarını nasıl yönettiği, ***siber dayanıklılığın temelini*** oluşturur. Bu nedenle afet senaryolarına uygun ***siber güvenlik tatbikatları*** ve ***farkındalık eğitimleri***, yalnızca BT ekiplerinin değil tüm organizasyonun hazırlık düzeyini artırır.

7.1. Tatbikat Senaryoları, Olay Müdahale Ekibi ve Simülasyonlar

Kurumların oluşturduğu ***Olay Müdahale Ekipleri (OME)***, kriz anında veri ihlali, sistem çökmesi ya da bilgi sızdırma olaylarına karşı ilk müdahaleyi gerçekleştiren birimdir. Bu ekiplerin yetkinliği, ancak düzenli ve gerçek senaryolara dayalı **simülasyon tatbikatlarıyla** artırılabilir.

2022' de ***Türkiye Siber Güvenlik Kümelenmesi*** tarafından düzenlenen "***Siber Tatbikat***" programına 40'tan fazla kamu kurumu katılmış, afet temalı siber senaryolar test edilmiştir.

Tatbikat türleri;

- Masa başı tatbikatı,

- Canlı sistem simülasyonu,
- Red Team / Blue Team senaryoları,
- Dijital kriz iletişimi uygulamaları.

7.2. Toplumsal Farkındalık Programları ve Kurumsal Eğitim Uygulamaları

Afetlerde dijital farkındalığın sadece teknik personele değil, tüm halka yayılması gerekir. *Sosyal medya kullanımı, sahte kampanya farkındalığı ve bilgi güvenliği* gibi konuların basit dille anlatıldığı ***farkındalık programları*** büyük önem taşır.

BTK, AFAD ve Milli Eğitim Bakanlığı iş birliğiyle geliştirilen "***Siber Farkındalık Eğitim Modülü***", afet sonrası dönem için halkın dijital davranışlarını yönlendirmeyi hedeflemiştir.

Uygulamalar;

- Okullarda ve halk eğitim merkezlerinde "***Afet ve Dijital Güvenlik Eğitimleri***",
- Belediyeler üzerinden SMS bilgilendirme sistemleri,
- Kamu spotları ve görsel farkındalık kampanyaları,
- Kamu personeline yönelik zorunlu siber hijyen eğitimi,
- ***Milli yazılım mühendisliği*** ile geliştirilen ***karar destek ve izleme sistemleri***,
- **TÜBİTAK**, **ASELSAN**, **HAVELSAN, BTK, OECD** gibi kurumların geliştirdiği afet ve güvenlik çözümleri ile yayımlanmış uyarılar[10],

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

"Dijital egemenlik", yalnızca teknik bir kavram değil; *ulusal karar alma süreçlerinin bağımsızlığı, veri yönetiminin kontrolü ve siber savaşlara hazırlık* açısından bir "***güvenlik doktrini"*** dir. 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.

[10] Bu konuda yapılan çalışmalar için bkz.; **TÜBİTAK BİLGEM** (2022), "*Kurumsal Siber Tatbikat Rehberi*". **BTK Akademi** (2023). "*Siber Farkındalık Eğitim Modülü*". **OECD** (2022), "*Cyber Resilience in Public Emergency Response*". **KVKK** (2021), "*Afet Dönemlerinde Kişisel Verilerin Korunması*"

Kaynakça

BBC News (2018), “Hawaii False Missile Alert: What Really Happened?”

BTK Akademi (2023), “Siber Farkındalık Eğitim Modülü”

KVKK (2021), “Afet Dönemlerinde Kişisel Verilerin Korunması”

TÜBİTAK BİLGEM (2022), “Kurumsal Siber Tatbikat Rehberi”

OECD (2022), “Cyber Resilience in Public Emergency Response”

Şen Revşan, Akgül Selma Koç, “WhatsApp Dayanışma Grupları ve İletişim Uygulamaları: 6 Şubat 2023 Kahramanmaraş Depremleri”, Araştırma Makalesi / Afet ve Risk Dergisi 6(4), 2023, (1410-1428).

Yıldız Kürşat (Ed.) (2025), Afet Yönetimi ve Lojistik, Kuramdan Sayısal Modellemeye Dijital Entegrasyon, Bölüm.2 **Keskin Büşra Nur**, Deprem Lojistiği, Serüven Yayınevi, Ankara.

İnternet Linkleri

https://www.haberturk.com/operatorler-yine-sinifta-kaldi-3564007-teknoloji, 15 Temmuz 2025 tarihinde ziyaret edildi.

https://nis2directive.eu/what-is-nis2/, 16 Temmuz 2025 tarihinde ziyaret edildi.

https://www.usom.gov.tr/faydali-dokumanlar/sektorel-some-rehberi, 16 Temmuz 2025 tarihinde ziyaret edildi.

https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-2023-AFAD, Kritik%20Altyap%C4%B1larin%20 Korunmasi%20Yol%20Haritasi.pdf

https://tubitak.gov.tr/tubitak_content_files//basin/siber-tatbikat-rapor/siber-tatbikat-rapor.pdf, (International Federation of Red Cross / IFRC), “Data Protection in Humanitarian Action”, 2021.

https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program, 16 Temmuz 2025 tarihinde ziyaret edildi.

https://dergipark.org.tr/tr/download/article-file/3120243, 16 Temmuz 2025 tarihinde ziyaret edildi.

https://www.bbc.com/turkce/haberler-dunya-60087288, 16 Temmuz 2025 tarihinde ziyaret edildi.

Afetlerde Bilişim ve İletişim Teknolojilerinde 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