"TEKNOLOJİ SINIR TANIMIYOR, TEHDİTLER DE..."
YAPAY ZEKÂ
DESTEKLİ
SUÇ ÖRGÜTLERİ
DİJİTAL DÜNYADAN SAVAŞ ALANINA
Deepfake, Siber Suç, Kritik Altyapılar, Savunma Sanayii ve Yeni Nesil Küresel Tehditler
SİBER SUÇ
DEEPFAKE
KRİTİK ALTYAPI
SAVUNMA SANAYİİ
UZAY GÜVENLİĞİ
HAVACILIK
ENERJİ
BAĞLANTILI ARAÇLAR
ULUSLARARASI HUKUK
YENİ TEHDİTLER
DAHA GÜVENLİ BİR DÜNYA MÜMKÜN
AI
BM
NATO
AB
ABD Savunma Bakanlığı
Rusya Savunma Bakanlığı
Siber Kuvvetler
Selçuk DİKİCİ
Endüstri Mühendisi
(Bilişim Teknolojileri ve Siber Güvenlik Uzmanı)
www.selcukdikici.com.tr
"Geleceği korumak, bugünü anlamakla başlar."
ARAŞTIRMA | SENARYO | ANALİZ | ÇÖZÜM

YAYIN NOTU

Bu kitap, gerçek olayları ve kamuya açık resmî kayıtları; açıkça “KURGU SENARYO” olarak işaretlenmiş öğretici senaryolarla bir araya getiren araştırma-anlatı çalışmasıdır. Gerçek olaylarda iddia, soruşturma, iddianame, mahkûmiyet ve kesinleşmiş karar kavramları birbirinden ayrılmıştır. Kurgu bölümlerde gerçek kişi veya kuruma suç isnadı yapılmaz.

Hava aracı, uzay aracı, bağlantılı araç, enerji, haberleşme, savunma ve kritik altyapı bölümleri saldırı gerçekleştirme kılavuzu değildir. Teknik ayrıntılar; dayanıklılık, segmentasyon, doğrulama, yedeklilik, insan gözetimi, olay müdahalesi, adli delil ve güvenli geri kazanım düzeyinde tutulmuştur.

Kitaptaki uluslararası kurum ve düzenleme bölümleri 11 Eylül 2026 tarihine kadar doğrulanabilen açık kaynak bilgileri esas alır. Birleşmiş Milletler Siber Suçlar Sözleşmesi bu tarih itibarıyla henüz yürürlükte değildir; BM Antlaşmalar Koleksiyonunda 82 imzacı ve 3 taraf görünmektedir.

KAYNAK NOTU
Birleşmiş Milletler Antlaşmalar Koleksiyonu; NATO; ICAO; ESA; UNECE; Avrupa Komisyonu; INTERPOL; ABD Adalet Bakanlığı; Hong Kong Hükümeti; Singapur Polisi; Türkiye Cumhuriyeti resmî kurumları.

YAZAR HAKKINDA

Selçuk DİKİCİ

Endüstri Mühendisi

(Bilişim Teknolojileri ve Siber Güvenlik Uzmanı)

Fotoğraf: Yazarın kişisel arşivi

Selçuk DİKİCİ, Bursa doğumlu Endüstri Mühendisidir. İstanbul Üniversitesi Endüstri Mühendisliği lisans mezunudur; Anadolu Üniversitesi İşletme Fakültesi lisans ve Hukuk/Adalet önlisans, Abant İzzet Baysal Üniversitesi Endüstriyel Elektronik önlisans eğitimlerini tamamlamıştır.

Bilgi Teknolojileri Kurumu onaylı Sistem Mühendisliği belgesi ile Cisco Ethical Hacker, Python Essentials ve AI Fundamentals eğitimlerinin yanı sıra SIEM, doğal dil işleme, veri modelleme, sosyal mühendislik, bilgi güvenliği yönetim sistemi ve siber olay tespit/müdahale gibi alanlarda eğitim kayıtları yer almaktadır.

DİKİCİ'nin yayımladığı çalışmalar; siber güvenlik, adli bilişim, yapay zekâ, risk yönetimi, sağlık bilişimi, savunma teknolojileri ve endüstri mühendisliği ekseninde çok disiplinli bir çizgi izlemektedir. Bu kitapta da mühendislikte risk analizi yaklaşımı; hukuk, kamu güvenliği, savunma, uluslararası ilişkiler ve dijital adli bilişimle birleştirilmiştir.

KAYNAK NOTU

Yazar özgeçmişi: www.selcukdikici.com.tr/selcuk-dikici/

ÖN SÖZ

Bir suç örgütünü tehlikeli yapan yalnızca sahip olduğu insan sayısı değildir. Onu tehlikeli yapan; para, bilgi, korku ve güven arasında kurduğu sistemdir. Yapay zekâ bu sisteme yeni bir hız kazandırdı. Bir zamanlar sahte kimlik hazırlamak, farklı dillerde yüzlerce kişiye ulaşmak, bir yöneticinin sesini taklit etmek veya kurbanın psikolojik profilini çıkarmak günler alabiliyordu. Bugün aynı süreçlerin bir bölümü dakikalara inebiliyor.

Bu kitapta okuyucu bazen Hong Kong'daki gerçek bir deepfake dolandırıcılığının içine girecek, bazen Singapur'da kamu görevlilerini taklit eden bir sahte toplantının nasıl milyonlarca dolarlık kayba dönüştüğünü görecek, bazen de tamamen kurgu olan bir senaryoda gece yarısı uydu telemetrisindeki tutarsızlığı fark eden bir operasyon merkezine girecek.

Ama her hikâyenin sonunda aynı soru sorulacak: Nerede durdurulabilirdi? Çünkü güvenlik, saldırganın ne kadar yaratıcı olduğuna hayran olmak değil; zincirin hangi halkasında kontrol kurulacağını bilmektir.

İÇİNDEKİLER — ANA BÖLÜMLER

1. Yapay Zekâ Çağında Organize Suç
2. Gerçek Vakalar: Deepfake, Dolandırıcılık ve Devlet Bağlantılı Ağlar
3. Kurgu Senaryolar: Olası Krizlerin İçinden
4. Birleşmiş Milletler ve Küresel Siber Suç Hukuku
5. NATO, Siber Savunma ve Yapay Zekâ
6. ABD Savunma Bakanlığı ve Sorumlu Askerî AI
7. Rusya, Çin, Kuzey Kore ve Devlet Bağlantılı Siber Kapasiteler
8. Avrupa Birliği AI Act ve Dijital Hukuk
9. INTERPOL, UNODC ve Ulusötesi Suç Ağları
10. Uluslararası Mahkemeler, Ceza Davaları ve Dijital Delil
11. Havacılık Siber Güvenliği
12. Uzay Araçları ve Uydu Siber Dayanıklılığı
13. Bağlantılı ve Otonom Araçlar
14. Enerji, Haberleşme ve Kritik Altyapılar
15. Savunma Sanayii ve AI Zafiyet Sınıfları
16. Türkiye İçin Ulusal Yapay Zekâ Suçlarıyla Mücadele Modeli
17. Kurumsal Olay Müdahalesi ve Adli Bilişim
18. Gelecek: Agentic AI, Otonom Suç Zincirleri ve Savunmanın Evrimi

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 001 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 002 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

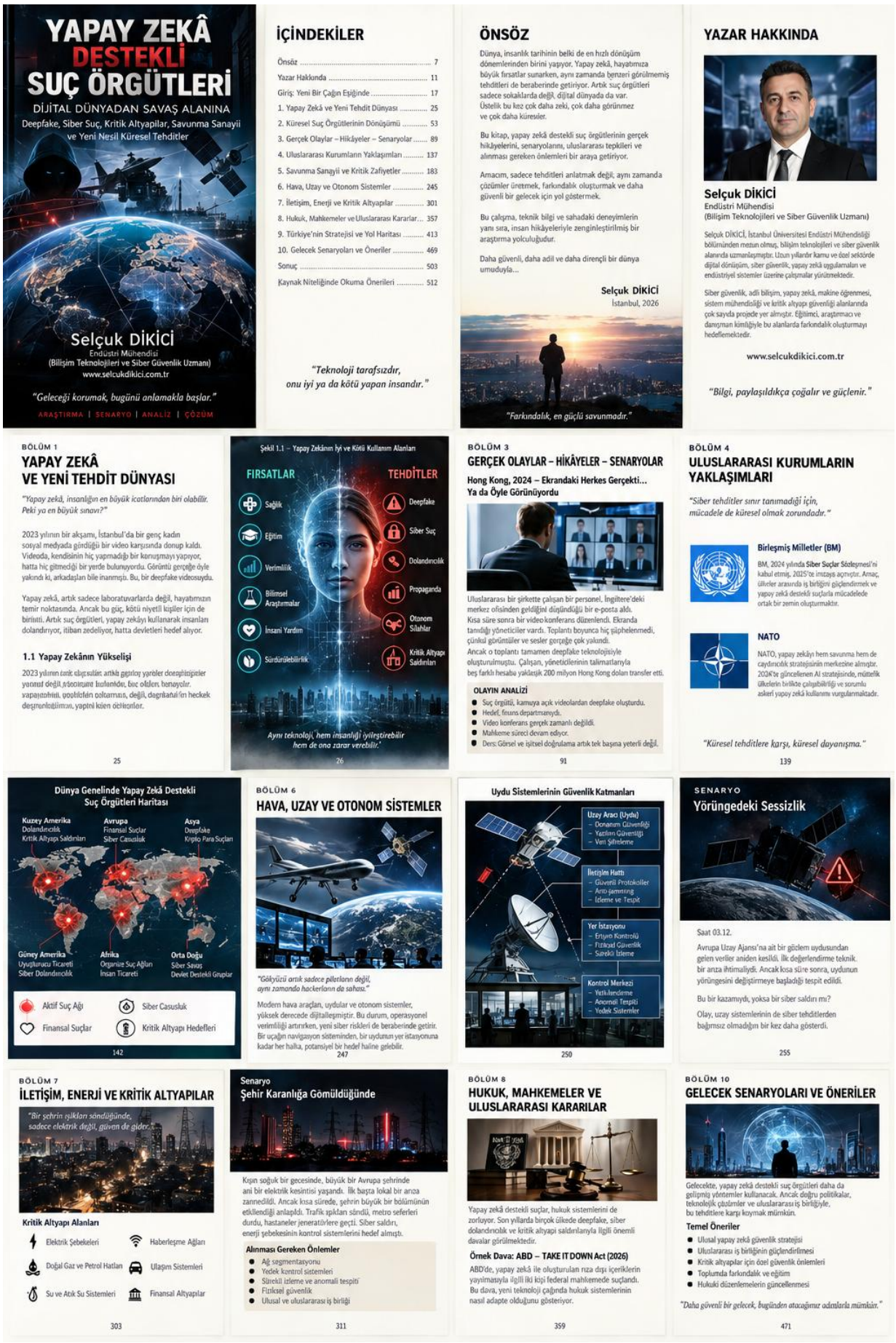
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 003 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 004 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

Saat 13.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 005 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 006 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

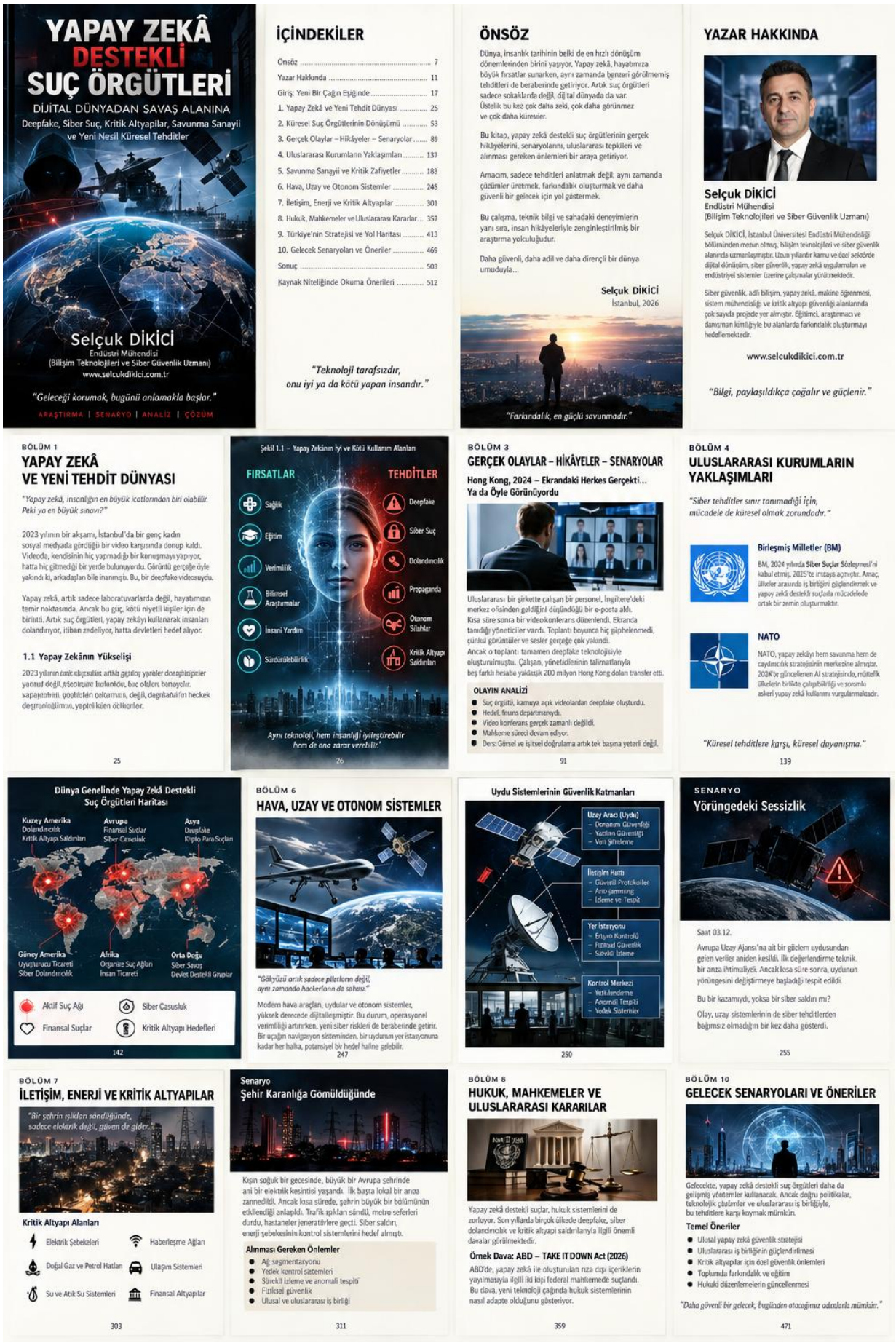
ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 007 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 008 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

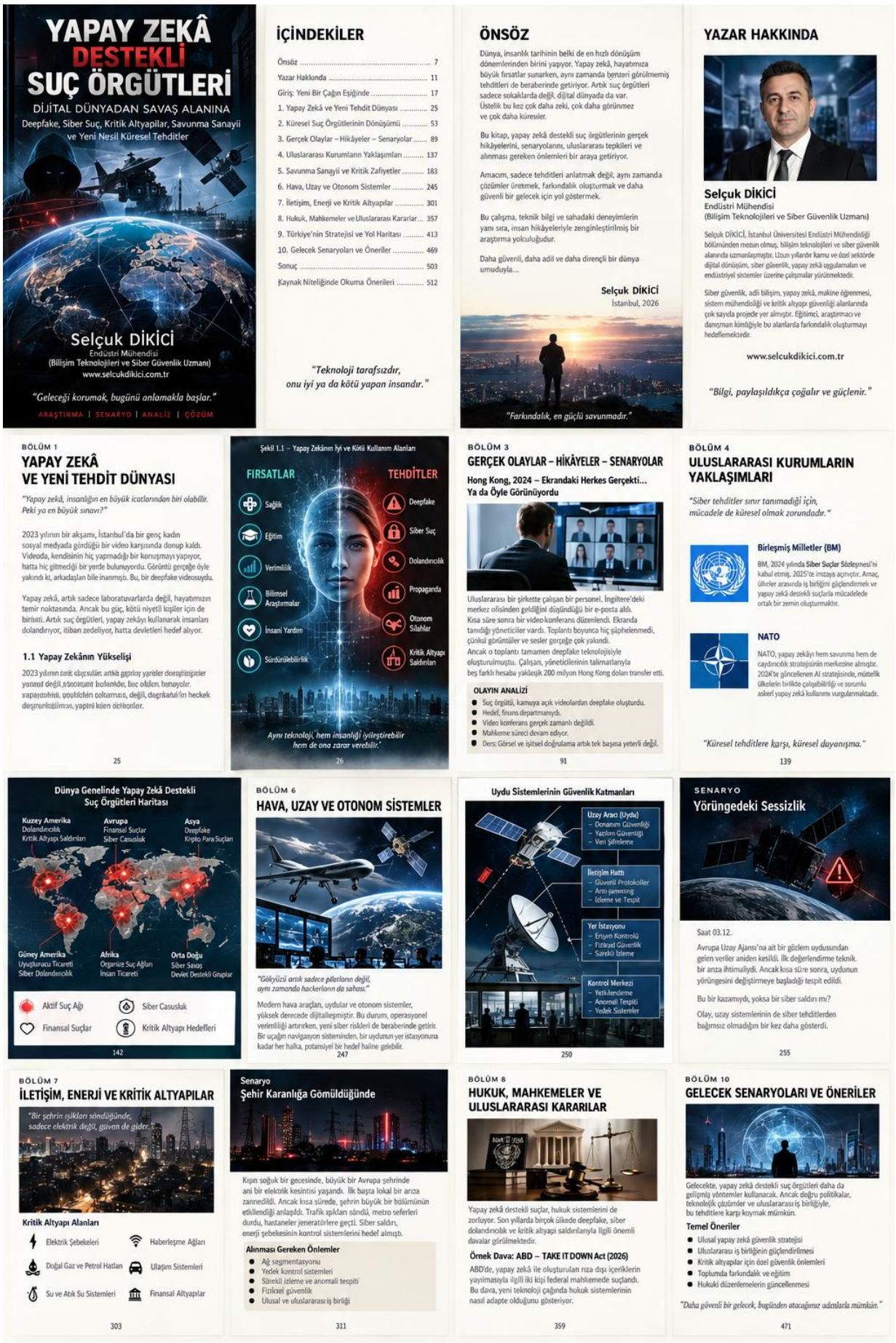
HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 009 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 010 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

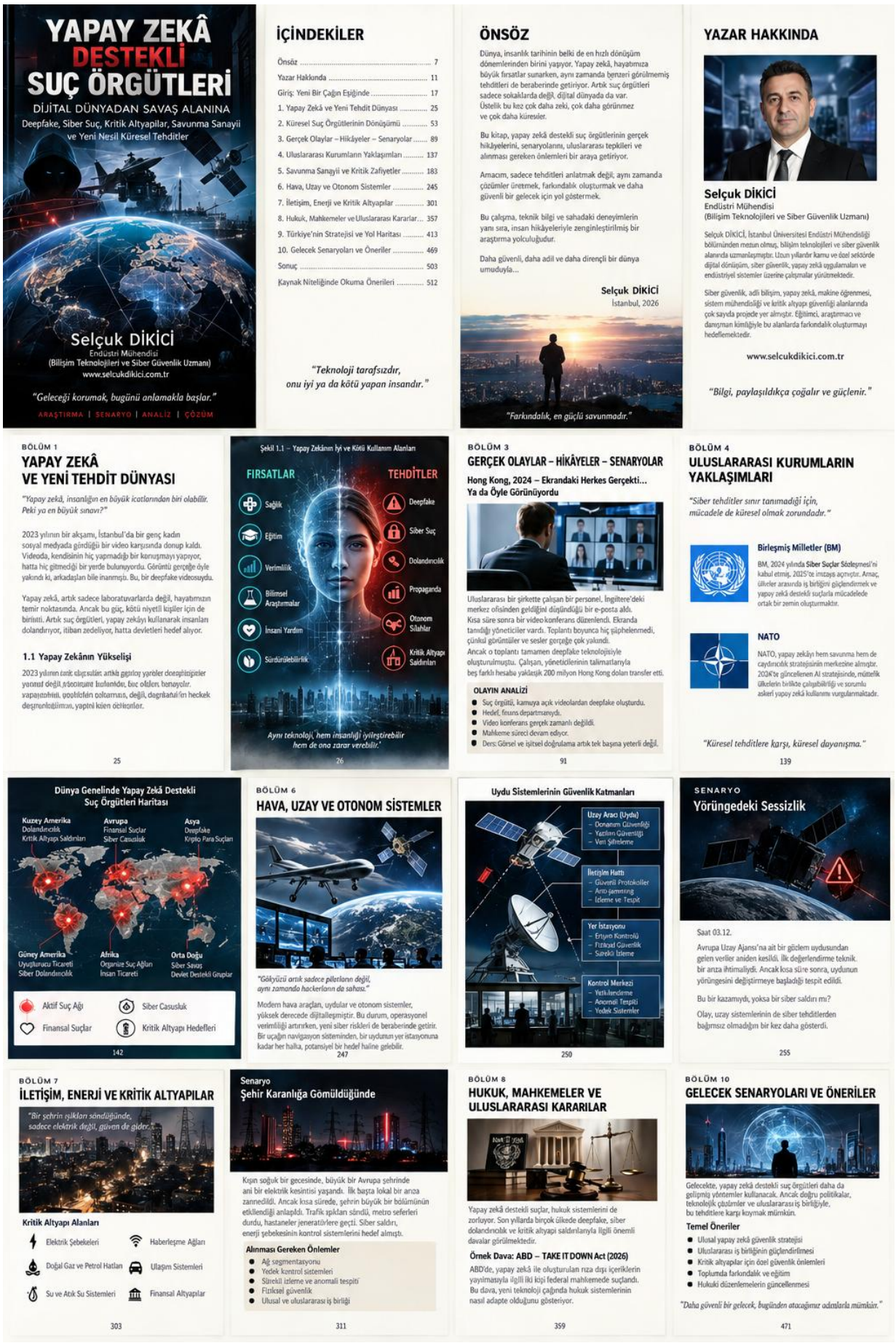
Saat 13.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 011 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 012 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 013 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 014 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

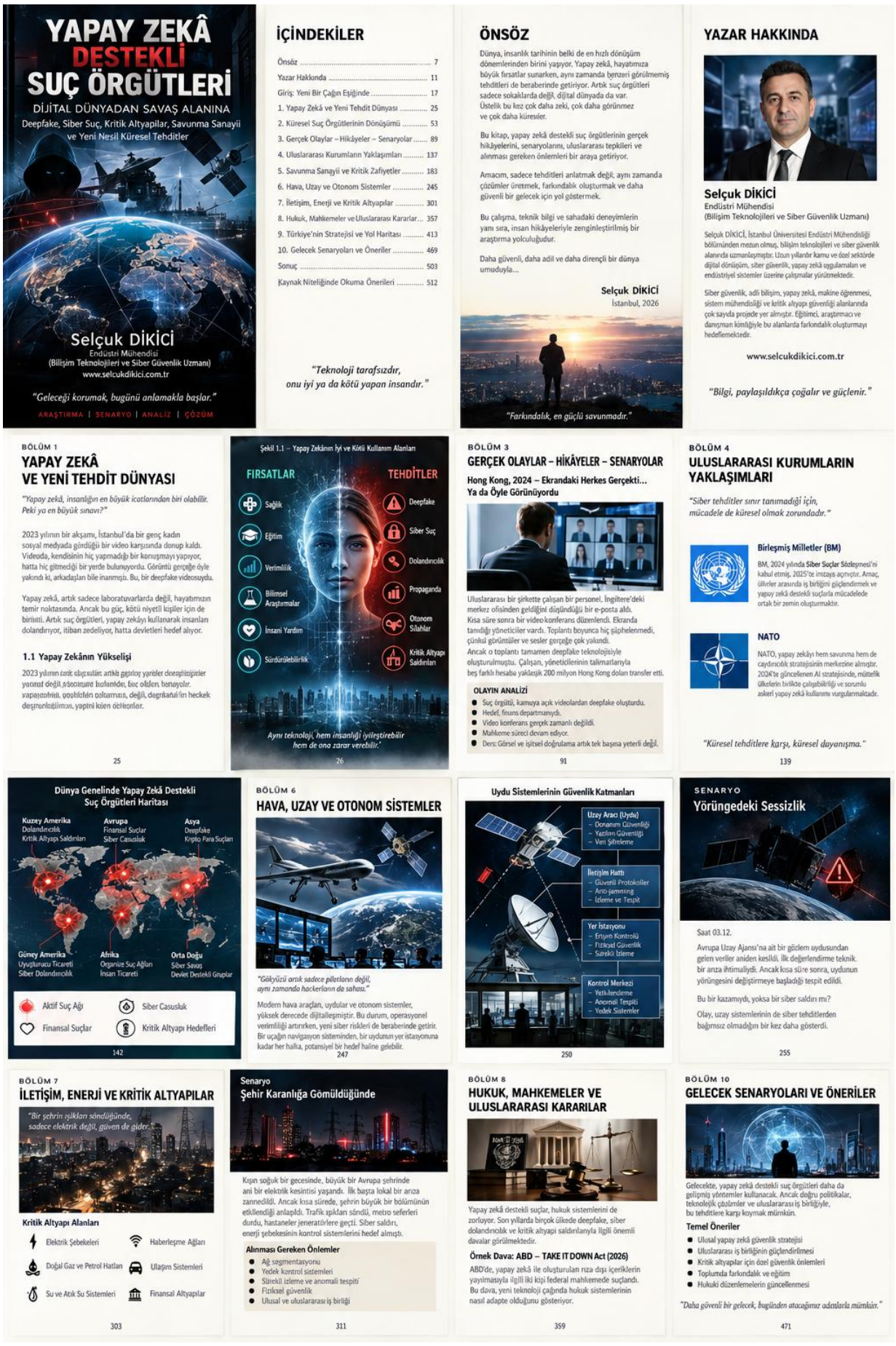
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 015 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 016 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Otonom Filoda Güven Krizi

Saat 13.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 017 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 018 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

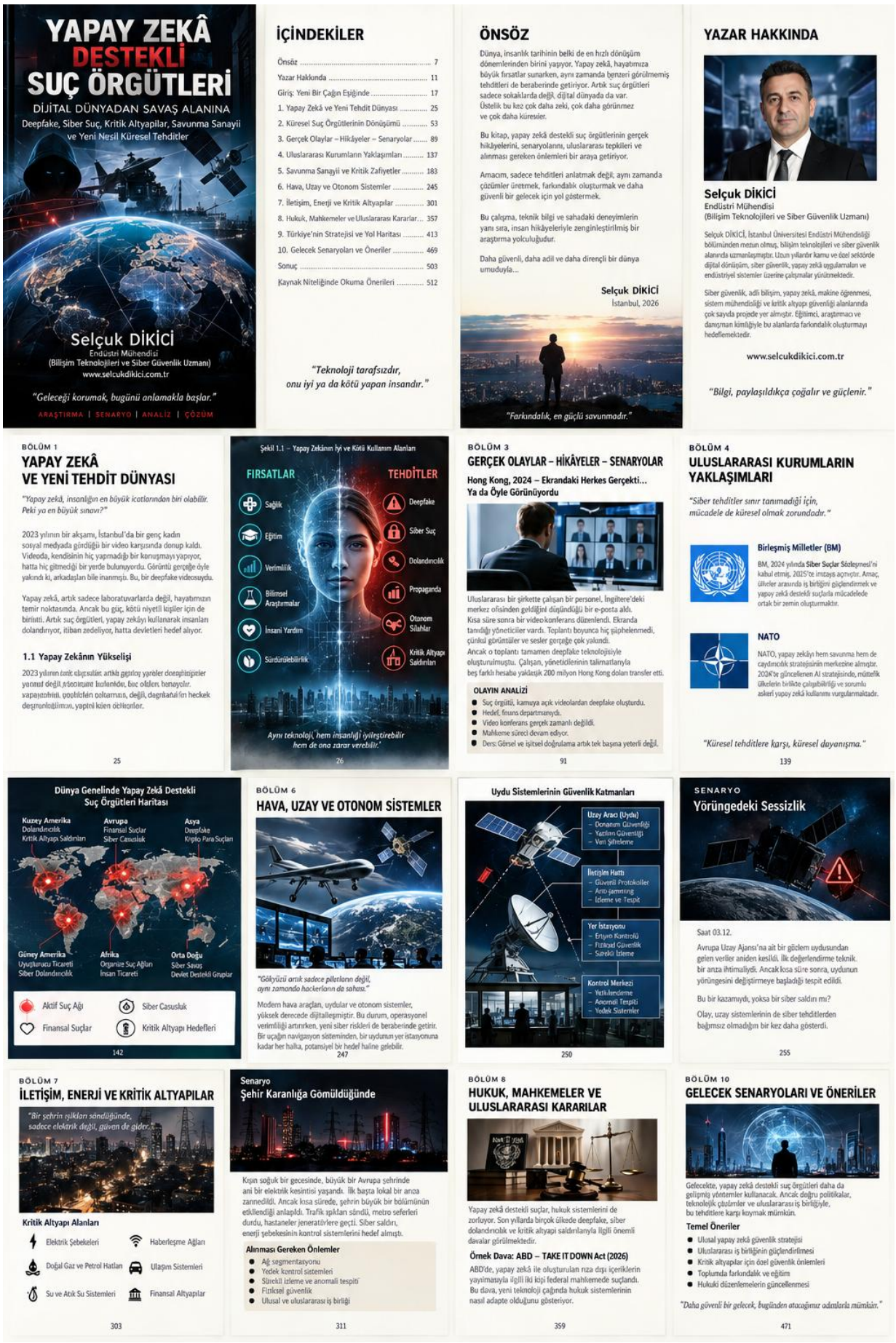
ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 019 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 020 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

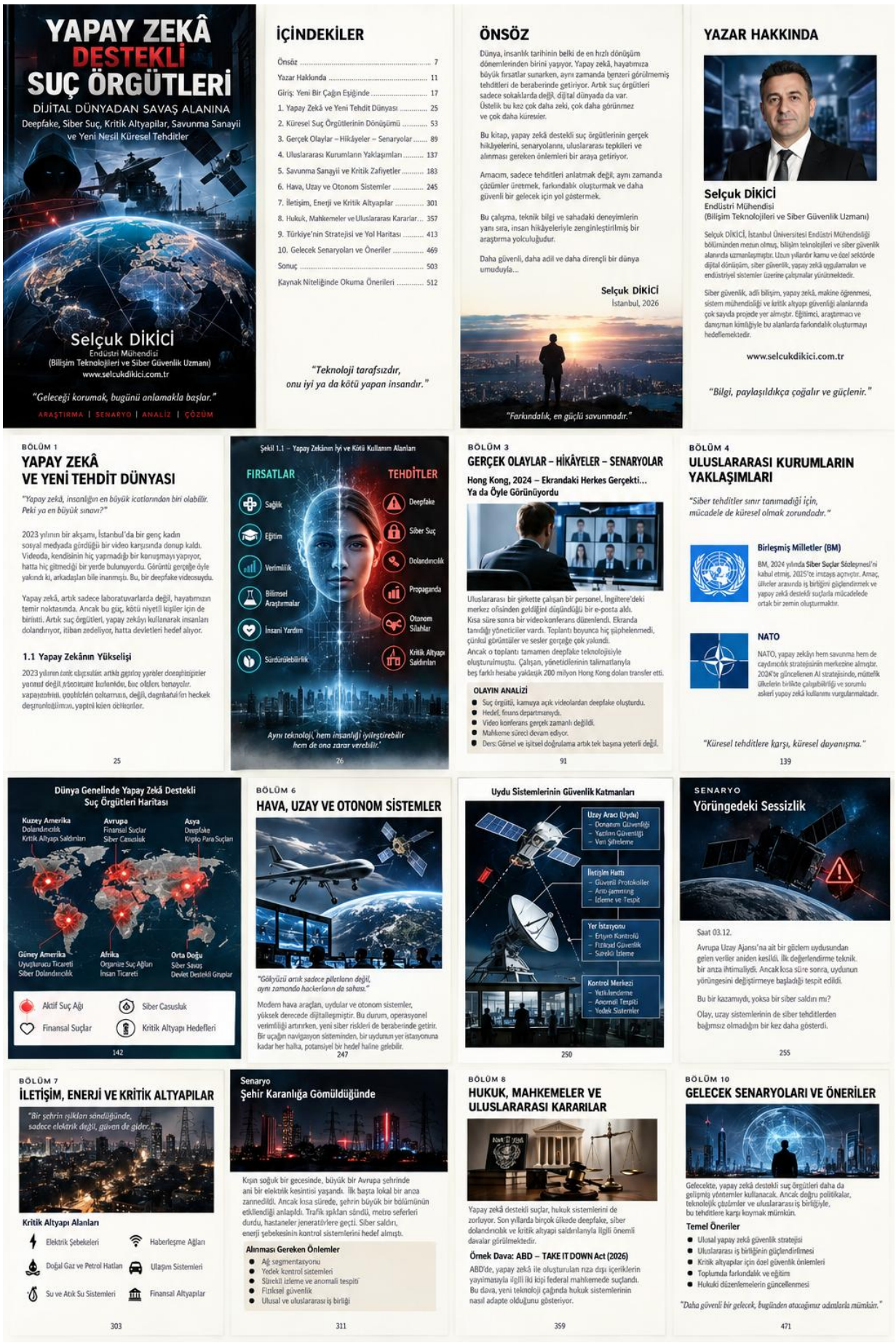
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 021 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 022 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

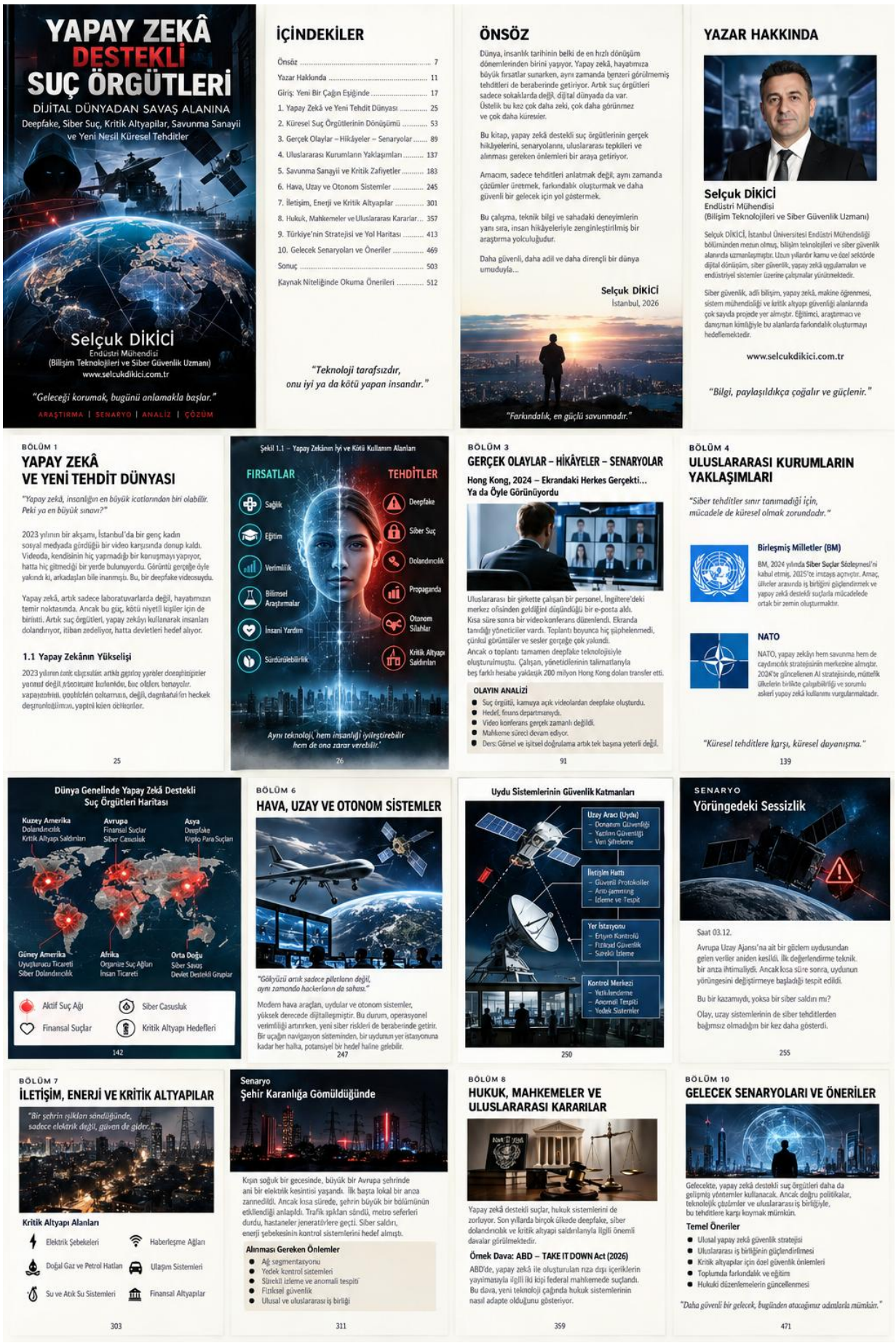
Saat 13.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 023 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 024 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

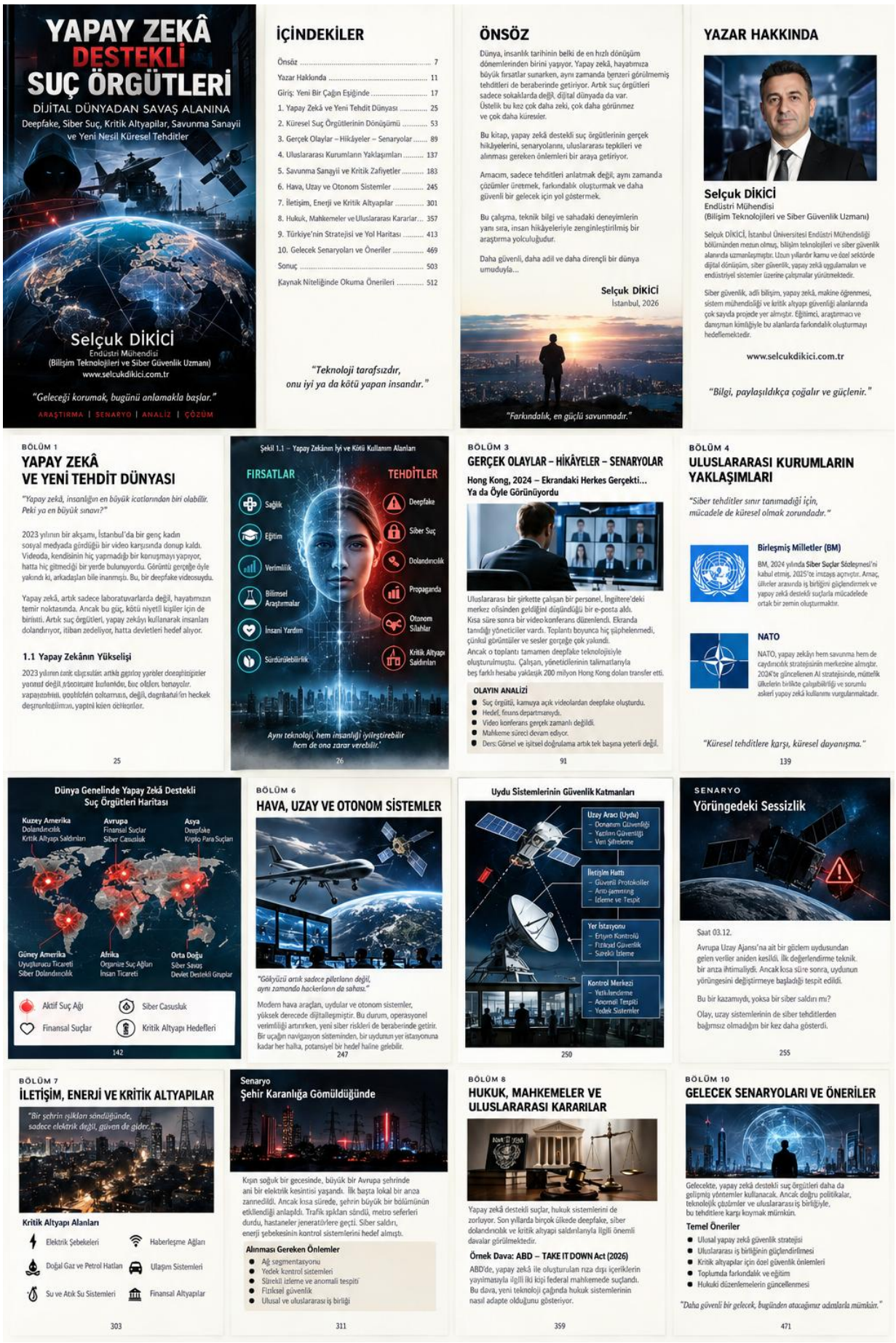
ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 025 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 026 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

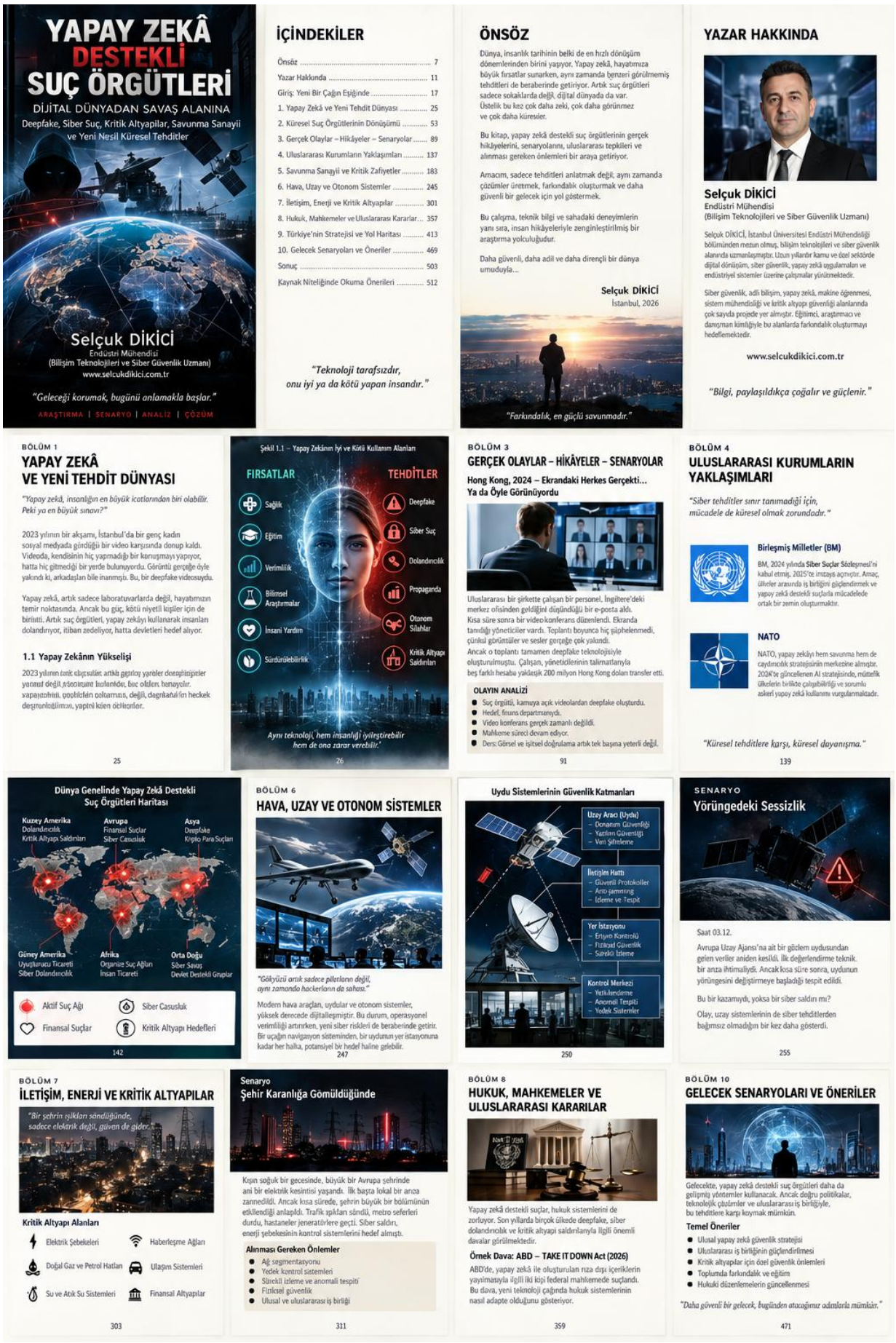
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 027 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 028 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

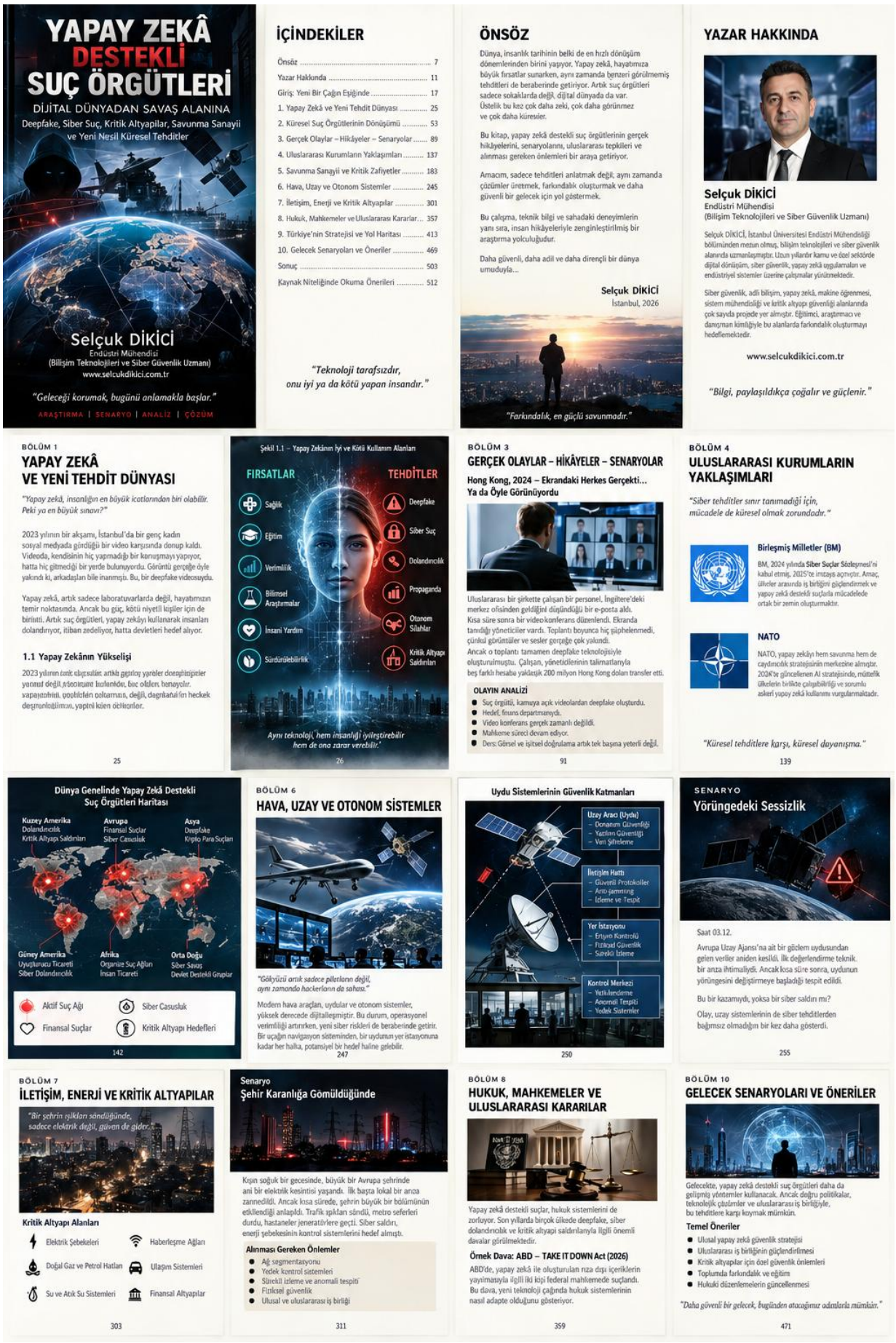
Saat 13.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 029 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 030 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

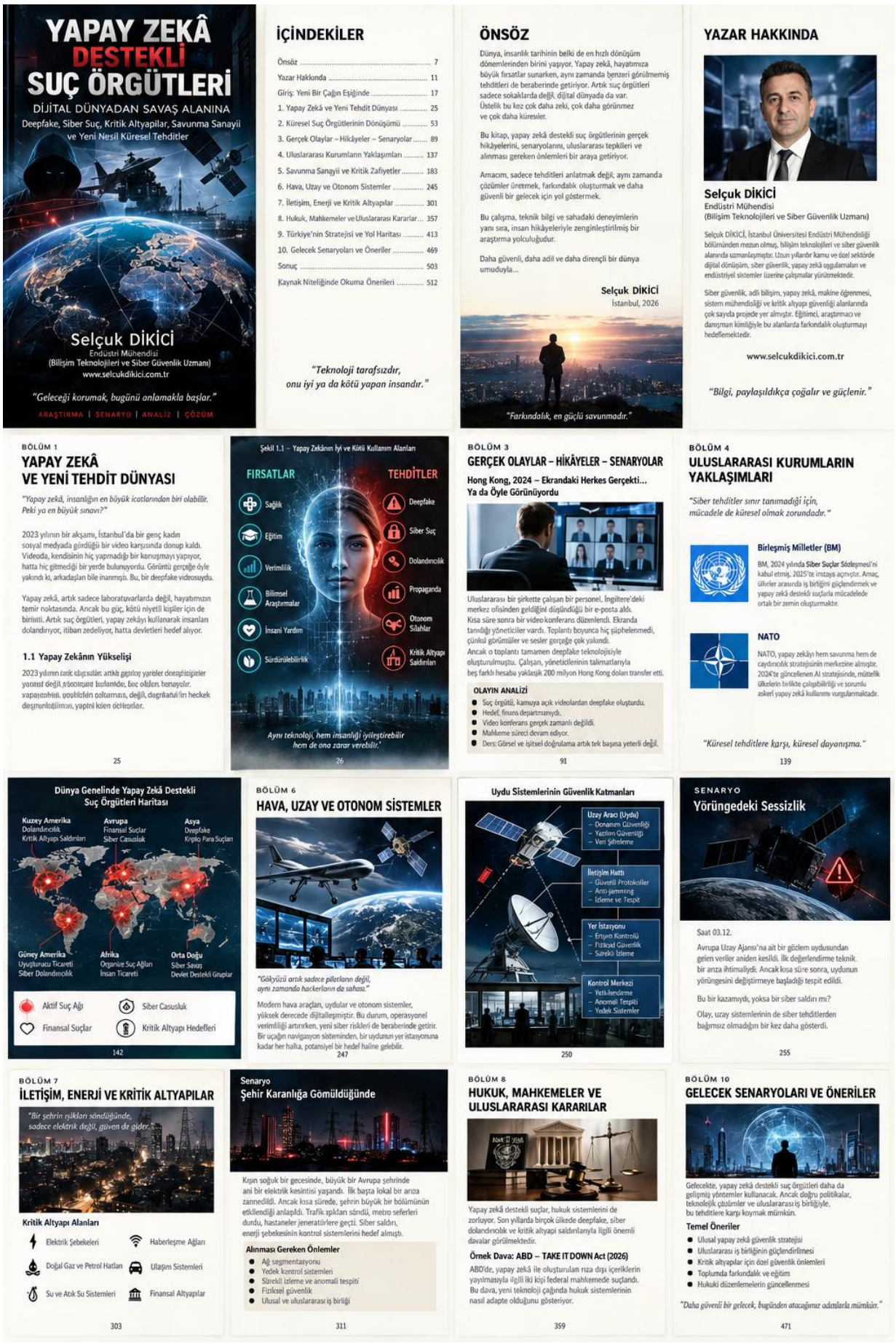
ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 031 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 032 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

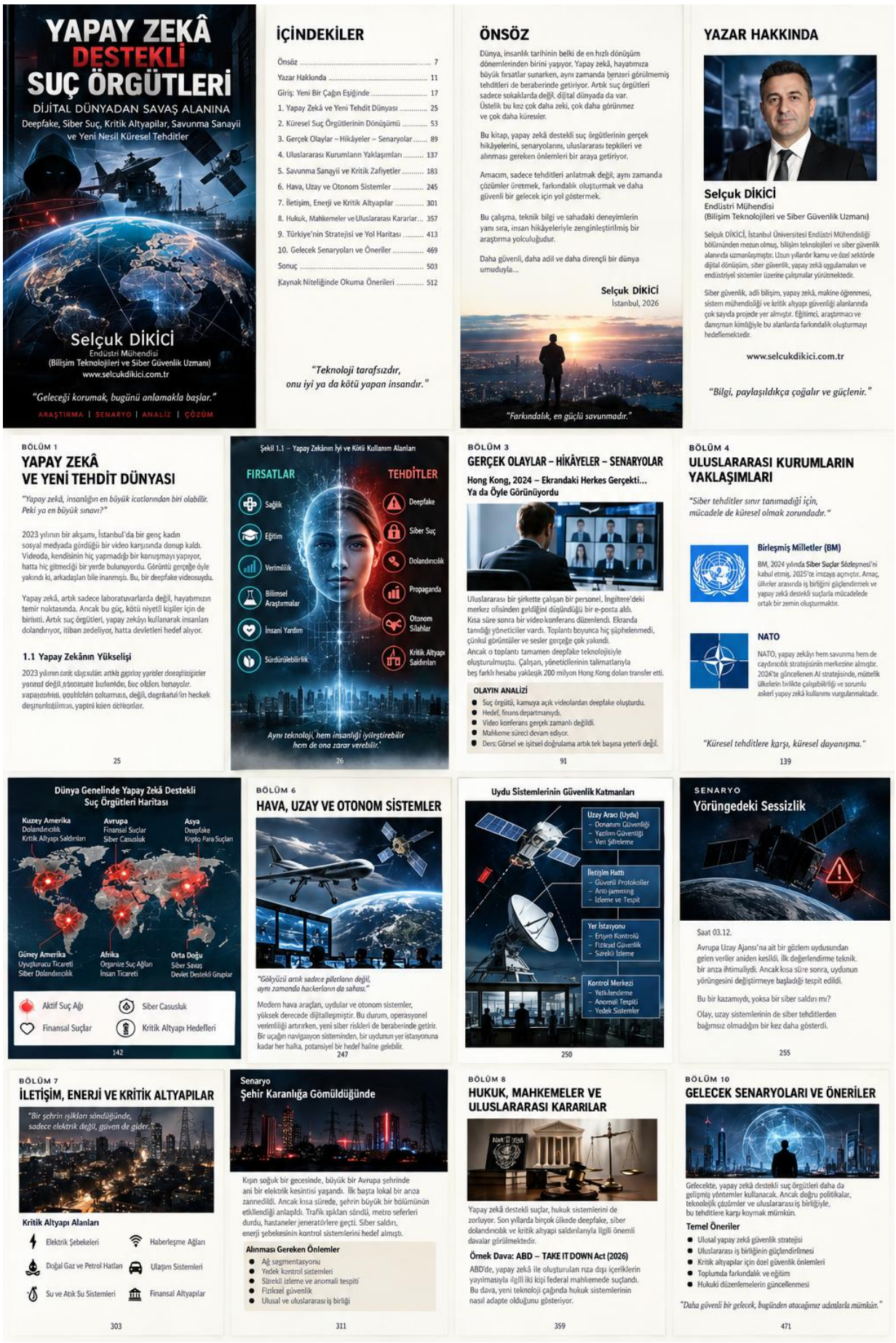
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 033 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 034 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Otonom Filoda Güven Krizi

Saat 13.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 035 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 036 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

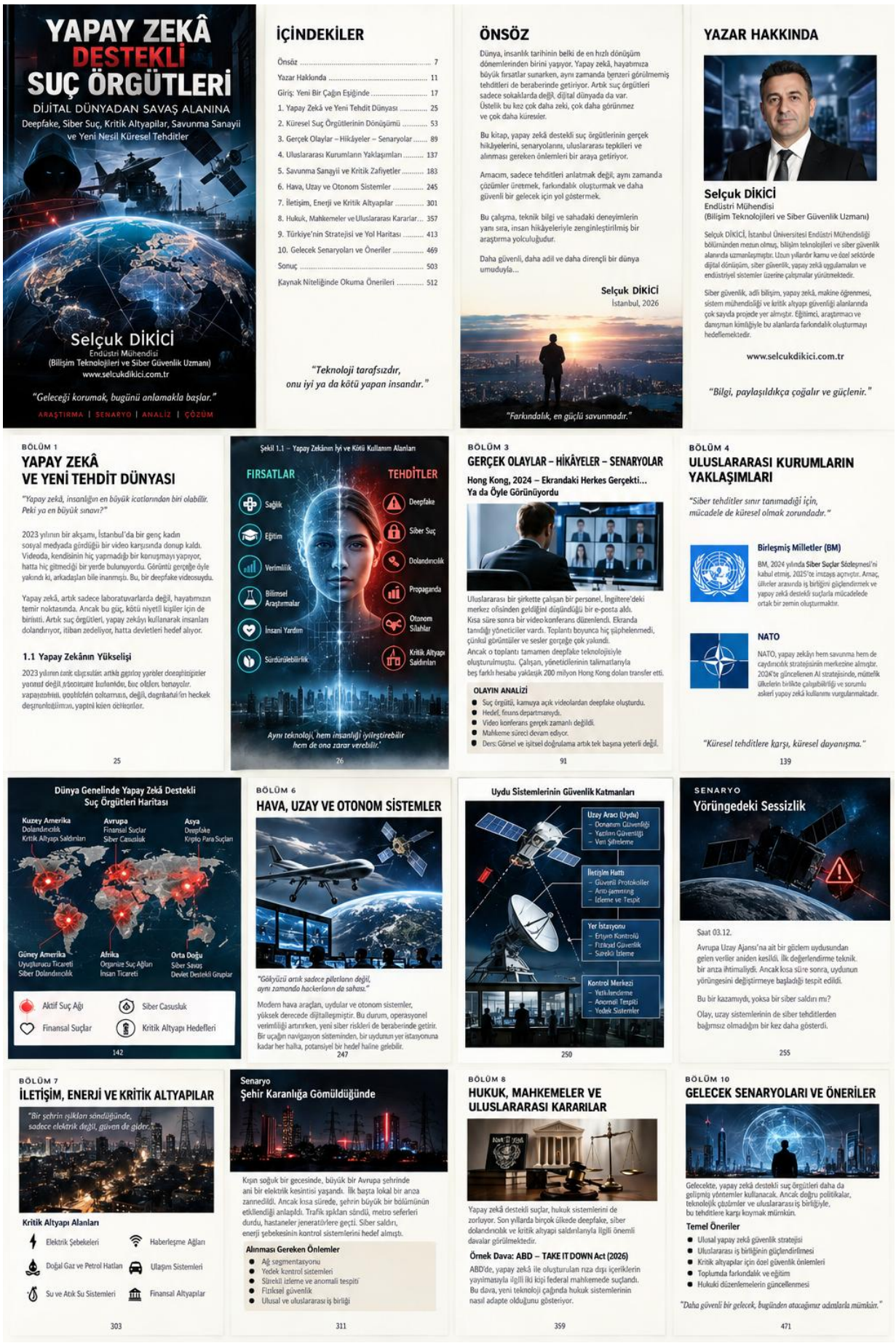
ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 037 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 038 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

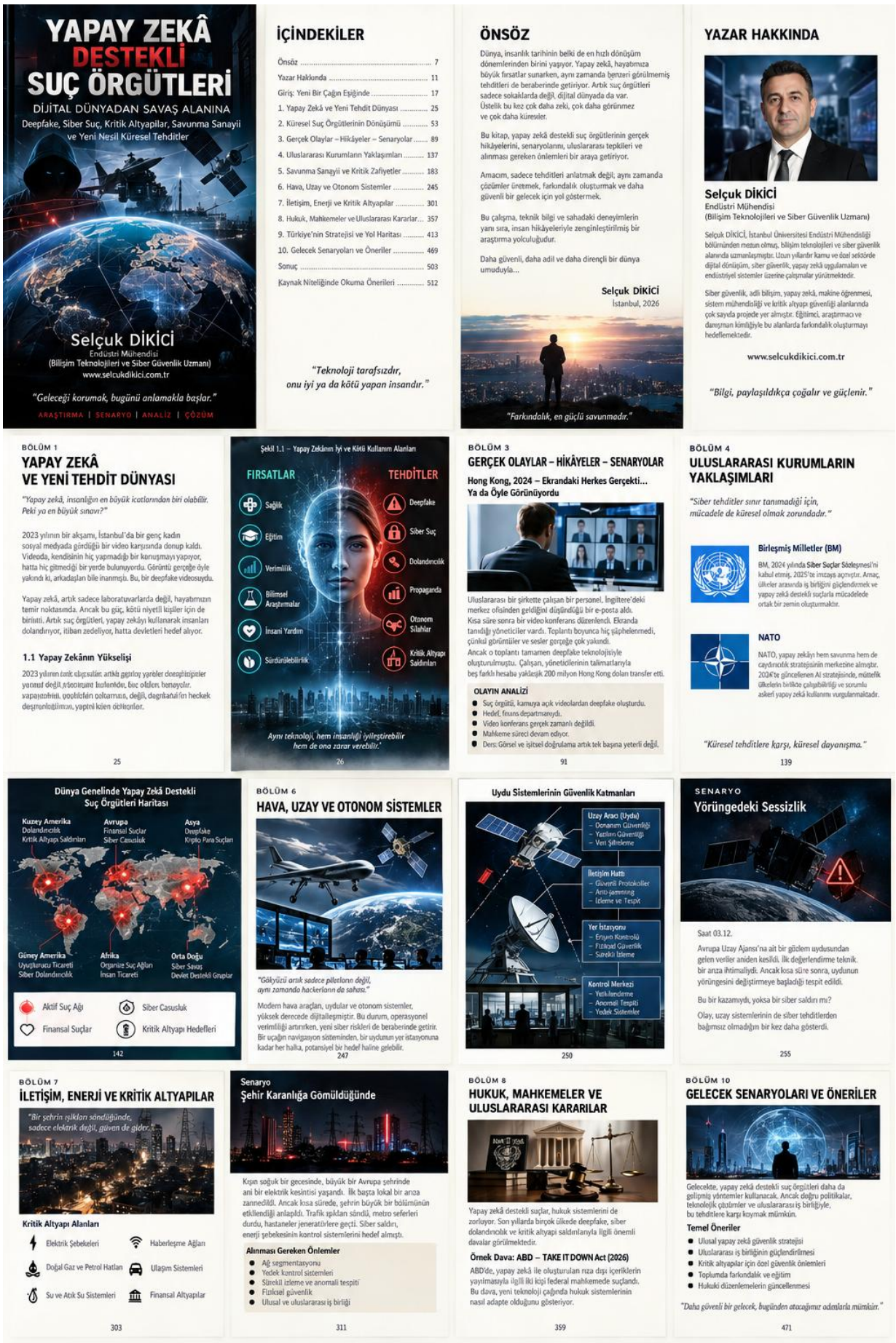
HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 039 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 040 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

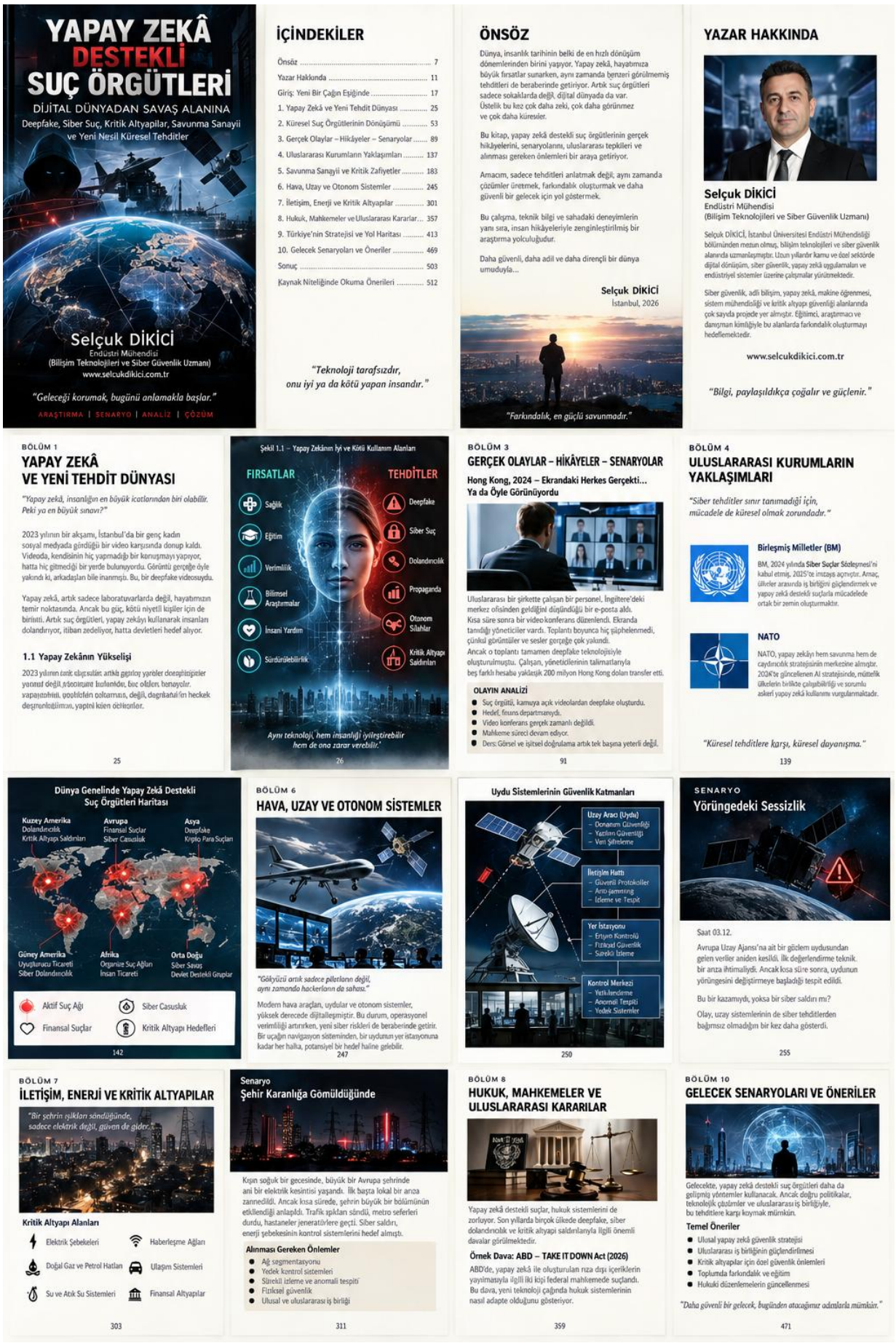
Saat 13.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 041 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 042 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 043 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 044 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

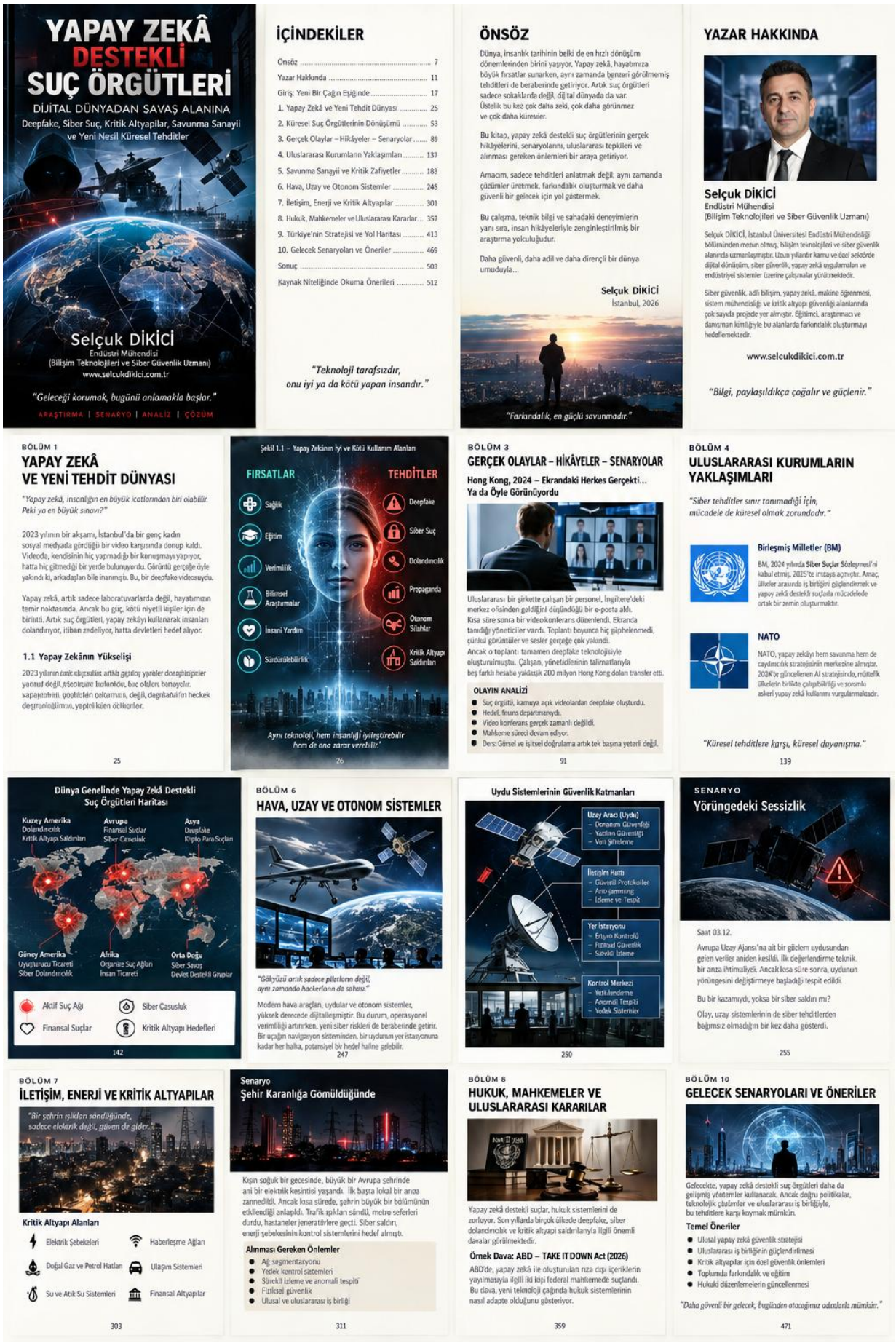
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 045 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 046 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

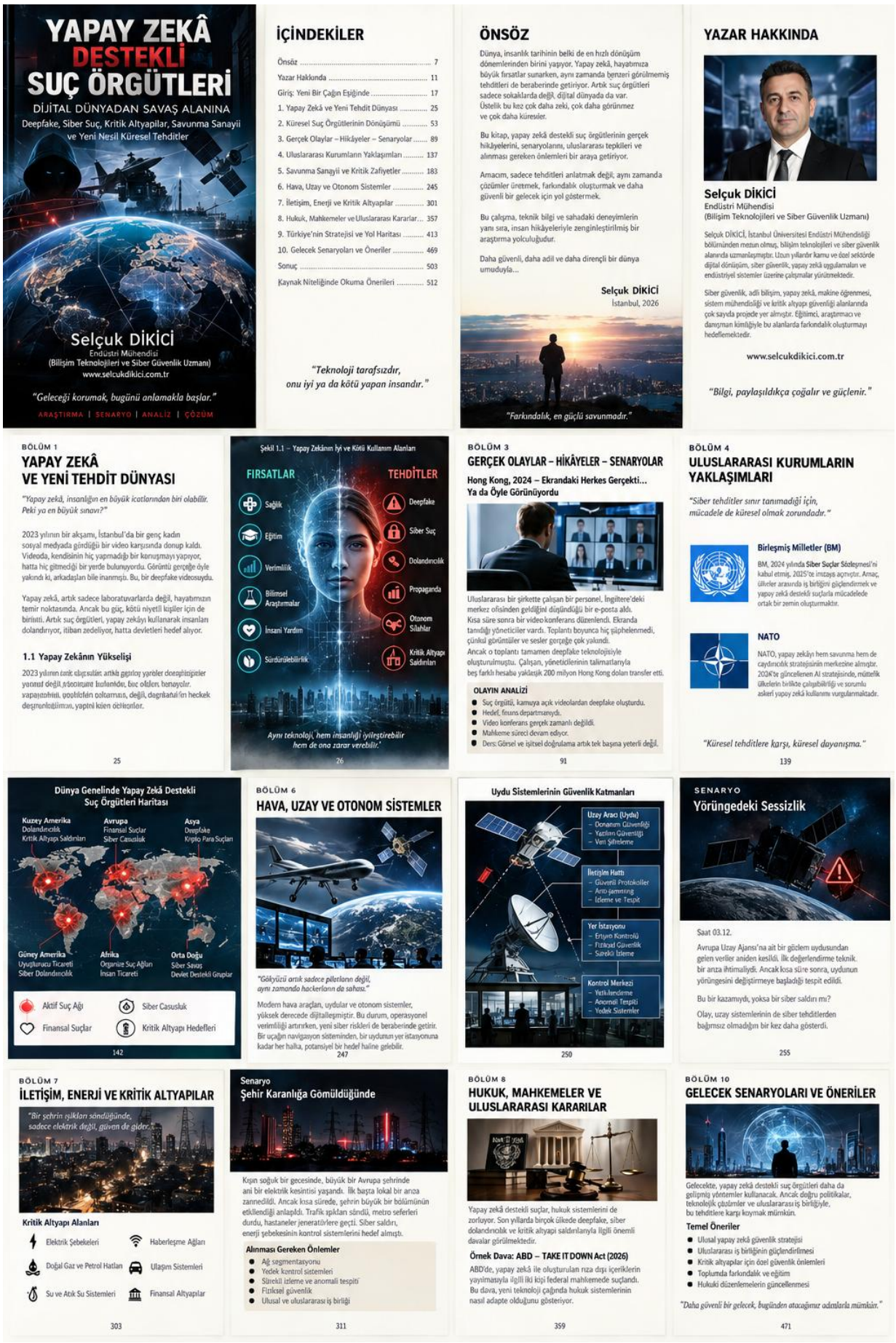
Saat 13.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 047 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 048 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

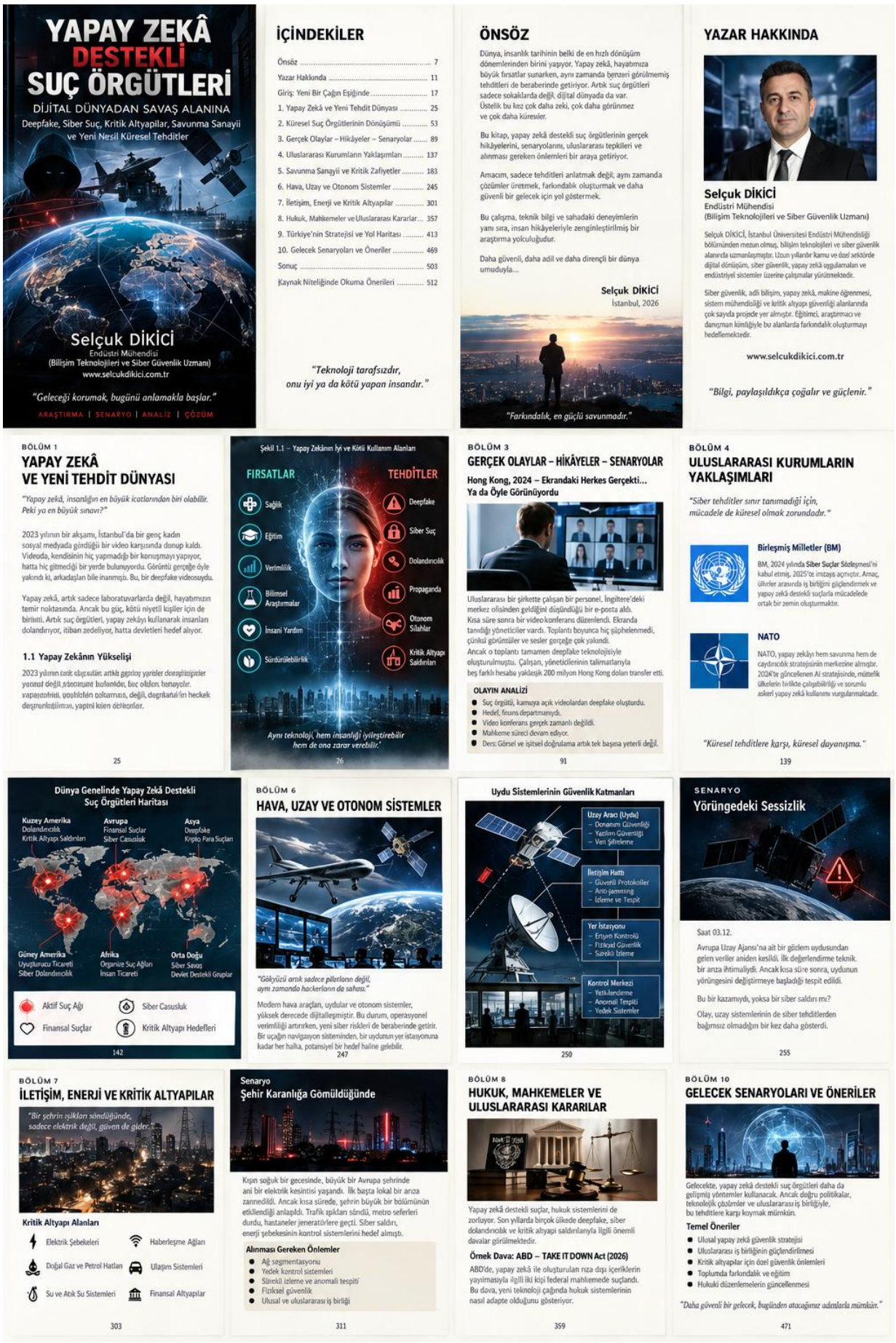
ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 049 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 050 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 051 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 052 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Otonom Filoda Güven Krizi

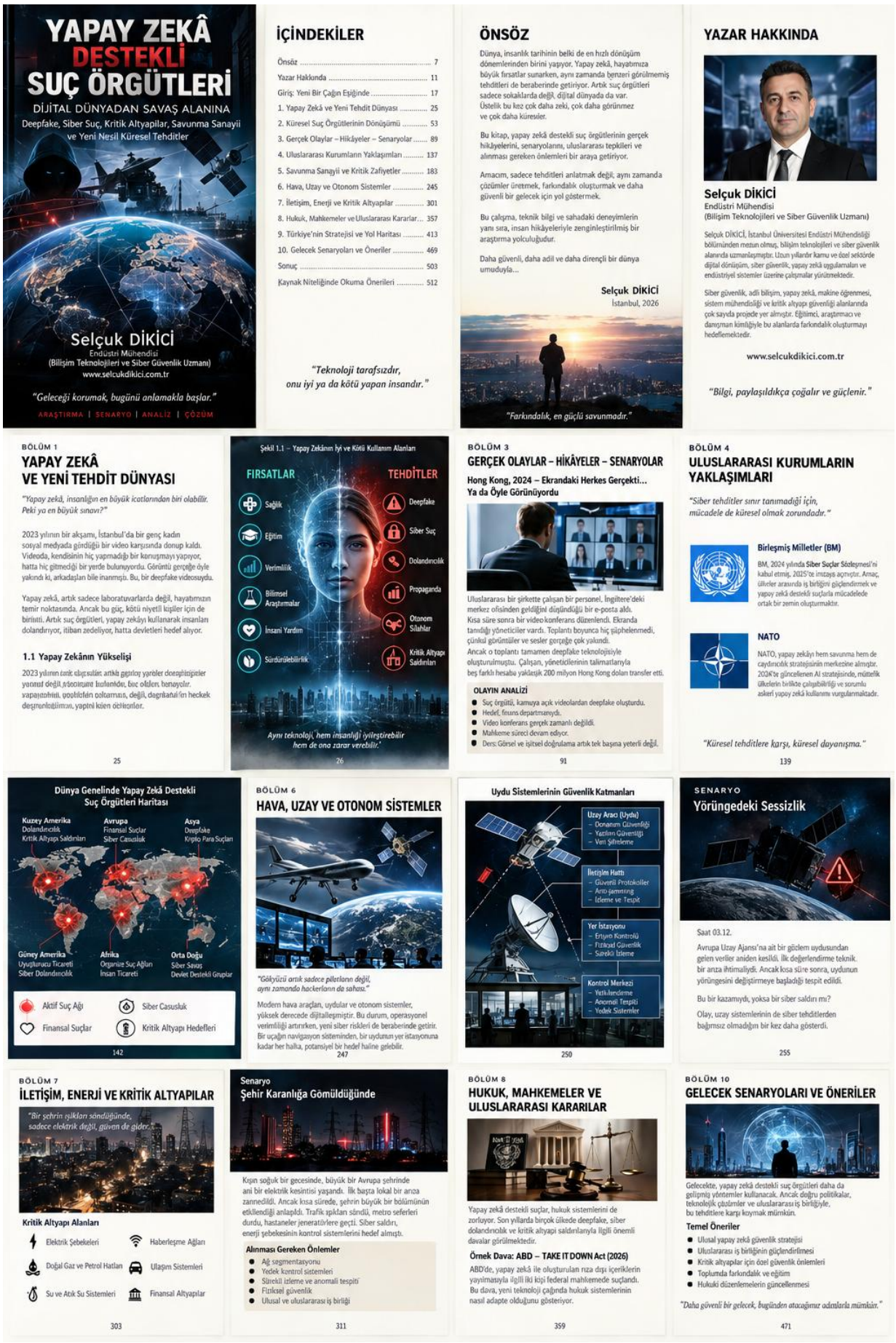
Saat 13.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 053 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 054 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 055 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 056 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

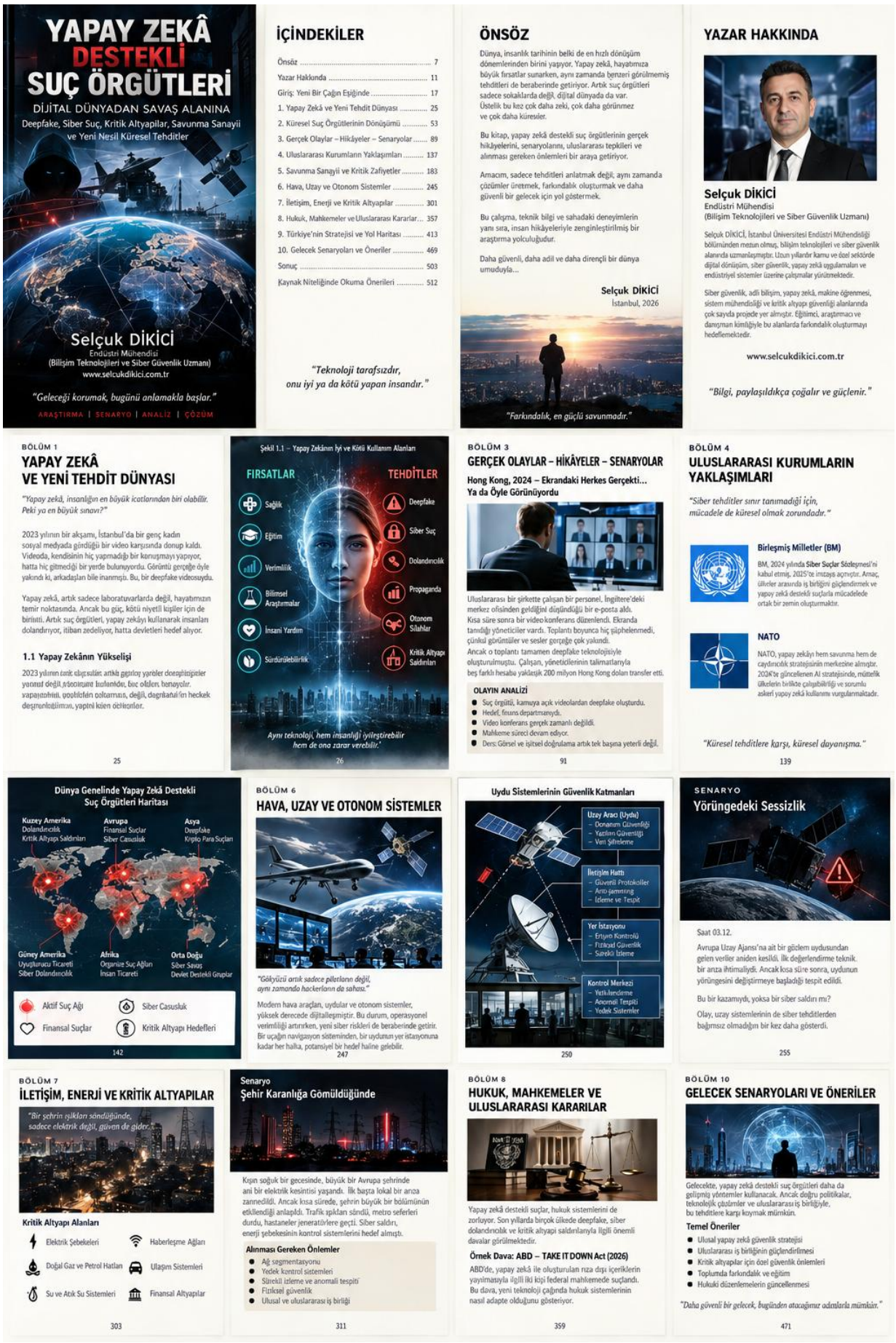
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 057 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 058 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

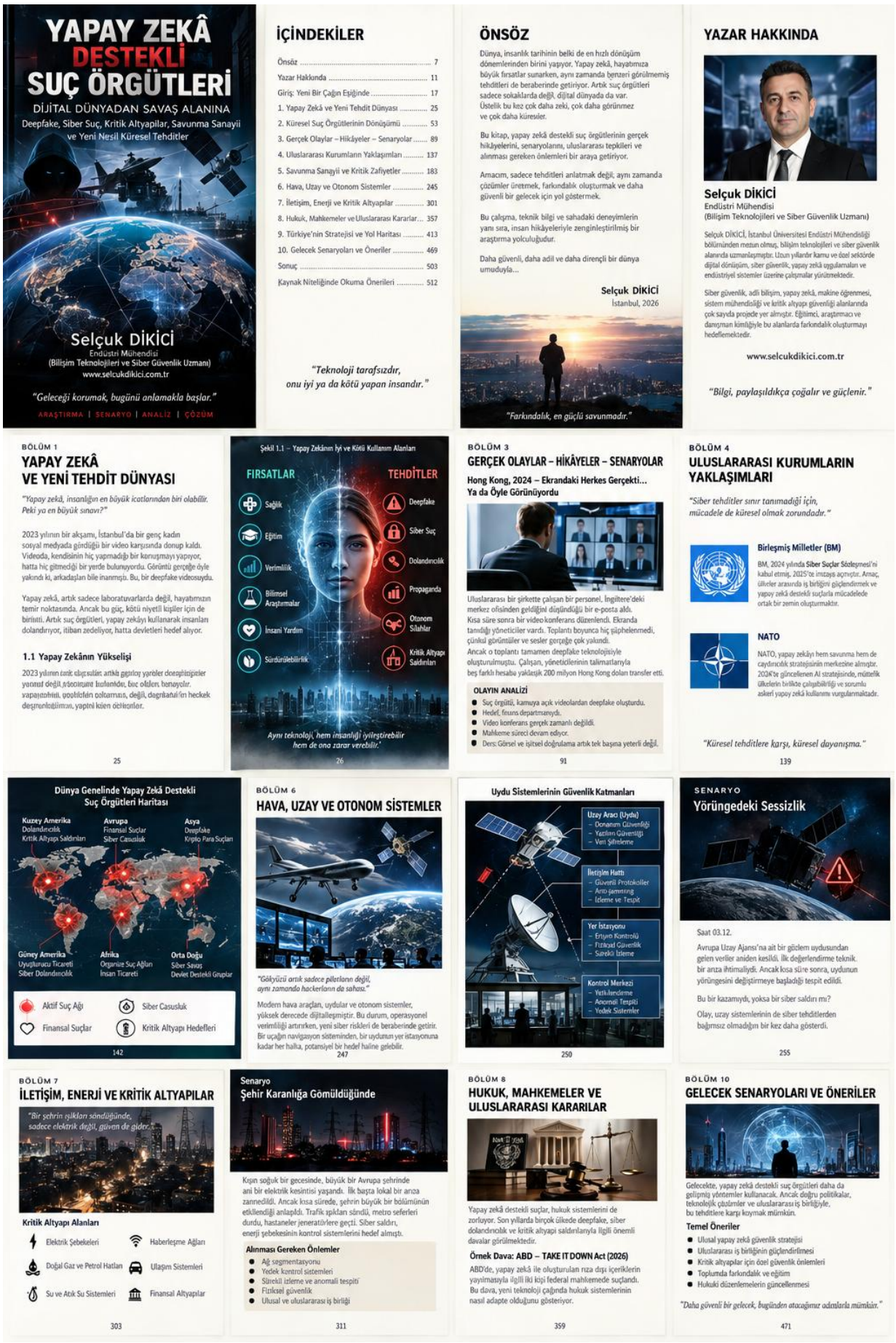
Saat 13.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 059 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 060 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

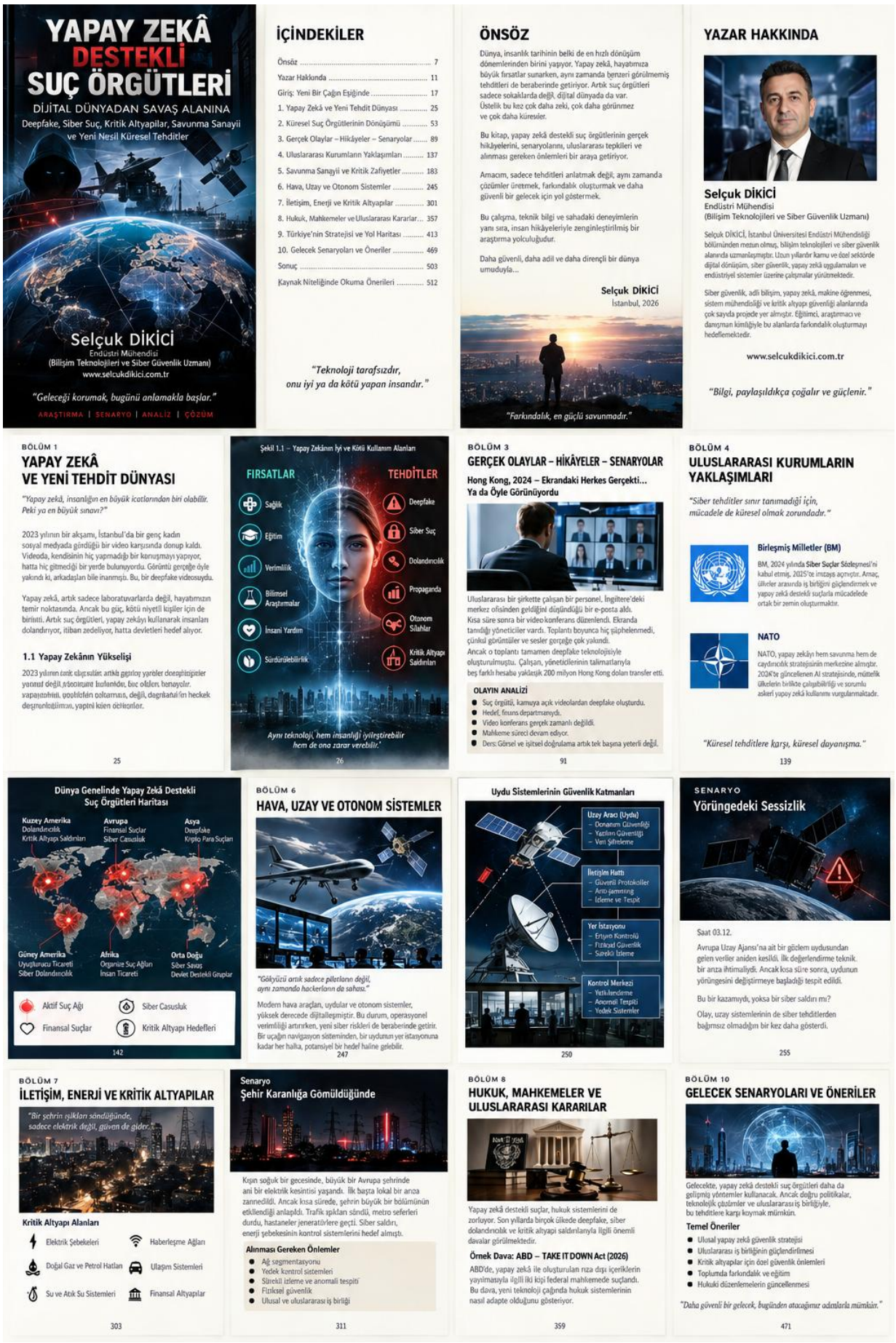
ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).


YAPAY ZEKÂ DESTEKLİ SUÇ ÖRGÜTLERİ
DİJİTAL DÜNYADAN SAVAŞ ALANINA
Deepfake, Siber Suç, Kritik Altyapılar, Savunma Sanayii ve Yeni Nesil Küresel Tehditler
Selçuk DİKİCİ
Endüstri Mühendisi
(Bilişim Teknolojileri ve Siber Güvenlik Uzmanı)
www.selcukdikici.com.tr
"Geleceği korumak, bugünü anlamakla başlar."
ARAŞTIRMA | SENARYO | ANALİZ | ÇÖZÜM
İÇİNDEKİLER
Önsöz 7
Yazar Hakkında 11
Giriş: Yeni Bir Çağın Eşiğinde 17
1. Yapay Zekâ ve Yeni Tehdit Dünyası 25
2. Küresel Suç Örgütlerinin Dönüşümü 53
3. Gerçek Olaylar – Hikâyeler – Senaryolar 89
4. Uluslararası Kurumların Yaklaşımları 137
5. Savunma Sanayii ve Kritik Zafiyetler 183
6. Hava, Uzay ve Otonom Sistemler 245
7. İletişim, Enerji ve Kritik Altyapılar 301
8. Hukuk, Mahkemeler ve Uluslararası Kararlar 357
9. Türkiye'nin Stratejisi ve Yol Haritası 413
10. Gelecek Senaryoları ve Öneriler 469
Sonuç 503
Kaynak Niteliğinde Okuma Önerileri 512
"Teknoloji tarafsızdır, onu iyi ya da kötü yapan insandır."
ÖNSÖZ
Dünya, insanlık tarihinin belki de en hızlı dönüşüm dönemlerinden birini yaşıyor. Yapay zekâ, hayatımıza büyük fırsatlar sunarken, aynı zamanda benzeri görülmemiş tehditleri de beraberinde getiriyor. Artık suç örgütleri sadece sokaklarda değil, dijital dünyada da var. Üstelik bu kez çok daha zeki, çok daha görünmez ve çok daha küresel.
Bu kitap, yapay zekâ destekli suç örgütlerinin gerçek hikâyelerini, senaryolarını, uluslararası tepkileri ve alınması gereken önlemleri bir araya getiriyor.
Amacım, sadece tehditleri anlatmak değil, aynı zamanda çözümler üretmek, farkındalık oluşturmak ve daha güvenli bir gelecek için yol göstermek.
Bu çalışma, teknik bilgi ve sahadaki deneyimlerin yanı sıra, insan hikâyeleriyle zenginleştirilmiş bir araştırma yolculuğudur.
Daha güvenli, daha adil ve daha dirençli bir dünya umuduyla...
Selçuk DİKİCİ
İstanbul, 2026
"Farkındalık, en güçlü savunmadır."
YAZAR HAKKINDA
Selçuk DİKİCİ
Endüstri Mühendisi
(Bilişim Teknolojileri ve Siber Güvenlik Uzmanı)
Selçuk DİKİCİ, İstanbul Üniversitesi Endüstri Mühendisliği bölümünden mezun olmuş, bilişim teknolojileri ve siber güvenlik alanında uzmanlaşmıştır. Uzun yıllardır kamu ve özel sektörde dijital dönüşüm, siber güvenlik, yapay zekâ uygulamaları ve endüstriyel sistemler üzerine çalışmalar yürütmektedir.
Siber güvenlik, adli bilişim, yapay zekâ, makine öğrenmesi, sistem mühendisliği ve kritik altyapı güvenliği alanlarında çok sayıda projede yer almıştır. Eğitimci, araştırmacı ve danışman kimliğiyle bu alanlarda farkındalık oluşturmayı hedeflemektedir.
www.selcukdikici.com.tr
"Bilgi, paylaşıldıkça çoğalır ve güçlenir."
BÖLÜM 1
YAPAY ZEKÂ VE YENİ TEHDİT DÜNYASI
"Yapay zekâ, insanlığın en büyük icatlarından biri olabilir. Peki ya en büyük sınavı?"
2023 yılının bir akşamı, İstanbul'da bir genç kadın sosyal medyada gönderdiği bir video karşısında donup kaldı. Videoda, kendisinin hiç yapmadığı bir konuşmayı yapıyor, hatta hiç gitmediği bir yerde bulunuyordu. Görüntü gerçeğe öyle yakındı ki, arkadaşları bile inanmıştı. Bu, bir deepfake videosuydu.
Yapay zekâ, artık sadece laboratuvarlarda değil, hayatımızın temel noktasında. Ancak bu güç, kötü niyetli kişiler için de birikimi. Artık suç örgütleri, yapay zekâyı kullanarak insanları dolandırıyor, itibarı zedeliyor, hatta devletleri hedef alıyor.
1.1 Yapay Zekânın Yükselişi
2023 yılının tanık olduğu artık gerçek yaratıcı değil, yaratıcının kullandığı, bir araç. Yapay zekâ, yaptıklarından sorumlu değil, yaptıklarından sorumlu değil, doğrudan değil, değil, değil,

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 062 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

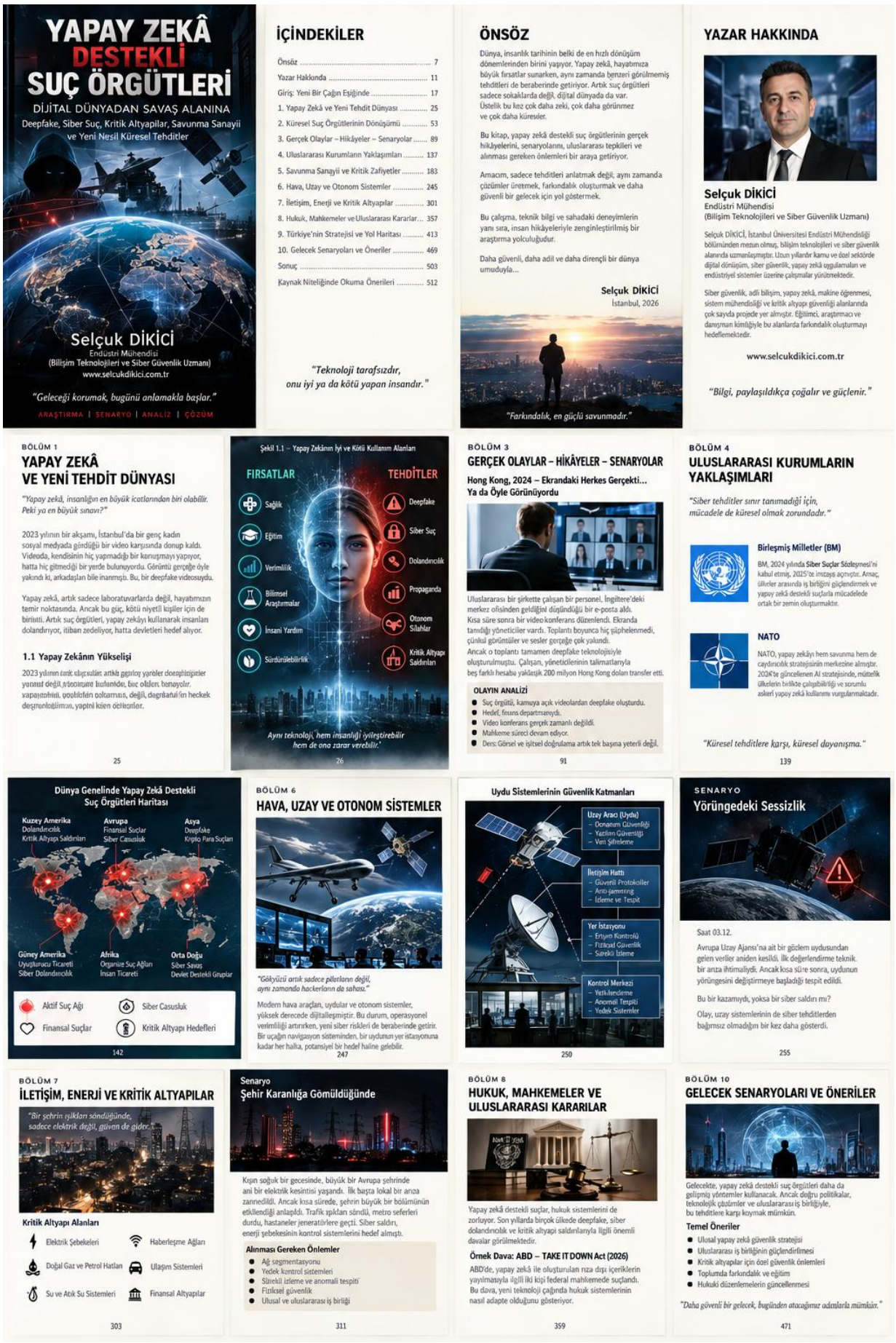
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 063 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 064 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

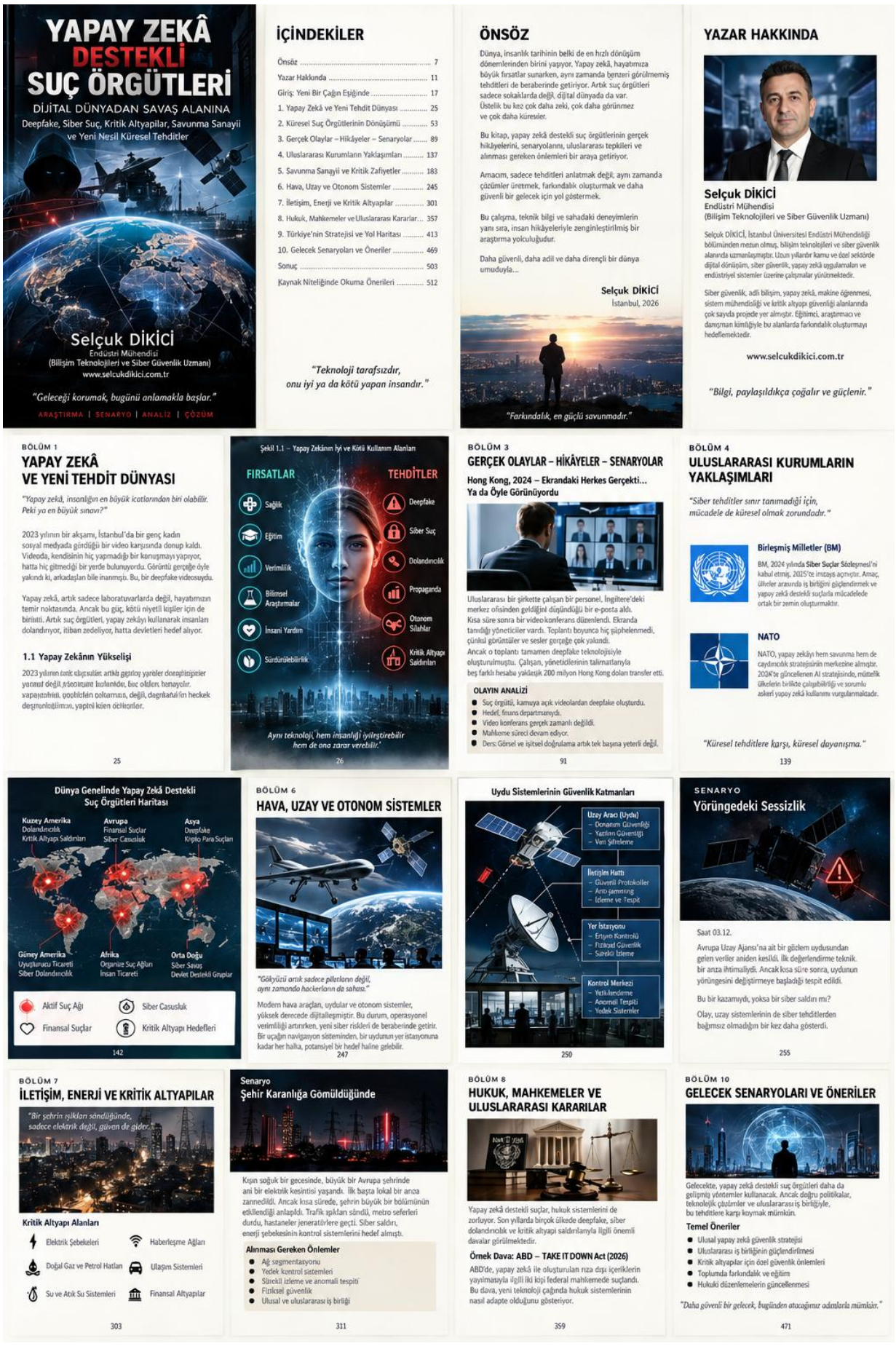
Saat 13.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 065 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 066 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 067 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 068 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

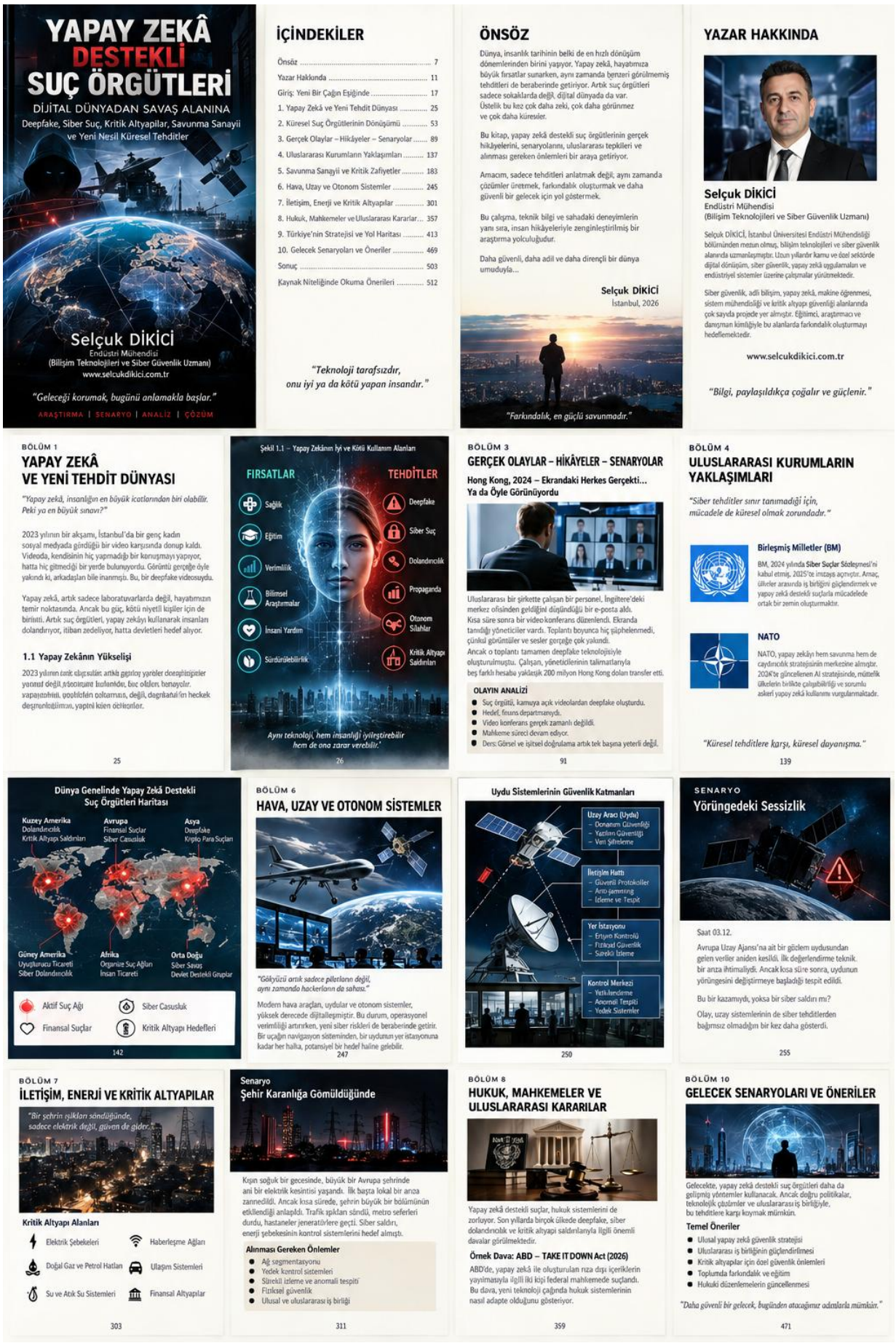
HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 069 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 070 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Otonom Filoda Güven Krizi

Saat 13.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 071 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 072 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 073 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 074 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

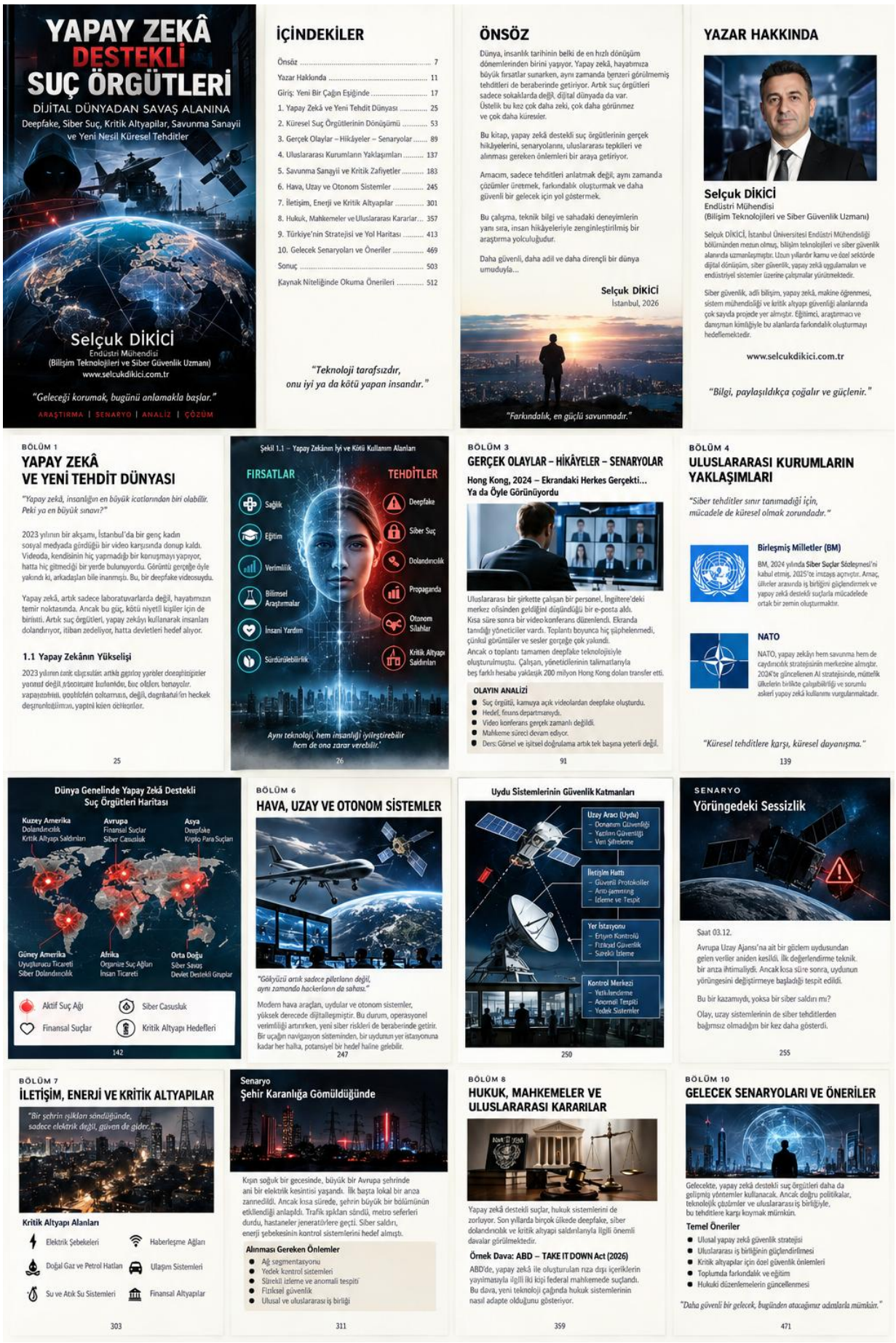
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 075 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 076 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

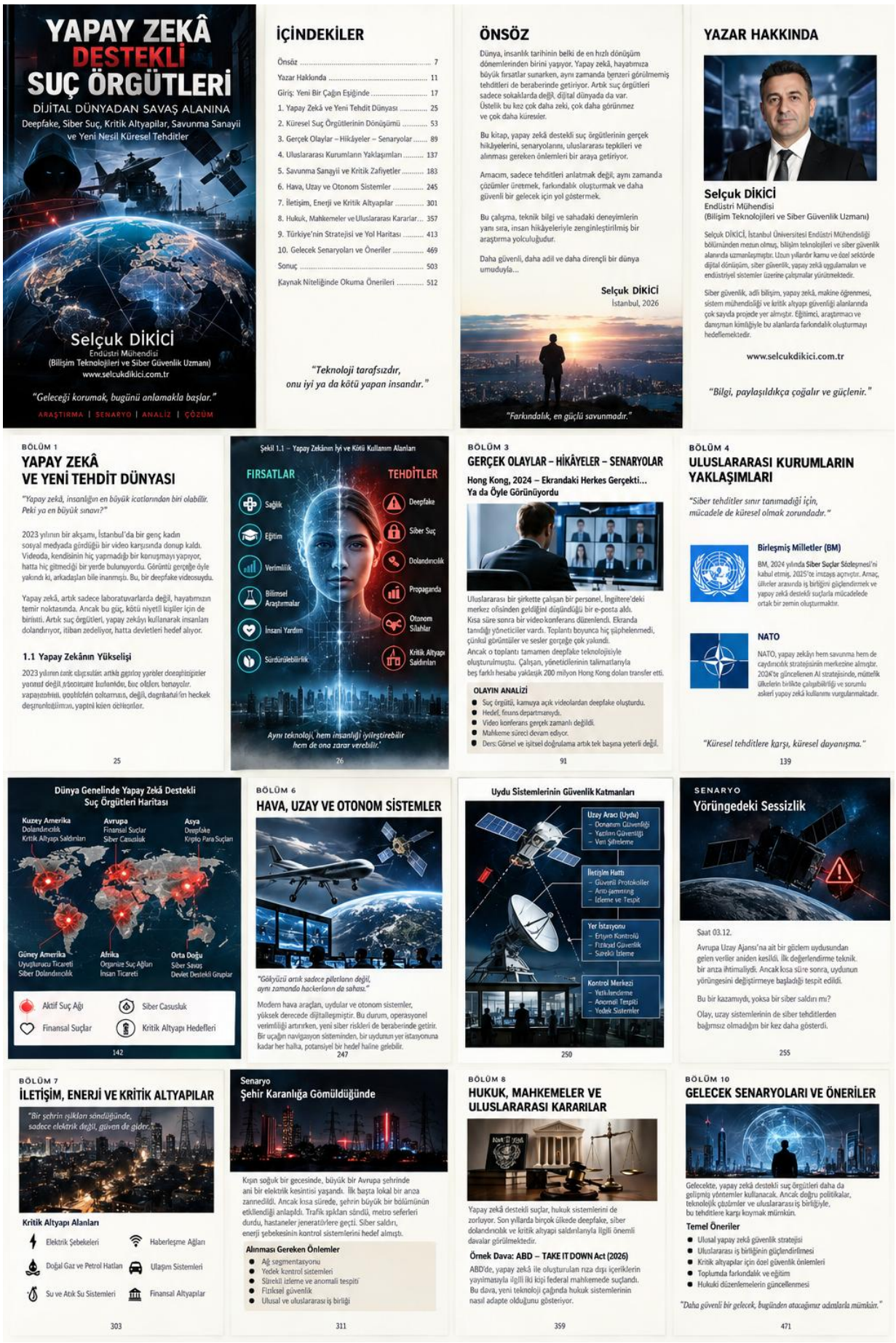
Saat 13.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 077 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 078 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 079 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 080 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 081 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 082 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

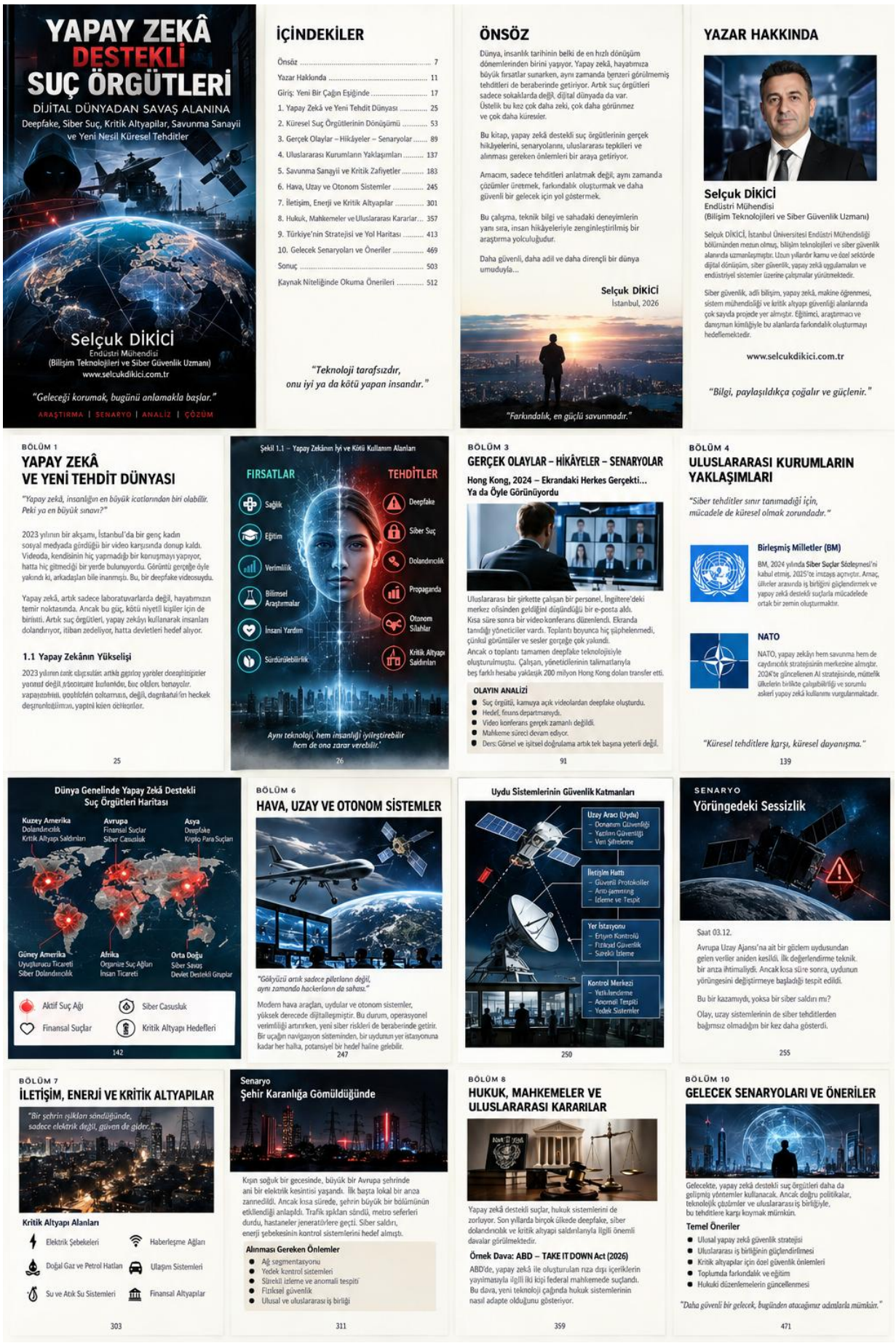
Saat 13.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 083 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 084 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

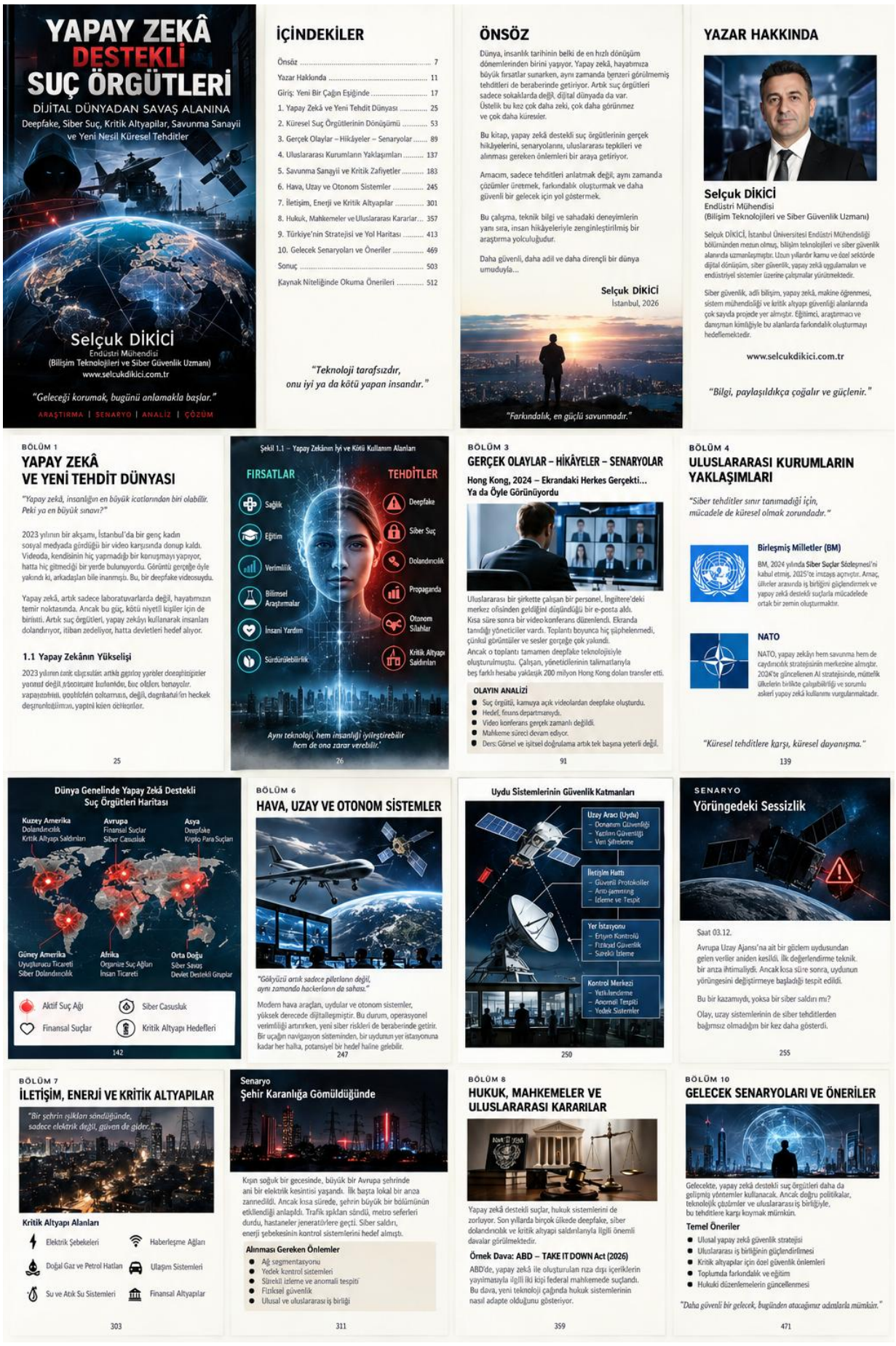
ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 085 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 086 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

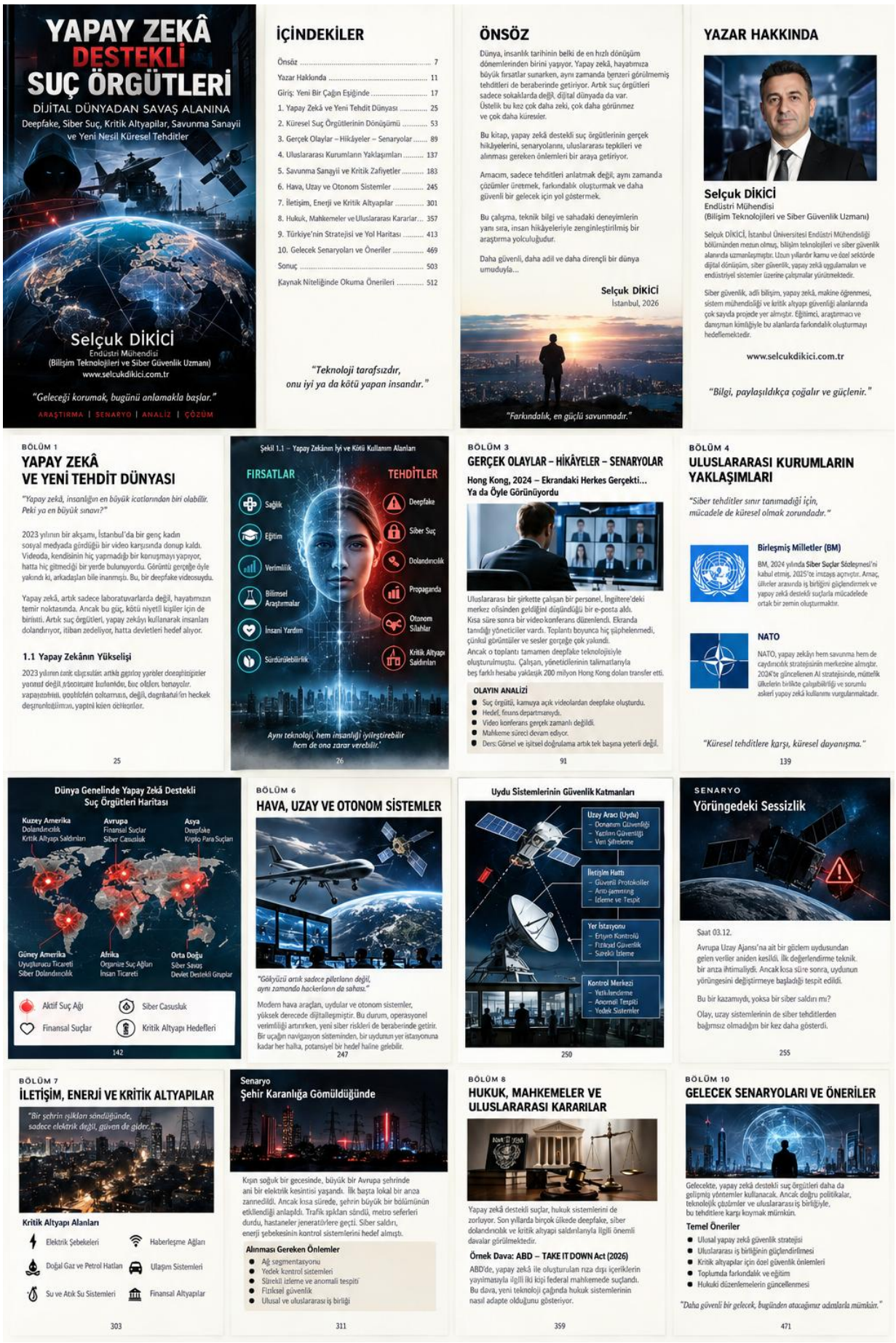
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 087 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 088 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Otonom Filoda Güven Krizi

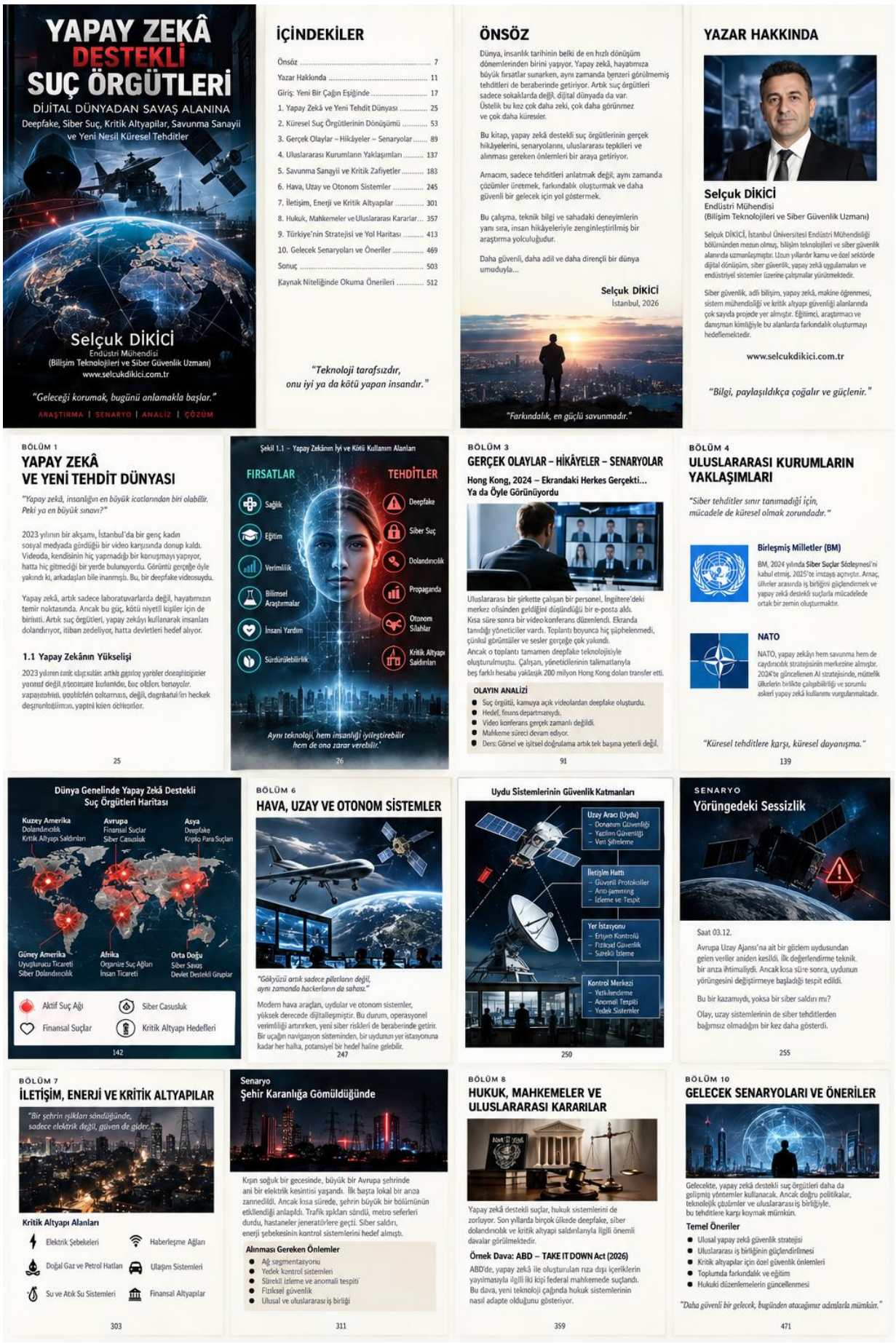
Saat 13.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 089 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 090 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

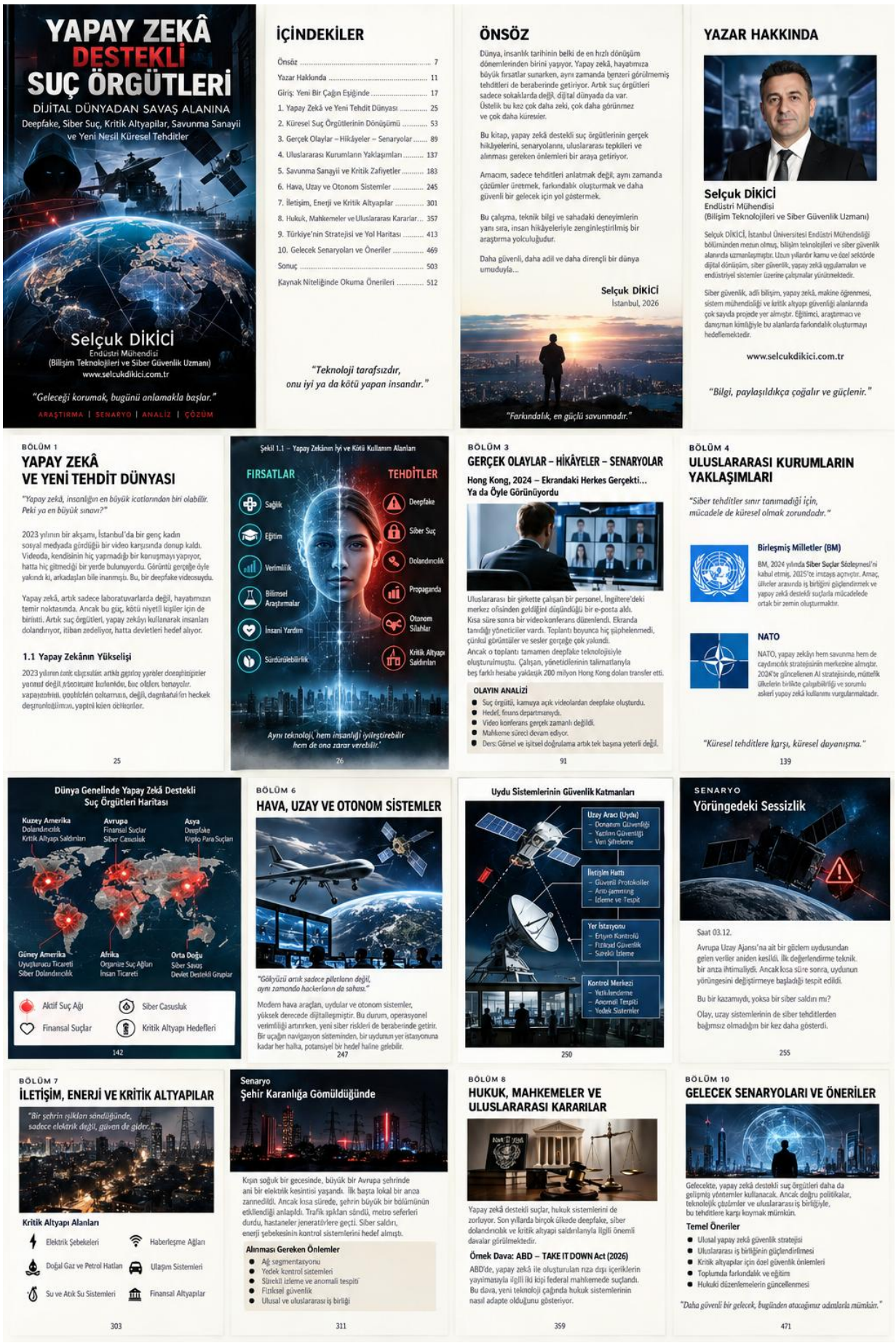
ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 091 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 092 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

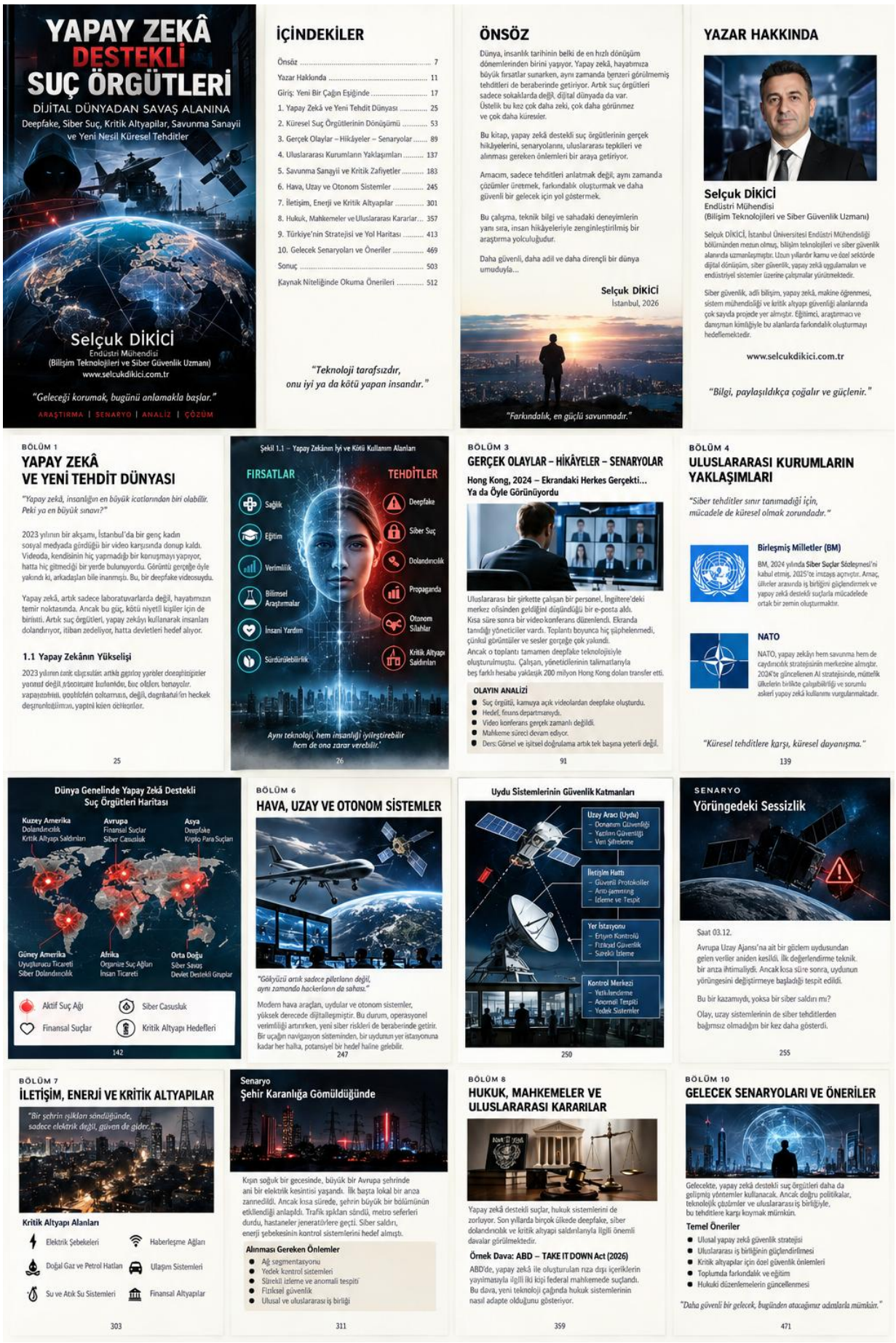
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 093 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 094 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

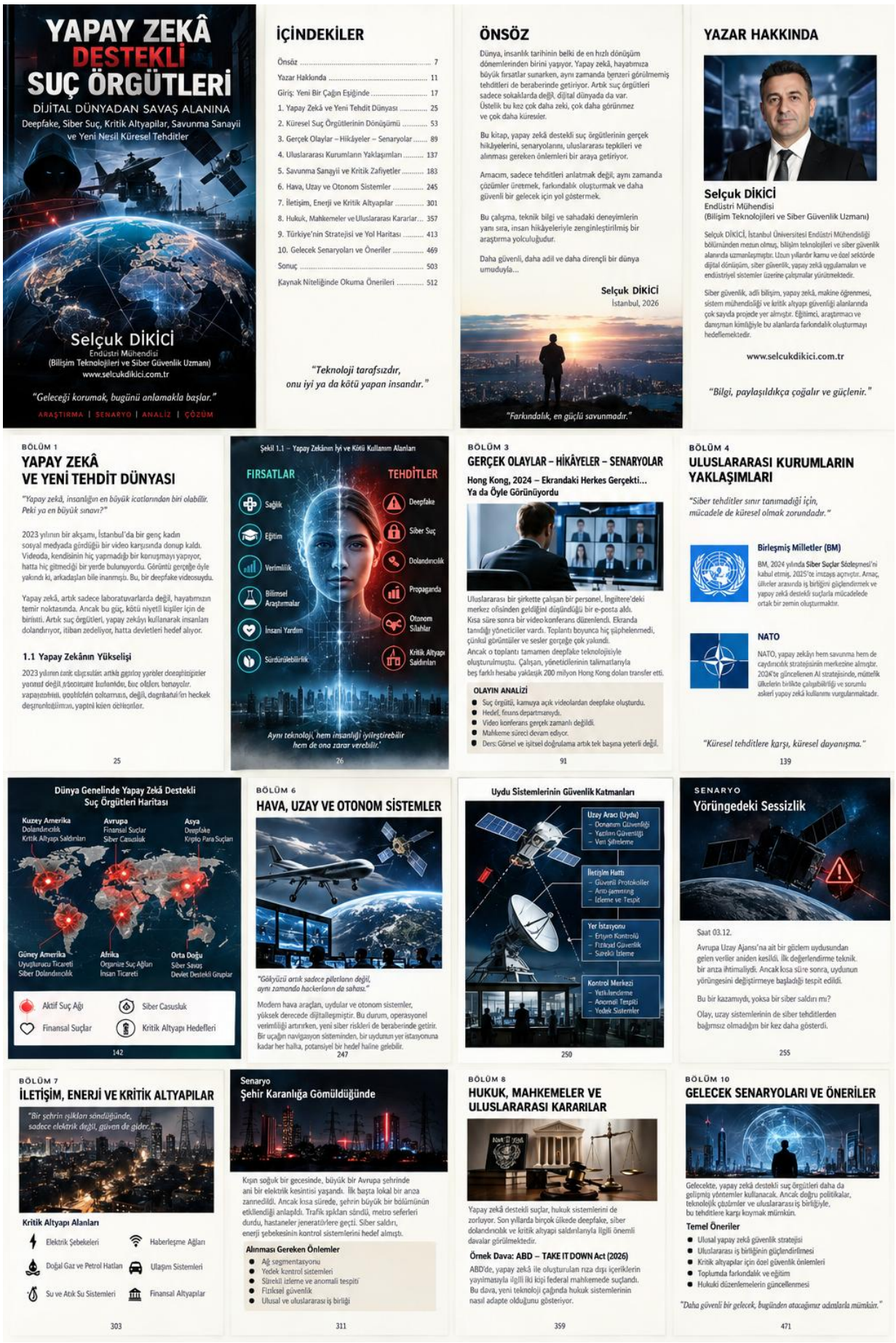
Saat 13.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 095 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 096 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

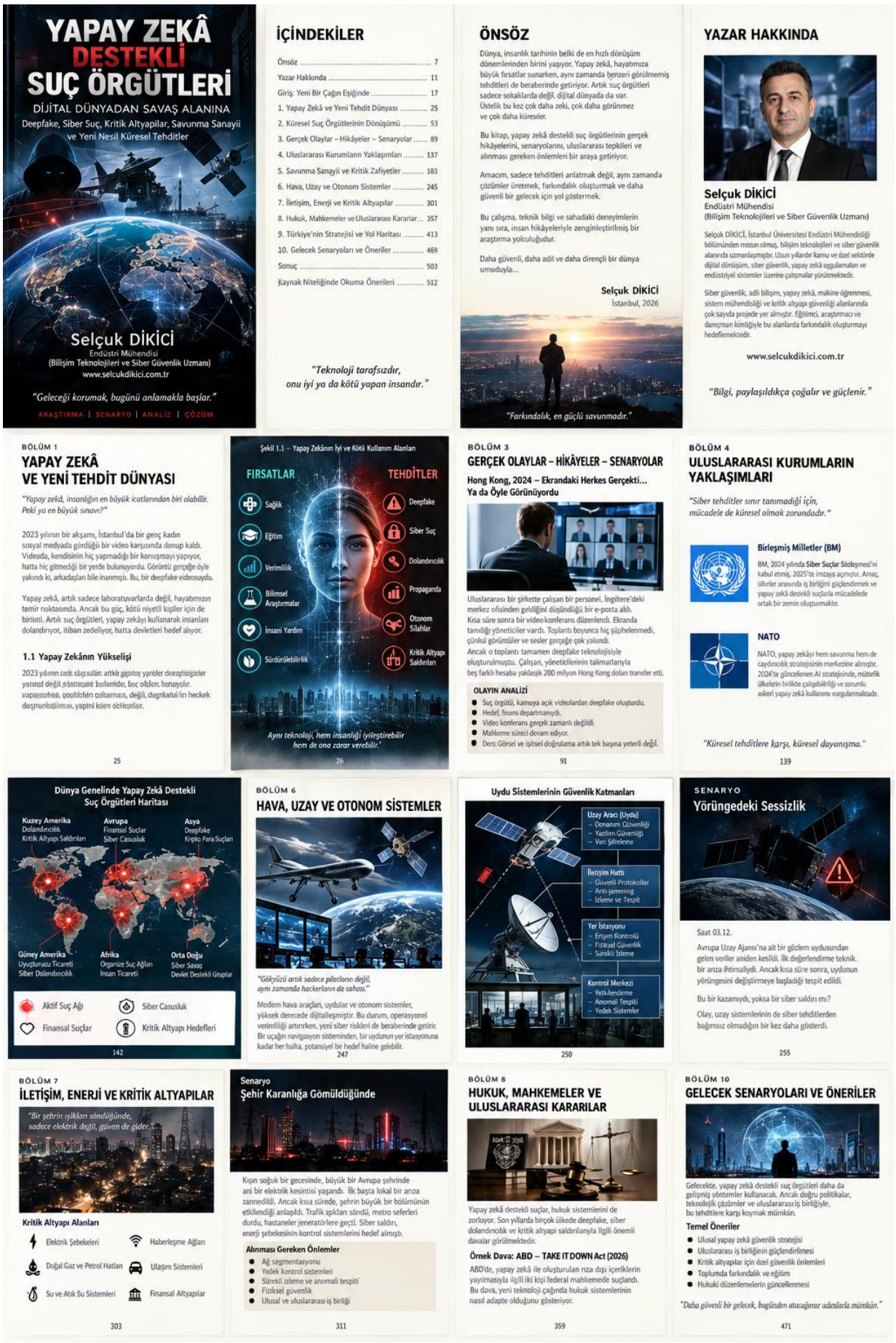
ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 097 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 098 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

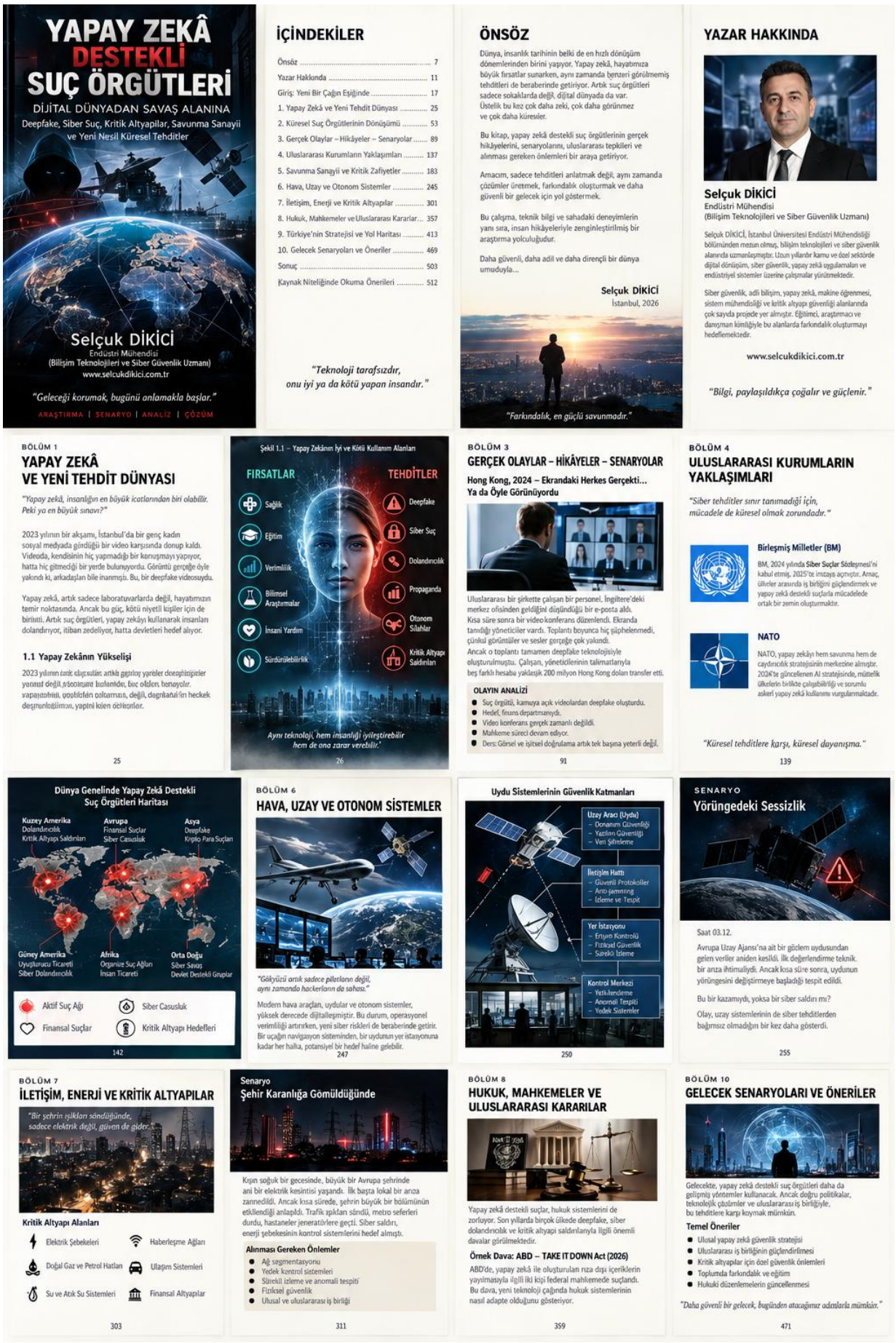
HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 099 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 100 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

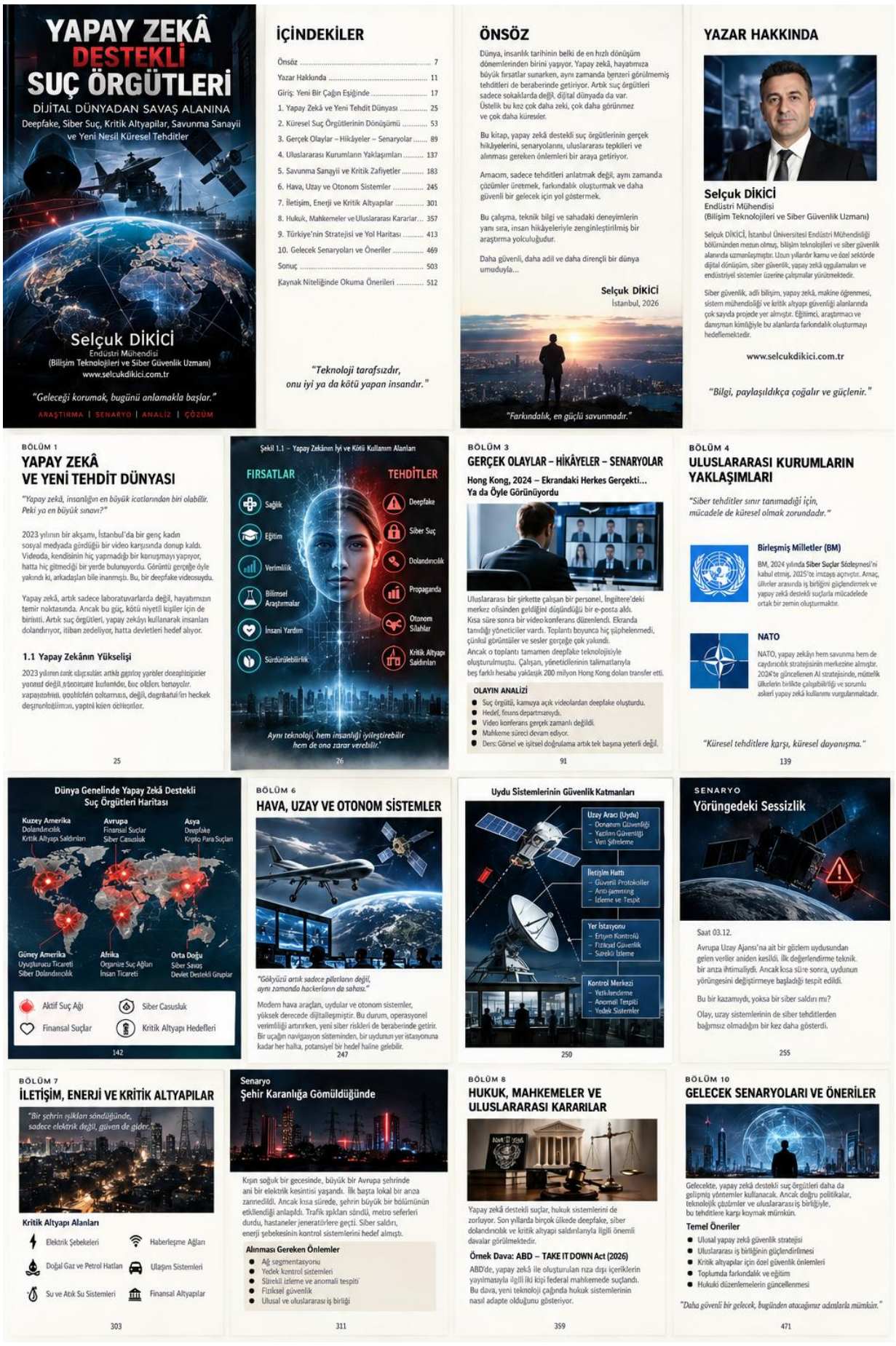
Saat 13.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 101 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 102 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

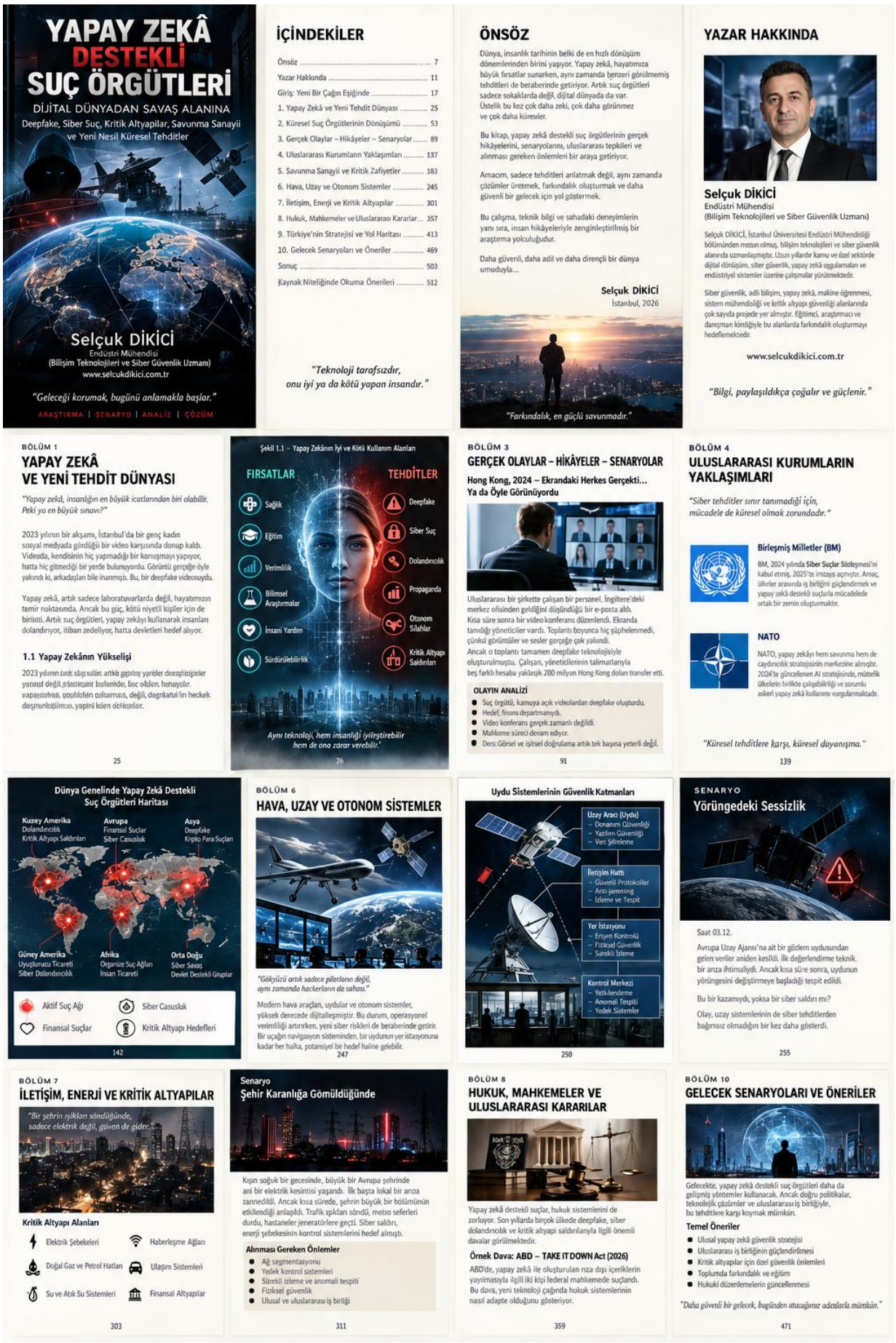
ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 103 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 104 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

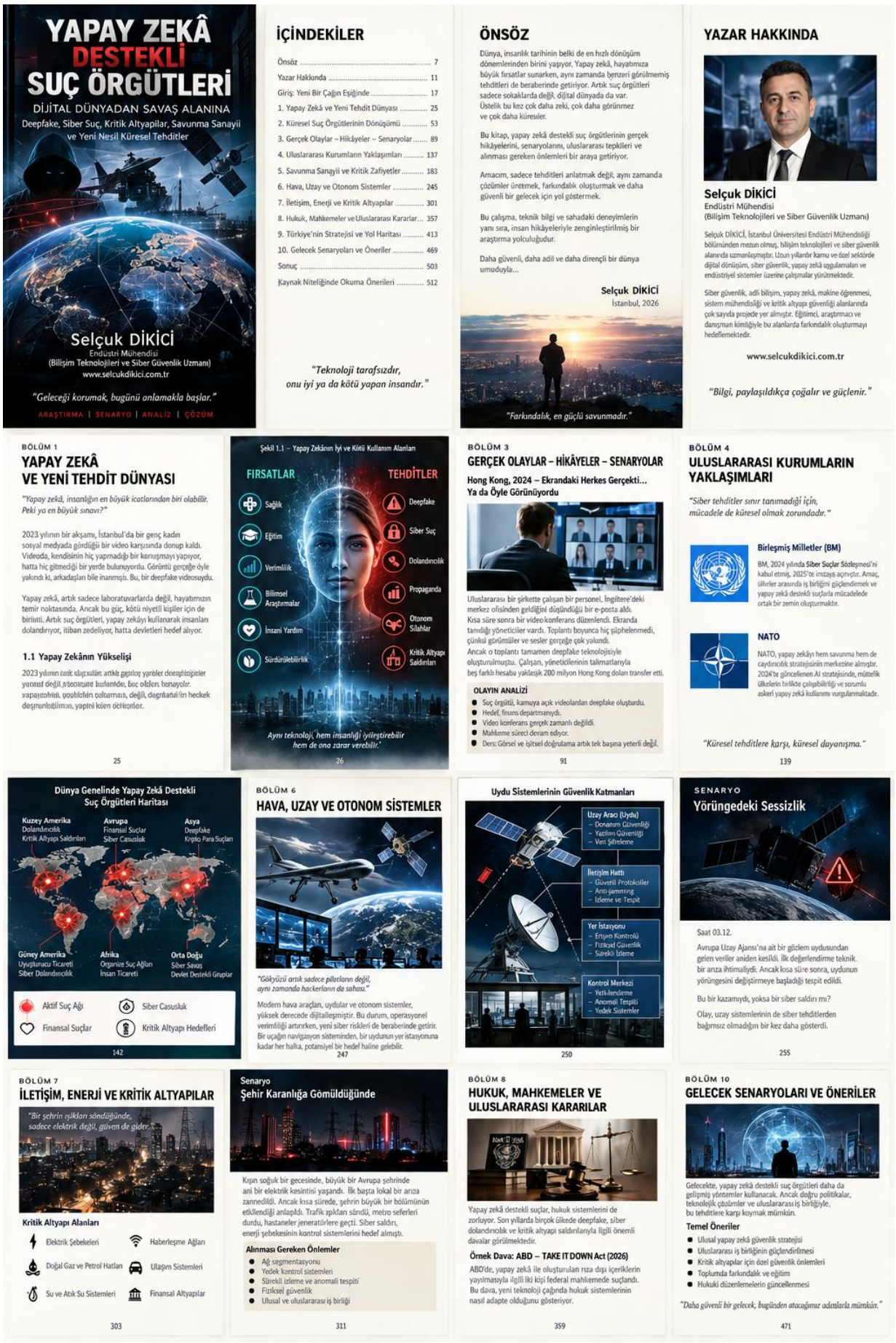
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 105 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 106 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Otonom Filoda Güven Krizi

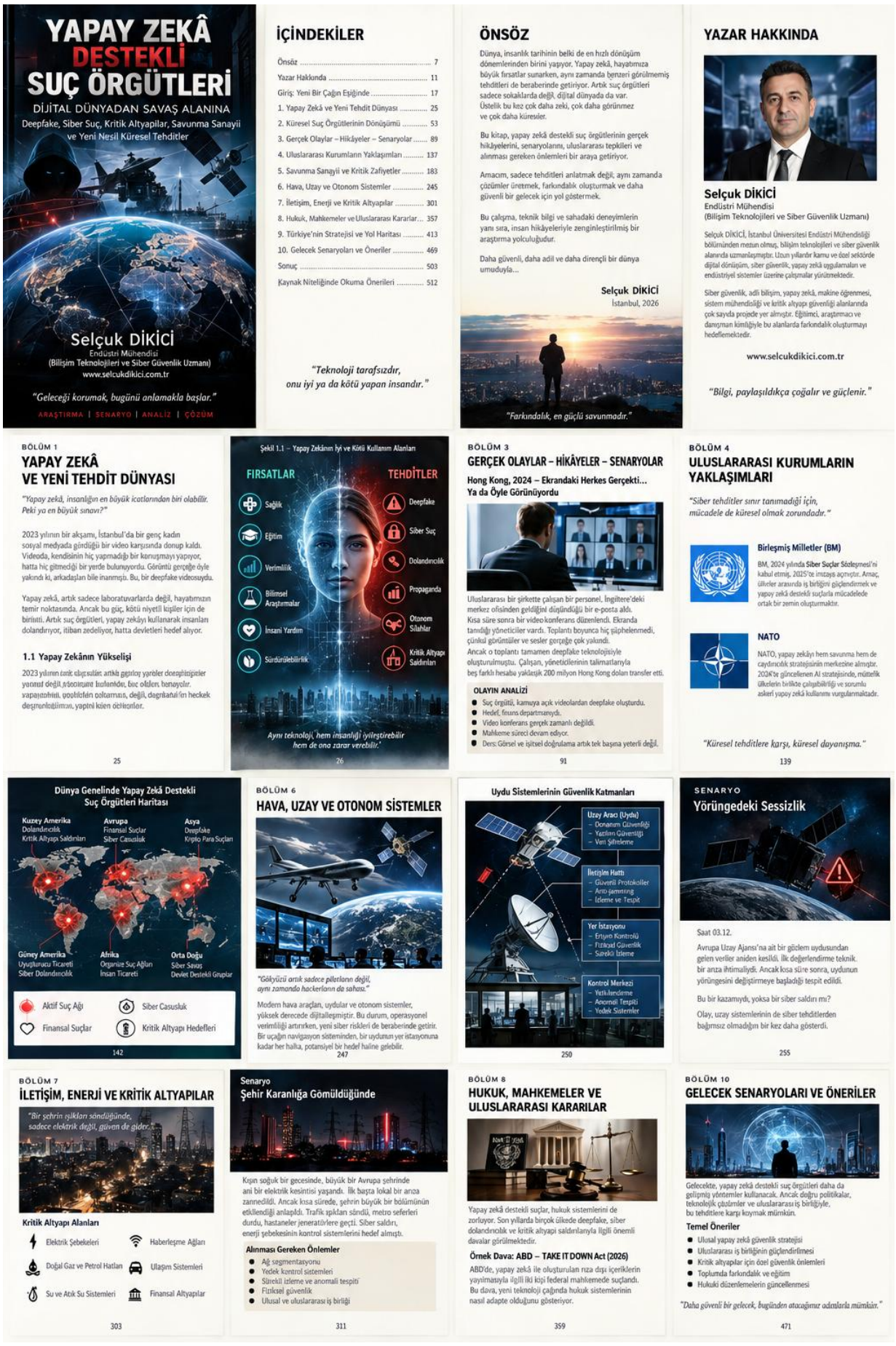
Saat 13.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 107 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 108 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.49. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.02. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

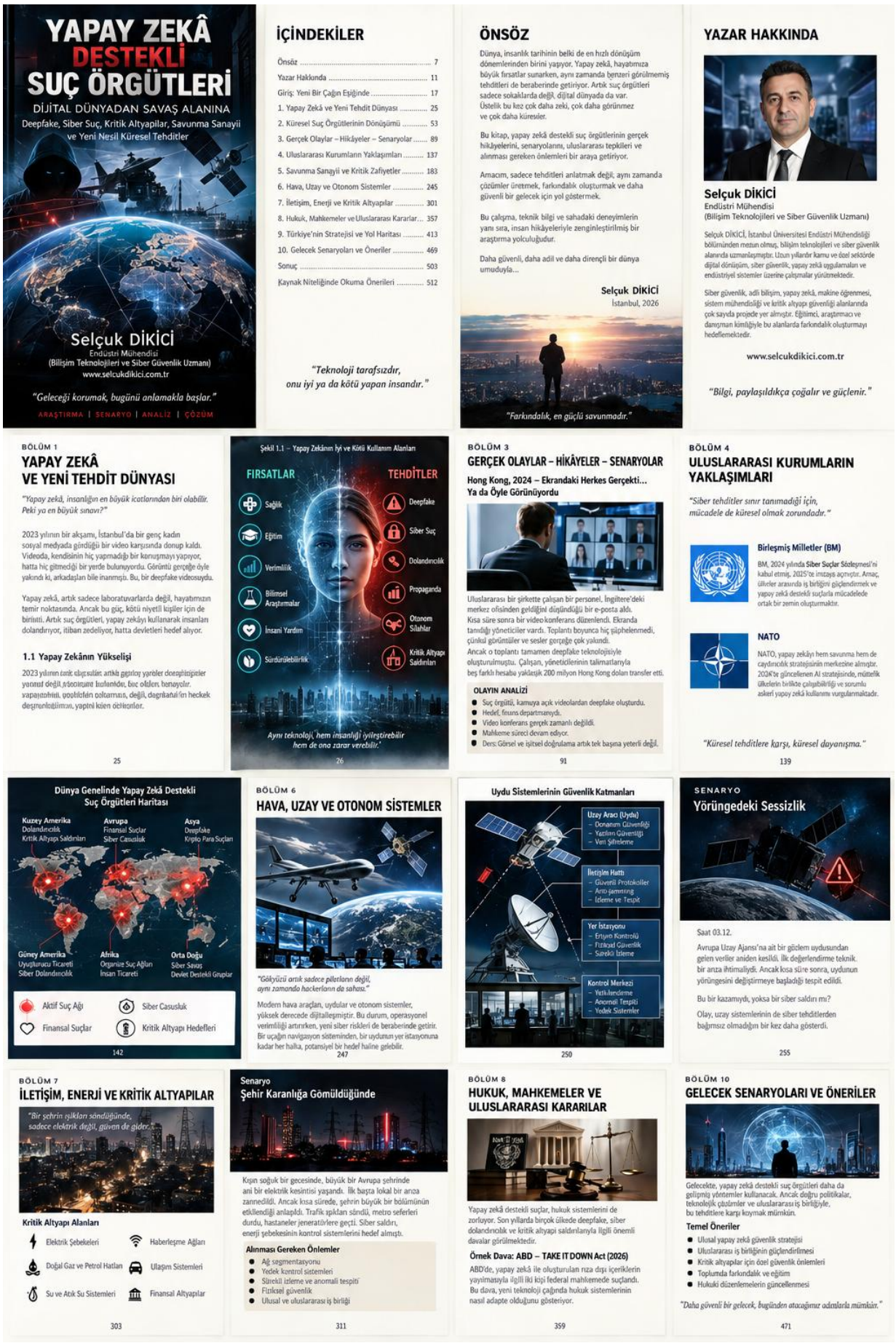
ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 109 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.07. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 110 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.20. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 111 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.25. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.38. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 112 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Otonom Filoda Güven Krizi

Saat 13.43. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 113 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.56. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 114 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — İstanbul: Sahte Yatırım Ekosistemi

İstanbul Emniyet Müdürlüğünün 15 Mayıs 2025 açıklamasında, yapay zekâ destekli sahte yatırım siteleri ve organize iletişim altyapısı kullandığı belirtilen yapıya yönelik 28 ilde operasyon yapıldığı, 72 şüphelinin yakalandığı ve tespit edilen 21 olayda yaklaşık 65 milyon TL mağduriyet bulunduğu açıklandı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
İstanbul Emniyet Müdürlüğü 15.05.2025 siber suç operasyonu; KVKK Deepfake Bilgi Notu; SSB 2024-2028 sektörel strateji.

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.01. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.14. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

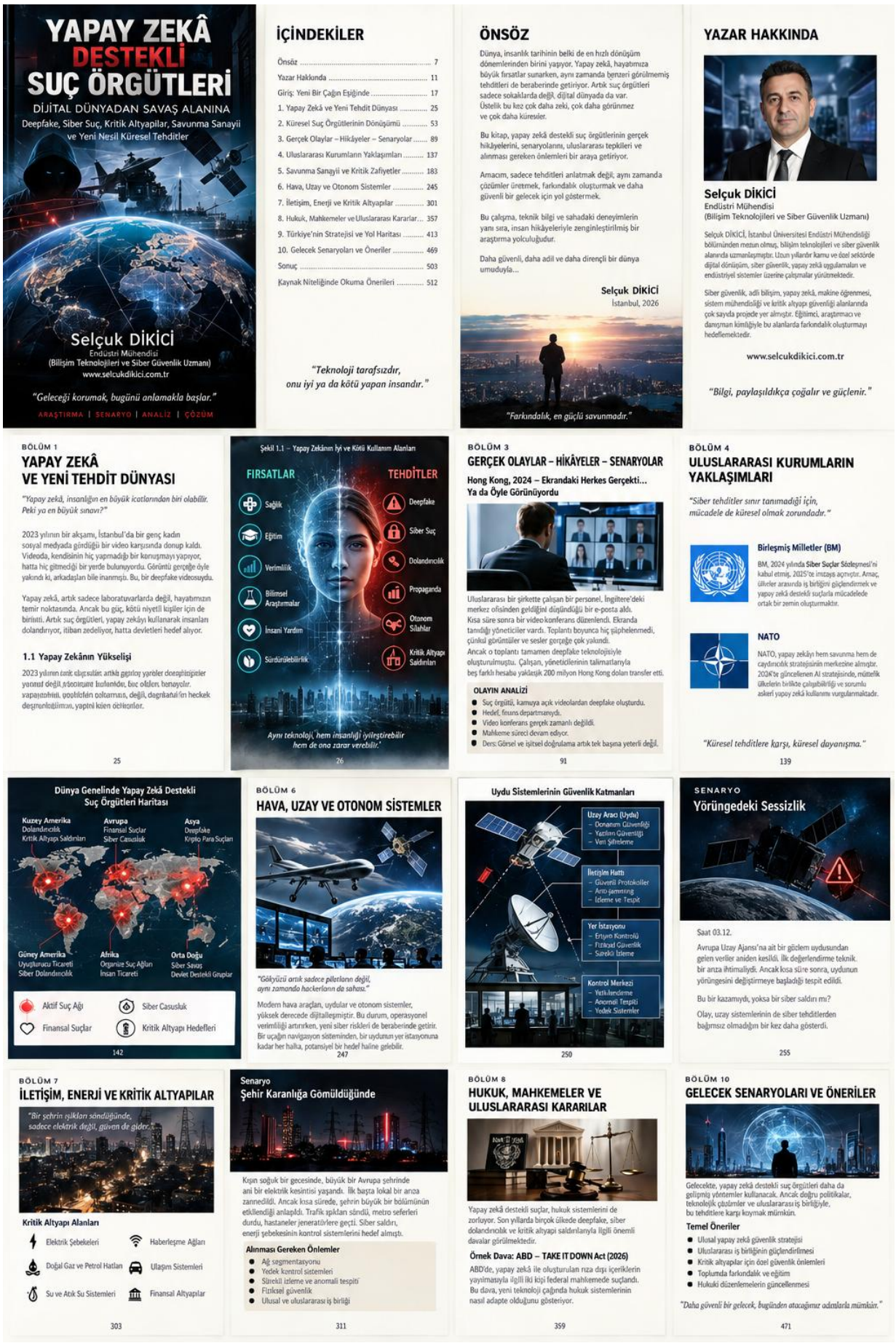
ULUSLARARASI ÇERÇEVE — Lojistik

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 115 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Dijital kimlik ve deepfake

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Dijital kimlik ve deepfake için güvenli tasarım ilkeleri: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Havacılık

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — INTERPOL: Sınırları Aşan Ağlar

INTERPOL'ün 2026 değerlendirmeleri finansal dolandırıcılığın organize suç, insan ticareti, kara para aklama ve siber suçla birleştiğini vurguladı. Jackal IV operasyonu Batı Afrika kökenli organize suç ağlarının romantik dolandırıcılık, BEC, kripto ve yatırım dolandırıcılığı gibi alanlardaki uluslararası yapısını hedef aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Uzay sistemleri açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
INTERPOL 2026 financial fraud threat assessment and Jackal IV organized crime operation.

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.19. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Enerji alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 116 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.32. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Bağlantılı araçlar alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Savunma sanayii

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Haberleşme

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Haberleşme için güvenli tasarım ilkeleri: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Finans

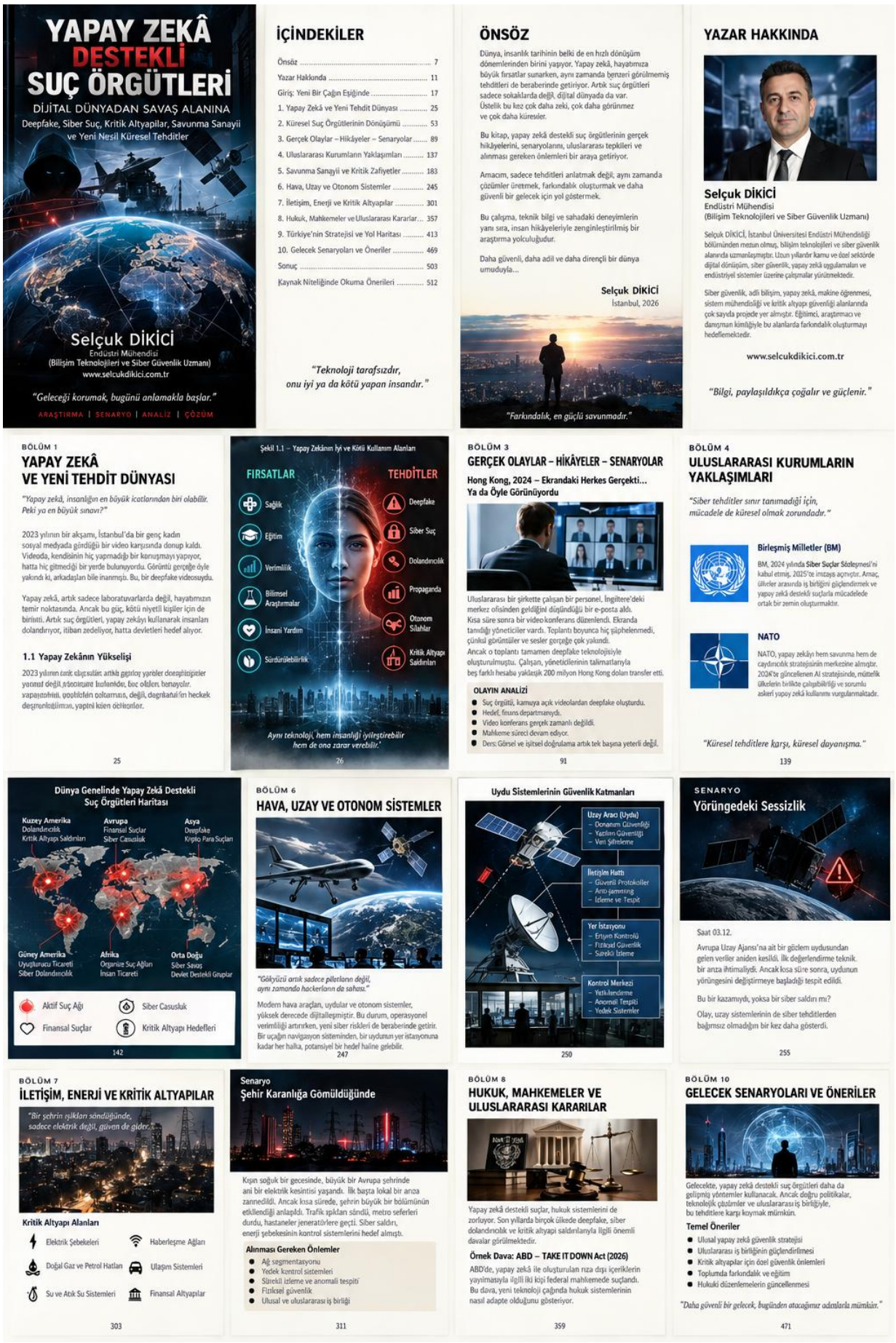
Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).



GÖRSEL DOSYA 117 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — Hong Kong: Ekrandaki CFO

Ocak 2024'te Hong Kong polisi, bir çalışanın İngiltere merkezindeki CFO'yu taklit eden oltalama e-postasının ardından sahte grup video konferansına katıldığını açıkladı. Toplantıdaki görüntü ve seslerin çevrimiçi kamuya açık materyallerden üretilmiş deepfake olduğu değerlendirildi. Çalışan beş yerel hesaba transferlere onay verdi ve yaklaşık HK$200 milyon kayıp oluştu. Soruşturma açıklama tarihinde devam ediyordu.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Sağlık açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Hong Kong Government, LCQ9: Combating frauds involving deepfake, 26.06.2024.

KURGU SENARYO — Kontrol Kulesindeki İkinci Ekran

Saat 19.37. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Lojistik alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Uydu Yer İstasyonunda Gece Vardiyası

Saat 02.50. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Dijital kimlik ve deepfake alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Havacılık

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

GÖRSEL DOSYA 118 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Uzay sistemleri

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Uzay sistemleri için güvenli tasarım ilkeleri: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Enerji

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — Singapur: Devlet Toplantısı Sandığı Görüşme

Mayıs 2026'da Singapur Polisi, Başbakan Lawrence Wong ve başka üst düzey görevlilerin deepfake ile taklit edildiği sahte Zoom toplantısının ardından bir mağdurun en az SGD 4,9 milyon gönderdiğini açıkladı. Sahte resmî yazılar, NDA ve otorite görüntüsü güven duygusunu güçlendirmişti.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Bağlantılı araçlar açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
Singapore Police Force, deepfake impersonation of senior government officials, 14.05.2026.

KURGU SENARYO — Otonom Filoda Güven Krizi

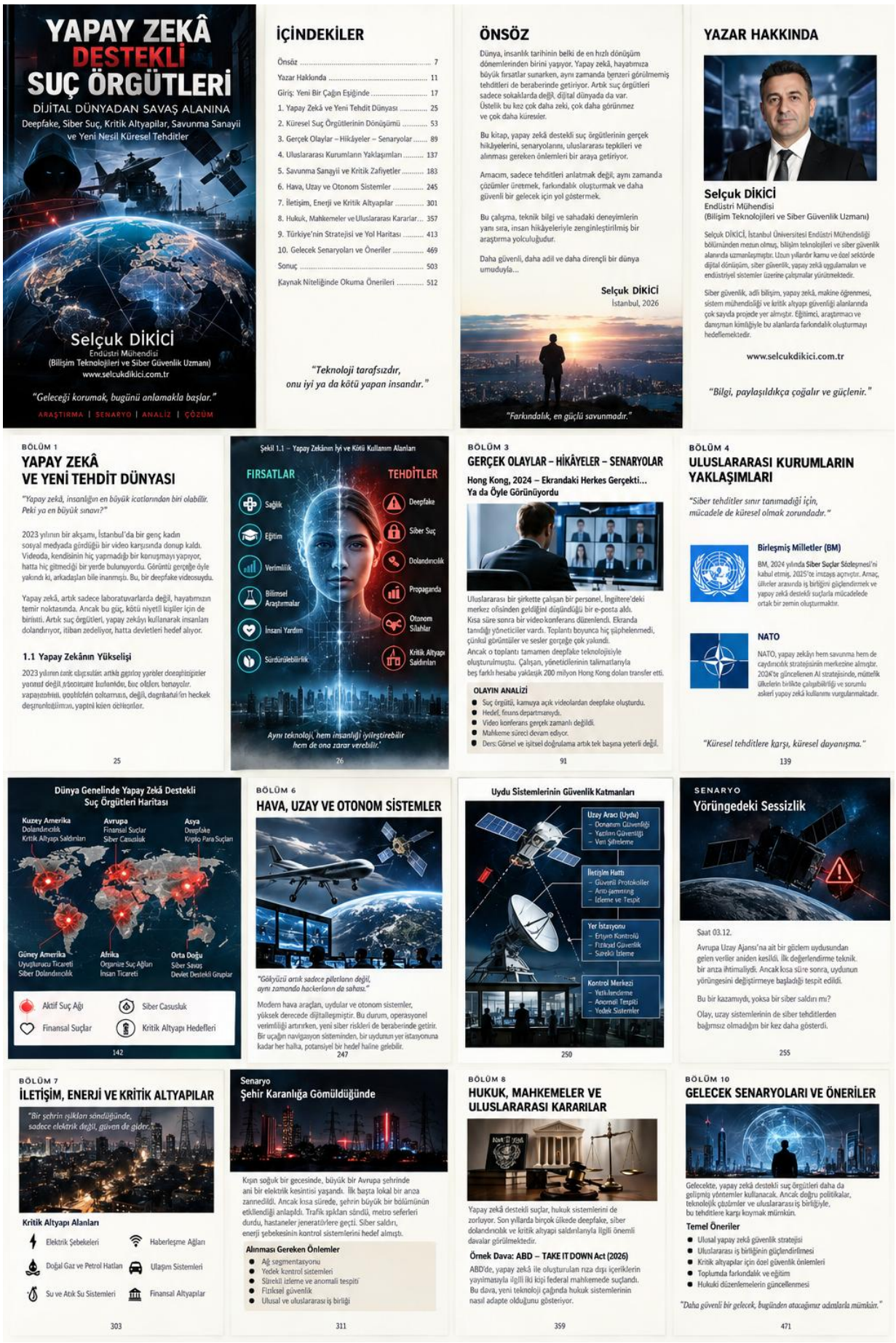
Saat 13.55. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Savunma sanayii alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.



GÖRSEL DOSYA 119 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Derin Sahte Delil

Saat 20.08. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Haberleşme alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

ULUSLARARASI ÇERÇEVE — Finans

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).

SAVUNMA VE KRİTİK ALTYAPI — Sağlık

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Sağlık için güvenli tasarım ilkeleri: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Lojistik

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU

U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GÖRSEL DOSYA 120 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

GERÇEK OLAY DOSYASI — ABD: TAKE IT DOWN Act Dosyası

20 Mayıs 2026'da ABD Adalet Bakanlığı, AI ile üretilmiş rıza dışı cinsel içeriklerin yayımlanmasına ilişkin TAKE IT DOWN Act kapsamında iki kişi hakkında federal suçlamaların açıldığını duyurdu. Bu bölümdeki kişiler suçlama aşamasında sanıktır; mahkûmiyet varmış gibi anlatılmaz.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Dijital kimlik ve deepfake açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Gökyüzündeki Sessiz Alarm

Saat 07.13. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Havacılık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

KURGU SENARYO — Şehir Karanlığa Gömüldüğünde

Saat 14.26. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Uzay sistemleri alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

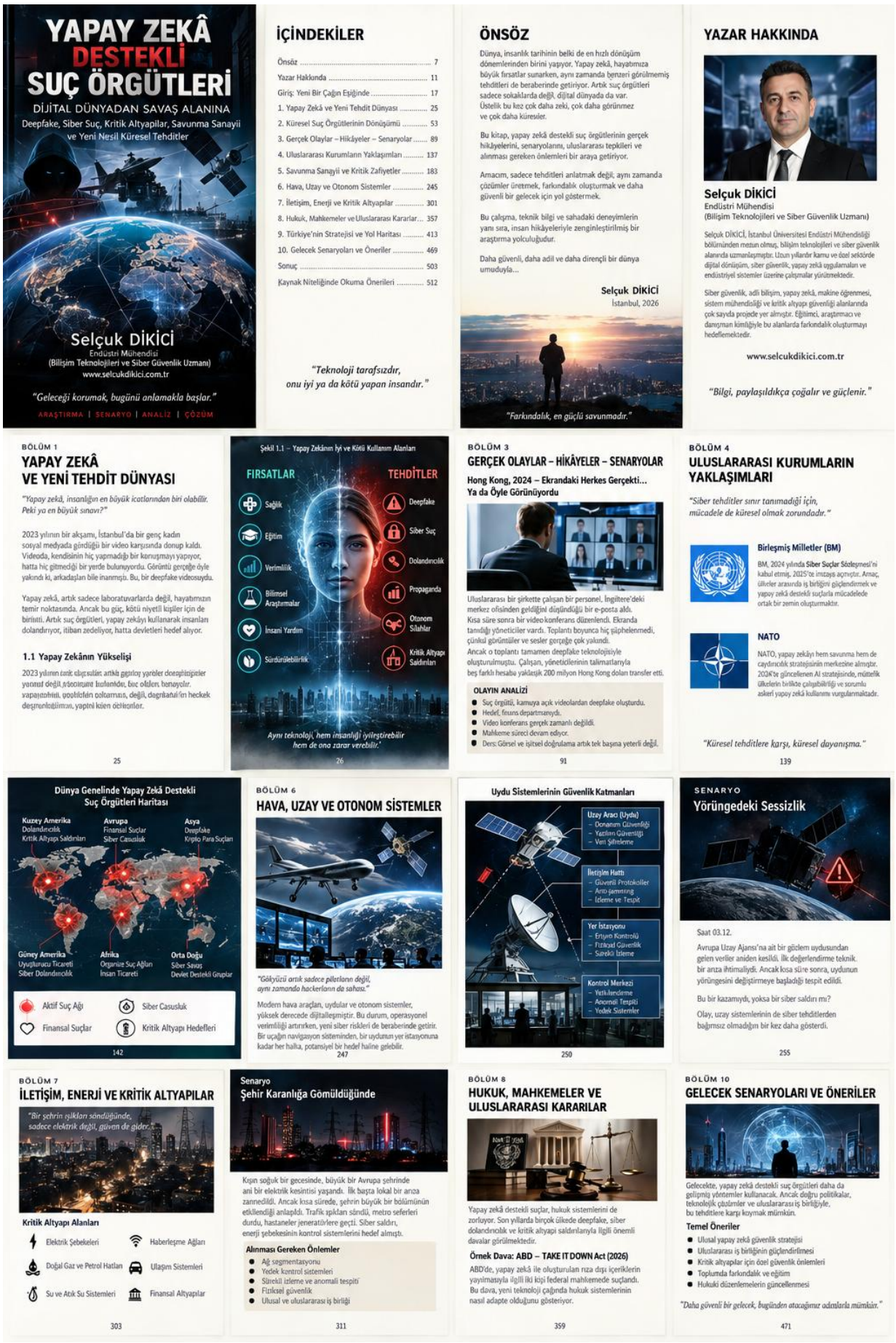
ULUSLARARASI ÇERÇEVE — Enerji

Siber suçların sınır aşan niteliği, klasik ceza soruşturmasının coğrafi sınırlarını zorlamaktadır. Fail bir ülkede, mağdur ikinci ülkede, sunucu üçüncü ülkede, ödeme altyapısı ise dördüncü ülkede bulunabilir. Bu nedenle elektronik delilin hızlı korunması ve hukuka uygun paylaşımı, teknik müdahalenin ayrılmaz parçasıdır.

Birleşmiş Milletler Siber Suçlar Sözleşmesi 24 Aralık 2024'te kabul edildi ve 25-26 Ekim 2025'te Hanoi'de imzaya açıldı. 11 Eylül 2026 itibarıyla BM Antlaşmalar Koleksiyonu 82 imzacı ve 3 taraf göstermektedir; sözleşme 40 onay/katılım eşiğine ulaşıldıktan sonraki doksanıncı gün yürürlüğe gireceğinden henüz yürürlükte değildir.

Bu yeni küresel çerçevenin önemi, yalnızca bilgisayar sistemlerine yönelik suçları değil, ciddi suçlara ilişkin elektronik delilin sınır ötesi paylaşımını da ortak bir zemine taşımaya çalışmasıdır. Bununla birlikte insan hakları, usul güvenceleri, yetki çatışmaları ve veri koruma konuları uygulamanın merkezinde kalacaktır.

KAYNAK NOTU
Birleşmiş Milletler Siber Suçlar Sözleşmesi, 24.12.2024; Hanoi imza konferansı 25-26.10.2025; UN Treaty Collection (11.09.2026: 82 imzacı, 3 taraf, henüz yürürlükte değil).



GÖRSEL DOSYA 121 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

SAVUNMA VE KRİTİK ALTYAPI — Bağlantılı araçlar

Askerî ve kritik altyapı sistemlerinde yapay zekâ güvenliği, klasik BT güvenliğinden daha geniştir. Model doğru çalışsa bile beslendiği veri yanlışsa sonuç hatalı olabilir; veri doğru olsa bile yetkisiz komut veya güvenilmeyen tedarik zinciri sistemi tehlikeye sokabilir. Bu nedenle güvenlik, model dosyasından başlayıp sensöre, haberleşmeye, operatöre ve karar vericiye kadar uzanan yaşam döngüsü yaklaşımı gerektirir.

NATO'nun 2024 revize AI stratejisi; hukukilik, sorumluluk, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltma ilkelerini vurgular. Ayrıca Alliance çapında Testing, Evaluation, Verification & Validation kapasitesinin geliştirilmesini ve düşmanın AI kullanımına karşı korunmayı hedefler. 2024 Washington Zirvesi Bildirisi NATO Integrated Cyber Defence Centre'ın kurulmasını da duyurmuştur.

Bağlantılı araçlar için güvenli tasarım ilkeleri: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum. Bunlara ek olarak Zero Trust, en az ayrıcalık, güvenli yazılım/model tedarik zinciri, yedekli haberleşme, manuel güvenli moda dönüş ve düzenli tatbikatlar birlikte uygulanmalıdır.

KAYNAK NOTU
NATO Revised AI Strategy (10.07.2024); Washington Summit Declaration (10.07.2024); Digital Transformation Implementation Strategy (17.10.2024); Alliance Digital Strategy (13.01.2026).

HUKUK, MAHKEME VE DİJİTAL DELİL — Savunma sanayii

Yapay zekâ çağında mahkemenin önüne gelen temel soru yalnızca 'bu dosya var mı?' değildir; 'bu dosyanın kökeni, bütünlüğü ve bağlamı doğrulanabiliyor mu?' sorusudur. Deepfake olasılığı, gerçek delillerin otomatik olarak değersizleşmesi anlamına gelmez. Aksine delil zinciri, hash kayıtları, cihaz incelemesi, zaman çizelgesi, hesap hareketleri ve bağımsız kaynaklarla çapraz doğrulama daha önemli hâle gelir.

ABD'deki TAKE IT DOWN Act dosyaları, AI ile üretilmiş rıza dışı mahrem içeriklerin ceza hukukunda doğrudan yeni düzenlemelerle karşılanmaya başladığını gösterir. Kuzey Kore bağlantılı uzaktan IT çalışanı dosyalarında ise kimlik sahteciliği, wire fraud, kara para aklama ve yaptırım ihlali gibi klasik suç tiplerinin yeni dijital yöntemlerle birleştiği görülür.

Mahkeme kararları ve iddianameler aktarılırken hukuki statü titizlikle korunmalıdır: tutuklama mahkûmiyet değildir; iddianame kesin hüküm değildir; soruşturma açıklaması suçun kesinleştiği anlamına gelmez. Bu ayrım, araştırma kitabının güvenilirliğinin temelidir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

GERÇEK OLAY DOSYASI — ABD: Laptop Farm ve Kuzey Kore

ABD Adalet Bakanlığının 2025-2026 dosyaları, Kuzey Kore bağlantılı uzaktan IT çalışanlarının çalıntı veya ödünç kimliklerle ABD şirketlerinde iş elde etmesine yardımcı olan 'laptop farm' yapılarını ortaya koydu. Nisan 2026'da iki ABD vatandaşı, 100'den fazla şirkete uzanan ve 5 milyon doların üzerinde gelir üreten şemadaki rolleri nedeniyle hapis cezaları aldı.

Olayın kritik noktası, saldırganın yalnızca teknoloji kullanması değildir. Güvenilir görünen bir bağlam yaratmasıdır. İnsan, ekranda tanıdığı bir yüzü gördüğünde veya kurumsal bir yazı biçimiyle karşılaştığında teknik şüphe eşiğini düşürebilir. Bu nedenle modern güvenlik mimarisi, kişinin 'inandım' kararını tek başına işlem yetkisine dönüştürmemelidir.

Bu vaka Haberleşme açısından değerlendirildiğinde önerilen temel savunma katmanları şunlardır: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme. Kontrollerin amacı saldırıyı tahmin etmekten çok, tek bir yanlış güven kararının geri döndürülemez sonuca dönüşmesini engellemektir.

KAYNAK NOTU
U.S. Department of Justice: TAKE IT DOWN Act deepfake charges (20.05.2026); DPRK remote IT worker cases (2025-2026).

KURGU SENARYO — Borsada Olmayan Haber

Saat 01.31. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Finans alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

GÖRSEL DOSYA 122 — Yapay zekâ, organize suç ve kritik altyapı güvenliğinin kesişimi

Görsel, kitabın kavramsal anlatımı için yapay zekâ ile üretilmiştir. Belirli bir gerçek saldırının fotoğrafı değildir.

KURGU SENARYO — Bir Başkanın Sahte Sesi

Saat 08.44. Operasyon merkezinde gece vardiyası sakin başlamıştı. Ekranlardaki göstergeler normal görünüyordu. Sonra küçük bir tutarsızlık belirdi. Tek başına bakıldığında önemsizdi; fakat birkaç dakika içinde başka sistemlerden gelen verilerle uyuşmazlık büyüdü. İlk refleks arızaydı. İkinci ihtimal insan hatasıydı. Üçüncü ihtimal ise kimsenin yüksek sesle söylemek istemediği kelimeydi: müdahale.

Bu senaryo Sağlık alanında geçmektedir. Güvenlik ekibi saldırganı 'avlamaya' çalışmak yerine önce emniyetli durumu korumaya yönelir. Kritik fonksiyonlar ayrıştırılır, şüpheli veri kaynakları tek başına karar üretmeyecek şekilde sınırlandırılır ve güvenilir yedek kanallar devreye alınır. Operasyon ekibi ile siber güvenlik ekibi aynı olay günlüğü üzerinden ilerler.

Dakikalar ilerledikçe asıl sorun ortaya çıkar: teknik sistemler kadar insanlar da baskı altındadır. Sosyal medyada olayla ilgili sahte görüntüler dolaşmaya başlamış, yöneticilere ait olduğu iddia edilen ses kayıtları farklı talimatlar vermektedir. Kriz artık yalnızca ağ güvenliği değildir; bilgi bütünlüğü, kamu güveni ve komuta zinciri problemidir.

Alınması gereken önlemler: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt. Ayrıca olayın adli boyutu için loglar değişmez biçimde korunmalı, saat senkronizasyonu doğrulanmalı, müdahale sırasında yapılan her değişiklik kaydedilmeli ve dış iletişim tek doğrulanmış kanaldan yürütülmelidir.

Senaryo tamamen kurgudur; gerçek kişi, kurum veya devam eden operasyonu temsil etmez.

EK — SEKTÖREL ACİL DURUM KONTROL LİSTELERİ

Dijital kimlik ve deepfake

Öncelikli kontroller: İkinci kanal doğrulama, içerik kökeni, hesap güvenliği, delil koruma.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Havacılık

Öncelikli kontroller: Uçuş emniyeti önceliği, bağımsız sensör doğrulaması, segmentasyon, yedek prosedür, olay raporlama.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Uzay sistemleri

Öncelikli kontroller: Yer istasyonu güvenliği, telemetri bütünlüğü, komut yetkilendirmesi, anahtar yönetimi, görev sürekliliği.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Enerji

Öncelikli kontroller: OT/IT ayrımı, güvenli manuel işletim, koruma röleleri, ağ segmentasyonu, yedek haberleşme.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Bağlantılı araçlar

Öncelikli kontroller: UNECE R155 yaklaşımı, CSMS, yazılım güncelleme güvenliği, filo izolasyonu, güvenli durum.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Savunma sanayii

Öncelikli kontroller: Zero Trust, tedarik zinciri, model/veri bütünlüğü, insan gözetimi, TEV&V.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri

korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Haberleşme

Öncelikli kontroller: PACE yedekliliği, kimlik doğrulama, ağ ayrıştırma, spektrum ve trafik anomali izleme.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Finans

Öncelikli kontroller: İşlem limiti, davranış analizi, geri arama, çift onay, hızlı dondurma.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Sağlık

Öncelikli kontroller: Hasta güvenliği, klinik ağ izolasyonu, cihaz envanteri, offline prosedür, yedek kayıt.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

Lojistik

Öncelikli kontroller: Tedarik zinciri görünürlüğü, kimlik doğrulama, rota/veri bütünlüğü, manuel doğrulama.

1) İnsan güvenliği ve fiziksel emniyet öncelenir. 2) Şüpheli dijital bileşen mümkünse güvenli biçimde izole edilir. 3) Kritik hizmetler yedek veya manuel prosedüre alınır. 4) Loglar, saat bilgileri ve konfigürasyon değişiklikleri korunur. 5) Yetkili kriz ekibi ve hukuki birim bilgilendirilir. 6) Kamuya açıklama yalnızca doğrulanmış bilgiyle yapılır. 7) Sistem geri dönüşü, temiz ve doğrulanmış durumdan gerçekleştirilir.

KAYNAKÇA

1. United Nations Treaty Collection — United Nations Convention against Cybercrime, New York, 24 December 2024.

2. United Nations Office of Legal Affairs — The United Nations Convention against Cybercrime opens for signature in Hanoi, 25-26 October 2025.

3. NATO — Summary of NATO's Revised Artificial Intelligence Strategy, 10 July 2024.

4. NATO — Washington Summit Declaration, 10 July 2024.

5. NATO — Digital Transformation Implementation Strategy, 17 October 2024.

6. NATO — Alliance Digital Strategy, 13 January 2026.

7. ICAO — Aviation Cybersecurity Strategy.

8. ICAO — Manual on Aviation Information Security (Doc 10204), 2025.

9. ESA — ESA inaugurates new Cyber Security Operations Centre, 27 May 2025.

10. UNECE — UN Regulation No. 155, Cyber Security and Cyber Security Management System.

11. Hong Kong Government — LCQ9: Combating frauds involving deepfake, 26 June 2024.

12. Singapore Police Force — Advisory on scams involving impersonation of senior government officials, 14 May 2026.

13. U.S. Department of Justice — Two Individuals Arrested for Publishing AI Deepfake Pornography in Violation of TAKE IT DOWN Act, 20 May 2026.

14. U.S. Department of Justice — DPRK Remote IT Worker cases and sentencing releases, 2025-2026.

15. INTERPOL — Global Financial Fraud Threat Assessment, 2026; Operation Jackal IV, 2026.

16. İstanbul Emniyet Müdürlüğü — Siber Suçlarla Mücadele Şube Müdürlüğü Basın Duyurusu, 15 Mayıs 2025.

17. Kişisel Verileri Koruma Kurumu — Deepfake Bilgi Notu.

18. T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı — 2024-2028 Savunma Sanayii Sektörel Strateji Dokümanı.

19. Selçuk DİKİCİ — Kişisel Akademik Sayfa ve Özgeçmiş, www.selcukdikici.com.tr/selcuk-dikici/.

SON SÖZ

Yapay zekâ suç örgütlerine hız kazandırabilir; fakat aynı teknoloji savunmaya da hız kazandırabilir. Asıl farkı yaratacak olan teknolojiye kimin önce sahip olduğu değil, kimin daha iyi yönettiğidir. Bir kurum, görüntülü görüşmeyi tek doğrulama kabul etmiyorsa deepfake'in etkisi azalır. Bir enerji işletmesi manuel güvenli işletimi koruyorsa dijital kesinti fiziksel felakete dönüşmeyebilir. Bir uydu operatörü komut bütünlüğünü, anahtar yönetimini ve yer istasyonu güvenliğini birlikte ele alıyorsa tek bir zafiyet görev kaybı anlamına gelmez.

Geleceğin güvenlik modeli; hukuk, mühendislik, istihbarat, adli bilişim, insan faktörü ve uluslararası iş birliğini aynı masaya oturtmak zorundadır. Çünkü yapay zekâ destekli suçun sınırı yoktur. Savunmanın da yalnızca kurum sınırları içinde kalması mümkün değildir.

Selçuk DİKİCİ
Endüstri Mühendisi
(Bilişim Teknolojileri ve Siber Güvenlik Uzmanı)
www.selcukdikici.com.tr