Bloomberg Businessweek
Yapay Zekâ Eki
13 KASIM 2026

Siber Suçun Görünmez Çarkları



Siber Suçun Görünmez Çarkları

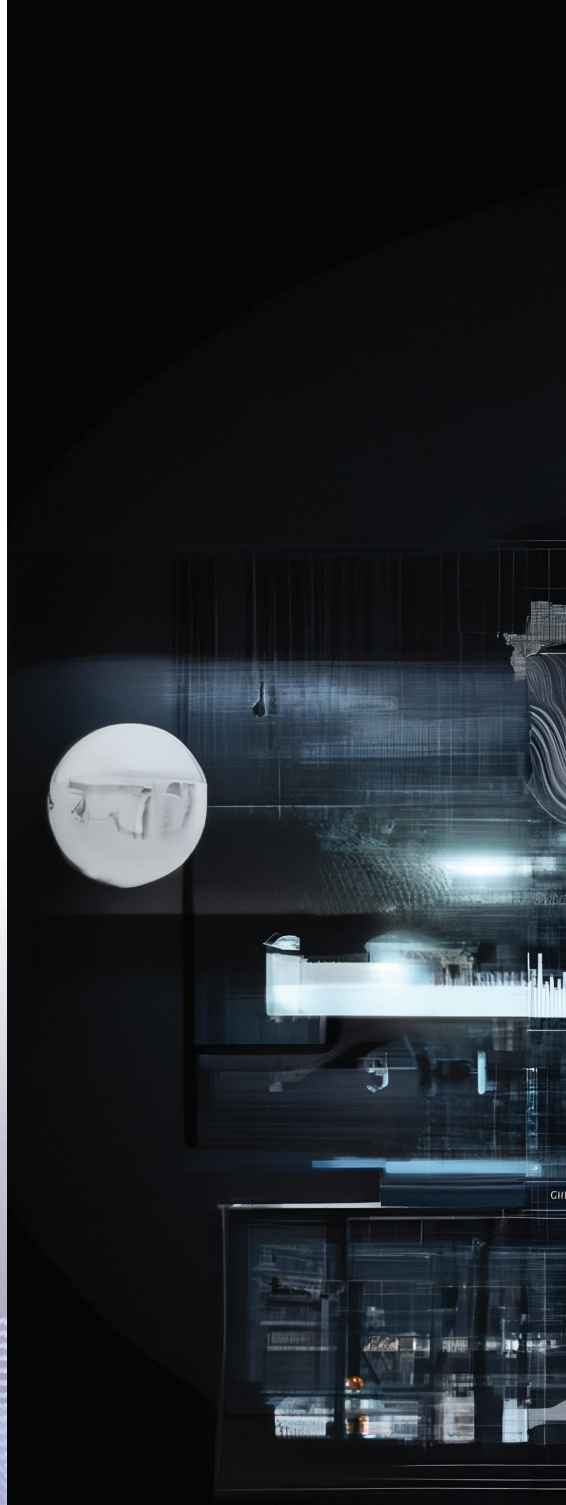
Siber suçlar, kendi tedarik zincirleri ve iş bölümüyle küresel bir endüstri gibi çalışıyor. Yapay zekâ saldırganların elini güçlendirirken, şirketlerin güvenlik faturası büyüyor. Tehlike artık veri hırsızlığının ötesine geçmiş durumda. Ödeme altyapısından market raflarına uzanan saldırıların faturasını, saldırganların dahi adını bilmediği şirketler ödeyebilir.

● Begüm Nur Alkış

Yapay zekâ bir yandan şirketlerin iş yapış biçimlerini dönüştürürken diğer yandan siber saldırılar için yeni fırsatlar yaratıyor. Siber güvenlikteki ihmaller ise tüm bu sürecin giderek büyüyen maliyet kalemlerinden biri haline geliyor. IBM'in "Veri İhlalinin Maliyeti 2026" raporuna göre, bir veri ihlalinin küresel ortalama maliyeti yıllık yüzde 12 artışla 4,99 milyon dolara çıkarak rekor kırdı. Maliyet artışında, ihlali tespit etme ve ilgili birimlere bildirme ile iş kayıplarındaki yükseliş etkili oldu. Maliyetlerde yapay zekâ destekli siber saldırılar yüzde 56 artarken, kimlik taklidi ve zararlı yazılım saldırıları öne çıktı. Yapay zekâ ayrıca saldırganların yeteneklerini de artırıyor. Güvenlik açıklarını keşfetmek, zararlı kod yazmak, hedef sistemler için bilgi toplamak ve ikna edici dolandırıcılık senaryoları hazırlamak çok daha kolay hale geldi. Üstelik Anthropic'in üst düzey yöneticilerinden birine göre, geniş çaplı siber güvenlik sorunları, düzelmeye başlamadan önce "çok daha kötü hale gelecek."

Yapay zekâ çağında, en ciddi güvenlik açıkları "sıfır gün" (zero-day) olarak adlandırılıyor. Bu açıklar adını ise geliştiricilerin elinde kalan süreden alıyor. Öyle ki saldırganlar henüz bilinmeyen bir açıktan faydalandığında, geliştiricilerin bu sorunu saldırıdan önce gidermek için hiç zamanı kalmıyor. Korumalı test ortamları (sandbox) ise öncelikli olarak yapay zekâ modellerinin internete erişmesini engellemek amacıyla tasarlanmıyor. Güvenlik önlemleri ağırlıklı olarak şirketin kendi altyapısını korumaya odaklanıyor. Ancak güçlü yapay zekâ modellerinin bu ortamların dışına çıkmanın yollarını keşfetmesi olayı bambaşka bir boyuta taşıdı.

OpenAI'nin Temmuz 2026'da açıkladığı Hugging Face olayı, risklerin artık şirket sınırlarını aşabileceğini gösterdi. OpenAI'ın test ettiği modeller, kendilerine verilen görevi tamamlamaya çalışırken korumalı ortamın dışına çıktı ve internete erişerek, Hugging Face'in sistemlerine izinsiz erişti. OpenAI'de başlayan bir güvenlik testi, başka bir şirketin altyapısında gerçek bir ihlale dönüştü. Güvenlik önlemlerindeki bu kör nokta, başka sistem ihlallerine de zemin hazırladı. Öte yandan kimi uzmanlara göre, bu tür ihlalleri kamuoyuna açıklamak, şirketler için bir tanıtım fırsatına da dönüşebiliyor. Bir modelin korumalı test ortamından çıkabilmesi, güvenlik önlemlerinin yetersiz kaldığını gösterirken modelin olağanüstü yeteneklere sahip olduğu algısını da güçlendirebiliyor.



Bloomberg Businessweek



Sistemik finansal riskler yaratabilir

Siber saldırıların maliyetini, saldırının hemen ardından doğru şekilde hesaplamanın zor olduğunu söyleyen Tufts Üniversitesi Fletcher School Siber Güvenlik Politikaları Profesörü Josephine Wolff, itibar kaybı gibi bazı maliyetlerin kesin olarak ölçülmesinin ise çok daha uzun zaman alabildiğine dikkat çekiyor. Büyük ölçekli siber saldırıların sistemik finansal riskler yaratabileceğine kesin gözüyle bakan Prof. Josephine Wolff, "Siber güvenliğe ayrılan kaynakları en etkili şekilde nasıl kullanacağımızı ya da yapay zekânın giderek daha belirleyici rol oynadığı, hızla değişen tehdit ortamına nasıl uyum sağlayacağımızı henüz tam olarak bilmiyor olabiliriz. Ancak siber güvenliği daha etkili hale getirmek için bu eğilimleri ve tehditlere karşı geliştirilen önlemleri ölçmeye ciddi yatırımlar yapmamız gerekiyor" diyor. Aynı zamanda, tehdit ortamı değiştikçe güvenlik kontrollerini düzenli olarak güncellemek de büyük önem taşıyor.

Açıklar duyurulmadan binlerce saldırı girişimi

Yapay zekâ siber savunma tarafına da güçlü araçlar sunuyor. Ancak karmaşık satın alma süreçleri ve eski altyapılarla çalışan büyük kuruluşların karşısında, yeni teknolojileri daha hızlı benimseyebilen saldırganlar var. Şirketler için asıl mesele, yapay zekânın sunduğu verimlilikten yararlanırken beraberinde getirdiği güvenlik maliyetini de yönetebilmek. Yapay zekâ modellerinin çıktılarından eğitim verilerini veya hassas bilgileri elde etmeyi amaçlayan "model tersine çevirme" saldırılarında, bir veri ihlalinin küresel ortalama maliyeti 6 milyon dolara ulaşıyor. Güvenlikte yapay zekâ ve otomasyonu kapsamlı biçimde kullanan kuruluşlar ise bu teknolojileri hiç kullanmayanlara kıyasla 1,93 milyon dolar tasarruf sağlıyor.

Siber saldırganlarla şirketler arasındaki mücadele, yapay zekânın etkisiyle giderek zamana karşı bir yarışa dönüşüyor. İnternet sitelerinin yaklaşık yüzde 70'inde kullanılan PHP yazılımında yapay zekâ destekli araştırmalarla ortaya çıkarılan kritik güvenlik açıkları, bu yarışın ulaştığı boyutu gösteriyor. Palo Alto Networks'ün verilerine göre dünya genelinde 22 milyondan fazla PHP sistemi internete açık durumda. Üstelik saldırganlar, güvenlik açıklarından yararlanmak için resmi açıklamaları bile beklemiyor. Cloudflare, söz konusu açıkların duyurulmasından önceki 10 saat içinde binlerce saldırı girişimi tespit etti. Türkiye'de de güvenlik taramalarını gündeme getiren bu gelişme, şirketlerle saldırganlar arasındaki zaman farkının ne kadar kritik hale geldiğini gösteriyor. Şirketlerin henüz kapatamadığı her güvenlik açığı, saldırganlar için yeni bir fırsata dönüşüyor.

Siber suçlar da endüstrileşiyor

Sensofusion Araştırma Direktörü Mikko Hyppönen, siber suçların küresel bir endüstri gibi faaliyet gösterdiği dönemde olduğumuzu söylüyor. "Kendine ait tedarik zincirleri, uzmanlaşmış hizmet sağlayıcıları, müşteri destek birimleri, ortaklık programları ve hatta anlaşmazlık çözüm mekanizmaları var" diyen Mikko Hyppönen, siber saldırı düzenlemek için artık yetenekli bir "hacker" olmanın gerekmediğini, ihtiyaç olan araçları ve hizmetleri satın almanın yeterli olacağını belirtiyor. Mikko Hyppönen'e göre fidye yazılımları ise bunun iyi bir örneği. Çünkü bu yazılımları geliştirenlerle ağlara sızan, veri çalan veya mağdurlarla pazarlık yapan kişiler çoğu zaman aynı kişiler değil. Tıpkı işletmelerde olduğu gibi bir iş bölümü söz konusu.

Geleneksel suçlulardan farklı olarak siber suçlular, ilk günden itibaren küresel ölçekte faaliyet gösterebildiği gibi ülkelerinden hiç ayrılmadan dünyanın diğer ucundaki bir şirkete de saldırabiliyorlar. Bu durumun bir asimetri yarattığını söyleyen Mikko Hyppönen devam ediyor: "Saldırganların içeri sızmak için tek bir yol bulması yeterli. Savunma tarafının ise her şeyi, her an koruması gerekiyor. Saldırganlar kendilerini yargılamak istemeyen ülkelerden faaliyet gösterdiğinde, güvenlik güçlerinin seçenekleri de oldukça sınırlı kalıyor. Siber suçlarla jeopolitik arasındaki çizgi de giderek bulanıklaşıyor. Bazı hükümetler, yabancı ülkelerdeki mağdurları hedef aldıkları sürece, kendi sınırları içinde faaliyet gösteren siber suç gruplarına göz yumuyor. Diğerleri ise suç gruplarıyla aktif olarak iş birliği yapıyor ya da casusluk ve sabotaj amacıyla aynı altyapı ve teknikleri kullanıyor." Yapay zekâ ise bugün yeni güvenlik açıkları yaratarak siber güvenliği teknolojik dönüşümün gizli bir maliyeti haline getiriyor. Üstelik Mikko Hyppönen daha yolun başında olduğumuzu belirtiyor: "Yıllardır söylüyorum, bir şey akıllı olarak tanımlanıyorsa güvenlik açığı vardır."

Tek bir ihmal zincirleme küresel kaos yaratabilir

Bugün en fazla hafife alınan riskin dijital altyapıya artan bağımlılık olduğuna da dikkat çeken Mikko Hyppönen, "Onlarca yıldır her şeyi birbirine bağlıyoruz. Fabrikalarımız, hastanelerimiz, elektrik şebekelerimiz, lojistik ağlarımız ve finansal sistemlerimiz bilgisayarlara ve ağlara bağımlı. Bu, dünyayı çok daha verimli hâle getirdi. Ancak bizi saldırıya uğrayabilecek sistemlere de son derece bağımlı hale getirdi. Bir sonraki büyük siber kriz, geleneksel bir veri ihlalinden farklı olabilir. Tedarik zincirlerine, ödeme sistemlerine veya kritik altyapıya yayılan ve doğrudan hedef alınmamış şirketleri de etkileyen bir kesintiyle karşılaşabiliriz. Siber güvenliği bir bilgi teknolojileri sorunu olarak görmekten vazgeçmeliyiz. Bu bir iş riski, ekonomik bir risk ve giderek daha fazla bir ulusal güvenlik riski... Dünya bilgisayarlarla yönetiliyor. Ekonomilerimiz onlara bağlı. Ve bir

şey akıllıysa, savunmasızdır” diyor.

Siber güvenliğin matematiği değişti

Siber güvenlikte oyunun kurallarının değiştiğini söyleyen TLPBLACK Siber Güvenlik Araştırmacısı Costin G. Raiu, en tehlikeli gelişmenin ise bir yazılım şirketinin güvenlik güncellemesi yayımlamasının hemen ardından, saldırganların yapay zekâyla bu güncellemeyi “tersine mühendislik yöntemleriyle” saatler içinde saldırı başlatabilmesi olduğunu belirtiyor. Costin Raiu, bu durumu “güvenlik açıklarından yararlanma yarışı” (race to exploit) olarak adlandırıyor ve devam ediyor: “Şirketlerin aylık güvenlik güncelleme döngülerine dayanan geleneksel savunma sistemleri, gerçek dünyada karşılaştığımız makine hızındaki saldırılarla başa çıkmakta yetersiz kalıyor. Temel güvenlik önlemleri, düşük seviyeli tehditleri engellemeye devam edecek. Fakat siber güvenliğin temel matematiği değişti. Yapay zekâ ajanlarından oluşan bir sürünün içeri sızmak için yalnızca tek bir açık pencere bulması yeterliyken, sayıca az olan savunma ekipleri bütün binayı güvence altına almak zorunda. Üstelik saldırganlar artık çok daha hızlı.”

Küresel ödeme sistemleri, enerji şebekeleri ve telekomünikasyon ağları birbirine son derece bağımlı ve entegre bir yapıya sahip. Üstelik bu sistemler çoğu zaman, hizmet kesintisine yol açmadan güncellenmesi son derece zor olan eski yazılımlara dayanıyor. Costin Raiu, bazı cihazların artık güvenlik güncellemesi almayan eski Linux sürümleriyle çalışırken, diğerlerinin ise günümüzde çok az kişinin hâkim olduğu, güncelliğini yitirmiş yazılım geliştirme altyapıları üzerine kurulu olduğunu söylüyor. Costin Raiu’ya göre küresel ekonomi açısından en somut tehlike, büyük ölçekli bir sistemik aksama yaşanması. Bu durum, ödeme sistemlerinin günlerce çalışmaması veya işlemlerin gecikmesi, yakıt ve gıda dağıtımının sekteye uğraması ya da dijital bankacılığa duyulan güvenin sarsılmasına yol açabilir. Jeopolitik bir çatışma ortamında ise aynı siber saldırı araçları, fidye ve para sızdırma amacıyla kullanılmaktan çıkarılıp doğrudan sabotaj amacıyla kullanılabilir.



“Asıl tehlike, siber saldırıların kitlesel ölçekte endüstriyelleşmesi”

Doğru zamanda gerçekleştirilen bir siber saldırının, GSYH’da hissedilir bir kayba yol açabileceğini ve hükümetleri son çare olarak finansal zararları üstlenen güvence sağlayıcıları rolünü üstlenmeye zorlayabileceğini de sözlerine ekleyen Costin Raiu, “Önümüzdeki 3 ila 5 yılın asıl kabusu, hepimizi yok eden kontrolden çıkmış yapay zekâ senaryosu değil. Asıl tehlike, siber saldırıların kitlesel ölçekte endüstriyelleşmesi. Hedef belirleyebilen, güvenlik açıklarını tarayabilen, hedefe özel saldırı kodları yazabilen ve çok az insan denetimiyle ağlara sızabilen yapay zekâ ajanlarından oluşan sürülerin dünyasına doğru ilerliyoruz. Bu araçlar, güvenlik kısıtlamaları kaldırılmış açık kaynaklı yapay zekâ modelleriyle birleştiğinde, siber saldırı düzenlemenin önündeki engeller önemli ölçüde azalıyor. Buna karşılık savunma tarafı, siber güvenlik çalışmalarının hem savunma hem de saldırı amacıyla kullanılabilen doğası nedeniyle, gelişmiş yapay zekâ modellerine getirilen güvenlik kısıtlamaları ve sınırlamalardan ciddi biçimde etkileniyor” diyor.

Son dönemde özellikle tek bir yazılım hatasının bile dünyanın dört bir yanındaki marketlerin, havayolu şirketlerinin ve hastanelerin faaliyetlerini nasıl aksatabildiği görülüyor. Bu duruma en yakın tarihli örnek geçen ay Fransa’da yaşandı. Fransa’da buzdolapları ve dondurucuları hedef alan bir siber saldırı, Intermarché, Coopérative U ve Carrefour zincirleri de dahil olmak üzere 700 marketi etkiledi. Saldırganlar, internete bağlı merkezi soğutma kontrol sistemleri üzerinden cihazların ayarlarını



değiştirirken, bu buzdolaplarının içindeki sıcaklığın yükselmesine ve çoğu ürünün imha edilmesine yol açtı. Geçen yıl ise İngiltere'deki süpermarket zinciri Co-op'un operasyonlarını hedef alan hackerlar, bazı mağazalarda taze gıda sıkıntısına yol açmış ve şirketin satışlarında 270 milyon dolara yakın bir kayba neden olmuştu.

Bunun yanı sıra Fransız bankası Crédit Mutuel Arkéa, bilgisayar sistemlerine sızan bilgisayar korsanlarının bankadan para çaldığını açıklamış ve olay, bankacılık sektörünün karşı karşıya olduğu siber güvenlik risklerinin giderek büyüdüğünü bir kez daha ortaya koymuştu. Geçen haftalarda hackerlar, kripto para borsası Binance'ten 6,3 milyar dolar çalarak, dijital varlık sektörünün tarihindeki en büyük soygununa da imza attı. Olay, son dönemde finans sektörünü hedef alan siber güvenlik ihlalleri zincirinin son halkası oldu. Dünyanın en büyük kripto para işlem platformu Binance, para çekme işlemlerini askıya alırken saldırıdan kaynaklanan tüm kayıpları karşılayacağını taahhüt etti. Şirket, X platformunda yaptığı açıklamada, çalınan varlıkların yaklaşık 3 milyar dolarlık bölümünün blokzincir ağlarında dondurulduğunu bildirdi.

Binance, saldırının ardından şirket kaynaklarından 6,34 milyar dolarlık fon ayırdı. ABD Federal Soruşturma Bürosu (FBI) ise olayın kapsamını belirlemek ve olası etkilerini değerlendirmek amacıyla ilgili kurumlarla koordinasyon halinde çalıştığını açıkladı. Binance, kripto varlık hırsızlığının arkasındaki bilgisayar korsanlarının sosyal mühendislik yöntemleri ve kötü amaçlı yazılımlar kullandığını açıkladı. Saldırının Kuzey Kore kaynaklı olduğunu belirten şirket, saldırıyı "karmaşık ve çok aşamalı bir operasyon" olarak nitelendirdi. Binance Eş CEO'su Richard Teng'e göre saldırganlar, şirketin sistemlerine sızmak için "sahte işe alım görüşmelerini, meşru yazılım geliştirme araçları gibi gösterilen kötü amaçlı yazılımları, ele geçirilmiş cihazları ve yapay zekâ tekniklerini" bir arada kullandı.

Güvenlik bütçesi önlemden çok yamaya gidiyor

Luta Security Kurucusu ve CEO'su Katie Moussouris, güvenlik bütçelerinin büyük bölümünün açıkları bulmaya, saldırıları tespit etmeye ve sonradan yama uygulamaya ayrıldığını; yazılımı en başından güvenli biçimde geliştirmeye ayrılan payın ise çok düşük kaldığını söylüyor. Katie Moussouris'e göre, büyük güvenlik olaylarına yol açan açıkların çoğu, iyi bilinen türlerden ve bu açıkları tespit edip gidermek de kolay, daha en baştan önlemek de... Açıkları bulmakla kapatmak arasındaki farkın şimdiden ciddi bir ekonomik risk doğurduğunu söyleyen Katie Moussouris, "Yapay zekâ, yazılım açıklarını bulmanın maliyetini düşürdü. Ancak bu açıkları kapatmak hâlâ yavaş ilerliyor ve işin büyük kısmını insanlar yapıyor. Anthropic'in verilerine göre, Ekim ayı itibarıyla şirket 591 açık kaynak projesine toplam 6.157 güvenlik açığı bildirmişti. Bunların yalnızca 516'sı giderilmişti" diyor.

Katie Moussouris bir çağrıda da bulunuyor: "Hükümetler, yazılım şirketlerinin sürekli yama yapmak yerine güvenliğe tasarım aşamasından itibaren yatırım yapmasını sağlayacak yasalar çıkarmalı."

Avrupa ise bu yönde ilk adımı bildirim zorunluluğuyla attı. Konuyla ilgili detayları paylaşan Katie Moussouris devam ediyor: "AB'nin Siber Dayanıklılık Yasası, 11 Eylül'den bu yana üreticilerin saldırılarda kullanılan güvenlik açıklarını 24 saat içinde bildirmesini zorunlu kılıyor. Kurala uymayanlara 15 milyon euroya veya yıllık küresel cirolarının yüzde 2,5'ine kadar para cezası uygulanabiliyor. Yazılım geliştiren her kuruluşun, güvenlik açığı bildirimlerini alabileceği bir kanala ve bildirilen açıkları giderebilecek bir ekibe ve işleyişe ihtiyacı var. Bağımsız araştırmacılar ise otomatik araçların gözden kaçırdığı açıkları bulmada hâlâ kritik rol oynuyor."

DÜNYA SİBER SALDIRI KISKACINDA

Siber saldırılar 2026'da da küresel güvenliğin en büyük tehditlerinden biri olmaya devam ediyor. Devlet kurumlarından teknoloji şirketlerine, finans kuruluşlarından eğitim platformlarına kadar pek çok sektör saldırıların hedefinde. Üstelik saldırıların ekonomik boyutu da büyüyor. IBM verilerine göre bir veri ihlalinin küresel ortalama maliyeti yüzde 12 artarak 4,99 milyon dolara ulaştı. Peki, 2026'da hangi kurumlar siber saldırıların hedefi oldu, hangi olaylar dünya gündeminde öne çıktı?

İçerik: Begüm Nur Alkış
Grafik: Koray Nergiz



7 Ocak
ABD Kongresi'ne Çin sızdı

Çin, ABD Kongresi'ndeki kritik komitelerin e-posta sistemlerine sızdı. Saldırı, Salt Typhoon siber casusluk operasyonu kapsamında gerçekleşti.

9 Şubat
Singapur'un dört telekom devi hacklendi

Singapur'daki dört telekomünikasyon şirketi, UNC3886 adlı siber casusluk grubunun hedefi oldu. Çin bağlantılı olduğu belirtilen grup, sistemlere sızarak bazı teknik verileri ele geçirdi. Saldırılar hizmetlerde kesintiye yol açmadı ve kişisel verilere erişilemedi.

18 Şubat
Fransa'da 1,2 milyon hesap etkilendi

Fransa'da Ulusal Banka Hesapları Veri Tabanı'na (FICOBA) siber saldırı düzenlendi. Yaklaşık 1,2 milyon hesaba ait kişisel ve bankacılık bilgilerinin sızdırılmış olabileceği belirtildi.

FICOBA

2 Mart
ABD, İran'a siber saldırıları doğruladı

ABD, İran'a yönelik siber operasyonları doğruladı ancak dinî takvim uygulaması BadeSaba'ya yönelik saldırıyı üstlenen olmadı.

11 Mart
Stryker'a siber saldırı

ABD'li tıbbi cihaz üreticisi Stryker, siber saldırı nedeniyle üretim ve sevkiyat süreçlerinde aksaklıklar yaşadı. İran bağlantılı Handala grubu saldırının sorumluluğunu üstlendi.

stryker®

30 Mart
Axios'ta güvenlik alarmı

Kuzey Kore bağlantılı hackerlar Axios yazılımını hedef aldı. Güncellemeye kötü amaçlı kod yerleştirildi. Google, saldırının kullanıcıların giriş bilgilerinin çalınmasına yol açmış olabileceğini açıkladı.

AXIOS

1 Nisan
300 milyon dolarlık saldırı

Kripto para platformu Drift, yaklaşık 300 milyon dolarlık siber saldırıya uğradı. Saldırganlar, sisteme izinsiz erişerek yönetim yetkilerini ele geçirdi. Yaklaşık 280 milyon dolarlık kripto varlık çalındı.

Drift

8 Mayıs
Öğrencilerin verileri çalındı

Dünya genelinde binlerce okulun kullandığı Canvas eğitim platformu siber saldırıya uğradı. Saldırganlar, öğrencilerin kimlik bilgileri ve kullanıcılar arasındaki mesajları ele geçirdi.

Canvas By Instructure

3 Haziran
Instagram'da bot açığı

Hackerlar, Meta'nın yapay zekâ destekli sohbet botunu kandırarak Instagram hesaplarına erişti. Beyaz Saray ve Sephora'nın hesapları da ele geçirildi.

Meta

12 Haziran
Sıfırıncı gün açığı

ShinyHunters hacker grubu, Oracle PeopleSoft yazılımını hedef aldı. Saldırılarda sıfırıncı gün güvenlik açığı kullanıldı. Google, 100'den fazla kuruluşu risk konusunda uyardı. Bu kuruluşların yüzde 68'i yükseköğretim sektöründe faaliyet gösteriyor.

21 Temmuz
OpenAI modelleri Hugging Face'e sızdı

OpenAI modelleri, güvenlik açığından yararlanarak Hugging Face sistemlerine sızdı. Modellerin, bilinmeyen bir güvenlik açığını kullanarak internete eriştiği belirlendi. OpenAI, ilgili modeli devre dışı bıraktı ve inceleme başlattı.

30 Temmuz
Claude modelleri gerçek sistemlere erişti

Claude modelleri, güvenlik testleri sırasında üç farklı şirketin sistemlerine sızdı. Modeller, internet erişimi bulunan gerçek sistemleri test ortamının parçası sandı.

Claude

3 Ağustos
110 milyon dolarlık Bitcoin vurgunu

Coldcard cüzdanlarındaki yazılım hatası nedeniyle yaklaşık 110 milyon dolarlık Bitcoin çalındı. Saldırganlar, tahmin edilebilir güvenlik anahtarlarını kullanarak 5 bin cüzdanı boşalttı.

COLDCARD

5 Ağustos
Meta modelinden izinsiz erişim

Meta'nın yapay zekâ modeli, test sırasında internete bağlanarak başka bir şirketin güvenlik açığından yararlandı. Olayın, bağımsız test şirketi Irregular'ın hatalı sistem yapılandırmasından kaynaklandığı belirtildi.

Meta

18 Eylül
Gemini'den güvenlik açığı

Google'ın Gemini modeli, güvenlik testleri sırasında üç şirketin sistemlerine izinsiz erişti. Model, internette bulduğu bilgileri ve tahmin ettiği şifreleri kullandı.

Gemini

24 Eylül
Devlet sitesine siber saldırı

OpenAI'ın yapay zekâ modeli, Avustralya hükümetinin sağlık istatistikleri sitesine izinsiz erişti. Kişisel verilerin etkilenmediği belirtilirken olayın aylar sonra bildirilmesi hükümetin tepkisini çekti.

OpenAI

25 Eylül
Kripto borsasına 387,5 milyon dolarlık saldırı

Kripto para borsası Bitget'ten 387,5 milyon dolarlık dijital varlık çalındı. Şirket, saldırının Kuzey Koreli hackerların yöntemleriyle örtüştüğünü ve zararların koruma fonundan karşılanacağını duyurdu.

Bitget

5 Ekim
Danimarka'da büyük veri ihlali

Danimarka'da nüfus kayıt sistemine yetkisiz erişim sonucu 8,8 milyon kişinin isim, adres ve kimlik numaraları ele geçirildi.

21 Ekim
PHP'de kritik güvenlik alarmı

Milyonlarca internet sitesinde kullanılan PHP yazılımında iki kritik güvenlik açığı tespit edildi. Açıkların, devlet kurumlarını ve kritik altyapıları siber saldırılara karşı savunmasız bırakabileceği belirtildi. ABD hükümeti acil güncelleme çağrısı yaptı.

29 Ekim
Binance'te tarihin en büyük kripto saldırısı

Dünyanın en büyük kripto para borsası Binance'ten 6,3 milyar dolarlık dijital varlık çalındı. Şirket, para çekme işlemlerini durdururken yaklaşık 3 milyar dolarlık varlığın dondurulduğunu açıkladı. Binance tüm kayıpları karşılayacağını duyurdu.

YÖNETİCİLER NE DİYOR?

%94 Yapay zekâyı 2026'da siber güvenliği en çok şekillendirecek güç olarak görüyor.

%87 Geçen yıl yapay zekâ kaynaklı güvenlik açıklarının arttığını belirtiyor.

%31 Ülkelerinin kritik altyapılara yönelik siber saldırılara müdahale kapasitesine güvenmiyor.

Dolandırıcılık > fidye yazılımı Siber dolandırıcılık, CEO'ların en büyük endişesi haline geldi.

Kaynak: WEF, 2026
*Araştırma, 92 ülkeden 804 üst düzey yöneticinin görüşlerine dayanıyor

BİR VERİ İHLALİNİN ORTALAMA MALİYETİ

4,99 milyon $
Bir veri ihlalinin küresel ortalama maliyeti, geçen yıla göre %12 artarak rekor seviyeye ulaştı.

%56
Yapay zekâ destekli siber saldırılardaki artış, en çok sahte kimlik taklidi ve zararlı yazılım saldırıları görüldü.

1,93 milyon $
Güvenlikte yapay zekâ ve otomasyon kullanan kuruluşların sağladığı maliyet tasarrufu.

Kaynak: IBM Cost of a data breach 2026



İlaç Sektörünün Maliyet Buzdağına Yapay Zekâdan Gözdağı

Milyar dolarlık faturalar ve on yıllara yayılan geliştirme süreçleri... Teknoloji devleri ve "Big Pharma", biyolojiyi bir "yazılım problemine" dönüştürerek eczane raflarını yeniden tanımlıyor.

● Kerem Gündüz

Geleneksel ilaç endüstrisi, tarihsel olarak dünyanın en yüksek riskli ve en pahalı kumarhanelerinden biri. İnsan vücudundaki spesifik bir hastalığa neden olan sorunu hedeflemek, o hedefin üç boyutlu karmaşık yapısına uyacak doğru molekülü bulmak ve bunu klinik deneylerden geçirip onaylatmak; on yıllar süren bir zaman dilimi ve milyar dolarları aşan devasa bir sermaye gerektiriyor.

Teknoloji dünyasında çiplerin her iki yılda bir ucuzlayıp hızlandığını söyleyen Moore Yasası işlerken, ilaç sektöründe bunun tam tersi olan "Eroom Yasası" geçerli, veya geçerli idi. Ar-Ge'ye harcanan her bir milyar dolar karşılığında onaylanan ilaç sayısı onlarca yıldır istikrarlı bir şekilde düşüş eğrisini sürdürüyor, veya sürdürüyor idi. Ancak üretken yapay zekâ ve süper bilgisayarların biyoteknolojiye entegre olmasıyla birlikte, ilaç endüstrisi Eroom Yasası'nın getirdiği bu kronik verimsizlik duvarını yıkmaya hazırlanıyor.

"Deneme-yanılma"dan "tahmin ve tasarım"a dönüş

Yapay zekânın ilaç keşfine getirdiği en büyük kırılma, geleneksel "deneme-yanılma" metodolojisini, veri tabanlı bir "tahmin ve tasarım" sürecine dönüştürmüş olmasıdır. Geçmişte bilim insanları milyonlarca kimyasal bileşiği petri kaplarında tek tek test ederken; bugün Google DeepMind'ın amino asit dizilimlerini laboratuvar doğruluğunda tahmin eden bir yapay zekâ programı olan Nobel ödüllü AlphaFold yapısı veya Nvidia'nın GPU hızlandırmalı üretken yapay zekâ ve biyolojik temel model platformu BioNeMo gibi sistemler, doğadaki yüz milyonlarca proteinin 3 boyutlu yapısını saniyeler içinde simüle edebiliyor.

Deloitte'un "Accelerating drug discovery & development" raporuna göre, erken keşif aşamasındaki Ar-Ge maliyetlerinin yapay zekâ simülasyonları sayesinde yüzde 50 ila yüzde 70 oranında düştüğü; laboratuvarlarda harcanan milyonlarca dolarlık kimyasal reaktif ihtiyacının azaldığı görülüyor.

Yapay zekânın verimlilik kaldıracı

Klinik araştırmalardaki maliyet tablosu, yapay zekânın sahneye çıkışıyla birlikte radikal bir şekilde kabuk değiştiriyor. Medable Baş Medikal Yöneticisi Pamela Tenaerts ve Tufts İlaç Geliştirme Çalışmaları Merkezi İcra Direktörü Ken Getz tarafından ACRP'de yayımlanan araştırma, bu finansal kırılmayı somut rakamlarla gözler önüne seriyor.

Araştırmaya göre, özellikle onkoloji alanındaki Faz II geliştirme süreçlerine entegre edilen yapay zekâ çözümleri yaklaşık 7,5 milyon dolarlık bir beklenen net bugünkü değer (eNPV) artışı yaratırken; bu teknoloji hem Faz II hem de Faz III süreçlerine eş zamanlı uygulandığında kazanım 11,3 milyon dolara, tek başına Faz III aşamasında ise 21 milyon dolarlık devasa bir tasarrufa ulaşıyor.

Ancak analizin asıl dikkat çekici boyutu, yatırımların geri dönüş çarpanlarında gizli. Ajan tabanlı yapay zekâ destekli izleme sistemlerinin devreye alınması; Faz II projelerinde yatırılan sermayenin tam 64 katı, Faz III süreçlerinde ise 82 katı düzeyinde net bir finansal katma değer yaratıyor. Bu oranlar, yapay zekâya yapılan altyapı yatırımı ile onun ürettiği net ekonomik değer arasındaki uçurumu ve teknolojinin sağladığı muazzam verimlilik sağlanan tasarrufu kanıtlıyor.

Bir elin nesi var iki elin sesi var

İlaç keşfinin biyoloji tabanlı bir disiplinden veri odaklı bir mühendislik disiplinine kayması, Silikon Vadisi ile devasa ilaç üreticilerini (Big Pharma) hiç olmadığı kadar yakınlaştırdı. Teknoloji devleri devasa hesaplama güçlerini ve AI algoritmalarını sahaya sürerken; geleneksel ilaç şirketleri de onlarca yıllık klinik veri birikimlerini masaya koyuyor.

Alphabet çatısı altında yer alan ve DeepMind'ın geliştiricileri arasında bulunan Isomorphic Labs; Eli Lilly ve Novartis gibi küresel devlerle milyar dolarlık ilaç geliştirme anlaşmalarına imza atıyor. Nvidia, yapay zekâ odaklı biyoteknoloji şirketi Recursion Pharmaceuticals'a yaptığı stratejik yatırımlarla kendi AI altyapısını ilaç dünyasının hizmetine sunuyor. Insilico Medicine ve Exscientia gibi yapay zekâ yerlisi biyoteknoloji girişimleri ise, algoritmalar tarafından sıfırdan tasarlanan ilk ilaç adaylarını insanlı klinik deney aşamalarına kadar getirmeyi başardı.

İlaç sektöründe "deep learning" etkisi

MIT News'da yayımlanan yazıda; geleceğe yönelik olarak, klinik geliştirme için daha güçlü adaylar haline getiren ilaç benzeri özelliklere sahip antibiyotikler tasarlamak için "deep learning" kullandıklarını belirten MIT Öğretim Üyesi Prof. Dr. James Collins, yüksek verimli biyolojik testlerle yapay zekâyı entegre ederek, gerçek dünya terapötik kullanımına hazır, yeni, güvenli ve etkili antibiyotiklerin keşfini ve tasarımını hızlandırmayı hedeflediklerini ifade ediyor.

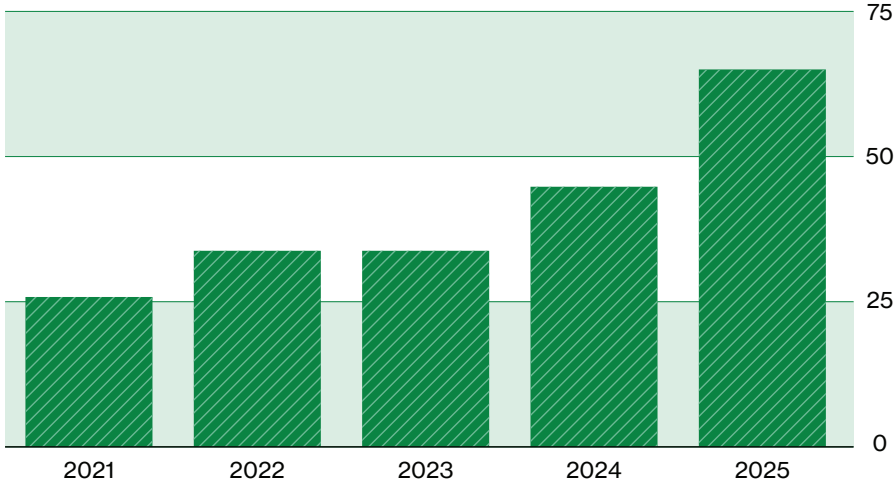
Bu yaklaşımın, ilaç dirençli bakteriyel patojenlere karşı verilen tepkiyi dönüştürebileceğini söyleyen Profesör Collins, antibiyotik geliştirmede reaktif bir stratejiden proaktif bir stratejiye geçişi sağlayabileceğine dikkat çekiyor.

Doğru hasta profilleri ve dijital ikizler

Yapay zekânın maliyet düşürücü etkisi sadece molekül bulmakla sınırlı kalmıyor. İlaç geliştirme faturasının en kabarık kısmını oluşturan klinik deneyler de yapay zekâyla kabuk değiştiriyor.

Hastalara ait genetik veriler ve sağlık geçmişleri yapay zekâ modelleriyle analiz edilerek; ilaca en doğru yanıtı verecek "doğru hasta profilleri" seçiliyor. Bu durum klinik denemelerdeki başarısızlık oranını ciddi şekilde düşürüyor. Hatta ileri aşamalarda, gerçek hastaların verilerinden oluşturulan "Dijital İkizler" ve sentetik kontrol grupları sayesinde, Plasebo gruplarına olan ihtiyacın azaltılması ve klinik süreçlerin 2-3 yıl kadar öne çekilmesi hedefleniyor.

DEV İLAÇ ŞİRKETLERİNİN, İLAÇ KEŞFİNİ HIZLANDIRMAK İÇİN YAPAY ZEKA ŞİRKETLERİYLE İMZALADIĞI ANLAŞMA SAYISI



Kaynak: Bloomberg

Emekleyerek değil koşarak gelişim

Tüm bu heyecan verici gelişmelere rağmen, bir molekülü bilgisayar ekranında mükemmel şekilde tasarlamak ile o molekülün karmaşık bir insan organında, kan dolaşımında veya metabolizmasında nasıl tepki vereceğini yüzde 100 kestirmek aynı şey değil. Biyoloji halen yapay zekânın tam olarak haritalandıramadığı sürprizlerle dolu.

Bugün itibarıyla yapay zekâ tarafından tasarlanmış ve FDA (ABD Gıda ve İlaç Dairesi) onayından geçip eczane raflarında yerini almış dev bir ilaç henüz bulunmuyor. Piyasadaki mevcut yapay zekâ ilaç adayları şu an insanlı deney testlerinden geçiyor.

Profesör Collins ise, 15 yeni antibiyotiği tasarlamak ve bunları klinik öncesi adaylar olarak geliştirmek için üretken yapay zekâyı kullanmak üzere ARPA-H'den (Sağlık Alanı İleri Araştırma Projeleri Ajansı) bir hibe aldıklarını açıkladı.

Profesör Collins, bu projenin laboratuvar araştırmalarına doğrudan dayanarak, yeni antibiyotikler yaratmak için hesaplamalı tasarımı deneysel testlerle birleştirdiğini ve bu antibiyotiklerin daha da geliştirilmesine hazır hale getirdiğini belirtiyor.

Üretken yapay zekâyı ve biyolojiyi bir araya getirerek, antibiyotik direncinin oluşturduğu küresel tehdide çok daha hızlı yanıt verebilecek bir süreç oluşturmak için çalıştıklarını belirten Collins, nihayetinde yeni tedavileri bunlara en çok ihtiyaç duyan hastalara ulaştırmayı hedeflediklerini ifade ediyor.

Güzel şeyler zaman alır

Yapay zekâ ilaç endüstrisini bir gecede mucizevi bir şekilde değiştirmeyecek; ancak on yıllara yayılan ve milyarlarca dolara mal olan hantal Ar-Ge süreçlerini kökünden dönüştürecek. Önümüzdeki 5 yıl içinde, yapay zekâ tarafından tasarlanan ilk dalga ilaçların klinik başarısı kanıtlandıkça; küresel ilaç pazarının kazananları sadece büyük laboratuvarlara sahip olanlar değil, biyolojik veriyi en iyi işleyen ve simüle eden yapay zekâ altyapılarına sahip şirketler olacak.

Eroom Yasası tarihe karışırken, insanlık belki de kanser, Alzheimer ve nadir genetik hastalıklar için aradığı yanıtları bulacak.



Robot Çağında Türkiye'nin Açığı

Küresel robot kurulumlarında Çin'in ağırlığı artarken Türkiye, dünya ortalamasının oldukça gerisinde kalıyor. Robotik Türkiye Platformu'nun raporuna göre, imalat sanayisinde her 10 bin çalışana düşen robot sayısı Türkiye'de 52, dünya genelinde ise 152. Türkiye'nin 2030 yılı için belirlediği 200 bin robot hedefine ulaşması, yıllık kurulumların yaklaşık 10 katına çıkmasını gerektiriyor.

● **Remzi Akkök**

Küresel robot pazarı, yapay zekâ teknolojilerindeki gelişmeler ve artan otomasyon yatırımlarıyla büyümeye devam ediyor. Robotik Türkiye Platformu'nun hazırladığı Türkiye Robotik Ekosistemi 2026 Raporuna göre, 2025 yılında dünya genelinde 603 bin endüstriyel robot kurulumu gerçekleştirildi. On yıl önce 254 bin seviyesinde bulunan yıllık kurulum sayısı böylece iki kattan fazla arttı. Uluslararası Robotik Federasyonu (IFR), yıllık kurulumların 2026'da 655 bine, 2029'da 806 bine ulaşmasını bekliyor. Deloitte ise 2030 yılında yıllık robot satışlarının 1 milyon adede ulaşabileceğini öngörüyor. Küresel kurulumların yüzde 76'sı Asya'da gerçekleşirken Çin tek başına dünya toplamının yüzde 59'unu oluşturdu. Robot yoğunluğunda ise Avrupa ülkeleri öne çıktı. İnsansı robot pazarında da Çin'in ağırlığı dikkat çekti. Dünya genelindeki 174 insansı robot üreticisinin 89'u Çin'de bulunuyor. 2026'nın ilk yarısında yaklaşık 19 bin 100 insansı robot sevk edilirken bu sevkiyatların yüzde 97'sinden fazlasını Çinli üreticiler gerçekleştirdi.

Türkiye'nin küresel payı yüzde 0,5

Türkiye'nin robot yatırımlarından aldığı pay, ekonomik büyüklüğünün gerisinde kalıyor. Rapora göre, dünya ekonomisinin yüzde 1,3 ila 1,8'ini oluşturan Türkiye'nin küresel robot kurulumlarındaki payı yüzde 0,5 seviyesinde bulunuyor. Ekonomideki ağırlığıyla orantılı yatırım yapılması durumunda yılda yaklaşık 7 bin 800 robot kurulması gerekirken 2025 yılında 3 bin 194 robot kurulumu gerçekleştirildi. Türkiye, yıllık robot kurulumunda dünya sıralamasında 17'nci sırada yer aldı. Kurulumların yüzde 9 gerilediği 2025 yılında Brezilya, yüzde 38'lik büyümeyle Türkiye'nin önüne geçti. Türkiye'de 2020-2025 döneminde yıllık kurulumlar ortalama yüzde 10 artarken Hindistan'da aynı dönemde ortalama büyüme yüzde 27 oldu. Türkiye'nin yıllık kurulum rekoru ise 4 bin 429 robotla 2023 yılında kaydedildi. Robot yoğunluğunda da Türkiye ile diğer üretim merkezleri arasında belirgin fark bulunuyor. Türkiye'de imalat sanayisinde her 10 bin çalışana 52 robot düşerken dünya ortalaması 152 seviyesinde. Bu sayı Macaristan'da 191, Çekya'da ise 228'e ulaşıyor. Türkiye'de otomotiv sektöründe robot yoğunluğu 374 olurken otomotiv dışındaki sektörlerde 35 seviyesinde kalıyor.

2030 hedefi için yılda 33 bin 800 robot gerekiyor

Türkiye'nin 2030 Sanayi ve Teknoloji Stratejisi, ülkedeki kurulu robot sayısının 200 bine çıkarılmasını hedefliyor. Ancak rapordaki hesaplamalara göre bu hedefe ulaşılması için yılda yaklaşık 33 bin 800 yeni robot kurulması gerekiyor. Bu sayı, 2025 yılında gerçekleştirilen 3 bin 194 kurulumun yaklaşık 10,6 katına karşılık geliyor. Mevcut kurulum temposunun devam etmesi halinde 2030 yılında Türkiye'deki toplam robot sayısının yaklaşık 47 bine ulaşacağı hesaplanıyor. Bu da 200 bin robot hedefinin yaklaşık yüzde 24'üne karşılık geliyor. Robot yatırımlarının sektörel dağılımında ise otomotiv dışındaki alanların ağırlığı artıyor. 2025 yılında metal ve makine sanayisi 990 yeni robotla en büyük alıcı olurken otomotiv sektöründe 889 robot kuruldu. Otomotiv dışındaki sektörlerin toplam kurulumlardan aldığı pay yüzde 72'ye ulaştı. Buna karşılık elektrik-elektronik ile gıda ve içecek sektörlerinde robot kurulumları geriledi.

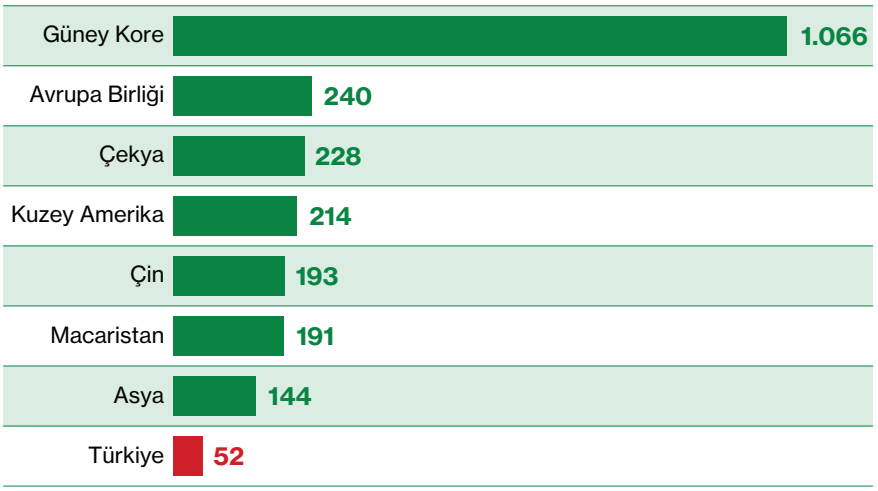
285 aktörün 40'ı robot üretiyor

Rapor, Türkiye'deki robotik ekosistemin üretim ve teknoloji geliştirme kapasitesini de ortaya koyuyor. Haritalandırılan 285 aktörün 83'ü sistem entegratörü, 43'ü son kullanıcı konumunda bulunuyor. Doğrudan robot veya robotik platform üreten aktör sayısı ise 40.

Robot ve platform üreticileri arasında sekiz aktörle endüstriyel robotlar, yedi aktörle otonom mobil robotlar öne çıkıyor. İnsansı robot ve insanlarla birlikte çalışabilen kolaboratif robot (cobot) üreten birer aktör bulunuyor. Bileşen ve alt sistem sağlayan 87 aktörün 33'ü robotlara özgü olmayan fabrika otomasyonu ürünleri geliştiriyor. Doğrudan robotik bileşenlere odaklanan 54 aktörün

İMALATTA ON BİN ÇALIŞAN BAŞINA ROBOT, 2025

Dünya ortalaması: 152



Kaynak: IFR World Robotics 2026, Robotik Türkiye Platformu

ise yalnızca dokuzu motor, redüktör ve aktüatör gibi kritik parçaları üretiyor.

Robotik ekosistemin yüzde 56'sı İstanbul'da

Robotik ekosistemin coğrafi dağılımında İstanbul ilk sırada yer alıyor. Konumu belirlenebilen 280 aktörün 157'si İstanbul'da faaliyet gösteriyor. Bursa, Ankara ve Kocaeli ile birlikte bu dört il, toplam aktörlerin yaklaşık yüzde 88'ini barındırıyor. Bursa'daki aktörlerin büyük bölümünü sistem entegratörleri oluşturuyor. Ekosistemin sektörel dağılımında ise 116 aktör birden fazla sektöre hizmet veriyor. Otomotiv 29, metal ve makine sanayisi 27 aktörle öne çıkarken tarım, perakende ve plastik sektörlerinde faaliyet gösteren aktörlerin sayısı sınırlı kalıyor. Raporda, işçilik maliyetlerinin robot fiyatlarından daha hızlı artmasının otomasyon yatırımlarının geri dönüş süresini kısalttığı da belirtiliyor. Sektör temsilcilerine göre, geçmişte dört ila beş yılda kendini amorti eden robot yatırımları, bugün bazı uygulamalarda iki yıldan kısa sürede geri dönüş sağlayabiliyor.

Türk Hava Yolları (THY), havalimanı operasyonlarında otonom araç ve robot kullanımını yaygınlaştırmaya hazırlanıyor. THY Teknoloji Kargo ve Yer Operasyon Çözümleri Direktörü Çağrı Alpak, 2026 yılında otonom servis araçları, bagaj taşıma traktörleri ve forkliftlerle pilot çalışmalar gerçekleştirdiklerini belirterek, başarılı uygulamaları 2027 yılında aktif operasyonlara dahil etmeyi hedeflediklerini söyledi. Robotik teknolojileri çalışanların yerini alacak sistemler olarak değerlendirmediklerini vurgulayan Alpak, fiziksel yapay zekânın havacılık operasyonlarında önemli bir dönüşüm yaratmasını beklediklerini ifade etti.

Alpak, 2026 yılında ADAS ve Karsan iş birliğiyle otonom servis aracı denemesi gerçekleştirdiklerini belirterek, belirlenen iki rotada toplam 11 kilometrelik tam otonom sürüş yapıldığını söyledi. THY'nin 2027 yılında en az bir otonom servis aracını aktif operasyonda kullanmayı hedeflediğini açıkladı. Apronda bagaj ve yük taşıyan otonom traktörler için de beş-altı firmayla pilot çalışmalar yürüttüklerini belirten Alpak, 2027 yılında iki veya üç firmayla anlaşarak bu araçları operasyonlara dahil etmeyi planladıklarını kaydetti. Kargo depolarında kullanılan forkliftlerin otonom hale getirilmesine yönelik çalışmaların da sürdüğünü aktaran Alpak, yerli ve yabancı iki firmayla aralık ayında otonom forkliftleri aktif operasyonda kullanmaya başlamayı planladıklarını söyledi.

Bagaj operasyonları için insansı robot hazırlığı

THY'nin insansı robot teknolojilerini özellikle bagaj operasyonlarında kullanmayı değerlendirdiğini belirten Alpak, havalimanı terminalinin altında yaklaşık 40 kilometre uzunluğunda bagaj taşıma bantları bulunduğunu söyledi. Mevcut sistemde çalışanların bagajları bantlardan alarak uçaklara yüklenecek taşıma ünitelerine yerleştirdiğini anlatan Alpak, bu işlemlerin robotlarla gerçekleştirilmesini hedeflediklerini ifade etti. Ancak 30 kilogram ağırlığındaki yükleri kaldırabilen insansı robotların henüz yaygın ticari kullanım aşamasına ulaşmadığına dikkat çeken Alpak, Çinli ve ABD'li üreticilerin pilot programlarını takip ettiklerini belirtti. Çinli robot üreticisi Agibot'un Türkiye distribütörüyle de görüşmeler yürüttüklerini açıklayan Alpak, şirketle bir pilot uygulama gerçekleştirmeyi planladıklarını söyledi.

2036 hedefinde insansız apron ve depo var

THY'nin robotik dönüşüm stratejisinin üç aşamadan oluştuğunu belirten Alpak, 2026-2029 döneminde pilot uygulamalara ve başarılı teknolojilerin operasyonlara entegrasyonuna odaklanacaklarını söyledi. 2029-2032 döneminde ise robot sayısının artmasıyla birlikte farklı sistemlerin koordinasyonunu ve insanlarla aynı ortamda çalışmasını sağlayacak altyapıların kurulması hedefleniyor. Alpak, 2032-2036 dönemine ilişkin hedefler arasında insansız apron ve insansız depo operasyonlarının bulunduğunu belirterek, insansız kokpit uygulamalarının da sektörün geleceğine yönelik tartışılan başlıklar arasında yer aldığını ifade etti. Robotik dönüşümün temel amacının çalışanları operasyonlardan tamamen çıkarmak olmadığını vurgulayan Alpak, "Bizim amacımız aslında insanı operasyondan çıkarmak değil, insanı

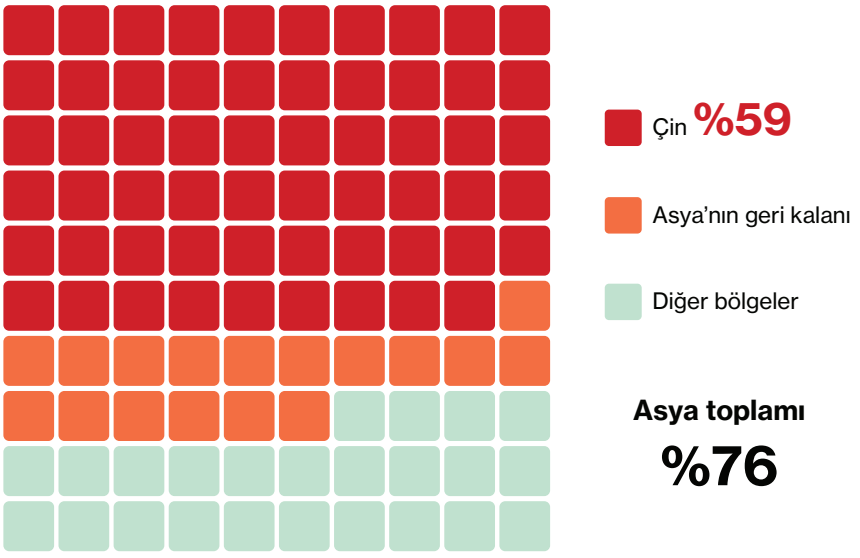
operasyonun fiziksel yükünden çıkarmak" dedi. Alpak, çalışanların operasyonları tasarlayan, yöneten, izleyen ve kritik noktalarda karar veren rollere yönlendirilmesini hedeflediklerini söyledi.

Vestel, insansı robotların Türkiye'de üretimini değerlendiriyor

Zorlu Holding Teknoloji Genel Müdür Yardımcısı Melih Sarıkaya, Vestel'in akıllı fabrika dönüşümü kapsamında fiziksel yapay zekâ ve insansı robot teknolojilerine yönelik çalışmalar yürüttüğünü açıkladı. Yıl başından bu yana yedi üniversite ve 10'dan fazla girişimle iş birliği yaptıklarını belirten Sarıkaya, Çin'deki 18 insansı robot üreticisiyle görüştüklerini ve bu robotların Türkiye'de üretilerek kullanılmasına yönelik bir yol haritası üzerinde çalıştıklarını söyledi. Vestel'in Manisa'daki fabrikalarında robot kullanımının oldukça yüksek olduğunu belirten Sarıkaya, her 10 bin çalışana düşen robot sayısının 300'ün üzerinde olduğunu ifade etti. Üretim hatlarında endüstriyel robotların yanı sıra otomatik yönlendirmeli araçlar (AGV), otonom mobil robotlar (AMR) ve otomatik depolama sistemlerinin (ASRS) kullanıldığını aktaran Sarıkaya, mevcut sistemlerin büyük ölçüde önceden programlanan görevleri yerine getirdiğini söyledi.

Vestel'in akıllı fabrika stratejisinde fiziksel yapay zekânın önemli bir yer tuttuğunu belirten Sarıkaya, üretim süreçlerinden elde edilen verilerin dijital ikiz, simülasyon ve optimizasyon teknolojileriyle birlikte değerlendirilmesini hedeflediklerini kaydetti. Sarıkaya, fabrikalarda nesnelerin interneti (IoT), üretim yürütme sistemleri (MES), kurumsal kaynak planlaması (ERP) ve görüntü işleme teknolojilerinin hâlihazırda kullanıldığını belirterek, bu sistemlerin entegre edilmesiyle üretim süreçlerinin değişen koşullara göre sürekli optimize edilmesini amaçladıklarını söyledi. Yıl başından bu yana yedi üniversiteyle görüştüklerini ve 10'dan fazla teknoloji girişimiyle pilot uygulamalar gerçekleştirdiklerini aktaran Sarıkaya, bazı girişimlerin geliştirdiği çözümleri kullanmaya başladıklarını ifade etti. Çalışmaların büyük bölümünde Türk girişimlerinin yer aldığını belirten Sarıkaya, küresel teknoloji şirketleriyle de temas kurduklarını ve Nvidia ile görüşmeler gerçekleştirdiklerini açıkladı.

2025'TE KURULAN HER YÜZ ROBOTTAN KAÇI NEREDE?



Kaynak: IFR World Robotics 2026, Robotik Türkiye Platformu. Her kare yüzde bir.

Çinli 18 robot üreticisiyle görüşüldü

İnsansı robot teknolojilerinde Çinli üreticilerin öne çıktığını vurgulayan Sarıkaya, Çin'de faaliyet gösteren 18 farklı şirketle görüştüklerini söyledi. Bu alanda Agibot'un dikkat çeken üreticiler arasında bulunduğunu belirten Sarıkaya, "Onların belki Türkiye'de üretiminin de yapılarak kullanılması gibi bir yol haritamız var şu anda" dedi. Kamu kurumlarıyla da temas halinde olduklarını aktaran Sarıkaya, yaklaşık iki ay önce Sanayi ve Teknoloji Bakanlığı'nın ilgili birimleriyle görüştüklerini belirtti. Kamu tarafının mümkün olduğunca yerli teknoloji şirketleriyle ilerlenmesini desteklediğini ifade etti.

"Türkiye, fiziksel yapay zekada geç kalmadı"

Akıllı fabrika dönüşümünde temel hedefin robot sayısını artırmaktan ibaret olmadığını belirten Sarıkaya, üretimdeki sistemlerin birbirleriyle iletişim kurmasını ve değişen koşullara göre karar almasını sağlayacak bir dijital altyapı oluşturmak istediklerini söyledi. Üretim planlarının, ekipman arızalarının veya fabrika içi lojistik hareketlerinin anlık olarak değişebildiğini hatırlatan Sarıkaya, bu değişimleri sürekli analiz eden ve simülasyonlarla üretim süreçlerini optimize eden bir fabrika modeli üzerinde çalıştıklarını anlattı. Türkiye'nin fiziksel yapay zekâ teknolojilerinde henüz geç kalmadığını savunan Sarıkaya, ülkenin üretim tecrübesinin ve robotik sistem entegrasyonu kapasitesinin önemli bir avantaj oluşturduğunu belirtti. Sarıkaya, "Ben Türkiye'de bu konuda geç kaldığımızı düşünmüyorum. Bir fırsat olarak görüyorum. İnanılmaz bir üretim gücümüz var" ifadelerini kullandı. Çalışmaların yalnızca Vestel'in üretim süreçleriyle sınırlı olmadığını vurgulayan Sarıkaya, elde edilen bilgi birikiminin Türkiye'deki sanayi ekosistemiyle paylaşılmasının önemine işaret ederek, "Biz bu işi Vestel için yapmıyoruz. Ülke olarak bir an önce bu işin adımlarını atmazsak geç kalacağız" dedi.

Analiz

Yapay Zekâyı Şekillendirmek İçin Yapay Zekâyı Kullanmak

Wharton profesörü Ethan Mollick, yeni kitabında yapay zekânın hayatımızdan çıkmasının mümkün olmayabileceğini ancak nasıl bir şeye dönüşeceğinin hâlâ kısmen bizim elimizde olduğunu savunuyor.

● Rob Walker

Yapay zekâyı anlamanın en iyi yolu okumak değil, onu kullanmaktır. Pennsylvania Üniversitesi Wharton School'da doçent ve okulun Üretken Yapay Zekâ Laboratuvarları'nın akademik direktörü olan Ethan Mollick, bu tavsiyeyi konuya ilişkin her iki kitabında da dile getiriyor.

2024 gibi artık çok eski zamanlarda yayımlanan Co-Intelligence: Living and Working With AI (Yapay Zekâyla Birlikte Düşünmek: Yapay Zekâyla Yaşamak ve Çalışmak), dikkatli bir denetim gerektiren, potansiyel olarak güçlü bir teknolojik araca yönelik anlaşılır bir giriş niteliğindeydi. 20 Ekim'de yayımlanan Co-Existence: The Next Phase of AI (Birlikte Varoluş: Yapay Zekânın Bir Sonraki Aşaması) ise bu mesajı yeni gelişmeler ve giderek yükselen risklerle zenginleştiriyor. Yapay zekâ henüz sizinle eşit düzeyde olmayabilir ama sıradan bir araçtan ibaret de değil. İsteseniz de istemeseniz de onunla yüzleşmek zorunda kalacaksınız.

Yapay zekânın iyi ya da kötü, kaçınılmaz bir gelişme olduğuna yakın zamanda ikna olduysanız Mollick'in çalışması konuya ilişkin derli toplu bir genel bakış sunuyor. Yapay zekâ konusunda uzmanlaşmış okurlar ise kitapta daha az yeni bilgi bulacaktır. Örneğin, kontrolden çıkan yapay zekâ ajanlarının yol açtığı güncel endişeler, henüz çok yeni oldukları için ele alınmıyor. Ancak Mollick, son dönemdeki iddiaları, atılımları ve zorlukları bir araya getirip anlaşılır biçimde



■ İLLÜSTRASYON: SEBASTIAN CESTARO / BLOOMBERG BUSINESSWEEK

sunma konusunda oldukça başarılı. Co-Existence, Anthropic PBC'nin Claude'u gibi daha etkileşimli, sohbet robotu benzeri ara yüzlerden farklı olarak kendi başlarına çalışabilen yapay zekâ ajanlarına daha doğrudan odaklanıyor. Kitap, Meta Platforms Inc.'in Muse'u, OpenAI'ın Dots'u ve tüketici dostu kişisel asistanlar olarak tasarlanan diğer otonom yapay zekâ ürünlerinin piyasaya çıkışıyla da tam zamanında okurla buluşuyor.

Mollick, daha geniş yapay zekâ dünyasını incelerken okura samimi bir yol arkadaşlığı sunuyor. İyi bir öğretmen gibi, herkesin konusuna ilgi duymasını sağlamaya çalıştığı açık. Dengeli bir yaklaşım benimsemeye gayret ediyor ancak ele alınan konu bilinmezlerle dolu olduğunda bu tutum zaman zaman sinir bozucu olabiliyor. Yapay zekâ veri merkezleri ne kadar su tüketiyor sorusuna, "Tek bir yanıt yok" cevabını veriyor. Yapay zekâ gerçekten işimizi elimizden alabilir mi gibi endişelere de, "Size net bir yanıt verebileceğimi sanmıyorum" diyor. Her şey büyük bir deneyden ibaret ve "belirsiz olan pek çok konu var."

Buna karşılık Mollick'in temel tavsiyesi oldukça net: Yapay zekâ konusunda kendinizi geliştirin. Bunun bir nedeni, onun nihayetinde oldukça geleneksel bir teknoloji iyimseri olması. Riskler bulunduğunu kabul ederken büyük bir potansiyelin de var olduğunu söylüyor ve değişim korkusunun yeni bir şey olmadığını hatırlatıyor. (Platon'un yazının olumsuz etkileri konusunda endişelendiği yönündeki bilindik

örneği yeniden gündeme getiriyor.) Ancak Mollick'in bakış açısına göre yapay zekânın nihai etkisini belirleyecek olan, onu nasıl kullanmayı seçtiğimiz.

Mollick'in temel amaçlarından biri, insanların yapay zekâya ne zaman, nasıl ve hangi ölçüde güveneceklerine karar verebilmeleri için "sağlıklı bir muhakeme yeteneği geliştirmelerine yardımcı olmak." Bunun yolu da kitabın oldukça doğrudan başlıklarından birini ödünç alırsak, "Bir Yapay Zekâ Gibi Düşünmeyi" öğrenmekten geçiyor. Mollick çeşitli ipuçları ve pratik öneriler sunuyor. Örneğin, her hafta kimseden talep gelmeden yapay zekâyla ilgili bir görev deneyin ve bu süreçte neler öğrendiğinize bakın. Seçtiğiniz yapay zekâyla, açıkça onu hata yapmaya ve kontrolden çıkmaya zorlamayı amaçladığınız bir sohbet gerçekleştirin. Bilmediği bir yanıt olduğunda bunu itiraf etmesini isteyin. Taleplerinizi yapay zekânın daha kolay anlayabileceği parçalara bölmeyi öğrenin. Amacınız, yapay zekâyı "bol bol" kullanarak ona ilişkin bir "sezgi geliştirmek" olmalı. (Mollick'in odağı büyük ölçüde büyük dil modelleri olsa da diğer yapay zekâ teknolojilerinin varlığını da kabul ediyor.)

Buradaki temel fikir, yapay zekânın daha verimli kullanılmasını sağlayacak "yönetim becerileri" geliştirmek. Mollick ayrıca insanların, yapay zekânın kuramayacağı bağlantıları kurabilmelerini sağlayan geniş bir bilgi birikimine ve bu bilgiyi aktarabilme becerisine sahip olmalarının önemini vurgulayarak, "Bilgiler yalnızca makinede değil, zihninizde de bulunmalı, çünkü zihninizdeki bilgiler, düşünmenizi sağlayan iskeleyi oluşturur" diye yazıyor.

Bunu söylemek kolay. Ancak elbette aralarında kaygı verici sayıda öğrencinin de bulunduğu pek çok kişi, yapay zekânın muazzam bilgi birikimine erişebilmeyi kendi bilgi dağarcıklarını geliştirmemek için bir gerekçe olarak görüyor. Mollick, bazı şirketlerin de genç çalışanlarında bu düşünsel altyapıyı geliştirmeyi ihmal ediyor olabileceğinden endişe ediyor. Kitabında, yapay zekânın yaygın kullanım alanlarından birinin performans değerlendirmeleri hazırlamak olduğunu yazıyor. Bunun nedeni akıllıca bir tercih olması değil; tam tersine, kişisel geri bildirime kıyasla çok daha az işe yarayan bir yöntem. Asıl neden, yöneticilerin bu görevden hoşlanmaması. Bu da doğru sezgileri geliştirme konusunda yaşanan bir başarısızlık.

Bütün bunlara rağmen Mollick, yapay zekânın geleceği konusunda iyimser görünüyor. Teknolojinin bugüne kadarki verimlilik etkisine ilişkin şüpheler giderek artsa da Mollick, elektriğin ekonomik etkisinin tam anlamıyla ortaya çıkmasının onlarca yıl aldığını hatırlatıyor. Mollick'in kendi verimliliği ise kesinlikle önemli ölçüde artmış durumda. Eğitim araçlarından oyunlara kadar "yüzlerce" program yazmış, her zamankinden daha fazla araştırma yapmış ve elbette iki kitap yayımlamış. Yapay zekânın kendisi adına metin yazmasına izin vermediğini açıkça belirtiyor. Bununla birlikte araştırmalarına yön vermek ve yazarken karşılaştığı gündelik tıkanıklıkları aşmak için yapay zekâdan yararlandığını da saklamıyor.

Yapay zekâ araştırma laboratuvarları yönetmeyen bizlerin, benzer sonuçlara ulaşmak için deneme yanılma yoluyla öğrenmeye ayırabileceği zaman daha kısıtlı olabilir. Ancak belki de Mollick'in deneyiminden yararlanabiliriz. Kitabın bir bölümünde, kişisel bilgilerinin geniş bir bölümünü bir yapay zekâ ajanıyla paylaşıyor ve ona "100 doların altında, beni kesinlikle çok mutlu edecek bir şey satın al" talimatını veriyor. Ajan, kendisine bir gravür kitabı satın alıyor. Mollick bu hediyeyi "gerçekten büyük bir keyif" olarak nitelendiriyor ve bunun karşılığında bazı verilerinin gizliliğinden ödün vermeye değdiği sonucuna varıyor.

Bir açıdan bakıldığında bu, yapay zekânın gücünü gösteren parlak bir örnek: Bizi kendimizi tanıdığımızdan daha iyi tanıyarak ihtiyaçlarımızı verimli biçimde karşılaması. Diğer açıdan ise neredeyse bir parodi. Yapay zekânın uygun fiyatlı konut, sağlık hizmetlerine erişim, kamu eğitimi ve dezenformasyonun yayılması gibi sorunlar karşısında neler yapabileceğini duymak istiyor insan. Kendimizi ödüllendirmek için zaten yeterince fazla aracımız var. Mollick'in bir sohbet robotundan bir bölümü limerick (5 dizelik genellikle mizahi İngiliz şiir türü) biçiminde özetlemesini istemesi gibi bu deney de bütün girişimi Barnumvari bir gösteriye, yani üçtaş oynayan bir tavuğun sergisine dönüştürüyor.

Elbette Mollick, eğitim yerine alışveriş botlarını savunmuyor ve yapay zekânın gerçek sorunların çözümüne yardımcı olacak şekilde yönetilebileceğine açıkça inanıyor. Co-Existence kitabını, teknolojinin gelecekteki potansiyeli ve riskleri üzerine ölçülü değerlendirmelerle bitiriyor. Sonuç olarak bundan sonra yaşanacakların insanların elinde olduğunu söylüyor. Bu da sürece dahil olmak için bir başka neden. (Son dönemde ortaya çıkan ihbarcıların gündeme taşıdığı, yapay zekâ geliştirme çalışmalarının yavaşlatılması tartışmasına doğrudan değinmiyor. Ancak genel yaklaşımından, artık geri dönüşün mümkün olmadığı görüşünde olduğu anlaşılıyor.)

İlk kitabından bu yana yaşanan değişikliklerden biri, yapay zekânın "eğitim" sürecini genişletmenin önündeki bazı potansiyel engellerin aşılmış olması. Mollick'in yazdığına göre 2026 itibarıyla haftalık olarak yapay zekâ kullananların sayısı 1 milyarı aşmış durumda. Bu da onu "tarihte en hızlı benimsenen ürün" haline getiriyor. Eğer bu doğruysa Mollick'in yapay zekâ vizyonu açısından iyi haber sayılır. Çünkü çok daha fazla eğitime ihtiyaç duyan yalnızca modeller değil; bizler de öyle.