

Bloomberg Businessweek

30 Ekim 2026

Yapay Zekâ Eki

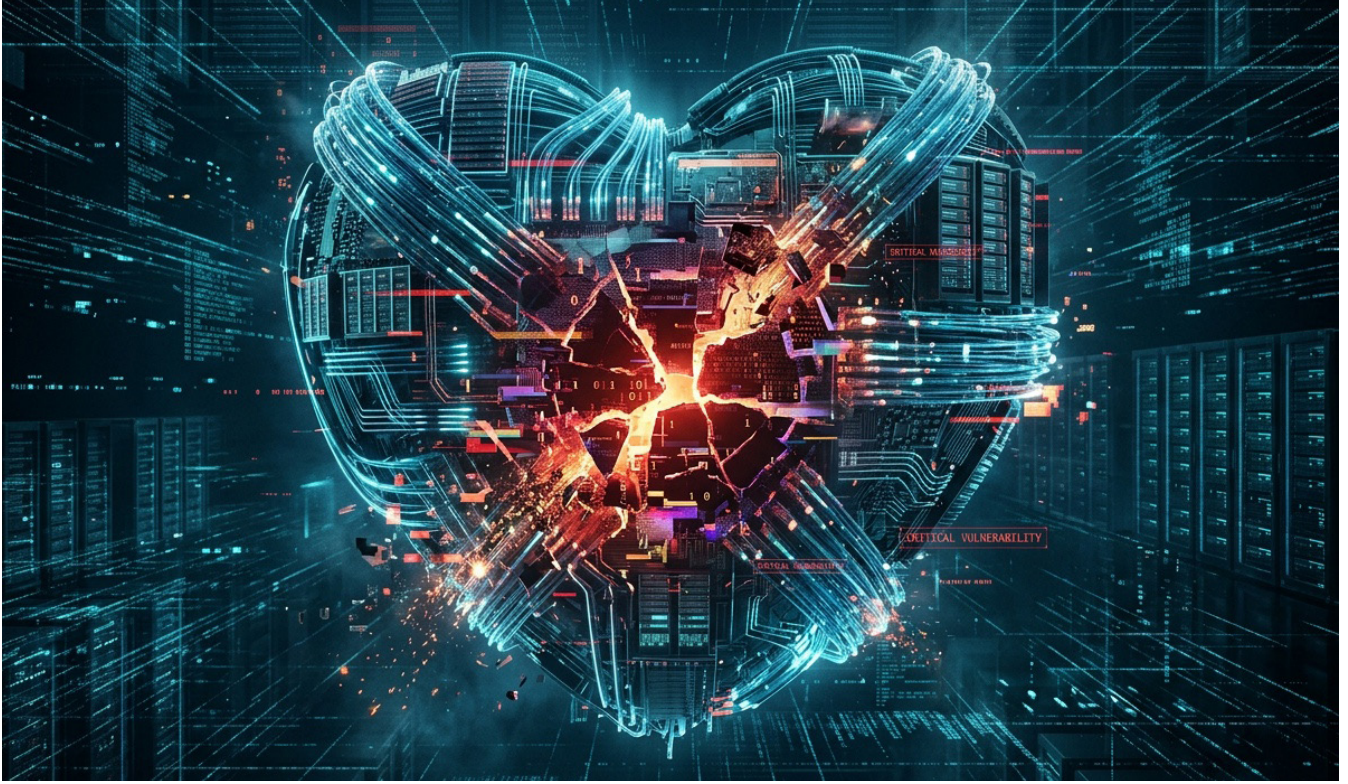


Yapay Zekâ Beden Arıyor

İnternetin Kalbindeki Açık

On yılı aşkın süredir fark edilmeyen kritik güvenlik açığı, yapay zekâ yardımıyla gün yüzüne çıkarıldı. İnternetin büyük bölümünün altyapısında kullanılan PHP'deki açıklar, dünya genelinde alarm yarattı. Yazılım tarihinin en ciddi güvenlik açıkları arasında gösterilen zafiyetlerin ardından siber saldırı girişimleri milyonlara ulaşırken, hükümetler ve şirketler güvenlik açıklarını kapatmak için zamana karşı yarışa girdi.

● Begüm Nur Alkış



Dünyanın dört bir yanında bankalar dijital hizmetlerini durdurdu, havayolu şirketleri uygulamalarını erişime kapattı, hükümetler acil güvenlik uyarılarında bulundu. Tüm bu küresel ölçekteki hareketliliğin başrolünde ise bir programlama dili olan PHP yer alıyor. Google'ın siber güvenlik platform Wiz tarafından paylaşılan bir rapora göre, PHP'deki güvenlik açıkları on yılı aşkın süredir fark edilmeden varlığını sürdürüyordu. Ta ki Ekim ayında araştırmacıların dünya genelindeki internet sitelerinin yüzde 70'inin altyapısında kullanılan programlama diline yönelik iki önemli güvenlik

açığı tespit ettiklerini açıklamalarına kadar...

Güvenlik açıklarını hızla kapatabilmek için hükümetler ve şirketler için adeta zamana karşı bir yarış başlarken, Wiz Research'e göre bu güvenlik açıklarının istismar edilmesi, saldırganların sunucuların kontrolünü ele geçirmesine, hassas verileri çalmasına ve bu sunuculardaki internet sitelerinin içeriklerini izinsiz değiştirmesine imkan tanıyabilir. Ayrıca söz konusu açıklar, saldırganların kimlik doğrulaması yapmadan etkilenen sunucularda kod çalıştırmasına veya işlemlerin belleğindeki hassas verilere

erişmesine olanak tanıyabilir. Wiz Research raporunda uyarıyor: "Üstelik açıklar, PHP üzerinde çalışan uygulamalardan bağımsız olarak doğrudan PHP'nin kendisinde bulunuyor."

PHP bugün WordPress, Wikipedia gibi birçok platformun altyapısında yer alan internetin temel yapı taşlarından biriyken aynı zamanda bu durum, etkilenen tüm internet sitelerini acil bir güvenlik riskiyle karşı karşıya bırakıyor. ABD merkezli siber güvenlik şirketi Palo Alto Networks'ün verilerine göre dünya genelinde internete açık 22 milyondan fazla PHP sistemi

bulunuyor. Palo Alto Networks'te yer alan blog yazısına göre en gelişmiş yapay zekâ modelleri, yazılım kodlarındaki güvenlik açıklarını tespit etme konusunda olağanüstü yeteneklere sahip. Ancak asıl zor olan kısım; güvenlik açıklarına yönelik yamalar yayımlanır yayımlanmaz, saldırganlar bu yamaları tersine mühendislik yöntemleriyle analiz ederek açığın temel nedenini tespit etmesi ve bu açıkları hedef alması.

Siber saldırı girişimleri milyonlara ulaştı

Tehdidin boyutunu büyüten bir diğer unsur ise saldırıların hızı. Şirketler ve hükümetler bir yandan güvenlik yamaları uygulayıp, internet sitelerini geçici olarak erişime kapatırken; bulut hizmetleri şirketi Cloudflare ve Amazon'un verilerine göre siber saldırı girişimlerinin sayısı milyonlara yükseldi. Cloudflare CEO'su Matthew Prince, çarşamba gecesi X platformunda yaptığı paylaşımda, "Güvenlik açıkları kamuoyuna duyurulmadan önceki 10 saat içinde, ağıımız genelinde bu açıklardan yararlanmaya yönelik binlerce girişim tespit ettik" ifadelerini kullandı.

Cloudflare CEO Matthew Prince, 22 Ekim'de X platformunda yaptığı paylaşımında, "Güvenlik açığının kamuoyuna duyurulmasından önceki 10 saat içinde, Cloudflare ağı genelinde bu açıktan yararlanmaya yönelik binlerce saldırı girişimi tespit ettik. Duyurunun ardından geçen yalnızca 45 dakika içinde bu sayı on binlere, 2 saat içinde yüz binlere yükseldi. Şu anda ise saldırı girişimlerinin sayısı milyonlara ulaşmış durumda" ifadelerini kullandı. Microsoft CEO'su Satya Nadella ise Almanya'da düzenlenen bir etkinlikte, "Uzun, çok uzun zamandır böyle bir şey görmedim" dedi ve ekledi: "Bilişim teknolojileri ve siber güvenlik alanında çalışan herkes için uzun bir gün ve uzun bir gece olduğunu biliyorum."

Tüm sistemlere güvenlik yamalarını uygulamak ise oldukça uzun

zaman alabiliyor. Peki, şirketler zamana karşı verilen bu yarışta neler yapmalı? Palo Alto Networks, saldırganların erişebileceği alanların azaltılması gerektiğini, en riskli sistemlere öncelik vererek güncellemeleri uygulamasını ve yapay zekâ altyapılarını güvence altına almasını öneriyor. Ayrıca güvenlik yamaları ve yapay zekâ destekli gerçek zamanlı savunma sistemleriyle saldırılara müdahale süresinin dakikalara indirilmesi gerektiğini vurguluyor. Öte yandan bugün güvenlik açığı taşıyan sistemlerin üçte birinden fazlası güncellenemeyen eski yazılımlarla çalışıyor. Dolayısıyla bazı kuruluşlar için çözüm, yeni bir güvenlik güncellemesini yüklemek kadar basit değil.

9,2 puanlık kritik siber güvenlik açığı

Olası risklerin son derece ciddi olduğunu söyleyen Kaspersky Asya Pasifik (APAC) ile Orta Doğu, Türkiye ve Afrika (META) Bölgeleri Küresel Araştırma ve Analiz Ekibi Başkanı Sergey Lozhkin, "Bugün siber güvenlik dünyasını yakından ilgilendiren kritik bir gelişmeyle karşı karşıyayız. PHP'nin dünya çapında milyonlarca web sunucusunun omurgasını oluşturduğu göz önüne alındığında, bu gelişme 2026 yılının en kritik güvenlik açıklarından biri olmaya aday görünüyor. Zafiyetin ciddiyet derecesi 9,2 (CVSS skoru) olarak belirlendi; bu da durumun ne denli acil ve tehlikeli olduğunu açıkça ortaya koyuyor" diyor.

Bu açığın kötüye kullanılması durumunda, siber saldırıların en tehlikeli türlerinden biri olan uzaktan kod yürütme (Remote CodeExecution - RCE) riskinin doğduğuna dikkat çeken Sergey Lozhkin, "Pratik açıdan bakarsak saldırganlar; etkilenen sistemler üzerinde zararlı kodlar çalıştırabilir, sunuculara 'web shell' yerleştirebilir ve nihayetinde savunmasız sunucuların kontrolünü tamamen ele geçirebilir. Bu ölçekte yaygın olarak kullanılan teknolojiler söz

konusu olduğunda, bu tür vakalar küresel siber tehdit ortamında çok hızlı bir şekilde tırmanışa geçebilir. Dolayısıyla verilecek yanıtın da anlık ve kararlı olması şart. Altyapınızda PHP kullanılıyorsa, yama yayımlanır yayımlanmaz vakit kaybetmeden sistemlerinize uygulamalısınız; zira maruz kalınabilecek riskleri en aza indirmek ve kritik sistemleri güvenceye almak için hızlı aksiyon almak hayati önem taşıyor" paylaşımında bulunuyor.

Aisle Kurucu Ortağı Jaya Baloo ise değerlendirmesinde, "Bir bilgisayar korsanı uzaktan bir web sitesi üzerinde kod çalıştırabilir. Hem hassas veriler çalınabilir hem de sitelerin kontrolü ele alınabilir. Mevcut tahminlerimiz internetteki yüzde 70'lik bir kısmın hassas bir noktada olduğu yönünde, etki alanı çok geniş. Hükümetle ilgili web siteleri de bu durumdan doğrudan etkilenebilir. Bu durum ayrıca küresel ekonomi üzerinde de çok ciddi kırılmalıklar yaratıyor" diyor.

Türkiye'de PHP güvenlik açığına karşı önlem

Küresel çapta siber güvenlik alarmına neden olan PHP güvenlik açıklarının ardından Türkiye'de de harekete geçildi. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı, olası risklerin erken tespit edilmesi ve etkilerinin sınırlandırılması amacıyla ülke genelinde güvenlik taramaları başlattı. Başkanlıktan yapılan açıklamada, başta kamu kurumları olmak üzere ilgili kuruluşlara acil güvenlik bildirimlerinin iletiliği belirtildi. Kamu kurumları, kritik altyapı işletmecileri ve özel sektör kuruluşlarına sistemlerini gözden geçirme ve gerekli güvenlik güncellemelerini gecikmeden uygulamaya çağırısı yapıldı. Açıklamada ayrıca, dijital altyapıların korunması ve kritik hizmetlerin kesintisiz sürdürülmesi amacıyla ulusal düzeyde koordinasyon ve önleyici güvenlik çalışmalarının devam ettiği vurgulandı.

Yapay Zekâ Beden Arıyor

Yapay zekanın geleceği artık yalnızca algoritmalarda değil, robotların ellerinde ve eklemlerinde şekilleniyor. ABD gelişmiş yapay zeka modelleriyle robotların beynini geliştirirken Çin, donanım ve tedarik zincirindeki üstünlüğüyle bedenlerine hayat veriyor.

● Remzi Akkök

Küresel teknoloji rekabetinde yeni bir cephe açılıyor. Son yıllarda yapay zekâ modellerinin geliştirilmesi ve bu alandaki yatırımlarla şekillenen ABD-Çin rekabeti, artık fiziksel dünyaya taşınıyor. İnsansı robotlar, yapay zekânın yalnızca bilgi üreten değil, çevresini algılayan, hareket eden ve fiziksel görevleri yerine getiren sistemlere dönüşmesinin en dikkat çekici örnekleri arasında bulunuyor. Teknoloji şirketlerinin laboratuvarlarında başlayan yarışın sonuçları, önümüzdeki yıllarda fabrikalardan depolara, lojistik merkezlerinden hizmet sektörüne kadar geniş bir alanda hissedilebilir. Robotların üretim süreçlerinde daha fazla görev üstlenmesi, şirketlerin maliyet yapılarını ve yatırım kararlarını değiştirebileceği gibi ülkelerin sanayi rekabetindeki konumlarını da yeniden şekillendirebilir. Bu dönüşümün ekonomik büyüklüğüne ilişkin tahminler ise oldukça iddialı boyutlara ulaştı. Morgan Stanley'nin Mayıs 2025'te yayımladığı araştırmaya

göre, insansı robotların oluştura-acağı küresel pazar, ilgili tedarik zincirleri, bakım ve destek hizmetleriyle birlikte 2050 yılında 5 trilyon doları aşabilir. Banka, aynı dönemde dünya genelinde kullanımda olan insansı robot sayısının 1 milyarı aşabileceğini, bunların yaklaşık yüzde 90'ının endüstriyel ve ticari alanlarda kullanılabileceğini öngörüyor. Ancak bu rakamlar bugünkü pazarın büyüklüğünü değil, teknolojinin önümüzdeki çeyrek yüzyılda ulaşabileceği ölçeğe ilişkin uzun vadeli bir projeksiyonu ortaya koyuyor. Robotların teknik kabiliyetlerinin gelişmesi, üretim maliyetlerinin düşmesi ve şirketlerin yatırımlarından ekonomik karşılık alabilmesi, söz



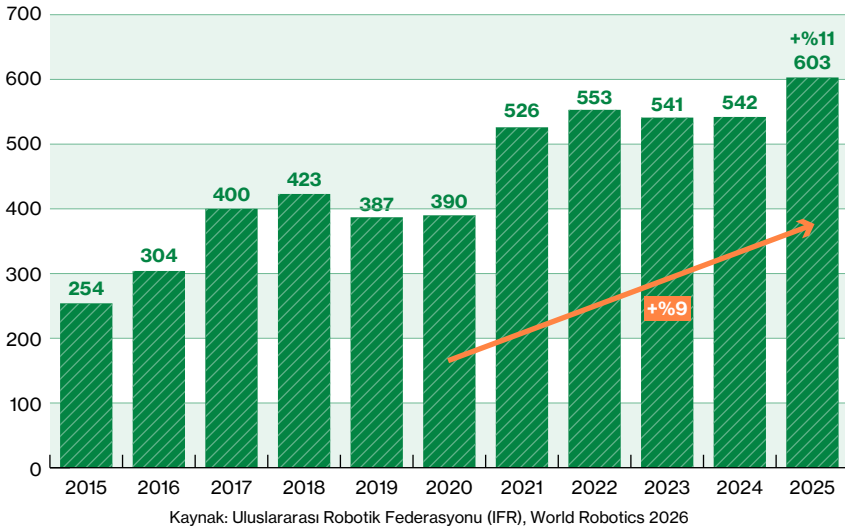
konusu büyümenin gerçekleşmesinde belirleyici olacak.

Robotun Beyninde ABD, Bedeninde Çin Önde

Küresel rekabetin merkezinde iki farklı teknolojik üstünlük bulunuyor. ABD, gelişmiş yapay zekâ modelleri ve robotların karar alma yeteneklerini geliştirmeye yönelik çalışmalarla öne çıkarken Çin, bu sistemlerin fiziksel olarak üretilebilmesini sağlayan donanım ve tedarik zincirlerinde güçlü bir konuma sahip. Pekin merkezli LinkerBot, gelişmiş robotik el teknolojilerinde dikkat çekici bir konuma ulaştı. ABD merkezli araştırma şirketi Smart Analytics Global'in verilerine dayandırılan haberde, şirketin dünya genelinde kullanıma alınmış ileri teknoloji robotik ellerin yüzde 80'inden fazlasını sağladığı belirtiliyor. LinkerBot'un müşterileri arasında Samsung, Meta ve Siemens gibi şirketler bulunuyor. Robotik ellerin geliştirilmesi, insansı robotların önündeki en karmaşık mühendislik sorunlarından biri olarak değerlendiriliyor. Bir robotun yürüebilmesi veya nesneleri taşıyabilmesi kadar, farklı biçimlerdeki parçaları kavrayabilmesi, hassas hareketler gerçekleştirebilmesi ve değişken koşullara uyum sağlayabilmesi de sanayide kullanılabilirliği açısından önem taşıyor. Çin'in avantajı yalnızca robotik ellerle sınırlı değil. Ülke, insansı robotların eklem hareketlerini sağlayan döner aktüatörlerde kullanılan kalıcı mıknatısların yüzde 90'ına kadar olan

ENDÜSTRİYEL ROBOT TALEBİ REKOR SEVİYEYE ÇIKTI

Dünya genelinde yıllık endüstriyel robot kurulumları (Bin Adet)



bölümünde, hassas rulmanların ve sensörlerin yaklaşık yüzde 40'ında, ilgili güç elektroniği bileşenlerinin ise yaklaşık yüzde 30'unda güçlü bir tedarik konumuna sahip. Bu yoğunlaşma, robot üreticileri açısından maliyet ve tedarik güvenliği tartışmalarını da beraberinde getiriyor. Morgan Stanley'in hesaplamasına göre, Tesla'nın geliştirdiği Optimus insansı robotunun üretiminde Çin kaynaklı bileşenlerin kullanılmaması, maliyeti yaklaşık üç katına çıkarabilir. Dolayısıyla robotik yarışın kazananını yalnızca en gelişmiş yapay zekâ modelini geliştiren şirketin belirlemesi beklenmiyor. Donanımı düşük maliyetle üretebilmek, kritik bileşenlere erişebilmek ve üretimi büyük ölçeğe taşıyabilmek de en az yazılım kadar önemli hale geliyor.

Fabrikalarda Robotlaşma Hızlanıyor

İnsansı robotların sanayiye etkisini anlamak için mevcut otomasyon düzeyine de bakmak gerekiyor. Uluslararası Robotik Federasyonu'nun (IFR) Eylül 2026'da yayımladığı World Robotics 2026 raporuna göre, dünya genelinde fabrikalarda çalışan endüstriyel robotların sayısı 2025 yılında yüzde 9 artarak 5 milyona ulaştı. Aynı yıl 600 binden fazla yeni

endüstriyel robot kurulumu gerçekleştirildi. Küresel robot yatırımlarının ağırlık merkezi ise Asya olmaya devam ediyor. IFR verilerine göre Çin'de 2025 yılında yaklaşık 354 bin yeni endüstriyel robot kuruldu. Bu rakam, dünya genelindeki yeni kurulumların yüzde 59'una karşılık geliyor. Çinli üreticilerin kendi iç pazarlarındaki payı da yüzde 55 düzeyinde gerçekleşti. Bu veriler, Çin'in yalnızca robot üreten değil, aynı zamanda robotları sanayi üretiminde yoğun biçimde kullanan bir ekonomi olduğunu gösteriyor. Üretim ölçeği, tedarik zinciri derinliği ve iç pazardaki talep, ülkenin robotik teknolojilerdeki gelişimini birbirini besleyen bir yapıya dönüştürüyor. Bununla birlikte geleneksel endüstriyel robotlarla insansı robotlar arasında önemli bir fark bulunuyor. Otomotiv fabrikalarında kaynak, boya ve montaj gibi belirli işlemleri yüksek hız ve hassasiyetle gerçekleştiren endüstriyel robotlar uzun yıllardır kullanılıyor. İnsansı robotların hedefi ise insanların çalışması için tasarlanmış ortamlarda daha çeşitli görevleri üstlenebilmek. Bu nedenle insansı robotların ilk aşamada mevcut endüstriyel robotların tamamının yerini alması yerine, otomasyonun zor veya ekonomik açıdan verimsiz olduğu görevlerde

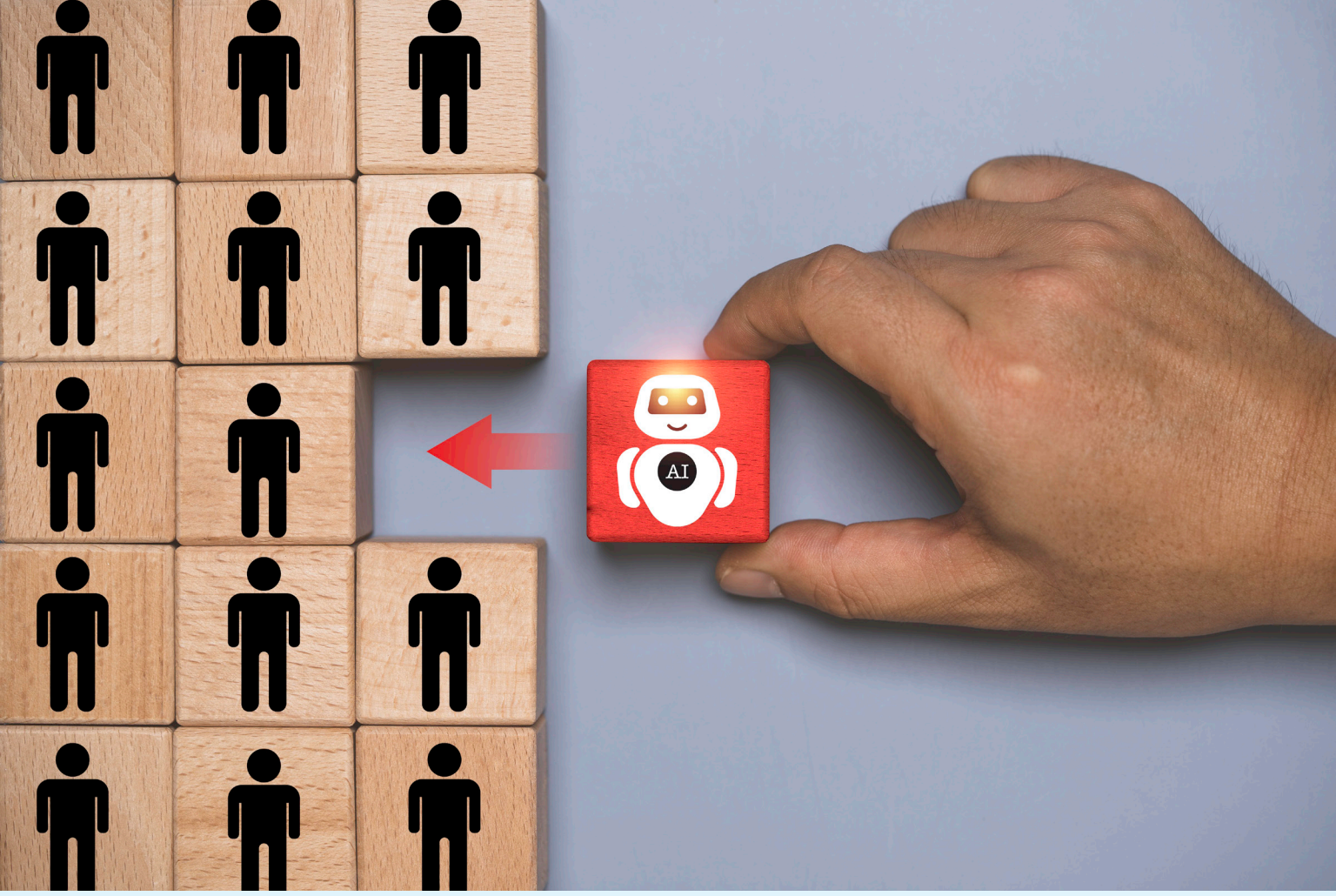
tamamlayıcı bir rol üstlenmesi daha olası görünüyor.

İnsansı Robotlarda Ticari Kullanım Henüz Başlangıç Aşamasında

İnsansı robotlara yönelik beklentiler hızla yükselse de bugünkü ticari ölçek, geleneksel endüstriyel robot pazarının oldukça gerisinde bulunuyor. Reuters'ın Eylül 2026'da IFR tahminlerine dayandırdığı habere göre, 2025 yılında dünya genelinde endüstriyel ve profesyonel hizmet uygulamaları için yaklaşık 7 bin insansı robot satıldı. Bu robotların önemli bir bölümü doğrudan üretim yapmak yerine araştırma, test ve yapay zekâ modelleri için veri toplama amacıyla kullanıldı. Otomotiv üreticileri ilk uygulamaları deneyen şirketler arasında yer alsa da fabrikalardaki denemeler henüz sınırlı sayıda robotla yürütülüyor. Bu tablo, insansı robotların potansiyeli ile bugünkü ekonomik katkısı arasında önemli bir mesafe bulunduğu işaret ediyor. Robotların sanayide yaygınlaşabilmesi için yalnızca satın alma fiyatlarının düşmesi yeterli olmayacak. Çalışma süreleri, hata oranları, bakım maliyetleri, enerji tüketimleri ve insan müdahalesi olmadan görevlerini sürdürebilme kabiliyetleri de yatırım kararlarında belirleyici olacak. Morgan Stanley'nin tahminlerine göre yüksek gelirli ülkelerde bir insansı robotun maliyeti 2024 yılında yaklaşık 200 bin dolar düzeyindeydi. Banka, teknolojik gelişmeler ve üretim ölçeğinin büyümesiyle bu maliyetin 2028'de yaklaşık 150 bin dolara, 2050'de ise 50 bin dolara gerileyebileceğini öngörüyor. Daha düşük maliyetli Çin tedarik zincirlerinden yararlanan pazarlarda ise 2050 yılında 15 bin dolar seviyesine kadar düşüş mümkün görülüyor.

Atlı: Robotları Üretip Sahaya Süren, Sahadan Veriyi Toplayacak

ABD ile Çin arasındaki teknoloji rekabetinin insansı robotlarla birlikte



yeni bir aşamaya geçtiğini belirten Atılı Global Direktörü Dr. Altay Atılı, Çin'in robotik donanım ve tedarik zincirlerindeki üstünlüğünün yapay zekâ alanındaki rekabeti de etkileyebileceğini söyledi. ABD'nin gelişmiş yapay zekâ modellerinde önde olduğunu ancak robotların düşük maliyetle ve büyük ölçekte üretilebilmesi açısından Çin'in önemli bir avantaja sahip bulunduğunu vurgulayan Atılı, bu üstünlüğün arkasında ülkenin güçlü sanayi altyapısının yer aldığını ifade etti.

Motorlardan sensörlere, bataryalardan hassas aktüatörlere kadar insansı robotlarda kullanılan birçok bileşenin Çin'in mevcut üretim ekosistemiyle örtüştüğüne dikkat çeken Atılı, elektrikli araç sektörünün bu alandaki gelişime önemli katkı sağladığını belirtti. Çin'in nadir toprak elementleri ve müknaş tedarikindeki güçlü konumunun da robotik üretimdeki avantajını pekiştirdiğini söyleyen Atılı, bazı Çinli üreticilerde

kritik parçaların yüzde 90'ından fazlasının yerli tedarikçilerden sağlandığını aktardı. Çin'in donanım üstünlüğünün uzun vadede yazılım alanındaki rekabeti de değiştirebileceğini ifade eden Atılı, "Bence stratejik açıdan asıl önemli nokta veri. Robotları büyük ölçekte üretilip sahaya süren, sahadan veriyi de toplayacak. Fiziksel yapay zekâ da en çok bu veriyle gelişiyor. Yani Çin'in bugünkü donanım avantajı, yarın yazılım tarafındaki açığı kapatmasına yardımcı olabilir" değerlendirmesinde bulundu.

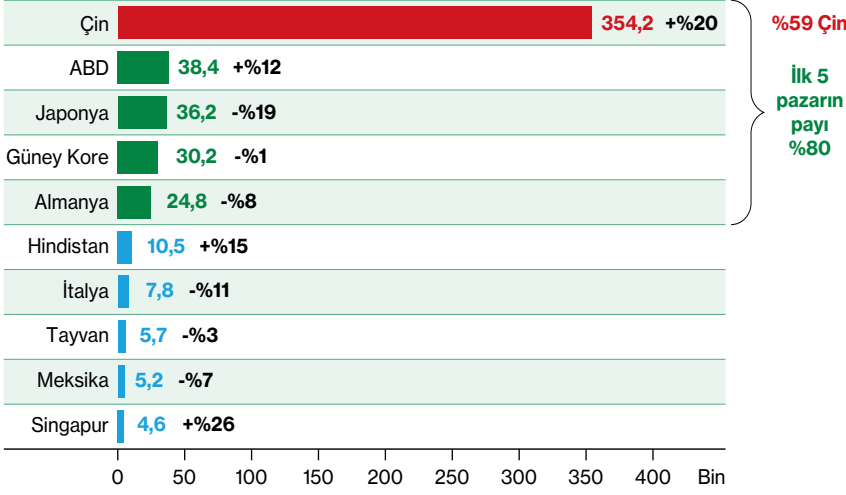
"Çin Robotikte Elektrikli Araçlara Benzer Bir Başarı Yakalayabilir"

Çin'in robotik teknolojilerdeki yükselişinin on yılı aşan sanayi politikalarının sonucu olduğunu belirten Atılı, 2015 yılında açıklanan "Made in China 2025" stratejisinin robotiği öncelikli sektörler arasına aldığını hatırlattı. Sonraki sanayi

planlarında ise insansı robotlar ve bedenlenmiş yapay zekânın doğru hedef haline geldiğini söyledi. Devletin sektörde yalnızca finansman sağlayıcı değil, aynı zamanda talep oluşturucu bir rol üstlendiğini vurgulayan Atılı, kamu kurumlarının yeni teknolojilerin ilk alıcısı olmasının ticarileşmeyi hızlandırdığını ifade etti. Çin'in elektrikli araç sektöründe izlediği modelin robotikte de tekrarlandığını belirten Atılı, devlet destekleriyle başlayan sürecin yoğun şirket rekabeti, düşen maliyetler ve pazarın belirli üreticiler etrafında yoğunlaşmasıyla devam ettiğini söyledi. Bununla birlikte iki sektör arasında önemli farklılıklar bulunduğuna dikkat çekti. Atılı, "Elektrikli araçlarda ürün belliydi. Otomobilin ne yapacağını biliyorduk, mesele onu daha ucuza ve daha iyi üretmekti. İnsansı robotun hangi işte gerçekten verimli olacağı ise hâlâ tartışmalı ve çözülmemiş sorunların çoğu yazılım tarafında" dedi. Robotik teknolojilerde

YENİ ENDÜSTRİYEL ROBOT KURULUMLARINDA EN BÜYÜK 10 PAZAR

2025 Yılında Ülkelere Göre Yıllık Endüstriyel Robot Kurulumları (Bin Adet)



güvenlik ve veri yönetimine ilişkin kaygıların uluslararası pazarlara erişimi zorlaştırabileceğini de belirten Atlı, Çin'in donanım alanında elektrikli araç sektöründekine benzer bir başarı yakalamasını beklediğini ancak küresel pazarda aynı ölçüde hâkimiyet kurmasının daha güç olacağını ifade etti.

“Çin 10 Binden Fazla İnsansı Robotu Sahaya Sürmeyi Hedefliyor”

Çin'in insansı robotları sanayi üretimine dahil etme yaklaşımının erken uygulama ve sahadan öğrenme üzerine kurulduğunu belirten Atlı, şirketlerin teknolojinin tamamen olgunlaşmasını beklemek yerine mevcut robotları üretim süreçlerinde deneyerek geliştirmeyi tercih ettiğini söyledi. Atlı'nın aktardığına göre Çin hükümeti, 2026 sonuna kadar 100'den fazla yüksek değerli uygulama senaryosu oluşturmayı ve 10 binden fazla insansı robotu sahaya sürmeyi hedefliyor. Şanghay yönetiminin ise 2030 yılına kadar fabrikalarda 100 bin insansı robot kullanılması yönünde hedef açıkladığını belirtti. Robotlaşmanın arkasında yalnızca teknolojik rekabetin değil, demografik dönüşümün

de bulunduğunu ifade eden Atlı, Çin'de çalışma çağındaki nüfusun azalması, ücretlerin yükselmesi ve gençlerin fabrika işlerine yönelik ilgisinin gerilemesinin otomasyonu stratejik bir zorunluluğa dönüştürdüğünü söyledi. Önümüzdeki 5-10 yılda Çin fabrikalarında insansı robot kullanımının belirgin biçimde artmasını beklediğini belirten Atlı, ilk uygulamaların malzeme taşıma, depolama, lojistik ve kalite kontrol gibi görece düzenli görevlerde yoğunlaşacağını öngördü.

Atlı, “Mevcut endüstriyel robot kollarının yerini almayacaklar, onların yanında çalışacaklar. Maliyet düştükçe ve yazılım olgunlaştıkça, on yıl içinde esnek üretim gerektiren alanlarda ciddi bir pay alacaklarını tahmin ediyorum” ifadelerini kullandı.

“Türkiye yalnızca montaj üssü olarak kalmamalı”

Küresel robotik tedarik zincirindeki dönüşümün Türkiye açısından hem fırsatlar hem de yeni bağımlılık riskleri oluşturduğunu belirten Atlı, otomotiv, beyaz eşya, makine ve metal işleme sektörlerindeki üretim birikiminin robotik teknolojilere yönelik yatırımlar için avantaj

sağlayabileceğini söyledi. Batılı ülkelerde korumacılığın artmasıyla Çinli robot üreticilerinin Avrupa pazarına yakın üretim ve montaj merkezleri arayabileceğini ifade eden Atlı, Türkiye'nin bu yatırımları çekerek robotik bileşen üretimi ve sistem entegrasyonu alanlarında konumlanabileceğini belirtti. Ancak hazır robot ithalatına dayalı bir modelin teknolojik bağımlılığı artırabileceği uyarısında bulunan Atlı, yazılım, veri ve kritik bileşenlerde tek bir tedarik kaynağına bağlı kalmanın ekonomik ve güvenlik açısından riskler taşıdığını vurguladı. Türkiye'nin Çin'le yatırım, ortak üretim ve teknoloji transferi alanlarında iş birliği geliştirirken Avrupa, Japonya ve Güney Kore ile mevcut ilişkilerini de sürdürmesi gerektiğini ifade eden Atlı, “Robotikte de hedef montaj noktası olmak değil, değer zincirinde kendi yeri olan bir oyuncu olmak olmalı” dedi.

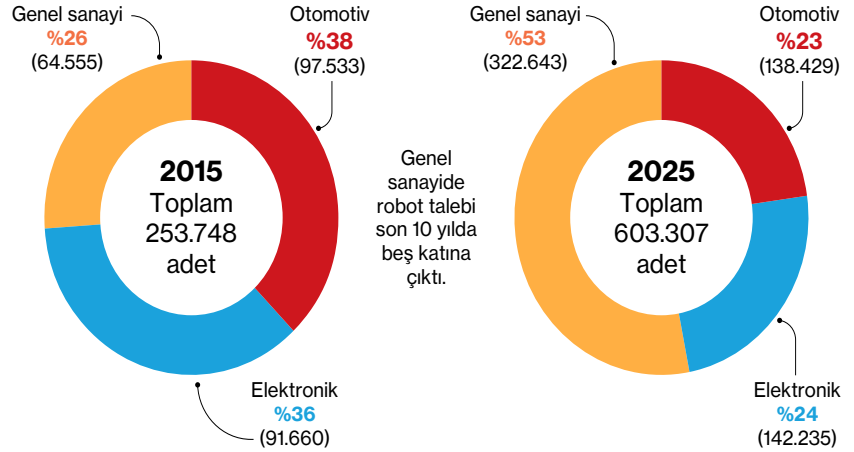
Şenkardeş: Robotik yarışta kazanan, teknolojiyi ekonomik değere dönüştüren olacak

ABD ile Çin arasında insansı robotlar ve fiziksel yapay zekâ alanında hızlanan rekabet, küresel teknoloji yatırımlarının yönünü de değiştiriyor. İstanbul Bilgi Üniversitesi Öğretim Üyesi ve Teknolojide Girişimcilik ve İnovasyon Anabilim Dalı Başkanı Dr. Çağla Gül Şenkardeş, robotik teknolojilerde rekabet avantajının yalnızca yazılım veya donanım üstünlüğüyle sağlanamayacağını, bu iki alanı üretim kapasitesiyle birleştiren ekosistemlerin öne çıkacağını söyledi. Yapay zekâ modelleri, robotik donanım ve üretim kapasitesinin birbirinden bağımsız değerlendirilemeyeceğini vurgulayan Şenkardeş, yatırımcıların özellikle teknolojinin ekonomik değere dönüştüğü alanlara odaklandığını belirtti. Crunchbase'in Ekim ayına ilişkin küresel girişim sermayesi yatırımları analizlerine dikkat çeken Şenkardeş, ABD ve Çin'de robotik teknolojiler üzerine

çalışan girişimlere yönelen yatırımların birbirine yakın büyüklüklerde olduğunu ifade etti. Önümüzdeki dönemde rekabetin belirleyici unsurlarından birinin şirketlerin ölçeklenme kapasitesi olacağını söyleyen Şenkardeş, “Yapay zekâ modeli, donanımı ve üretim kapasitesini dinamik bir şekilde bir arada kurabilen ve güçlendiren tarafta olacaktır rekabet avantajı” değerlendirmesinde bulundu. ABD ve Çin’in yanı sıra Japonya ve Güney Kore’nin de yakından izlenmesi gerektiğini belirten Şenkardeş, özellikle hassas mühendislik ve robotik bileşenlerde bu ülkelerin önemli potansiyele sahip olduğuna dikkat çekti. İnsansı robotlara yönelik yatırım ilgisinin artmasını yapay zekânın dijital dünyadan fiziksel dünyaya geçişiyle ilişkilendiren Şenkardeş, “Yapay zekâ kafesten çıkıyor” ifadesini kullandı. Büyük dil modellerinin ilk aşamada dijital süreçleri dönüştürdüğünü, insansı robotların ise mevcut fiziksel altyapıyı köklü biçimde değiştirmeden yeni bir otomasyon dalgası yaratma potansiyeli taşıdığını belirten Şenkardeş, bu dönüşümün yazılım alanındaki gelişmelerden daha uzun ve maliyetli bir süreç olacağını söyledi. Dijital ortamda yapay zekâ modellerinin eğitimi için büyük miktarda veriye erişilebildiğini, fiziksel dünyada ise robotların hareket ve davranışlarını geliştirmek için gereken verilerin toplanmasının daha güç olduğunu ifade eden Şenkardeş, bu durumun teknolojinin ticarileşme süresini uzatabileceğine dikkat çekti. Robotik yatırımlarının 2025 yılından itibaren girişim sermayesi piyasasında giderek daha fazla pay almaya başladığını belirten Şenkardeş, sektörün yakın gelecekte girişim sermayesi yatırım fonlarının öncelikli alanlarından biri olmasını beklediğini söyledi. Bununla birlikte yatırım kararlarında robotların insan biçimine ne kadar benzediğinden çok, ekonomik faydalarının belirleyici olacağını vurgulayan Şenkardeş, “Girişim sermayesi açısından belirleyici olan,

ROBOTİKTE AĞIRLIK MERKEZİ OTOMOTİVDEN GENEL SANAYİYE KAYDI

Dünya genelinde sektörlere göre endüstriyel robot kurulumları (Adet ve Yüzde Pay)



Kaynak: Uluslararası Robotik Federasyonu (IFR), World Robotics 2026

robotun ne kadar insansı olduğu olmayacak elbette, hangi ekonomik problemi, ne kadar düşük maliyetle ve ne ölçekte çözebildiği olacak” dedi. Teknik belirsizliklerin yanı sıra düzenleyici çerçevenin henüz olgunlaşmamış olmasının da sektör açısından önemli bir risk oluşturduğunu belirten Şenkardeş, robotik teknolojilere ilişkin küresel standartların oluşmasının zaman alacağını ifade etti.

“Türkiye’nin mutlaka insansı robot üreticisi olması gerekiyor”

Türkiye’nin robotik teknolojilerdeki yatırım potansiyelini değerlendiren Şenkardeş, otomotiv, savunma sanayisi, endüstriyel otomasyon ve mühendislik alanlarındaki birikimin önemli avantajlar sağladığını belirtti. Avrupa pazarına coğrafi yakınlığın da Türkiye’nin küresel robotik değer zincirine entegrasyonu açısından fırsat oluşturduğunu söyledi. Türkiye’deki robotik girişimcilik ekosisteminin henüz erken aşamada olduğunu ancak yatırım almış büyük projelerin de bulunduğunu ifade eden Şenkardeş, uzun vadeli derin teknoloji finansmanı, üniversite-sanayi iş birliklerinin ticarileştirilmesi ve uluslararası sermayeye erişim alanlarında gelişime

ihtiyaç duyulduğuna dikkat çekti. Türkiye’nin küresel rekabette mutlaka nihai insansı robot üreticisi olarak konumlanmasının gerektiğini vurgulayan Şenkardeş, robotik yazılımlar, sensör teknolojileri, otonom sistemler ve endüstriyel yapay zekâ uygulamalarında uzmanlaşmanın da güçlü bir strateji olabileceğini belirtti. Şenkardeş, “Türkiye’nin küresel rekabette mutlaka insansı robot üreticisi olması gerekiyor. Robotik yazılımlar, sensör teknolojileri, otonom sistemler ve endüstriyel yapay zekâ uygulamalarında uzmanlaşarak küresel değer zincirinde güçlü bir konum elde etmeyi hedeflemek de alternatif ama gerçekçi ve iyi bir strateji olabilir” ifadelerini kullandı. Türkiye’deki girişimlerin uluslararası rekabette kalıcı bir yer edinebilmesi için teknolojik yetkinliğin tek başına yeterli olmayacağını belirten Şenkardeş, temel meselenin geliştirilen teknolojilerin ticari karşılık bulması olduğunu vurguladı. Şenkardeş, “Burada kritik mesele, teknolojiyi geliştirmek kadar onu ölçeklenebilir ve uluslararası yatırımcı için cazip bir iş modeline dönüştürebilmek” değerlendirmesinde bulundu.

Meta ve OpenAI, İlk Kullanıcıları Kendilerine Çekmek İçin Sevimli Yapay Zekâ Ajanlarına Sarılıyor

İki şirket şu anda farklı müşteri gruplarına odaklansa da izledikleri yolların zamanla kesişmesi muhtemel.

● Riley Griffin

Meta Platforms Inc. ve OpenAI, Eylül ayında yeni yapay zekâ ajanlarını piyasaya sürdüklerinde bu yardımcı botların dikkat çekici bir ortak noktası vardı: Her birinin kendine özgü, çocuksu ve biraz da gösterişli bir maskotu bulunuyordu. Meta'nın Muse'u, pembe yanaklı, tüylü, yetiyi andıran Jolly adlı bir yaratığa sahip. OpenAI'nin Dots'u ise bereler ve papyonlar takmış, sarılıp sarmalanacakmış gibi görünen bir grup şekilden oluşuyor.

Kullanıcıları adına çevrimiçi görevleri yerine getiren otomatik kişisel asistanlar olan bu yapay zekâ ajanları, kendileriyle paylaşılan veriler ölçüsünde işe yarıyor. E-posta kutusuna, takvime ve kredi kartı hesabına erişimi



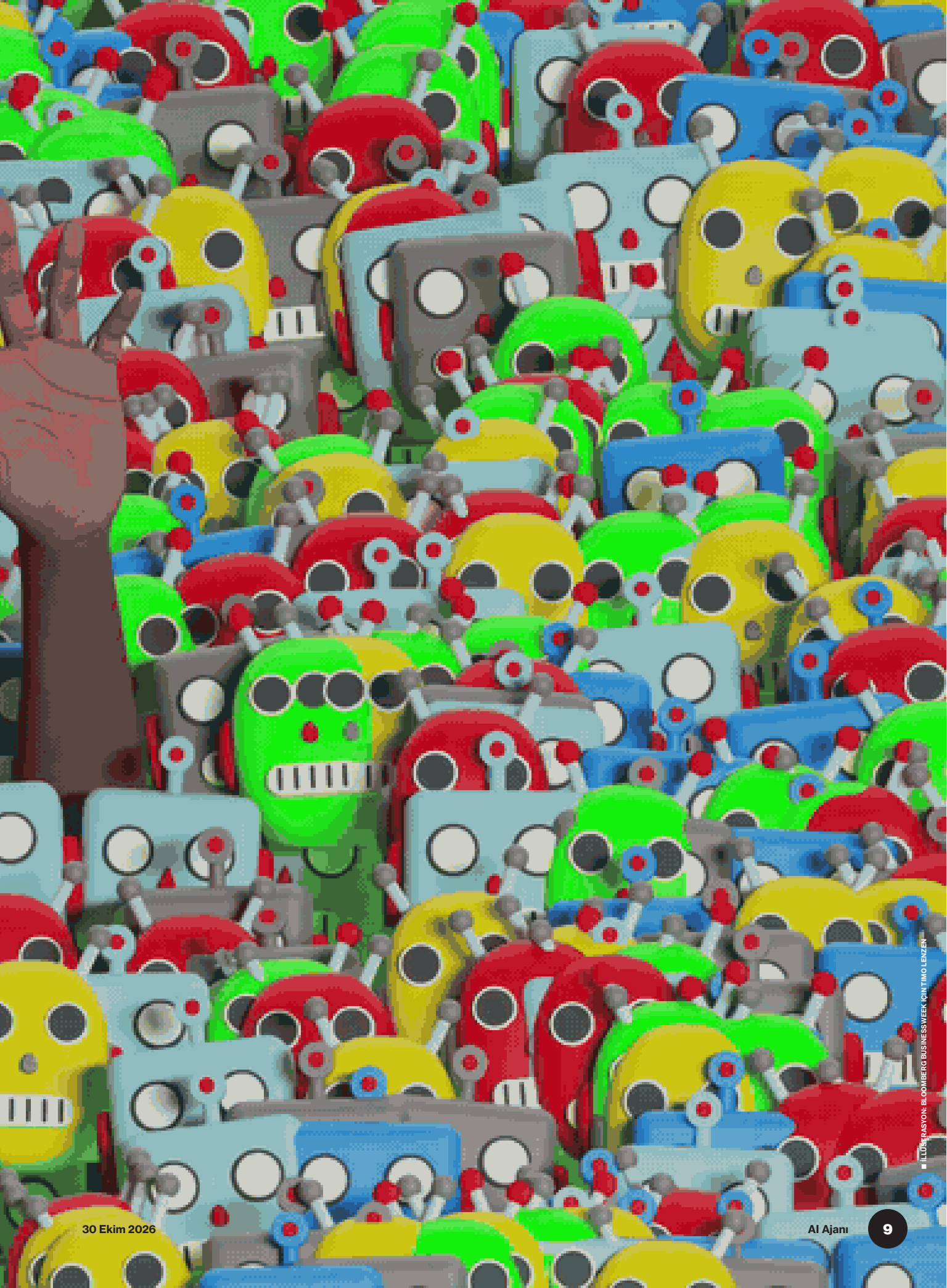


ILLUSTRATION: BLOOMBERG BUSINESS WEEK ON TINO LENZEN



Eylül ayında California'nın Oakland kentinde Meta'nın Muse yapay zekâ ajanı için hazırlanan bir reklam. Fotoğraf: Smith Collection/Gado/Getty Images

olan bir ajan, bu tür izinlere sahip olmayan bir ajanın sunamayacağı ölçüde fayda sağlayabilir. Maskotların, ürünlerin sunduğu kolaylık karşılığında kişisel verileri paylaşma fikrinin yarattığı tüketici kaygılarını hafifletmek üzere tasarlandığı açık. Ancak tüketicileri buna ikna etmek zor olabilir. Meta'nın gizlilik konusunda tartışmalı ve uzun bir hata geçmişi var. Pew Research Center'in araştırmasına göre ABD'deki yetişkinlerin her 10 kişiden 7'si, yapay zekânın daha yaygın kullanılmasının kişisel bilgilerini daha az güvenli hale getireceğini düşünüyor.

Yapay zekâ alanında sıkça görüldüğü üzere, şirketlerin nereye gittiklerinden tam olarak emin olmadan ileri atıldıkları izlenimi var. Bu yıl, ilk kullanıcılar market alışverişi sipariş etmek veya partiler organize etmek için kısa mesajla çağrılabilen Instinct adlı bir ajanı kullanmaya başlayınca rekabet daha da kızıştı. Kullanıcılar, ajanın yeteneklerini övgüyle anlatmaya başladı; ancak kişisel bilgileri üzerindeki kontrolün ne kadarını ona devrettiklerini fark ettiklerinde zaman zaman tedirgin de oldular. (Eylül ayında girişim sermayedarları, Instinct'in arkasındaki

girişime 10 milyar dolar değer biçti.) Üstelik Gmail ve Google Takvim gibi hizmetlerden gelen geniş erişim ağına ve çok miktarda ilgili veriye sahip Alphabet Inc. gibi rakiplerin oluşturduğu tehdit de giderek büyüyor.

Rakipler arasındaki farklılıklar şimdiden belirginleşiyor. OpenAI, Dots'un iş amaçlı nasıl kullanılabileceği konusunda çok şey söylerken Meta'nın Yapay Zekâdan Sorumlu Üst Yöneticisi Alexandr Wang, Muse'un "en başından beri tüketicilere yönelik amiral gemisi ürünümüz olarak tasarlandığını" söylüyor. Wang'a göre ajan, öncelikle mobilya alışverişi yapmak, akşam yemeği rezervasyonu ayarlamak ve okul formlarını doldurmak gibi "kişisel kullanım senaryolarını karşılamak" üzere geliştirildi.

Meta'nın sosyal medya ürünleri gibi Muse'un temel hizmeti de ücretsiz ve nihayetinde milyarlarca kullanıcıya ulaşmayı hedefliyor. Pazar istihbaratı şirketi Sensor Tower'ın verilerine göre uygulama, bir ay içinde ABD'de 7 milyon indirmeyi aştı. Meta'nın yeni bir hit yakaladığına ilişkin beklentiler, ajanın tanıtılmasından bu yana şirketin his-selerini yüzde 20'den fazla yükseltti.

Wang, "Dünyada tüketici ürünlerini büyütme konusunda Meta'dan daha iyi bir şirket yok" diyor. (Muse'un piyasaya sürülmesi, banka ve seyahat acentesi hisselerini olumsuz etkiledi. Bunun nedeni, ajanların kullanıcıların daha düşük faiz oranları için alışveriş yapmasına ve kendi seyahat rezervasyonlarını düzenlemesine yardımcı olarak bu şirketlerin işlerini daraltabilecek olması.)

Ürünün mühendislik çalışmalarını yöneten David Singleton'a göre Meta, Muse'dan para kazanmak için çeşitli olasılıkları değerlendiriyor. Ürünü yoğun kullananlar, aylık 20 dolarlık ya da daha yüksek kullanım limitleri sunan 100 dolarlık abonelik seçeneklerinden yararlanabiliyor. Şirket, ilerleyen dönemde ajanın aracılık ettiği işlemlerden komisyon almayı da hedefliyor. Singleton, Muse'un şu anda Meta'nın reklam sistemiyle veri paylaşmadığını belirterek, "Ancak elbette, anlamlı olabilecek tüm iş modellerini her zaman araştıracağız" diyor. Meta pazartesi günü, şirketin OpenAI ve Anthropic'in en gelişmiş modelleriyle rekabet edebilecek düzeyde olduğunu söylediği ve uzun süredir beklenen bir yapay zekâ

modelini piyasaya sürdü. Bu model, yakında Muse uygulamasının abonelik sürümüne güç verecek.

OpenAI ise ajanı için başlangıçta daha yavaş büyümesini neredeyse garanti eden bir yol seçti. Şirket, Dots'u 29 Eylül'de tanıttığında uygulamayı yalnızca aylık en az 100 dolar ödeyen mevcut müşterilerine açtı. Dots, kod yazmak ve araştırma üretmek gibi işlerde OpenAI ürünlerine zaten güvenen kullanıcılara hizmet vermek üzere tasarlandı.

OpenAI Üst Yöneticisi Sam Altman, rakibi Muse'un adını anmadan onun benimsediği yaklaşımı küçümseyen açıklamalarda bulundu. Altman, OpenAI'nin geliştirici konferansında, "Bir rezervasyon yapmanıza veya uçak bileti satın almanıza yardımcı olan sanal asistanlarda bunun nasıl görünebileceğine ilişkin ilk işaretleri görmüş olabilirsiniz. Bu tür işleri devretmek kullanışlı, ancak teknolojinin yapabilecekleriyle kıyaslandığında bunlar önemsiz kalıyor. Çok daha iddialı olmak istedik" ifadelerini kullandı.

Citizens Bank analisti Andrew Boone, bu ajanların başlangıçta nasıl konumlandırıldığını yalnızca şirketlerin hedeflediği müşteri türünün belirlemiyor olabileceğini söylüyor. Meta, OpenAI henüz ortada yokken bile veri merkezi altyapısını genişletmeye başlamıştı. Ayrıca şirketin kazançlı reklam işi, ücretsiz bir ürün için pahalı bilgi işlem kapasitesine agresif biçimde yatırım yapma ve bunun karşılığında hemen finansal getiri beklememe konusunda ona daha fazla hareket alanı sağlıyor.

Buna karşılık OpenAI, şimdiden 1 milyardan fazla ChatGPT kullanıcısına hizmet veriyor olsa da altyapısını genişletmeye ancak son yıllarda başladı. Şirket, yakın gelecekte bir noktada halka açılmaya hazırlanırken milyarlarca doları hızla tüketiyor. Boone'a göre Dots gibi yoğun bilgi işlem gücü gerektiren bir ajanı ücretsiz sunmayı haklı çıkarmak zor olurdu.

Bununla birlikte Meta ve OpenAI'nin izlediği yollar zamanla kesişebilir. Meta, Muse'u şimdiden küçük işletmelere pazarlıyor; OpenAI ise Dots'un düğün



Altman, 29 Eylül'de San Francisco'da düzenlenen OpenAI geliştirici konferansında açılış konuşmasını yaparken. Fotoğraf: Heather Diehl/Getty Images

planlamak gibi işler için de yararlı olduğunu savunuyor. Altman da OpenAI konferansında, "Elbette bir gün milyarlarca insana ulaşacak, kitlesel pazara yönelik bir ürün sunmamızı beklemelisiniz" dedi.

Boston Consulting Group'un Kuzey Amerika dijital büyüme birimini yöneten Rob Derow, pazarı değerlendirirken kısa vadede en büyük gelir artışının kurumsal uygulamalardan geleceğini düşündüğünü söylüyor. Ancak uzun vadede, "Tüketici kullanım senaryoları konusunda her zaman daha iyimser oldum" diye ekliyor.

Derow'a göre geniş çaplı benimsemeye ulaşmanın yolu, "tüketiciyle güven ilişkisi kurmaktan ve bu güveni nasıl kazanacağınızdan" geçiyor. Gartner'ın araştırmasına göre ABD'li tüketicilerin yalnızca onda biri, ucuz

ev ihtiyaçlarını satın alma kararlarını yapay zekâya bırakmaya hazır. McKinsey & Co.'nun araştırması ise tüketicilerin yarısının market alışverişi için yapay zekâ destekli ürün aramalarını denemeye istekli olduğunu, ancak yalnızca yüzde 20'sinin kendi incelemeleri olmadan tamamen otomatik sipariş vermeyi deneyeceğini ortaya koyuyor.

Üstelik kamuoyunun dikkatini çeken tek bir büyük hata bile bütün sektörü geriye götürebilir. Derow, "Bir sonraki veri ihlali, sorun ya da kontrol dışı satın alma, güveni koparacak ve büyümeyi yavaşlatacak" diyor. Yakın gelecekte böyle bir olay yaşanırsa şirketlerin işleri rayında tutabilmek için sevimli maskotlardan daha fazlasına ihtiyacı olabilir.

Sıcak Başlangıç

ABD'de piyasaya sürüldükten sonraki ilk 30 gün içinde her bir yapay zeka uygulamasının indirilme sayıları.



Not: İndirme rakamları, iPhone ve iPad için Apple App Store ve Google Play'den yapılan toplam ABD indirmelerinin tahmini değerleridir. Sensor Tower'a göre, dört uygulamadan yalnızca Muse, ilk 30 gün boyunca Google Play'de herkese açık olarak mevcuttu.

Kaynak: Sensor Tower

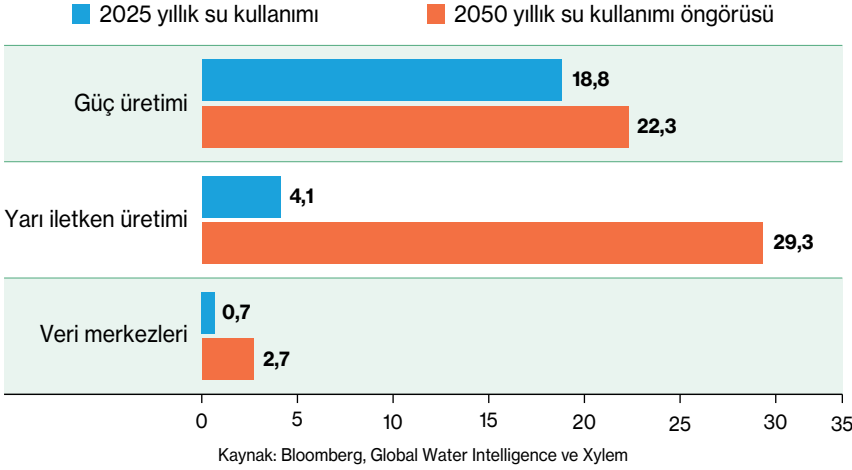
Yapay Zekâ Rekabetini Soğutmaya Su Yetmiyor

Eriyen silikonlar, dikey sıçrayan enerji ihtiyacı ve aşırı ısınan rekabet. Yapay zekâ yarışında fiziki sınırların algoritmaların önüne geçmesi, teknoloji şirketlerinin çözmesi gereken en sıcak denklem.

● Kerem Gündüz



YAPAY ZEKA SU TALEBİ (Trilyon litre)



Yapay zekâ yarışında küresel rekabetin temeli, uzun süre boyunca bilişim gücü ve devasa veri setleri üzerinden tanımlandı. Ancak üretken yapay zekâ modelleri büyüdükçe ve işlem gücü ihtiyacı sürekli artan bir ivmeyle yükseldikçe, teknoloji dünyası beklenmedik bir fiziki duvarla yüzleşti: Isı.

Bugün yapay zekâ devriminin geleceğini sadece kod satırları veya çip tasarımları değil; o çipler erimeden, veri merkezleri alev almadan altyapıyı ayakta tutabilen termal mühendislik çözümleri belirliyor.

Geçtiğimiz yıllarda yazılım mimarilerinin getirdiği verimlilik artışları konuşulurken, günümüzde hyper-scaler olarak adlandırılan teknoloji devlerinin, işlemcileri soğutabilmek için akarsu kıyılarına, deniz altı projelerine ve hatta doğal soğuk iklimlerin hakim olduğu İskandinav coğrafyalarına adeta hücum ettiği bir döneme girdik. Rekabet kızışırken, küresel altyapı bu devasa termal ve enerji yükünü artık soğutmakta zorlanıyor.

Veri merkezlerini soğutmada hava yetersiz kalıyor

Geleneksel veri merkezlerinde sunucular, yıllar boyunca tanıdık bir yöntemle soğutuldu: Devasa klima santralleri, hava kanalları ve yüksek devirli fanlar. Bir sunucu rafının geçmişte tükettiği 5 ila 10 kilovatlık (kW) güç, havayı işlemcinin yüzeyinden

geçirerek tahliye etmeye fazlasıyla yetiyordu. Ancak Nvidia'nın H100, H200 ve ardından gelen Blackwell (B200) mimarili yeni nesil yapay zekâ GPU'larının sahneye çıkmasıyla bu denklem tamamen altüst oldu.

Gelişen teknolojiyle birlikte artık tek bir yapay zekâ çipi 1.000 Watt civarında ısı üretiyor. Devasa bir sunucu rafına yan yana dizilen bu sistemler, raf başına güç tüketimini 40 ila 100 kW seviyesine çıkarıyor. Fizik kuralları gereği, havanın ısı taşıma kapasitesi bu noktada yetersiz kalıyor. Fanları daha hızlı döndürmek veya ortama daha çok klima konuşturmak artık silikonun merkezindeki aşırı ısınmayı engellemiyor. Hava soğutma teknolojisi, yapay zekâ çağında fiziki sınırlarına dayanmış durumda.

Veri merkezlerinin su kullanımının, enerji kullanımı ve karbon emisyonlarıyla yakından paralellik gösterdiğine dikkat çeken Çevre ve Enerji Çalışmaları Enstitüsü Proje Müdürü Miguel Yanez-Barnuevo; veri merkezlerinin daha fazla enerji kullandıkça, aşırı ısınmayı ve olası hasarı önlemek için işlemci çiplerini soğutmak üzere daha büyük miktarda su tükettiklerini ifade etti.

Veri merkezlerinde sıvı soğutma devrimi

Havanın pes ettiği bu kırılma noktasında veri merkezleri, radikal bir

altyapı dönüşümüne zorlanıyor: Sıvı soğutma. Suyun ve özel soğutucu sıvıların ısıyı iletme kapasitesinin havadan yüzlerce kat daha yüksek olması durumu, veri merkezlerini geleneksel bir bilgisayar odası olmaktan çıkarıp, devasa boru hatlarının, pompa istasyonlarının ve sızdırmazlık teknolojilerinin yönetildiği sanayi tesislerine dönüştürüyor.

Bugün sektörde öne çıkan iki temel sıvı soğutma mimarisi bulunuyor:

Çip Üstü Sıvı Soğutma (Direct-to-Chip): Özel soğutucu sıvılar, mikro kanallar aracılığıyla doğrudan işlemcinin üzerindeki bakır plakaya temas ettiriliyor. Çipin ürettiği ısı anında sıvıya aktarılıyor ve dışarıdaki soğutma kulelerine pompalanıyor.

Daldırma Soğutma (Immersion Cooling): Sunucu raflarının tamamı, elektrik iletmeyen dielektrik bir yağ veya özel sıvı tankının içine tamamen batırılıyor. Isınan sıvı tank içinde yükselerek harici bir eşanjör üzerinden soğutuluyor.

Bu dönüşüm, veri merkezlerinin kurulum maliyetlerini muazzam seviyede artırıyor. Ancak sıvıya geçiş de sorunu tek başına çözmeye yetmiyor: Yapay zekâyı soğutmaya ve beslemeye yönelik küresel su faturası, sanılanın çok ötesinde bir boyuta ulaşıyor.

"Çipe doğrudan" (direct-to-chip) tek fazlı soğutmanın henüz ilk aşamalarında olduğunu ve geniş ölçekte kullanılmadığını belirten Mitsubishi Electric Hydronics Temel Teknoloji Ar-Ge ve Laboratuvar Teknolojileri Müdürü Alessandro Talini, önümüzdeki 10 yıl içinde, yeni GPU'ların ısı yükü arttıkça, çipe doğrudan tek fazlı soğutmanın giderek daha yaygınlaştığını göreceğimizi söyledi.

"Bunu, iki fazlı soğutmaya ve nihayetinde daldırmalı (immersion) soğutmaya (önce tek fazlı, ardından iki fazlı) geçiş izleyecektir" öngörüsünde bulunan Talini, 10 yıldan daha uzun bir süre sonra, bu sistemlerin

artık yeterli olmayabileceğini ve yeni soğutma teknolojilerine ihtiyaç duyulabileceğini söyledi. Ancak bu süreçte hesaplama verimliliğinde önemli bir artış yaşanmasının mümkün olduğunu belirten Talini, QPU'ların (Kuantum İşlem Birimleri) ortaya çıkmasının da olası olduğuna dikkat çekti.

30 trilyon litrelik su faturası

Yapay zekâ teknolojilerinin ekolojik ayak izi tartışılırken akla ilk olarak su tüketimi geliyor. Global Water Intelligence ve Xylem projeksiyonlarına göre, yapay zekâ ekosisteminin küresel su talebine ekleyeceği miktar 2050 senesine kadar yıllık 30 trilyon litre gibi devasa bir büyüklüğe ulaşacak.

Bu tablonun detayları incelendiğinde ilginç bir sektörel gerçeklik karşımıza çıkıyor: Veri merkezlerinin doğrudan sıvı soğutma için tükettiği su, 2025'te 0,7 trilyon litre seviyesinden 2050'de 2,7 trilyon litreye yükselerek, buz dağının yalnızca küçük bir kısmını oluşturuyor. Asıl devasa su tüketimi, sistemin iki ana sütununda yaşanıyor: Çip üretimi ve elektrik santralleri.

Yapay zekâ modellerini çalıştıracak güçlü GPU'ların üretildiği devasa dökümhanelerde kullanılan su ihtiyacı, 2025'teki 4,1 trilyon litre seviyesinden 2050 yılında 29,3 trilyon litreye ulaşarak adeta dikey bir sıçrama yapıyor. Benzer şekilde, bu veri merkezlerini ve çip fabrikalarını besleyecek enerji santrallerinin soğutma su kullanımı da 2050 yılında 22,3 trilyon litreye dayanıyor.

Veri merkezlerinin sayısı, boyutu ve karmaşıklığı arttıkça su tüketiminin de artmaya devam etmesinin beklendiğini ifade eden Yanez-Barnuevo, tüketilen suyun genellikle buharlaşan veya başka bir şekilde insan kullanımından çıkarılan su olduğuna dikkat çekiyor.

Yerel akarsulardan veya yeraltı su kaynaklarından tatlı su çekilmesinin, özellikle su kıtlığı yaşanan bölgelerde, su kaynaklarının

tükenmesine yol açabileceğine işaret eden Yanez-Barnuevo, veri merkezlerinin su kullanımının; konum, iklim, su mevcudiyeti, boyut ve bir raftaki çip yoğunluğu gibi çeşitli faktörlere bağlı olduğunu söylüyor.

Özellikle ABD'nin güneybatısı gibi daha sıcak iklimlerde yaşanan zorluklara dikkat çeken Yanez-Barnuevo, bu durumda veri merkezlerinin binayı ve ekipmanı soğutmak için daha fazla su kullanması gerektiğini belirtiyor.

Dolayısıyla "yapay zekâyı soğutmak", sadece veri merkezindeki sunucunun üzerine su dökmekten ibaret değil: Çip dökümhanelerinden enerji şebekelerine kadar uzanan devasa bir zinciri ıslatmak anlamına geliyor. Önümüzdeki dönemde yerel tatlı su kaynakları üzerindeki bu baskının, su kullanımına yönelik sert yasal yaptırımları, çevre vergilerini ve kısıtlayıcı regülasyonları beraberinde getirmesi kaçınılmaz görünüyor.

Veri merkezlerinin muazzam miktarda su tükettiği fikrinin kolektif bir histeriyi körükleyen ciddi bir yanlış anlaşılma olduğuna dikkat çeken Talini, ABD özelinde durumun böyle olduğunu; ancak bunun ülkede buharlaştırmalı soğutma kulelerinin kullanılmasından kaynaklandığını söyledi.

"Örneğin Avrupa'da, buharlaştırmalı soğutma kulelerinin kullanımı oldukça sınırlıdır. Bunun yerine, su yalnızca bir ısı taşıyıcı akışkan olarak kullanılmaktadır, hiçbir su tüketimi gerçekleşmez, aynı derecede verimli başka çözümler tercih edilmektedir" ifadelerini kullanan Talini, bu alanda Avrupa'nın, ABD'nin çok önünde olduğunu söyledi.

Coğrafi yer değiştirme: Kutupsal rota ve veri merkezlerinin geleceği

Soğutma maliyetleri, devasa enerji ihtiyacı ve ekolojik baskılar, veri merkezlerinin lokasyon stratejilerini de kökünden değiştiriyor. Şirketler artık tesislerini sadece finans merkezlerine veya büyük

nüfus yoğunluklarına yakın yerlere değil; termal verimliliğin, su imkanlarının ve temiz enerji erişiminin en yüksek olduğu coğrafyalara kurmayı hedefliyor.

İskandinav ülkeleri (Finlandiya, Norveç, İsveç) doğal soğuk iklimleri ve bol hidroelektrik/jeotermal enerji kaynakları ile OpenAI gibi şirketlerin yapay zekâ veri merkezlerinin yeni cazibe merkezi haline geliyor. Diğer yanda ise, devasa veri raflarını okyanusun soğuk derinliklerine indirmeyi hedefleyen deniz altı veri merkezi projeleri ve bölgesel su havzalarına odaklanan konumlama stratejileri test ediliyor.

Bir veri merkezinin enerji verimliliğini ölçen metriğin (PUE – Güç Kullanım Etkinliği), tesisin bulunduğu coğrafi konumdan ve iklim koşullarından büyük ölçüde etkilendiğini belirten Talini, soğuk iklimlerde verimliliğin çok daha yüksek olduğunu söyledi.

Ancak ne yazık ki veri merkezlerini yalnızca İzlanda veya Norveç gibi yerlerde konumlandırmanın mümkün olmadığını ifade eden Talini, nitekim birçok uygulama için, daha kısa yanıt süreleri elde edebilmek adına veri merkezlerinin kullanıcılara yakın olması gerektiğine dikkat çekti.

Algoritmik düşlerden fiziki gerçeklere

Yapay zekâda rekabet günden güne ısınırken, bu rekabeti taşıyan silikon çipler ve devasa üretim alt yapısı da kelimenin tam anlamıyla aşırı ısınıyor.

Önümüzdeki dönemde yapay zekâ pazarının kazananlarını yalnızca daha akıllı modeller geliştirenler değil, bu modelleri erimeden ve gezegenin kaynaklarını kurutmadan çalıştıracak termal mühendislik çözümlerini üretenler belirleyecek. İşte bu, teknoloji dünyasının çözmesi gereken en sıcak denklem.

Siber Güvenlik

Asimetrik Tehdit Çağında Siber Güvenlik

Yapay zekânın getirdiği asimetrik riskler ve son PHP krizinde görüldüğü gibi ortaya çıkan anlık altyapı zafiyetleri, siber güvenliği finansal ve operasyonel stratejilerin tam merkezine konumlandırdı; bu doğrultuda siber güvenlik yatırımlarını doğru konumlandıran şirketler, yarının dijital ekonomisinde sadece varlıklarını korumakla kalmayıp rekabette de öne geçen taraf olacak.

● Semih Albayrak

Ekim ayı, küresel ölçekte Siber Güvenlik Farkındalık Ayı olarak idrak edilirken, iş dünyası ve ekonomi çevreleri meseleyi yalnızca bir bilgi teknolojileri konusu olarak görmekten çoktan vazgeçti. Artık dijital güvenlik, bilançoların doğrudan kaderini belirleyen, sermaye koruma stratejilerinin merkezine oturan ve kurumsal itibarın en kırılgan zırhını oluşturan stratejik bir parametre haline geldi. Dünya genelinde finansal piyasalar, tedarik zincirleri ve operasyonel süreçler

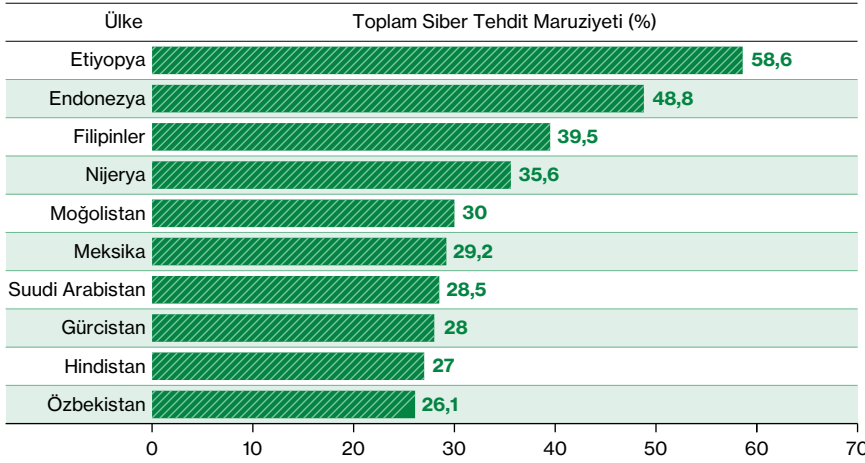
tamamen dijital ağlara entegre olurken, bu ağların güvenliği de doğrudan makroekonomik istikrarın ve mikroekonomik sürdürülebilirliğin anahtarı durumundalar. Günümüzde bir şirketin piyasa değerini, sahip olduğu fiziki varlıklardan ziyade verilerini de ne kadar koruyabildiği ve olası bir kriz anında operasyonel devamlılığını ne kadar hızlı sağlayabildiği belirliyor. Teknoloji dönüşümünün yapay zekâ gelişmeleri ile vites artırdığını son dönemde siber güvenlik artık masraf

kalemi olmaktan çıkıp, rekabet avantajını doğrudan besleyen yatırım alanına dönüştü.

Fidye saldırıların ana odağı kurumsal altyapı

2026 yılı itibarıyla siber güvenlik dünyasında, yapay zekâ hem saldırının hem de savunma tarafının ana omurga haline gelirken geleneksel çevre güvenliğinin büyük ölçüde etkisizleştiği bir dönem yaşıyor. Check Point, Cloudflare, EY, NordVPN ve

SİBER TEHDİT RİSKİ ALTINDAKİ İLK 10 ÜLKE



Not: Toplam siber tehdit maruziyeti; botnet'ler, bilgi çalan yazılımlar, bankacılık truva atları, fidye yazılımları ve mobil saldırılar olmak üzere beş belirli tehdit türüne maruz kalan sistemlerin yüzdesini bir araya getirir.

KAYNAK: CHECK POINT, BLOOMBERG

APWG tarafından açıklanan 2026 siber tehdit ve güvenlik verilerine göre, bu yıl kurumsal dünyayı ve bireyleri en çok tehdit eden siber saldırı türleri e-posta temelli saldırılardaki dilbilgisi ve üslup hatalarını tamamen ortadan kaldırarak hiper-kişiselleştirilmiş ortalama yöntemleri olarak çıktı. Check Point 2026 Siber Güvenlik Raporu verilerine göre, tespit edilen zararlı dosya ve bağlantı saldırılarının yüzde 82'si e-posta kanalıyla iletiliyor. NordVPN 2026 istatistiklerine göre ise simülasyon yapılan kimlik avı e-postalarında bağlantıya tıklayan kişilerin yüzde 51,6'sı sahte giriş sayfalarına parolalarını teslim etti. Bunun yanı sıra APWG verileri, doğrudan e-posta dışına taşan QR kodlu (quishing) ve SMS tabanlı (smishing) ortalama saldırılarının dönem bazında yüzde 2500'ün üzerinde devasa bir artış kaydettiği belirtildi.

İki faktörlü ve çok faktörlü kimlik doğrulama (MFA) sistemlerinin yaygınlaşması ise saldırganların klasik parola kırma tekniklerinden vazgeçerek doğrudan kullanıcı oturumlarını çalmaya odaklanmasına neden oldu. Cloudflare 2026 Tehdit Analizi verilerine göre; web sistemlerine yönelik giriş denemelerinin yüzde 94'ü botlar aracılığıyla yapılmakta ve bu girişimlerin yüzde 63'ünde daha

önce sızdırılmış geçerli kimlik bilgileri ile çalınan belirteçler (tokens) kullanılıyor. Şirketlerin kendi altyapılarını korumadaki başarısına karşılık, hizmet aldıkları üçüncü taraf SaaS sağlayıcıları veya yazılım tedarikçileri ana hedef haline geldi. EY Küresel Siber Güvenlik 2026 Araştırması verilerine göre, kurumların yüzde 49'u üçüncü taraf ekosistemleri ve entegrasyonlarından kaynaklanan doğrudan güvenlik açıklarıyla karşı karşıya. NordVPN 2026 raporu ise yıl genelinde kaydedilen fidye vakalarında ortalama her iki saatte bir yeni bir olayın gerçekleştiğini, bildirilen vakaların yüzde 55,5'inin 1 milyon dolar ile 10 milyon dolar arasında, yüzde 34,6'sının ise 10 milyon dolar ile 50 milyon dolar arasında doğrudan finansal hasara yol açtığını ortaya koydu. Semperis 2026 Fidye Yazılımı Risk Raporu da bu fidye saldırılarının yüzde 87'sinin doğrudan kurumsal kimlik altyapılarını hedef aldığını vurguladı.

Hızlanan saldırılar ve zaman darlığı

Teknolojik dönüşümün en yıkıcı ve heyecan verici unsuru olan yapay zekâ, siber tehdit ve savunma ekosisteminde gerekli hareket hızını da artırdı. Yapay zekânın sunduğu geniş imkânlar, bir yandan kurumların iş

yapış şekillerini verimli kılarken diğer yandan saldırganlar için eşsiz bir cephanelik yaratıyor. Fortinet Kıdemli Direktörü Arzu Akkaya, yapay zekânın siber saldırıları çok daha hızlı, karmaşık ve hedef odaklı hale getirdiğine dikkat çekerken, savunma metodolojilerinin de bu ivmeye ayak uydurmak zorunda olduğunu ifade ettir. Fortinet FortiGuard Labs tarafından hazırlanan 2026 Küresel Tehdit Ortamı Raporu verilerine atıfta bulunan Arzu Akkaya, yapay zekâ destekli saldırılarda kritik güvenlik açıklarının istismar edilme süresinin 24 ila 48 saate kadar gerilediğini vurguladı. Akkaya, zamansal daralmanın geleneksel güvenlik yaklaşımlarını tamamen geçersiz kıldığını, bunun yerine sürekli izleme, gerçek zamanlı tehdit tespiti ve otomatik müdahale sistemlerinin geçirilmesinin şart olduğunu belirtti. Arzu Akkaya'ya göre, yapay zekâ saldırganlara önemli bir hız avantajı sağlasa da savunmacılar da aynı teknolojiyen yararlanarak tehditleri henüz oluşma aşamasında yakalayabilir. Dolayısıyla buradaki temel dengeyi kurumların yapay zekâ destekli güvenlik altyapılarına ne kadar hızlı adaptasyon sağlayacağı belirleyecek.

Gölge yapay zekâ ve görünmeyen kurumsal riskler

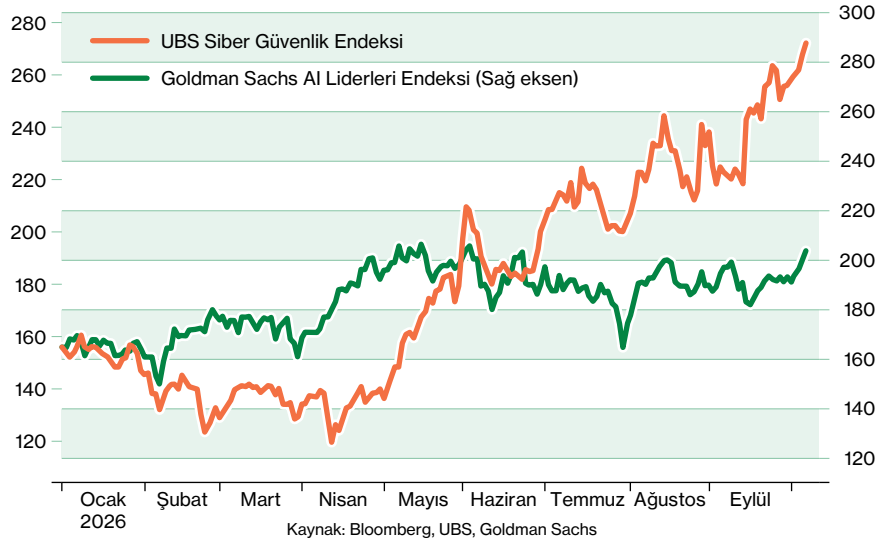
Yapay zekâ ekosisteminin kurumsal yapılarda yarattığı bir diğer derin kriz alanı ise mevzuatların ve resmi denetimlerin dışında gelişen dijital alışkanlıklar. Kaspersky Türkiye Genel Müdürü Zafer Akın, tam da bu noktada günümüz iş dünyasının en büyük ve en az fark edilen tehlikelerinden birine işaret etti. Zafer Akın, yapay zekâ alanındaki hızlı ilerlemenin siber güvenlik dinamiklerini köklü biçimde yeniden tanımladığını vurgulayarak, kurumların önündeki en kritik zafiyet noktalarından birinin "Gölge Yapay Zekâ" (Shadow AI) kullanımı olduğunu belirtti. Çalışanların resmi yönetim ve denetim mekanizmalarının dışında kalan halka açık büyük dil modellerinden giderek daha fazla yararlandığını ifade eden

Akın, kontrolsüz kullanım alışkanlıklarının doğrudan mevzuat ve uyumluluk riskleri doğurduğunu, özellikle yetersiz korunan kullanıcı hesapları veya hedef alınan üçüncü taraf platformlar üzerinden veri hırsızlığı ihtimalini ciddi şekilde artırdığını dile getirdi. Ayrıca yapay zekâ ajanlarının yepyeni bir saldırı yüzeyi oluşturduğunu hatırlatan Zafer Akın; karmaşık tespit mimarilerinde çok katmanlı makine öğrenimi modellerinin, kural tabanlı geleneksel sistemler ve insan uzmanlığı ile harmanlanarak bütüncül bir savunma kurgusu oluşturulması gerektiğinin altını çizdi.

Asimetrik savaş ve dijital kimlik krizleri

Siber güvenlik perspektifinde yapay zekânın oluşturduğu bu çift taraflı dinamik, asimetrik bir savaş alanını da beraberinde getiriyor. Konuyla ilgili değerlendirmelerde bulunan Bilişim Uzmanı Fusun Sarp Nebil, yapay zekânın siber güvenliği adeta yapay zekâların birbirleriyle mücadele ettiği amansız bir alana dönüştürdüğünü aktardı. Fusun Sarp Nebil, saldırganların güvenlik açıklarını çok daha hızlı tespit ettiğini ve kişiselleştirilmiş saldırıları otomatikleştirdiğini, savunmacıların ise tehditleri gerçek zamanlı tespit edip müdahale etme gayretinde olduğunu ifade etti. Ancak işin asimetrik boyutu ise şurada yatmakta; Salırganın tek bir açık bulması içeri girmesi için yeterliyken, savunmacı taraf sistemi tamamıyla ve henüz ortaya dahi çıkmamış meçhul açıklardan korumak zorunda. Nebil, bu sebeple kısa vadede salırganların bir adım öne geçtiğini, fakat uzun vadeli üstünlüğün yapay zekâyı güçlü bir güvenlik mimarisi ve yetkin bir insan denetimiyle birleştirmeyi başaran kurumlarda kalacağını belirtti. Günümüzün en kritik tehdidinin dijital kimliğin ele geçirilmesi ve güven ilişkisinin zayıflatılması olduğunu ifade eden Fusun Sarp Nebil, artık sistemlerin doğrudan kırılmadığını, çalınmış oturum bilgileri, yetkili hesaplar ve yapay zekâyla üretilmiş ses ve görüntüler

SİBER GÜVENLİK HİSSE PERFORMANSI YAPAY ZEKAYI GERİDE BIRAKTI



üzerinden içeri sızıldığını ekledi.

Siber harcamalarda vites arttı

Gartner'ın 2026 yılı verilerine göre küresel bilgi güvenliği harcamaları yaklaşık yüzde 12,7 oranında artış göstererek 248,9 milyar dolara ulaşmış olup, bu büyüme genel bilişim teknolojileri bütçe artış hızını geride bıraktı. Fortune Business Insights ve Mordor Intelligence raporları da pazarın bu ivmeyle 264 milyar dolar sınırını zorladığını, özellikle bulut güvenliği, sıfır güven (zero trust) mimarileri ve yapay zeka entegre savunma sistemlerinin bütçelerden en büyük payı aldığını gösteriyor. Bu finansal ve stratejik yatırımlar; IBM'in 2026 raporunda 4,99 milyon dolar olarak kaydedilen rekor ortalama veri ihlali maliyetlerinin ve otonom fidye yazılımı ile yapay zekâ tabanlı siber saldırıların yarattığı finansal kayıpların önüne geçilmesinde etken oluyor. Maddi ve operasyonel açıdan sağlanan bu avantajlar sayesinde şirketler, kritik kurumsal varlıklarını koruma altına alırken proaktif güvenlik harcamaları; veri sızıntılarından kaynaklanan ağır yasal ve idari para cezası risklerini minimize ederken, operasyonel kesintileri önlemekte ve tedarik zinciri ekosistemlerindeki üçüncü taraf risklerini etkin biçimde yöneterek kurumların küresel pazardaki

itibarını, finansal sürdürülebilirliğini ve müşteri güvenini güvence altına alıyor.

Kuantum çağının eşliğinde bulut teknolojileri erişim kırımları

Fortinet Kıdemli Direktörü Arzu Akkaya, kimlik ihlallerinin bulut sistemlerine yönelik saldırılarda en yaygın yöntem olduğunu belirterek; şifrelerin ve tarayıcı verilerinin ele geçirilmesiyle sistemlere yetkili kullanıcı gibi girilmesinin yanı sıra bulut kaynaklarının kripto madenciliği ve yapay zeka istismarı için kullanılmasının büyük bir risk ve maliyet oluşturduğunu vurgularken mevcut tehditlerin ötesindeki kuantum riskine dikkat çeken Kaspersky Türkiye Genel Müdürü Zafer Akın, Ekim 2026'daki "Operation FlashHole" vakasını örnek göstererek salırganların şimdiden kuantum sonrası kriptografiden yararlanmaya başladığını söyledi. Akın kurumların kuantuma dirençli altyapılara ve "kriptografik çeviklik" anlayışına geçmesi gerektiğini belirtti. Bilişim Uzmanı Fusun Sarp Nebil ise NIST standartları doğrultusunda şirketlerin şifreleme envanterlerini çıkararak kademeli geçiş planlarını zaman kaybetmeden devreye sokmaları gerektiğini ifade etti.