

Yapay Zekânın Yeni Cephesi: Veri Merkezleri

Dr. Emine Çelik, 1 Eylül 2026

<https://www.fokusplus.com/dosya-teknoloji/yapay-zekanin-yeni-cephesi-veri-merkezleri>

Yapay zekâ çoğu zaman algoritmalar, büyük dil modelleri, çipler ve yazılımlar üzerinden tartışılıyor. Oysa yapay zekânın küresel güç mücadelesindeki asıl belirleyicilerinden biri olan veri merkezleri giderek daha görünür hâle geliyor. Bilindiği üzere, yapay zekâ modelleri soyut bir dijital evrende çalışmıyor: Milyonlarca hatta milyarlarca parametrenin işlenebilmesi için devasa hesaplama kapasitesine, yüksek miktarda elektriğe, gelişmiş soğutma sistemlerine, fiber bağlantılara, çiplere ve fiziksel güvenliğe ihtiyaç duyuluyor. Dolayısıyla veri merkezlerini yalnızca bir teknoloji şirketinin sunucularını barındırdığı ticari bir tesis olarak göremeyiz. Özellikle yapay zekâ çağında veri merkezleri; enerji altyapısı, yarı iletken tedarik zincirleri, denizaltı kabloları, bulut sistemleri ve savunma teknolojileriyle birleşerek yeni nesil stratejik altyapının merkezine yerleşmiş durumda.

“Bulut”un fiziksel gerçekliği

Teknoloji sektöründe “cloud” yani “bulut” kavramı uzun süredir zihinlerde; fiziksel mekândan bağımsız, sınırsız ve esnek bir dijital alan izlenimi yaratıyor. Ancak bulutun gerçekte veri merkezleri, enerji hatları, jeneratörler, soğutma sistemleri, fiber kablolar ve fiziksel sunuculardan oluştuğunu ifade etmek gerekiyor. 2026’da Körfez’deki İran saldırıları bu gerçeği stratejik güvenlik açısından daha görünür hâle getirdi.

1 Mart 2026 tarihinde İran’ın saldırıları sonucunda BAE’de iki AWS tesisi doğrudan zarar gördü; Bahreyn’deki bir AWS tesisi ise yakınındaki saldırıdan fiziksel olarak etkilendi. AWS, saldırıların yapısal hasara, enerji beslemesinin kesilmesine ve yangın söndürme sistemlerinin devreye girmesi nedeniyle ek su hasarına yol açtığını açıkladı. Burada kritik nokta yalnızca üç veri merkezinin zarar görmesi olarak değerlendirilmemelidir. Asıl önemli olan, bu tesislerin bölgedeki bankacılık, ödeme sistemleri, şirketler ve kamu hizmetleri açısından taşıdığı bağımlılıktır. Bir diğer önemli parametre ise saldırılar sonrasında AWS’nin müşterilerine verilerini yedeklemeleri ve iş yüklerini etkilenmeyen bölgelere taşımaları yönünde tavsiyelerde bulunmasıdır. Dolayısıyla modern savaş açısından bir veri merkezinin vurulması yalnızca “bir teknoloji şirketinin binasının zarar görmesi” olarak değerlendirilemez. Eğer o veri merkezi finansal işlemlerden lojistiğe, kamu hizmetlerinden yapay zekâ uygulamalarına kadar çok sayıda sistemi çalıştırıyorsa, saldırının etkisi fiziksel tesisin çok ötesine taşınmaktadır. Bu durum da kritik altyapı kavramının yeniden düşünülmesini gerektiriyor.

Kritik altyapı olarak veri merkezleri

Geleneksel güvenlik anlayışında kritik altyapı denildiğinde enerji santralleri, petrol rafinerileri, limanlar, havalimanları, telekomünikasyon ve ulaşım ağları öne çıkarken; dijital dönüşümle birlikte bu listeye internet altyapısı, denizaltı kabloları ve veri merkezleri dâhil olmuştur. Yapay zekâ ise bu dönüşümü daha da hızlandırmaktadır. Nitekim büyük yapay zekâ modellerinin eğitimi ve çalıştırılması, geleneksel veri işlemenin ötesinde devasa bir hesaplama gücü gerektirdiğinden veri merkezleri ile enerji sistemleri arasındaki bağ her geçen gün güçlenmektedir.

Büyük bir yapay zekâ veri merkezi yalnızca sunucu raflarından oluşmamaktadır. Detaylara bakıldığında kapsam olarak; yüksek gerilim hatları, trafo merkezleri, jeneratörler, batarya sistemleri, soğutma altyapısı ve fiber bağlantılarla birlikte düşünülmesi gereken devasa bir endüstriyel kompleks olarak değerlendirilmelidir.

Gözden Kaçmasın

ABD yönetiminin 2025 yılında yayımladığı başkanlık kararnamesi bu değişimi açık biçimde ortaya koyuyor. Washington, 100 MW'ın üzerinde yeni elektrik yükü gerektiren yapay zekâ veri merkezlerini özel bir “data center project (veri merkezi projesi)” kategorisinde tanımlarken, bu tesislerin ihtiyaç duyduğu elektrik iletim hatlarını, doğal gaz altyapısını, trafo ve şalt sistemlerini, yarı iletkenleri, ağ ekipmanlarını ve veri depolama sistemlerini de aynı stratejik ekosistemin parçaları olarak değerlendiriyor. Başka bir ifadeyle Washington'ın yaklaşımında veri merkezi artık tek başına bir bina olarak değerlendirilmek yerine, kompleks bir yapı olarak tasvir ediliyor.

Kısaca yapay zekâ stratejik altyapısı; veri merkezi, enerji, çip, ağ ve depolama sistemlerinin bir araya geldiği bütünleşik bir yapı olarak değerlendirilmektedir. Bu tanım ise yapay zekâ jeopolitiğinin neden salt yazılım rekabeti olarak okunamayacağını da göstermektedir.

Bu yaklaşım aynı zamanda veri merkezleri ve enerji güvenliği arasında yeni bir organik bağ kurulmaya çalışıldığını gösteriyor. Bu bağlamda ikinci bir jeopolitik dönüşümün yapay zekânın artık enerji jeopolitiğinin bir parçası olarak ortaya çıkması olduğunu ifade edebiliriz. Dolayısıyla Washington'ın 2025 tarihi itibarıyla veri merkezlerine ilişkin stratejik altyapı kapsamında doğal gaz boru hatlarından nükleer enerji ekipmanlarına, elektrik iletim hatlarından trafo merkezlerine kadar çok geniş bir alanı sayması tesadüf değildir. Gelecekte ise veri merkezi yatırımlarının yalnızca “en iyi internet bağlantısı”nın bulunduğu bölgelere değil, güvenilir ve ucuz elektrik üretiminin bulunduğu bölgelere yönelmesine yol açabilir. Öyle ki ABD'nin yeni yapay zekâ altyapı yatırımlarında veri merkezi ile enerji üretiminin aynı proje içerisinde kurgulanması bu durumun göstergesi olarak okunabilir. Böylece yapay zekâ ekonomisinin coğrafyası ile enerji altyapısının coğrafyasının giderek örtüştüğünü söyleyebiliriz. Bu gelişme Türkiye açısından da büyük önem taşıyor. Nitekim

geleceğin veri merkezi yatırımlarında salt fiber altyapısı veya pazar büyüklüğü değil; elektrik arz güvenliği, enerji fiyatları, soğutma kapasitesi, su kaynakları ve jeopolitik riskler belirleyici olacaktır.

Washington'ın 2025 "AI Action Plan"ı da bu yaklaşımı destekler niteliktedir. Planın; veri merkezleri ve yarı iletken fabrikalarının izin süreçlerinin hızlandırılmasını, ABD'nin yapay zekâ altyapısının genişletilmesini ve Washington'ın yapay zekâ teknolojilerinin müttefik ülkelere "full-stack" paketler hâlinde ihraç edilmesini hedeflediğini söyleyebiliriz. Bu perspektiften ABD'nin yapay zekâ rekabetinin; model, çip, veri merkezi, enerji, ağ, güvenlik ve küresel teknoloji ekosistemi şeklinde bütünleşik bir strateji olarak kurgulandığı açıktır.

ABD'nin son dönemdeki politikaları, Washington'ın yapay zekâ rekabetini yalnızca model geliştirme veya yazılım üstünlüğü üzerinden görmediğini ortaya koyuyor. Bunun en dikkat çekici örneği ise Stargate Projesi olarak karşımıza çıkıyor. OpenAI, SoftBank, Oracle ve MGX tarafından duyurulan Stargate, ABD'de yapay zekâ altyapısı oluşturmak amacıyla dört yıl içerisinde 500 milyar dolara kadar yatırım gerçekleştirmeyi hedefliyor. Projenin ölçeği zaman içinde daha da büyüdü. OpenAI ve Oracle, 2025'te 4,5 GW ek Stargate veri merkezi kapasitesi geliştirme anlaşması açıkladı. Buradaki stratejik mesele, yatırımın büyüklüğünden çok ABD'nin hesaplama kapasitesini ulusal güç unsuru olarak kurumsallaştırmasında yattığını söylemek mümkündür.

Körfez'de enerjiden hesaplama gücüne

ABD-İran Savaşı itibarıyla Körfez'de yer alan veri merkezlerine gerçekleştirilen saldırılar, söz konusu merkezlerin varlıkları ve hedef olmalarına dair bir dizi tartışmayı beraberinde getirdi. BAE ve Suudi Arabistan, sahip oldukları enerji kaynaklarını, finansal sermayeyi ve coğrafi konumlarının avantajlarını yapay zekâ yatırımlarına dönüştürme eğilimindedir. Bu ülkeler açısından hedef, salt veri merkezi kurmaktan çıkıp bölgesel hesaplama merkezleri hâline gelmektir. Ancak bilindiği üzere 28 Şubat'tan bu yana yaşanan saldırılar bu stratejinin temel paradokslarını ortaya çıkardı. Körfez ülkeleri bir taraftan enerji ve sermaye avantajlarını kullanarak yapay zekâ altyapısının yeni merkezleri hâline gelirken, diğer taraftan aynı altyapının kaçınılmaz jeopolitik çatışmalara maruz kalma riski artıyor. Bu nedenle "AI Hub" olmanın karşılığında yeni bir güvenlik maliyeti ortaya çıktığını söyleyebiliriz. Ek olarak dijitalleşmenin getirmiş olduğu avantajlar kadar son dönem aktif çatışma ve savaş alanlarına baktığımızda, bir ülke ne kadar fazla küresel veri merkezi barındırıyorsa dijital sistemler bağlamında potansiyel bir stratejik hedef hâline gelme ihtimali de yükseliyor.

İran'ın AWS tesislerine yönelik saldırılarının ardından ortaya çıkan tartışmanın temelinde de aslında bahsi geçen bu durum bulunuyor. ABD'nin ve müttefiklerinin bölgedeki askerî ve istihbarat faaliyetleriyle bağlantılı görülen ticari teknoloji altyapılarının, karşı taraf açısından artık tamamen "sivil" ve çatışmadan bağımsız tesisler olarak değerlendirilmediğini ifade etmek gerekiyor. Buradan hareketle geline nokta veri

merkezlerinin potansiyel durumuna dair tartışmaların yeni bir merkeze doğru kaydığını ifade edebiliriz. Özellikle İran'a yakın bir haber ajansının saldırıların AWS altyapısının askerî ve istihbarat faaliyetlerini desteklediği iddiasıyla gerçekleştirildiğini ileri sürmesi bu algıyı gösteriyor; her ne kadar bu gerekçenin bağımsız olarak doğrulanmadığını vurgulasak bile kritik olan, iddianın doğruluğundan ziyade hedef algısının değişmesidir.

Savaşın yeni hedef seti: Veri merkezleri

Günümüzde artık modern hedef setinin giderek genişlediğini söyleyebiliriz. Bir devletin askerî kapasitesini sadece tankların, uçakların ve füze sistemlerinin oluşturmadığı kabul edilen bir gerçektir. İstihbarat alanlarının genişlemesi bağlamında veri işlenmesi, hedef tespiti, lojistik planlama, iletişim, finansal sistemler ve yapay zekâ destekli otonom karar destek mekanizmaları giderek dijital altyapıya bağımlı hâle evriliyor. Dolayısıyla bir veri merkezinin stratejik değeri, içerisinde bulunan sunucuların maliyetinden çok hangi sistemleri ayakta tuttuğuyla ölçülebilir duruma gelmiştir.

Son dönemlerde veri merkezleri ile ilgili yapılan analizlere bakıldığında ortak kanı; büyük dijital veri merkezi kampüslerinin geleceğin savaşlarında “yüksek değerli hedefler” hâline gelebileceği ve yapay zekâ altyapısının savunma planlamasının yeni unsurlarından biri olarak değerlendirilmesi gerektiğidir. Bu perspektiften bakıldığında veri merkezlerinin petrol rafinerilerine benzer bir stratejik karakter kazanabileceği iddia edilebilir. Söz konusu iddianın altyapısına bakıldığında ise petrol rafinerileri enerji ekonomisinin sürekliliğini sağlarken, yapay zekâ veri merkezlerinin de hesaplama ekonomisinin sürekliliğini sağladığını söylemek mümkündür. Sonuç olarak birinin kesintiye uğraması ilk olarak enerji ve üretim sistemlerini etkiliyor; diğerinin kesintiye uğraması ise dijital ekonomi, finans, kamu hizmetleri ve yapay zekâ uygulamalarını etkileyebiliyor.

Yeni jeopolitik denklem: Hesaplama egemenliği

Bu dönüşümün devletler açısından en önemli sonucu ise yeni bir egemenlik tartışması yaratmasıdır. Geçmişte enerji bağımsızlığı nasıl stratejik bir hedefse, gelecekte hesaplama kapasitesi bağımsızlığı da benzer bir önem kazanabilir. Bir ülke kendi yapay zekâ modellerini geliştirmek istiyorsa yalnızca yazılıma değil; yeterli GPU kapasitesine, veri merkezlerine, elektrik üretimine, yüksek hızlı ağlara, veri depolama kapasitesine ve çip tedarikine ihtiyaç duyacaktır. Dolayısıyla ABD'nin stratejisini dikkatle takip etmek gerekiyor.

Washington yalnızca kendi topraklarında veri merkezi kapasitesini artırmaya çalışmıyor; aynı zamanda Amerikan yapay zekâ ekosistemini müttefik ülkelere taşımayı öngören teknik altyapılar üzerinde de politikalar üretiyor. Böylece yapay zekâ altyapısını bir anlamda ABD'nin dış politika aracına dönüştürdüğünü söylemek mümkündür. Bu durumun önümüzdeki dönemde ülkeler arasında yeni bir rekabet alanı oluşturabilecek kapasiteye sahip olduğunu vurgulamak gerekiyor. Özellikle büyük dil modelleri ve yapay zekâ entegreli otonom sistemler bağlamında literatür genişlese bile sorulması gereken bir

diğer önemli soru, “Kim daha iyi yapay zekâ modeline sahip?” sorusuna ek olarak “Kim daha fazla güvenli hesaplama kapasitesine sahip?”tir.

Sonuç yerine

Yapay zekâ çağında jeopolitik rekabetin merkezinde yalnızca veri bulunmuyor. Verinin anlamlandırılmasını sağlayan hesaplama kapasitesi de stratejik bir kaynak hâline geliyor. Bu bağlamda veri merkezleri geleceğin dijital ekonomisinin fabrikaları olarak görülebilir. Nasıl sanayi çağında fabrikaların bulunduğu bölgeler ekonomik ve stratejik açıdan önem kazandıysa, yapay zekâ çağında da yüksek kapasiteli veri merkezlerinin bulunduğu bölgeler yeni güç merkezlerine dönüşebilir. Fakat burada önemli bir farkın altını çizmek gerekiyor: Bu fabrikalar yalnızca üretim yapmıyor; devletlerin karar destek sistemlerinden finansal piyasalara, askerî istihbarattan yapay zekâ modellerine kadar çok geniş bir ekosistemi çalıştırıyor. ABD’nin Stargate gibi projelerle milyarlarca dolarlık hesaplama kapasitesi inşa etmeye yönelmesi, Washington’ın bu altyapıyı ulusal güç unsuru olarak gördüğünü ortaya koyuyor.

İran-ABD çatışmasında AWS tesislerinin hedef alınması ise bu stratejik dönüşümün savaş alanındaki karşılığını açık bir biçimde gösterdi. Veri merkezleri artık savaşın dışında kalan nötr teknoloji tesisleri olarak düşünülemeyebilir. Özellikle askerî, istihbari, finansal ve kamu sistemleriyle bütünleşmiş büyük veri merkezleri, geleceğin çatışmalarında yüksek değerli kritik altyapı kategorisine girebilir. Sonuç olarak yaşanan tüm gelişmelerle doğru orantılı olarak asıl sorulması gereken soru şudur:

“Yapay zekâyı kim geliştiriyor?” sorusu kadar, “Yapay zekâyı çalıştıracak fiziksel altyapıyı kim kontrol ediyor?”

Bu sorunun cevabı bizi çip fabrikalarından enerji santrallerine, veri merkezlerinden denizaltı kablolarına, nadir toprak elementlerinden elektrik şebekelerine kadar uzanan yeni bir jeopolitik haritaya götürüyor. Ve bu haritada veri merkezi artık yalnızca bir teknoloji yatırımı değil; enerji, ekonomi, egemenlik ve uluslararası güvenliğin kesiştiği stratejik bir altyapı olarak değerlendirilmelidir.