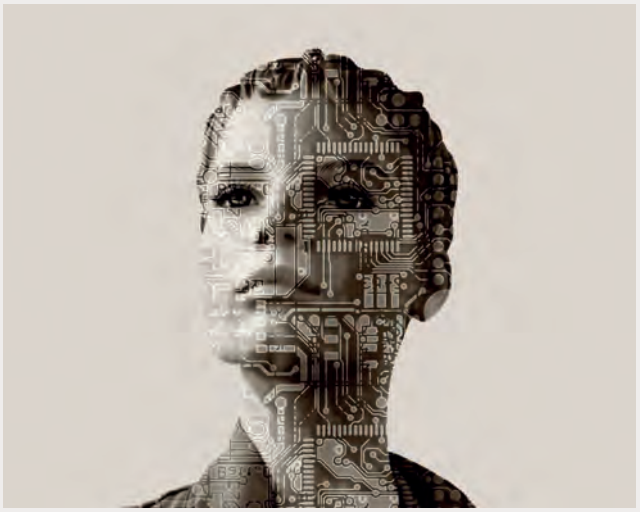
Levent Daşkıran

Teknoloji Devleri Yapay Zekâyı Kontrol Etmek İçin Birleşti

Yapay zekâ uygulamaları hayatın pek çok alanında insanların yaptığı işleri ellerinden alırken, bu yolun sonunda *Terminatör* filminin gerçeğe dönüşebileceğine dair endişelenenlerin sayısı hızla artıyor. Aslında haksız da değiller. İnsana özgü düşünce sisteminden ve vicdandan yoksun otomasyona dayalı bir sistemin, günün birinde kendi varlığını sürdürmeyi öncelik olarak belirleyip bu yönde kararlara imza atmayacağını kim bilebilir? İşte bu yöndeki olası bir gelişmeyi engellemek için dünya teknoloji devleri Amazon, Facebook, Google, IBM ve Microsoft yapay zekâ gelişiminin etik değerlere uygunluğunu sağlamak üzere Partnership on AI (*Partnership on Artificial Intelligence*-Yapay Zekâ Ortaklığı) adını verdikleri bir birliği hayata geçirdiklerini duyurdu. Bu birlik, yapay zekâ alanında faaliyet gösteren pek çok şirketin bu alanda araştırmalar yapan bilim insanlarının katkısıyla yapay zekânın etik, eşitlik, şeffaflık, uyumluluk gibi niteliklerini kontrol altında tutmasını hedefliyor. Aslında bu gerçekten önemli bir çaba. Zira yapay zekâ dediğiniz kavram mevcut verilerin yanı sıra edindiği tecrübelerden beslenerek kendini geliştirdiği için, bu süreçte yapay zekâyı denetim altında tutmanız ve neyin doğru neyin yanlış olduğunun sınırlarını net olarak çizmeniz büyük önem taşıyor. Örneğin bundan birkaç ay önce Microsoft'un Tay adını verdiği yapay zekâ temelli sohbet robotu, kullanıcılarla arasındaki sohbetlerden aldığı verileri yorumlarken ırkçı söylemleri benimsemeye başlamış ve deneme apar topar sonlandırılmıştı. Birliğin web sitesine partnershiponai.org adresinden ulaşabilirsiniz.



Amazon, Facebook, Google, IBM ve Microsoft yapay zekâ gelişimini kontrol altında tutmak için yeni bir birliğe imza attıklarını duyurdu.

Nesnelerin İnternetinin Karanlık Yüzü Ortaya Çıkıyor

İnternet üzerinde DDoS adı verilen yaygın bir saldırı biçimi var. Çalışma ilkesi de şöyle: Önce bir grup bilgisayarın kontrolünü ele geçiriyorsunuz. Daha sonra bu bilgisayarların tamamını aynı anda belli bir hedefe yönlendiriyorsunuz. Böylece hedeflenen web sitesi veya web servisi bir anda on binlerce, hatta yüz binlerce bilgisayardan gelen isteklerle karşı karşıya kalıyor. Doğal olarak da aynı anda gelen bunca isteğe yetişemiyor ve hizmet veremez hale geliyor. İşte geçen ay bilgisayar güvenliği ve siber suçlar konusunda yayınlar yapan KrebsOnSecurity adlı blog da böyle bir saldırıya maruz kaldı ve 24 saat boyunca hizmet veremez hale geldi. Bu saldırıyı diğerlerinden ayıran şey ise saldırı için kullanılan cihazların ele geçirilmiş bilgisayarlar değil web kameralar olmasıydı. Söz konusu saldırıda, bulundurdukları bir sistem açığı nedeniyle bilgisayar korsanlarının kontrolü altına giren 145 binden fazla internete bağlı kameranın kullanıldığı tahmin ediliyor. Bu da web sunucuları üzerinde saniyede 1,1 terabite ulaşan inanılmaz bir trafik yaratarak altyapının çökmesine neden olmuş.

Olay internete bağlı -bilgisayarlar dışındaki- cihazların, yani nesnelerin internetinin neden olabileceği zararlara dair çarpıcı bir örnek olarak nitelendiriliyor. Çamaşır makinesi, aydınlatma lambası, televizyon, kahve makinesi, elektrik ve su sayacı, hava durumu ölçüm cihazı derken 2020 yılında sayılarının 24 milyara ulaşması beklenen internete bağlı bu cihazların güvenliğine yeterince önem verilmediği taktirde nasıl bir tehlike oluşturabileceklerini varın siz hayal edin. Detayları bit.ly/iotattack adresinde okuyabilirsiniz.

Son yaşanan olaylarda olduğu gibi nesnelerin internetine bağlı cihazların oluşturduğu güvenlik riskinin, önem verilmediği taktirde büyük bir sorun oluşturma potansiyeli var.