Yapay Zekâyı Yapay Zekâyla Aldatmak

Yapay zekânın hayatın her alanında kendine yer bulması işleri kolaylaştırıyor olsa da bir icadın iyilik ve kötülük için kullanılabilmesi gibi, yapay zekâ da kötü amaçlarla kullanılabilir.
Dijital teknolojiler üzerine kurulu bir dünyada bazı açıkların tespit edilmesi ve kötüye kullanılması için yapay zekâdan faydalanılabilir. Örneğin görüntü işleme tekniklerini kullanarak yüz tanıma yöntemiyle güvenlik sağlayan bir yazılımda, bir kişinin yüzüne birkaç çizik atarak o kişiyi farklı bir kişi gibi göstermek mümkün olabilir. Yapay zekâ yazılımları çok sayıda veriyi analiz ederek seçilen problem için en uygun çözüm algoritmasını belirliyor. Yazılımın nasıl çalıştığını dikkatle inceleyip yazılımı kandıracak bazı özel işlemler yapmak mümkün. Benzer veriler için benzer çözüm algoritmaları üretileceği varsayılarak eldeki bir yapay zekâ yazılımı ile karşı taraftaki bir yapay zekânın nasıl çalıştığı öğrenilebilir. Daha sonra yazılımın çalışmasını sekteye uğratacak özel durumlar oluşturulabilir. Örneğin finans firmaları piyasaları takip edip milisaniye düzeyinde anlık işlemler yapmak için karmaşık yazılımlar kullanıyor. Bu tür firmalar rakip firmaların yazılımlarını yanlış yönlendirmek için birkaç işlem yapıp farklı bir algı oluşturmaya çalışıyor. Rakip firmaların yazılımları bu yanlış algıya dayanarak yanlış işlemler yapabiliyor. Böylece rakiplerini yanlış yönlendiren firma yüksek kazanç elde edebiliyor. İşleri daha da karmaşıklaştıran bir başka husus da tek işi başka yapay zekâ yazılımlarını aldatmak olan yapa zekâ yazılımları. Böyle bir durumda açıkları tespit etmek ve bunu kötü amaçlar doğrultusunda kullanmak için uğraşan yapay zekâ yazılımlarına karşı özel önlemler almak gerekir. Örneğin sürücüsüz otomobillerde çalışan yapay zekâ yazılımlarının nasıl çalıştığını analiz eden kötü amaçlı bir yapay zekâ yazılımı, otomobilin kaza yapmasına neden olabilecek özel durumlar oluşturabilir. Yolda ilerleyen sürücüsüz bir otomobile özel bir zamanlamayla farklı noktalardan yansıtılacak ışıklarla otomobildeki yazılım "yanıltılarak" beklenmedik bir kaza olması sağlanabilir. Her ne kadar bu tür işlemleri yapmak son derece zor olsa da teknik olarak imkânsız olmadığı unutulmamalı.

_
https://arxiv.org/pdf/1607.02533v1.pdf

İçeceğiniz Ağzınızı Yakmayacak

Ember Teknoloji tarafından geliştirilen termos bardak ile kahvenizi belirlediğiniz sıcaklıkta tutabilirsiniz. Piyasada farklı tasarımlarda, farklı özellikleri olan pek çok termos bardak var, ama bunlar içecekleri içlerine koyuldukları sıradaki sıcaklıkta tutuyor. Bu da eğer içeceğinizi çok sıcakken bardağa boşalttıysanız ağzınızın yanmasına neden olabiliyor. 150 dolardan satışa sunulan Ember termos ise içeceğin sıcaklığının seçeceğiniz dereceye kadar düşmesini sağlıyor.

_
embertech.com