YAPAY ZEKA VE GÜVENLİK: FIRSAT MI YOKSA TEHDİT Mİ?

Yapay Zeka son dönemde uluslararası gündemi en fazla meşgul eden konulardan birisi olarak ön plana çıkmaktadır. Yapay zekanın getirmiş olduğu yenilikler hemen hemen herkes tarafından kullanılmakta ve olumlu yanları sürekli olarak ön plana çıkartılmaktadır.

Doç. Dr. Mehmet Emin Erendor

Fakat yapay zeka gerçekten herkesin belirttiği gibi olumlu bir etkiye mi sahiptir? Yapay Zeka sistem içerisinde olumsuzluk yaratamaz mı? Ya da bu ürün kötü amaçlı bireyler, örgütler, gruplar ya da devletler tarafından kendi amaçları için kullanılamaz mı? Aslında bu soruların tamamını farklı yapılar ve olgular çerçevesinde ele almak ve hem olumlu hem de olumsuz taraflarının olduğunu da net bir şekilde açıklamak gerekmektedir.

Yapay Zeka konusu her ne kadar son 10 yıldır sistemi etkisi altına almış olsa da bu konu ile ilgili çalışmaların 1950'li yıllardan itibaren başladığı literatürdeki çalışmalardan net bir şekilde görülmektedir. Hatta ülkemizde de Cahit Arf'ın 1959 yılında yazmış olduğu "Makine düşünebilir mi ve nasıl düşünebilir?" başlıklı makale de yapay zeka ya da makinelerin düşünmesine yönelik çalışmaların olduğunu göstermektedir. Günümüze kadar geçen süreçte yapay zekaya yönelik özellikle Amerika merkezli çalışma grupları oluşturularak çeşitli projeler hayata geçirilmek hatta neredeyse insan ve insanüstü robotlar yapılma hayali ortaya atılmış olsa da 1990'lı yıllara kadar bunların bir hayal ürünü olarak kaldığını söylemek daha doğru olacaktır.

"Hatta ülkemizde de Cahit Arf'ın 1959 yılında yazmış olduğu "Makine düşünebilir mi ve nasıl düşünebilir?" başlıklı makale de yapay zeka ya da makinelerin düşünmesine yönelik çalışmaların olduğunu göstermektedir."

Çalışmalar Amerika merkezli başlamış olsa da 1990 sonrası Çin'in de etkin bir şekilde yapay zeka çalışmalarına ağırlık vermesi iki ülkeyi çoğu zaman karşı karşıya getirmiştir. Çin'in Amerika'da silikon vadisinde bu konuda çalışmada bulunan kişileri kendi ülkesine davet etmesi, olağanüstü koşullar sunması ve sadece Çin vatandaşlarını değil yabancı ülke vatandaşlarını da ülkesinde çalışmaya ikna etmesi Çin'in de yapay zeka konusunda muazzam ilerlemeler sağlamasına hatta batı dünyasının geliştirmiş olduğu ürünler dışında ya taklit ya da orijinal kendi ürünlerini oluşturmasına da imkân tanımıştır. Hatta 2017 yılından itibaren yapay zeka öğretimine ve geliştirilmesine yönelik ortaöğretim müfredatının geliştirilmesi de Çin'in yapay zeka konusunda ne kadar ileri gitmek istediğini bizlere göstermektedir. Bu bilgilerin verilmesinin temel nedeni bir bakıma yapay zekanın önemi ve gelecekteki etkisini göstermektir. Günümüzde devletler artık siyasi ya da ekonomik alanda

1 Doç. Dr. Mehmet Emin Erendor, Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü, Uluslararası Siyaset Anabilim Dalı Öğretim Üyesi.

değil dijital/teknolojik alanda da rekabet ederek kendilerini üstün konuma getirmeyi amaçlamaktadırlar. Bunun birçok nedeni bulunmaktadır ve bunlardan birçoğu da yukarıda sorduğumuz soruların cevaplarında gizlidir.

Örneğin yapay zekanın güvenlik alanında sunmuş olduğu en önemli avantaj siber güvenlik alanındaki tehditlerin algılanması ve engellenmesinde etkili bir şekilde kullanılmasıdır. Siber saldırılar günümüzde bireyler başta olmak üzere sistemdeki herkes ve her kurum için büyük tehlikeler oluşturmaktadır. Devletler son 30 yılda siber saldırılar nedeniyle büyük ekonomik zararlarla karşılaşmış ve bu durum çoğu zaman siyasi anlamda da devletlerin sorun yaşamasına neden olmuştur. Bu nedenle yapay zeka algoritmaları özellikle siber güvenlik alanında şüpheli hareketleri ve anormallikleri belirlemekte kullanılmaya başlanmıştır. Böylece devletler kritik altyapılarına yönelebilecek potansiyel saldırılar konusunda erken uyarı sistemine sahip olarak ciddi tehlikelerin de önüne geçebilme kapasitesine ulaşmışlardır. Bu durum aynı zamanda devletlerin özellikle hangi tehditlerin öncelikli olup olmadığının belirlenmesi için de büyük önem arz etmektedir. Bu sistemler Siber Olaylara Müdahale Merkezlerinin (SOME) daha etkin bir şekilde çalışmalarına da imkân tanımaktadır. Yapay Zeka sadece saldırıların önlenmesi değil aynı zamanda sosyal mühendislik saldırıları gibi saldırılarında önlenebilmesi için kullanıcılara fırsatlar sunabilmektedir.

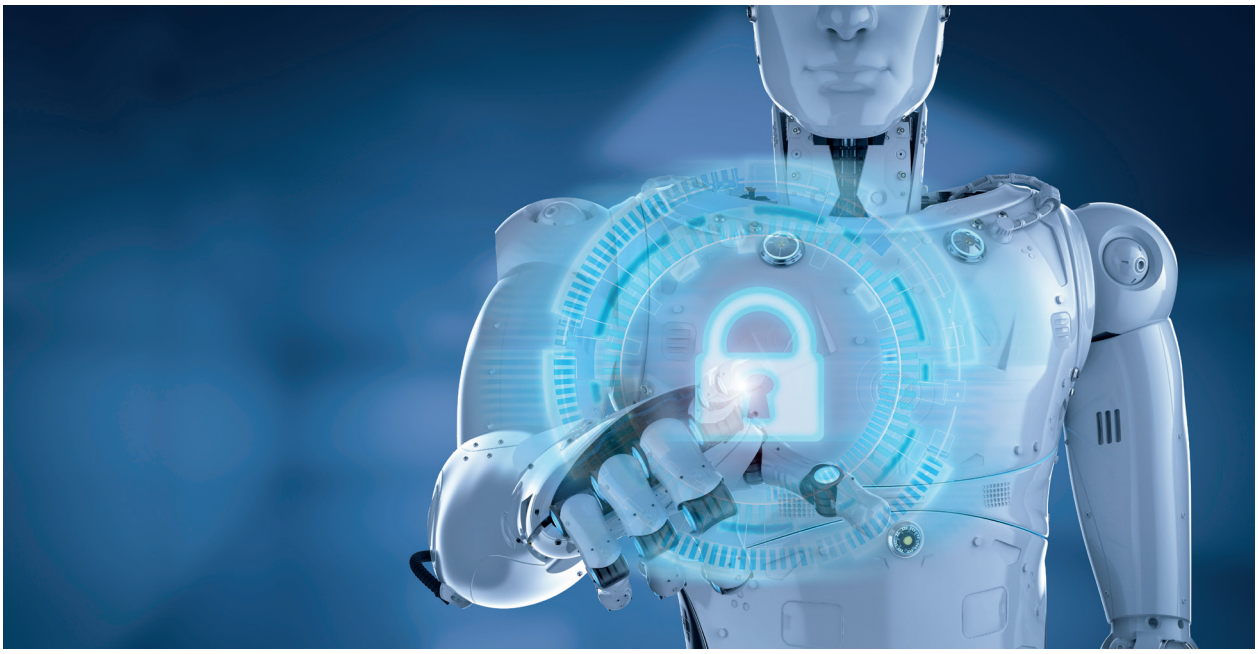
Bir diğer husus ise bireysel anlamda sürekli gözetim yapılması bazı olayların gözden kaçabilmesine imkân tanımaktadır. Yapay Zeka özellikle kamera görüntülerinin incelenmesini kolaylaştırmakta ve şüpheli davranışları da belirleyebilmektedir. Özellikle Çin tarafından etkin bir şekilde kullanılan yüz tanıma, parmak izi ve iris tarama gibi teknolojiler yapay zeka ile birlikte daha etkin kullanılabilmekte ve daha etkin güvenlik önlemlerini alınmasını ve suçluların daha kısa sürede yakalanabilmesini sağlamaktadır.

Bu faydalarının yanında sistemlerde yaşanan zayıflıkların belirlenmesi, bunlara yönelik tedbirlerin alınması, olası saldırı senaryolarına yönelik modelleme, kritik altyapı ve sektörlere yönelik erken uyarı sistemleri geliştirme, savunma sanayinde kullanılma gibi farklı konularda da olumlu etkilere sahiptir.

"Yapay zekanın güvenlik alanında sunmuş olduğu en önemli avantaj siber güvenlik alanındaki tehditlerin algılanması ve engellenmesinde etkili bir şekilde kullanılmasıdır. "

Buraya kadar yapay zekanın özellikle güvenlik alanında getirmiş olduğu faydalardan bahsettik. Bu yapay zekanın olumsuz yanları olmadığı anlamına gelmemektedir. Özellikle belirtilmesi gereken hususlardan birisi yapay zekanın kötü amaç çerçevesinde kullanılmasıdır. Yani kötü niyetli bireyler, gruplar, terör örgütleri hatta devletler siber saldırıları yapay zeka aracılığı ile otomatikleştirerek daha karmaşık saldırılar gerçekleştirebilir ve karşı tarafa daha fazla zarar verebilir. Yine bununla beraber günümüzün en büyük sorunlarından birisi olan manipülasyon konusu da yapay zeka araçları ile gerçekleştirilebilir. Liderlerin sesleri, görüntüleri taklit edilerek sahte görüntüler oluşturulabilir ve kamuoyu manipüle etmeye çalışılabilir. Hedef ülkenin iç siyasi mekanizması hedef alınarak iç karışıklık bile çıkarılabilecek veriler yapay zeka aracılığı ile ortaya çıkarılabilir.

İkinci olarak veri gizliliği ve etik konusudur. Günümüzde en fazla tartışılan ko-



nulardan birisi olan veri gizliliği ve etik konusu yapak Zeka ile birlikte daha fazla gündeme gelmeye başlamıştır. Siber güvenlik konusu ile ortaya çıkan mahremiyet konusu yapay zeka ile birlikte derinleşmiştir. Özellikle bireylerin hassas bilgilerinin izinsiz ve habersiz bir şekilde toplanması, kullanılması veya farklı amaçlar çerçevesinde ele geçirilmesi etik ve mahremiyet sorunlarını daha fazla arttırmıştır.

Diğer bir unsur ise yapay zekaya olan bağımlılık giderek artmakta ve bireyler başta olmak üzere toplumlar tüm gereksinimlerini yapay zeka araçları ile gidermeye çalışmaktadırlar. Bu durum ilerleyen dönemlerde ortaya çıkabilecek sorunlarda yapay zekanın çalışmaması ya da etkin müdahalede bulunmaması durumunda sorunların daha fazla büyüyebilmesine neden olabilecektir.

Ayrıca belirtilmesi gereken bir diğer ve en önemli husus ise yapay zekanın öğrenen bir yapıya sahip olması ve kendisini geliştirmesidir. Bu ürünü ithal eden ülkeler kendi geliştirmedikleri için güvenlik zafiyetlerini de onu üreten devletlere verebilmekte ve ilerleyen dönemlerde daha ciddi sorunlar yaşayabilmelerine hatta olası bir siyasi krizde dezavantajlı konuma düşmelerine bile neden olabilecektir.

Veriler çerçevesinde yapay zekanın büyük fırsatlar sunarken bununla beraber risk ve tehditleri de beraberinde getirdiği yukarıda sorulan soruları cevaplayabiliriz. Yapay Zeka son 10 yılda muazzam bir şekilde gelişmiş ve hayatımızın neredeyse tamamına girmiştir. Güvenlik, sanayi, eğitim, ticaret vb. tüm alanlarda yapay zeka araçları kullanılmakta ve daha da fazla kullanılacağı da öngörülmektedir. Yapay zekanın avantajlarını getirmiş olduğu olumlu durumları kullanırken olumsuz taraflarını da görmeli ve buna göre tedbir alınmalıdır. Aksi takdirde avantajlı görünen her durum ilerleyen dönemlerde daha ciddi sorunlara neden olabilecektir. Özellikle mahremiyet ve etik konusu ciddi boyutlara ulaşabilecek ve dünyadaki siyasi krizlerin daha derin yaşanmasına da imkân tanıyabilecektir. Özellikle milli yazılımlara sahip olmayan ve yapay zeka teknolojilerini ithal eden ülkeler bunları geliştiren toplumlara daha fazla bağımlı hale gelebilecek ve tüm sırları bu toplumlar kullanabileceklerdir.