Ziya Gökalp
Cyber Security Leader & Advisor

Oyun Teorisinden Yapay Zekaya ve Siber Güvenliğe

Günümüzde ‘Oyun Teorisi’ ve ‘Yapay Zeka’ benzer köklerden gelen iki olgu ve iki araştırma konusudur. Nitekim bu iki disiplin arasındaki bağlantıların geçmişten günümüze derin olduğu tartışılmaz bir gerçektir. Oyun teorisi, Amerikalı matematikçi John Neumann’ın 1944 yılında Princeton Üniversitesi yayınlarından çıkardığı Ekonomik Davranışlar ve Oyun Teorisi kitabı ile popüler hale gelmiştir.

Öğrenme hem oyun teorisi hem de yapay zeka için en temel konudur. Her ikisinde de gözlemlere, geribildirimlere, şartlara ve davranışlara dayanarak belirsiz ortamlarda getiri, yani en doğru kararı verme durumunu gerçekleştirmek için algoritmalar kullanarak hesap yapmak söz konusudur.

Oyun teorisi alanındaki çoğu araştırma, insanların ve insan gruplarının nasıl etkileşime girdiğine odaklanmaktadır. Öte yandan oyun teorisi akıl kullanarak bireylerin kendi hedeflerine ulaşma çabasıyla birbirleriyle nasıl etkileşime girdiği ile ilgilenir. Oyun teorisi, davranışlarımızın birçoğunun yanı sıra sosyal varlıklar olarak davranışlarımızın temel yapı taşlarıyla da ilgilenmektedir. İnsana ve insan topluluklarına bağlı, onların yaşama ve karar verme mekanizmalarını tetikleyen sosyolojik, psikolojik, siyasi ve hatta felsefi etkenleri de göz önünde tutar. Bu bağlamda birey seçim yaparken etkileşimde bulunduğu diğer bireyi, onun değişkenlerini ve davranışlarını göz önünde bulundurur ve en iyi sonucu alma adına en iyi tercihi yapar, yani en iyi kararı verir.

Konuya yapay zekaya bağlı öğrenme sistemleri bağlamında bakacak olursak, günümüzde farklı yapay zeka uygulamalarının ortak bir hedefe ulaşmak için etkileşime girmesi ve/veya rekabet etmesi gerekmektedir. Bir başka ifade ile, farklı kullanıcı profillerinin davranışlarını analiz eden farklı yapay zeka uygulamaları da birbirlerinden beslenerek karar vermektedirler. Bu noktada yapay zekanın temelleri oyun teorisi/kuramı ile atılmıştır demek yanlış olmayacaktır.

Her iki disiplinde de beklenen faydanın temeli, seçim teorisinin kazandığı sonucunu almaktır. Bir başka ifade ile bu disiplinler, eylemler arasında seçim yapma konusunda koşulları değerlendirerek, daha önceki tecrübeleri veya sonuçları göz önünde bulundurarak ve mevcut koşulları göz önünde tutarak verilecek karar kriterini belirlerler. Ortaya çıkan sonuç “kazanmak” olmalıdır, yani doğru karar vermiş, doğru tercih yapmış ve en iyi sonucu almış olmaktır.

Günümüzde yapay zekanın bir örneği olan makine öğrenimi, bilgisayarların deneyim yoluyla öğrenmelerini ve adapte olmasını sağlayan teknolojilere atıfta bulunan yapay zekanın bir dalıdır. İnsan-makine ilişkisindeki davranışı analiz eder, yani sebep-sonuç çıkarımdan ziyade deneyime dayalı öğrenme ile hareket eder. Makine öğrenimi sayesinde yüz milyonlarca kullanıcıdan gelen son derece değerli davranışsal veri ile bir veri hazinesi kurmak Google, Amazon, Facebook gibi birçok kurum için mümkün hale gelmiştir. Temel olarak kullanıcı ve tüketici davranışlarına ait verileri etkili bir şekilde toplamak, temizlemek, sınıflandırmak, organize etmek ve analiz etmek için birçok şirket ölçeklendirilebilir büyük veri tabanları ve yapay zeka uygulamaları oluşturmuşlardır. Elde edilen davranışsal analizler ile kullanıcı profillerine göre ürün ve hizmet sağlamak, ve hatta ihtiyaçları analiz ederek yeni ürünler ve servisler tasarlamak söz konusudur.

Konuya siber güvenlik alanındaki uygulamalar açısından bakacak olursak, organizasyonlar siber güvenliği desteklemek ve sofistike ataklara ve bilgisayar korsanlarına karşı daha fazla proaktif önlem alabilmek adına yapay zekayı kullanmaya başlamıştır. Bu bağlamda kullanıcılara ve kullanıcı gruplarına ait davranışları analiz ederek risk düzeyini ölçmek, riski tanımlamak ve aksiyon almak kaçınılmazdır. Farklı sistemlere farklı lokasyonlardan erişim yapan kullanıcıların farklı davranışlar sergilemesi olasıdır. Olağanlığın dışı davranışlar risk seviyesini ve düzeyini artırır.

Hiç şüphesiz bu davranışsal analizleri yapan farklı yapay zeka uygulamaları siber güvenlik çözümleri içinde entegre olarak çalışmaktadır.

Öte yandan saldırıları ve zafiyetleri gerçek zamanlı tespit etmek, veri sızıntısı ve veri ihlallerine karşı tepki vermek için karmaşık süreçleri otomatikleştiren farklı yapay zeka uygulamalarının kullanımı her geçen gün artmaktadır. Örneğin, yapay zekaya sahip veri aldatma teknolojisi ürünleri, saldırganları proaktif olarak algılamak ve kandırmak suretiyle gelişmiş saldırılara karşı otomatik olarak tespit, analiz ve savunma yapabilmektedirler. Bu teknolojiler aynı zamanda bilgisayar korsanlarının davranışlarını, atak vektörlerini de analiz ederek, yaklaşımları önceden anlamak adına istihbari bir veri tabanı oluşturmaktadırlar.

En yalın haliyle, basit bir güvenlik amaçlı yapay zeka uygulaması, kullanıcıların bir sisteme giriş yaparken gösterdikleri davranışları analiz eder. Bir diğer yapay zeka uygulaması, kullanıcıların bu sistem içinde çalışırken gösterdikleri davranışları analiz eder. Buradaki amaç sistemin güvenliğini sağlamak ise, sisteme giriş yaparken analiz edilen davranış ile sistem içinde çalışırken sergilenen davranışların etkileşimi bütün olarak ele alınmalıdır. Yani kullanıcı sisteme doğru davranışları sergileyerek girmiş olsa da, sistem içinde çalışırken daha önceye veya mevcut koşula göre farklı davranışlar sergiliyorsa burada anormal ve risk içeren davranışlar bütünü söz konusu olabilir.

Böylesi bir durumda, davranışları analiz eden yapay zeka uygulamasının kullanıcıyı sistem dışına çıkarması ve sisteme girişleri analiz eden uygulama ile istihbarat niteliğindeki durum bilgisini paylaşması gerekebilir ki, sisteme doğru davranışlar sergilenerek giriş yapılmış olsa bile, bir sonraki giriş talebi reddedilsin.

Hiç şüphesiz alınacak proaktif aksiyon; durum, kurum, alan, risk, zafiyet, hassasiyet, güvenlik politikası, sistem, yönetim v.b. gibi konularda yaptırım farkı gösterecektir. Ancak temel olan; farklı yapay zeka uygulamalarına ait verilerin bütünleşik olarak bir kazanım ve amaç için ortak çalışması ve farklı koşullardaki davranışlara ait bilgileri işleyerek sonuca varmasıdır.

Bilgi güvenliği olay yönetimi (SIEM), Veri sızıntısı önleme (DLP), Saldırı önleme sistemi (IPS), Kullanıcı davranış analizi (UBA), Dahili tehdit koruması (Insider Threat Protection), İzole veri güvenlik tarama sistemi (Sandbox) ve Genişletilmiş tehdit algılama ve müdahale sistemleri (EDR/XDR) gibi uygulamalar, entegre yapay zeka fonksiyonlarına sahip en bilindik Siber Güvenlik uygulamaları için örnek olarak gösterilebilinir.

Ziya GÖKALP

Cyber Security Leader & Advisor

MSc.IT, SSCP®, ECSA , CEH, OCOE,
MPM®, ITIL, Certified ISO/IEC 27001 LA,
CIW Security Analyst,
CompTIA Project+,
Senior Certified Leadership Practitioner,
Certified Information Security Executive™