

ÇİN'İN YAPAY ZEKAYI İSTİHBARATTA KULLANMASI ÜZERİNE BİR ANALİZ

Giriş: Dijital Çağda Gücün Dönüşümü ve Yapay Zekâ

İçinde bulunduğumuz 21. Yüzyıl itibariyle teknolojinin gelişmesi belli başlı gelişmeleri beraberinde getirmiştir. Güç artık sadece askeri kapasiteyle değil, geliştirilen veri ve algoritma ağları üzerinden de ölçülmektedir. Bu veri ve algoritma ağlarının sağladığı potansiyel üstünlük, verileri anlamlandırabilecek ve geri dönüş (feedback) alınmasını sağlayabilecek ileri düzey sistemlere duyulan ihtiyacı artırmıştır. Böylece yapay zekâ stratejik karar alma ve tehdit saptama süreçlerinde belirleyici bir unsur haline gelmiştir.

Çin Halk Cumhuriyeti'nin 2017 Yeni Nesil Yapay Zekâ Gelişim Planı çerçevesinde yapay zekâyı devlet kapasitesinin artırılması bağlamında kullanması, ülkede mevcut yüz tanıma sistemleri, büyük veri analitiği ve küresel teknolojik rekabette üstünlük sağlama amacıyla yapay zekâyı güvenlik ve istihbarat aygıtına entegre etme stratejisi ülkeyi bu alanda incelenmeye değer bir aktör haline getirmiştir.

Bu çalışma Çin Halk Cumhuriyeti'nin yapay zekâ teknolojilerini istihbarat toplama, veri analizi ve tehdit tespiti süreçlerinde nasıl kullandığını inceleyen bir analiz sunmayı amaçlamaktadır.

Çin'in İstihbarat Mimarisi: Yapay Zekânın Güvenlik ve İstihbarata Entegrasyonu

Geçmişten günümüze bakıldığında Çin'in istihbarat faaliyetleri oldukça ilginç bir evrilme göstermiştir. İmparatorluk dönemindeki geleneksel bilgi toplama ve saray içi gözetim faaliyetleri modern döneme doğru ilerledikçe teknolojinin de getirdiği yeniliklerle beraber gelişmiştir. 1949 sonrası Mao döneminde iç güvenlik ve rejimin istikrarı öncelik olmuş, tek partili devlet yapısının içerisinde istihbarat, ideolojik denetim ve karşı devrimci(espiyonaj) faaliyetlerinin de bastırılması amacıyla kullanılmıştır. Reform ve dışa açılma süreci sonrasında Batı'dan teknoloji transferi alan Çin, Soğuk Savaş sonrası dönemde ise siber alanlar ve açık kaynak istihbaratı (OSINT) önem kazanmıştır. 21. Yüzyılda ise tüm dünyanın yaşadığı küreselleşmenin mecburi sonucu olan dijitalleşme, büyük veri ve yapay zekâ teknolojilerinin istihbarat alanına entegrasyonu sayesinde Çin'in istihbarat kapasitesi hem ülke içinde hem ülke dışında genişlemiş, dış operasyonel kabiliyetini oldukça yetenekli bir şekilde kullanmaya başlamıştır. Bunun yanı sıra siber casusluk, veri analitiği ve Batıyla olan kıyasıya teknolojik rekabet, ülkenin stratejisinin çekirdek unsurunu oluşturmaktadır.

Bu bağlamda gelişmeyi anlayabilmek için öncelikle neler yaptığını bakılması yerinde olacaktır. Çin'in 2017 yılında yayımlanmış olduğu "Yeni Nesil Yapay Zekâ Gelişim Planı

(AIDP) bir teknoloji belgesinden çok daha fazlasıdır. Kendine 2030 yılına kadar üç aşamalı bir yol haritası oluşturarak yapay zekayı entegrasyona sistematik bir zamana yayma uygulamıştır. Planın ilk adımı 2020 yılında Batı'ya teknolojik olarak yetişmek ve yapay zekâ sektörünün değerini 22 milyar dolara çıkarmaktır. 2025 yılında ise atılım yapmayı hedefleyen ikinci adıma göre amaç, bazı yapay zekâ teknolojilerinde en önde olmak ve neredeyse her alanda yapay zekâyı ana odak yapmaktır. 2030 yılında ise dünyanın bir numaralı yapay zekâ inovasyon merkezi haline gelmek ve sektörün değerini 150 milyar doların üzerine taşımak hedefiyle planı tamamlamak istemektedir.

Planda dikkat çeken bir unsur Savunma ve Askeri uygulamalar alanında görülmektedir. Kısaca sivil-askeri füzyon da denilebilecek bu faz, yapay zekâ teknolojilerinin askeri alanla paralel olarak geliştirilmesini amaçlar. Buna insansız hava araçları, siber savunma da dahil olmakla beraber akıllı üretim, hukuk ve etiğe dikkat çekmesi ve bu konuda dünyada bir standart oluşturması açısından oldukça önemlidir.

Çin bu entegrasyonu diğer devletlerden farklı olarak 3 stratejik öncelikte inşa etmektedir. Buna göre Çin 'in algoritmaları eğitmek için dünyanın en büyük veri setine sahip olması, devlet desteğini Milli Şampiyon denen yerli şirketleri bağlamında genişletmesi ve tersine beyin göçünü uygulaması onu yapay zekâ entegrasyonu alanında farklı kılmaktadır.

Askeri ve stratejik üstünlük düşüncesi için çalışan Çin, Başkan Xi Jinping önderliğinde orduyu sadece bilgi odaklı değil, akıllandırılmış (intelligentized warfare) bir hale getirme uğraşına girmiştir. Böylelikle yapay zekâ, askeri ve istihbari alanların öznesi haline gelmekte ve Xi'nin bizzat başkanlık ettiği "Merkezi Sivil Askeri Füzyon Geliştirme Komitesi" aracılığıyla da yerli teknoloji devlerinin (Alibaba, Baidu, Tencent) sivil inovasyonlarını savunma sanayiye ve istihbarata entegre etmektedir.

Uluslararası sistem ve ilişkiler bağlamında incelendiğinde bu alandaki en önemli örnek yakın tarihte erişime açılan Deepseek yapay zekasıdır. Bahsedilen Sivil-askeri füzyonun en güçlü örneği olan Deepseek, Çin ordusuna (PLA) sağladığı teknolojik kolaylık ile değerlendirilmektedir. Ordu Deepseek modellerini çeşitli savaş simülasyonları, lojistik planlama, hastane yönetimi ve savaş arenasında durumsal farkındalık kazanmak için kullanmaktadırlar.

İstihbarat bağlamda ise algoritmik verimliliği yüksek olan Deepseek, pek çok istihbari operasyonu daha ucuz ve kolay hale getirmiştir. Örneğin Çinli siber güvenlik devleri olan şirketler (TopSec, Qihoo, 360 gibi) Deepseek modellerini kendi ürünlerine entegre ederek tehditlerin algılanması ve siber saldırı tespit kapasitelerini artırmaktadırlar.

Önemli bir nokta şudur ki, istihbarat uygulamalarını sadece dış dünyaya karşı istihbarat olarak düşünmemek gerekir. NetEase gibi şirketler Deepseek'i dijital içeriklerin sansürlenmesi ve kamuoyu takibi süreçlerini iyileştirmek için kullanmaktadırlar. Devlet kontrolündeki China Mobile ile arka plan altyapısı uyuşan Deepseek, Çin Halk Cumhuriyeti vatandaşlarının verilerini potansiyel olarak devlet kurumlarıyla paylaşmakla beraber veri güvenliği, gözetleme ve sansür için de kullanılmaktadır.

Geliştirilen bu yapay zekâ, aslında Çin'in ABD ambargolarını nasıl etkisiz kıldığına da bir kanıtı olarak görülmelidir. Deepseek'in Batı'ya kıyasen daha az işlem gücü ve maliyetle elde ettiği başarı Çin'in ABD'yi yakaladığı algısını oluşturmuştur.

Çin 'in tüm istihbari teknolojisi bununla da sınırlı kalmış değildir. Deepseek gibi modellerin yabancı dildeki askeri veya stratejik belgeleri açık kaynak istihbaratı (OSINT) kullanarak saniyeler içinde analiz ederek istihbarat açığı saptama gibi özellikleri de bulunmaktadır. Sosyal medyayı da aktif kullanarak çeşitli yapay zekâ modelleri tarafından üretilen deepfake videolar ve bot hesaplar sayesinde insanları adeta manipüle etmekte, dezenformasyona sebep olmaktadır. Böylelikle kitlelerin beynine etki etmekte ve algı yönetimi için girdiği bu mücadelede ön plana çıkmaktadır.

Ayrıca ülke çıkarına uygun bazı projeleri desteklerken de yapay zekayı ve istihbaratı kullanmaktadır. Bunun en güzel örneği olan "Kuşak Yol" projesi için de istihbarattan faydalandığını belirtmek gerekir. Dünya çapındaki merkezi ağları tarayarak bilgi almak asıl amaçtır. Proje kapsamında kurduğu 5G istasyonları ve deniz altı fiber optik kabloları sayesinde küresel internet ağlarının ciddi şekilde büyük bir biçimine erişim sağlayabilmektedir. Yapay zekayı da bu hattan akan verileri (metadata) tarayıp şüpheli veri akışını ve istihbarat kanallarının mesajlaşmalarını tespit edebilir, hatta bazı yapay zekâ modelleri şifreli mesajları kolayca çözebilir, mesajın ne sıklıkta kimden kime gittiğini anlayabilecek halde tasarlanmışlardır. Bu sinyal istihbaratı (SIGINT) faaliyeti de Çin'e rakiplerinin hamlelerini yapmadan önce keskin bir stratejik görüş sağlamaktadır.

Bu uygulamalar tüm dünyanın ilgisini çekmekte, bilhassa Batı bu konudaki hassasiyetini ortaya koymaktadır. Özellikle yapay zekâ etiği ve veri güvenliği konusunda Çin'e duyduğu güvensizlik ön plana çıkmaktadır. Toplum üzerinde tam bir gözetim amaçlı yapay zekâyı kullanması sonucu ortaya çıkan dijital otoriteriyizm, insan haklarına uygunsuz bulunmaktadır. Hakların ihlali vb. pek çok konunun mevcudiyeti, Avrupa Birliği'nin bu konuda tedbir almasını sağlamıştır. Çin modeline tepki olarak dünyanın ilk kapsamlı yapay zekâ yasasını olan "EU Ai Act"i çıkaran Avrupa Birliği, Çin'de yaygın olan "Sosyal Kredi Sistemi ve Puanlama Sistemi" gibi uygulamaları yasaklamıştır. Aynı zamanda İnsan Hakları İzleme Örgütü (HRW) Çin'in Sincan (Xinjiang) bölgesindeki gözetleme sistemlerini teknolojiyle baskılanmış bir baskı sistemi olarak nitelendirmiştir.

Amerika'da da bununla alakalı çeşitli dönüşümler yaşanmaktadır. Eski Amerikan başkanı Joe Biden Çin'e karşı teknolojik ittifak kurma çağrısında bulunmuş, ortaya "Demokrasiler İçin Teknoloji" hareketi çıkmıştır. Eski Pentagon Yazılım Birimi Başkanı Nicholas Chaillan ise Çin'in yapay zekadaki hızına yetişemediklerini ifade etmiş, eski Google CEO'su ve yapay zekâ komisyonu başkanı Eric Schmidt de "Eğer ABD ve müttefikleri stratejik bir adım atmazsa geleceğin küresel güvenlik mimarisini Çin belirleyecek." şeklinde uyarıda bulunmuştur.

Sonu olarak teknolojinin hızla gelişmesinin istihbaratı artık gizli bilgiyi almaktan ziyade verileri daha hızlı anlamlandırmak haline getirdiğini vurgulamak gerekir. Mevcut paradigma deęişimi insan ve makinelerin beraber alışmasını gerektirmektedir. Her ne kadar yapay zeka bir istihbaratçının yerini alamasa da yapay zekayı kullanmayan bir istihbaratçı, olaylar karşısında adeta kör kalmış olacaktır.

KAYNAKA:

Stanford University - DigiChina evirisi

The State Council of PRC - China's National Defense in the New Era

NSCAI Final Report - Full PDF

Department of Defense - 2023 CMPR

ASPI - Mapping China's Technology Giants

Financial Times - DeepSeek and the Chinese Military

Reuters - Chinese Military Research using DeepSeek

HRW - China's Algorithms of Repression

CSET - AI and the Future of SIGINT