thinktech
STM Teknolojik Düşünce Merkezi

Veri Odaklı Çağda İstihbarat

"Bir ordunun casusluk kanadını en iyi kullanan hükümdar bilge hükümdar, en iyi değerlendiren komutan usta komutandır. Ordunun harekât başarısı casusların becerisiyle doğru orantılıdır. Savaş sanatından anlayan kişi bir kenti kuşatmadan alan kişidir."

Tam olarak bilinmese de yaklaşık 3000 yıl önce yazıldığı düşünülen, Sun Tzu'nun *Savaş Sanatı* adlı kitabındaki bu alıntıda "casusluk" yerine "istihbarat" kelimesini koyabilir ve dünyanın en eski meslek dallarından biri olduğunu dile getirebiliriz.

Günümüzde istihbarat alanında insan faktörü, akıl dışı boyutta veri örneklerinde gezinip analiz edilebilme becerisine sahip yapay zekâyla ortaklık yapıyor. İstihbarat faaliyetleri artık eski casus filmlerindeki gibi aksiyon dolu sahnelerden hatırladığımız gibi yürümüyor; kılık değiştirmeler, farklı kimliğe bürünmeler yerini siber istihbarata bıraktı. Bugünün istihbaratı, analiz etme becerisi sayesinde geleceği okuyabilme yetisi olarak tanımlanabilir. Farklı veri gruplarından oluşan inanılmaz büyük bir veri öbeğini değerlendirerek anlamlı cevaplar elde etme becerisi 21'inci yüzyıl istihbaratını tanımlamak için en doğru cümle belki de.

Bugünün savaş alanları da eskisinden farklı, bu alanlar sadece gemi, tank ya da füzelerden oluşmuyor. Uydu sistemleri, elektrik şebekeleri, iletişim ağları, ulaşım sistemleri de alışılagelmiş savaş enstrümanlarının yanına çoktan eklendiler. Yarının savaşlarının başrolüyse şüphesiz algoritmalar, büyük veri, yapay zekâ gibi yeni teknolojilere ait olacak.

Çin'in Hızı

Bilim ve teknoloji alanındaki gelişmeler askeri istihbarat alanında mücadele anlamında yenilenme ve gelişim gerektiriyor. İstihbaratta insan unsuru yerini yapay zekâya, bilgisayar sistemlerine bırakıyor. Verilerin vektörü, hacmi, hızı, çeşitliliği ve her yerde bulunması, ulusal güvenlik politikasının, operasyonlarının ve istihbaratının geleneksel araç ve yöntemlerini dönüştürüyor. "Bilgi güçtür" mottosu altında veriden veri üretebilen teknolojilerle, verinin stratejik bir varlık olarak ele alındığı bir dönemde yaşıyoruz.

Amerika Birleşik Devletleri'nde, yakın zaman önce yayımlanan Ulusal Güvenlik Stratejisi ve Ulusal Savunma Stratejisi, yapay zekânın ulusal güvenlik ve savaş mücadelesinde otonom olarak kullanımının önemini ele aldı. Bu stratejinin, henüz kapsamlı bir ulusal strateji olduğu söylenemez. Bununla birlikte Çin yapay zekâ alanında ciddi ölçüde vites yükseltmiş durumda. Çin, önümüzdeki beş sene içinde yapay zekâ araştırmalarına milyarlarca dolar yatırım yapacağını açıkladı. Google'ın ana şirketi olan Alphabet'in Yönetim Kurulu Başkanı Eric Schmidt,

Çin'in yapay zekâ alanındaki atılımını şöyle değerlendiriyor: "2020 yılına kadar bizi yakalayacaklar. 2025 yılında bizi geçecek, 2030'a gelindiğinde de endüstriye hükmedecek noktaya gelecekler[1]."

Kontra Yapay Zekâ

ABD İstihbarat Topluluğu (IC) karmaşıklık düzeyi her gün artan veri çeşitliliğini yönetmek, ilişkilendirmek ve analiz etmek durumunda. İstihbarat döngüsünün ilk halkadan itibaren en büyük zorluğu çok kaynaklı verilerin kaynaşamaması ve analistlere daha zor, ham kaynaklar sunması. Bu zorlukların üstesinden gelebilmek de verileri ayrıştırabilen, veriden öğrenen ve cevap verebilen, istihbarat çalışanları tarafından kullanılabilecek makine öğrenmesi algoritmaları kullanımıyla mümkün. Yani samanlıktaki iğneyi doğru araçla aramak önemli; büyük veriyi manipüle edebilen ve anlayabilen sistemler ve makinelerle işbirliğini ilerletmekse bu yeni ortama uyum sağlamaya yönelik en yaratıcı yol. Bu sayede analistler değerli zamanlarını daha verimli kullanabilecekler. Bu esnada makine öğrenmesinin ve yapay zekânın istihbarat faaliyetlerine entegrasyonu, değiştirilmiş ya da manipüle edilmiş verilerden kaynaklanan aldatmalar için de yeni fırsatlar yaratma potansiyeline sahip. "Kontra-yapay zekâ" yaygınlaşabilir, dost bilinen teknoloji anında düşmana dönüşebilir. İstihbarat birimlerinin, analistlerin önlerindeki verinin bir rakip tarafından değiştirilmiş olma olasılığına karşı eğitimli olması da önemli.

Sosyal Medya İstihbaratı

Günümüzün en popüler büyük veri kaynaklarından biri olan sosyal medya, bireysel olarak paylaştığımız verileri sadece ticari unsurlar için değil aynı zamanda askeri istihbarat anlamında da önemli bir hale taşıyor. İnternetten yaptığınız bir alışveriş sonrasında "Şunları da beğenebilirsiniz" sorusu karşınıza çıkmıyor mu? Basit bir satın alma eylemi (hatta sadece araştırma) bir veri analizine giriyor ve bu analiz milisaniyeler içinde size 40 yıllık dostunuzmuşçasına tavsiyede bulunabiliyor. Üstelik bulunduğu tavsiye de büyük ölçüde ilginizi çekecek bir nesneyle ilgili oluyor. Artık alıştığımız bu durum stratejik olarak da kullanılabilme potansiyeline sahip. Kişisel verilerin internet üzerinden paylaşılması kontrolü zorlaştırdığı ölçüde manipülasyonu da mümkün kılabilecek bir zemin yaratıyor[2].

Bloglar, mikro bloglar, internet forumları, kullanıcı odaklı "sıkça sorulan sorular" alanları, podcast'ler, internet etiketleri, online oyunlar, arama motorları, sosyal medya siteleri… Hayatımızda fazlasıyla yer edinen tüm bu sanal araçlar ekseninde iki taraflı düşünmekte fayda var çünkü sosyal medya, askeri ve istihbarat operasyonları için son derece önemli oldukları kadar, aşırıcılar ve terör odakları için propaganda yapmak ve ideolojik mesajlarını yaymak anlamında da son derece etkili araçlar. DAEŞ Twitter'ı sempatizan kazanmak ve üyelerinin adreslerini bulmak adına seri ilan sayfaları gibi kullanmadı mı? ABD'deki "yalnız kurtlar"* Facebook, LinkedIn ve Twitter gibi sosyal medya sitelerini kullanarak uyandırılmadı mı? Sözün özü sosyal medya sadece hükümetler tarafından değil terör birimleri tarafından da sıklıkla kullanılıyor, terör örgütlerinin istihbarat birimleri de sosyal medyayı kullanıyor[3].

Veri koruma, gizlilik ve bilgi güvenliği politikaları konusunda bağımsız araştırmalar yürüten Ponemon Institute, IBM'in sponsor olduğu ve 10 ülkeden 314 şirketi kapsayan "Veri İhlali Maliyet Analizi" raporunda, veri ihlali maliyetinin bir senede yüzde 15 oranında artarak 3,5 milyon dolara yükseldiğini söylüyor. Şirketlerin yüzde 40'lık bir bölümünün son iki yıl içinde maddi güvenlik ihlali yaşadığını ve bu ihlallerin yüzde 80'ni istihbarat bilgisiyle engellenebileceğini açıklıyor[4].

---

1 https://www.rand.org/pubs/external_publications/EP67661.html
2 The Role of Social Media in The Intelligence Cycle, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc248/p804615_A1b.pdf
3 https://www.usnews.com/opinion/blogs/world-report/2015/08/14/when-social-media-meets-military-intelligence
4 https://www.ponemon.org/library/2015-cost-of-data-breach-global
* Herhangi bir terör örgütü ile "fiziki" teması olmayan, ancak onun ideolojik görüşlerini paylaşan, yöntemlerini benimseyen veya kendi inanç ve ideolojisiyle, kendi eylem kararını alan tek kişilik terör eylemine verilen ad.

İnternet ve teknolojinin sunduğu imkânlar ulusal güvenlik ve istihbarat alanlarında inanılmaz fırsatlar barındırdığı gibi bir silah gibi de kullanılabiliyor. Günümüzde saldırıların büyük kısmı kimlik hırsızlıkları üzerinden gerçekleştiriliyor. Açık kaynak istihbaratı (OSINT), sosyal medya istihbaratı (SOCMINT) gibi alt uzmanlıklar gelişiyor ve Bilişim Teknolojileri Birimleri bu yeni uzmanlıklarla ilgili işe alım ve teknik ekipman kaynağını arttırma yoluna gitmedikce şirketler ve kurumların siber uzayda karşılaştıkları tehlikenin boyutu her geçen gün artıyor.