thinktech
STM Teknolojik Düşünce Merkezi

Anayurt Güvenliğinde Son Teknolojiler

Eylemde sınır tanımayan terör örgütleri, toplumsal güvenlik algısını zedeleyen bireysel katliamlar, izlenmesi güçleşen uluslararası suç şebekeleri, gelişen iletişim olanaklarıyla anlık olarak örgütlenebilen ve toplumsal huzursuzluk yaratabilecek eylemler düzenleyebilen gruplar, küresel ısınmaya bağlı olarak sıklaşan ve yarattığı yıkım giderek artan aşırı iklim olayları ve doğal felaketler, ekonomiye büyük zararlar veren siber saldırılar…

Günümüzde giderek sıklaşan ve karmaşıklaşan iç güvenlik tehditleri, anayurt güvenliği faaliyetinden sorumlu kurum ve kuruluşların klasik yöntem ve kabiliyetlerle cevap verebileceğinin ötesine geçti. Üstelik kamuoyu baskısı altındaki bu kurumlar maliyet ve insan kaynağı sıkıntısı çekiyor. Bu nedenle anayurt güvenliği kurumları gelişmiş teknolojiler kullanarak verimlilik ve kabiliyetlerini artırmaya, öte yandan kurumlar arası eşgüdümü güçlendirerek anayurt güvenliği zümresinin (emniyet, istihbarat, sahil güvenlik, itfaiye vb.) güvenilirliğini artırmaya çalışıyor.

Neyse ki yeni ve giderek olgunlaşan teknolojiler, anayurt güvenliği zümresine hiç olmadığı kadar yardımcı oluyor. Genişbant bağlantılar, nesnelerin interneti uygulamaları, gelişmiş görüntü toplama cihazları, otonom nesneler (İHA, otonom araçlar ve robotlar) anayurt güvenliği kurumlarının “büyük resmi” görmesini sağlarken, büyük veri analitiği, yapay zekâ, bilgisayarlı görselleştirme, artırılmış gerçeklik, sanal gerçeklik ve diğerleri, anlık ve isabetli karar alma mekanizmalarının oluşturulmasına yardım ediyor.

Büyük Veri ile “Azınlık Raporu” Gerçek Oluyor

Tüm dünyada dijitalleşme, mobil ve kablosuz bağlantıların artmasına paralel olarak büyük veri patlaması yaşanıyor. İnternet, mobil iletişim, giyilebilir elektronik ürünleri, internet bağlantılı kara araçları, akıllı ev cihazları ve nesnelerin interneti uygulamaları, hemen her sektörde olduğu gibi, anayurt güvenliğinden sorumlu kurumlara da benzersiz fırsatlar sunuyor.

Veri toplanması, saklanması, analizi ve görselleştirilmesinde sağlanan teknolojik gelişmeler, anayurt güvenliği kuruluşlarına daha fazla veri elde edip, daha fazla eyleme geçirilebilir istihbarat üreterek gerçek zamanlı karar alma süreçlerini destekliyor. Hatta bu verilerden elde edilecek modellemeler herhangi bir suçun, terör saldırısının, afetler ve kitlesel olayların önceden tahmin edilip önlenmesini bile sağlayabiliyor.

Gelişmiş büyük veri analizi teknikleri sayesinde Steven Spielberg’in 2002 tarihli *Azınlık Raporu* filminde olduğu gibi suçu işlenmeden önceden tahmin etme kabiliyetine sahip emniyet teşkilatları bugünden oluşmaya başladı.

Örneğin Türkiye'de STM Savunma Teknolojileri ve Mühendislik A.Ş., siber saldırılara karşı proaktif ve önleyici bir sistem geliştirdi. STM'nin Siber Füzyon Merkezi bünyesindeki Siber Operasyon (Harekât) Merkezi adı verilen bu sistem, farklı güvenlik kaynaklarından gelen kayıtları topluyor, inceliyor ve bir tehdit ya da anomali oluşturup oluşturmadığını analiz ediyor. İngiltere'de ise polis teşkilatı, büyük veri analizine dayalı "Predictive Crime Mapping" (Öngörülebilir Suçları Haritalamak) adı verilen bir sistemi 2018'de tüm polis teşkilatının kullanımına sundu. Sistem, suç tipi, suçun işlendiği yer ve zamanına ilişkin veriler girildiğinde, bunları geçmiş suç verileriyle karşılaştırarak suç işlenmesi olasılığı yüksek bölgelerin tespit edilmesini kolaylaştırıyor[1]. Benzeri önceden tahmin analizleri sayesinde ABD'nin Lancester kentinde suç oranının dört yılda yüzde 42, Memphis kentinde ise yüzde 28 azaldığı belirtiliyor[2].

İstihbaratın Yüzde 90'ı Dijitalleşti

Büyük veri ve büyük veri analizi teknolojisi özellikle istihbarat kuruluşlarının nitelikli ve eyleme geçirilebilir veri ihtiyacının karşılanması konusunda büyük potansiyel taşıyor. İstihbarat kuruluşlarının bilgi edinme faaliyetleri geleneksel olarak şu unsurlara dayanmaktaydı:

- Diplomatik ve insani ilişkilere (İnsani istihbarat -HUMINT);
- Gözetleme uçakları, uydular ve insansız hava araçları (İHA) ile havadan toplanan verilere (Coğrafi konum istihbaratı -GEOINT);
- Akustik, elektromanyetik, kızılötesi ve benzeri gelişmiş algılama cihazlarının sunduğu olanaklara (Ölçüm ve akustik istihbarat -MASIST);
- Terör ve suç örgütleriyle düşman hedeflerinin mali işlemlerinin takibine (Finansal İstihbarat -FININT);
- Elektronik haberleşme takibine (SIGINT);
- Kamuoyuna açık medya haberleri ve yayınların takibine (OSINT).

İstihbarat kuruluşlarının bilgi edinme faaliyetleri, bu kuruluşların faaliyetlerine ilişkin medya, edebiyat ve sinemada oluşturulan yanıltıcı gizeme karşın, yüzde 90 oranında açık kaynak istihbaratına (OSINT) dayanıyor[3]. Ancak günümüzde OSINT faaliyetlerini yürütmek hayli güçleşti. Zira her gün milyonlarca haber metni, milyarlarca sosyal medya gönderisi, binlerce akademik makale veya yayını takip etmek herhangi bir istihbarat örgütünün kabiliyetlerinin ötesine geçti. İnternetin, dijital bağlantılılığın ve sosyal medya platformlarının yaygınlaşması OSINT faaliyetlerinin dijitalleşmesini bir zorunluluk haline getirdi. Bugün OSINT faaliyetlerinin önemli bölümü bilgiye erişme faaliyetleri oluşturmuyor. Bilgi patlaması yaşanan bir çağda istihbarat örgütleri, daha çok, bölük pörçük verilerin anlamlı hale getirilmesi, açık kaynaklarda paylaşılan bilgilerin doğrulanması ve kaynağın tespiti ile meşgul oluyor.

İstihbarat birimleri bu ihtiyacı karşılamak üzere bünyelerinde OSINT birimleri oluşturduğu gibi bu birimlerin nitelikli bilgiye ulaşabilmeleri için OSINT yazılımları geliştiriyor veya geliştirilen platformları kullanıyorlar. Bu yazılımlar, akademik yayınlardan medya haberlerine, internet sitesi içeriklerinden sosyal medya mesajlarına, ticari olarak yayınlanmamış belgelerden, suç amaçlı derin internet paylaşımlarına (Deepweb veya Darknet) kadar milyonlarca kaynaktan elde edilen verileri topluyor ve analiz ediyor. Böylece internet ortamında tamamen alakasız gibi duran, çok çeşitli veriler istihbarat tekniklerince süzülerek istihbarat bilgisi olarak kullanıcıya sunuluyor. Veri toplanması ve analizinin otomasyonuyla analistler çok sayıda kaynaktan elde edilen verileri neredeyse gerçek zamanlı olarak analiz edebiliyor.

---

1 https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html
2 https://channels.theinnovationenterprise.com/articles/how-predictive-analytics-is-revolutionising-public-safety
3 https://fas.org/irp/nsa/ioss/threat96/part02.htm

Örneğin ABD Ulusal Güvenlik Ajansı (NSA), Mayıs 2019'da bu amaçla geliştirdiği Ghidra yazılımını tanıttı. Yapılan açıklamaya göre Ghidra sadece açık kaynakların taranmasında değil, kötü amaçlı yazılımların kimler tarafından yazıldığını tespit etmekte de kullanılıyor[4]. ABD Merkezi Haberalma Teşkilatı CIA'in ise sosyal medya mesajlarını analiz ederek olası saldırıları tahmin edebilmek için Maltego adı verilen bir yazılım kullandığı belirtiliyor[5]. Shodan, Google Dorks, The Harvester ve Metagoofil diğer açık kaynak araması yapılabilen ve herkesin kullanımına açık yazılımlar[6]. Türkiye'de de STM Savunma Teknolojileri ve Mühendislik A.Ş., OSINT faaliyetlerinde kullanılabilecek bir büyük veri analitiği platformu geliştirdi. OVERA adı verilen bu platform, metin dosyalarından ve ilişkili ve ilişkisiz veritabanlarından akışkan kaynaklara, görüntü ve video kaynaklarına kadar her türlü veri kaynağından veri toplanması ve analiz edilmesi desteğini veriyor[7].

Bilgisayarın Gözünden Hiçbir Şey Kaçmaz

Anayurt güvenliği kurumları canlı veya olay sonrası görüntü incelemeleri için ciddi miktarda zaman ve kaynak harcıyor. Buna karşılık insanlar tarafından yapılan incelemelerde ilk 20 dakikadan sonra nesnelerin yarıya yakını gözden kaçıyor[8]. Görüntü takibi ve analizi günümüzde güçlü bir araç haline geldi. Sabit güvenlik kameraları, araç üstü kameralar, kameralı insansız hava araçları, polis üniforması üstüne monte edilebilen kameralar, sosyal medya videoları ve video akış hizmetleri anayurt güvenliği kurumlarına görüntülerin toplanması, modellemelerin çıkarılması ve analizler yapılmasında bulunmaz fırsatlar sunuyor.

"Bilgisayarla Görü (Computer Vision)" adı verilen yapay zekâ çözümleri, görüntü ve videoların eyleme geçirilebilir sonuçlar doğuracak şekilde yorumlamasını sağlıyor. Bazı ülkelerin anayurt güvenliğinden sorumlu kuruluşları, enerji santralleri, havaalanları ve limanlar gibi ekonomik açıdan kritik öneme sahip üstyapıları gözetim altında tutmak, suçları araştırmak ve terör saldırılarına hedef olabilecek spor müsabakaları, konserler, mitingler ve yürüyüşlerde güvenliği sağlamak üzere bilgisayarlı görü ve analiz sistemlerini kullanmaya başladı.

Bu ülkelerin başında ABD geliyor. Bilgisayarlı görü teknolojisinin ilk örneklerinden biri 2013'te ABD'de, Boston Maratonu bombalamasında saldırganların tespit edilmesi için kullanılmıştı[9]. ABD istihbarat kurumlarına bilimsel ve teknolojik araştırmalar yapması için kurulan IARPA'nın (The Intelligence Advanced Research Projects Activity), şehirlerde insanların hareketlerini takip etmeyi kolaylaştıran bir bilgisayarla görü algoritması üzerinde çalıştığı belirtiliyor[9]. Teknoloji şirketleri de bilgisayarla görü yazılımları geliştiriyor. Amazon'un Mart 2019'da tanıttığı "Rekognition" bunlardan biri. Video ve görüntülerden kimlik tespiti yapılabilmesini sağlayan Rekognition'ın, ABD istihbarat kurumları tarafından kısa sürede temin edildiği ileri sürülüyor[10]. ABD'de bazı yerleşim yerlerinde görüntülerden plakanın tanınmasını sağlayan yapay zekâlı bir cihaz trafikten sorumlu polislerin araçlarına yerleştirilmeye başlandı[11]. Canlı görüntüleri takip edip önleyici uyarılarda bulunan algoritmalar da geliştirildi. Merkezi ABD'nin California eyaletinde bulunan Vintra tarafından geliştirilen FulcrumAI adındaki video analiz çözümünün, yapay zekâ ve makine öğrenmesi algoritmalarıyla, canlı görüntüleri izleyerek anayurt güvenliği sorumlularına önleyici uyarılar verdiği belirtiliyor[8]. Royal Holding tarafından geliştirilen SWORD ise daha basit bir yapıya sahip. Bir akıllı cep telefonu kılıfı görünüşündeki SWORD, emniyet personeline 40 metre mesafeden silahlı kişilerin varlığı konusunda uyarıda bulunabiliyor. Bunun için emniyet personelinin akıllı cep telefonunun kamerasını açıp çevresini taratması yeterli oluyor[12].

---

4 https://www.wired.com/story/nsa-ghidra-open-source-tool/
5 https://www.theguardian.com/technology/2014/nov/12/tracking-isis-stalking-cia-big-brother-online-nsa
6 https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools
7 https://www.stm.com.tr/tr/urunler/overa
8 https://i-hls.com/archives/89945
9 https://i-hls.com/archives/91367
10 https://www.cnet.com/news/what-is-amazon-rekognition-facial-recognition-software/
11 https://i-hls.com/archives/89993
12 https://engt.co/2XEHZZS

Japon teknoloji devi Canon'un yan kuruluşlarından BriefCam tarafından geliştirilen Footprint de benzeri bir çözüm sunuyor. BriefCam'a göre Footprint, her türlü güvenlik kameraları görüntülerini hızla tarayarak şüphelileri tespit edebiliyor. Tutuklama kayıtları, telefon çağrıları ve daha pek çok kaynaktan verileri analiz edebilen web tabanlı bir analiz uygulaması olan Footprint, öngörüsel çözümlemeler yaparak güvenlik güçlerinin suçları önlemesine ve suçluların ivedi biçimde yakalanmasına yardımcı oluyor[13].

"Sosyal Fizik" Bilimi Güvenliğin Emrinde

Emniyet teşkilatı, istihbarat kuruluşları, afet müdahale ekipleri, itfaiye, ilk yardım kuruluşları, kıyı güvenliği kuruluşları ve diğer anayurt güvenliği kuruluşları yapay zekâ uygulamalarından da yaygın olarak yararlanmaya başladı. Accenture'ın 2018'de 25 ülkede yaptığı araştırmaya göre, anayurt güvenliğine ilişkin kurumların yüzde 70'i yapay zekâ uygulamalarına yatırım yaptı veya yapmaya hazırlanıyor[14].

Bu ilginin nedenini anlamak güç değil: Yeni teknolojiler, anayurt güvenliğinde, insan eliyle yapılması imkânsız analizleri mümkün kılıyor. İleri analiz teknikleri anayurt güvenliği yetkililerinin modeller yapabilmesini ve bağlantılar kurabilmesini sağlıyor. Örneğin Hollanda polisi, yapay zekâ sayesinde 1988'den bu yana faili meçhul kalmış 1500'den fazla vakanın dosyasını yeniden incelemeye alabildi. Yapay zekâ olmasa 30 milyondan fazla sayfa tutan bu dosyaların yeniden incelemesi 100 yıldan fazla sürebilirdi. Ancak bu vakaların dosyaları dijital ortama aktarıldıktan sonra yapay zekâ, yeni ipuçları ve tanık ifadelerinden da yararlanarak vakayı çözebiliyor. Hollanda polisi yapay zekâ sayesinde faili meçhul kalmış vakaların yüzde 40'nın çözülebileceğine inanıyor[15].

Yapay zekâ uygulamaları arasında ön plana çıkan makine öğrenmesi, sayılar, kelimeler, görüntüler, tıklamalar ve dijital olarak saklanabilen pek çok türde veriden elde edilen istatistikleri model çıkarmak için kullanıyor. Bu algoritmalar yaptıkları analizlerden öğrendiklerini sonraki araştırmalarda veri olarak kullanabiliyor. Bu sayede anayurt güvenliği uzmanları, havaalanlarına yönelik saldırı tehdidini tespit edebiliyor, insansız hava araçlarını takip edebiliyor, olay yeri incelemelerinde farkındalıkları artıyor, şüphelileri kolaylıkla tespit edebiliyor.

New York polis teşkilatı bu tür bir algoritmayı 2006 yılından beri kullanıyor. Teşkilat uzmanlarının 10 yıllık bir çalışmayla geliştirdiği "Patternizr", bir makine öğrenmesi algoritmaları bütünü. Teşkilat Patternizr'ı suç olayları arasında modellerin çıkarılması için kullanıyor. Patternizr, bir olaydaki davranışsal kalıpları (Hedef seçimi, suç mahalline giriş yöntemi, başvurulan şiddet yöntemi, kullanılan silah ve aletler vb.) inceliyor ve bunları binlerce hırsızlık, kundaklama, gasp, cinayet ve diğer suçlara ilişkin kayıtlarla karşılaştırıyor. Karşılaştırma sonunda olası şüphelilerin bir listesi kısa sürede ortaya çıkarılıyor[16].

Davranış kalıplarının algoritmalarla incelenmesi farklı alanlarda da anayurt güvenliği birimlerinin elini rahatlatıyor. "Sosyal fizik" adı verilen yeni bir alan, kalabalıkların davranışlarını önceden tahmin etmek için matematiksel modelleri ve makine öğrenmesini kullanıyor. Örneğin, ABD'nin Massachusetts Institute of Technology (MIT) Üniversitesi bilim insanlarının geliştirdiği Endor adı verilen bir platform sosyal fizik prensipleri üzerine kurulu. Bir arama motoru gibi çalışan Endor'a gerekli veriler girildiğinde normalde çıkarılması haftalar sürecek modellemeler 15 dakikada elde ediliyor. Endor ile örneğin şehir trafiğinin yoğunlaşma modelleri çıkarılabiliyor. ABD'nin Savunma İleri Araştırma Projeleri Ajansı (DARPA), Endor ile cep telefonu verileri izlenerek patlak verebilecek protesto gösterilerinin önceden tahmin edilebildiğini belirtiliyor. Geliştiricinin iddiasına göre Endor, 15 milyon veri noktasını inceleyerek terör örgütü DAEŞ üyelerinin gizli 50 Twitter hesabını da tespit edebildi[17].

13 https://i-hls.com/archives/90764
14 https://voicesfrompublicservice.accenture.com/unitedkingdom/five-technology-trends-for-public-safety
15 https://thenextweb.com/the-next-police/2018/05/23/how-the-dutch-police-is-using-ai-to-unravel-cold-cases/
16 https://i-hls.com/archives/89939
17 https://i-hls.com/archives/80466

Öğrenen algoritmalar, sadece suçlular veya kamu güvenliği tehditlerini değil anayurt güvenliğinden sorumlu kişilerin sivillere karşı şiddetini de önceden tahmin edebiliyor. Örneğin, ABD'de polisin üniforma üstü kameraları (Bodycam) üreticisi Axon, Chicago Üniversitesi tarafından geliştirilen bir istatistik model üzerinden polis memurlarının stres seviyesini takip ediyor ve sapmalar olduğunda yetkililere haber veriyor. Böylece polis memurlarının sivillere karşı şiddet uygulamasının önüne geçme fırsatı yakalanıyor[18].

Robot Polisler Devriyede

Gelişen teknolojiler, insan kaynağı sorunları ile boğuşan anayurt güvenliği kuruluşlarının da yardımına koşuyor. Otonom nesneler olarak adlandırılan insansız kara ve hava taşıtlarıyla robotlar anayurt güvenliği alanında da kullanılıyor. Örneğin Çin'de kamuya açık alanlarda robot polis devriyeler görev yapmaya başladı. Robot polisler, yüz tanıma teknolojisi ile şüphelileri tespit ediyor ve elektro-şok silahları ile etkisiz hale getirip gözaltına alıyor[19]. ABD'de trafik kurallarını ihlal edenleri takip edip kenara çektirmeyi başaran bir robot trafik polisi prototipi Mayıs 2019'da tanıtıldı[20]. Robot polisler Singapur[21] , Birleşik Arap Emirlikleri'nin Dubai kenti[22] ve Hindistan'da[23] devriye gezmeye başladı.

İnsansız hava araçları ise, otonom nesneler arasında anayurt güvenliği kurumlarının en çok başvurduğu araçlar. Türkiye dahil pek çok ülkede İHA'lar, trafik kontrol, izleme, afet bölgelerine yardım malzemesi gönderilmesi, havaalanı güvenliğinin sağlanması ve benzeri görevlerde kullanılıyor[24]. Anayurt güvenliği kurumları İHA'ların veriminden oldukça hoşnut. Öyle ki Meksika'nın Ensenade kentinde polis teşkilatı envanterine katılan tek bir İHA'nın 500'den fazla tutuklama yapılmasına yardım ettiği, kentteki ev soygunlarında yüzde 30, genel suç oranında ise yüzde 10 düşüş sağladığı açıklandı[25].

Yakında İHA sürüleri (Drone Swarms) de anayurt güvenliği görevlerinde yer almaya başlayacak. ABD'de DARPA, özellikle arama ve kurtarma misyonlarında kullanılmak üzere, yapay sinir ağları ile eşgüdümlü olarak hareket edebilen İHA sürüleri geliştirmek üzere çalışıyor[26].

GBT Artık TakBul ile Taranıyor

Anayurt güvenliği alanında kullanımı hızla artan teknolojilerden biri de artırılmış gerçeklik (AR). AR teknolojisi, durumsal farkındalığını artıracak çözümleri ile anayurt güvenliği birimlerinin en önemli yardımcısı haline geliyor. Örneğin Türkiye'de Jandarma Genel Komutanlığı, SimBT firması tarafından geliştirilen "TakBul" AR gözlüklerini kullanmaya başladı. TakBul ile güvenlik birimleri, kişilerin yüzlerini, kimlik kartlarını ve araç plakalarını birkaç saniye içinde tarayabiliyor ve şüphelileri tespit edebiliyor. TakBul aynı zamanda, araç ve motosiklet plakalarını ve kimlik numaralarını sesli olarak da sorgulayabiliyor[27]. İngiliz polisi, Black Marble tarafından Microsoft HaloLens akıllı gözlükleri için geliştirilen bir AR çözümü ile suç mahalinin tamamının üç boyutlu haritasının çıkarılmasını sağlıyor[28]. Çin'in başkenti Pekin'de polis Şubat 2018'den bu yana, yüz ve plaka tanıma teknolojisine de sahip olan AR gözlüklerini denemeye başladı. LLVision tarafından geliştirilen gözlük ile polis memurları kuşkulanılan şahısların aranılan 10 bin kişilik listede olup olmadığını 100 milisaniyede öğrenebiliyor, çalıntı araçları plakalarından tespit edebiliyor[29].

18 https://i-hls.com/archives/91337
19 https://www.ozy.com/fast-forward/china-turns-to-robotic-policing/86559
20 https://futurism.com/the-byte/police-robot-pull-over-driver
21 https://www.youtube.com/watch?v=It2L9Vxrp_o
22 https://www.bbc.com/news/technology-41268996
23 https://futurism.com/india-robot-police-officer
24 https://www.uavsystemsinternational.com/top-drones-for-law-enforcement-best-police-drone-fleet/
25 https://www.wired.com/story/ensenada-mexico-police-drone/
26 https://www.bbc.com/news/technology-47555588
27 http://www.simbt.com.tr/urunler/id/28/takbul_gozluk
28 https://arpost.co/2018/08/22/improving-law-enforcement-and-security-through-vr-and-ar-technology/
29 https://www.businessinsider.com/china-police-using-smart-glasses-facial-recognition-2018-3