Sayı: 16

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ VE İLETİŞİM TEKNOLOJİLERİNDE GELİŞMELER, YENİLİKLER VE ÖRNEK ÇALIŞMALAR

EKİM-KASIM-ARALIK 2024

SEKRÖREL ARAŞTIRMA VE STRATEJİ GELİŞTİRME DAİRESİ BAŞKANLIĞI

İÇİNDEKİLER

ÖNSÖZ

Dünyada haberleşme teknolojilerinin ve altyapılarının büyük bir hızla geliştiği, dijital dönüşümün tüm sektörlerin gelecek vizyonlarının belirleyici unsuru haline geldiği, ülkemiz ve şirketlerimiz açısından çok önemli fırsatları da barındıran bir dijital dönüşüm süreci içindeyiz. 5G'den yapay zekâya, nesnelerin internetinden blok zincire, mobil finans ve ödeme uygulamalarından büyük veriye, verinin gizliliğine ve siber güvenliğe kadar geniş bir yelpaze içinde olan ancak tamamı birbiriyle ilişki içerisinde ve birbirini besleyerek gelişen yeni teknolojilerin, önümüzdeki dönemde ekonomimizi ve toplumsal yaşamımızı daha da fazla şekillendirmesi bekleniyor. Teknoloji alanında yaşanan hızlı gelişmeler ile gerek bireysel gerekse kurumsal olarak hepimiz için sosyal yaşam ve iş görme şekillerimiz değişiyor. Kişisel olarak sahip olduğumuz teknolojik imkânların, aldığımız hizmetlere de yansımasını bekliyor ve her alanda sayısal dönüşümü talep eder durumda oluyoruz. Bu sayısal dönüşümün gerçekleştirilmesinde temel unsurlardan birisi güçlü genişbant altyapısına sahip olmaktan geçiyor. Elektronik haberleşme altyapılarının her zaman daha iyiye götürülmesi ve herkese eşit şartlarda sağlıklı iletişim altyapısı sunulmasının sağlanması çabaları bu dönemde daha da artıyor.

Gelişen genişbant erişim imkânları ve artan hızlar her gün daha fazla cihazın internete bağlanmasını sağlarken internet üzerinden birbirleriyle veri alışverişi yapan cihaz sayısı da sürekli artmaktadır. Bunun neticesinde giyilebilir teknolojilerden yapay zekâ ile donatılmış cihazlara kadar pek çok yeni ürün sadece endüstriyel seviyede değil tüketici elektroniği pazarında da yerini alıyor. Günlük hayatımızı sürdürürken sağlıkla ilgili temel ölçümleri düzenli olarak yapan ve gerektiğinde bizi hatta doktorumuzu haberdar eden saatler, güvenlik, su ve elektrik gibi temel ihtiyaçları sensörler vasıtası ile otomasyon içinde yürüten akıllı şehir uygulamaları, suçluların tespiti için geliştirilen yapay zekâ temelli kamera güvenlik sistemleri gibi birçok ürün sektörde ardı ardına tanıtılıyor. Dünyanın en büyük şirketleri artık yatırımlarını yapay zekâ, büyük veri ve makineler arası iletişim gibi teknolojilere yapıyor. Bağlantılı cihaz sayısındaki artış beraberinde daha hızlı ve daha güçlü mobil altyapılara olan ihtiyacı da getiriyor. Günümüzde bu ihtiyacı karşılayacak teknolojilere bakıldığında 5G altyapısı bunların başında geliyor. Bugün ülkemiz gibi pek çok ülke 5G konusunda çalışmalar yürütüyor, gerekli spektrum tahsislerini gerçekleştiriyor ve 5G'nin yaygınlık kazanması için yatırımlar yapıyor. Önümüzdeki 5 yıl içerisinde dünyadaki aboneliklerin yaklaşık %20'sinin 5G abonesi olması ve 5G şebekelerinin 2026'ya kadar dünya nüfusunun %60'ını kapsaması bekleniyor. Hizmete başlamasının ardından geçen dört yılda 4.5G abonelerinin toplam mobil abonelere oranının %92'yi aşmış olması, 5G hizmetinin başladıktan sonra kısa süre içerisinde ülkemizde önemli bir abone sayısına ulaşacağını göstermektedir.

Ülkemizin bu teknoloji yarışında en önlerde olabilmesi için endüstri, akademi ve kamu kesiminde büyük bir çalışma sürmektedir. Bu anlayışla, genişbant internet hizmetinde neredeyse nüfusu kadar abonenin bulunduğu ülkemizde dinamik bir yapıda sürekli olarak evrilen teknolojik ve toplumsal şartlara uyum için en büyük faydayı sağlayacak stratejik, politik ve düzenleyici yaklaşımların geliştirilmesine katkı yapacağına inandığımız güvenilir ve kaliteli bilgi kaynaklarına erişimi değerli buluyoruz.

Bu doğrultuda Kurum olarak, uluslararası arenada bilgi ve iletişim sektöründeki teknolojik gelişmeleri ve önemli olayları yakından takip ederek, sizlerle paylaşmak amacıyla 2021 yılı ocak ayından itibaren üç aylık periyotlar halinde "Bilgi ve İletişim Teknolojilerinde Gelişmeler, Yenilikler ve Örnek Çalışmalar" bültenini yayımlamaya başladık. Bugüne kadar yayımlanan on beş sayıya paydaşlarımızdan ve sektöre ilgi duyan kişiler tarafından olumlu geri dönüşler alınması bundan sonraki bülten araştırmaları konusundaki motivasyonumuzu daha da artırıyor. Bu sayıda **"Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Siber Güvenlikte Yeni Nesil Tehditler ve Savunma Yöntemleri"** ile ilgili makaleleri de okuyabilirsiniz.

Bu kapsamda, bültenimizin 2024 yılı Ekim-Kasım-Aralık dönemine ait 16. sayısını sunmaktan memnuniyet duyuyoruz.

Ömer Abdullah KARAGÖZOĞLU
Kurul Başkanı

SEKTÖRDEN MAKALELER

Kore Yarımadası'ndaki Dijital Savaşta Yapay Zekâ ve Siber Güvenlik

Yazan: AI and Cybersecurity in Digital Warfare on the Korean Peninsula, EOM T. Y., Georgetown Journal of International Affairs, 10 Temmuz 2024

Gayri Resmi Tercümesi: Sektörel Araştırma ve Strateji Geliştirme Dairesi

2023 yılında Güney Kore kamu kurumları, benzeri görülmemiş bir siber saldırı artışıyla karşı karşıya kalmış; günlük saldırı sayısı 1,62 milyona ulaşmış ve bunların yüzde sekseninin Kuzey Kore kaynaklı olduğu bildirilmiştir. Savunma sanayi ve özel sektör gibi, bu saldırıları her zaman rapor edemeyen veya takip edemeyen farklı hedefler dikkate alındığında, Kuzey Kore'nin korsanlık girişimlerinin gerçek sayısının muhtemelen çok daha yüksek olduğu tahmin edilmektedir. Siber saldırılardaki bu artış, Kuzey Kore'nin ChatGPT gibi gelişmiş bilgi işlem ve yapay zeka (YZ) teknolojilerini kullanarak siber yeteneklerini geliştirdiğini ve YZ'nin siber casusluk ve sabotajdaki artan rolünü gözler önüne sermektedir.

Bu yeni saldırganlık biçimine yanıt olarak Güney Kore, siber tehditlere karşı koymayı hedefleyen, gelişmiş savunma stratejileri, uluslararası işbirliği ve en son teknolojilerin benimsenmesini içeren güncellenmiş Ulusal Siber Güvenlik Stratejisi'ni yayımlamıştır. Kore Yarımadası, teknolojinin hem ciddi güvenlik riskleri yaratabilen hem de bu riskleri önleyebilen iki yönlü doğasını yansıtarak bu alandaki ilerlemelerin çifte etkisini simgelemektedir. Bu makale, Güney Kore'nin siber güvenlik yaklaşımının; belirli siber saldırı örnekleri ile bunların geniş kapsamlı jeopolitik ve teknolojik sonuçlarına dayanarak, bu karmaşık dijital savaş çağında etkili karşı önlemler ve politika önerileri geliştirmeye yönelik değerli bilgiler sunduğunu savunmaktadır.

Kuzey Kore'nin Siber Savaş Stratejisi

Kuzey Kore'nin giderek daha sofistike hale gelen siber yetenekleri, özellikle 2014'te Sony Pictures'ın sistemlerine sızılmasıyla birlikte, dünya genelinde alarm zillerini çalmıştır. Bu olay, siber saldırıların özel şirketlere verebileceği ciddi zararları gözler önüne sermekle kalmamış, aynı zamanda devlet destekli siber terörizmin büyüyen tehdidine karşı bir uyarı niteliği taşımıştır.

Devlet altyapısını ve şirketleri hedef almanın yanı sıra Kuzey Kore'nin siber operasyonları mali kazanç ve yaptırımlardan kaçınma amacı taşımaktadır. Birleşmiş Milletler Güvenlik Konseyi'nin Mart 2024 tarihli raporuna göre, sanal varlık hırsızlığı Pyongyang için kazançlı bir yol haline gelmiştir. BM'nin tahminlerine göre, Kuzey Kore 2017-2023 yılları arasında silah programlarını finanse etmek için yasa dışı yollarla üç milyar dolar değerinde kripto para elde etmiştir. Bu stratejilerden biri, yurt dışında çalışan Kuzey Koreli teknoloji işçilerinin sahte özgeçmişler kullanarak küresel teknoloji geliştirme şirketlerinde işe girmeleri ve kazançlarını hükümete aktarmalarıdır. Kuzey Koreli bilgisayar korsanlarının ayrıca yazılım tedarik zincirlerine kötü amaçlı yazılım enjekte ettikleri ve şirket ağlarını felç eden fidye yazılımı saldırıları düzenleyerek ödeme talep ettiklerinden de şüphelenilmektedir. Mali kazanç amacı güden bu siber operasyonlar, geleneksel hedeflerin ötesine geçerek halktan kişilere yönelik rastgele saldırıları da kapsamaktadır. Örneğin, bilgisayar korsanları Güney Koreli bir çevrimiçi kripto para forumunun üyelerinden bilgi çalmış ve kimlik avı e-postaları kullanarak kullanıcıları, cüzdan kimlik doğrulama bilgilerini girmeleri konusunda kandırarak milyonlarca sanal para çalmıştır.

Kim Jong Un'un liderliğinde, Kuzey Kore stratejik çıkarlarla uyumlu sektörleri hedef almak amacıyla bilgisayar korsanlığı gruplarını kullanmaktadır. Ocak 2023'te Kim'in tahıl üretimini vurgulamasının ardından, bilgisayar korsanları üç Güney Koreli tarım kurumunu hedef alarak gıda araştırma verilerini çalmıştır. Kim'in Temmuz ve Ağustos 2023'te deniz kuvvetlerini geliştirme hedefini açıklamasının ardından ise Kuzey Koreli bilgisayar korsanları dört Güney Koreli gemi inşa şirketine sızmıştır. Benzer şekilde, Ekim 2023'te Kim'in insansız hava aracı üretimini destekleme planlarını duyurmasının ardından, Kuzey Koreli korsanlar Güney Koreli drone şirketlerinden motor verilerini çalmıştır.

Şubat 2024'te yayımlanan bir siber güvenlik tehdit istihbarat raporunda Microsoft, Kuzey Koreli bilgisayar korsanlarının, potansiyel hedefleri belirlemek ve araştırmak için OpenAI'nin büyük dil modellerini kullandıklarını ve ardından otomatik olarak kimlik avı sayfaları oluşturduklarını açıklamıştır. Microsoft, 2023 yılı boyunca aktif olan ve "Emerald Sleet" adlı Kuzey Koreli bir tehdit grubunu tespit etmiş ve bu grubun Microsoft yapay zeka ürünlerine erişimini yasaklamıştır. Bu grubun, "Kimsuky" ve "Velvet Chollima" gibi isimlerle bilinen ünlü hacker kolektifleriyle bağlantıları olduğu belirtilmiştir. ABD İç Güvenlik Bakanlığı'na bağlı Siber Güvenlik ve Altyapı Güvenliği Ajansı, Kimsuky'yi 2012'den beri Kore Yarımadası, nükleer politika ve Kuzey Kore'ye yönelik yaptırımlarla ilgili istihbarat toplamak amacıyla Güney Kore devlet kurumlarını ve

Kore-ABD-Japonya eksenindeki uzmanları hedef alan bir Kuzey Koreli hacker grubu olarak tanımlamaktadır.

Bu örnekler, Kuzey Kore'nin kitlesel kötü amaçlı yazılım üretimi ve sofistike kimlik avı saldırıları için gelişmiş yapay zekâ teknolojilerini kullanmasıyla şekillenen ve siber operasyonların gerektirdiği zaman ve çabayı önemli ölçüde azaltan gelişen tehdit ortamını gözler önüne sermektedir. Bu durum, Kuzey Koreli bilgisayar korsanlarının uzun vadeli ve hedefli siber saldırılara yönelik gelişmiş kalıcı tehdit (GKT) taktiklerini içeren koordineli çabalarının bir parçasıdır. GKT'ler, tek seferlik saldırılardan veya sıradan kimlik avı dolandırıcılıklarından farklı olarak Kuzey Koreli korsanların uzun süre fark edilmeden ağlarda kalmalarına olanak tanımakta; böylece değerli verileri ele geçirme ve kritik sistemleri tehlikeye atma imkânı sunmaktadır. Bu siber saldırıların etkileri, yalnızca geçici operasyonel aksaklıklarla sınırlı kalmayıp uzun vadeli ulusal güvenlik ve ekonomik istikrarı da tehdit etmekte, sağlam siber güvenlik savunmalarına duyulan ihtiyacı ve müttefikler arasında proaktif tehdit istihbaratı paylaşımının önemini ortaya koymaktadır.

Güney Kore'nin Stratejik ve Diplomatik Yanıtı

Kuzey Kore'nin siber saldırganlığına karşılık olarak Güney Kore, Şubat 2024'te Kuzey'den gelen çok yönlü siber tehditleri bertaraf etmek üzere kapsamlı şekilde güncellenmiş bir Ulusal Siber Güvenlik Stratejisi yayımlamıştır. Bu strateji, proaktif bir savunma mekanizmasına, ülkenin kritik altyapılarının siber saldırılara karşı güçlendirilmesine ve sağlam bir siber güvenlik çerçevesi oluşturmak için uluslararası iş birliğine daha fazla vurgu yapmaktadır. Güney Kore, bu stratejik yaklaşım sayesinde yalnızca kendi dijital güvenliğini sağlamayı değil, aynı zamanda Kuzey Kore kaynaklı siber tehditlerin artışı karşısında uluslararası toplumun istikrar ve güvenliğine katkıda bulunmayı hedeflemektedir.

Güney Kore, siber güvenliğin küresel bir mesele olduğunun ve güçlü ittifakların öneminin farkında olarak, ortak siber güvenlik çerçeveleri ve anlaşmalar geliştirme çabalarını sürdürmektedir. Bu çabaların bir örneği, Güney Kore ve Amerika Birleşik Devletleri'nin Nisan 2023'te başlattığı Stratejik Siber Güvenlik İşbirliği Çerçevesi olup, siber tehditlere karşı koyma ve kritik istihbarat paylaşımı konusundaki kararlılıklarının bir göstergesidir. Aralık 2023'te ise Güney Kore'nin ABD ve Japonya ile birlikte Kuzey Kore'nin siber faaliyetlerine dair üçlü görüşmelere katılması, Kuzey Kore'nin siber saldırganlığına karşı iş birliğini güçlendirmiştir. Bu görüşmeler, savunma stratejilerinin uyumlaştırılmasını ve ülkelerin altyapılarını güçlendirmeyi amaçlamış; ayrıca siber tehditleri caydırmak için birleşik bir yaklaşımı ortaya koymuştur.

Uzun Vadeli Etkin Siber Güvenliğin Sağlanması

İş birliğine dayalı savunmalar oluşturmadaki başarılarına rağmen, Güney Kore'nin uluslararası siber güvenlik normları belirleme, gelişmiş tehdit tespiti ve sınır ötesi olaylara müdahale koordinasyonunu güçlendirme potansiyelini harekete geçirmesi gerekmektedir. Ülkenin, siber

güvenlik ve yapay zeka güvenliği konularında Mayıs YZ Seul Zirvesi ve Mart Demokrasi Zirvesi gibi önemli etkinliklerde küresel politika yapıcılar ve girişimcilerle proaktif olarak tartışmalara öncülük etmesi, dijital alanlarda uluslararası hukuk savunuculuğunda iyi bir konumda olduğunu göstermektedir. Birleşmiş Milletler tartışmalarına aktif katılımıyla birlikte Güney Kore, BM Güvenlik Konseyi'nin daimi olmayan bir üyesi olarak, barış zamanında dijital davranış normları oluşturulmasına öncülük etmektedir. ABD Siber Komutanlığı tarafından düzenlenen çok uluslu Siber Bayrak tatbikatlarına katılımı ve Seul Savunma Diyaloğu gibi uluslararası güvenlik forumlarında siber güvenlik konularını ele alması da Güney Kore'nin, küresel siber güvenlik işbirliğini ve tehditlere yanıt verme kapasitesini güçlendirme konusundaki aktif rolünü ve liderliğini vurgulamaktadır.

Bu diplomatik ve güvenlik kanallarını kullanarak Güney Kore, güvenli ve istikrarlı bir siber uzay ihtiyacı konusunda küresel bir fikir birliği oluşturabilir. Aynı zamanda, siber güvenlikteki uzmanlığını ve kaynaklarını gelişmekte olan ülkelerle paylaşarak jeopolitik konumunu güçlendirebilir, daha sağlam ittifaklar kurabilir ve küresel siber istikrarı teşvik edebilir. Bu yaklaşımlar, özellikle Kuzey Kore kaynaklı siber güvenlik sorunlarının ortak eylem ve sorumluluk gerektiren küresel bir sorun olduğunu kabul etmektedir.

Yapay zekanın siber güvenliğe entegrasyonu, Güney Kore için önemli teknolojik fırsatlar sunmaktadır. Yapay zekâdaki ilerlemeler, siber güvenlik savunmalarını geliştirme, sofistike tehditleri daha etkili şekilde tespit etme ve olaylara insan kabiliyetlerinin ötesinde hızla yanıt verme gibi alanlarda dönüştürücü bir potansiyel taşımaktadır. Örneğin, yapay zekâ destekli anomali tespit sistemleri, siber saldırıların belirtilerini geleneksel yöntemlere göre çok daha hızlı algılayabilir. Ayrıca, yapay zekâ sayesinde Güney Kore siber güvenlik güçleri, geniş veri kümelerini analiz ederek potansiyel siber saldırıları öngörebilir ve önleyici tedbirler alabilir. Güney Kore'nin Ulusal Siber Güvenlik Stratejisi de gerçek zamanlı tehdit tespiti ve müdahalesi için yapay zekâ güdümlü sistemlerin entegrasyonuna vurgu yapmaktadır. 2024 yılı sonuna kadar faaliyete geçmesi planlanan Yapay Zekâ Güvenlik Enstitüsü gibi girişimler de bu ileri teknolojilerin geliştirilmesi ve uygulanmasını hedeflemektedir.

Bununla birlikte, yapay zekânın siber güvenlik stratejilerine entegrasyonu, verilerin kapsamlı toplanması ve analiz edilmesi bireysel haklara yönelik ihlal riskleri yaratabileceğinden, etik ve gizlilik ikilemlerini de beraberinde getirmektedir. Güney Kore, siber güvenliği desteklemek için yapay zekâdan faydalanırken aynı zamanda bu teknolojinin getirdiği riskleri en aza indirmek konusunda hassas bir denge kurmalıdır. Bu, etik yapay zekâ çerçeveleri geliştirme, dijital normlar konusunda uluslararası iş birliğini teşvik etme ve teknoloji geliştiriciler, güvenlik uzmanları ve politika yapıcılar arasında sürekli bir diyalog sürdürmeyi içeren bütüncül bir yaklaşımı gerektirir. Böyle bir strateji, Güney Kore ve müttefiklerinin, demokratik ilkeler ve insan haklarını koruyarak siber güvenlik çabalarını yapay zekânın potansiyelinden yararlanarak güçlendirmelerine olanak tanıyacaktır.

Sonuç

ABD'nin Siber ve Gelişen Teknolojilerden Sorumlu Ulusal Güvenlik Danışman Yardımcısı Anne Neuberger, Kuzey Korelileri "gelişen teknolojiden yararlanma konusunda en yaratıcı ve yenilikçi olanlar" arasında göstermektedir. Kuzey Kore'den gelen siber tehditlerin artması ve yapay zekanın hem saldırganlık hem de savunma alanındaki kritik rolü, Kore Yarımadası'nda siber dayanıklılığı artırmanın aciliyetini ve karmaşıklığını gözler önüne sermektedir. Güney Kore'nin Ulusal Siber Güvenlik Stratejisi, bu tehditlere karşı güçlü, proaktif bir yanıt sunarak, uluslararası iş birliği, ileri teknolojilerin benimsenmesi ve güçlü savunma mekanizmalarının oluşturulmasına odaklanmaktadır.

Ancak, siber tehditlerin değişken ve dinamik yapısı, sürekli bir tetikte olma, yenilikçilik ve iş birliği ihtiyacını doğurmaktadır. Üretken yapay zekâ, iki ucu keskin bir kılıç gibi etkiler yaratırken, ülkeler önleyici siber güvenlik yatırımları yapmazsa, yapay zekâ çağında güç dengesi hacker gruplarının lehine değişebilecektir. Bu yüzden, görünüşte sakin dönemlerde dahi siber güvenlik bilinci ve yatırımlarının artırılması hayati önem taşımaktadır. Dünya genelinde bu zorluklarla mücadele devam ederken, Güney Kore'nin deneyimleri ve stratejileri, dijital çağda siber çatışma ve savunma dinamiklerine ilişkin önemli dersler sunmaktadır. Yapay zekanın potansiyelini savunma stratejilerinde etkin bir şekilde kullanarak güvenli bir siber alan oluşturmayı hedefleyen küresel iş birliği ve stratejik bir yaklaşımın önemi böylelikle daha da vurgulanmaktadır.[1]

[1] https://gjia.georgetown.edu/2024/07/10/ai-and-cybersecurity-in-digital-warfare-on-the-korean-peninsula/

Siber Güvenliğin Ulusal Güvenlik Üzerindeki Etkisi: Eğilimler ve Politika Perspektifleri

Yazan: The Impact Of Cybersecurity On National Security: Trends And Policy Perspectives, Grady ANDERSEN, Georgetown Journal of International Affairs, 17 Ocak 2024

Gayri Resmi Tercümesi: Sektörel Araştırma ve Strateji Geliştirme Dairesi

Günümüzün hızlı dünyasında teknoloji, ulusal güvenlik de dahil olmak üzere hayatımızın her alanında önemli bir rol oynamaktadır. Ülkeler yeni zorluklarla karşılaşmaya devam ederken, gelişen teknolojiler uluslarımızı korumak için hem fırsatlar hem de engeller sunmaktadır.

Gelişen Teknolojiler Aracılığıyla Ulusal Güvenliğe Yönelik Zorlukların ve Fırsatların Keşfedilmesi

Zorluklar:

1. Siber Güvenlik Tehditleri:

Veri odaklı sistemlere olan bağımlılığın artmasıyla birlikte, siber güvenlik tehditleri ulusal güvenlik kurumları için her zaman mevcut bir zorluk haline gelmiştir. Cihazların, ağların ve altyapının birbirine bağlı olması, kötü niyetli aktörler tarafından istismar edilebilecek güvenlik açıklarını ortaya çıkarmaktadır. Karşılaşılan bazı temel zorluklar şunlardır:

- **Gelişmiş Kalıcı Tehditlerin (APT'ler) Yükselişi:** APT'ler, kritik altyapıyı ve hassas verileri hedef alan ve genellikle tespit edilemeyen sofistike, uzun vadeli saldırılar olduğundan önemli bir zorluk teşkil etmektedir.
- **Nesnelerin İnternetinin (IoT) Ortaya Çıkışı:** Daha fazla cihaz birbirine bağlandıkça, IoT bilgisayar korsanları için saldırı yüzeyini artırır ve olası ihlalleri önlemek için bu cihazların güvenliğini sağlamayı çok önemli hale getirir.
- **İçeriden Gelen Tehditler:** Ulusal güvenlik, hassas bilgilere erişimi olan ve bunları kötüye kullanabilecek kurum içindeki bireyler de dahil olmak üzere içeriden kaynaklanan riskleri de ele almalıdır.

2. Yapay Zeka (YZ) ve Etik:

YZ, ulusal güvenlik çabalarını geliştirmek için muazzam bir potansiyele sahip olsa da kullanımını çevreleyen etik kaygılar bir zorluk olmaya devam etmektedir. YZ teknolojilerinin geliştirilmesi ve uygulanması aşağıdaki gibi soruları gündeme getirmektedir:

- **Otonom Silahlar:** YZ'nin silah sistemlerinde kullanılması, karar verme yetkisini makinelere devrettiği için etik kaygıları da beraberinde getirmektedir. İstenmeyen sonuçların

ortaya çıkma potansiyeli ve insan sorumluluğunun olmaması, dikkatli bir değerlendirme gerektirmektedir.

- **Gizlilik:** YZ sistemleri genellikle büyük miktarda kişisel veriye dayanır ve bu verilerin nasıl toplandığı, depolandığı ve kullanıldığı ve kötüye kullanım veya istismar potansiyeli hakkında endişeleri artırır.
- **Algoritmik Önyargı:** YZ algoritmalarındaki önyargı riski, toplumsal eşitsizlikleri sürdürebilir, tarama ve profilleme gibi ulusal güvenlik süreçlerinde karar vermenin adilliğini ve doğruluğunu etkileyebilir.

Fırsatlar:

1. **Büyük Veri Analitiği:**

Verilerin çoğalması, ulusal güvenlik kurumlarına karar verme ve tehdit değerlendirmesi için değerli bilgiler toplama fırsatı sunmaktadır. Temel faydalar şunlardır:

- **Desenleri ve Anormallikleri Belirleme:** Büyük miktarda veriyi analiz etmek, potansiyel tehditlerin erken tespitini sağlayan desenleri ve anormallikleri ortaya çıkarabilir ve ulusal güvenlik çabalarını geliştirebilir.
- **Öngörücü Analiz:** Makine öğrenimi algoritmalarından yararlanarak, kurumlar geçmiş verilere dayanarak tehditleri tahmin edebilir ve azaltabilir ve böylece koruyucu önlemlerinin etkinliğini artırabilir.
- **Sosyal Medya İzleme:** Sosyal medya platformlarını izlemek, kurumların gerçek zamanlı istihbarat toplamasına, güvenlik tehditlerini belirlemesine ve kamuoyunun duygusunu izlemesine yardımcı olur.

2. **Blockchain Teknolojisi:**

Blockchain teknolojisi, ulusal güvenlik önlemlerini geliştirmek ve hassas bilgileri korumak için yeni fırsatlar sunmaktadır. Temel avantajlar şunlardır:

- **Veri Bütünlüğü ve Güvenliği:** Blockchain'in merkezi olmayan yapısı veri bütünlüğünü sağlayarak onu kurcalamaya karşı oldukça dirençli hale getirir. Bu, kritik altyapının ve hassas bilgilerin siber saldırılardan korunmasına yardımcı olabilir.
- **Güvenli İletişim:** Blok zinciri tabanlı iletişim platformları şifreli ve güvenli iletişim sağlayabilir
- **Şeffaflık ve Hesap Verebilirlik:** Blockchain'in şeffaf ve değişmez yapısı, ulusal güvenlik operasyonlarında hesap verebilirliği ve güveni artırır. Süreçlerin ve işlemlerin bütünlüğünü sağlayan bir denetim izi sağlayabilir.

Teknoloji hızla gelişmeye devam ederken, ulusal güvenlik kurumlarının zorluklara uyum sağlaması ve yeni teknolojilerin sunduğu fırsatlardan yararlanması gerekmektedir. Bu tartışmadan çıkarılacak temel sonuçlar şunlardır:

- Etkili siber güvenlik önlemleri kritik altyapının ve hassas verilerin korunması için çok önemlidir.
- Ulusal güvenlik operasyonlarında yapay zekâ teknolojileri uygulanırken etik hususlar ön planda olmalıdır.
- Büyük veri analitiği, erken tehdit tespiti ve karar alma süreçleri için değerli içgörüler sunar.
- Blockchain teknolojisi, ulusal güvenlik operasyonlarının güvenliğini, şeffaflığını ve hesap verebilirliğini artırabilir.

Ülkeler, bu yeni teknolojileri benimseyerek ve ilgili zorlukları ele alarak ulusal güvenlik aygıtlarını güçlendirebilir, dijital çağda vatandaşlarının güvenliğini ve refahını sağlayabilir.

Siber Güvenlik Politikası: Dijital Çağda Savunmaları Güçlendirmek

Siber Güvenlik Politikasının Önemi

Siber güvenlik politikası, bir kuruluşun dijital varlıklarını ve bilgilerini korumak için tasarlanmış bir dizi kural ve uygulamadır. Siber tehditlerin belirlenmesi, önlenmesi ve bunlara yanıt verilmesine ilişkin yönergeleri ana hatlarıyla belirtir. Sağlam bir siber güvenlik politikası uygulamak çeşitli nedenlerden dolayı gereklidir:

- **Hassas Verilerin Korunması:** Bir siber güvenlik politikası, hassas verilerin yetkisiz erişim, hırsızlık veya manipülasyona karşı korunmasına yardımcı olur. Buna kişisel bilgiler, finansal kayıtlar, iş stratejileri ve müşteri verileri dahildir.
- **Finansal Kayıpların Önlenmesi:** Kuruluşlar siber güvenliğe öncelik vererek mali kayıplara, yasal yükümlülüklere ve itibarlarının zedelenmesine yol açabilecek maliyetli siber saldırılardan kaçınabilirler.
- **İş Sürekliliğinin Sağlanması:** İyi tanımlanmış bir politika ile kuruluşlar siber olayların etkisini azaltabilir ve siber güvenlik risklerinin arttığı dönemlerde bile kesintisiz operasyonlar sağlayabilir.
- **Uyumluluk Gerekliliklerini Karşılamak:** Birçok sektörün belirli siber güvenlik düzenlemeleri ve uyumluluk standartları vardır. Yasal sorunlardan ve olası cezalardan kaçınmak için bu düzenlemelere uymak çok önemlidir.

Etkili Bir Siber Güvenlik Politikasının Temel Özellikleri

Etkili bir siber güvenlik politikası aşağıdaki temel özellikleri kapsamalıdır:

- **Risk Değerlendirmesi:** Kapsamlı bir risk değerlendirmesi, potansiyel güvenlik açıklarının ve tehditlerin belirlenmesine yardımcı olur. Uygun güvenlik önlemlerini belirlemek için kuruluşunuzun karşı karşıya olduğu belirli riskleri anlamak çok önemlidir.

- **Erişim Kontrolü:** Hassas veri ve sistemlere erişimin sınırlandırılması çok önemlidir. Güçlü kimlik doğrulama mekanizmaları, rol tabanlı erişim kontrollerinin uygulanması büyük önem taşırken, kullanıcı erişim ayrıcalıklarının düzenli olarak güncellenmesi gerekmektedir.
- **Teknoloji Altyapısı:** Ortaya çıkan tehditlere karşı koruma sağlamak için yazılımların, güvenlik duvarlarının ve antivirüs araçlarının düzenli olarak güncellenmesi gerekmektedir. Veri iletimini güvence altına almak için şifreleme tekniklerinin uygulanması önem taşımaktadır.
- **Çalışan Eğitimi:** Çalışanların kimlik avı e-postalarını tespit etme, güçlü parolalar oluşturma ve sosyal mühendislik tekniklerini tanıma gibi en iyi siber güvenlik uygulamaları konusunda eğitilmesi oldukça önemlidir. Düzenli güvenlik farkındalığı programları insan hatası riskini önemli ölçüde azaltabilmektedir.
- **Olay Müdahale Planı:** Bir siber saldırı durumunda hızlı ve etkili bir müdahale sağlamak için açık ve iyi tanımlanmış bir olay müdahale planının geliştirilmesi gerekmektedir. Bu plan, bir olayın kontrol altına alınması, hafifletilmesi ve kurtarılması için ayrıntılı prosedürleri içermelidir.

Güçlü Bir Siber Güvenlik Politikasının Avantajları

Güçlü bir siber güvenlik politikası uygulamak çeşitli avantajlar sağlar:

- **Siber** Tehditlerden Korunma: Güçlü bir politika, siber tehditlerin önlenmesine ve azaltılmasına yardımcı olarak veri ihlalleri ve diğer kötü niyetli faaliyetler riskini azaltmaktadır.

- **Geliştirilmiş Müşteri Güveni:** Siber güvenliğe bağlılığın gösterilmesi müşterilerde güven yaratır, itibarı artırır ve potansiyel olarak yeni iş fırsatları yaratmaktadır.
- **Düzenlemelere Uyumluluk:** Kapsamlı bir siber güvenlik politikası oluşturarak kuruluşlar sektöre özgü düzenlemelere uyabilmekte, olası yasal sorunlardan ve cezalardan kaçınabilmektedir.
- **Geliştirilmiş Dayanıklılık:** Güçlü bir siber güvenlik politikası, siber güvenliğe proaktif bir yaklaşım sağlayarak bir kuruluşun potansiyel siber olaylara karşı direncini artırmaktadır.

Sürekli gelişen dijital ortamda, dijital varlıkları ve bilgileri siber tehditlere karşı korumak hayati önem taşımaktadır. Güçlü bir siber güvenlik politikası uygulayarak;

- Hassas veriler korunabilmekte ve mali kayıplar önlenebilmektedir.
- İş sürekliliği sağlanabilmekte ve uyumluluk gereksinimleri karşılanabilmektedir.
- Güvenlik açıkları ve tehditlerin anlaşılması için bir risk değerlendirmesi yapılması gerekmektedir.
- Erişim kontrollerinin uygulanması ve teknoloji altyapısının düzenli olarak güncellenmesi önem taşımaktadır.
- Kapsamlı çalışan eğitimi ve farkındalık programlarını yapılmalıdır.
- Etkili olay yönetimi için iyi tanımlanmış bir olay müdahale planı oluşturulmalıdır.
- Gelişmiş koruma, müşteri güveni, uyumluluk ve esneklik avantajlarından yararlanılmalıdır.

Siber güvenliğin devam eden bir süreç olduğunu unutmamak gerekmektedir. Yeni tehditlere ve teknolojilere uyum sağlamak için siber güvenlik politikalarının düzenli olarak gözden geçirilmesi ve güncellenmesi gerekmektedir.

Boşluğu Kapatmak: Hükümet ve Özel Sektör Arasındaki İşbirliğini Geliştirmek

Bu makale, işbirliğinin faydalarını, temel zorlukları ve hükümet ile özel sektör arasındaki boşluğu kapatma stratejilerini incelemektedir.

İş Birliğinin Önemi

Hükümet ile özel sektör arasındaki işbirliğinin çok sayıda avantajı vardır:

- **Optimum kaynak tahsisi:** Kaynakları bir araya getirerek, her iki taraf da karmaşık zorluklarla başa çıkmada daha fazla verimlilik ve etkinlik elde edebilir. Bu, vergi mükelleflerinin parasının ve özel sektör yatırımlarının daha iyi kullanılmasına yol açabilir.
- **Uzmanlığa erişim:** Özel sektör genellikle hükümetlerin bilinçli kararlar almasına ve yenilikçi çözümler uygulamasına yardımcı olabilecek uzmanlaşmış bilgi, beceri ve deneyime sahiptir.

- **Hızlandırılmış inovasyon:** İşbirliği, fikir alışverişini teşvik ederek inovasyonun gelişmesi için bir ortam yaratır. Hükümetler ve işletmeler birlikte çalışarak teknolojik gelişmeleri daha hızlı bir şekilde ilerletmek için birbirlerinin güçlü yanlarından yararlanabilirler.
- **Ekonomik büyüme:** İşbirliği yeni iş kolları yaratmayı kolaylaştırır, yatırımları çeker ve ekonomik büyümeyi hızlandırır. Hükümet ve özel sektör çabalarını uyumlu hale getirerek işletmelerin gelişmesi için elverişli bir ortam yaratabilirler.

İşbirlikçi Çabalardaki Zorluklar

Hükümet ile özel sektör arasındaki iş birliği çok sayıda avantaj sunarken, ele alınması gereken zorluklar da vardır:

- **Farklı hedefler:** Hükümetin odak noktası genellikle kamu yararı iken, işletmeler karlılığa öncelik verir. Ortak bir zemin bulmak ve hedefleri uyumlu hale getirmek zor olabilir.
- **Bürokrasi:** Devlet kurumları bazen karar vermeyi yavaşlatabilen karmaşık bürokratik prosedürlerle çalışır. Bu, çevikliğin ve hızlı karar almanın önemli olduğu işbirlikçi çabalarda bir engel olabilir.
- **Bilgi paylaşımı:** Hükümet ile özel sektör arasında hassas bilgilerin paylaşılması, ulusal güvenlik ve rekabet avantajıyla ilgili endişeler göz önüne alındığında hassas bir konu olabilir.
- **Uyumsuz zaman çizelgeleri:** Hükümetler genellikle daha kısa vadeli hedefler ve amaçlar doğrultusunda çalışan özel işletmelerden daha uzun zaman çizelgelerinde çalışır. Bu zaman çizelgelerini uyumlu hale getirmek dikkatli planlama ve koordinasyon gerektirebilir.

Boşluğu Kapatma Stratejileri

Hükümet ve özel sektör arasındaki işbirliğini artırmak için belirli stratejiler kullanılabilir:

1. **Şeffaf iletişim:** Açık iletişim hatları kurmak, güven ve anlayış oluşturmak için hayati önem taşır. Düzenli diyalog ve bilgi paylaşımı, anlayıştaki boşlukları kapatmaya ve hedefleri uyumlu hale getirmeye yardımcı olabilir.
2. **İşbirlikçi platformlar:** Teknoloji platformlarından yararlanmak, bilgi paylaşımı ve projeler üzerinde birlikte çalışma için güvenli bir ortam sağlayarak iş birliğini kolaylaştırabilir. Bu, verimliliği artırabilir ve süreçleri düzene sokabilir.
3. **Kamu-özel sektör ortaklıkları:** Anlaşmalar yoluyla ortaklıkları resmileştirmek, iş birliği için bir çerçeve sağlayabilir. Bu ortaklıklar, belirli zorlukları ele almak veya belirli uzmanlık alanlarından yararlanmak üzere yapılandırılabilir.
4. **İş birliği için teşvikler:** Hükümetler, iş birliği girişimlerine özel sektör katılımını teşvik etmek için vergi avantajları veya hibeler gibi teşvikler sağlayabilir. Bu, farklı hedeflerin üstesinden gelmeye ve aktif katılımı teşvik etmeye yardımcı olabilir.

5. **Sektörler arası uzmanlık oluşturma:** Hükümetler, özel sektör deneyimi olan kişileri işe alarak ve bunun tersi şekilde fayda sağlayabilir. Yetenek ve uzmanlığın bu çapraz değişimi, karşılıklı anlayışı teşvik edebilir ve iş birliğini geliştirebilir.

Hükümet ve özel sektör arasındaki işbirliği, inovasyonu, ekonomik büyümeyi yönlendirmek ve toplumsal zorlukları ele almak için olmazsa olmazdır. Birbirlerinin güçlü yönlerinden yararlanarak, bu ortaklıklar optimum kaynak tahsisine, hızlandırılmış inovasyona ve artan ekonomik refaha yol açabilir. Ancak, etkili bir işbirliğini teşvik etmek için farklı hedefler ve bürokrasi gibi zorlukların üstesinden gelinmesi gerekir.

Şeffaf iletişim, işbirlikçi platformlar, kamu-özel sektör ortaklıkları ve işbirliği için teşvikler gibi stratejileri benimseyerek, hükümetler ve işletmeler açığı kapatabilir ve işbirliğini artırabilir. Sonuç olarak, daha parlak bir geleceğe giden yolu açacak olan her iki sektörün ortak çabalarıdır.

Siber Tehditlerin Yükselişi: Kapsam ve Sonuçları Anlamak

Siber tehditlerin kapsamını ve sonuçlarını anlamak, herkesin çevrimiçi güvenliği için çok önemlidir.

Siber Tehditlerin Kapsamı

Siber tehditler, bireyleri, işletmeleri ve hatta hükümetleri hedef alan, çevrimiçi olarak gerçekleştirilen çok çeşitli kötü amaçlı faaliyetleri kapsar. Siber tehditlerin yaygın olduğu bazı temel alanlar şunlardır:

- **Kimlik avı saldırıları:** Bu saldırılar, genellikle e-posta veya sahte web siteleri aracılığıyla bireyleri parolalar veya kredi kartı bilgileri gibi hassas bilgileri paylaşmaya kandırmayı içerir.
- **Fidye yazılımı:** Fidye yazılımı, bir kurbanın bilgisayarındaki dosyaları şifreleyen ve şifre çözme anahtarı karşılığında fidye talep eden bir tür kötü amaçlı yazılımdır.
- **Kötü amaçlı yazılım:** Kötü amaçlı yazılımlar bilgisayarlara bulaşabilir, kişisel bilgileri çalabilir veya bilgisayar korsanlarının sistemlere yetkisiz erişimini sağlayabilir.
- **Kimlik hırsızlığı:** Siber suçlular, dolandırıcılık faaliyetlerinde bulunmak için sosyal güvenlik numaraları veya banka hesap bilgileri gibi kişisel bilgileri çalabilir.
- **Veri ihlalleri:** Kredi kartı bilgileri veya müşteri kayıtları gibi hassas verilere yetkisiz erişim, önemli mali ve itibar kaybına yol açabilir.

Siber tehditlerin kapsamı hızla genişliyor ve düzenli olarak yeni taktikler ortaya çıkıyor. Bireylerin ve kuruluşların bilgili kalması ve kendilerini bu gelişen tehditlerden korumak için proaktif önlemler alması hayati önem taşıyor.

Siber Tehditlerin Sonuçları

Siber tehditlerin, bireyleri, işletmeleri ve hatta ulusal güvenliği etkileyebilecek geniş kapsamlı sonuçları vardır. İşte en dikkat çekici sonuçlardan bazıları:

- **Finansal kayıplar:** Siber saldırılar hem bireyler hem de kuruluşlar için önemli finansal kayıplara neden olabilir. FBI'a göre, siber suçlar yalnızca 2020'de mağdurlara 4,2 milyar dolardan fazla kayba mal olmuştur.
- **İtibar hasarı:** Veri ihlali veya başarılı bir siber saldırı, bir kuruluşun itibarına ciddi şekilde zarar verebilir, müşteri güvensizliğine ve iş kaybına yol açabilir.
- **Yasal etkiler:** Müşteri verilerini yeterli şekilde koruyamayan kuruluşlar, para cezaları ve davalar dahil olmak üzere yasal sonuçlarla karşı karşıya kalabilir.
- **Hizmetlerin kesintiye uğraması:** Başarılı siber saldırılar, sağlık, ulaşım veya enerji gibi temel hizmetleri kesintiye uğratarak bireylere önemli kesintiler ve potansiyel zararlar verebilir.
- **Fikri mülkiyet kaybı**: Siber suçlular genellikle ticari sırlar veya araştırma verileri gibi uzun vadede inovasyon ve rekabet gücü üzerinde olumsuz etkilere yol açabilen değerli fikri mülkiyetleri hedef alırlar.

Siber tehditlerin sonuçları finansal kayıpların ötesine geçerek hayatımızın çeşitli yönlerini etkiler. Bu nedenle, siber güvenlik önlemlerine öncelik vermek ve bu tehditlere karşı uyanık kalmak esastır.

Siber tehditlerin kapsamını ve sonuçlarını anlamak, kendimizi ve değerli bilgilerimizi korumak için hayati önem taşır. Bu kapsamda elde edilen bazı önemli çıkarımlara aşağıda yer verilmektedir:

- **Eğitimli kalın:** En son siber tehditler ve güvenlik uygulamaları konusunda kendinizi sürekli eğitin.
- **Güçlü parolalar kullanın:** Tüm çevrimiçi hesaplarınız için benzersiz ve karmaşık parolalar oluşturun.
- **İki faktörlü kimlik doğrulamayı (2FA) etkinleştirin:** Mümkün olan her yerde 2FA'yı etkinleştirerek ekstra bir güvenlik katmanı ekleyin.
- **Yazılımı güncel tutun:** Güvenlik açıklarını gidermek için işletim sisteminizi, virüsten koruma yazılımınızı ve diğer uygulamalarınızı düzenli olarak güncelleyin.
- **Çevrimiçi ortamda dikkatli olun:** Şüpheli bağlantılara tıklamaktan veya bilinmeyen kaynaklardan dosya indirmekten kaçının.
- **Verilerinizi yedekleyin:** Fidye yazılımı saldırılarına karşı korunmak için önemli dosyalarınızı düzenli olarak yedekleyin.

Bu uygulamaları uygulayarak, bireyler ve kuruluşlar daha güvenli bir çevrimiçi deneyim yaşarken siber tehditlere karşı savunmasızlıklarını önemli ölçüde azaltabilirler.[2]

[2] https://moldstud.com/articles/p-the-impact-of-cybersecurity-on-national-security-trends-and-policy-perspectives

Devletin Ulusal Güvenliğinin Bir Bileşeni Olarak Siber Güvenlik

Yazan: Cybersecurity As A Component of The National Security of The State, Olga VAKULYK vd., Journal of Security and Sustainability Issues, 30 Mart 2020

Gayri Resmi Tercümesi: Sektörel Araştırma ve Strateji Geliştirme Dairesi

Giriş

Bilgi ve iletişim teknolojilerinin gelişmesi, bunların kullanımında bir takım güvenlik risklerinin ortaya çıkmasına neden olmaktadır. Dünya nüfusunun yarısından fazlası internet kullanmaktadır. 2018 yılı sonu itibariyle dünya nüfusunun %51,2'si, yani 3,9 milyar kişi internet kullanmaktadır. Bu, daha küresel bir bilgi toplumuna doğru atılmış önemli bir adım olmakla birlikte, siber savunmanın geliştirilmesi ihtiyacını da ortaya koymaktadır. ITU Connect tarafından sağlanan verilere göre, 2023 yılına kadar küresel nüfusun %70'i interneti serbestçe kullanabilecek ve bu da daha fazla siber güvenlik ihtiyacını bir kez daha ortaya koyacaktır. İnternet'in güvenli kullanımı, bilgi arama, depolama ve yayma, bankacılık işlemleri ve diğer işlemlerin yürütülmesi, işletmelerin, kurumların, kuruluşların yazılım çalışmaları gibi önemli tehditler siber tehditler olarak nitelendirilmektedir. Bir süre önce, Ukrayna muhtemelen tarihindeki en ciddi siber saldırıyla karşı karşıya kaldı. "Petya", "Petya.A", "PetrWrap", "GoldenEye", "Diskcoder.C" olarak adlandırılan virüs, Ukrayna sistemleri arasında hızla yayıldı ve hükümet kurumlarını, havaalanlarını, bankaları, medya şirketlerini, teslimat hizmetlerini ve hatta eski Çernobil nükleer santralindeki radyasyon izleme sistemlerini geçici olarak devre dışı bıraktı. Aynı zamanda, ABD, Rusya Federasyonu, Büyük Britanya, Fransa ve Avustralya'daki bir dizi şirkete zarar verildi. Böyle bir durum, ilk olarak, bir dizi sürecin bilgisayar teknolojilerine olan mevcut bağımlılığını ve ikinci olarak da Ukrayna'nın siber saldırılara karşı güvensizliğini kanıtlamaktadır. Bu durum, resmi verilere göre 2018 yılı itibariyle ülkedeki Ulusal Siber Güvenlik Endeksi'nin %58,44 olmasıyla da teyit edilmektedir. Yani Ukrayna, temel siber tehditleri önleme ve siber suçlarla mücadele etme, ulusal bir siber savunma politikası geliştirme ve elektronik kimlik ve imza hizmetleri sağlama konusunda yalnızca %50 oranında hazırdır. Siber güvenlik konusunun devletin ulusal güvenliğinin bir bileşeni olarak incelenmesi bir tesadüf değildir, çünkü bugün Petya, Petya.A, PetrWrap, GoldenEye, Diskcoder.C olarak adlandırılan siber saldırılar sadece Ukrayna'da değil dünyanın diğer ülkelerinde de siber güvenliğin sağlanmasındaki mevcut boşlukları açıkça göstermiştir. Dolayısıyla, siber uzayın küreselleşmesi nedeniyle, istisnasız tüm devletler güvenli siber uzayla ilgilenmektedir.

Literatür Araştırması

Zine Homburger, siber güvenlik kapasitesinin geliştirilmesinin, bilgi ve iletişim teknolojilerine erişim ve kullanımla ilişkili dijital güvenlik risklerini azaltarak insanların, toplulukların

ve hükümetlerin kalkınma hedeflerine ulaşma yeteneklerini güçlendirmenin bir yolu olduğunu belirtmektedir. Bu tanım, sadece devletin istenen siber güvenlik seviyesine ulaşma potansiyelinin geliştirilmesini değil, aynı zamanda bilgi ve bilgisayar teknolojilerinin kullanımının olumsuz sonuçlarının en aza indirilmesini de vurgulamaktadır. Bununla birlikte, siber güvenliğin ulusal güvenliğin öncelikli alanlarından biri olarak algılanması, modern küreselleşmiş dünyada hem gelişmiş hem de gelişmekte olan devletler arasında yaygın olmasına rağmen, bugün bilimsel doktrinde "siber güvenlik" teriminin tek bir tanımı yoktur. Bu nedenle, G.V. Foros ve K.S. Kondrasheva, siber güvenliğin dijital ortamda bilgi ve bilgi altyapısının güvenliği olduğunu ve bilgi güvenliğinin; bilginin gizliliği, bilginin ve ilgili süreçlerin bütünlüğü, bilginin kullanılabilirliği, tüm bu süreçlerin izlenmesi gibi hedeflere ulaşılmasını sağladığını belirtmektedir. Buna karşılık Miguel Ferreira Da Silva, Fransa'da siber güvenliğin, depolanan, işlenen veya iletilen verilerin ve sistemlerin sağladığı ilgili hizmetlerin kullanılabilirliğini, bütünlüğünü veya gizliliğini tehdit edebilecek dış faktörlerle karşı karşıya kalabilecekleri bilgi sistemlerinin arzu edilen durumu olarak kabul edildiğini belirtmektedir. Rossouw von Solms ve Johan van Niekerk, siber güvenliğin siber uzayın, elektronik bilginin, siber uzayı destekleyen bilgi ve bilgisayar teknolojilerinin ve siber uzayın bir kullanıcısı olarak bir kişinin korunması olduğu gerçeğine odaklanmaktadır. "Siber güvenlik" kavramının bu şekilde anlaşılması, onu otomatik olarak bir diğer benzer tanım olan "bilgi güvenliği"nin özünden ayırmaktadır. Bilim adamlarına göre, bilgi güvenliğiyle değil de yalnızca siber güvenlikle ilgili olan mevcut tehditlerin canlı örnekleri şunlardır: (a) Modern toplumda büyük bir sorun haline gelen siber zorbalık; modern teknoloji giderek daha fazla zorbalık, şiddeti kışkırtma ve psikolojik zarara neden olmak için kullanılmaktadır.

(b) Uzaktan ev kontrolüne izin veren yeni teknolojilerin ortaya çıkmasıyla mümkün hale gelen akıllı evler; yeterince kullanışlı olmasına rağmen bu avantaj, yetkisiz bir kişinin kullanılan teknolojilerin güvenlik sistemini kırarak eve yetkisiz erişim sağlaması gibi önemli bir tehdit oluşturmaktadır. (c) Dijital medya, filmlerin, şarkıların, oyun uygulamalarının yetkisiz dağıtımı olasılığı nedeniyle her yıl daha fazla zarar açıklayan eğlence sektörüdür; telif hakkı sahiplerine doğrudan zarar vermektedir. (d) Çoğunlukla kritik altyapı nesnelerine saldıran siber terörizm; bunların korunması siber güvenlik politikasının önemli bir bileşenidir. Bütün bunlar, siber güvenliğin bilgi güvenliğinden daha geniş bir yelpazedeki sorunları kapsadığını göstermektedir. Buna karşılık bilgi güvenliği, örneğin, banka ve bankacılık kuruluşlarının çalışanları arasında gerçekleşen, banka sırrı olarak kabul edilen bilgilere hukuka aykırı erişim; ifşa ve imhadan oluşabilmektedir.

Bilim insanları tarafından önerilen oldukça kapsamlı sınıflandırmayı tamamlayan Sharikov Pavel A., istisnasız her siber tehdidin içerdiği en az üç unsuru vurgulamaktadır: (1) Kaynaklar, (2) Hedefler ve (3) Siber saldırıların uygulanma araçları. Sağlam bir siber güvenlik stratejisi geliştirirken siber tehditlerin tüm bileşenleri dikkate alınmalıdır.

Siber uzayın güvenli bir şekilde işlemesi ve birey, toplum ve devlet çıkarları doğrultusunda kullanılabilmesi için yalnızca bir siber güvenlik stratejisi geliştirmek yeterli değildir. Tomas Plėta, Sergii Karasov ve Tadas Jakštas'ın vurguladığı gibi, ayrıca şu adımların atılması gerekmektedir:

(a) N. Tkachuk'un 2018'deki tanımına göre, devlet siber güvenliğini sağlayan tüm unsurların toplamı, bunların etkileşim ve koordinasyon mekanizması, siber tehditlere karşı korunma, siber terörizm ve siber istihbarata karşı mücadele ile bu alanı düzenleyen yasal çerçeveyi içeren bir ulusal siber güvenlik sistemi oluşturmak,

(b) Askeri siber tehditler, siber casusluk, siber terörizm ve siber suçlarla etkin mücadele için güvenlik ve savunma sektörlerinin kapasitesini güçlendirmek ve bu alandaki uluslararası iş birliğini derinleştirmek,

(c) Devlet elektronik bilgi kaynaklarının, gerekli bilgilerin ve bilgi altyapısının siber korumasını sağlamak.

Yöntemler

Devletin siber güvenliğinin sağlanması, birden fazla yetkili kurumun birden fazla yöntem kullanarak katılması gereken karmaşık bir süreçtir. Bu yöntemler arasında, her şeyden önce, siber alanı korumanın teorik temellerini doğru bir şekilde belirlemeye ve ulusal siber savunma sisteminin kuruluşlarının faaliyetleri için yasal bir çerçeve oluşturmaya izin veren yasal yöntemi ayırmak gerekir. İlgili kamu ve özel kuruluşların faaliyetleri, yalnızca devletin mevcut siber uzay durumuna dayanarak, yeni kuruluşlara olan ihtiyacı belirlemeye, bunları oluşturmaya ve etkin işleyişleri için tüm koşulları sağlamaya olanak tanıyan organizasyonel yöntemin kullanılmasının sonucudur. Teknolojik yöntemler de unutulmamalıdır çünkü yazılım

ve teknolojiler olmadan siber tehditlerle mücadele etmek mümkün olmayacaktır. Dolayısıyla, devletin siber alanının korunması, devletin bu tür yasal, örgütsel ve teknolojik yöntemlere dayanan sistematik bir faaliyetidir.

Sonuçlar

Ukrayna'nın 5 Ekim 2017 tarihli Ukrayna'nın Siber Güvenliğinin Sağlanmasının Temel İlkeleri Hakkında Kanunu, siber güvenliği, bir kişinin ve vatandaşın, toplumun ve devletin siber uzayı kullanırken hayati çıkarlarının korunması olarak tanımlar. Bu koruma, bilgi toplumunun ve dijital iletişim ortamının sürdürülebilir gelişimini, siber uzaydaki ulusal güvenliğe yönelik gerçek ve potansiyel tehditlerin zamanında tespit edilmesini, önlenmesini ve etkisiz hale getirilmesini sağlar. Ukrayna yasama organı, siber güvenlik nesnelerini şu şekilde sıralamaktadır: İnsan ve vatandaşın anayasal hak ve özgürlükleri; Toplum, bilgi toplumunun sürdürülebilir gelişimi ve dijital iletişim ortamı; Devlet, anayasal düzeni, egemenliği, toprak bütünlüğü ve dokunulmazlığı; Bireyin, toplumun ve devletin yaşamının tüm alanlarındaki ulusal çıkarlar; Kritik altyapı tesisleri. (Ukrayna Siber Güvenliğin Temelleri Kanunu, 2017).

Ukrayna'nın "Bilgi Yasası", bilgi alanındaki devlet politikasının ana yönlerinin özellikle şunları içerdiğini öngörmektedir: (a) Herkesin bilgiye erişiminin sağlanması, (b) Bilginin oluşturulması, toplanması, alınması, depolanması, kullanılması, dağıtılması, güvenliği ve korunması konusunda eşit fırsatların sağlanması, (c) Ukrayna'da bir bilgi toplumunun oluşumu için koşulların oluşturulması, (d) İktidar kuruluşlarının faaliyetlerinin açıklığının ve şeffaflığının sağlanması, (e) Bilgi sistemleri ve bilgi ağlarının oluşturulması, elektronik yönetimin geliştirilmesi, (f) Ulusal bilgi kaynaklarının sürekli güncellenmesi, zenginleştirilmesi ve depolanması, (g) Ukrayna'nın bilgi güvenliğinin sağlanması, (h) Bilgi alanında uluslararası işbirliğinin teşvik edilmesi ve Ukrayna'nın küresel bilgi alanına girmesi. Ancak, bu normatif yasal düzenlemede, yasa koyucunun yalnızca "bilgi güvenliği" kavramına odaklandığı açıktır (Ukrayna Bilgi Yasası, 1992). Bu nedenle, mevcut siber uzay tehditlerine dikkat çeken ve bunları en aza indirmek için uygulanması gereken önlemlerin bir listesini içeren diğer normatif hukuki düzenlemelere ve bilimsel doktrinin hükümlerine dikkat edilmesi tavsiye edilmektedir.

Özellikle, Ukrayna Cumhurbaşkanı'nın 6 Mayıs 2015 tarihli Ukrayna Ulusal Güvenlik ve Savunma Konseyi Kararı ile onaylanan Ukrayna Ulusal Güvenlik Stratejisi, 26 Mayıs 2015 tarihli "Ukrayna Ulusal Güvenlik Stratejisi Hakkında" siber güvenliğe ve bilgi kaynaklarının güvenliğine yönelik başlıca tehditler arasında şunları belirtmektedir: (1) Kritik altyapı tesislerinin, siber saldırılarda devlet bilgi kaynaklarının savunmasızlığı, (2) Devlet sır koruma sisteminin ve kısıtlı bilgiye sahip diğer bilgi türlerinin fiziksel ve manevi olarak eskimiş olması (Ukrayna Ulusal Güvenlik Stratejisi, 2015). Mykola Syomych, Iryna Markina, Dmytro Diachkov, Ulusal Siber Güvenlik Endeksi'ne göre Ukrayna'daki siber koruma zayıflıklarını şu şekilde vurgulamaktadır: (a) Dijital hizmetlerin korunmaması (dijital hizmetler için sağlayıcıların sorumluluğunun olmaması), kamu sektörü ve yetkili siber güvenlik gözetim organı için siber güvenlik standartları, (b) Ulusal düzeyde siber kriz yönetimi uygulamalarının olmaması, siber kriz yönetimi alanındaki

uluslararası faaliyetlere ilgisizlik, siber kriz sırasında gönüllülere operasyonel destek eksikliği, (c) Askeri siber operasyonların olmaması (askeri siber operasyonları uygulayacak birimlerin olmaması, uluslararası girişimlere ilgisizlik, askeri siber operasyonları yürütme konusunda deneyim eksikliği).

Şekil: Ukrayna 2016 Siber Güvenlik Stratejisi

Ukrayna Ulusal Güvenlik ve Savunma Konseyi'nin 4 Mart 2016 tarihli "Ukrayna Güvenlik ve Savunma Sektörünün Geliştirilmesi Konsepti" kararında, ülkenin güvenlik ve savunma sektörünün bileşenlerinin gerekli operasyonel ve diğer yeteneklere ulaşması için ana yönler vurgulanmış olsa da, özellikle siber güvenlikle ilgili olanların da öne çıkarılması gerekmektedir. Bunlar arasında şunlar yer almaktadır: (a) Bilgi ve siber güvenlik sistemlerinin iyileştirilmesi, (b) Bilgi koruma ve bilgi kaynağı güvenlik sistemleri, (c) Askeri siber tehditlerle mücadele yoğunluğunun artırılması, (d) Siber casusluk, (e) Siber terörizm, (f) Siber suçlar, (g) Bu alandaki uluslararası iş birliğinin derinleştirilmesi. Ukrayna'nın genel Ulusal Güvenlik Stratejisine ek olarak, özellikle devletin ulusal siber güvenlik sisteminin kuruluşlarını tanımlayan Ukrayna Siber Güvenlik Stratejisi de onaylanmıştır.

Buna göre, Ukrayna Savunma Bakanlığı, Ukrayna Kabinesi'nin 26 Kasım 2014 tarihli kararıyla onaylanan düzenlemeye göre, barış zamanı ve özel dönemde ulusal güvenlik ile ilgili devlet politikasının oluşturulması ve uygulanmasını sağlayan, merkezi yürütme organları

sistemindeki başlıca kurumdur. Ayrıca, 2019 yılında sadece bilgi güvenliği, siber güvenlik ve siber savunma sağlamak için tedbirler alma yetkisiyle, devletin siber uzayda askeri saldırılara karşı savunmaya hazırlıklı olmasını sağlama görevleri de eklenmiştir.

Ukrayna Savunma Bakanlığı'nın yapısı, Bilgi Teknolojileri Dairesi'nin faaliyetlerini öngörmektedir. Bu dairenin amacı, barış zamanı ve özel dönemde bakanlık sisteminde bilgi güvenliği, siber güvenlik ile ilgili devlet politikasının uygulanmasını sağlamak, en son bilgi teknolojilerinin uygulanması için tedbirler almak ve koordine etmek, bakanlığın tek bir bilgi altyapısının oluşturulmasını sağlamaktır. Aynı zamanda, Ukrayna Savunma Bakanlığı'nın Bilgi Teknolojileri Dairesi, bilgi ortamını izlemek, savunma alanında Ukrayna'nın ulusal güvenliğine yönelik potansiyel siber tehditleri tespit etmek ve Ukrayna'nın ulusal güvenliğine yönelik askeri tehdit düzeyini değerlendirmek, bilgi ve analitik faaliyetler yürütmek ve siber tehditlerin uygulanmasıyla ilgili gelişmeleri öngörmekle de ilgilenmektedir.

Ulusal siber güvenlik sisteminin bir sonraki birimi, bugün yalnızca siber güvenlik sorunlarıyla ilgilenen Ukrayna Özel İletişim ve Bilgi Koruma Devlet Servisi'dir. Servisin temel faaliyetleri arasında UA idari alanıyla etkileşim, devlet bilgi kaynaklarının korunması, kamu otoriteleriyle etkileşim ve bilgi kaynaklarının korunması alanında uluslararası işbirliği, birleşik bir anti-virüs koruma sisteminin işleyişinin güvence altına alınması ve bilgi sistemleri ve telekomünikasyonların koruma düzeyinin belirlenmesi yer almaktadır.

N. Tkachuk, devletin siber güvenlik sisteminin mevcut siber tehditlere uygun olarak geliştirilmesi gerektiğini vurgulamaktadır; bu tehditlere karşı koyması gerekmektedir. Bilim insanına göre, devlet için bugün en büyük tehlike, yabancı devletlerin ve terörist örgütlerin kritik altyapı üzerindeki yasa dışı sibernetik etkisidir. Bu nedenle, Ukrayna Güvenlik

Servisi'nin (SBU) statüsüne özel bir dikkat gösterilmesi gerektiği ifade edilmektedir. SBU, devlet güvenliğine yönelik dış ve iç tehditleri, istihbarat, terörizm ve yabancı devletlerin, organizasyonların, bireysel grupların ve şahısların devletin hayati çıkarlarına yönelik diğer yasa dışı saldırılarını engelleme ve siber uzayda Ukrayna'ya karşı özel bilgi operasyonlarına karşı koyma yetkisine sahiptir. Özel hizmetlerin statüsü, Ukrayna'nın Ulusal Siber Güvenlik Sistemi'ndeki kilit rolünü göstermektedir. Bu rol, siber güvenlik alanında devlet çıkarlarına karşı istihbarat koruması sağlamak için şunları içermektedir: (1) Siber casusluk ve siber terörizme karşı koymak, (2) Siber suçları tespit etmek ve açığa çıkarmak.

Ukrayna Güvenlik Servisi ile birlikte, Ukrayna Ulusal Siber Güvenlik Sistemi'nin bir bileşeni olarak başka bir kolluk kuvveti kurumu olarak Ukrayna Ulusal Polisi faaliyet göstermektedir. Polis teşkilatının yapısında, Ukrayna Ulusal Polisi Siber Polisi Dairesi oluşturulmuştur. Aynı zamanda, V. Bereza, Ukrayna Ulusal Polisi Siber Polisi Dairesi'nin, kolluk kuvveti fonksiyonlarını yerine getirebilmesi için sahip olduğu yasal haklar (olası davranış tedbirleri) ve yükümlülükler (zorunlu davranış tedbirleri) sisteminin yetkisi altında değerlendirilmesi gerektiğini ifade etmektedir. Söz konusu kurumun resmi web sitesinde yer alan bilgilere göre görevleri şunları içermektedir: (a) Siber suçlarla mücadele alanında devlet politikasının uygulanması, (b) Yeni siber suçluların ortaya çıkışı hakkında halkın zamanında bilgilendirilmesi, (c) Siber olayları sistematize etmek için yazılımın uygulanması, (d) Yabancı ortaklardan gelen taleplere yanıt verilmesidir. Böylece, 2018 yılında Ukrayna Siber Polisi Dairesi siber güvenlik alanında 2688, yasadışı içerik alanında 1139, elektronik ticaret alanında 3607 ve ödeme sistemleri alanında 3697 suç hakkında soruşturma yürütmüştür.

Bununla birlikte, ilgili siber birimlerin polis teşkilatındaki faaliyetlerinin uygulanması yabancı ülkeler için yeni değildir. Özellikle, Siber Suç Dairesi, Aralık 2012'de İçişleri Bakanlığı Merkez Kriminal Polis Müdürlüğü bünyesinde İçişleri Bakanı Kararnamesi ile kurulmuştur. Şu anda, dairenin siber suç suçlarını araştıran 15 soruşturma dedektifi bulunmaktadır ve ayrıca siber suçları araştırmak ve Gürcistan genelindeki polis birimleri tarafından elektronik delilleri işlemek konusunda tavsiye ve diğer yardımları sağlamaktadır.

Siber güvenlik sisteminin bir parçası olarak Ukrayna Ulusal Polisi ve Ukrayna Güvenlik Servisi'nin yetkilerinin benzer olduğunu belirtmekte fayda var, ancak işlevlerinin dağılımı polis ve özel servislerin sorumluluk alanıyla ilgilidir. Bu nedenle, Ulusal Polis organları insanların, şirketlerin, kurumların, örgütlerin haklarını ve devletin ve toplumun çıkarlarını yasadışı eylemlere karşı korumaya büyük önem vermektedir. Buna karşılık, Ukrayna Güvenlik Servisi'nin faaliyetleri yalnızca devleti, anayasal düzenini, devlet güvenliğini korumaya ve karşı istihbarat faaliyetleri yürütmeye odaklanmaktadır.

Ukrayna'nın polisinin ve özel servislerinin siber uzay koruma alanındaki bu tür yetkileri dikkate alındığında, A. I. Bespalova'nın şartlı olarak dahili (polis organları ve birimleri çerçevesinde) ve harici olarak ayırdığı bu varlıklar arasındaki etkileşime önemli bir rol düşmektedir. Bilim adamı, faaliyetlerinin yönlerine bağlı olarak, bu varlıklar arasındaki aşağıdaki etkileşim türlerini ayırt etmeyi önermektedir: (1) Telekomünikasyon alanındaki suçlara karşı koyma ile ilgili etkileşim,

(2) Elektronik ticaret alanındaki suçlara karşı koyma ile ilgili etkileşim, (3) Dolandırıcılık ve suç gelirlerinin yasallaştırılması (aklanması) alanındaki suçlara karşı koyma ile ilgili etkileşim, vb.

Ukrayna'nın siber güvenlik sisteminin tüzel kişileri arasında yer alan Ukrayna Ulusal Bankası'na gelince, bankanın siber alanı güvence altına alma alanında sınırlı yetkiye sahip olduğunu belirtmekte fayda vardır. Çünkü bu alandaki yetkisi yalnızca bankaların faaliyetlerindeki siber güvenlikle ilgilidir. Dolayısıyla, 20 Mayıs 1999 tarihli "Ukrayna Ulusal Bankası Hakkında Kanun"a göre, Ukrayna Ulusal Bankası, Ukrayna bankacılık sisteminde ve para transfer eden tüzel kişiler için siber koruma ve bilgi güvenliğinin sağlanması için prosedürü, gereklilikleri ve önlemleri belirlemeye, bunların uygulanmasını izlemeye, Ukrayna Ulusal Bankası'nın siber koruma merkezini oluşturmaya ve Ukrayna bankacılık sisteminde siber koruma sisteminin işleyişini sağlamaya yetkilidir.

Petya virüsünün bankaların çalışmalarını engellemesinin ardından Ukrayna Ulusal Bankası, bankaları 2018 yılı içerisinde siber güvenliklerini güçlendirmek için önlemler almaya mecbur eden "Ukrayna bankacılık sisteminde bilgi güvenliğinin sağlanmasına yönelik tedbirlerin organizasyonuna ilişkin Yönetmeliğin onaylanması hakkında" 95 sayılı Kararnameyi kabul etmiştir. Söz konusu yasaya göre, her banka bilgi güvenliği yönetim sisteminin (ISMS) uygulanması ve işletilmesi konusunda kolektif bir organ oluşturmalı, bilgi güvenliğinden sorumlu bir kişi atamalı ve bilgi güvenliği sistemini uluslararası standartlara uygun şekilde güncellemelidir. Bu nedenle bankaların güncellenmiş siber güvenlik sistemlerini sunmaları gerekiyordu. Ancak Ukrayna Ulusal Bankası'nın bu yasası, belirlenen gerekliliklerin ihlali için özel yaptırımlar öngörmüyordu.

Fransa'da faaliyetleri Başbakan tarafından kontrol edilen Ulusal Siber Güvenlik Ajansı'nın (ANSSI) siber güvenlik ve siber savunma yetkililerine ait olduğunu belirtmekte fayda vardır. ANSSI, Fransız ekonomisinin modern teknolojiler olmadan gelişemeyeceğini kabul eder ve bu nedenle rekabetçi bir devlet ekonomisini korumak için kullanıcı gizliliğini korurken güvenli siber alanı teşvik etmek için faaliyetlerini yönlendirir.

Finlandiya'da, Ulusal Siber Güvenlik Merkezi (NCSC-FI), siber güvenliği destekleme konusunda hükümet kurumlarını, iş çevrelerini ve diğer kuruluşları destekleyen ulusal bir bilgi güvenliği kurumu olarak 2014 yılında kurulmuştur. Merkez, CERT-FI ve GOV-CERT'in işlevlerinin Ulusal İletişim Güvenliği Otoritesi FICORA (NCSA-FI) ile birleştirilmesiyle oluşturulmuştur. Günümüzde, Finlandiya Ulusal Siber Güvenlik Merkezi: (1) Eyaletteki siber güvenliğin gerçek durumu hakkında bilgi sağlar. (2) Mevcut siber tehditleri tespit eder ve analiz eder. (3) Yetkilileri desteklemek için mevcut kaynakları ve araçları sağlar. (4) Ulusal, eyaletler arası ve uluslararası düzeylerde siber uzay güvenliği sorunları ile ilgili iş birliği kurar. Merkezin sorumlulukları arasında ayrıca, sınıflandırılmış bilgilerin elektronik yollarla iletilmesi ve işlenmesinin güvenliğinden sorumlu olmak da yer almaktadır.

Almanya'da Federal Bilgi Güvenliği Ofisi'ne (BSI) bağlı olan Cyberdefense Center (Cyber-AZ) faaliyet göstermektedir. Cyber-AZ, yetki alanı içerisinde Federal Sivil Savunma ve Afet

Yönetimi Ofisi ve Federal Anayasa Koruma Ofisi ile iş birliği yapmaktadır. Ayrıca, Cyber-AZ'nin faaliyetleri Federal Kriminal Polis Müdürlüğü, Federal Polis Müdürlüğü, Federal İstihbarat Servisi ve askeri birimler tarafından kapsamlı bir şekilde desteklenmektedir. Bu kadar geniş bir kuruluş ağı ve aralarındaki iş birliği sayesinde Cyber-AZ, bilgi ve en iyi uygulama alışverişi için önemli bir merkezdir. Buna göre, Cyber-AZ siber saldırıları değerlendirmekte, bunların uygulanması için kanalları, bunların gerçekleştirilmesinden sorumlu kişileri belirlemekte ve Ulusal Siber Güvenlik Konseyi'ne önerilerle birlikte ilgili bilgileri sağlamaktadır.

Tartışma

Boes, S., Leukfeldt, E.R.'nin görüşüne göre kolluk kuvvetleri siber suçla mücadelede önemli bir rol oynamaktadır. Ancak, bu tür suçlarla mücadele stratejilerinden biri özel kuruluşlarla ortaklıklar kurmaktır. Özellikle Streltsov, Lev, Ukrayna'nın siber güvenliğini sağlama görevine sahip olan yapıların dört ana gruba ayrılabileceğini belirtmektedir: Savunma ve istihbarat yapıları, kolluk kuvvetleri, teknik koruma düzenleyicileri, özel sektör ve koordinatör olarak Ulusal Siber Güvenlik Koordinasyon Merkezi. Devlete yönelik siber güvenlik tehditlerinin seviyesi ne kadar yüksek olursa, farklı yapıların birlikte çalışması olasılığı da o kadar artmaktadır. Ancak, Petya virüsünün yayılmasıyla ilgili son olay sırasında çeşitli yapıların iş birliği yapmış olmasına rağmen, bu iş birliğinin anlamı kamuya açık değildir ve dolayısıyla halk tarafından değerlendirilememektedir. Bir diğer önemli nokta, siber güvenliğin sağlanmasında özel sektörün rolüdür. Ukrayna'da kamu-özel sektör iş birliği alanı henüz kuruluş aşamasındadır. Bu tür bir iş birliği için gerekli olan yasal çerçeve tam olarak geliştirilmemiştir. Ayrıca, Ukrayna'da siber güvenliğe katkı sağlayabilecek uzmanlaşmış araştırma kurumları hâlâ eksiktir. Bununla birlikte, bu sorunların yalnızca Ukrayna'ya özgü olmadığına, gelişmiş bir hukuk sistemine sahip olan devletlerde bile kamu-özel sektör iş birliğinin işleyişinin tartışma konusu olduğuna dikkat çekmek gerekmektedir.

D. Dubov, V. Boiko, S. Hnatyuk, T. Isakova, M. Ozhevan ve A. Pokrovska, günümüzde Ukrayna'da siber güvenlik alanında kamu-özel sektör iş birliğinin

bulunmadığını belirtmektedir. Siber uzayın korunmasındaki yetersiz durum bağlamında bu konu giderek daha önemli hale gelmektedir. Buna bağlı olarak, yetkili makamların öncelikli görevi, sivil sektörle iletişim/iş birliği kurmak ve bu tür bir iletişim/iş birliği için etkili kurumsal ve hukuki araçlar geliştirmektir. Bir diğer önemli sorun ise Ukrayna siber güvenlik sektörünün kapalı yapısıdır; mevcut bilgiler, sektörün durumu ve geleceği hakkında objektif bir tablo sunmamaktadır.

Aynı zamanda, Tkachuk Nataliya, siber güvenlik alanında kamu-özel sektör iş birliği sorununa ek olarak, Ukrayna'nın 2005 yılında Avrupa Konseyi Siber Suçlar Sözleşmesi'ni uluslararası işbirliği için önemli bir araç olarak onaylamasına rağmen, hâlâ var olan mekanizmaların optimize edilmesine acil bir ihtiyaç duyduğuna dikkat çekmektedir. Bu, siber tehditlere hızlı ve uygun bir şekilde yanıt verilmesini ve siber suçların ulusal ve uluslararası düzeyde soruşturulmasını sağlamak için taraflar arasında bilgi paylaşımını içeren karşılıklı adli yardım anlaşmalarını da kapsamaktadır.

Yorum

İnternetin güvenli bir şekilde arama, depolama, bilgi yayma, bankacılık işlemleri ve diğer işlemleri yürütme, işletmelerin, kurumların, kuruluşların yazılımları için kullanımına yönelik önemli tehditlerden biri siber saldırılar da dahil olmak üzere siber tehditlerdir. Her ülkenin siber güvenlik mekanizması, bir siber güvenlik stratejisinin geliştirilmesini ve benimsenmesini, ulusal bir siber güvenlik sisteminin kurulmasını, siber tehditlerle, siber terörizmle vb. etkili bir şekilde mücadele etmek için güvenlik ve savunma yeteneklerinin güçlendirilmesini, devlet elektronik bilgi kaynakları ve bilgi altyapısı için siber güvenliğin sağlanmasını öngörmektedir.

Ukrayna'da, Ukrayna Siber Güvenlik Stratejisi'ne ek olarak, siber tehditlere karşı koyma ve mücadele etme konusundaki yasal dayanak, Ukrayna Anayasası, Ukrayna Siber Güvenliğinin Temel İlkeleri Hakkındaki Ukrayna Yasası, Ukrayna Bilgi Yasası, Ukrayna Ulusal Güvenlik Stratejisi, Ukrayna Güvenlik ve Savunma Sektörünün Gelişimi Kavramı vb.'den oluşmaktadır. Buna karşılık, ulusal siber güvenlik sistemi, Ukrayna Savunma Bakanlığı, Ukrayna Özel İletişim ve Bilgi Koruma Devlet Servisi, Ukrayna

Güvenlik Servisi, Ukrayna Ulusal Polisi, Ukrayna Ulusal Bankası ve istihbarat teşkilatları gibi yetkili kuruluşların faaliyetlerini öngörmektedir. Bu kuruluşlar arasında özel bir yer Ukrayna Siber Polis Departmanı'na aittir. Buna karşılık, Fransa, Finlandiya, Almanya'da, Ukrayna'nın aksine, siber güvenlik sistemindeki merkezi yer sırasıyla Ulusal Siber Güvenlik Ajansı, Ulusal Siber Güvenlik Merkezi ve Siber Güvenlik Merkezi tarafından oluşmaktadır.

Böylece, Ukrayna Anayasası'nın 17. maddesi, Ukrayna'nın egemenliğini ve toprak bütünlüğünü korumanın, ekonomik ve bilgi güvenliğini sağlamanın devletin en önemli işlevi, tüm Ukrayna ulusunun işi olduğunu hükme bağlamıştır. Aynı zamanda, siber güvenlik bu anayasal normda açıkça belirtilmese de, yalnızca en önemli koruma alanları dikkate alınsa bile, siber güvenliğin bilgi güvenliğinin ayrılmaz bir parçası olduğu sonucuna varılabilmektedir.

Ukrayna'nın ülkedeki siber tehditlere karşı devletin çıkarlarının korunma düzeyini artırma yönünde attığı önemli adımlara rağmen, siber güvenlik alanında kamu-özel sektör iş birliği bulunmamaktadır. Devletin bu yöndeki faaliyetlerinin birincil odak noktası, devlet dışı sektörle iletişim/iş birliği kurmak ve bu iletişim/iş birliği için etkili kurumsal ve yasal araçlar oluşturmak olmalıdır. Aynı zamanda, mevcut siber tehditlerin küresel niteliği göz önüne alındığında, siber güvenlik alanında kamu-özel sektör iş birliği konusu istisnasız tüm dünya ülkeleri için acil bir durumdur.[3]

3 https://www.researchgate.net/publication/340440328

Siber Güvenlik Üzerine Kapsamlı Bir İnceleme: Modern Tehditler ve Gelişmiş Savunma Stratejileri

Yazan: Comprehensive Review on Cybersecurity: Modern Threats and Advanced Defense Strategies, Ogugua Chimezie OBİ vd., ResearchGate, 3 Şubat 2024

Gayri Resmi Tercümesi: Sektörel Araştırma ve Strateji Geliştirme Dairesi

Giriş

Dijital bağlantılılığın hâkim olduğu bir çağda, siber uzayın yaygınlaşması eşi benzeri görülmemiş fırsatların ve yeniliklerin önünü açmıştır. Bununla birlikte, bu dijital evrimin, birbirine bağlı sistemlerimizdeki güvenlik açıklarından yararlanan siber tehditlerin artışı gibi karanlık bir karşılığı da olmuştur.

Bu gelişen tehditleri anlama, öngörme ve bunlara karşı koyma zorunluluğu hiç bu kadar acil olmamıştı. Bu kapsamlı inceleme, dijital ekosistemlerin bütünlüğünü korumak için çok önemli olan gelişmiş savunma stratejilerini incelerken modern tehditlerin inceliklerini çözmeyi amaçlayan çağdaş siber güvenlik paradigmasının ayrıntılı bir araştırmasına girişmektedir. Sinsi kötü amaçlı yazılımlar ve fidye yazılımlarından titizlikle düzenlenmiş kimlik avı kampanyalarına ve sofistike gelişmiş kalıcı tehditlere (APT'ler) kadar uzanan siber tehditlerin yaygın doğası, metodolojilerinin ve motivasyonlarının incelikli bir şekilde anlaşılmasını gerektirmektedir. Son vaka çalışmalarının, ampirik araştırmaların ve sektörel içgörülerin bir sentezine dayanan bu inceleme, siber tehditlerin çok yönlü manzarasına panoramik bir bakış sağlamayı amaçlamaktadır. Siber düşmanları harekete geçiren güdüleri araştırıyor, hackerlardan ulus devlet kuruluşlarına kadar tehdit aktörlerinin çeşitli profillerini inceliyor ve geleneksel siber güvenlik önlemlerinin etkinliğine meydan okuyan gelişen taktikleri inceliyoruz. Siber saldırganlar ve savunmacılar arasındaki silahlanma yarışı yoğunlaştıkça, inceleme odağını siber güvenlik direncinin öncüsünü oluşturan en son savunma mekanizmalarına kaydırmaktadır. Yapay zekâ ve makine öğrenimi algoritmalarının entegrasyonundan davranışsal analitiğin kullanımına kadar, teknolojik inovasyonun dijital savunmayı güçlendirmedeki rolünü değerlendiriyoruz.

Aynı zamanda, küresel siber tehditlere karşı birleşik bir cephe oluşturmada ortak çabaların, tehdit istihbarat paylaşımının ve uluslararası iş birliğinin öneminin altını çizmekteyiz. Teknolojik hususların ötesinde, bu inceleme siber güvenlik denklemindeki vazgeçilmez insan unsurunu kabul etmektedir. Savunmaların etkinliğinin kod ve algoritmalar alanının ötesinde, bireylerin uyanıklığı ve eylemlerine uzandığını kabul ederek, kuruluşlar içinde güvenlik bilincine sahip bir kültürün geliştirilmesinde siber güvenlik farkındalığı ve eğitiminin kritik rolü araştırılmıştır.

Ayrıca düzenleyici çerçeveler ve uyum standartları siber güvenlik politikaları ve uygulamalarının şekillendirilmesinde önemli bir rol oynamaktadır. Bu inceleme, siber güvenlik duruşlarını şekillendirme ve dijital savunmaya yönelik proaktif bir yaklaşımı teşvik etme üzerindeki etkisini değerlendirerek gelişen düzenleyici ortamı incelemektedir.

En son gelişmeleri, ortaya çıkan eğilimleri ve yerleşik en iyi uygulamaları sentezleyen bu kapsamlı inceleme, sürekli gelişen siber güvenlik alanında politika yapıcılar ve araştırmacılar için bir yol gösterici olmayı amaçlamaktadır. Okuyucularını çağdaş tehditler hakkında bütünsel bir anlayışla donatmaya ve dijital geleceğimizi güvence altına almak için gerekli olan gelişmiş savunma stratejileri cephaneliğine ilişkin içgörülerle güçlendirmeye çalışmaktadır.

Dijital Çağda Siber Güvenlik

Dijital etkileşimlerin hayatımızın her alanına nüfuz ettiği bir çağda, sağlam siber güvenlik önlemlerine duyulan ihtiyaç hiç bu kadar kritik olmamıştır. Benzeri görülmemiş teknolojik gelişmelerin ve birbirine bağlı sistemlerin damgasını vurduğu dijital çağ, hem inovasyon fırsatlarını hem de yaklaşan siber saldırı tehdidini beraberinde getirmektedir. Bu araştırmada, dijital çağda siber güvenlik ortamını keşfedecek, karşılaştığımız zorlukları ve dijital geleceğimizi korumaya yönelik stratejileri inceleyeceğiz.

Dijitalleşmenin durmak bilmeyen hızı; yaşama, çalışma ve iletişim kurma biçimlerimizde devrim yapmıştır. Nesnelerin İnterneti (IoT), yapay zekâ ve bulut bilişim günlük varlığımızın ayrılmaz parçaları haline gelmiştir. Ancak bu dijital dönüşümün bir bedeli var: siber tehditler için genişletilmiş bir saldırı yüzeyi. Dünyamız birbirine daha bağlı hale geldikçe, potansiyel güvenlik açıkları artmakta ve siber güvenliğe proaktif ve uyarlanabilir bir yaklaşım gerektirmektedir.

Siber tehditler basit virüslerin ötesine geçmiş ve artık sofistike bir dizi saldırıyı kapsar hale gelmiştir. Kötü amaçlı yazılımlar, fidye yazılımları, kimlik avı ve gelişmiş kalıcı tehditler (APT'ler), siber düşmanlar tarafından kullanılan araçların cephaneliği arasındadır. Bu saldırıların motivasyonları finansal kazanç ve bilgi hırsızlığından ideolojik motiflere ve hatta devlet destekli siber savaşa kadar uzanmaktadır. Bu tehditlere etkili bir şekilde karşı koymak için siber suçlular tarafından kullanılan ve sürekli değişen taktikleri anlamak çok önemlidir.

Gelişen tehditler karşısında hem kuruluşlar hem de bireyler proaktif savunma önlemleri benimsemelidir. Sürekli izleme, tehdit tespiti ve güvenlik açığı yönetimi, sağlam bir siber güvenlik stratejisinin temel bileşenleridir. Hızlı olay müdahale ve kurtarma planları, başarılı bir saldırı durumunda esneklik sağlamaktadır. Uluslararası siber güvenlik düzenlemelerine uyum, etkili siber güvenlik uygulamaları için bir çerçeve oluşturarak savunma duruşunu daha da güçlendirmektedir.

Yapay zeka ve makine öğrenimi, siber tehditlerin önüne geçilmesinde çok önemli bir rol oynamaktadır. Davranışsal analitik, anormalliklerin ve potansiyel güvenlik ihlallerinin tespit

edilmesini sağlarken, uyarlanabilir savunma stratejileri saldırıları tahmin etmek ve önlemek için bu teknolojilerden yararlanmaktadır. Tehdit istihbaratı paylaşımı ve uluslararası iş birliği yoluyla ortak çabalar, küresel siber tehditlere karşı birleşik bir cephe oluşturmaktadır.

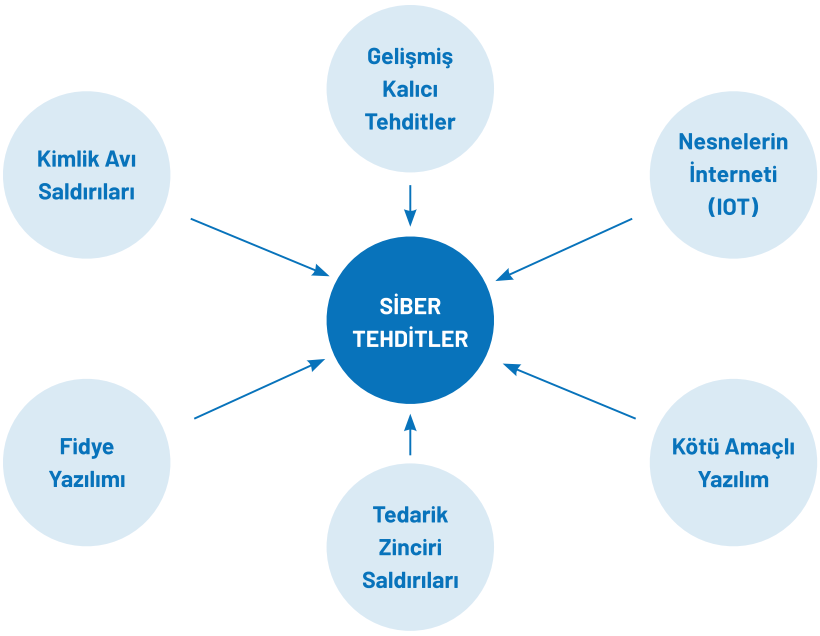
Teknolojik çözümler çok önemli olsa da insan unsuru siber güvenlikte kritik bir faktör olmaya devam etmektedir. Siber güvenlik farkındalığı ve eğitim programları, bir güvenlik bilinci kültürünün geliştirilmesi için hayati önem taşımaktadır. Sosyal mühendislik taktiklerinin tanınması ve azaltılmasının yanı sıra siber tehditlere karşı insan direncinin artırılması, genel savunmaya önemli ölçüde katkıda bulunur.

Gelecekteki eğilimleri öngörmek, ortaya çıkan siber tehditlere hazırlanmak için çok önemlidir. Teknoloji gelişmeye devam ettikçe, siber suçluların taktikleri de gelişmektedir (Alrousan ve Faqir, 2023.). Kuantum bilişim, uyarlanabilir güvenlik mimarileri ve savunma stratejilerindeki sürekli yenilikler siber güvenliğin geleceğini şekillendirecektir.

Dijital çağın dinamik ortamında, dijital geleceğimizi güvence altına alma sorumluluğu bireylerin, kuruluşların ve politika yapıcıların kolektif omuzlarındadır. Modern siber tehdit ortamını anlayarak, gelişmiş savunma mekanizmaları uygulayarak ve siber güvenlik farkındalığı kültürünü teşvik ederek, dijital çağın zorluklarının üstesinden gelebilir ve gelecek nesiller için daha güvenli ve emniyetli bir çevrimiçi ortam sağlayabiliriz.

Modern Siber Tehdit Ortamı

Modern siber tehdit ortamı, düşmanların birbirine bağlı dijital dünyamızdaki güvenlik açıklarından yararlanmak için gelişmiş taktik ve teknolojilerden yararlandığı, sürekli değişen bir savaş alanıdır.



Şekil 1. Siber Tehditlerin Sınıflandırılmasının Şeması

Bu manzaranın inceliklerini araştırdıkça, etkili savunma stratejileri geliştirmek için çeşitli siber tehditlerin kapsamlı bir şekilde anlaşılmasının gerekli olduğu ortaya çıkmaktadır. Şekil 1 siber tehditlerin kategorizasyonunu vermektedir. "Kötü amaçlı yazılım" anlamına gelen Malware, dijital çağın en yaygın ve uyarlanabilir tehditlerinden biri olarak karşımıza çıkmaktadır. Artık basit virüslerle sınırlı olmayan kötü amaçlı yazılımlar, truva atları, solucanlar ve fidye yazılımları da dahil olmak üzere sofistike varlıklara dönüşmüştür. Kötü amaçlı yazılımların dinamik doğasını ve çeşitli dağıtım mekanizmalarını anlamak, dijital savunmaları güçlendirmek için çok önemlidir. Fidye yazılımları özellikle sinsi bir siber tehdit biçimi olarak ortaya çıkmış ve bireyler, işletmeler ve hatta devlet kurumları arasında hasara yol açmıştır. Failler, kritik verilere erişimi kilitlemek için şifreleme algoritmaları kullanır ve bunların serbest bırakılması için fidye talep etmektedir. Fidye yazılımı saldırılarının ardındaki finansal motivasyon, onları siber suçlular için kazançlı bir girişim haline getirmiştir. Yüksek profilli olayların yaygın ilgi görmesiyle birlikte fidye yazılımı tehdidi, sağlam siber güvenlik önlemlerine ve etkili olay müdahale planlarına duyulan ihtiyacın altını çizmektedir. Siber tehditler alanında, insan faktörü kalıcı bir güvenlik açığı olmaya devam etmektedir. Aldatıcı e-postalar, mesajlar veya web siteleri ile karakterize edilen oltalama saldırıları, hassas bilgileri ifşa etmeleri için bireyleri kandırmak amacıyla insanların güvenini istismar etmektedir. Spearphishing ve whaling gibi oltalama taktiklerinin evrimi, siber suçluların ikna edici ve hedefli kampanyalar hazırlama konusundaki uyarlanabilirliğini göstermektedir. Siber güvenlik farkındalık programları ve gelişmiş e-posta filtreleme teknolojileri, oltalama saldırılarıyla ilişkili riskleri azaltmak için gereklidir.

Gelişmiş Kalıcı Tehditler (APT'ler), genellikle ulus-devlet aktörleriyle ilişkilendirilen sofistike ve uzun süreli bir siber saldırı biçimini temsil etmektedir. Bu saldırılar, sıfırıncı gün istismarları, sosyal mühendislik ve tehlikeye atılmış ağlarda gizli kalıcılık gibi gelişmiş tekniklerin bir kombinasyonu ile karakterize edilmektedir. APT'ler tipik olarak casusluk, fikri mülkiyet hırsızlığı veya stratejik bozulma için düzenlenmektedir. APT'lere karşı savunma, gelişmiş tehdit tespit araçları, dikkatli izleme ve proaktif tehdit istihbaratı paylaşımını birleştiren çok yönlü bir yaklaşım gerektirir.

Nesnelerin İnterneti (IoT) cihazlarının yaygınlaşması, siber tehditler için saldırı yüzeyini katlanarak artırmıştır. Akıllı ev aletlerinden endüstriyel sensörlere kadar değişen güvensiz IoT cihazları, siber suçluların ağları tehlikeye atması için giriş noktaları sağlar. IoT ekosistemleri büyümeye devam ettikçe, cihaz tasarımı, dağıtımı ve bakımındaki güvenlik açıklarının ele alınması, büyük ölçekli saldırıların önlenmesi için çok önemli hale gelmektedir.

Siber düşmanlar, daha büyük hedeflere sızmak ve onları tehlikeye atmak için tedarik zincirlerindeki güvenlik açıklarından giderek daha fazla yararlanmaktadır. Saldırganlar, güvenilir bir tedarikçiyi veya hizmet sağlayıcıyı tehlikeye atarak hassas verilere veya sistemlere

yetkisiz erişim elde edebilir. Tedarik zinciri saldırıları, modern iş operasyonlarının birbirine bağlı doğasını vurgulamakta ve risk yönetimi ve üçüncü taraf ortakların incelenmesi için kapsamlı bir yaklaşım gerektirmektedir. Modern siber tehdit ortamının inceliklerini anlamak, etkili siber güvenlik stratejileri geliştirmek için bir ön koşuldur. Tehditler gelişmeye devam ettikçe, gelişmiş teknolojileri, tehdit istihbarat paylaşımını ve insan merkezli güvenlik uygulamalarına odaklanmayı kapsayan proaktif ve uyarlanabilir bir yaklaşım, dijital geleceğimizi korumak için elzem hale gelmektedir.

Siber Saldırıların Arkasındaki Motivasyonlar ve Amaçlar

Siber saldırıların arkasındaki motivasyonlar ve hedefler, siber uzayın karmaşık manzarasını ve bu tür faaliyetlere katılanların çeşitli çıkarlarını yansıtacak şekilde çeşitlilik göstermektedir. Siber saldırganlar veya tehdit aktörleri arasında bireyler, organize suç grupları, hacktivistler ve hatta ulus devletler yer alabilir. Siber saldırıların arkasındaki motivasyonları anlamak, etkili siber güvenlik stratejileri geliştirmek için çok önemlidir. Siber saldırılar için bazı yaygın motivasyonlar ve hedefler Şekil 2'de gösterilmektedir.

Şekil 2. Siber Saldırılar İçin Motivasyon ve Amaçların Şeması

Birçok siber saldırı finansal olarak motive edilmektedir. Suçlular, kredi kartı bilgileri, bankacılık kimlik bilgileri veya kişisel olarak tanımlanabilir bilgiler (PII) gibi karanlık web'de para kazanılabilecek hassas bilgileri çalmaya çalışırlar. Saldırganların veri veya sistemlere erişimin yeniden sağlanması karşılığında ödeme talep ettiği fidye yazılımı saldırıları bu motivasyonu örneklendirmektedir. Ulus devletler, askeri, ekonomik veya siyasi konularla ilgili hassas bilgileri çalarak stratejik bir avantaj elde etmek için siber casusluk yapabilirler. Bu saldırılar genellikle devlet kurumlarını, savunma müteahhitlerini ve kritik altyapıyı hedef alır.

Hacktivistler, belirli bir siyasi veya sosyal gündemi desteklemek için siber saldırılarda bulunurlar. Amaçlarına dikkat çekmek için web sitelerini tahrif edebilir, hassas bilgileri sızdırabilir veya çevrimiçi hizmetleri kesintiye uğratabilirler. Hacktivist saldırılar genellikle devlet kurumlarını, şirketleri veya düşman olarak algılanan kuruluşları hedef almaktadır. Kurumsal casusluk, pazarda rekabet avantajı elde etmek için fikri mülkiyetin, ticari sırların veya tescilli bilgilerin çalınmasını içerir. Rakip işletmeler ve hatta devlet destekli aktörler bu tür faaliyetlere dahil olabilir. Bazı siber saldırılar elektrik şebekeleri, su kaynakları veya ulaşım sistemleri gibi kritik altyapıları bozmayı veya sabote etmeyi amaçlar. Bu saldırılar bir ülkenin güvenliği ve kamu emniyeti üzerinde ciddi sonuçlar doğurabilir.

Ulus-devletler daha geniş bir askeri stratejinin parçası olarak siber saldırılarda bulunabilirler. Siber savaş, düşman iletişimini bozmayı, savunma sistemlerini devre dışı bırakmayı veya bir düşmanı zayıflatmak için ekonomik hasara neden olmayı içerebilir.

Siber saldırılar kamuoyunu manipüle etmek, seçimleri etkilemek veya siyasi ortamları istikrarsızlaştırmak için kullanılabilir. Bu, dezenformasyon yaymayı, sosyal mühendislik kampanyaları yürütmeyi veya siyasi figürlerin iletişimlerini tehlikeye atmayı içerebilir. Bazı siber saldırılar, tehdit aktörlerinin hassas veya utanç verici bilgileri ifşa etme tehdidi altında bireylerden veya kuruluşlardan ödeme talep ettiği şantajı içerir. Bu, veri sızıntısı tehditleri veya dağıtılmış hizmet reddi (DDoS) saldırıları yoluyla gerçekleşebilir. Bireysel bilgisayar korsanları veya gruplar kişisel nedenlerle siber saldırılarda bulunabilir, intikam arayışına girebilir. Bu motivasyonları anlamak, incelikli ve etkili bir siber güvenlik stratejisi geliştirmek için çok önemlidir. Kuruluşlar ve bireyler, dijital ortamda gelişen tehditleri azaltmak için teknik savunma, kullanıcı eğitimi ve proaktif risk yönetiminin bir kombinasyonunu kullanarak uyanık kalmalıdır.

Tehdit Aktörlerinin Profilinin Çıkarılması

Tehdit aktörlerinin profilini çıkarmak, siber faaliyetlerde bulunan çeşitli gruplar tarafından kullanılan özellikleri, motivasyonları ve taktikleri anlamayı içermektedir. Bahse konu dört tür tehdit aktörleri şunlardır: Bireysel bilgisayar korsanları genellikle kişisel merak, bilgisayar korsanlığı topluluğu içinde tanınma arzusu veya mali kazanç nedeniyle hareket etmektedir. Bireysel bilgisayar korsanları, algılanan güvenlik açıklarına veya kişisel motivasyonlara dayalı olarak bireyleri, küçük işletmeleri veya kuruluşları hedef alabilir.

Hacktivist gruplar ideolojik, siyasi veya sosyal motivasyonlarla hareket etmektedir. Belirli bir davayı ilerletmeyi, farkındalık yaratmayı veya algılanan adaletsizlikleri protesto etmeyi amaçlamaktadır. Saldırıları genellikle gündemlerine dikkat çekmek için halka dönük bir unsur içerir. Hacktivist gruplar tipik olarak orta ila ileri düzeyde bilgisayar korsanlığı becerilerine sahiptir ve tahrifat, veri ihlalleri veya çevrimiçi hizmetlerin kesintiye uğratılmasına odaklanmaktadır.

Organize siber suçlar öncelikle kâr odaklıdır. Bu gruplar, parasal kazanç için finansal dolandırıcılık, kimlik hırsızlığı ve fidye yazılımı saldırıları gibi faaliyetlerde bulunan işletmeler gibi çalışmaktadır. Organize siber suç grupları finansal kurumlar, büyük şirketler ve değerli varlıklara veya hassas bilgilere sahip bireyler gibi genellikle daha büyük bir suç ağının parçası olarak faaliyet gösterir.

Ulus-devlet aktörleri siyasi, ekonomik ve askeri hedefler de dahil olmak üzere ulusal çıkarları ilerletmek için siber operasyonlar yürütmektedir. Bu saldırılar casusluk, sabotaj veya etki kampanyalarını içerebilir. Bu tehdit aktörlerinin motivasyonlarını ve profillerini anlamak, kuruluşlar ve siber güvenlik uzmanları için çok önemlidir. Siber tehditlerin etkisini azaltmak için hedefli savunma stratejilerinin geliştirilmesini, tehdit istihbaratının paylaşılmasını ve uluslararası iş birliğini mümkün kılmaktadır. Siber ortam geliştikçe, uyanık kalmak ve savunmaları uyarlamak, çeşitli tehdit aktörlerine karşı koymak için çok önemlidir.

Siber Saldırı Taktiklerinin Evrimi

Sürekli gelişen siber güvenlik alanında, tehdit aktörleri savunmaları aşmak, güvenlik açıklarından yararlanmak ve kötü niyetli hedeflerine ulaşmak için taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) sürekli olarak uyarlamaktadır. Siber saldırı taktiklerinin dinamik doğasını anlamak, kuruluşların savunmalarını etkili bir şekilde güçlendirmeleri için çok önemlidir.

Stuxnet 2010 yılında denetim kontrol ve veri toplama (SCADA) sistemlerini hedef almıştır. Hava boşluklu sistemleri enfekte etmek için sıfır günlük güvenlik açıklarını kullanmıştır. Özellikle İran'ın nükleer programını bozmayı amaçlayan devlet destekli siber saldırılar için bir emsal oluşturmuştur.

SolarWinds Tedarik Zinciri Saldırısı 2020 yılında güvenilir bir yazılım tedarik zincirini tehlikeye atmıştır. Ağlara sızmak için arka kapılı yazılım güncellemeleri kullandı. Çok sayıda hükümet ve özel sektör kuruluşuna yetkisiz erişim sağlamıştır.

Siber saldırı taktiklerinin evrimi, siber güvenlik uzmanlarının ortaya çıkan tehditleri yakından takip etme ihtiyacının altını çizmektedir. Kuruluşlar, bu dinamik ve sofistike siber saldırı metodolojilerinin yarattığı riskleri etkili bir şekilde azaltmak için tehdit istihbaratı paylaşımı, gelişmiş tespit teknolojileri ve düzenli güvenlik bilinci eğitimi dahil olmak üzere proaktif önlemler almalıdır.

Gelişmiş Savunma Mekanizmaları

Siber tehditler karmaşıklığı arttıkça, savunma mekanizmaları geliştirme zorunluluğu daha önemli hale gelmiştir. Kuruluşlar, en son teknolojilerden ve iş birliğine dayalı stratejilerden yararlanarak siber güvenlik duruşlarını güçlendirebilirler. Davranışsal analitik, potansiyel tehditlerin göstergesi olan sapmaları belirlemek için kullanıcı davranış kalıplarının izlenmesini

ve analiz edilmesini içerir. Yapay zekâ ve makine öğrenimi algoritmaları, normal davranışların bir temelini oluşturmak için oturum açma modelleri, veri erişimi ve iletişim davranışları gibi kullanıcı etkinliklerini analiz etmektedir. Bu temel çizgiden sapmalar, potansiyel kötü niyetli faaliyetler için uyarıları tetiklemektedir. Geleneksel kural tabanlı sistemlerin gözden kaçırabileceği anormal davranışları tespit ederek proaktif bir yaklaşım sağlar. İçeriden gelen tehditlerin ve sıfırıncı gün saldırılarının erken tespit edilmesini sağlamaktadır.

Anomali tespiti, beklenen kalıplardan veya davranışlardan sapmaları belirlemek için yapay zeka ve makine öğrenimi algoritmalarını kullanır. Algoritmalar, normal kalıplar oluşturmak için geçmiş verilerden öğrenir. Olağandışı ağ trafiği veya atipik sistem erişimi gibi sapmalar meydana geldiğinde, anomali tespiti daha fazla araştırma için bu anomalileri işaretler. Yeni ve gelişen saldırı modellerini tanımlayarak tehdit tespitini geliştirir. Siber tehditlerin değişen doğasına uyum sağlayarak yanlış pozitifleri azaltır.

Tehdit istihbaratı, siber tehditler hakkında bilgi toplamayı, analiz etmeyi ve yaymayı içerir ve kuruluşların potansiyel saldırılara karşı proaktif olarak savunma yapmasını sağlamaktadır. Kuruluşlar, açık kaynak beslemeleri, endüstri grupları ve devlet kurumları dahil olmak üzere çeşitli kaynaklardan istihbarat toplar. Otomatik sistemler bu bilgilerin işlenmesine ve bağlamsallaştırılmasına yardımcı olarak eyleme geçirilebilir iç görüler sağlar. Bilgi paylaşımı, siber güvenlik topluluğunun tehditlere işbirliği içinde yanıt verdiği, iç görüleri ve en iyi uygulamaları paylaştığı kolektif bir savunma yaklaşımını teşvik etmektedir. Siber tehditler ulusal sınırları aşar ve siber saldırıların küresel doğasını ele almak için uluslararası iş birliğini gerektirir. Uluslar, kuruluşlar ve siber güvenlik birimleri bilgi paylaşımı, ortak tehdit araştırmaları ve uluslararası siber güvenlik normları ve anlaşmalarının geliştirilmesi konularında iş birliği yapar. Kaynakları ve uzmanlığı bir araya getirerek siber tehditlere karşı birleşik bir yanıt verilmesini kolaylaştırır. Ulus-devlet destekli saldırılara ve sınır aşan siber suçlara karşı toplu savunmayı güçlendirir.

Proaktif savunma önlemleri, siber tehditlerin ortaya çıkmadan önce öngörülmesini ve önlenmesini içerir. Kuruluşlar sürekli izleme, güvenlik açığı değerlendirmeleri ve düzenli güvenlik denetimleri uygulamaktadır. Çalışanlar için güvenlik farkındalığı eğitimine öncelik verir ve sağlam erişim kontrolleri ve kimlik doğrulama mekanizmaları uygularlar. Güvenlik açıklarını istismar edilmeden önce tespit ederek ve yamalayarak saldırı yüzeyini azaltır. Kullanıcıları potansiyel tehditleri tanımaları ve bildirmeleri konusunda eğiterek güvenlik bilincine sahip bir kurum kültürüne katkıda bulunur.

Siber güvenliğin dinamik ortamında, gelişmiş savunma mekanizmalarını benimsemek sadece bir strateji değil; bir gerekliliktir. Davranışsal analitik ve anomali tespiti için yapay zekâ ve makine öğrenimini entegre ederek, tehdit istihbarat paylaşımını benimseyerek, uluslararası iş birliğini teşvik ederek ve proaktif savunma önlemleri uygulayarak kuruluşlar, dijital çağı tanımlayan gelişen ve sofistike tehditlere karşı dayanıklılıklarını artırabilirler.

Siber Güvenlikte İnsan Unsuru

Teknolojik gelişmeler siber güvenlikte çok önemli bir rol oynasa da insan unsuru dijital savunmanın güçlendirilmesinde çok önemli bir faktör olmaya devam etmektedir. Siber güvenlik farkındalığı, eğitimi ve uyanıklığı yoluyla insani güvenlik açıklarının anlaşılması ve ele alınması, kapsamlı bir savunma stratejisinin temel bileşenleridir.

İnsan hatası, siber tehditler için yaygın bir giriş noktasıdır. Çalışan eğitim programları, personeli potansiyel riskleri belirlemek ve azaltmak için gereken bilgi ve becerilerle donatmak üzere tasarlanmıştır. Düzenli eğitim oturumları kimlik avı girişimlerini tanıma, sosyal mühendislik taktiklerini anlama ve en iyi güvenlik uygulamalarına bağlı kalma gibi konuları kapsar. Eğitim, uygunluğu sağlamak için bir kuruluş içindeki farklı rollere göre uyarlanır. Çalışanları siber güvenliğe proaktif katkıda bulunmaları için güçlendirir. Güvenlik ihlallerine yol açabilecek kasıtsız eylemlerin olasılığını azaltarak kuruluşun genel güvenlik duruşunu geliştirmektedir.

Güvenlik bilincine sahip bir kültür oluşturmak, siber güvenliğin bir kurumun tüm üyeleri tarafından önceliklendirildiği bir zihniyetin teşvik edilmesini içermektedir. Liderlik, kurumsal hedeflerde siber güvenliğin önemini vurgulayarak ortamı belirlemektedir. Düzenli iletişim, haber bültenleri ve kurum içi kampanyalar, genel güvenliğe bireysel katkıların önemini pekiştirir. Siber güvenlik için ortak bir sorumluluk duygusu aşılar. Çalışanları uyanık olmaya, şüpheli faaliyetleri bildirmeye ve güvenli bir ortamın sürdürülmesine aktif olarak katkıda bulunmaya teşvik eder. Sosyal mühendislik, bireyleri hassas bilgileri ifşa etmeye veya güvenliği tehlikeye atan eylemlerde bulunmaya yönlendirmek için insan psikolojisinden yararlanmaktadır. Eğitim programları, çalışanları oltalama e-postaları, bahane uydurma ve kimliğe bürünme gibi yaygın sosyal mühendislik taktikleri hakkında eğitir. Simüle edilmiş oltalama egzersizleri farkındalığı güçlendirmeye yardımcı olur ve kuruluşların eğitimlerinin etkinliğini ölçmelerine olanak tanımaktadır. Sosyal mühendislik saldırılarına kurban gitme riskini azaltır. Saldırganlar tarafından kullanılan taktikler hakkında farkındalık yaratır, bireyleri manipülasyonu fark etme ve direnme konusunda güçlendirir.

İster kasıtlı ister kasıtsız olsun, içeriden kişiler siber güvenlik için önemli riskler oluşturabilir. Bu tehditler hoşnutsuz çalışanlardan, insan hatalarından veya hassas bilgilerin yanlışlıkla paylaşılmasından kaynaklanabilir. Çalışan farkındalık programları, içeriden gelen tehditlerin potansiyel göstergelerini vurgular. Kullanıcı faaliyetlerinin düzenli olarak izlenmesi, içeriden risklere işaret edebilecek olağandışı modellerin tespit edilmesine yardımcı olur. İçeriden gelen tehditlerin erken tespit edilmesini ve müdahale edilmesini sağlar. Şeffaflık ve raporlama kültürü yaratarak kazara veya kötü niyetli içeriden öğrenenlerin eylemlerinin etkisini azaltır.

Kullanıcı dostu sistemler ile sağlam güvenlik önlemleri arasında bir denge kurmak, kullanıcı direncini ve güvenlik protokollerinin atlatılmasını önlemek için kritik öneme sahiptir. Sezgisel ve kullanıcı dostu arayüzler tasarlamak ve en iyi güvenlik uygulamaları konusunda sürekli

eğitim vermek, kullanıcıların kendilerini engellenmiş hissetmeden güvenlik önlemlerinin önemini anlamalarına yardımcı olur. Kullanıcı üretkenliğinden ödün vermeden genel sistem güvenliğini artırır. Güvenlik önlemlerine karşı olumlu bir tutumu teşvik eder.

Sürekli gelişen siber güvenlik ortamında insan unsuru hem potansiyel bir zayıflık hem de güçlü bir savunma hattıdır. Kuruluşlar siber güvenlik farkındalığına, eğitime yatırım yaparak ve güvenlik bilincine sahip bir kültürü teşvik ederek, personellerini insani açıklardan yararlanan çok çeşitli tehditlere karşı proaktif savunucular haline getirebilirler. Bireylerin güvenli bir dijital ortamın sürdürülmesinde oynadıkları kritik rolü kabul etmek, kapsamlı bir siber güvenlik stratejisinin temelini oluşturmaktadır.

Düzenleyici Çerçeveler ve Uyumluluk

Dijital ortam gelişmeye devam ettikçe, düzenleyici çerçeveler ve uyum standartları, sektörler genelinde siber güvenlik uygulamalarının şekillendirilmesinde etkili hale gelmiştir. Mevzuat ortamını anlamak sadece yasal bir bağlılık meselesi değil, aynı zamanda sürekli genişleyen bir dizi siber tehdide karşı savunmalarını güçlendirmek isteyen kuruluşlar için stratejik bir zorunluluktur. Dünya çapında hükümetler kritik altyapıyı korumak, hassas verileri muhafaza etmek ve siber tehditleri azaltmak için siber güvenlik düzenlemeleri uygulamaya koymuştur. Bu düzenlemeler, bölgelere göre değişmekle birlikte genellikle ortak ilkeleri paylaşmaktadır: Avrupa'da GDPR (Genel Veri Koruma Yönetmeliği), ABD'de HIPAA (Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası) ve Çin'de Siber Güvenlik Yasası.

Çeşitli endüstriler, sektöre özgü siber güvenlik sorunlarını ele almak için standartlar oluşturmuştur. Bu standartlara uyum, kritik sistemlerin ve verilerin bütünlüğünü ve güvenliğini sağlamak için genellikle zorunludur. Bilgi güvenliği yönetimi için ISO/IEC 27001, ödeme kartı endüstrisi için PCI DSS (Ödeme Kartı Endüstrisi Veri Güvenliği Standardı) ve ABD'deki kritik altyapı sektörleri için NIST Siber Güvenlik Çerçevesi örnek verilebilir.

Düzenlemeler genellikle kişisel ve hassas verilerin korunması için sıkı önlemler alınmasını zorunlu kılmaktadır. Buna şifreleme, erişim kontrolleri ve düzenli veri gizliliği değerlendirmeleri dahildir. Kuruluşlar veri yönetişimi uygulamalarını geliştirmeli, sağlam şifreleme protokolleri uygulamalı ve şeffaf veri işleme süreçleri sağlamalıdır.

Düzenlemeler genellikle kuruluşların olay müdahale planları oluşturmalarını ve test etmelerini ve siber güvenlik olaylarını derhal rapor etmelerini gerektirir. Kuruluşlar olay müdahale ekipleri geliştirmeli, düzenli tatbikatlar yapmalı ve olayları ilgili makamlara bildirmek için mekanizmalar oluşturmalıdır. Uyumluluk standartları ağların, sistemlerin ve verilerin sürekli olarak izlenmesi gerektiğini vurgulamaktadır. Düzenli denetimler, güvenlik politikalarına ve standartlarına uyulmasını sağlamaktadır.

Uyumluluğun sağlanması ve sürdürülmesi, özellikle sınırlı bütçeye sahip küçük işletmeler için bir kuruluşun kaynaklarını zorlayabilmektedir. Etkili kaynak tahsisi, uygun maliyetli teknolojilerden yararlanma ve stratejik planlama, kuruluşların mali durumlarına aşırı yük getirmeden uyumluluk gerekliliklerini karşılamalarına yardımcı olabilmektedir.

Uyumluluk önlemleri, siber tehditlerin hızla gelişen doğasına ayak uydurmakta zorlanabilmektedir. Siber güvenliğe risk tabanlı bir yaklaşım uygulamak, kuruluşların sürekli risk değerlendirmeleri ve güvenlik protokollerinde güncellemeler yoluyla uyumluluğu sürdürürken ortaya çıkan tehditlere uyum sağlamasına olanak tanımaktadır.

Küresel bir varlığı olan kuruluşlar, çeşitli düzenlemeler ve standartlardan oluşan karmaşık bir ağda gezinmek zorundadır. Birden fazla yönetmelikle uyumlu birleşik bir siber güvenlik çerçevesi geliştirmek, bir uyumluluk bilinci kültürünü teşvik etmek ve hukuk ve siber güvenlik uzmanlarından yararlanmak bu karmaşıklığın üstesinden gelmeye yardımcı olabilir.

Sonuç olarak, düzenleyici çerçeveler ve uyum standartları, sağlam siber güvenlik uygulamaları oluşturmaya çalışan kuruluşlar için paha biçilmez kılavuzlar olarak hizmet etmektedir. Uyumluluk zorlukları beraberinde getirirken, kurumların güvenlik duruşlarını geliştirmeleri, müşterilerin güvenini kazanmaları ve sorumlu veri yönetimine bağlılıklarını göstermeleri için fırsatlar da sunmaktadır. Dijital ortamın dinamik doğası ile uyumluluğu dengelemek, siber güvenlik yönetişimine bütüncül ve uyarlanabilir bir yaklaşım gerektirir.

Vaka Çalışmaları ve Pratik Uygulamalar

Sürekli gelişen siber güvenlik ortamında gerçek dünya deneyimlerinden öğrenmek çok önemlidir. Gelişmiş savunma stratejilerinin başarılı uygulamalarını incelemek, son olaylardan çıkarılan dersleri anlamak ve en iyi uygulamaları benimsemek, kurumların ve bireylerin siber tehditlere karşı dayanıklılığını önemli ölçüde artırabilir.

Microsoft'un Dijital Suçlar Birimi (DCU) Vaka Çalışmasında Microsoft'un DCU'su, siber suç ağlarını bozmak ve kötü niyetli faaliyetleri engellemek için gelişmiş savunma stratejilerini başarıyla uygulamıştır. Tehdit istihbaratından, yasal işlemlerden ve iş birliğine dayalı ortaklıklardan yararlanan Microsoft, proaktif bir şekilde siber suç altyapısını hedef alarak botnetlerin kaldırılmasına ve büyük ölçekli siber operasyonların aksamasına yol açmıştır. Yasal, teknik ve iş birliğine dayalı önlemlerin entegrasyonu, siber suçlarla mücadelede ve kötü niyetli ağları bozmada güçlü bir strateji olabilir.

Bir diğer Örnek Uygulama da Google'ın Gelişmiş Koruma Programıdır. Google'ın Gelişmiş Koruma Programı, siyasi aktivistler, gazeteciler ve iş dünyası liderleri de dahil olmak üzere yüksek riskli kullanıcılar için ekstra bir güvenlik katmanı sağlamaktadır. Program, hesapları kimlik avı ve hesap ele geçirme girişimlerine karşı korumak için donanım güvenlik anahtarları, gelişmiş hesap koruması ve titiz doğrulama süreçleri kullanmaktadır. Gelişmiş güvenlik

önlemlerinin belirli kullanıcı profillerine ve tehdit ortamlarına göre uyarlanması, hedefli saldırı riskini önemli ölçüde azaltabilir.

SolarWinds olayı, yazılım tedarik zincirlerinin kırılganlığını ve sofistike saldırıların güvenilir satıcıları tehlikeye atma potansiyelini vurgulamıştır. Kuruluşların, üçüncü taraf yazılım sağlayıcılarının kapsamlı bir şekilde incelenmesi ve yazılım bütünlüğünün sürekli izlenmesi de dahil olmak üzere sağlam tedarik zinciri güvenlik önlemleri uygulaması gerekmektedir.

Colonial Pipeline olayı, fidye yazılımı saldırılarının kritik altyapı üzerindeki etkisini ve olay müdahale planlarının önemini vurgulamıştır. Kuruluşlar, fidye yazılım saldırılarının etkisini en aza indirmek için olay müdahale planlamasına öncelik vermeli, düzenli olarak tatbikatlar yapmalı ve net iletişim ve karar alma protokolleri oluşturmalıdır.

Güvenin asla varsayılmadığı ve ağ içindeki kaynaklara erişmeye çalışan herkesten doğrulamanın istendiği Sıfır Güven yaklaşımı benimsenmelidir. Çalışanlar için en son tehditleri, kimlik avı farkındalığını ve güvenli uygulamaları vurgulayarak devam eden siber güvenlik eğitimi verilmelidir. Kişisel hesaplara ekstra bir güvenlik katmanı eklemek için mümkün olan her yerde Çok Faktörlü Kimlik Doğrulamayı (MFA) etkinleştirilmelidir. Güvenlik açıklarını kapatmak ve bilinen istismarlara karşı koruma sağlamak için yazılımlar, işletim sistemleri ve uygulamalar güncel tutulmalıdır.

Siber güvenlik alanında, gerçek dünyadaki vaka çalışmaları ve pratik uygulamalar, teorik çerçevelerin ötesine geçen değerli bilgiler sunmaktadır. Kuruluşlar ve bireyler uyanık kalmalı, başarılı uygulamalardan ders almalı, son olaylardan çıkarılan dersleri anlamalı ve en iyi uygulamaları benimsemelidir. Siber ortam geliştikçe, sürekli öğrenme ve iş birliği ile beslenen proaktif ve uyarlanabilir bir yaklaşım, dijital esneklik için devam eden arayışta çok önemli hale gelmektedir.

Gelecek Trendler ve Gelişen Teknolojiler

Teknoloji ilerledikçe hem siber tehditler hem de savunma mekanizmaları tarafından kullanılan stratejiler ve teknolojiler de gelişmektedir. Gelecekteki eğilimleri öngörmek, siber güvenliğin sürekli gelişen ortamında bir adım önde olmak için çok önemlidir. Siber suçlular tarafından saldırıların karmaşıklığını artırmak, görevleri otomatikleştirmek ve geleneksel güvenlik önlemlerinden kaçınmak için yapay zekâ kullanımı önemlidir. Yapay zekâ güdümlü saldırılar, güvenlik açıklarından daha verimli bir şekilde faydalanabilir, savunma önlemlerine gerçek zamanlı olarak uyum sağlayabilir ve belirli kişi veya kuruluşları benzeri görülmemiş bir hassasiyetle hedef alabilir. Özellikle fidye yazılımlarının, RaaS (Hizmet Olarak Fidye Yazılım) platformları aracılığıyla metalaştırılması, teknik bilgi seviyesi düşük aktörlerin bile sofistike saldırılar gerçekleştirmesine olanak tanımaktadır. Fidye yazılım araçlarına ve altyapısına kolay erişim, bu tür saldırıların sıklığını artıran önemli bir faktördür. Bu durum, fidye yazılım saldırılarının yaygınlaşmasının önümüzdeki dönemde daha büyük bir tehdit oluşturacağını göstermektedir.

Tedarik zincirlerinin sürekli hedef alınması ve dijital casusluğun artması, saldırganların güvenilir kuruluşları hedefleyerek hassas bilgilere yetkisiz erişim sağlama girişimlerini artırmaktadır. Saldırganların birbirine bağlı ağları sömürmesi ve tespit edilmeden kalmak için sofistike taktikler kullanması nedeniyle, organizasyonlar için risk seviyesi yükselmektedir.

Kullanıcı davranışları ve ağ aktivitelerindeki anormallikleri tespit etmek için gelişmiş davranış analitiği ve makine öğrenimi algoritmaları kullanılmaktadır. Normal kalıplardan sapmalar temelinde tehditlerin proaktif şekilde belirlenmesi, erken tespit ve müdahale imkanı sağlamaktadır. Güvenlik araçları ve teknolojilerinin entegre edilerek merkezi bir platformda tespit, inceleme ve müdahale süreçlerinin birleştirilmesi, görünürlüğü artırmakta ve olaylara müdahale yeteneklerini optimize etmektedir. Bu sayede siber tehditlerin tespit ve etkisiz hale getirilme süresi kısalmaktadır.

Bulut ortamlarına özel olarak tasarlanmış güvenlik çözümlerinin geliştirilmesi, bulut tabanlı altyapının getirdiği benzersiz zorluklara odaklanmaktadır. Bulut ortamlarındaki veri ve uygulamalar için artırılmış koruma sağlanarak, güvenlik önlemlerinin bulut bilişime geçişle birlikte gelişmesi garanti altına alınmaktadır.

RSA ve ECC gibi yaygın olarak kullanılan kriptografik algoritmaları kırabilecek kapasitede kuantum bilgisayarların ortaya çıkışı, güvenlik alanında önemli bir değişimi beraberinde getirmektedir. Kuantum saldırılarına dayanıklı post-kuantum kriptografi algoritmalarına duyulan ihtiyaç, kuantum güvenli kriptografik çözümler üzerine araştırma ve geliştirmeyi hızlandırmaktadır. Kuantum mekaniği, QKD (Kuantum Anahtar Dağıtımı) aracılığıyla iletişim kanallarını güvence altına almak için kullanılmakta ve anahtar değişimi için teorik olarak güvenli bir yöntem sunmaktadır. Kuantum bilişimin oluşturabileceği potansiyel tehditlere

karşı iletişim sistemlerinin güvenliği artırılmaktadır. Post-kuantum hesaplama çağında verilerin korunması için kuantum güvenli şifreleme algoritmalarına yönelik standartlar oluşturulmaktadır. Gelecekteki kuantum saldırılarından hassas veri ve iletişimleri korumak amacıyla kuantum güvenli şifreleme algoritmalarına geçiş yapılmaktadır.

Siber tehditlerin evrilmesi ve teknolojinin ilerlemesiyle birlikte, siber güvenliğin geleceği proaktif uyum sağlamaya bağlıdır. Siber tehditlerdeki gelişmeleri öngörmek, değişen savunma stratejileri ve teknolojilerini benimsemek ve kuantum bilişimin etkisine hazırlıklı olmak, dijital dünyada başarılı bir şekilde yol almak için kritik adımlardır. Siber güvenlik ortamı dinamik kalmaya devam edecek ve bu da dijital alanı koruma konusunda sürekli yenilik, iş birliği ve stratejik bir yaklaşımı zorunlu kılmaktadır.

Öneri

Gelişen siber tehditleri proaktif olarak belirlemek ve bunlara yanıt vermek için davranışsal analitik ve makine öğrenimi dahil olmak üzere gelişmiş tehdit algılama teknolojilerini uygulanmalıdır. Her seviyedeki çalışanlar için kapsamlı siber güvenlik farkındalık programları ve eğitim girişimleri oluşturulmalıdır. İyi bilgilendirilmiş bir işgücü, sosyal mühendislik ve diğer insan merkezli saldırılara karşı çok önemli bir savunma hattıdır. Güvenin asla varsayılmadığı ve ağa erişen tüm kullanıcılar ve cihazlar için sürekli doğrulamanın gerekli olduğu Sıfır Güven modeli benimsenmelidir. Bu yaklaşım, saldırganların ağ içinde yanal hareket riskini azaltmaya yardımcı olur. Kuruluşlar bulut bilişimi giderek daha fazla benimsedikçe, bulut ortamları için özel olarak tasarlanmış güvenlik önlemleri uygulanmalıdır. Güvenlik protokollerinin buluta geçişle birlikte geliştiğinden emin olunmalıdır. Siber olaylara hızlı ve koordineli bir müdahale sağlamak için olay müdahale planları geliştirilmeli ve düzenli olarak test edilmelidir. Buna açık iletişim protokolleri, tanımlanmış roller ve güvenlik ihlallerinin etkisini azaltmaya yönelik kapsamlı bir strateji dahildir. Ortaya çıkan siber tehditlerin ve güvenlik açıklarının sürekli izlenmesi için mekanizmalar oluşturulmalıdır. Gelişen tehdit ortamının bir adım önünde olmak için tehdit istihbaratı paylaşım girişimlerine aktif olarak katılım sağlanmalıdır.

Kuantum bilişimin kriptografik sistemler üzerindeki etkisini öngörülmelidir. Hassas veri ve iletişimlerin uzun vadeli güvenliğini sağlamak için kuantum sonrası kriptografi standartlarına geçilmeye başlanmalıdır.

Sonuç

Sonuç olarak, siber güvenlikle ilgili kapsamlı inceleme, gelişmiş savunma stratejileri aracılığıyla modern tehditlerin önünde kalmanın kritik önemini vurgulamaktadır. Siber tehditler daha karmaşık hale geldikçe, kuruluşlar siber güvenliğe proaktif ve uyarlanabilir bir yaklaşım benimsemelidir. Gelişmiş teknolojilerden yararlanarak, güvenlik bilincine sahip bir kültür oluşturarak ve kuantum bilişim gibi gelecekteki gelişmelere hazırlanarak kuruluşlar dayanıklılıklarını artırabilir ve dijital varlıklarını etkili bir şekilde koruyabilir. Şifreleme bir seçenek değildir ve güvenlik olayları kelimenin her anlamıyla çok pahalıdır.

Siber ortamın dinamik yapısı, insanları, süreçleri ve teknolojileri kapsayan bütünsel bir strateji gerektirmektedir. Sadece çevre güvenliği artık bir seçenek değildir. Belirsizlik yoluyla güvenlik de değildir. Siber güvenlik tek seferlik bir çaba değil, bilgi sahibi olmaya, güvenlik önlemlerini geliştirmeye ve siber güvenlik topluluğu içinde iş birliği yapmaya yönelik sürekli bir taahhüttür. Kuruluşlar dijital çağın karmaşıklığı içinde yol alırken, dijital geleceği güvence altına almak için siber güvenliğe yönelik ileriye dönük ve stratejik bir yaklaşım çok önemlidir.[4]

4 https://www.researchgate.net/publication/377957344

YENİLİK VE ÖRNEK ÇALIŞMALAR
YAPAY ZEKÂ

Litvanya'da Yapay Zekanın Gelişimi

Litvanya, "AI Sandbox" olarak bilinen pilot yapay zeka (AI) ortamını başlatan Avrupa Birliği'ndeki (AB) ilk ülkelerden biri haline gelmiştir. Bu alan, Litvanyalı teknoloji şirketlerinin IoT çözümlerini pazara sunmadan önce güvenli bir şekilde tasarlamalarına, test etmelerine ve geliştirmelerine olanak tanıyacaktır. Bu durum ayrıca, ülkenin işletmelerinin inovasyonu hızlandırmasını ve küresel pazarda rekabet etmesini sağlayacaktır. Hükümet, AB'nin IoT düzenlemesinin uygulanmasını hızlandırmak için gereken yeni düzenlemeleri onaylamıştır. İnovasyon Ajansı ve İletişim Düzenleme Kurumu bu alandan sorumlu ana kuruluşlar olacaktır. Amaçları, yeni kurulan şirketlere ve diğer işletmelere destek sağlamak ve IoT çözümlerinin kullanıcılar için güvenilir ve emniyetli olmasını sağlamaktır.

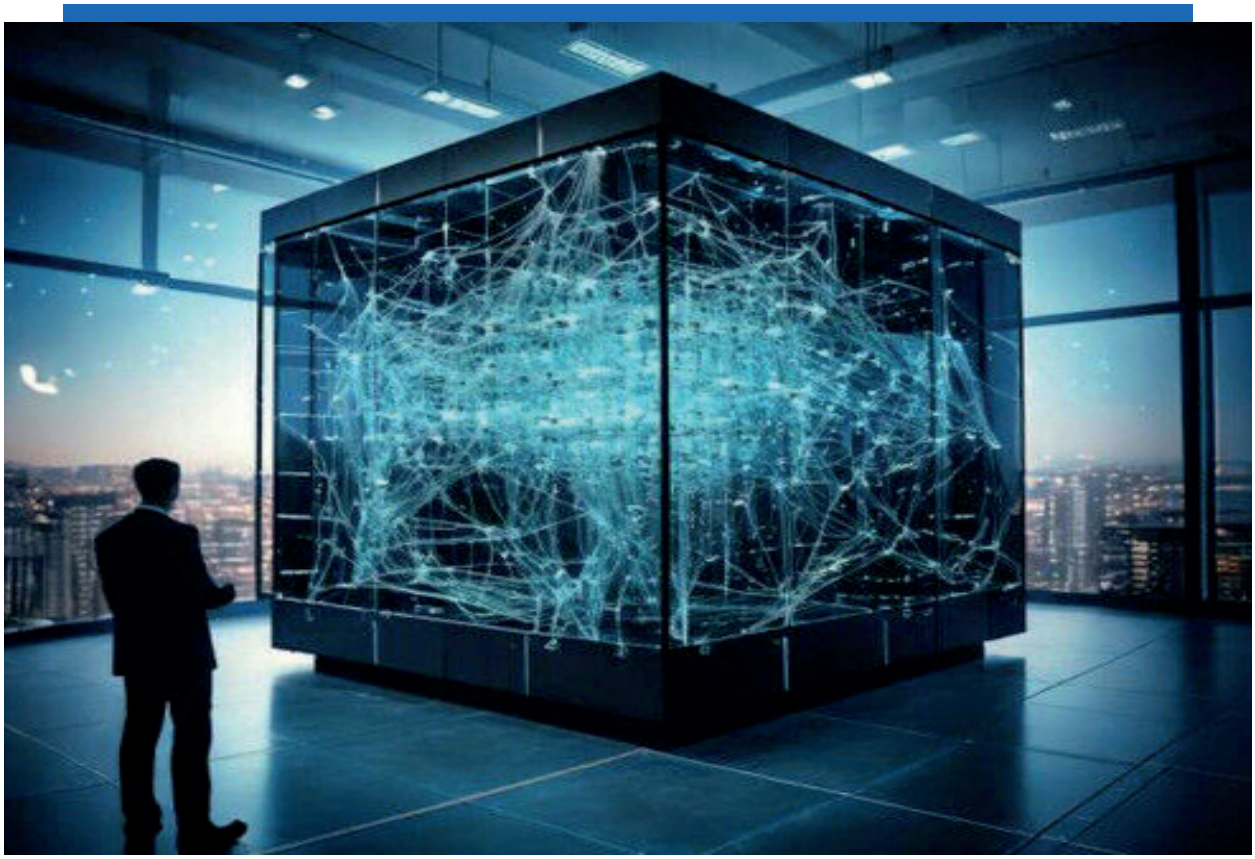
Ekonomi ve Yenilik Bakanı Aušrinė Armonaitė yaptığı açıklamada yapay zeka teknolojilerinin ekonomiler için büyük bir potansiyeli olduğunu, bir 'kum havuzu' oluşturarak, işletmelerin yeniliklerini güvenli bir şekilde test edebilecekleri ve tüketicilerin IoT ürünlerinin tüm güvenlik gereksinimlerini karşıladığından emin olabilecekleri bir alan açtıklarını söylemiştir. Ekonomi

ve İnovasyon Bakan Yardımcısı Erika Kuročkina ise yaptığı açıklamada şunları söylemiştir. "Bu yeni yaklaşım, Litvanya şirketlerinin IoT'nin sunduğu fırsatları daha hızlı yakalamasını sağlayacak ve girişimciler teknolojilerinin Avrupa standartlarını karşıladığından daha emin hissedebilecek. Ayrıca, İnovasyon Ajansı, Avrupa genelinde IoT sistemleri için sertifika hizmetleri sağlamak isteyen kuruluşları değerlendirecek. Bu, ülkenin inovasyon ekosistemini daha da güçlendirmeye yardımcı olacak".

Hükümet tarafından kabul edilen değişiklikler, İletişim Düzenleme Kurumu ile birlikte AB'nin Yapay Zeka Yasası'nı uygulamaktan sorumlu ana organ olacak olan Yenilik Ajansı için farklı bir rol de belirlemiştir. Yenilik Ajansı ulusal bildirim makamı olarak belirlenirken, İletişim Düzenleme Kurumu pazar denetçisi ve tek iletişim noktası olarak hareket edecektir. Yenilik Ajansı, Bildirilmiş Kuruluş olmak isteyen kuruluşlar için Yapay Zeka Yasası gerekliliklerine uyumu değerlendirecek ve AB genelinde IoT sistemleri için değerlendirme hizmetleri sağlayacaktır. İletişim Düzenleme Kurumu ise IoT sistemlerinin piyasa gözetimini gerçekleştirecektir.[5]

5 https://eimin.lrv.lt/en/structure-and-contacts/news-1/lithuania-accelerates-development-of-artificial-intelligence-by-creating-a-sandbox-to-test-the-technology/

Araştırmacılardan Yapay Zekanın Yasalara Uyma Durumuna Test



Avrupa Birliği Yapay Zekâ Yasası, yapay zekanın şeffaf ve güvenilir olmasını sağlamak için tasarlanmıştır. ETH bilgisayar bilimcileri, Yasayı ilk kez yapay zekâ için ölçülebilir teknik gerekliliklere dönüştürmüştür. Bunu yaparken, günümüz yapay zekâ modellerinin yasal gerekliliklere ne kadar iyi uyduğu gösterilmiştir.

ETH Zürih'ten araştırmacılar, ETH ve EPFL ortaklığıyla oluşturulan Bulgar yapay zekâ araştırma enstitüsü INSAIT ve ETH yan kuruluşu LatticeFlow AI, Genel Amaçlı AI (GPAI) modelleri için AB Yapay Zekâ Yasası'nın ilk kapsamlı teknik yorumunu sağlamıştır. Bu, onları AB'nin gelecekteki yapay zekâ modellerine koyduğu yasal gereklilikleri somut, ölçülebilir ve doğrulanabilir teknik gerekliliklere dönüştüren ilk kişiler haline getirmektedir. Araştırmacılar, model geliştiricilerin gelecekteki AB yasal gereklilikleriyle ne kadar uyumlu olduklarını görmeleri için pratik bir yaklaşım sunmaktadır.

Araştırmacılar, yaklaşımlarını ChatGPT, Llama, Claude veya Mistral gibi on iki popüler üretken yapay zekâ modeli üzerinde test etmiştir. Sonuçta, bu büyük dil modelleri yapay zekanın (YZ) günlük yaşamda artan popülaritesine ve dağıtımına muazzam bir katkıda bulunmaktadır, çünkü kullanımları çok yetenekli ve sezgiseldir. Bu ve diğer yapay zekâ modellerinin artan dağıtımıyla, YZ'nin sorumlu kullanımı için etik ve yasal gereklilikler de artmaktadır. Örneğin, veri koruması, gizlilik koruması ve YZ modellerinin şeffaflığı konusunda hassas sorular ortaya

çıkmaktadır. Modeller "kara kutular" olmamalı, bunun yerine mümkün olduğunca açıklanabilir ve izlenebilir sonuçlar sunmalıdır. Ayrıca, adil bir şekilde çalışmalı ve kimseye karşı ayrımcılık yapmamalıdırlar. Bu bağlamda, AB'nin Mart 2024'te kabul ettiği AB Yapay Zekâ Yasası, bu teknolojilere olan kamu güvenini kapsamlı bir şekilde en üst düzeye çıkarmayı ve istenmeyen riskleri ve yan etkilerini en aza indirmeyi amaçlayan dünyanın ilk yapay zekâ yasa paketidir.

ETH Güvenli, Güvenilir ve Akıllı Sistemler Laboratuvarı başkanı ve INSAIT kurucusu Prof. Martin Vechev "AB Yapay Zeka Yasası, sorumlu ve güvenilir yapay zeka geliştirmeye yönelik önemli bir adımdır ancak şu ana kadar AB Yapay Zeka Yasası'ndaki üst düzey yasal gerekliliklerin açık ve kesin bir teknik yorumundan yoksunuz. Bu, hem yasalara uygun yapay zekâ modelleri geliştirmeyi hem de bu modellerin mevzuata ne ölçüde uyduğunu değerlendirmeyi zorlaştırıyor." açıklamasında bulunmuştur.

AB Yapay Zekâ Yasası, sözde Genel Amaçlı Yapay Zekâ (GPAI) risklerini sınırlamak için açık bir yasal çerçeve belirlemektedir. Ancak yasa, geniş yasal gerekliliklerin teknik olarak nasıl yorumlanacağını belirtmemektedir. Yüksek riskli YZ modelleri için düzenlemeler Ağustos 2026'da yürürlüğe girene kadar teknik standartlar hala geliştirilmektedir. Araştırmacılar tarafından geliştirilen metodoloji, tartışma için bir başlangıç noktası ve temel sunmaktadır. Ayrıca araştırmacılar, YZ modellerinin AB YZ Yasası'nın olası gerekliliklerine ne kadar iyi uyduğunu değerlendirmek için kullanılabilecek bir dizi ölçüt olan ilk uyumluluk denetleyicisini de geliştirmiştir. Araştırmacılar bulgularını bir çalışmada kamuya açık hale getirmiştir ve sonuçlar, YZ Yasası'nın uygulanmasında ve dolayısıyla model değerlendirmesi için de önemli bir rol oynayan AB YZ Ofisi'ne de sunulmuştur.

Araştırmacılar, kıyaslama yaklaşımlarını 12 önemli dil modeline (LLM) uygulamıştır. Sonuçlar, bugün analiz edilen dil modellerinin hiçbirinin AB YZ Yasası'nın gerekliliklerini tam olarak karşılamadığını açıkça ortaya koymuştur. Bu büyük dil modellerinin karşılaştırılması, özellikle sağlamlık, çeşitlilik ve adalet gibi gereklilikler açısından eksiklikler olduğunu ortaya koymuştur. Bunun ayrıca, son yıllarda model geliştiricilerinin ve araştırmacıların, adalet veya ayrımcılık yapmama gibi daha etik veya sosyal gereklilikler yerine öncelikle genel model yeteneklerine ve performansına odaklanmasıyla da ilgisi bulunmaktadır.

Martin Vechev açıklamasının devamında, çalışmalarını YZ Yasası'nın uygulanmasını sağlamak ve model sağlayıcıları için uygulanabilir öneriler elde etmek için bir itici güç olarak gördüklerini, ancak metodolojilerinin AB YZ Yasası'nın ötesine geçebileceğini ve diğer karşılaştırılabilir mevzuatlar için de uyarlanabileceğini söylemiştir.

Araştırmacılar, teknik tartışmayı başlatmak için kıyaslama aracı COMPL-AI'yi bir GitHub web sitesinde kullanıma sunmuştur. Kıyaslamalarının sonuçları ve yöntemleri orada analiz edilebilecek ve görselleştirilebilecektir.[6]

6 https://www.myscience.ch/news/2024/how_law_abiding_is_ai_researchers_put_it_to_the_test-2024-ethz

Yapay Zeka Sayesinde Sohbet Edebilen Dodo

Cambridge'deki bir müze deneyi; yapay zeka yardımıyla ziyaretçilerin bir Dodo ve diğer ölmüş hayvanlarla sohbet etmesine olanak sağlamaktadır. En son 17. yüzyılda görülen Mauritius dodo kuşunun sanal bir versiyonu ile yapay zeka teknolojisi sayesinde ziyaretçiler artık akıllı cihazları aracılığıyla gerçek zamanlı konuşmalar yapabilmektedir. Yapay zeka destekli deneyim; dodonun, denizcilerin ana adası Mauritius'a gelmesinden sonra neslinin nasıl tükendiği de dahil olmak üzere yaşamıyla ilgili soruları yanıtlamasına olanak tanımaktadır. Hatta bilim insanları tarafından yeniden klonlanmak isteyip istemediği gibi daha etik soruları bile algılayabilmektedir.

Cambridge Zooloji Müzesi müdür yardımcısı Jack Ashby, yapay zekanın ziyaretçilerin müze sergileriyle etkileşime girmesi için yeni bir yol sunduğunu düşünmektedir. Projede her biri kendine özgü bir sese sahip 12 hayvan örneği daha yer almaktadır. Yapay zeka deneyiminde yer alan bu hayvanlar arasında Ornitorenk, Megatherion, bir deniz gergedanı, bir kelebek, bir yüzgeçli balina ve bir hamamböceği bulunmaktadır.[7]

7 https://www.euronews.com/culture/2024/10/15/extinct-no-more-ai-is-bringing-the-dodo-back-to-life-kinda-at-a-museum-in-cambridge

BAE'den, Bölgenin İlk Yapay Zeka Destekli Hukuk Uzmanı Sanal Avukat

Adalet Bakanlığı, Devlet Geliştirme ve Gelecek Ofisi ve BAE Hükümeti Yapay Zeka, Dijital Ekonomi ve Uzaktan Çalışma Uygulamaları Ofisi ile ortaklaşa olarak, GITEX etkinlikleriyle bağlantılı şekilde, yapay zeka tarafından etkinleştirilen "Sanal Avukat" projesini duyurmuştur.

Proje, hukuk kurumlarının basit davalarda savunma geliştirmelerine yardımcı olmakta ve adalet sektörünün gelecekteki fırsatlara ve değişkenlere ve bunların adalet sektörü ve hukuk meslekleri üzerindeki etkilerine hazırlıklı olmasına ve dijital ve interaktif bir dava ortamında hizmetleri hızlandırmak ve müşteri deneyimini iyileştirmek için yeni devlet modelleri oluşturmak üzere ileri teknoloji ve yapay zeka kullanılmasına katkıda bulunmaktadır.

BAE, bölgede türünün ilk örneği olan sanal avukat ile dava sürecinin hızlandırılması, hizmetlerin ve küresel liderliğin geliştirilmesi ve davacının yolculuğunun kolaylaştırılması konularında katma değer elde etmeyi amaçlamaktadır. Adalet Bakanlığı tarafından oluşturulacak birleşik ulusal mevzuat metinleri veri tabanını kullanacak olan sanal avukatı kullanmak isteyen hukuk büroları, sanal avukatı bakanlığa kaydettirdikten sonra veri tabanını beslemek zorunda olacaktır.

Pilot versiyon 2025'te başlatılacak ve gelecekteki hükümetlerin sağlamayı hedeflediği gelişmiş dijital çözümlerle geliştirilmiş hizmetler için bir model olacaktır. İlk aşamada, avukatlara basit davalarda, özellikle de bir insan hakimle etkileşim kurma, sesi metne ve tersine çevirme ve muhtıra ve belge gönderme gibi özelliklerle yardımcı olmakla sınırlıdır.

Adalet Bakanı Abdullah Sultan Bin Awad Al Nuaimi, bakanlığın sürekli olarak adalete hizmet eden ve prosedürlerin verimliliğini artıran yenilikleri ve vizyonları kullanmaya çalıştığını ve en iyi uluslararası uygulamalara uygun şekilde yararlanıcılara sağlanan hizmetlerin kalitesini artırmak istediklerini açıklamıştır. Ayrıca, yapay zeka teknolojilerinin, güvenli bir toplum ve rekabetçi bir ekonomide adaleti tesis eden modern, esnek ve etkileşimli yollarla yargı sistemini geliştirmede kendilerine yeni ufuklar açtığını, operasyonel verimliliğin artırılmasına, zaman ve çabanın kısaltılmasına, prosedürlerin etkinliğinin artırılmasına, karar vermede doğruluk ve hızın artırılmasına ve yargı sistemi üzerindeki idari yükün azaltılmasına katkıda bulunacağını; bu teknolojilere tam anlamıyla yatırım yaparak bilgi ekonomisinin ve dijital açıklık çağının gerekliliklerine ayak uydurmak için çalıştıklarını sözlerine eklemiştir.

Proje, ülkedeki yasal çalışma ortamını ilerletmek ve küresel düzeyde taklit edilecek bir model haline getirmek için yapay zekayı kullanarak yeni ve farklı fırsatlar sunacaktır. Adalet Bakanlığı ayrıca, vatandaşların hayatını kolaylaştırmak için sürekli çaba göstererek devlet hizmetlerini geliştirme çabalarını artırmaya yönelik bilge liderliğin direktiflerinin uygulanmasında, yeni hukuk mesleklerine ayak uydurmak için yasal boyutların incelenmesi ve mevzuat formülasyonlarının hazırlanması ve hukuk mesleklerinde ulusal dijital altyapının en iyi dijital güvenlik standartlarıyla kullanılması için mevzuat geliştirilmesi üzerinde çalışmaktadır.[8]

8 https://www.gulftoday.ae/news/2024/10/20/uae-to-launch-virtual-lawyer-the-first-ai-guided-legal-professional-in-the-region

14 Yaşındaki Çocuğun Ölümünden Yapay Zekâ Sorumlu Tutuluyor

ABD'nin Orlando kentinde yaşanan bir olayda, dokuzuncu sınıfta okuyan 14 yaşındaki Sewell Setzer intihar etmişti. Gencin ailesi ise bu intiharın sorumlusu olarak Character.AI adlı yapay zekâyı suçlamaktadır. Anneye göre oğlu, sohbet botlarıyla konuşmaya başlayınca kendini izole etmiştir. İddialara göre, Setzer, intihara meyilli düşüncelerini sohbet botuna da itiraf etmiş, hatta ölümünden kısa bir süre önceye kadar da botla mesajlaşmayı sürdürmüştür. Setzer, Character.AI'ın rol yapma uygulamasındaki botlarla, özellikle de "Dany" adındaki botla duygusal bir bağ geliştirmiş ve sürekli olarak onunla mesajlaşmaya başlamıştır. Bu durum onu zamanla gerçek dünyadan uzaklaştırmıştır.

Character.AI ise benzer durumların tekrar yaşanmaması için harekete geçmiştir. Firmadan yapılan açıklamada, hizmet şartlarını ihlal eden sohbetlerle ilgili olarak "geliştirilmiş tespit, yanıt ve müdahale" ve bir kullanıcı bir sohbette bir saat zaman geçirdiğinde bildirim gönderme gibi özellikler üzerinde çalışıldığı bildirilmiştir.[9]

9 https://www.nbcnews.com/tech/characterai-lawsuit-florida-teen-death-rcna176791

RNA Virüslerini Tanımlamada Yapay Zeka Kullanımı

Bilim insanları yapay zeka yardımıyla 160 binden fazla ribonükleik asit (RNA) virüsü türü tespit ederek belki de en büyük virüs türü keşfini gerçekleştirmiştir. Keşifle ilgili bir rapor Ekim ayında uluslararası bilim dergisi Cell'de yayımlanmıştır. Araştırma Sun Yatsen Üniversitesi, Alibaba Cloud Intelligence, Sydney Üniversitesi ve diğer bazı kurumlardan bilim insanları tarafından ortaklaşa yürütülmüştür.

Sun Yat-sen Üniversitesi Zhongshan Tıp Fakültesi'nde profesör olan Shi Mang, RNA virüslerinin en uç ortamlarda bile bulunduğunu, en gizemli mikroorganizmalar olduğunu, bu mikroorganizmaların küresel ekosistemde önemli bir rol oynadığını ve bazılarının insanlarda bulaşıcı hastalıkların ortaya çıkmasına neden olan patojenler olduğunu söylemiştir.

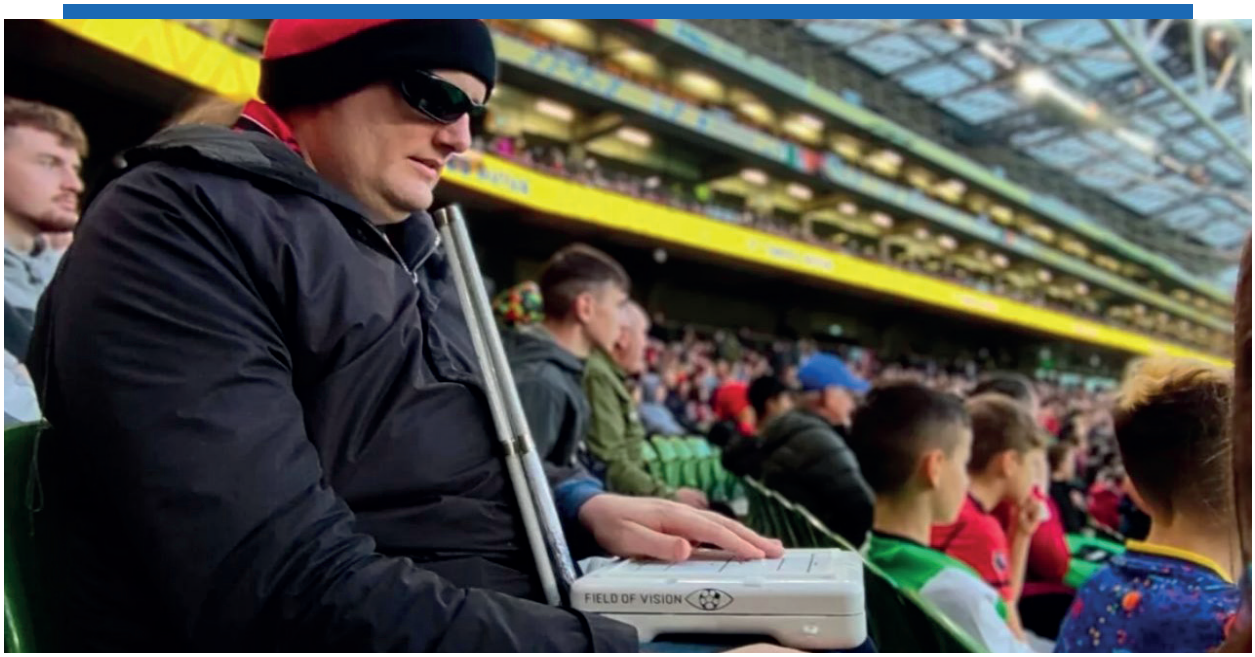
Araştırma sırasında, hava, kaplıcalar ve hidrotermal bacalar da dahil olmak üzere çeşitli ortamlardaki örneklerden elde edilen 10.487 RNA dizileme verisini analiz etmek için LucaProt adı verilen bir derin öğrenme algoritması geliştirilmiştir. Algoritma, 161.979 RNA virüsü türü ve 180 RNA virüsü süper grubunun yanı sıra daha önce yeterince çalışılmamış birçok grubu ve olağanüstü uzunluktaki RNA virüsü genomlarını tanımlamıştır.

Sydney Üniversitesinde profesör olan Edwards Holmes yaptığı açıklamada şunları söylemiştir: "Bu virüslerin büyük çoğunluğu zaten dizilenmişti ve halka açık veri tabanlarında bulunuyordu, ancak o kadar farklıydılar ki kimse ne olduklarını bilmiyordu. Bunlar genellikle 'karanlık madde' dizisi olarak adlandırılan şeyi oluşturuyordu. Yapay zeka yöntemimiz, tüm bu farklı bilgileri organize edip kategorize ederek bu karanlık maddenin anlamına ilk kez ışık

tutmayı başardı. Yapay zeka aracı, "karanlık maddeyi" hesaplamak ve tüm RNA virüslerinin replikasyon için kullandığı proteinin sekanslarına ve ikincil yapılarına dayalı olarak virüsleri tanımlamak üzere eğitildi ve normalde yoğun zaman alan virüs keşfini hızlandırdı. Bu kadar çok yeni virüsü bir çırpıda bulmak akıllara durgunluk veriyor ve bu sadece yüzeyi çizerek bir keşif dünyasının kapılarını açıyor. Keşfedilecek daha milyonlarca virüs var ve aynı yaklaşımı bakteri ve parazitleri tanımlamak için de uygulayabiliriz. Yapay zeka algoritma modeli, daha önce bilinmeyen veya ihmal edilen virüsleri ortaya çıkarmamızı sağlıyor. Bu yetenek özellikle hastalık kontrolünde ve yeni patojenlerin hızlı bir şekilde tanımlanmasında önemlidir."[10]

10 https://www.chinadaily.com.cn/a/202410/12/WS67077e17a310f1265a1c6e64.html

İrlanda'da Görme Engelli Sporseverler İçin Yeni Bir Cihaz



Dublin merkezli bir girişim olan Field of Vision, görme engelli taraftarların stadyumlarda maçları daha iyi takip edebilmelerini sağlayan bir cihaz geliştirmiştir. Field of Vision adlı bu cihaz, kullanıcıların sadece dinlemekle kalmayıp maçın heyecanını da hissetmelerini sağlamaktadır.

Field of Vision'ın kurucu ortaklarından David Deneher, cihazın taraftarları oyunun bir parçası gibi hissettirdiğini belirtmiştir. Bu girişim Covid-19 karantinası sırasında üç arkadaş tarafından kurulmuş ve kısa sürede büyük ilgi görmüştür. Field of Vision, görme engelli ve kısmen görme engelli spor hayranları için tasarlanmış, elde taşınabilir ve dokunsal geri bildirim sağlayan bir cihazdır. Stadyumlardaki özel kameralar aracılığıyla maçı takip ederek, yapay zekâ kullanarak önemli anları algılamaktadır. Algıladığı bilgileri kullanıcıya titreşimlerle iletebilmektedir. Kullanıcılar cihazın üzerinde bulunan manyetik halka sayesinde, maçın anlık durumunu hissedebilmektedir. Cihazın üzerinde yer alan küçük, kabartmalı spor sahası şeklindeki tablet, yaklaşık yarım saniye içinde maçın durumunu kullanıcıya aktarabilme özelliğine sahiptir. Kullanıcılar parmağını bu tablet üzerinde hareket ettirerek topun yerini ve maçtaki önemli olayları hissedebilecekler ve ayrıca cihazda bulunan kulaklık girişi sayesinde, stadyumdaki sesli betimlemeyi de dinleyebileceklerdir.

Görme engelli taraftarlara maçları anlatan kulüp gönüllüleri ile birlikte cihazın test edilmesi, olumlu geri bildirimler alınmasına yol açmıştır. Field of Vision, Manchester City'nin Etihad Stadyumu ve Melbourne'daki Marvel Stadyumu gibi büyük stadyumlarda prototip testleri gerçekleştirmiş ve cihazın spor deneyimini önemli ölçüde geliştirdiğini kanıtlamıştır. Field of Vision, Avrupa'nın büyük futbol liglerine ve ABD pazarlarına açılmayı planlamaktadır. Field of Vision cihazı, görme engelli taraftarlara stadyumlardaki maçları hissetme ve daha aktif bir şekilde katılma imkânı sunarak, spor deneyimini herkes için daha erişilebilir hale getirmektedir.[11]

11 https://www.webtekno.com/gorme-engelli-sporseverler-icin-maclari-hissedebilecekleri-yeni-bir-cihaz-gelistirildi-h150338.html

Araçlarda Emniyet Kemeri Takılmaması ve Telefon Kullanımının Yapay Zeka ile Tespiti

Yeni ve son teknolojiye sahip yapay zeka kamera sistemi piyasaya sürülmüş olup söz konusu kamera sayesinde Greater Manchester'da beş haftalık bir süre boyunca 3200'den fazla kişinin araç kullanırken cep telefonu kullandığı veya emniyet kemeri takmadığı tespit edilmiştir.

'Heads Up' kamera sistemi tarafından yakalanan görüntülerde, sürücülerin direksiyon başındayken cep telefonlarını yüzlerinin önüne ya da kulaklarına doğru tuttukları, bazen ise bu durumlarda yanlarında yolcuların da (çocuklar dahil) olduğu görülmüştür. Sistem, direksiyon başında cep telefonu kullanarak dikkati dağılan 812 sürücüyü ve emniyet kemeri uyumsuzluğuyla ilgili 2393 olayı kaydetmiştir.

Greater Manchester aktif seyahat komisyon üyesi Dame Sarah Storey konuya ilişkin olarak, "Deneme sonuçları; araç direksiyonunda yapılan davranışların, sürücülerin kendilerini, yolcuları ve yolları kullanan diğer insanları nasıl etkileyebileceğini düşünmeyen sürücü sayısının ardındaki korkunç gerçeği gösteriyor." açıklamasını yapmıştır.[12]

12 https://www.bbc.com/news/articles/ce8dpvxexz8o

Yapay Zeka ile Toplantılar Sırasında Yabancı Bir Dilde Konuşma İmkânı

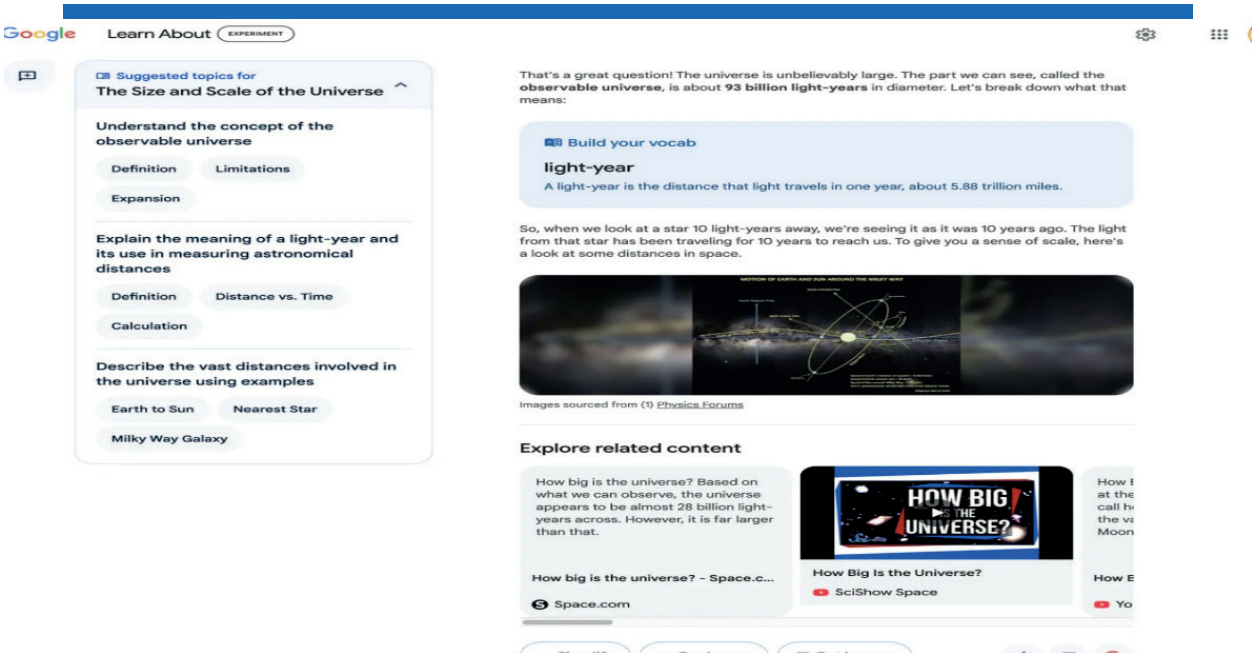
Microsoft Teams, farklı diller konuşan kişiler arasındaki dil engelini ortadan kaldıracak olan çevirmen özelliğini duyurmuştur. Bu özellik sayesinde her kullanıcı, yapay zekâ yardımıyla konuşmaları istediği dilde dinleyebilecek ve böylece dil bariyeri aşılmış olacaktır. Yeni özelliğin ön izlemesi ise 2025 yılının başlarında yayımlanacaktır. Bu ön izlemede dokuz farklı dil seçeneği bulunacaktır. Ayrıca yapay zekâ, konuşan kişinin isteğine bağlı olarak konuşmacının sesini taklit edebilecek ve bu sayede diyalogların daha az yapaylaşması ya da konuşmacılarla dinleyicilerin birbirlerine daha az yabancılaşması sağlanacaktır.

Bu özellik, Microsoft Teams'e gelecek olan yapay zekâ temelli bir dizi yenilik arasında yer alacaktır. Yakın zamanda gelecek olan bir diğer yapay zekâ özelliği ise toplantı transkriptlerini farklı dillere çevirebilme özelliği olacaktır. Bu özellik sayesinde transkriptler 31 farklı dile çevrilebilecektir.

2025 yılının başlarında Microsoft'un ön izlemesini yapacağı bir diğer özellik ise Teams'in ekrandaki herhangi bir görseli anlayıp özetleyebilmesini sağlayacak olmasıdır. Ayrıca Copilot da paylaşılan dosyaların özetlerini oluşturarak sohbetteki katılımcılar ile paylaşabilecek ve böylelikle bütün dosyayı açmak ya da incelemek gerekmeyecektir. Öte yandan, Copilot Plus PC aracılığıyla bilgisayarların üzerindeki NPU çipleri kullanılarak aramalardaki video görüntü kalitesinin arttırılması amaçlanmaktadır. Bu özellik, internet bağlantısının zayıf olduğu durumlarda cihaz üzerinde görüntüyü geliştirmeyi sağlayacaktır.[13]

13 https://www.theverge.com/2024/11/19/24300266/microsoft-teams-ai-interpreter-speech-to-speech-translation

Google'dan Eğitim Odaklı Yapay Zekâ



ABD merkezli teknoloji devi Google, "Learn About" olarak isimlendirdiği yeni yapay zekâ aracını tanıtmıştır. ChatGPT ve Gemini gibi aslında yapay zekâ destekli sohbet botu olarak karşımıza çıkan Learn About, eğitim odaklı yapısı ile dikkat çekmektedir.

"LearnLM AI" isimli yapay zekâ modeli üzerinde inşa edilen Learn About, akademik olarak bir şeyler öğrenmek veya araştırmalar yapmak isteyen tüketicilere odaklanmıştır. Etkileşimli ve görsel destekli sonuçlar veren yapay zekâ, doğrudan sonuca odaklanmaktadır.

Halihazırda test aşamasında olduğu açıklanan Learn About, Türkiye'de henüz erişime açık değildir ve yapay zekâ destekli sohbet botunun ne zaman geniş kapsamda kullanıma sunulacağına ilişkin bir açıklama yapılmamıştır.[14]

14 https://www.theverge.com/2024/11/11/24293891/google-learn-about-ai-search-educational

Sesleri Değiştirebilen ve Yeni Sesler Üreten Yapay Zekâ Modeli

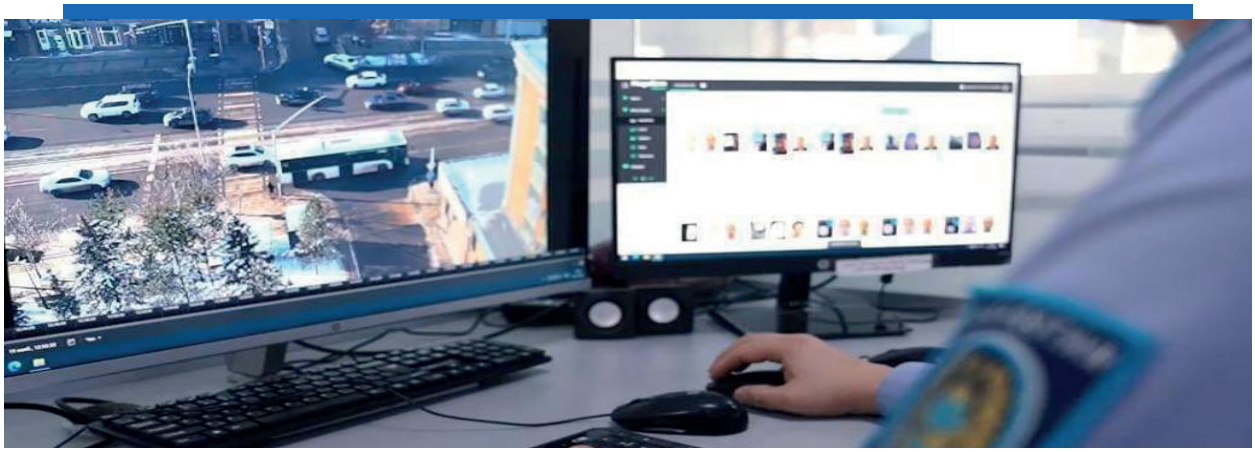
Teknoloji şirketi Nvidia, sesleri değiştirebilen ve yeni sesler üretebilen yapay zekâ modelini tanıtmıştır. Şirket bu teknoloji ile müzik, film ve video oyunu üreticilerini hedeflediğini açıklamıştır.

Yapay zekâ sistemleri oluşturmak için kullanılan çip ve yazılımlara yönelik en büyük tedarikçilerden biri olan Nvidia, Fugatto adını verdiği bu teknolojiyi kullanılması için halihazırda kamuoyuna sunmayacağını belirtirken, yapay zekâ modeli ile metin açıklamasından ses efektleri ve müzik üretildiği ifade edilmiştir. Söz konusu modeli, diğer yapay zekâ teknolojilerinden farklı kılan özelliği var olan sesi alıp değiştirebilmesi olarak ifade edilmektedir. Bu kapsamda, piyanoda çalınan bir notayı insan sesiyle söylenen bir notaya dönüştürebildiği veya konuşulan bir kelime kaydını alıp kullanılan aksanı ve ifade edilen ruh halini değiştirebildiği açıklanmıştır. Üretken yapay zekâ modelinin, müziğe ve video oyunlarına yeni yetenekler getireceği belirtilirken, modelin açık kaynaklı verilerle eğitildiği de ifade edilmiştir.

Diğer bir taraftan şirket, üretken yapay zekâ modellerinin bir kullanıcının yanlış bilgi oluşturması veya telif hakkıyla korunan eserler üreterek, telif haklarını ihlal etmesi gibi kötüye kullanımının nasıl önleneceğini henüz belirleyemediğini açıklamıştır.[15]

15 https://indianexpress.com/article/technology/artificial-intelligence/nvidia-shows-ai-model-that-can-modify-voices-generate -novel-sounds-9690517/

Kazakistan'da İki Şehirde Yapay Zeka Yüz Tanıma Sistemine Test



Kazakistan, yapay zekâ teknolojileriyle desteklenen ulusal bir video izleme sistemi başlatmıştır. İçişleri Bakanlığı, Ulusal Güvenlik Komitesi ile Dijital Kalkınma, İnovasyon, Havacılık ve Uzay Sanayi Bakanlığı tarafından geliştirilen proje, ülkenin kilit noktalarındaki gözetim yeteneklerini geliştirmeyi amaçlamaktadır. Sistem yüzleri tanımak, terk edilmiş nesneleri tespit etmek, suçluları yakalamak ve araçları marka, model ve renklerine göre tanımlamak üzere tasarlanmıştır. Tren istasyonları, havaalanları, oteller, caddeler, kavşaklar ve alışveriş merkezleri gibi kritik yerler uygulama için öncelikli alanlardır.

Astana'da düzenlenen Dünya Göçebe Oyunları sırasında bu teknolojinin kayıp çocukların ve kayıp kişilerin yerlerinin tespit edilmesinde etkili olduğu bildirilmiştir. Yetkililer ayrıca sistemin Astana'da aranan 46 ve Almatı'da 30 kişinin gözaltına alınmasına yardımcı olduğunu da kaydetmiştir. Savunucular bu teknolojilerin kamu güvenliğinin artırılmasına ve suçun azaltılmasına katkıda bulunabileceğini ileri sürmektedir. Kazakistan'ın girişimi, Çin, Rusya ve bazı Avrupa ülkelerindeki gelişmelere benzer şekilde, yapay zekayı "akıllı şehir" sistemlerine entegre etme yönündeki daha geniş bir küresel eğilimi takip etmektedir. Yetkililer, izleme kapsamını artırmak için sistemin ülke çapında ek kameralarla genişletileceğini söylemektedir.

Bugüne kadar Kazakistan'da 1,3 milyondan fazla video kamera kurulmuş ve bunların 310.000'i operasyonel kontrol merkezlerine ve polis görev istasyonlarına bağlanmıştır. Sistemin savunucuları, suçu caydırma ve kamu güvenliğini destekleme potansiyelinin altını çizmekle birlikte, mahremiyet ve gözetim teknolojisinin kötüye kullanımı ile ilgili endişeler uluslararası alanda dile getirilmektedir.

Dünya çapında, yapay zekalı video gözetim sistemleri kolluk kuvvetlerini ve kamu güvenliğini iyileştirmek için benimsenmektedir. Çin'de suçluları takip etmek ve suçları önlemek için yüz tanıma amacıyla kullanılmaktadır. Rusya, potansiyel tehditleri tespit etmek için video sistemlerine yapay zekayı entegre ederken, İngiltere'de akıllı kameralar kalabalık yönetimi ve etkinlik güvenliği için kullanılmaktadır. Destekçiler bu tür sistemlerin olaylara daha hızlı müdahale etme ve suçu azaltma konusundaki faydalarını vurgularken, yapay zekanın gözetimde kullanılması mahremiyet, sivil özgürlükler ve kötüye kullanım potansiyeli konusunda süregelen tartışmalara yol açmıştır.[16]

16 https://timesca.com/ai-facial-recognition-system-being-tested-in-two-cities-in-kazakhstan/

Amazon'dan Yeni Bir Yapay Zeka

ABD'li e-ticaret şirketi Amazon, metnin yanı sıra görüntü ve videoları da işleyebilen yeni bir üretken yapay zeka geliştirmiştir. Yeni yapay zeka modelinin geliştirilmesinin Amazon'un, Amazon Web Services'ta (AWS) popüler bir hizmet olan Anthropic'in Claude sohbet robotuna olan bağımlılığını azaltmasına yardımcı olacağı açıklanmıştır. Olympus kod adlı yeni büyük dil modelinin (LLM), görsellerdeki ve videolardaki sahneleri anlayabildiği ve müşterilerin basit metin komutlarını kullanarak, örneğin kazanılan bir basketbol atışı gibi belirli sahneleri aramasına yardımcı olabileceği belirtilmektedir. Amazon, Kasım ayı içerisinde OpenAI'nin rakibi olan Anthropic'e 4 milyar dolar daha yatırım yapmıştır.[17]

17 https://www.reuters.com/technology/artificial-intelligence/amazon-develops-video-ai-model-information-reports-2024-11-28/

Çin'de Üretken Yapay Zeka Ürünü Kullanıcı Tabanı 230 Milyona Ulaştı

Yayınlanan bir rapora göre, Çin'deki üretken yapay zekâ (YZ) ürünlerinin kullanıcı tabanı Haziran 2024 itibariyle 230 milyona ulaşmış ve ülkenin çeşitli sektörlerde üretken YZ odaklı yükseltmeleri yaygın olarak benimsediğinin altı çizilmiştir.

Çin İnternet Ağı Bilgi Merkezi (CNNIC) tarafından yayınlanan üretken yapay zekanın gelişimine ilişkin bir rapora göre Çin, sektördeki 4.500'den fazla ilgili şirketle nispeten kapsamlı bir yapay zeka endüstrisi ekosistemi inşa etmiştir.

Ülkenin üretken YZ endüstrisi, çekirdek sektörün 600 milyar yuan'a (82,84 milyar $) yaklaşan değeri ile gelişmeye devam etmektedir. Endüstri ekosistemi, çipler, algoritmalar, veriler, platformlar ve uygulamalar dahil olmak üzere hem yukarı hem de aşağı yönde önemli alanları kapsamaktadır. Raporda, Temmuz 2024 itibariyle 190'dan fazla üretken yapay zeka modelinin kayıtlı ve çevrimiçi olduğu ve kullanıcılara çok çeşitli seçenekler ve özel deneyimler sunduğu belirtilmiştir. Çin, Temmuz 2023'te üretken YZ hizmetleri için bir dizi geçici yönetim kuralı yayınlayarak küresel çapta türünün ilk örneği olmuştur.

Temmuz 2024'te 20. Çin Komünist Partisi Merkez Komitesi'nin üçüncü genel kurulunda kabul edilen önemli bir reform kararı da ülkenin üretken yapay zekayı geliştirme ve yönetme mekanizmalarını iyileştireceğini belirtmiştir.[18]

18 https://www.chinadaily.com.cn/a/202412/01/WS674c190ba310f1265a1d06d4.html

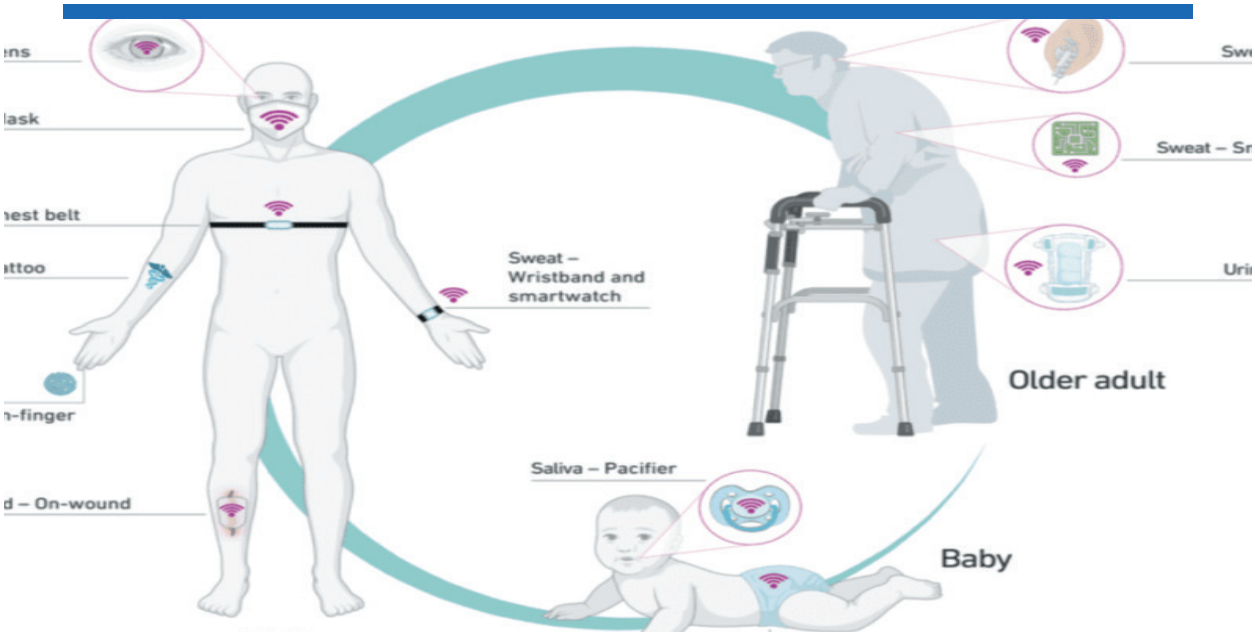
Polonya'da Hukuk Firmalarında Yapay Zeka Uygulamaları

Günlük çalışmalarında yapay zeka araçlarını kullanan ve Polonya pazarında faaliyet gösteren hukuk bürosu Sołtysiński Kawecki & Szlęzak, yapay zekanın uygulanmasıyla rekabet gücünü artırmayı ve kurumun hukuki süreçlerini hızlandırmayı amaçlamaktadır. Yapay zeka uygulamaları sayesinde hem verimlilik artacak hem de müşterilere daha rekabetçi hizmetler sunulacaktır. Microsoft Copilot gibi yapay zeka destekli araçlar, firma bünyesindeki avukatlar için hukuki belgelerin özetlenmesi, uzun metinlerin kısaltılması, e-posta taslaklarının hazırlanması ve terminolojik doğrulama gibi görevlerde birer yardımcı işlevi görmektedir. Bu araçlar, hukuki süreçlerin hızlanmasına katkı sağlamakta ve kavramsal analizlerde destek sunmaktadır.

SK&S, yapay zeka çözümlerini kullanırken avukatların nihai denetim sorumluluğunu korumasına büyük önem vermekte ve bu araçların avukatların yerine geçmediğini, aksine onları tamamlayıcı bir rol üstlendiğini belirtmektedir. Veri güvenliği, SK&S için öncelikli bir alan olarak öne çıkmaktadır. Müvekkil bilgilerinin gizliliğini sağlamak için gelişmiş politikalar benimseyen firma, güvenilir yapay zeka sağlayıcılarıyla çalışmaktadır. Firma, Microsoft Copilot'un yanı sıra yapay zeka araçlarını mevcut sistemlerle entegre ederek ve daha ileri teknolojilere uyum sağlayarak sürekli gelişim sağlamayı hedeflemektedir. Tekrarlayan görevlerin otomasyonu, avukatların daha karmaşık işlere odaklanmasına olanak tanırken, müşteri memnuniyetini artıracak çözümler geliştirilmesine de katkıda bulunmaktadır.[19]

19 https://news.microsoft.com/pl-pl/2024/12/10/one-of-polands-largest-law-firms-brings-ai-to-everyday-work/

İsviçre'den Vücut Sıvılarını Analiz Eden Sensörler



ETH Zürih'teki araştırmacılar ve uluslararası uzmanlar, bu tür sensörlerle neler yapılabileceğini ve geliştiricilerinin gelecekte başarılı bir şekilde kullanılabilmeleri için hangi soruları dikkate almaları gerektiğini gösteren bir araştırma yayınlamıştır. Giyilebilir sensörler vücudun hayati fonksiyonlarından bazılarını oldukça güvenilir bir şekilde takip etmekte ve bu cihazlardan bazıları klinik teşhislerde kullanılabilmektedir. Ancak, biyokimyasal verilere dayalı teşhisler hala kan ve idrar gibi vücut sıvılarından örnekler gerektirmektedir ve bunların analiz için laboratuvara gönderilmesi şarttır. Bunları toplamak acı verici ve karmaşık olabileceği gibi zaman alıcı ve maliyetli de olabilmektedir.

Ancak yeni nesil giyilebilir sensörler biyokimyasal analizler de sunacaktır. Gelecekte bu tür sensörler, ter, nefes, tükürük, gözyaşı ve idrar gibi vücut sıvılarını analiz ederek kullanıcılarının sağlık durumu hakkında değerli bilgiler toplayacaktır. Bu gelişmelerin çoğu henüz pazara sunulmaya hazır olmasa da uygulanabilecektir. Collegium Helveticum'da Dr. Noé Brasier ve ETH Profesörü Jörg Goldhahn'ı giyilebilir sensörler alanında önde gelen araştırmacılarla güçlerini birleştirmeye ve kapsamlı bir inceleme yapmaya itmiştir. Çalışmaları yakın zamanda Nature dergisinde yayımlanmıştır.

Giyilebilir sensörlerin avantajları açıktır. Hastaların bir doktor muayenehanesine veya eczaneye gitmesine gerek kalmadan sağlık değişkenlerinin sürekli izlenmesine olanak tanımaktadır. Brasier, "Isı stresinden muzdarip yaşlılar için, giyilebilir bir cihaz onlara zamanında yeterli su içmelerini hatırlatabilseydi veya bir sensör elektrolitleri kritik bir seviyeye ulaştığında alarm çalabilseydi, hayat çok daha kolay olurdu. Bebeklerden ve küçük çocuklardan kan alma girişimleri, kateter takmaktan bahsetmiyorum bile, her zaman başarılı

olmuyor. Bu önemli gecikmelere yol açabilir ve genellikle genç hastalar ve ebeveynleri için sıkıntı vericidir. Laboratuvar ve/veya idrar analizini yapmak için bebeğin cildinde veya bezinde bir sensör olması çok daha kolay ve rahat olurdu." açıklamasında bulunmuştur.

Makalenin kıdemli yazarı Goldhahn yaptığı açıklamada, bir yıl önce mühendisler, doktorlar ve diğer disiplinlerden meslektaşlarıyla olasılıkları tartıştıklarında, hangi tür sensörlerin mantıklı olduğunu ve bu tür cihazları geliştirirken hangi noktalara özellikle önem verilmesi gerektiğini düşünmeleri gerektiğini fark ettiklerini söylemiştir.

Temel husus giyilebilir cihazlar hastaların giymek isteyeceği bir şey olmalıdır. Brasier bu yüzden sensörleri her zaman daha sonra ihtiyaç duyacak kişilerle birlikte geliştirmeyi önerdiklerini açıklamıştır. Ancak bu tür cihazların tıbbi faydalarının da eleştirel bir şekilde değerlendirilmesi gerekmektedir. Ölçülebilen her şey klinik bir fayda sağlamaz.

Örneğin, CRP vücuttaki inflamasyonun bir belirtecidir ve litre başına miligram olarak ölçülmektedir. Sağlıklı yetişkinlerde, CRP seviyesi normalde fizyolojik olarak 5 mg/l'nin altındadır. Bir hastanın kanındaki CRP seviyesi 150 mg/l ise, bu bize yalnızca çok az şey söyler. Klinik değerlendirme için belirleyici olan, bir önceki günkü değerin normal olup olmadığı veya 300 mg/l olup olmadığıdır. Daha sonra kişinin sağlığının kötüleştiği mi yoksa iyileştiği mi söylenebilir.

Bunun yanı sıra teknik engeller de mevcuttur. Bir sensör ne kadar süre ölçüm yapmaya devam edebilir? Nasıl saklanabilir ve temizlenebilir? Ne kadar elektrik tüketir ve hangi kaynaktan? ve en önemlisi, sağladığı veriler ne kadar iyi ve güvenilirdir? Goldhahn, ölçüm verilerinin dikkatli bir şekilde doğrulanmasının, belirli bir cihazın kurulup kurulmayacağı açısından çok önemli olacağını söylemiştir. Bir sonraki adımda, giyilebilir cihazlardan gelen sinyaller, kullanıcılar için mantıklı bir şekilde işlenmeli, yorumlanmalı ve görüntülenmelidir.[20]

20 https://www.eenewseurope.com/en/how-the-latest-sensors-analyse-body-fluids/

Google'dan Gemini'ye Yeni Dil Seçenekleri

Google, yapay zekâ destekli araştırma asistanı olan Gemini'nin derinlemesine araştırma modunu 40 farklı dilde daha kullanılabilir hale getirmiştir. Yeni özellik Gemini'nin kullanıcılar araştırma yaparken daha verimli olmasını sağlayacaktır. Gemini'nin yeni araştırma modu, kullanıcıların araştırma planları oluşturmasına, bilgi toplamasına ve bu bilgileri analiz ederek bir rapor hazırlamasına yardımcı olacaktır.

Google One AI premium plan kullanıcıları, bu aracı kullanarak daha ayrıntılı ve derinlemesine araştırmalar yapabiliyor olacaktır. Yeni işlev birçok adımda bilgi aramayı ve her adımda elde edilen verileri analiz ederek sonuçları derlemeyi içerecektir.

Google, bu süreçte modelin daha doğru ve tutarlı sonuçlar vermesi için yerel dil verileri üzerinde kapsamlı testler ve düzeltmeler yapmaktadır. Şirket, yerel ekiplerin de veri setlerini gözden geçirerek kaliteyi artırmayı amaçlamaktadır.

Desteklenen diller ise aşağıdaki gibidir: Arapça, Bengalce, Çince, Danca, Fransızca, Almanca, Guceratça, Hintçe, Endonezce, İtalyanca, Japonca, Kannada, Korece, Malayca, Marathi, Lehçe, Portekizce, Svahili, İspanyolca, Tamilce, Telugu, Tayca, Ukraynaca ve Urduca[21]

21 https://techcrunch.com/2024/12/20/google-is-expanding-geminis-in-depth-research-mode-to-40-languages/?guccounter=1

Dünyanın İlk Yapay Zekalı Kamerası ile Alkollü Sürücü Tespiti

Birleşik Krallık'ta alkol veya uyuşturucu etkisi altındaki sürücüler ilk kez test edilen bir yapay zekâ kamerasıyla yakalanmıştır. Daha önce bu yapay zekâ kameraları, polislerin direksiyonda cep telefonu kullanan veya emniyet kemeri takmayan sürücüleri yakalamasına yardımcı olmak için kullanılmıştır.

Son teknoloji ürünü olan Heads-Up adlı makinenin, içki veya uyuşturucu etkisi altında olan sürücülerin yol kullanımını ve davranışlarını da tespit edebildiği ifade edilmiştir. Böylelikle yolun ilerisinde konumlanan polis, aracı durdurabilmekte, sürücüye yol kenarında alkol ve uyuşturucu testi yapabilmektedir. Kameranın herhangi bir uyarı olmaksızın yolda hızla hareket ettirilebildiği ve sürücülerin, polis onları durdurana kadar durumu fark etmediği açıklanmıştır.

Alkollü sürücülerin ölümcül kazalara karışma olasılığının altı kat daha fazla olduğu göz önüne alındığında, Heads-Up sisteminin hayat kurtarmaya yardımcı olmasının beklendiği açıklanmıştır.[22]

22 https://www.bbc.com/news/articles/cj0rqz003zdo

OpenAI ve WhatsApp Entegrasyonu

OpenAI, popüler yapay zeka sohbet robotu ChatGPT'nin WhatsApp ile entegrasyonunu duyurmuştur. Bu yenilik sayesinde, ABD'deki kullanıcılar Meta'ya ait anlık mesajlaşma platformu üzerinden ChatGPT ile doğrudan etkileşim kurabilecektir. Bu özellik, OpenAI'nin erişilebilirlik çabalarının önemli bir parçası olarak öne çıkmaktadır.

ChatGPT'yi WhatsApp üzerinde etkinleştirmek için kullanıcılar, 1-1800-242-8478 numarasını arayarak veya mesajlaşarak bu hizmetten faydalanabilmektedir. Metin tabanlı sohbetler, Hindistan dahil olmak üzere ChatGPT'nin desteklendiği tüm bölgelerde kullanılabilirken, sesli arama özelliği şu anda yalnızca ABD ve Kanada ile sınırlıdır. Kullanıcılar, ChatGPT ile ayda 15 dakikaya kadar ücretsiz sesli etkileşim kurabilmektedir. ChatGPT'nin WhatsApp üzerinde kullanımı için herhangi bir özel hesap gerekmemektedir. Bu da sesli arama ve mesajlaşma erişimini kolaylaştırmaktadır. Ancak OpenAI, gelecekte sohbet geçmişi entegrasyonu ve ek işlevler sunabileceğine dair sinyaller vermektedir. WhatsApp entegrasyonu, kullanıcıların metin tabanlı sohbetler gerçekleştirmesine imkan tanırken, şu an için grup sohbetlerinde ChatGPT kullanımı desteklenmemektedir. Ayrıca, kullanıcıların günlük mesaj gönderiminde bir sınır bulunmakta ve sınır yaklaşırken bildirimler sağlanmaktadır. Gizlilik önlemleri açısından OpenAI, ChatGPT'nin asla bir arama veya mesaj başlatmayacağını vurgulamıştır. Gelecekteki güncellemeler arasında ChatGPT Arama, görüntü tabanlı etkileşimler ve konuşma belleği günlükleri gibi özelliklerin eklenmesi planlanmaktadır. Bu gelişmeler, özellikle chatbot'u üretkenlik ve yaratıcı amaçlar için kullananların kullanıcı deneyimini iyileştirecektir. Bu entegrasyon, Meta'nın WhatsApp platformunda kendi yapay zeka sohbet robotunu tanıttığı bir döneme denk gelmektedir. Her iki şirketin de yapay zeka alanındaki bu yenilikleri, platform üzerinde ilgi çekici bir rekabet ortamı oluşturmaktadır.

Öte yandan OpenAI, ChatGPT destekli internet arama özelliğini tüm kullanıcılara genişleteceğini duyurmuştur. Bu hamlenin uzun süredir arama motoru pazarında lider konumda olan Google ile rekabeti daha da yoğunlaştırması beklenmektedir.[23]

23 https://www.livemint.comæ/ai/artificial-intelligence/openai-brings-chatgpt-to-whatsapp-new-voice-and-text-feature-unveiled -how-it-works-11734590861810.html

Washington Üniversitesi'nden Yeni Yapay Zeka Teknolojisi: Varyasyonel Tercih Öğrenimi

Yapay zeka sohbet robotlarının bilgi sağlama yetenekleri her geçen gün genişlerken, Washington Üniversitesi (UW) araştırmacıları, bu robotların yanıtlarını kullanıcı tercihlerine göre daha iyi uyarlamak için yeni bir yöntem geliştirmiştir. "Varyasyonel Tercih Öğrenimi" (VPL) olarak adlandırılan bu yöntem, büyük dil modellerinin çıktısını bireysel kullanıcıların belirttiği tercihlere göre şekillendirmeyi hedeflemektedir.

Günümüzde yapay zeka sistemleri, genellikle "insan geri bildirimlerinden takviye öğrenimi" (RLHF) adı verilen bir strateji ile eğitilmektedir. Bu yöntem, sohbet robotlarının yanıtlarını güvenli, doğru ve kabul edilebilir hale getirmek için bir grup insanın çıktıları incelemesini gerektirmektedir. Ancak bu süreç, çoğunlukla bu modelleri oluşturan kuruluşların belirlediği değerlere dayanmakta ve kullanıcıların geniş kapsamlı görüşlerini içermeyebilmektedir.

Varyasyonel Tercih Öğrenimi, sohbet robotlarının kullanıcıdan aldığı yalnızca dört sorgu ile bireyin tercihlerini öğrenebilmesini sağlamaktadır. Bu, yapay zekanın yanıtlarının: özgüllük seviyesini, yanıtların uzunluğunu ve tonunu, içerilen bilgileri kullanıcıya göre uyarlamasını mümkün kılmaktadır. VPL ayrıca, kişisel ortamlarda görev yerine getiren robotlar gibi sözlü olmayan etkileşimlere de uygulanabilmektedir. Ancak araştırmacılar, bu yöntemin yanlış bilgi, dezenformasyon ve uygunsuz yanıtlara karşı dikkatli şekilde geliştirilmesi gerektiğini belirtmektedir. Bu araştırma, yapay zekanın farklı bakış açılarını destekleme yeteneğini güçlendirmeyi amaçlamaktadır. Washington Üniversitesi'nin bu öncü çalışması, yapay zekanın bireysel kullanıcı deneyimini iyileştirme ve daha çeşitli bakış açılarını destekleme yolunda atılmış önemli bir adım olarak değerlendirilmektedir.[24]

24 https://www.geekwire.com/2024/university-of-washington-researchers-craft-method-of-fine-tuning-ai-chatbots-for-individual-taste/

GİYİLEBİLİR TEKNOLOJİLER

Çin'de Felçlilerin Yeniden Yürümesine Yardımcı Olacak Cihaz

Şangay'daki Fudan Üniversitesi'nden bilim insanları, beyin ve omuriliğe elektrotlar yerleştirerek ve iki vücut parçası arasında bir "sinir bypass" sistemi kurarak beyin-omurga arayüzü araştırmalarında bir dönüm noktasına ulaşmış ve felçli insanların tekrar yürümesini sağlayabilecek bir cihaz geliştirmişlerdir.

Fudan Üniversitesi Beyinden İlham Alan Zeka Bilim ve Teknoloji Enstitüsü'nden araştırmacılar, bu cihaz sayesinde omurilik yaralanmaları nedeniyle felçli olan kişilerin alt uzuvlarındaki kasların kontrolünü yeniden kazanabileceklerini ve böylece ayakta durup yürüyebileceklerini belirtmişlerdir. Baş araştırmacı Jia Fumin, klinik denemelerin bu yıl içinde yerel bir üçüncü basamak hastanede başlamasının beklendiğini söylemiştir.

Omurilik, beyin ve periferik sinir sistemini birbirine bağlayan yüksek hızlı bir kanal işlevi görmektedir. Omurilik hasar görürse, beyinden gelen ve kaslara hareket etmelerini söyleyen talimatlar iletilemez ve felce neden olur. Sinir hasarı geri döndürülemez olduğundan, bu tür hastalar için mevcut tedaviler sınırlıdır. Çin Fiziksel Engelliler Derneği de dahil olmak üzere bir dizi kurum tarafından geçtiğimiz Eylül ayında yayınlanan ulusal bir rapor, Çin'de 3,74 milyon omurilik yaralanmalı hasta olduğunu ve ülkede her yıl yaklaşık 90.000 yeni vaka görüldüğünü göstermiştir.

Geçtiğimiz yıl Lozan'daki İsviçre Federal Teknoloji Enstitüsü'nden bir araştırma ekibi felçli hastalar üzerinde beyin-omurga arayüzü araştırması gerçekleştirmiştir. Beyin sinyallerini

toplayıp çözerek, alt uzuvların ilgili bölgelerini elektriksel olarak uyararak ve beyin ile omurilik sinir yollarını birbirine bağlayarak, omurilik yaralanması olan felçli hastaların kaslarının kontrolünü yeniden kazanmalarına ve yürümelerine yardımcı olabilmişlerdir. Ancak, beyindeki elektriksel aktivitenin kodunun çözülmesi, omurilik sinir köklerinin yeniden yapılandırılması ve sistem entegrasyonu ile klinik uygulamanın kolaylaştırılması gibi zorluklar devam etmektedir.

Jia, "Bu sorunlara yanıt olarak, beyin-omurga arayüzünün son derece hassas olmasını sağlayan yeni nesil cihazlar geliştirdik ve bunlar yüksek verim ve düşük gecikme süresine sahip" şeklinde konuşmuştur. Örneğin, cihaz omuriliğin sinir köklerini hassas bir şekilde uyarabilmekte ve alt uzuvların ilgili kas gruplarını dönüşümlü olarak aktive edebilmekte ve böylece bir hasta daha doğal bir şekilde yürüyebilmektedir. Dahası, sorunsuz bir yürüme süreci sağlamak için cihaz, hastanın duruşuna ve alt uzuvlarının hareketlerine göre omurilik üzerinde etkili olan stimülasyon parametrelerinde gerçek zamanlı ayarlamalar yapmaktadır.

Jia, "Kızılötesi hareket yakalama, elektromiyografi, atalet sensörleri ve plantar basınç pedleri gibi multimodal teknolojileri entegre eden ekibimiz, sağlıklı yürüme duruşlarının yanı sıra çeşitli anormal duruşlardan oluşan bir veri seti oluşturdu ve bir algoritma modeli kurdu, böylece sürekli yürüme duruşlarının yüksek performanslı takibini sağladık" ifadelerini kullanmıştır. Hastaların beyin sinyali toplama ve omurilik stimülasyonu için beyin yarım kürelerine üç cihaz yerleştirilmesini gerektiren İsviçreli ekibin araştırmasıyla karşılaştırıldığında, Jia'nın ekibi ameliyat sonrası yara sayısını azaltmak için cihazları beyne yerleştirilen tek bir küçük cihaza entegre etmiştir. Araştırmacılar, böyle bir çözümün aynı zamanda kod çözme sürecini vücudun dışından vücudun içine kaydırabileceğini, bunun da beyin sinyali toplamanın istikrarını ve verimliliğini artırabileceğini ve beyin sinyallerinin kod çözme hızına ve normal bir kan basıncına sahip (ambulatuvar) kişininkine benzer stimülasyon talimatı çıktısına ulaşabileceğini belirtmiştir.

Jia, bunun, gelecekte omurilik yaralanması olan hastaların yürüme duruşlarının daha doğal ve pürüzsüz olacağı anlamına geldiğini söylemiştir.[25]

25 https://www.chinadaily.com.cn/a/202410/08/WS67049364a310f1265a1c6617.html

Çin'de Bilim İnsanlarından Yeni Yapay Kaslar

Amerika'da HBO'nun (Home Box Office) bilimkurgu dizisi Westworld'de yer alan kas liflerinin 3D baskısı gerçekten hayranlık uyandırıcıdır. İlginçtir ki, Çinli bilim insanlarının yakın zamanda gerçekleştirdiği bir buluş, bu fütüristik teknoloji çağını hayal edilenden daha erken başlatabilecektir.

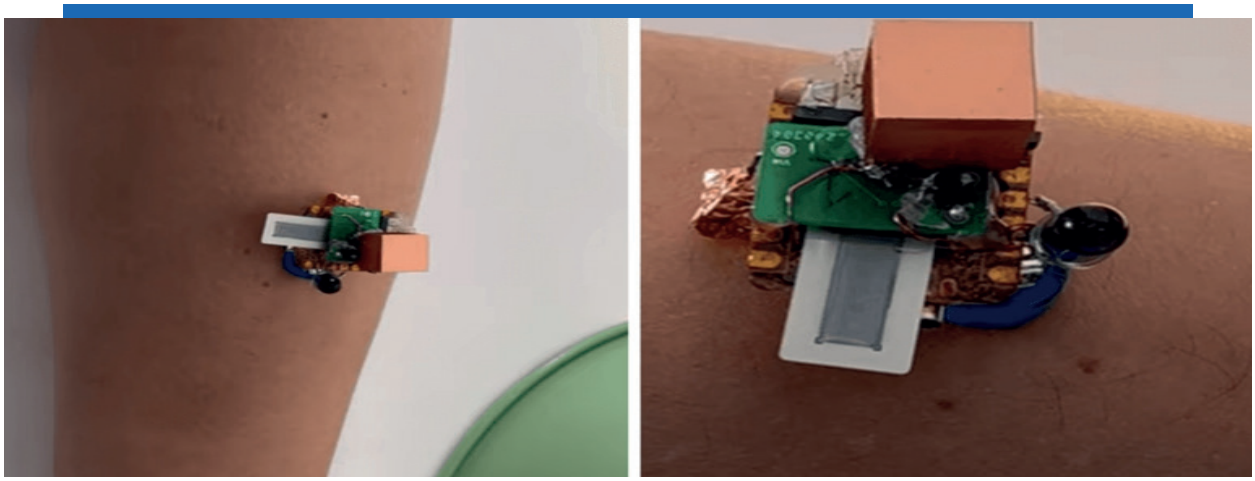
Çin Bilimler Akademisi'ne bağlı Kimya Enstitüsü ve Çin Okyanus Üniversitesi'nden bilim insanları, gezegenimizde bilinen tüm canlı organizmaların temel bir bileşeni olan karbona dayanan yeni bir yapay kas türü geliştirmiştir. Hafifliği, üstün mukavemeti, olağanüstü elektrik iletkenliği ve esnekliği ile tanınan karbon malzemeler, yapay kaslar alanında büyük potansiyel göstermektedir. Cyborglar önemli bir pazar potansiyeli sergilerken, yapay kaslar gerçekten öne çıkmaktadır. Sadece doğal kasları taklit etmekle kalmayıp aynı zamanda kendi kendini onarma, olağanüstü esneklik ve geleneksel mekanik "eklemlerden" daha iyi performans gösteren hızlı tepki süreleri gibi benzersiz avantajlar da sunmaktadır. Yaşlanan nüfus ile birlikte yapay kas teknolojisi yardımcı cihazlar, giyilebilir cihazlar ve çeşitli tıbbi uygulamalarda giderek daha değerli hale gelmektedir.

Araştırma ekibi, bir kelebeğin hortumundan - böceğin uzun, tüp benzeri ağzı - ilham almıştır. Ürettikleri biyomimetik malzemeler, asimetrik bir yüzey yapısına sahip son teknoloji ürünü, hidrojen ikameli grafdiyne film kullanmaktadır. Bu kas, bir kelebeğin ağzına benzer şekilde tersine çevrilebilir, hızlı ve sürekli ayarlanabilir deformasyon özelliklerine sahiptir. National Science Review dergisinde kısa süre önce yayınlanan çalışmaya göre, hareket karbon bağlarının dönüştürülmesiyle tetiklenmektedir.

Bilim insanları yapay kası robotik bir kola başarıyla entegre ederek, kola konumunu hızla değiştirme ve kendisinden 11 kat daha ağır yükleri kaldırma yeteneği kazandırmıştır. Çalışmaya göre, -25 C gibi düşük sıcaklıklarda bile stabilitesini ve uyum yeteneğini korumaktadır. Ayrıca, filmin boyutları yaklaşık 1 santimetreden 100 mikrona kadar özelleştirilebilmektedir. Yapay kasların küçültülmesi, özellikle mikromedikal cihazların ve mikrorobotların geliştirilmesinde önemli bir eğilimdir. Yapay kas şimdi insan parmak bükme hareketlerini izleyen gerçek zamanlı bir izleme sistemine entegre edilmiştir. Bu uygulama gerçek zamanlı simülasyon ve büyük elden küçük ele kontrolü mümkün kılmıştır. Araştırmacılar, buluşun akıllı robotiklerin geliştirilmesi ve hassas tıbbın ilerletilmesi için önemli bir potansiyel gösterdiğini belirtmektedir.[26]

26 https://www.chinadaily.com.cn/a/202411/12/WS6732af33a310f1265a1ccc9e.html

Gelecekte Akıllı Saatleri 'Vücut Enerjinizle' Çalıştırabileceksiniz



Akıllı saatler artık hayatımızın bir parçası olmuş durumdadır ve araştırmacılar artık akıllı saat teknolojisini bir adım öteye taşıyarak pil kullanmadan nasıl çalıştırabileceklerini düşünmektedirler.

Carnegie Mellon Üniversitesi'nin yeni bir çalışması bu alanda umut vadetmektedir. Araştırmacılar, akıllı saatlere cilt ile temas üzerinden güç sağlayabilecek bir yöntem geliştirmiştir. "Power-over-Skin" adı verilen bu yenilikçi teknik, akıllı saatlerin gelecekte pile gerek duymadan çalışabilmelerini sağlayabilecektir. Future Interfaces Group araştırmacıları, insan vücudunun RF enerjisini etkili bir şekilde iletebildiğini keşfederek, bu enerjiyi akıllı saatlere güç olarak aktarmada kullanmayı başarmışlardır. Power-over-Skin yöntemiyle tek bir vücut üzeri vericiden, deriye temas eden bir dizi pilsiz cihaza enerji gönderilmektedir. Araştırmalar, insan vücudunun 40 MHz radyo frekansı enerjisini başarılı bir şekilde ilettiğini ve bu özelliğin enerji aktarımı için uygun bir ortam sağladığını göstermektedir. Araştırmacılar Andy Kong, Daehwa Kim ve Chris Harrison, deneylerinde vücudun çeşitli bölgelerine yerleştirilen verici ve alıcıların birbirine yakınlığına göre güç aktarım miktarının değiştiğini bulmuştur. Örneğin bir vericiyi ön kola, alıcıyı ise bileğe yerleştirdiklerinde daha yüksek mikrowatt düzeyinde enerji aktarımı gerçekleşmiştir. Bu sayede araştırmacılar LED ışıklı bir küpe, basit bir hesap makinesi ve Bluetooth özellikli bir yüzüğe başarıyla enerji sağlayabilmişlerdir.

Power-over-Skin'in en önemli avantajı ise cihazları pilsiz hâle getirerek onları daha küçük ve hafif yapabilmesidir. Pil ihtiyacını ortadan kaldırmak, ayrıca çevresel açıdan önemli kaynak tasarrufları sağlayarak sürdürülebilirliği desteklemektedir. Teknolojinin henüz yüksek güç gerektiren cihazlarda kullanımı mümkün görünmese de düşük enerjili akıllı saatler veya fitness takip cihazları için kısa vadede kullanılabileceği düşünülmektedir.[27]

27 https://www.webtekno.com/gelecekte-akilli-saatleri-vucut-enerjinizle-calistirabileceksiniz-h151659.html

SANAL GERÇEKLİK

İngiltere'de Dijital Yenilik Merkezi

Northamptonshire, Kettering'deki Tresham College; öğretmenleri en son teknolojilerle tanıştırmayı ve sürükleyici öğrenme deneyimleri sağlamayı amaçlayan Dijital Yenilik Merkezini resmen tanıtmıştır. Tesiste sanal gerçeklik (VR) istasyonları, artırılmış gerçeklik (AR) ekipmanları, 3D baskı makineleri, robotlar ve etkileşimli ekranlar yer almaktadır.

Bedford College Group'un CEO'su Yiannis Koursis, merkezin öğretmenlere en son teknolojileri öğrenmeleri için güvenli bir alan sağlayacağını ve öğretmenlerin öğrencilere öğretme şeklini geliştirmek için farklı teknolojileri deneyebileceklerini ve öğretebileceklerini söylemiştir.

Üniversite tarafından finanse edilen merkez, yeni teknolojilerin derslerde nasıl kullanılabileceğini göstermek için atölyeler ve oturumlar düzenleyen Mark Tinney tarafından yönetilecektir. Yenilik merkezi, bilgi teknolojileri ve danışmanlık hizmetleri sunan bir şirket olan Cisco ile iş birliği içinde geliştirilmiştir.[28]

28 https://www.bbc.com/news/articles/c079x2z57j5o

SİBER GÜVENLİK

Azerbaycan'da Çocuklar İçin Güvenli Bir Dijital Ortama Katkı

Sosyal sorumluluk girişimleriyle bilinen Azerbaycan mobil telefon işletmecisi Nar, 20 Kasım'da kutlanan Uluslararası Çocuk Haklarını Koruma Günü için yeni bir proje başlatmak üzere Bölgesel Kalkınma Kamu Birliği (RIIB) ile ortaklık kurmuştur. Bir ay boyunca Nahcivan, Bakü, Gence, Lenkeran ve Gabala'da çocukların dijital alanda güvenliğini teşvik etmek amacıyla bir dizi farkındalık artırma etkinliği düzenlenecektir.

Projenin ilk aşamasında "Çocukların Zararlı ve Tehlikeli Bilgilerden Korunması" başlıklı çevrimiçi bir oturum düzenlenmiştir. Katılımcılar arasında Nahcivan, Bakü, Gence, Lenkeran ve Gabala'daki 10 okuldan yedi ila on birinci sınıf öğrencileri ve öğretmenler yer almıştır. Oturum sırasında hükümet yetkilileri ve uzmanlar dijital kaynakların güvenli ve sorumlu kullanımı konusunda pratik rehberlik sağlamış ve katılımcıların sorularını yanıtlamıştır. Bu girişim, Bilim ve Eğitim Bakanlığı, Aile, Kadın ve Çocuk İşleri Devlet Komitesi, Azerbaycan Cumhuriyeti İnsan Hakları Komiseri, Azerbaycan Siber Güvenlik Kuruluşları Birliği ve ADA Üniversitesi'nin desteğiyle hayata geçirilmiştir.

Nar, bu projeyle eğitimi destekleme ve çocuk haklarını koruma konusundaki kararlılığını pekiştirmektedir. Şirket, güvenli dijital uygulamaları öğreterek gelecek nesiller için güvenli bir dijital ortam oluşturmayı hedeflemekte ve gelecek nesillerin güvenli bir dijital ortamda büyümesini sağlamak için önemli bir platform görevi görmektedir.[29]

29 https://azertag.az/en/xeber/__nar_contributes_to_a_safe_digital_environment_for_children-3293604

Krispy Kreme Donuts'a Siber Saldırı

Donut zinciri Krispy Kreme, ABD Menkul Kıymetler ve Borsa Komisyonu'na (SEC) yaptığı düzenleyici bir başvuruda çevrimiçi sistemlerini bozan bir siber saldırıya uğradığını açıklamıştır. Gerçekleşen saldırı sonucunda ABD'deki bazı müşteriler çevrimiçi sipariş verememiştir. Olayın şirketin iş operasyonları üzerinde maddi bir etki oluşturmasının oldukça muhtemel olduğu söylenmiş ancak fiziksel mağazaların açık kalmaya devam ettiği belirtilmiştir. Krispy Kreme web sitesinde, "Amerika Birleşik Devletleri'nin bazı bölgelerinde çevrimiçi sipariş de dahil olmak üzere siber güvenlik olayı nedeniyle operasyonel kesintiler yaşıyoruz. Bunun bir rahatsızlık olduğunu biliyoruz ve sorunu çözmek için gayretle çalışıyoruz." ifadesine yer verilmiştir.

Şirket olayı araştırmak ve kontrol altına almak için hemen adımlar attığını ve siber güvenlik uzmanları getirdiğini söylemiş, "Biz de onlarla birlikte, çevrimiçi siparişin yeniden sağlanması da dahil olmak üzere, olayın etkisini azaltmak ve buna yanıt vermek için gayretle çalışmaya devam ediyoruz." açıklamasında bulunmuştur.

Dünya çapında 1400'den fazla mağazası bulunan Krispy Kreme, ABD'de büyük bir gıda zinciri konumunda yer almaktadır. Söz konusu şirket, İngiltere'de daha küçük bir yapıya sahip olmasına rağmen 120 mağazasıyla ülkenin yine en büyük özel donut perakendecisi konumundadır.[30]

30 https://www.bbc.com/news/articles/c4gl9np1g2go

5G VE ÖTESİ

Çin 5G'yi 5G-A Ağına Yükseltiyor

Çin, 5G ağını 5G-A standardına yükseltmek ve 6G ile ilgili araştırma, geliştirme ve inovasyonu teşvik etmek de dahil olmak üzere ülkenin veri altyapısı inşası için taslak yönergeleri açıklamıştır. Çin, doğu, orta ve batı bölgelerinde uluslararası iletişim ağ geçitlerinin konuşlandırılmasını dengeleyecek ve uluslararası denizaltı ve kara kablo bilgi kanallarını genişletecektir. Ulusal veri bürosu tarafından 22 Kasım Cuma günü yayınlanan belgeye göre, uzay ve yer tesislerini entegre eden bir uydu interneti de kurulacaktır.

Görüş almak amacıyla yayımlanan kılavuzda, Çin'in büyük ölçekli, düşük maliyetli, güvenli serbest veri akışını kolaylaştıracağı iletilmektedir. Ayrıca hem merkezi hem de merkezi olmayan işlemler için düşük maliyetli, verimli, güvenilir bir veri dağıtım ortamı sağlamak amacıyla endüstrileri ve bölgeleri blok zinciri ve gizliliği koruyan bilgi işlem gibi alanlarda yeni teknolojik altyapıyı aktif olarak keşfetmeye teşvik edeceği belirtilmektedir. Bununla birlikte kılavuza göre Çin uygun bir bilgi işlem kaynakları düzeni izleyecek ve genel amaçlı bilgi işlem gücü, akıllı bilgi işlem gücü ve süper bilgi işlem gücünün yeşil gelişimini ve koordinasyonunu hızlandıracaktır.

Ülke, gelişmekte olan ağ teknolojilerinin yenilikçi uygulamalarını güçlendirmeyi, ağ faturalama yöntemlerini optimize etmeyi ve doğu ve batı bölgeleri arasındaki veri iletim maliyetini azaltmayı planlamaktadır. 5G-A ağı, hız, gecikme süresi, bağlantı ölçeği ve enerji tüketimi açısından mevcut 5G ağını aşarak indirme işlemleri için saniyede 10 Gigabit ve yükleme işlemleri için saniyede 1 Gigabitlik en yüksek veri hızı seviyesine ulaşmanın yanı sıra milisaniye düzeyinde gecikme süresi ve Nesnelerin İnterneti için düşük maliyetli bağlantı sağlamaktadır. Halihazırda Pekin ve Şanghay gibi şehirlerin bazı bölgelerinde 5G-A şebeke hizmeti sunulmaya başlanmıştır.[31]

31 https://www.chinadaily.com.cn/a/202411/23/WS6741cea7a310f1265a1cf3ba.html

Küresel 5G Uzay Ağı

Araştırmacılar, uzay destekli 5G telekomünikasyonunun geleceğini haritalayarak bir atılım gerçekleştirmiştir. Avrupa Uzay Ajansı (ESA)'nın Bağlantı ve Güvenli İletişimler Müdürlüğü tarafından finanse edilen 5G Altyapı Çalışması (5G-IS), dünya çapında güvenilir bağlantı sağlamak için kapsamlı bir plan sunmaktadır.

Geleneksel uydu internetinden farklı olarak, bu yeni sistem yer tabanlı 5G ağlarıyla sorunsuz bir şekilde entegre olacak ve kullanıcıların şehir merkezlerinde veya uzak okyanusları geçerken bağlantıda kalmalarını sağlayacaktır. Etkileri oldukça kapsamlı olan hizmet ile; otonom araçlar kıtalar arasında sürekli bağlantıyı koruyabilecek, acil durum hizmetleri doğal afetler sırasında kesintisiz çalışabilecek ve uzak topluluklar kentsel alanlarla aynı yüksek hızlı internete erişebilecektir.

Airbus Defense and Space, Eurescom, Fraunhofer FOKUS ve IIS ile Münih Bundeswher Üniversitesi'nden oluşan bir konsorsiyum tarafından yürütülen çalışma, uzay tabanlı 5G altyapısının sadece teorik olarak mümkün olmadığını, ticari olarak da uygulanabilir olduğunu ve 2025 gibi erken bir tarihte konuşlandırılmaya başlayabileceğini göstermektedir.

Araştırma, sistemin kullanıcılar için uygun fiyatlı kalırken finansal olarak sürdürülebilir olacağını göstermektedir. Aylık abonelik ücretleri, temel bağlantı için 6 avrodan premium hizmetler için 60 avroya kadar değişebilmekte ve bu da hem bireysel tüketiciler hem de iş kullanıcıları için erişilebilir olmaktadır.

Otomotiv endüstrisi için sistem, gerçek zamanlı navigasyon güncellemelerinden gelişmiş otonom sürüş özelliklerine kadar her şeyi mümkün kılmaktadır. Aslında çalışma, uzay tabanlı 5G bağlantısından faydalanabilecek ulaşım, iş hizmetleri ve kamu hizmeti sektörlerinde 77 farklı kullanım durumu belirlemiştir. Ancak çalışma, daha fazla enerji tasarruflu uydu yükleri ve gelişmiş anten sistemleri de dahil olmak üzere daha fazla geliştirmeye ihtiyaç duyan kritik teknolojilerle ilgili zorlukları da belirlemiştir. ESA, 5G/6G ve Sürdürülebilir Bağlantı için Uzay Programı aracılığıyla bu zorlukları ele almak için ek araştırmalara halihazırda fon sağlamaktadır. Sonraki adımlar, teknolojik gelişmeyi hızlandırmayı ve uzay endüstrisi oyuncuları ile telekomünikasyon operatörleri arasındaki iş birliğini teşvik etmeyi içermektedir. Çalışma, mobil ağ operatörleri ile uydu operatörleri arasındaki ortak girişimlerin bu teknolojiyi pazara sunmanın en etkili yolu olabileceğini öne sürmektedir.

Bu tamamlanmış çalışmayla Avrupa, uzay ve karasal iletişim ağlarının entegrasyonuna öncülük edecek ve potansiyel olarak dünya genelinde nasıl bağlantı kurduğumuzu dönüştürecek bir konuma gelmiştir. Çalışma, 2025 gibi erken bir tarihte dar bant uygulamalarıyla başlayıp, 2029'dan itibaren genişbant hizmetleri ve 2032'den sonra tam genişbant yetenekleriyle devam edecek aşamalı bir uygulamayı ana hatlarıyla açıklamakta ve telekomünikasyon tarihinde yeni bir dönemi işaret etmektedir.

ESA'da Kıdemli 5G/6G SatCom Çözümleri Mimarı Maria Guta, çalışmanın, teknik ve pazar uyumu kriterleri altında 5G uzay tabanlı altyapı tarafından daha iyi hizmet verilen kullanım durumlarını belirlemek, kategorize etmek ve önceliklendirmek için dikey sektörlerin temsilcilerini içeren bir ortaklık oluşturma ve ortak tasarım yaklaşımını izlediğini açıklamıştır.[32]

32 https://techxplore.com/news/2024-12-path-global-5g-space-network.html

OTONOM ARAÇLAR

Avrupa'nın İlk Otomatik Uygulanabilir Otobüs Garajı

Uygulanabilir bir otomatik otobüs garajı konsepti için ekonomik, teknolojik ve yasal fizibiliteyi doğrulayan kapsamlı bir ön çalışmanın ardından AutoDepot projesi bir sonraki aşamasını, yani ilk prototipin inşasını duyurmuştur. Birkaç İsviçreli toplu taşıma operatörü ise şimdiden söz konusu projeyle ilgilenmeye başlamıştır. Proje, gelişmiş altyapı tabanlı teknolojiden yararlanmaktadır. Buna göre; otobüsler yalnızca kablo kumandalı (drive-by-wire) teknolojiye sahip olup, araç içi otomasyonu bulunmamaktadır. Sistem uzaktan denetime dayanmaktadır. Altyapı, otobüsleri bakım noktalarına ve park alanlarına yönlendirmek için sensörler, kameralar ve otomatik kontrol sistemlerinin bir kombinasyonunu kullanmaktadır.

Bu proje ile otobüs garajlarındaki otobüs sürücülerinin garajlarda otobüsleri beklemek, manevra yapmak ve park etmek gibi önemli zaman harcadıkları bazı verimsiz faaliyetlerin çözümlenmesi istenmektedir. Çünkü bu faaliyetlerin doğrudan yolcu hizmetine katkıda bulunmadığı ve toplu taşımada önemli bir gizli maliyet unsurunu temsil ettiği düşünülmektedir. Garajlarda maddi hasara yol açan ve garaj başına yılda 3 ila 50 arasında değişen kazalara neden olan bu faaliyetler, toplu taşımada artan şoför açığı sorunu oluşmasına da sebebiyet vermektedir. Bu süreçlerin otomatikleştirilmesinin ise sürücülere toplu taşıma operasyonları için zaman kazandıracağı ve böylece sürücülere, yolculara ve operatörlere fayda sağlayacağı düşünülmektedir.[33]

33 https://www.connectedautomateddriving.eu/blog/introducing-the-first-automated-viable-bus-depot/

Çin'den İnsansız Kargo Uçağı

Çinli havacılık girişimi Air White Whale, şirketin dünyanın en büyük nakliye drone'u olduğunu söylediği ilk insansız W5000 kargo uçağını tanıtmıştır. W5000, Jiangsu eyaletinin Changzhou kentinde düzenlenen bir törenle şirketin üretim hattından çıkmış ve kamuoyuna tanıtılmıştır. Pekinli girişimin Yönetim Kurulu Başkanı ve CEO'su Hu Zhendong törende yaptığı konuşmada şirketinin, yüksek operasyonel verimlilikleri ve rekabetçi maliyetleri nedeniyle büyük kargo drone'larının gelecekte hava kargo taşımacılığı sektöründe temel bir unsur haline geleceğine inandığını söylemiştir.

Air White Whale'e göre W5000, maksimum 10,8 metrik ton kalkış ağırlığına, 5 ton yük taşıma kapasitesine ve 65 metreküpten fazla iç kargo alanına sahip çift turboprop bir drone'dur. Uçak yaklaşık 22.9 metre uzunluğunda ve 22.7 metre kanat açıklığına sahiptir. Tek bir uçuşta 2.600 kilometre uçabilmektedir. Air White Whale, insansız hava aracının son derece ekonomik olduğunu - taşıma maliyetlerinin benzer taşıma kapasitesine sahip herhangi bir insanlı kargo uçağının yaklaşık yüzde 60'ı olduğunu - ve her bir yer ekibinin aynı anda yedi adede kadar insansız hava aracını çalıştırabileceğini açıklamıştır. Şirket, W5000'in uçuşa elverişlilik sertifikasyon başvurusunun inceleme ve onay için Çin Sivil Havacılık İdaresi'ne sunulduğunu ve ilk modelin 2026 yılında kullanıcısına teslim edilmesinin beklendiğini, drone'un kasım ayında Guangdong eyaletinin Zhuhai kentinde düzenlenecek olan 15. Çin Uluslararası Havacılık ve Uzay Fuarı'nda sergileneceğini de ilave etmiştir. Drone, güneydoğu ve orta Asya ülkelerinin yanı sıra Rusya ve Japonya'ya da ulaşabilecektir. Şirket, Suudi Arabistan ve Ürdün gibi bazı yabancı ülkelerin niyet siparişleri imzaladığını bildirmiştir.

Sektör gözlemcileri, Çin'in alçak irtifa hava sahası üzerindeki kontrolünü gevşetmesi ve ülkenin online alışveriş işletmelerinin sayısının artmaya devam etmesi nedeniyle kargo drone'larının birçok iş fırsatı yaratmasının beklendiğini söylemektedir. Ülkenin önde gelen devlete ait uçak üreticisi Çin Havacılık Endüstrisi Şirketi ve birkaç özel uçak üreticisi test için çeşitli kargo drone'ları üretmiştir ve yakın gelecekte bunları ticari operasyona sokmayı ummaktadır.[34]

34 https://www.chinadaily.com.cn/a/202410/22/WS6717074aa310f1265a1c8dd2.html

Hibrit Modüler İnsansız Kara Aracı Azman Saha Expo'da

Türkiye'nin ve Avrupa'nın en büyük sanayi kümelenmesi olan SAHA İstanbul tarafından, İstanbul Fuar Merkezi'nde (İFM) düzenlenen SAHA EXPO Uluslararası Savunma, Havacılık ve Uzay Sanayii Fuarı'nda görücüye çıkan AZMAN ile sarp araziler daha kolay aşılacak ve sarp arazilerde görev yapabilen, yüksekliği ayarlanabilen 6x6 taktik tekerlekli ve hidrolik tahrikli hibrit modüler insansız kara aracı AZMAN, Mehmetçik'e güç katacaktır.

HİDROAN Ankara Hidrolik Makine Sanayi Ticaret Limited Şirketi Fabrika Müdürü Neşet Dağdelen, son 10 yılda savunma sanayisi şirketlerine AR-GE danışmanlığı ve çözüm ortaklığı yaptıklarını söylemiştir. Savunma sanayisi üzerine bugüne kadar 15'in üzerinde proje tamamladıklarını ifade eden Dağdelen şunları ilave etmiştir: "AZMAN Projesi de bunlardan birisidir. AZMAN, 8 yıllık bir proje. Projeye, Sanayi ve Teknoloji Bakanlığından AR-GE ve TÜBİTAK'tan destek alarak başladık. Prototip ürün olarak tamamlanan AZMAN, otonom keşif aracı. Diğer araçlardan ayıran özelliği, her tekerleği bağımsız hidropnömatik sistemle çalışan bir araç. İçinde dizel ve elektrikli motorumuz var. Ayrıca onların yanında hibrit çalışan bir araç. Aracın 4 bin 600 kilogram yük taşıma kapasitesi bulunuyor ve kendi ağırlığı ise 6 ton."

Aracın önünde bulunan derinlik kameralarıyla, aynı zamanda lidar ve radar kameralarıyla direkt GSM şirketleriyle bölgesindeki konumunu tespit ettiğini belirten Dağdelen, şu bilgileri vermiştir: "Sonrasında Harita Genel Müdürlüğünün sayfasındaki genel dünya haritasına ulaşarak konumunu sabitliyor. Sabitledikten sonra yazılımı da bize ait olmak kaydıyla sizin konumlandırdığınız bölgeye hareket ediyor. Hareket ederken engel tanımlayabiliyor.

Karşısına çıkan engelleri aşabiliyor. Aşamayacağı bir engel varsa kullanıcısına bunu bildiriyor.

Yöneticisiyle arasındaki irtibatı koparırsa gittiği yolu hafızasına aldığı için tekrar geri komuta merkezine dönebiliyor. Araç tamamıyla yerli üretim. HİDROAN, bu üretimde Sanayi ve Teknoloji Bakanlığından AR-GE desteği ve TÜBİTAK desteği haricinde herhangi bir firmadan destek almamıştır. Yazılım, hidrolik, elektronik dahil kendi bünyesinde üretimini gerçekleştirmiştir. Bunu gerçekleştirirken Orta Doğu Teknik Üniversite ve diğer üniversitelerden yardım almıştır. Yazılım konusunda tamamıyla kendi personelini kullanmıştır. Prototip bir ürün olduğu için ihracatıyla ilgili çalışmalarımız devam etmekte. Bunu gerçekleştirmek için Milli Savunma Bakanlığı ve Savunma Sanayii Başkanlığından kuruluş ve üretim izin belgeleri alındı."

Dağdelen, AZMAN'ın, 6x6, 4x4 ve 8x8 üretilmesi için izin belgeleri olduğunu aktararak, ihtiyaç halinde bunların da direkt üretilip Türk Silahlı Kuvvetleri (TSK) envanterine katılmaya hazır olduğunu anlatmıştır. AZMAN'ın zorlu arazi koşullarına göre üretildiğine dikkati çeken Dağdelen, şunları kaydetmiştir: "AZMAN'ın hızı saatte 30 kilometre. Aracımız hidrolik olduğu için alt kısmını yere indirecek kadar yaklaşmakta, 70 santimetre yerden yükselebilmekte. Noktasal dönüş yapabilmekte. Bu özellikler araca ayrı bir güç katıyor. Arazideki gücü ve performansıyla TSK'ya uzun soluklu hizmet edecek, Mehmetçik'e can kurtarıcı güç olacak."[35]

35 https://www.aa.com.tr/tr/bilim-teknoloji/azman-sarp-arazileri-asarak-mehmetcike-guc-katacak/3370399

NESNELERİN İNTERNETİ (IOT)

Sensörsüz IoT Algılamada THz Altı 6G Ar-Ge Çalışmaları

Finlandiyalı şirket Nokia'nın araştırma ve geliştirme (Ar-Ge) kolu olan Nokia Bell Labs, Fraunhofer Derneği'nin elektrik mühendisliği grubu olan Fraunhofer Heinrich Hertz Enstitüsü (HHI) ve Almanya'daki Avrupa'nın en büyük üniversite hastanesi olan Charité ile birlikte, Terahertz altı (THz altı) kablosuz teknolojilerin invaziv olmayan tıbbi izleme çözümlerine nasıl uygulanabileceğini araştırmaktadır. Söz konusu çalışma kapsamında; THz altı IoT algılamanın, hastaları standart tıbbi cihazlara bağlamaya gerek kalmadan, uzaktan, toplu halde izlemek için yüksek çözünürlüklü mekansal taramalar yapmak amacıyla nasıl kullanılabileceği konusu ele alınmaktadır.

Araştırma grupları, THz altı algılama ağlarının, hastaların hastanelerde hareket ederken kalp atışları gibi bazı hayati belirtilerini sürekli olarak tespit edebileceğini öne sürmüştür. Nokia THz altı frekanslara ilişkin olarak, "Örneğin bir hastane odasında, algılama ağı, elektrokardiyografi elektrotları veya parmak ucu nabız oksimetreleri gibi müdahaleci sensörlerin yardımı olmadan odadaki her hastanın bireysel kalp atışlarını ve solunum hızlarını tespit edip ayırt edebilir. Sensör ağı, ışın oluşturma teknolojilerini kullanarak teorik olarak bireysel hastaları takip edecek ve tuvaletleri kullanırken veya hastanede hareket ederken sürekli olarak izlenmelerini sağlayacaktır." açıklamasını yapmıştır.

6G ağlarının temel bir bileşeni, ağların çevrelerini algılamasına olanak tanıyan ortak iletişim ve algılamadır. Nokia Bell Labs'da temel araştırma başkanı olan Peter Vetter, "Araştırmalarımız

için iletişim sektörünün ötesinde yeni uygulamalar bulabildiğimiz güzel bir gün. Kablosuz algılama, uzun vadeli 6G vizyonumuzun temel bir bileşenidir, ancak bu kavramları daha iyi sağlık çözümleri oluşturmak için uygulayabilirsek, toplum için daha da fazla fayda üretmiş oluruz." demiştir.

Charité Üniversite Eğitim Hastanesi Berlin'deki Benjamin Franklin Kampüsünde anesteziyoloji ve yoğun bakım tıbbı bölüm başkanı Profesör Sascha Treskatsch, "Günlük hayata kolayca entegre edilebilen ve hastanelerin bilgi sistemlerine dahil edilebilen daha esnek ve daha az invaziv izleme çözümlerine ihtiyacımız var." açıklamasını yapmıştır. Fraunhofer HHI'de kablosuz iletişim bölüm başkanı ve Berlin Teknik Üniversitesi ağ bilgi teorisi grubu başkanı Profesör Slawomir Stanczak ise, "THz altı iletişim teknolojisinin tıpta çığır açma potansiyeli muazzamdır. İletişim ve algılama için yüksek bant genişlikleriyle, vücut fonksiyonlarının gerçek zamanlı izlenmesini ve tedavi ilerlemesinin daha hassas bir şekilde gözlemlenmesini sağlar. Bu teknoloji, hastalıkları tespit etme ve hastaları tedavi etme şeklimizi kökten değiştirebilir." diyerek konuya ilişkin düşüncelerini belirtmiştir.[36]

36 https://www.rcrwireless.com/20241217/internet-of-things/nokia-6g-iot-healthcare

UYDU SİSTEMLERİ

Çin'den Uzaya İki Yeni Uydu

Ülkenin önde gelen uzay yüklenicisi China Aerospace Science and Technology Corp'a göre, Çin 25 Kasım Pazartesi sabahı bir Long March 2C taşıyıcı roket fırlatarak iki uyduyu önceden belirlenmiş yörüngelerine yerleştirmiştir. Devlete ait şirket tarafından yapılan açıklamada roketin sabah 7:39'da Kuzeybatı Çin'deki Jiuquan Uydu Fırlatma Merkezi'nden havalandığı ve kısa süre içinde Siwei Gaojing 2C ve 2D uydularını yörüngeye yerleştirdiği belirtilmiştir.

Bir CASC iştiraki olan Şanghay Uzay Uçuş Teknolojisi Akademisi tarafından geliştirilen uydular yüksek çözünürlüklü radarlarla donatılmış olup doğal kaynakların yönetimi, şehir güvenliği, acil durum müdahalesi ve denizcilik operasyonları için veri elde etmek üzere kullanılacaktır. Yine bir CASC iştiraki olan Pekin'deki Çin Fırlatma Aracı Teknolojisi Akademisi'nin bir ürünü olan Long March 2C roket tipi 43 metre uzunluğunda ve 3,35 metre genişliğinde olup 242,5 metrik ton kalkış ağırlığına sahiptir. Roket esas olarak uyduları alçak Dünya ve güneşle eşzamanlı yörüngelere yerleştirmek için kullanılmaktadır.

Görev, Çin'in bu yılki 57. uzay fırlatması ve ülkenin ana fırlatma aracı filosu olan Long March roket ailesinin 547. uçuşu olmuştur.[37]

37 https://www.chinadaily.com.cn/a/202411/25/WS6743c6f8a310f1265a1cf4c9_1.html

Space42 ve BAE Hükümeti Arasında 5 Milyar Dolarlık Sözleşme

Abu Dabi merkezli küresel bir uzay teknolojisi şirketi olan Space42, 2026'dan 2043'e kadar 17 yıl daha kritik, güvenli uydu iletişim hizmetleri sağlamak üzere BAE hükümeti ile 18,7 milyar AED (5,1 milyar $) tutarında bir sözleşme imzalamıştır. Sözleşme kapsamında, BAE şirketi G42'nin bir yan kuruluşu olan Abu Dabi borsasına kayıtlı şirket, yörüngedeki mevcut Al Yah 1 ve Al Yah 2 uyduları ile uydu kapasitesi ve ilgili yönetilen hizmetleri sağlayacaktır. Bu uydulara, sırasıyla 2027 ve 2028 yıllarında fırlatılması beklenen Al Yah 4 ve 5 adlı iki yeni gelişmiş uydu daha eklenmesi beklenmektedir.

Sözleşme, sırasıyla Kasım ve Aralık 2026'da sona erecek olan kapasite hizmetleri anlaşmasının ve yönetilen hizmetler yetkisinin yerini alacaktır. Yeni anlaşma, halihazırda ayrı bir anlaşma kapsamında sağlanan yer segmenti uydu sistemleri ve terminallerinin ilgili operasyon, bakım ve teknoloji yönetimi hizmetlerini birleştirmektedir. Space42, Al Yah 4 ve 5 uydularını inşa etmek için 3,7 milyar AED tutarında avans ödemesi alacaktır. Bu yeni uydular, Orta Doğu, Afrika, Avrupa ve Asya genelinde güvenli devlet iletişimleri sağlayacaktır.

Space42, uyduları inşa etmesi için yakın zamanda Avrupa'nın Airbus firmasıyla anlaşmıştır ve Falcon 9 roket fırlatma aracını kullanarak uyduları yörüngeye fırlatması için Elon Musk'ın SpaceX firmasını seçmiştir. Al Yah 4 ve 5 geliştirme programının uzay aracı, yer segmenti altyapısı, fırlatma ve sigorta dahil maliyeti 3,9 milyar AED olacaktır. Şirketin sözleşmeye bağlanmış 26 milyar AED tutarındaki birikmiş gelirleri, 30 Eylül 2024 itibariyle son 12 aylık gelirlerin 10 katına eşittir ve 2043 yılına kadar gelecekteki nakit akışları için uzun vadeli görünürlük sağlamaktadır. [38]

38 https://www.agbi.com/telecoms/2024/12/space42-bags-5bn-contract-from-uae-government/

YAZILIM

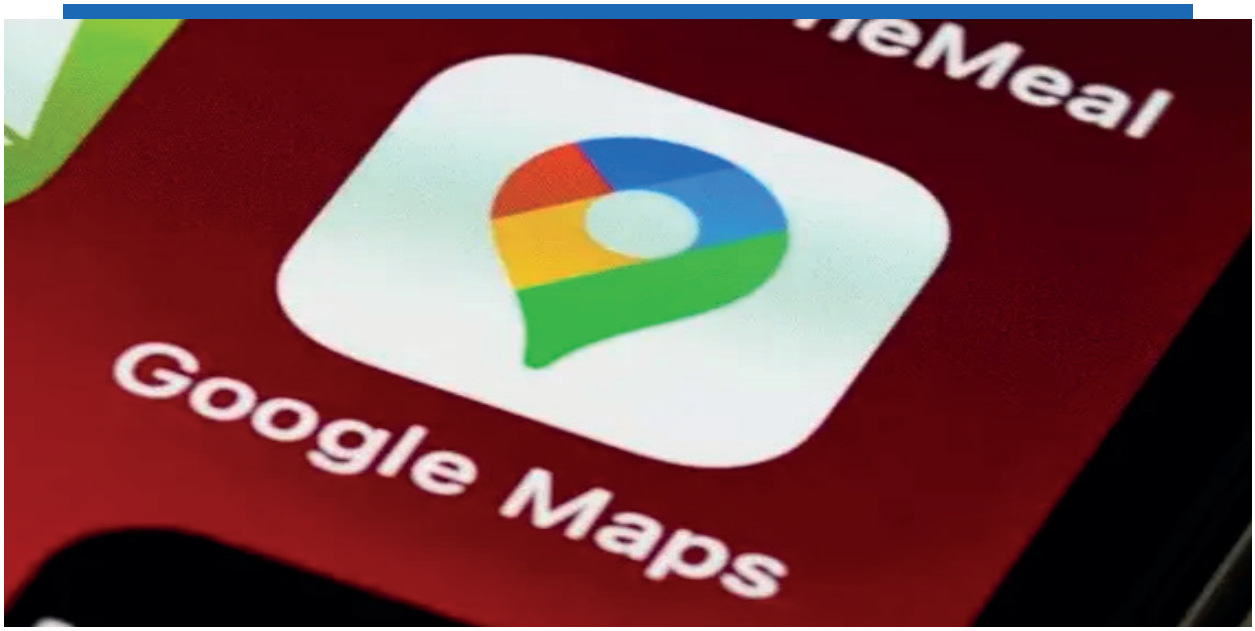
ABD'de Sinir Ağlarının Sürekli Öğrenmesini Sağlayan Yeni Algoritma

Sinir ağları, el yazısıyla yazılmış rakamları tanımlama gibi belirli görevleri öğrenme konusunda dikkate değer bir yeteneğe sahiptir. Ancak, bu modeller ek görevler öğretildiğinde sıklıkla unutma durumu yaşarlar. Yeni ödevleri başarıyla öğrenebilirler, ancak orijinalini nasıl tamamlayacaklarını unuturlar. Otonom arabaları yönlendirenler gibi birçok yapay sinir ağı için, ek görevleri öğrenmek tamamen yeniden programlanmayı gerektirmektedir.

Öte yandan biyolojik beyinler oldukça esnektir. İnsanlar ve hayvanlar, örneğin, yürümeyi ve konuşmayı yeniden öğrenmek zorunda kalmadan yeni bir oyunu nasıl oynayacaklarını kolayca öğrenebilmektedirler. İnsan ve hayvan beyinlerinin esnekliğinden ilham alan Caltech araştırmacıları, sinir ağlarının sıfırdan başlamak zorunda kalmadan öğrenebilecekleri yeni verilerle sürekli olarak güncellenmesini sağlayan yeni bir algoritma türü geliştirmiştir. İşlevsel olarak değişmez yol (FIP) algoritması olarak adlandırılan algoritma, çevrimiçi mağazalardaki önerileri iyileştirmekten otonom arabaları ince ayarlamaya kadar geniş kapsamlı uygulamalara sahiptir. Algoritma, hesaplamalı biyoloji yardımcı doçenti ve Heritage Medical Research Institute (HMRI) Araştırmacısı Matt Thomson'ın laboratuvarında geliştirilmiştir. Araştırma, Ekim'de Nature Machine Intelligence dergisinde yayınlanan yeni bir çalışmada açıklanmıştır.[39]

39 https://www.technology.org/2024/10/19/new-algorithm-enables-neural-networks-to-learn-continuously/

Google Haritalarda Güncelleme



Google, kullanıcı deneyimini geliştirmek amacıyla Haritalar uygulamasında önemli bir güncelleme gerçekleştirmektedir. Şirket hava durumu sekmesinin tasarımını değiştirerek uygulamanın daha sade bir görünüm kazanacağını duyurmuştur. Artık hava durumu bilgileri, uygulamanın alt kısmında yeni bir sekme aracılığıyla sunulacaktır. Kullanıcılar, bulundukları şehrin veya bölgenin adıyla etiketlenmiş olan bu sekmeyi yukarı kaydırarak hava durumu verilerine erişebilecektir. Hava durumu bilgileri, sekme genişletildiğinde uygulamanın sağ üst köşesinde görünür hale gelecektir. Eğer sekme tamamen açılmazsa, hava durumu verisi alt sağ köşede kalmaya devam edecektir. Google, uygulama içindeki karmaşayı azaltmayı ve daha kullanıcı dostu bir deneyim sağlamayı hedeflemektedir. Ancak bu süreçte hava durumu bilgilerine hızlı erişim sağlamak için yeni sekmenin açılması gerektiği kullanıcılar için dikkate alınması gereken bir durumdur.

Yeni tasarım şu anda Google Haritalar'ın beta sürümünde test edilmektedir ancak genel kullanıma ne zaman sunulacağına dair kesin bir tarih açıklanmamıştır.[40]

40 https://www.gizchina.com/2024/10/18/google-maps-update-whats-happening-to-the-weather-tab/

Azerbaycan'dan İklim Konferansı İçin Dijital Ulaştırma Haritası

COP29 Azerbaycan İşletme Şirketi, 11-22 Kasım tarihleri arasında Bakü'de düzenlenmiş olan COP29 iklim konferansına dünyanın dört bir yanından gelen ziyaretçiler için bir Dijital Ulaşım Haritası sunduğunu açıklamıştır. Bu çevrimiçi kaynak, stratejik olarak konumlandırılmış ulaşım merkezleri, mekan erişimi ve otel konaklamaları hakkında önemli bilgiler sağlayarak kullanıcıların COP29 sırasında ulaşım gereksinimlerini kolayca yönetmelerine olanak tanımıştır. Ulaşım merkezleri ağı şehir genelinde stratejik konumları kapsamakta ve bir dizi güzergah ve ulaşım planını bir araya getirmektedir. Merkezler, servis otobüsleri, metro hatları, metro istasyonları ve taksiler de dahil olmak üzere bir dizi çok modlu ulaşım seçeneğine kolay erişim sağlayarak delegeleri ve ziyaretçileri konaklama yerlerinden Bakü Stadyumu'na bağlamaktadır.

COP29 web sitesinde yer alan yeni Dijital Ulaşım Haritası, kullanıcılara önemli merkezlerin nerede olduğunu göstermek üzere tasarlanmıştır. Bu merkezler, COP29 boyunca fuar alanı ve konaklama yerleri arasındaki yolculukları etkin bir şekilde birbirine bağlayarak delegelerin yolculuklarını optimize etmek ve basitleştirmek üzere tasarlanmıştır. Bu kullanıcı dostu kaynak, Mavi ve Yeşil Bölgeler de dahil olmak üzere Bakü Stadyumu, Haydar Aliyev Havaalanı, büyük oteller ve konut komplekslerinin yanı sıra COP29 ulaşım merkezi ağı ve ilgili servis hizmetleri ile ekspres havaalanı transfer güzergahlarına navigasyon sağlamaktadır. Ayrıca park alanları, otobüs durakları ve yolcu alma ve bırakma noktaları hakkında bilgiler de içermektedir. Kullanıcılar, dijital ulaşım haritasındaki ilgili alanları seçerek varış noktaları arasında araçla veya yürüyerek gitmek için en verimli rotaları seçebilmişlerdir.

İnteraktif ulaşım haritası, COP29 Azerbaycan İşletme Şirketi'nin konferans sırasında ziyaretçi akınını etkin bir şekilde yönetmek ve COP29 süresince hem konuklar hem de şehir sakinleri için sorunsuz ve rahat bir hareket sağlamak için uygulamaya koyduğu çeşitli önlemlerden biridir. Alınan diğer önlemler arasında yüzlerce taksi ve 400'e yakın otobüsün hizmete sokulması yer almaktadır. Bunların arasında ekspres halk otobüsleri, özel konferans servisleri ve havaalanı transferleri de yer almakta ve tüm bunlar güvenilir yolcu taşıma hizmetleri sağlamayı amaçlamaktadır. Konferans ulaşım hizmetlerine erişimle ilgili tüm bilgiler COP29 web sitesinde bulunabilmektedir.

Bu yeni, çok modlu ulaşım sisteminin oluşturulması, güvenli ve sorunsuz bir seyahat deneyimi sağlamak üzere tasarlanmıştır ve bir yolcunun Azerbaycan'da kaldığı süre boyunca yaşayacağı uçtan uca deneyimin tamamına uyacak şekilde şekillendirilmiştir.[41]

41 https://news.az/news/digital-transport-map-launched-for-cop29

Google Play Store'dan "Kalitesiz" Uygulamalar İçin Uyarı

ABD merkezli teknoloji devi Google'ın, Android uygulama mağazası Play Store için önemli bir özellik üzerinde çalıştığı ortaya çıkmıştır. Uygulamanın "43.7.19-31" sürümlü kodlarında tespit edilen özellik, Google Play Store'un yakında düşük kaliteli uygulamalarla ilgili uyarılar vereceğini duyurmaktadır.

Google Play Store uygulamasının kodlarında tespit edilen yeni özellik, kullanıcılara bazı bilgilendirmeler yapacaktır. Bu bilgilendirmeler, kullanıcıların söz konusu uygulamalardan uzaklaşmasına yardımcı olacak ve böylelikle potansiyel olarak riskli olan uygulamalara daha az ulaşılmış olacaktır.

İşte bu uyarılar, Google Play'de yüklemeyi planladığınız bir uygulamanın neden kalitesiz olduğuna ilişkin bilgi sahibi olmanızı sağlayacaktır. Eğer bu tür bir uygulamaya denk gelirseniz aynı alandaki diğer uygulamalara bakmanız, daha iyi bir deneyim yaşamanızı sağlamış olacaktır. Ancak bu özelliğin ne zaman kullanılabilir olacağına ilişkin bir bilgi paylaşılmamıştır.[42]

42 https://www.webtekno.com/google-play-store-kalitesiz-uygulamalar-uyaracak-h152371.html

Katar'dan Gelişmiş Konum Zekası Aracı

Katar'ın önde gelen telekomünikasyon ve BT sağlayıcısı Ooredoo, İletişim ve Bilgi Teknolojileri Bakanlığı'nın (MCIT) TASMU Platformu tarafından desteklenen son teknoloji konum analitiği ve istihbarat çözümü Ooredoo Flow'un lansmanını duyurmuştur. Platform, Katar genelindeki işletmeler için stratejik yetenekleri geliştirmek ve operasyonel verimliliği iyileştirmek üzere tasarlanmıştır. Ooredoo Flow Platformu, Katar'ın gelişen pazarının benzersiz taleplerini karşılamak üzere tasarlanmış olup, işletmelere gizlilik ve veri güvenliğine odaklanarak değerli içgörüler sunmaktadır.

Platform, kuruluşlara 4G ve 5G hizmetlerini kullanarak Ooredoo ağının geniş kapsamı aracılığıyla anonimleştirilmiş ve toplanmış veriler sağlamaktadır. Bu tür veriler, yaş, cinsiyet ve işe gidip gelme kalıpları gibi temel demografik eğilimlerin daha net anlaşılmasını sağlamaya katkıda bulunmaktadır. Bu bilgiler, işletmelerin bireysel gizlilikten ödün vermeden müşterilerine daha iyi hizmet vermek için bilinçli kararlar almasını sağlamaktadır. Ooredoo Flow, TASMU Platformu'nu kullanarak günlük 4,3 milyondan fazla benzersiz cihazdan veri toplayarak 200 milyondan fazla veri noktasını işlemektedir. Bu süreçte, en yüksek etik standartlara uyarak Katar yasalarına ve yönetmeliklerine tam uygunluk sağlamaktadır.

Ooredoo Katar CEO'su Şeyh Ali bin Jabor Al Thani yaptığı açıklamada şunları söylemiştir: "İletişim ve Bilgi Teknolojileri Bakanlığı'nın TASMU Platformu tarafından desteklenen, Katar'daki işletmelere stratejilerini iyileştirmeleri, müşteri memnuniyetini artırmaları ve büyümeyi yönlendirmeleri için veri odaklı içgörüler sağlayan çığır açıcı bir platform olan Ooredoo Flow'u tanıtmaktan mutluluk duyuyoruz. MCIT ile iş birliğimiz, Ooredoo Flow'un yalnızca akıllı ve güvenli bir çözüm değil, aynı zamanda ülkemizin dijital dönüşümünü ilerletmek için önemli bir araç olmasını da sağlıyor".

TASMU Platformu tarafından desteklenen Ooredoo Flow'un tanıtımı, şirketin inovasyona olan kalıcı bağlılığını ve işletmeleri son teknoloji aracılığıyla güçlendirmedeki rolünü daha da vurgulamaktadır. Verimliliği, güvenliği ve sürdürülebilirliği artıran araçlar sunarak Ooredoo, Katar'ın gelişen dijital geleceğinde öncü olmaya devam edecektir.[43]

43 https://techafricanews.com/2024/12/09/ooredoo-and-mcit-launch-advanced-location-intelligence-tool-to-propel-qatars-digital-economy/

AKILLI CİHAZLAR

Gıda Teslimatları İçin Kaldırım Robotları ile Drone'ların İşbirliği

Kaldırım robotları, sektörün önemli oyuncuları arasında yapılan bir anlaşmayla Dallas'taki teslimatlarda havadaki bazı meslektaşlarına yardımcı olmaya hazırlanmaktadır. Yapılan açıklamaya göre, otomatik dört tekerlekli makineler geliştiren Serve Robotics, siparişlerin taşınmasında verimliliğin artırılmasına yardımcı olmak amacıyla bir drone teslimat şirketi olan Wing ile birlikte çalışmak üzere bir pilot ortaklık başlatmıştır. Serve'in Teksas'a girişini işaret eden bu girişimin önümüzdeki aylarda hayata geçmesi planlanmaktadır.

Serve CEO'su Ali Kashani yaptığı açıklamada, Serve ve Wing'in birlikte, geniş ölçekte güvenilir ve uygun fiyatlı robotik teslimat için iddialı bir vizyonu paylaştığını ve uçtan uca robotik teslimat çözümlerinin, teslimatların önemli bir çoğunluğu için en verimli yöntem olacağını söylemiştir.

Ortaklık, bazı teslimatlar için bir zorluğu ele almaktadır. Bu da siparişleri dronların fırlatılabileceği bir yere götürmektir. Uçan cihazlar, kalabalık şehir ortamlarında zor olabilen toplama alanlarında alana ihtiyaç duyarken, kaldırım robotları, menzil sınırlı olsa bile şehir sokaklarında gezinmek için üretilmiştir. Yeni düzenlemeye göre, Serve teslimat robotları restoran siparişlerini kaldırım kenarından alacak ve yemekleri aktarmak üzere bir drone "Otomatik Yükleyiciye" teslim edecektir. Paket buradan da altı mil uzaklıktaki müşterilere havadan teslim edilecektir.

Açıklamada, Serve ve Wing'in her iki teknolojinin güçlü yanlarından yararlanarak daha güvenilir yemek teslimatı sağlayacağı belirtilmiştir.

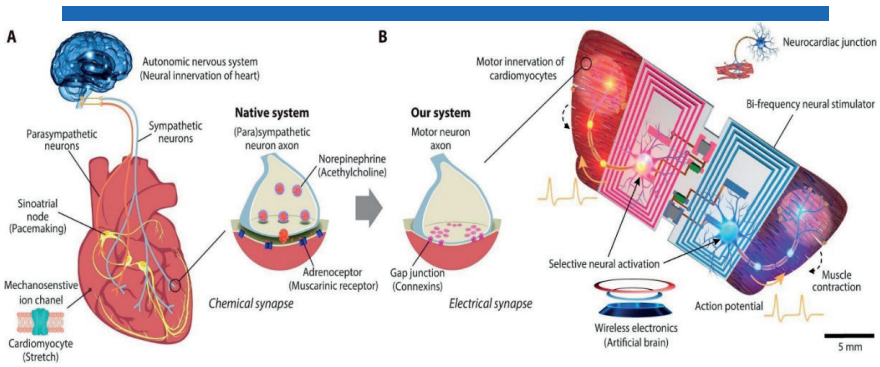
Wing CEO'su Adam Woodworth yaptığı açıklamada, bu pilot ortaklık sayesinde Wing'in, Serve'i teslimat yarıçapını genişletmek için çalışırken desteklediğini ve çok yoğun bölgelerde daha fazla müşteriye ulaşmayı ümit ettiklerini söylemiştir.

Serve teslimat hizmetini Los Angeles'ta yürütmekte olup Vancouver, British Columbia'da da bir pilot uygulama gerçekleştirmiştir. Uber'den 2021 yılında bağımsız bir şirket olarak ayrılan Serve, Uber Eats ve 7-Eleven gibi iş ortakları için teslimatlar gerçekleştirmiştir. Dallas bölgesinde faaliyet gösteren ve Wal-Mart'a teslimatlarda yardımcı olan Wing, 2018'de Google'ın ana şirketi Alphabet'in bir yan kuruluşu haline gelmiştir.

Dallas kaldırım robotlarına yabancı bir şehir değildir. Örneğin Dallas'taki Teksas Üniversitesi, otonom makineler aracılığıyla yemek teslimatı yapılmasını sağlamaktadır.[44]

44 https://techxplore.com/news/2024-10-sidewalk-robots-teaming-drones-dallas.html

ABD'de Biyohibrit Yüzme Robotu



ABD'deki Brigham and Women's Hastanesi ve İsviçre'deki iPrint Enstitüsü'nden biyo araştırmacılar ve robotikçilerden oluşan bir ekip, insan motor nöronları ve kas dokusunu taklit etmek için yetiştirilen kardiyomiyositleri kullanarak küçük bir yüzme robotu geliştirmiştir. Çalışmaları Science Robotics dergisinde yayımlanmıştır. Colorado Boulder Üniversitesi'nde makine mühendisi olan Nicole Xu, aynı derginin Focus sayısında hayvan dokusu kullanarak biyo-esinli robotlar oluşturmaya yönelik devam eden çalışmaları özetleyen bir makale yayınlamıştır.

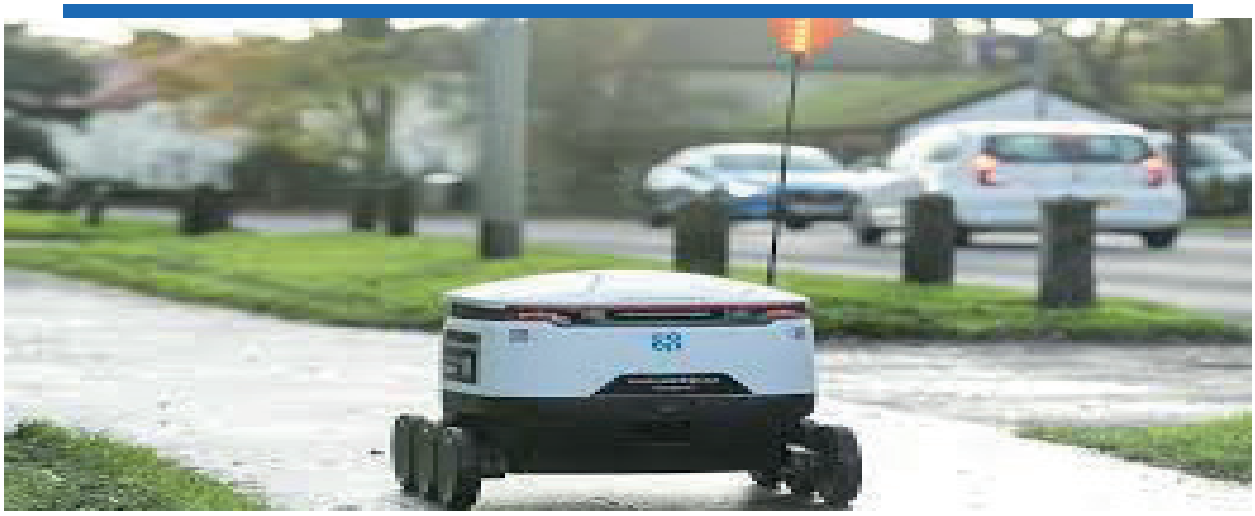
Bilim kurgu yazarları ve film yapımcıları uzun yıllar boyunca elektronik, bilgisayar ve hayvan dokusunu bir araya getirerek benzersiz ve bazen de ürkütücü özelliklere sahip robotlar oluşturma fikrini kullanmışlardır. Xu, gerçek dünyada bu tür çalışmaların devam ettiğini belirtmektedir.

İnsanlar da dahil olmak üzere hayvanlar, robotların yapabileceklerinin çok ötesinde yeteneklere sahiptir. Örneğin çamaşır yıkamak, kirli çamaşırları ayırmak, çamaşır makinesi ve kurutucu ayarlarını seçmek ve çamaşırları katlamak ya da asmak gibi sayısız beceri gerektirmektedir. Bu tür faaliyetler hem el becerisi hem de zihinsel işlem gerektirmektedir. Bu nedenle robotikçiler biyohibrit robotların geliştirilmesini araştırmaktadır. Araştırma ekibi, insan motor nöronları tarafından aktive edilen insan kas hücrelerini kontrol eden bir bilgisayar beynine sahip ışın benzeri bir yüzme robotu oluşturmuştur. Robotu oluşturmak için araştırmacılar, insan pluripotent kök hücreleri kullanılarak üretilen hem motor nöronları hem de kardiyomiyositleri kültüre almışlardır. Kardiyomiyositler, motor nöronlarla birleşmelerine izin verecek şekilde ışın yüzgeçlerine benzeyen bir iskele üzerinde kas hücresi dokusuna dönüşecek şekilde programlanmıştır. Bu da elektriksel sinapsların oluşmasını sağlamıştır. Motor nöronlardan bazıları daha sonra robotun beyni olarak görev yapan bir elektronik işlemciye bağlanmıştır. Bu işlemci, insan kontrolörlerden gelen sinyalleri sol veya sağ yüzgece ya da her ikisine birden aktaran Wi-Fi devresini barındırmaktadır. Bu şekilde, araştırmacılar robotlarının hareketini kontrol edebilmişler ve sonunda ona yüzme yeteneği kazandırmışlardır.

Zamanla araştırma ekibi, keskin dönüşler yapmak da dahil olmak üzere robotu hassas bir şekilde manevra ettirebildiklerini keşfetmişlerdir. Ayrıca robotu 0,52 ± 0,22 mm/s'ye varan hızlarda yüzdürebildiklerini de fark etmişlerdir.[45]

45 https://techxplore.com/news/2024-10-biohybrid-robot-motor-neurons-cardiomyocytes.html

Estonya'da Robot Teslimatı

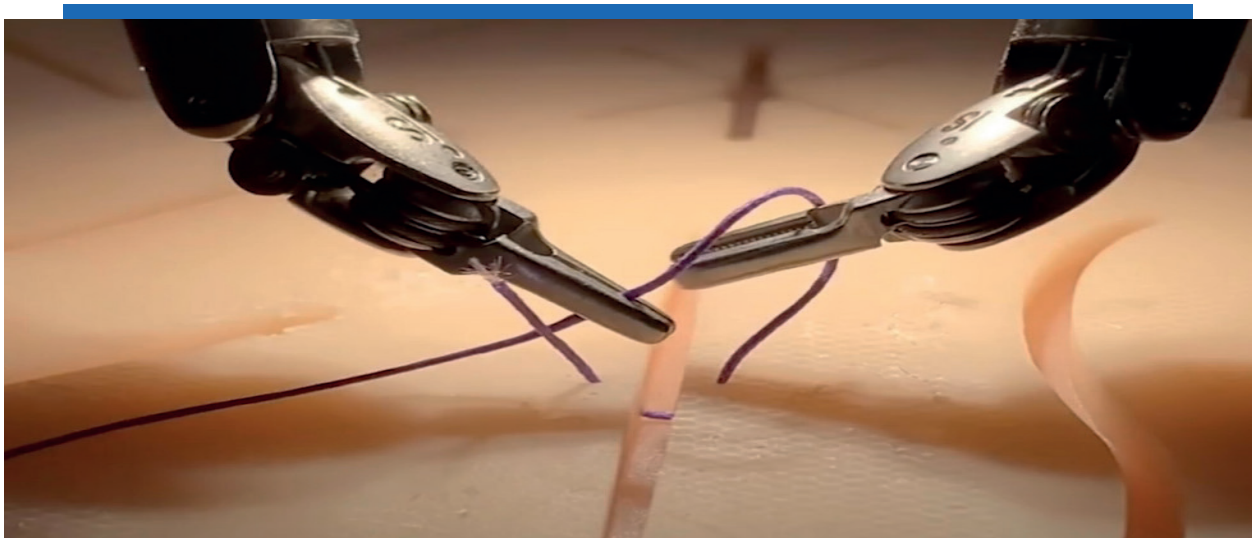


Estonya'da Starship Technologies ve Bolt firmaları önderliğinde yürütülen çalışmalar sonuç vermiş ve Tallinn'deki üç Bolt Market mağazasından Bolt Food uygulaması aracılığıyla çevre dostu bir teslimat seçeneği olan Robot teslimatları başlamıştır. 180 binden fazla sakin, robot teslimatlarından lansman dönemine özel olarak ücretsiz yararlanabilecektir. Starship Technologies'in Kurucu Ortağı ve CEO'su Ahti Heinla yaptığı açıklamada şunları söylemiştir: "Bugün Bolt ile lansman yapmaktan ve otonom yemek teslimatını Tallinn'de daha fazla müşteriye ulaştırmaktan heyecan duyuyoruz. Bu iş birliği yalnızca kolaylık ve daha fazla seçenekle ilgili değil; robotlarımızı Bolt Food uygulamasına entegre ederek, yerel trafiği ve emisyonları azaltan sürdürülebilir, ölçeklenebilir bir son nokta teslimat çözümü sunuyoruz. Bu, Avrupa genelinde daha yeşil şehirler için yenilik yapmaya ve yol açmaya devam ederken her iki şirket için de heyecan verici bir adımdır".

Bolt Başkanı Jevgeni Kabanov ise şunları söylemiştir: "Starship Technologies robot teslimatlarının Tallinn'de başlatılmasıyla birlikte Bolt Market müşterilerine yeni bir teslimat deneyimi sunuyoruz. Bu, Estonya inovasyonunda Starship ile paylaştığımız yeniliklerin bir yansımasıdır ve bu deneyimi Bolt Market yenilikçi teknolojileriyle güçlendirmek için kullanmaktan gurur duyuyoruz. Teknolojinin farklı sektörlerde kullanılması hizmet kalitesinin arttırılması ve aynı zamanda çevrenin korunarak sürdürülebilir bir dünya oluşturulması için oldukça önemlidir."[46]

46 https://retailtechinnovationhub.com/home/2024/10/16/starship-technologies-and-bolt-launch-eco-friendly-robot-powered-grocery-delivery-service-in-estonia

Cerrahi Robotları Eğitmek İçin Taklit Öğreniminin Kullanımı



Deneyimli cerrahların videolarını izleyerek ilk kez eğitilen bir robot, aynı cerrahi prosedürleri insan doktorlar kadar ustalıkla uygulamıştır. Cerrahi robotları eğitmek için taklit öğrenmenin başarılı bir şekilde kullanılması, tıbbi bir prosedür sırasında gereken her bir hareket için robotları programlama ihtiyacını ortadan kaldırmakta ve robotik cerrahi alanını, robotların insan yardımı olmadan karmaşık ameliyatları gerçekleştirebileceği gerçek otonomiye yaklaştırmaktadır.

Johns Hopkins Üniversitesi Makine Mühendisliği Bölümü'nde yardımcı doçent olan kıdemli yazar Axel Krieger, "Bu modele sahip olmak gerçekten büyüleyici ve tek yaptığımız onu kamera girdisiyle beslemek. Ameliyat için gereken robotik hareketleri tahmin edebiliyor. Bunun tıbbi robotikte yeni bir sınıra doğru atılmış önemli bir adım olduğuna inanıyoruz." diye konuşmuştur.

Stanford Üniversitesi araştırmacılarının da dahil olduğu ekip, sezgisel da Vinci Cerrahi Sistem robotunu cerrahi prosedürlerde gerekli olan üç temel görevi yerine getirecek şekilde eğitmek için taklit öğrenmeyi kullanmıştır. Bu görevler arasında bir iğneyi yönlendirmek, vücut dokusunu kaldırmak ve dikiş atmak yer almaktadır. Her durumda, ekibin modeli üzerinde eğitilen robot, aynı cerrahi prosedürleri insan doktorlar kadar ustalıkla gerçekleştirmiştir.

Model, taklit öğrenimini ChatGPT'nin temelini oluşturan aynı makine öğrenimi mimarisiyle birleştirmiştir. Ancak ChatGPT'nin kelimeler ve metinlerle çalıştığı yerde, bu model robotik hareketin açılarını matematiğe döken bir dil olan kinematikle konuşmaktadır.

Araştırmacılar modellerini, cerrahi prosedürler sırasında da Vinci robotlarının kollarına yerleştirilen bilek kameralarından kaydedilen yüzlerce video ile beslemişlerdir. Dünyanın dört bir yanındaki cerrahlar tarafından kaydedilen bu videolar, ameliyat sonrası analiz

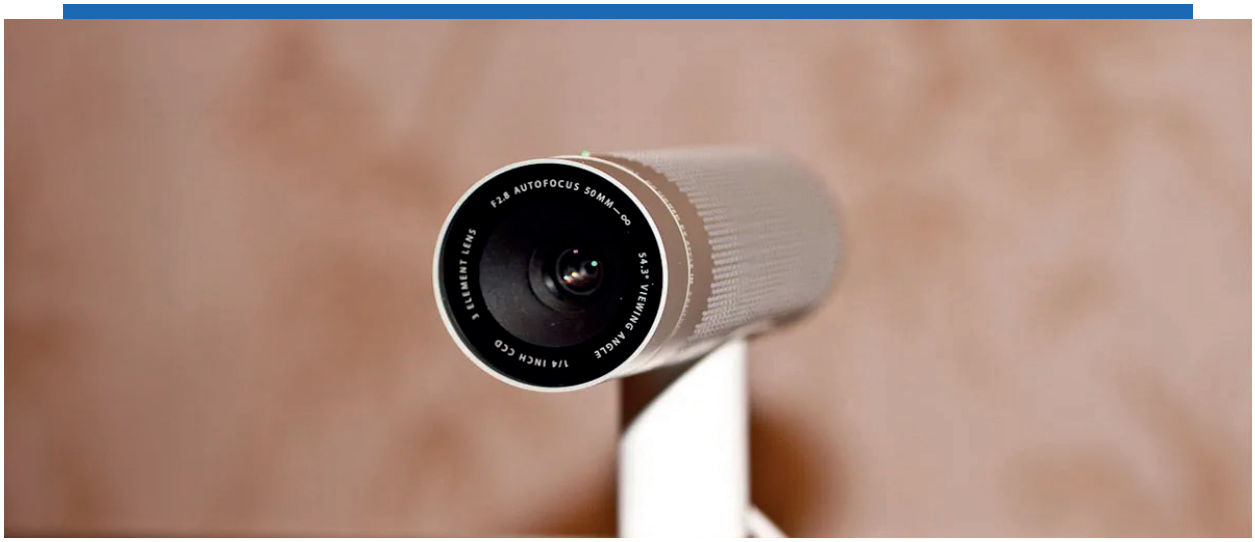
için kullanılmakta ve daha sonra arşivlenmektedir. Dünya çapında yaklaşık 7.000 da Vinci robotu kullanılmakta ve 50.000'den fazla cerrah sistem üzerinde eğitilerek robotların "taklit edebileceği" geniş bir veri arşivi oluşturulmaktadır. Da Vinci sistemi yaygın olarak kullanılıyor olsa da, araştırmacılar bu sistemin herkesin bildiği gibi kesin olmadığını söylemektedir. Ancak ekip kusurlu girdiyi çalıştırmanın bir yolunu bulmuştur. Anahtar, modeli hatalı olan mutlak eylemler yerine göreceli hareketler gerçekleştirecek şekilde eğitilmektir.

Johns Hopkins'te doktora sonrası araştırmacı baş yazar Ji Woong "Brian" Kim, "İhtiyacımız olan tek şey görüntü girdisi ve ardından bu yapay zeka sistemi doğru eylemi buluyor. Birkaç yüz demo ile bile modelin prosedürü öğrenebildiğini ve karşılaşmadığı yeni ortamları genelleştirebildiğini gördük." diye belirtmiştir. Krieger ise şu ifadeleri eklemiştir: "Model ona öğretmediğimiz şeyleri öğrenmekte çok başarılı. Örneğin iğneyi düşürürse otomatik olarak alıp devam ediyor. Bu benim ona öğrettiğim bir şey değil."

Araştırmacılar, modelin cerrahi robotları her türlü cerrahi prosedürü gerçekleştirecek şekilde hızla eğitmek için kullanılabileceğini belirtmektedir. Ekip şimdi bir robotu sadece küçük cerrahi görevleri değil, tam bir ameliyatı gerçekleştirecek şekilde eğitmek için taklit öğrenimini kullanmaktadır. Bu ilerlemeden önce, bir robotu bir ameliyatın basit bir yönünü bile gerçekleştirecek şekilde programlamak, her adımı elle kodlamayı gerektiriyordu. Krieger, birinin dikiş atmayı modellemeye çalışmak için on yıl harcayabileceğini söylemiştir ve bu sadece tek bir ameliyat türü için dikiş atmak anlamına gelmektedir.[47]

47 https://www.therobotreport.com/researchers-use-imitation-learning-to-train-surgical-robots/

Apple'dan İnsanları Yüzlerini Görmeden Tanıyabilen Güvenlik Kameraları



Apple'ın 2026 yılında piyasada olması beklenen akıllı kameraları, insanları tanımak için yüzlerini görmek zorunda olmayacaktır. Bu kamerada Apple Intelligence yapay zekâ araçlarının kullanılabileceği ifade edilmiştir. Yeni ortaya çıkan patentler de Apple'ın bu yönde ilerlemeyi planladığını ortaya koymaktadır.

Apple'ın yeni patentine göre güvenlik kamerası, yüz tanıma teknolojisinden daha ileride olacak ve bir kişinin kimliğini, kişinin yüzünü göremese bile tespit edebilecektir. Sistem, yüz tanıma ile kimliğini doğruladığı kişilerin vücut özelliklerini hafızasına kaydedebilecektir. Bu özellikler arasında kıyafetleri tanıma ve vücut şeklini öğrenme gibi özellikler yer almaktadır.

Patente göre bu bilgiler değişen sürelerde güvenlik kamerasının hafızasında tutulacaktır. Örneğin kıyafetler yalnızca bir günlüğüne kameranın hafızasına alınacak ancak vücut yapısı verisi daha uzun süre saklanabilecektir. Sistem ayrıca kişilerin yürüyüş şekli gibi hareket izlerini de analiz edebilecek ve bu teknoloji ile birlikte Apple, kişileri yüzlerinin görünmediği durumlarda bile tanıyabilecektir.[48]

48 https://9to5mac.com/2024/11/26/an-apple-security-camera-could-recognize-people-even-if-their-face-isnt-visible/

Amazon Depolarında Robot Kullanımına Ağırlık Veriyor

ABD'li e-ticaret şirketi Amazon, depolarında verimliliği artıracağını ve çalışan yaralanmalarını azaltacağını açıkladığı bir dizi robotu tanıtmıştır. Robin ve Cardinal adlı iki robotik kol, yaklaşık 23 kilograma kadar ağırlıktaki paketleri kaldırabilmektedir. Sparrow adlı üçüncü robot ise kutuların içinden eşyaları alıp diğer kutulara yerleştirebilmektedir. Zeminde çalışan mobil robot Proteus, depoda yer alan içi kargo yüklü arabaları hareket ettirerek ilgili istasyonlara aktarabilmektedir. Buna ek olarak Amazon, iki ayaklı insansız robotları da test etmektedir. Digit adı verilen bu robot, boş kutuların taşınması için test edilmektedir.

Amazon yetkilileri, Robin adlı robotun halihazırda düzinelerce depoda kullanıldığını ve siparişlerin teslimi için gereken süreyi azaltmak ve çalışanların tekrarlayan görevlerden kaçınmasına yardımcı olmak gibi önemli faydalar sağladığını ifade etmektedirler.[49]

49 https://www.usnews.com/news/best-states/tennessee/articles/2024-11-25/as-amazon-expands-use-of-warehouse-robots-what-will-it-mean-for-workers

SOSYAL AĞLAR

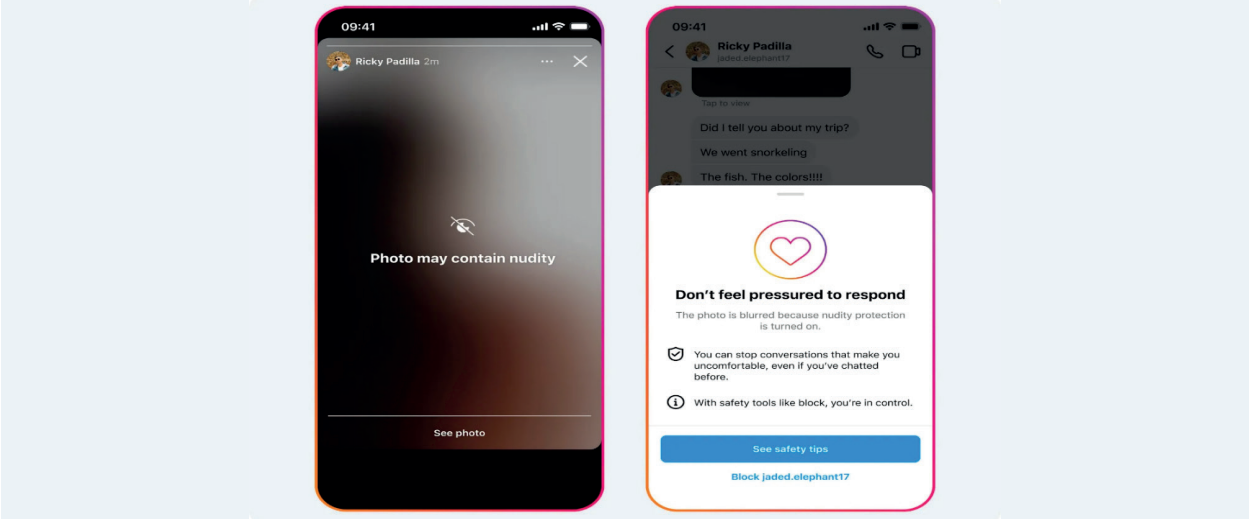
Google'dan Yapay Zekâ ile Oluşturulan Metinlere Filigran

Üretken yapay zekâlar gelişmeye devam ettikçe teknoloji devleri de yapay zekâların çıktılarının tespit edilebilmesi için araçlar geliştirmeye devam etmektedir. Google da SynthID TexT adını verdiği teknoloji ile birlikte kamuya açık yapay zekâ modellerinin ürettiği içerikleri ayırt etmeyi sağlayacak dijital filigran üzerinde çalışmaktadır. SynthID TexT, Hugging Face yapay zekâ platformu ve Responsible GenAI Toolkit üzerinden indirilebilecektir. Firmanın resmi X hesabı üzerinden yapılan açıklamada "SynthID TexT filigran aracını açık kaynak kodlu hâle getiriyoruz. Geliştiriciler ve işletmeler için ücretsiz olarak kullanıma açık ve yapay zekâ ile üretilmiş içerikleri anlamalarını sağlayacak." ifadesi kullanılmıştır.

Yapay zekâ modelleri çalışırken Token dağılımı kullanmaktadır. Google'ın yeni teknolojisi de metinleri bu tokenler ile eşleme prensibi üzerinden çalışmaktadır. SynthID TexT, kelimelerin oluşturulma olasılıkları üzerinden bir desen oluşturmakta ve bu desene göre işaretlemelerde bulunmaktadır. Google bu teknolojinin bazı sınırları olduğunu da kabul etmektedir. Özellikle kısa metinler, yeniden yazılan ya da başka dile çevrilen makaleler ve bilgiye dayalı metinler söz konusu olduğunda model çok başarılı bir performans sergilememektedir.[50]

50 https://www.thedrum.com/news/2024/10/23/expanded-access-google-s-synthid-text-watermarking-tool-may-help-advertisers-win

Instagram'dan Gençleri Cinsel Şantaja Karşı Korumada Yeni Güvenlik Özellikleri



Instagram, çocukları ve gençleri cinsel şantaj gibi durumlardan korumak için yeni güvenlik araçları ekleyerek platformdaki güvenliği artırmayı hedeflemektedir. Şirketin duyurduğu en son güvenlik önlemleri arasında Instagram üzerinden mesaj yoluyla gönderilen geçici fotoğraf ve videoların ekran görüntüsü alınmasını ve ekran kaydı yapılmasını engelleyen bir özellik yer almaktadır. Bu hamle ile son dönemde giderek yaygınlaşan cinsel şantaj gibi durumların önüne geçilmesi amaçlanmaktadır.

Instagram ayrıca çocuklar ve gençler için sextortion adı verilen, kişinin cinsel içeriklerini kullanarak istediklerini yaptırma amacı güttüğü durumları tespit etmeyi ve bu duruma maruz kalanların nasıl davranması gerektiğini anlatan bir bilgilendirme kampanyasını da uygulama içinde kullanıma sunacaktır. Instagram buna ek olarak bu tarz eylemlerde bulunan hesapların belirlenmesi durumunda bu hesapların başkalarının takipçilerini veya takip listelerini görmelerini engelleyecek bir özellik de eklemeyi planlamaktadır. Bu sayede kötü niyetli kişinin, sextortion uyguladığı gencin yakınlarına da ulaşması engellenecektir.[51]

51 https://techcrunch.com/2024/10/17/instagram-rolls-out-new-safety-features-to-protect-teens-from-sextortion/

Meta'dan Dolandırıcıların Ünlüleri Kullandığı Reklamlara Yüz Tanıma Sistemi

Yapay zekâ tabanlı teknolojilerin gelişmesi, sahtecilik girişimlerinin artmasına yol açmıştır. Artık geliştirilen teknolojiler, ünlü isimlerin yüzlerinin ve seslerinin kullanılarak sahte içerikler üretilmesini sağlamaktadır. Bu durumun farkında olan Meta, konuyla ilgili dikkat çeken bir açıklama yapmıştır. Yapılan açıklamaya göre dolandırıcılık amacıyla ünlülerin ses ve görüntülerinin kullanıldığı reklamlar, artık yüz tanıma sistemleriyle denetlenecektir.

Meta, dolandırıcılık amaçlı reklamlar için yeni bir yüz tanıma mekanizması oluşturmuştur. Geliştirilen algoritma, sahte reklamlarda kullanılan ünlü isimlerin yüzleri ile o kişilerin profil fotoğraflarını kıyaslayacaktır. Meta'nın resmî açıklamasına göre yüz tarama sistemi, Facebook ile Instagram reklamlarında kullanılacaktır. Ünlüler ile bilindik kamu görevlilerinin yüzlerini tarayacak olan sistem, sonraki aşamada reklamları analiz edecektir. Eğer olağan dışı bir durum tespit edilirse reklam içeriğindeki yüz ile o kişiye ait profil fotoğrafı arasında kıyaslama yapılacaktır. Böylelikle yapay zekâ ile oluşturulmuş sahte görüntüler tespit edilip, kullanıcılara ulaşması engellenmiş olacaktır. Meta, söz konusu özelliğin sadece dolandırıcılık amaçlı reklamlara özel olmayacağını açıklamıştır. Yapılan açıklamaya göre bir şekilde hesap bilgilerini kaybeden kullanıcılar, hesap kurtarmak için yüz tarama sisteminden faydalanabileceklerdir. Ancak bu özellik isteğe bağlı olacaktır. Meta'ya göre yüz tarama sistemi için kullanılacak veriler, tarama işleminin ardından sunuculardan silinecektir.[52]

52 https://www.theguardian.com/technology/2024/oct/22/meta-to-use-facial-recognition-technology-in-fight-against-celebrity-investment-scam-ads

İsveç'te Sosyal Medyaya Yaş Sınırlaması

İsveç'teki yetkililer, çocukların çevrimiçi olarak çetelere katılmalarından endişe duymaktadır. İsveç polisine göre, suçlular İsveçli çocuklarla ilk kez TikTok, Instagram veya Snapchat'te onları takip ederek sosyal medyada temas kurmakta ardından, suç eylemlerinin Signal veya Telegram gibi şifreli uygulamalara geçilerek söz konusu süreci sürdürmektedir. 2024 Uluslararası Öz Bildirim Suçluluğu Çalışmasına göre, İsveç %11'lik bir genç çete katılım oranına sahiptir. Bu duruma istinaden İsveç tarafından, çevrimiçi çete katılımıyla mücadele konusunda Avustralya'daki uygulamaya benzer şekilde sosyal medyaya girişte yaş sınırlaması getirilmesi konusu değerlendirilmektedir.[53]

53 https://www.euronews.com/next/2024/12/15/sweden-considers-australia-style-social-media-age-limits-to-fight-online-gang -recruitment

Tiktok, Romanya Seçimlerine Müdahale Endişeleri Nedeniyle Soruşturma Altında

Günümüzde sosyal medya platformları birçok referandum için ciddi baş aktörler ve etkileyiciler olarak görülmektedir. Bu bağlamda, TikTok, Romanya seçimleri bağlamında seçim bütünlüğünü tehlikeye atabilecek sistemik riskleri değerlendirme ve azaltma yükümlülüğünü yerine getirip getirmediği konusunda Avrupa Birliği (AB) düzenleyicileri tarafından soruşturma altına alınmıştır. Bahsi geçen soruşturma, TikTok'un tavsiye algoritmaları ile platformdaki hizmetin manipüle edilmesi veya kötüye kullanılması risklerine odaklanmaktadır. Ayrıca TikTok'un siyasi içerikler ve reklamlar için uyguladığı ödeme politikaları da incelenen başlıklar arasındadır.

Soruşturmanın odağındaki Romanya seçimleri, geçtiğimiz hafta 85.000'den fazla siber saldırıya uğramasının ardından iptal edilmiştir. Bu saldırılar sonucunda seçim sitelerine erişim bilgileri çalınmış ve ülkedeki seçim sistemi önemli bir güvenlik kriziyle karşı karşıya kalmıştır.

AB'nin Dijital Hizmetler Yasası (DSA) çerçevesinde yürütülen bu inceleme, Avrupa genelinde ciddi tartışmalara yol açmıştır. Özellikle aşırı sağcı politikacılar soruşturmayı sert bir şekilde eleştirmiştir. Polonyalı Patryk Jaki, bu adımı "sansür" olarak tanımlarken, Fransız Catherine Griset ise AB'nin yanlış bilgilendirmeler ile mücadelesinde "totaliter bir rejim" gibi hareket ettiğini savunmuştur.

Bu yıl dünya genelinde seçimlere yönelik müdahaleler artış gösterirken, sosyal medya platformları propaganda ve yanlış bilginin yayılması konularında kritik bir araç hâline gelmiştir. AB'nin TikTok'a yönelik bu hamlesi, yalnızca bu platform için değil, aynı zamanda diğer teknoloji devleri için de emsal oluşturabilecek bir karar sürecini başlatabilecektir.[54,]

54 https://www.techradar.com/pro/tiktok-is-under-investigation-for-romanian-election-interference-concerns

Sürükleyici Navigasyon Deneyimi için 3D Sokak Görünümü

Güney Kore'nin önde gelen portalı Naver Corp, Naver Harita uygulaması için yeni bir "3-D" navigasyon özelliğini duyurmuştur. Bu gelişmiş hizmet, sokak görünümü özelliği içinde bile ayrıntılı bina ve işletme bilgilerini 3 boyutlu formatında görüntüleyerek daha sürükleyici, üç boyutlu bir keşif deneyimi sağlamayı amaçlamaktadır.

Resmi olarak 16 Aralık'ta başlatılan "Street View 3D" hizmeti, Naver'in uzamsal zeka yeteneklerini önemli ölçüde genişletmektedir. İlk olarak Seul'deki önemli ticari bölgelerde kullanıma sunulan güncelleme, ayrıntılı, gerçek dünya görsellerini konum verileriyle sorunsuz bir şekilde harmanlayarak kullanıcılara zenginleştirilmiş bir navigasyon deneyimi sunmak üzere tasarlanmıştır. 16 Aralık Pazartesi gününden itibaren Naver'in "Street View 3D" özelliği Gangnam, Yongsan, Mapo, Songpa, Yeongdeungpo, Jongno, Jung gibi Seul'ün önemli bölgelerinin yanı sıra Gyeonggi Eyaletindeki belirli bölgelerde de kullanılabilecektir. Şirket, hizmeti kademeli olarak diğer bölgelere genişletmeyi planlamaktadır. Hassas mekansal verileri yakalamak için Naver, gelişmiş sensörleri ve LiDAR teknolojisini birleştiren tescilli P1 panoramik haritalama sistemini kullanmıştır. Bu hizmet, geleneksel iki boyutlu sokak görünümüne kıyasla daha sürükleyici, üç boyutlu bir görünüm sunarak kullanıcıların konumları daha derinlemesine keşfetme becerisini artırmaktadır. Bu özellik, kullanıcılar farklı alanlarda gezinirken bina dizinleri ve işletme ayrıntıları gibi ek bilgiler sağlamaktadır. Örneğin, kullanıcılar konuma ulaşmadan önce bile rotaları üzerindeki işletmelerin menülerini, çalışma saatlerini ve özel tekliflerini görüntüleyebilmektedir. Daha önce Naver Map'in masaüstü versiyonunda bulunan bu bilgilere artık mobil uygulama üzerinden de erişilebilecektir. Yeni bir otomatik oynatma modu, kullanıcıların yürüyüş rotaları boyunca gerçek zamanlı hareketi simüle etmelerine olanak tanıyarak daha etkileşimli bir deneyim sunmaktadır.

Naver, yıllık geliştirici konferansında yaptığı bir ön gösterimde, gelecekteki güncellemelerin kullanıcıların Google'ın Street View'ına benzer şekilde büyük binaların iç mekanlarını

havaalanları ve simge yapıların içinde keşfetmelerine olanak tanıyabileceğini ima etmiştir. Bu, alışveriş merkezleri veya kongre merkezleri içinde ayrıntılı gezinmeyi de içerebilmektedir. Şirket ayrıca işletme menülerini ve promosyon kuponlarını doğrudan Street View arayüzünden kontrol etme becerisini de sergilemiştir.

Street View 3D ayrıca vurgulanmış girişler ve park yerleri gibi daha spesifik özellikler de içermektedir. Hizmet, kavşaklarda daha net rehberlik sağlayarak kullanıcıların yol işaretlerine ve yakındaki önemli noktalara göre bilinçli kararlar vermesine yardımcı olmaktadır. Bu iyileştirmeler, Naver Maps'i hem kullanıcılar hem de işletmeler için giderek daha değerli bir araç haline getirerek daha akıcı ve bilgilendirici bir navigasyon deneyimi sunmayı amaçlamaktadır. Geliştirilmiş görsel deneyime ek olarak Naver, gerçek zamanlı trafik sıkışıklığı verileri ve restoranlardan popüler menü önerileri gibi özellikler ekleyerek Street View 3D'nin işlevselliğini genişletmeyi planlamaktadır. Platform ayrıca, kullanıcıların yolları boyunca gerçek zamanlı hareketi simüle edebilecekleri etkileşimli rota oynatma gibi dinamik unsurları da entegre etmeyi amaçlamaktadır. Bu yaklaşım sadece kullanıcıların daha etkili bir şekilde gezinmesine yardımcı olmakla kalmamakta, aynı zamanda yerel işletmelerin kuponlar sunarak ve en popüler yemeklerini tanıtarak potansiyel müşterilerle etkileşim kurmaları için fırsatlar sunmaktadır. Naver Map başkanı Choi Seung-rak, bu hizmetin gelecekteki potansiyelini vurgulayarak, bu yeniliklerin kullanıcı deneyimini önemli ölçüde geliştireceğini ve kullanıcılara daha değerli, gerçek zamanlı bilgiler sağlayacağını belirtmiştir.[55]

55 https://www.koreatechtoday.com/naver-launches-3d-street-view-for-immersive-navigation-experience/

Yandex'ten Türk Kullanıcılar İçin Yapay Zeka Entegreli Arama Hizmeti

Yandex, Türk kullanıcılar için özel olarak geliştirdiği yapay zekâ (AI) entegreli arama hizmetini kullanıma sunmuştur. Yandex Arama ile "Yazeka" adı verilen hizmet, kullanıcı odaklı yaklaşımıyla karmaşık sorgulara hızlı ve net yanıtlar vermeyi amaçlamaktadır. Tüm online bilgi kaynaklarını alıntılarla destekleyerek en doğru cevapları sunmayı hedefleyen servisin, kullanıcıların arama alışkanlıklarını dönüştürmesi beklenmektedir.

Türkiye pazarı için özel olarak geliştirilen sistem, Android ve masaüstü platformlarında kullanılabilmektedir. Yakın zamanda iOS versiyonunun da kullanıma sunulması beklenmektedir. Yandex Arama ile Yazeka, birden fazla kaynaktan derlenmiş özet cevaplar sunarak geleneksel arama motorlarını yeniden tanımlamaktadır.

Tek bir kaynak tarafından yanıtlanamayan karmaşık sorguları ele alarak kullanıcılara zaman kazandıran hizmet, güvenilir alıntılar içererek kullanıcıların daha detaylı bilgiye ulaşmasını sağlamaktadır. Doğal dil işleme teknolojisi ile desteklenen hizmet, kullanıcıların sorgularını doğal bir şekilde ifade etmelerini sağlamaktadır. Yapay zeka bu sorguları analiz ederek daha net ve daha doğru sonuçlar sunmaktadır. Örneğin, kullanıcılar "Amsterdam'da bir günlük seyahat programı" gibi sorular sorabilmekte ve ayrıntılı bilgi alabilmektedirler.[56]

56 https://www.aa.com.tr/en/artificial-intelligence/yandex-launches-ai-integrated-search-service-yazeka-for-turkish-users/ 3427290

ABD'de TikTok'un Yasaklanma Riski

ABD'de TikTok'un yasaklanma ihtimali, platformu gelir kaynağı ve yaratıcı projeler için kullanan binlerce içerik üreticisini tedirginliğe sürüklemektedir. Başkan Joe Biden tarafından imzalanan iki ihtimalli yasa tasarısı, TikTok'un Çin merkezli ana şirketi ByteDance'in platformu bir Amerikan şirketine satmasını veya 19 Ocak'ta yürürlüğe girecek bir yasakla karşılaşmasını öngörmektedir. TikTok'un bu yasağa yönelik itirazı, 10 Ocak tarihinde Yüksek Mahkeme tarafından ele alınacaktır.

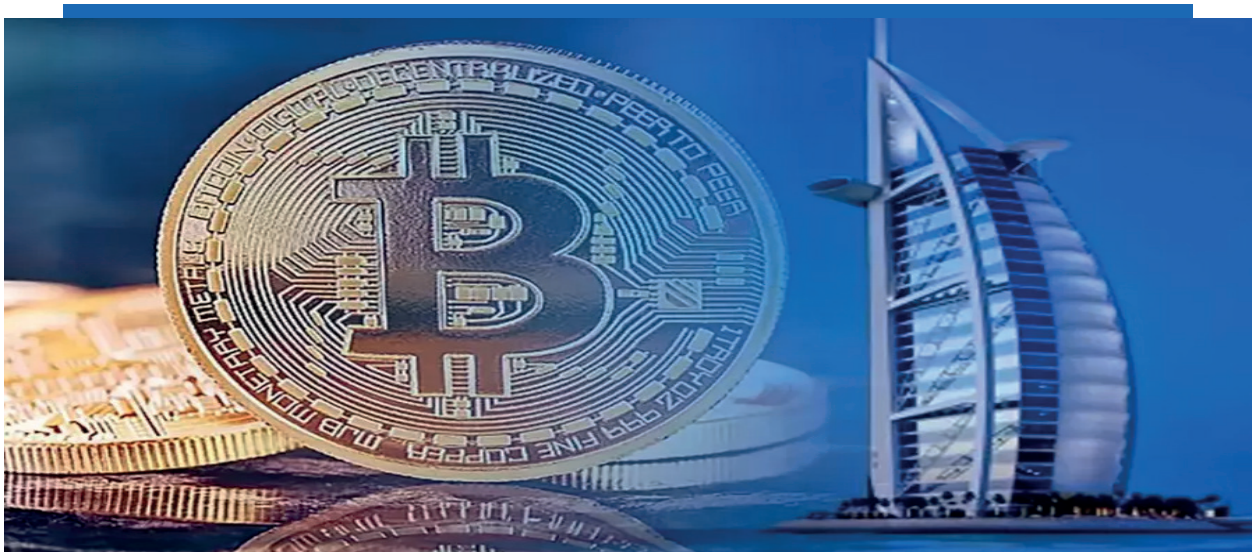
TikTok'u savunanlar, platformun ekonomideki yerinin altını çizerken, yasak yanlısı yasa koyucular, TikTok'un Çinli sahipliğinin ulusal güvenlik tehdidi oluşturduğunu savunmaktadır. Ancak platform, ABD'li küçük işletmelerin ve sosyal medya içerik üreticilerinin bir ay içinde 1,3 milyar dolarlık kazanç kaybedeceğini iddia etmektedir. Influencer Marketing Hub'ın yakın tarihli raporu, TikTok'un influencer pazarlama stratejilerinde en sık kullanılan platform olduğunu göstermektedir. Pazarlamacıların %50'si, TikTok'un kısa biçimli video içeriklerinin en iyi yatırım getirisi sağladığını düşünmektedir. Platformun oluşturduğu yaratıcı ekonomi, marka anlaşmaları, izleyici abonelikleri ve içerik üreticisi gelir modelleriyle bir dev haline gelmiştir. Goldman Sachs, yaratıcı ekonominin toplam pazar değerinin 2027'ye kadar 480 milyar dolara ulaşabileceğini öngörmektedir.

Pek çok içerik üreticisi, gelir kayıplarını telafi etmek ve kitlelerini yeniden oluşturmak için diğer platformlara yönelmeye başlamıştır. Pek çok kişi şimdiden Instagram, YouTube ve diğer platformlara yönelerek yeni takipçi kitleleri oluşturmaya başlamıştır. Yasağın, yalnızca TikTok'un değil, aynı zamanda sosyal medya platformlarının geleceği için de bir dönüm noktası olacağı değerlendirilmektedir.[57]

57 https://www.nbcnews.com/tech/tech-news/tiktok-ban-american-creators-prepare-rcna185158

BLOK ZİNCİRİ

BAE'de Kripto Para Transferleri Vergiden Muaf



Birleşik Arap Emirlikleri (BAE) Federal Vergi İdaresi, kripto ekosistemini heyecanlandıran bir karara imza atmıştır. Bundan sonra kripto para varlıklarının transferini katma değer vergisinden muaf tutmaya başlayacaktır. KDV muafiyeti, 1 Ocak 2018'e kadar olan işlemleri de geriye dönük olarak kapsayacaktır.

BAE, fintech ve Blockchain teknolojileri alanında lider olmayı amaçlamaktadır. Bu amaca hizmet eden düzenlemede kripto para varlıklar "dijital olarak alınıp satılabilen veya dönüştürülebilen ve yatırım amaçlı kullanılabilen bir değer temsili" olarak nitelendirilmiştir. Bu tanım sayesinde kripto varlıklar geleneksel finansal araçlardan ayrılmıştır. Bu karar genel olarak ülkenin Blockchain politikalarının en son adımı olarak değerlendirilmektedir. Dubai ve Abu Dhabi gibi önemli finans merkezlerine sahip olan Birleşik Arap Emirlikleri böylece küresel kripto şirketlerini ve yatırımcıları bölgeye çekmeyi amaçlamaktadır. Uzmanlara göre bu vergi avantajı sayesinde özellikle girişimciler ülkeye büyük ilgi gösterecektir. Küresel olarak Singapur, Malta ve İsviçre gibi ülkeler de kripto yatırımlarına merkez olmak için mücadele etmektedir. Birleşik Arap Emirlikleri'nin yeni kararları, kripto para girişimcilerine ve yatırımcılarına da yeni imkanlar sağlamaktadır. Körfez ülkesi daha önce "dijital ekonomi vizyonunu" duyurmuştu. Kripto para uzmanları şimdi bu kararın Bitcoin, Ethereum ve diğer büyük kripto para birimleri üzerindeki potansiyel etkilerini masaya yatırmış vaziyettedir.[58]

58 https://www.haberler.com/kripto-para/bae-kripto-para-transferlerini-vergiden-muaf-tuttu-17899258-haberi/

İngiltere'de Kripto Para Sektörüne Yönelik Düzenleme

İngiliz finansal hizmetler düzenleyicisi Finansal Yönetim Kurumu (FCA), 2026 yılına kadar kripto para sektörü için kapsamlı bir düzenleme uygulamaya koyma planını duyurmuştur. Ayrıca, bankacılık ve yatırım ürünlerini denetleyen Finansal Yönetim Kurumu (FCA) kripto paralara yönelik oluşturduğu yol haritasındaki önemli tarihleri ve kilometre taşlarını ayrıntılarıyla belirten bir zaman çizelgesi de açıklamıştır.

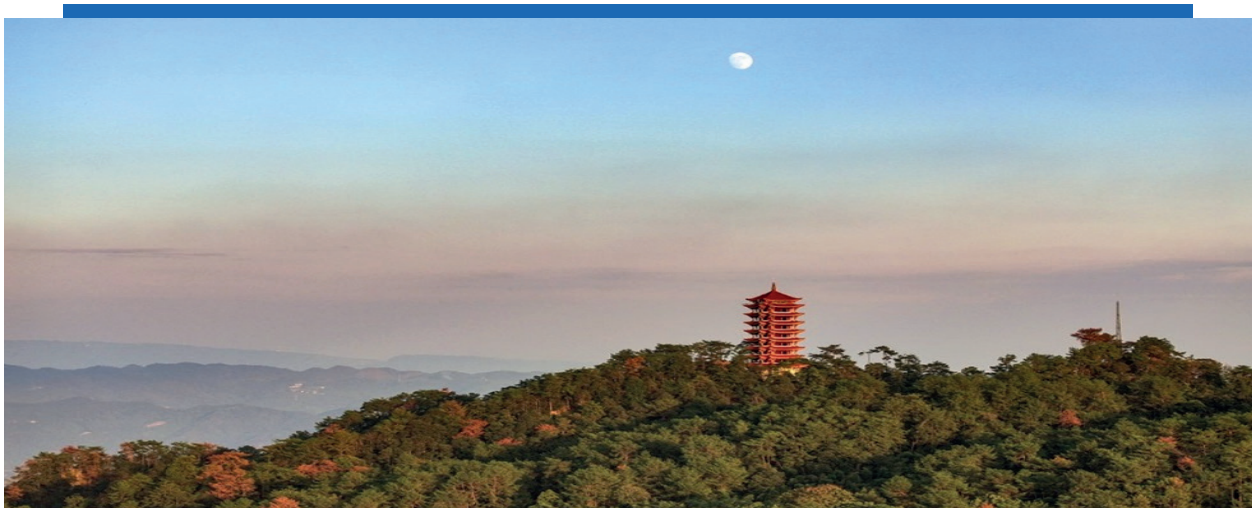
2024 yılının dördüncü çeyreğinde düzenleyici kurum, Stablecoin'lerin ihracı ve saklanmasıyla ilgili kuralların yanı sıra kabul ve açıklama süreçleri ile piyasa suistimaliyle nasıl mücadele edileceği konusunda da belgeler yayımlayacağını ifade etmiştir. Ayrıca FCA, 2025 yılının ilk yarısında ticaret platformları, aracılık, borç verme ve ihtiyati kripto maruziyeti hakkında belgeler yayımlamayı planladığını belirtmiştir. Bununla birlikte Kurum, 2025 yılında nihai politika açıklamalarının yayımlanmasının ardından 2026 yılına kadar kripto varlıkları yöneten tam bir düzenlemenin İngiltere'de hayata geçeceğini açıklamıştır.

FCA'nın yaptığı araştırmaya göre İngiltere'de kripto para kullanımının arttığı ve kişilerin elindeki kripto paraların ortalama değerinin, geçen yıla kıyasla 1.595 sterlinden 1.842 sterline yükseldiği ifade edilmiştir. Bu durumun İngiltere'de güvenli, rekabetçi ve sürdürülebilir bir kripto sektörünü destekleyen net düzenlemelere olan ihtiyacı vurguladığı da belirtilmiştir.[59]

59 https://www.cnbc.com/2024/11/26/britains-fca-sets-out-plan-to-implement-crypto-regime-by-2026.html

UZAY

Çin'den Bitki Haşereleri ve Hastalıkları İçin Gökyüzü-Yer Akıllı İzleme Sistemi



Çin Bilimler Akademisi'ne bağlı Havacılık ve Uzay Bilgi Araştırma Enstitüsü'ne göre Çin, bitki haşereleri ve hastalıkları için gökyüzünde akıllı bir izleme ve erken uyarı sistemi geliştirmiştir. Araştırma ekibi, çok ölçekli bir izleme ve uyarı sistemi kurmak için kendi geliştirdiği çip düzeyinde akıllı haşere ve hastalık tespit cihazlarını ve alçak irtifa haşere denetimleri için özel drone uzaktan algılama çözümlerini kullanmıştır. Geliştiricilerden biri olan Havacılık ve Uzay Bilgi Araştırma Enstitüsü'ne göre "Akıllı Göz" sistemi, haşerelerin ve hastalıkların yere yakın düzeyde hızlı ve hassas bir şekilde tespit edilmesini sağlamakta, arsa düzeyinde dinamik izlemeyi ve verimli yönetimi kolaylaştırmakta ve bölgesel düzeyde 20'den fazla önemli zararlı ve hastalık için çok ölçekli dinamik izleme ve uyarı imkanı sunmaktadır.

Enstitüde araştırmacı olan Huang Wenjiang, sistemin, geleneksel bitki koruma izleme tekniklerinin saha araştırmaları ve tanımlamadaki zorluklar, düşük irtifa izlemede düşük doğruluk ve zayıf bölgesel erken uyarı yetenekleri gibi zorluklarını etkili bir şekilde ele alabileceğini açıklamıştır. Yapay zeka teknolojisi, havacılık ve uzay bilgileri ile bitki koruma teorisini bir araya getiren sistem, geçtiğimiz günlerde Doğu Çin'in Zhejiang eyaletinin Hangzhou kentinde düzenlenen bitki haşereleri ve hastalıklarının uzaktan algılanması konulu 5. konferansında tanıtılmıştır.[60]

60 https://www.chinadaily.com.cn/a/202410/21/WS6715ff59a310f1265a1c8b96.html

Çin'den Gelecekte Ay Üssü İnşa Etmek İçin Ay Tuğlaları Üretimi

Çinli araştırmacılar, gelecekte bir Ay üssü inşa etmek için kullanılabileceği umuduyla, Ay toprağına benzer bir bileşime sahip bir malzemeden tuğlalar geliştirmiştir. Huazhong Bilim ve Teknoloji Üniversitesi (HUST) tarafından Xinhua'ya sağlanan yeni bir video klibe göre, Ding Lieyun liderliğindeki bir araştırma ekibi, standart kırmızı tuğla veya beton tuğlalardan üç kat daha güçlü olan "ay tuğlaları" yapmak için bir ay toprağı simülatörü kullanmıştır. Ekip ayrıca eklemeli üretim teknolojisini kullanarak başka bir inşaat seçeneği geliştirmiştir. Araştırmacılar, ay toprağı kullanarak ev basmak için bir 3D baskı robotu da icat etmiştir.

HUST'tan Zhou Cheng'e göre, ekip beş farklı simüle edilmiş ay toprağı bileşimi ve üç farklı sinterleme süreci kullanmıştır; bu da gelecekteki ay üssü inşaatı için malzeme seçimi ve süreç optimizasyonunda daha doğru bilimsel veriler sağlayabilecektir. Ay toprağının bileşiminin Ay'ın farklı yerlerinde değişiklik gösterdiğini belirten Zhou, Chang'e 5'in iniş alanındaki Ay toprağını simüle eden ve esas olarak bazalt olan bir bileşim olduğunu kaydetmiştir. Diğer bazı bileşimler ise başka yerlerde bulunan ve çoğunlukla anortozit olan toprağı simüle etmektedir. Zhou, tuğlaların Ay ortamında mekanik performanslarının düşüp düşmeyeceğini ve yüksek sıklıktaki Ay depremlerine dayanıp dayanamayacaklarını belirlemek için performans testlerinden geçmeleri gerektiğini açıklamıştır. Ay, önemli ölçüde kozmik radyasyon içeren vakumlu bir ortama sahiptir ve sıcaklıklar gün boyunca 180 santigrat dereceyi aşmakta, geceleri ise eksi 190 santigrat dereceye düşmektedir. Zhou, ekibin tuğlaların ne kadar iyi yalıtım sağlayabileceğini ve radyasyona dayanıp dayanamayacağını belirlemesi gerektiğini söylemiştir.

Çin Merkez Televizyonu'na göre, Ay tuğlaları mekanik ve termal performanslarının yanı sıra kozmik radyasyona dayanma kabiliyetlerini doğrulamak için Tianzhou-8 kargo uzay aracıyla Çin'in uzay istasyonuna gönderilecektir. İlk Ay tuğlasının 2025 yılı sonuna kadar Dünya'ya dönmesi beklenmektedir.

Çin, 15 Ekim günü uzay bilimi için orta ve uzun vadeli ulusal kalkınma programını açıklayarak 2050 yılına kadar Çin'de uzay biliminin gelişimi için bir yol haritası belirlemiştir. Çin tarafından başlatılan uluslararası Ay araştırma istasyonu, programın 2028-2035 yılları arasındaki ikinci aşamasında inşa edilecektir.[61]

61 https://www.chinadaily.com.cn/a/202410/20/WS6714d958a310f1265a1c88aa.html

Suudi Uzay Ajansı'ndan 'Uzay Gelecekleri Merkezi' Açılışı

Suudi Uzay Ajansı (SSA), Dünya Ekonomik Forumu'na bağlı Dördüncü Sanayi Devrimi Merkezleri ağının ilk örneği olan Uzay Gelecekleri Merkezi'nin açılışını duyurmuştur. Bu girişim, Suudi Arabistan'ın küresel uzay sektöründeki liderliğini güçlendirme ve bu hayati alanda ekonomik kalkınma, araştırma ve inovasyonda büyümeyi teşvik etme yönünde devam eden çabalarının bir parçasıdır.

Suudi Uzay Ajansı CEO'su ve Uzay Gelecekleri Merkezi Başkanı Dr. Muhammed bin Saud Al Tamimi, merkezin küresel uzay sektörüne önemli bir katkı sağladığını, Suudi Arabistan'ın sürdürülebilir bir uzay ekonomisi inşa etme, bilgiyi ilerletme ve uluslararası ortaklıkları teşvik etme konusundaki kararlılığını vurgulamıştır.

Merkezin Genel Müdürü Mishaal Ashemimry, lansmanın önemini ve sürdürülebilir bir uzay geleceğine ulaşmak için ortak zorlukların ele alınmasında uluslararası iş birliğinin değerini vurgulamış ve merkezin teknik ve düzenleyici zorluklara çözümler sunarak Suudi Arabistan'ın küresel uzay sektöründeki liderliğini güçlendireceğini sözlerine eklemiştir.

Uzay Gelecekleri Merkezi, uzay sektörünün ekonomik ve çevresel değerini en üst düzeye çıkarmak, güçlü düzenleyici politikalar geliştirmek ve teknolojik yeniliği teşvik etmek için küresel bir platform kurmayı hedeflemektedir. Ayrıca, Suudi Arabistan'a Dördüncü Sanayi Devrimi topluluğuna erişim imkânı sağlamakta ve uzay sektöründeki iddialı hedeflerine ulaşmak için küresel ortaklarla yakın iş birliğini teşvik ederek Krallığın gelecek vizyonunu güçlendirmektedir.[62]

62 https://www.gulf-insider.com/saudi-launches-centre-for-space-futures/

Güneş Sistemimizin Yörüngeleri

Gezegenlerin Güneş etrafındaki yörüngeleri birçok bilimsel tartışmanın kaynağı olmuştur. Mevcut yörünge özellikleri iyi anlaşılmış olmakla birlikte, gezegen yörüngeleri Güneş Sistemi'nin oluşumundan bu yana evrim geçirmiş ve değişmiştir. Gezegensel göçler, gezegensel etkileşimlerin genç gezegenlerin orijinal konumlarından içe veya dışa doğru göç etmelerine neden olduğunu öne süren son on yılların en önde gelen fikri olmuştur. Şimdi yeni bir teori, Güneş Sistemi'nden geçen 2-50 Jüpiter kütleli bir nesnenin buna neden olabileceğini öne sürmektedir.

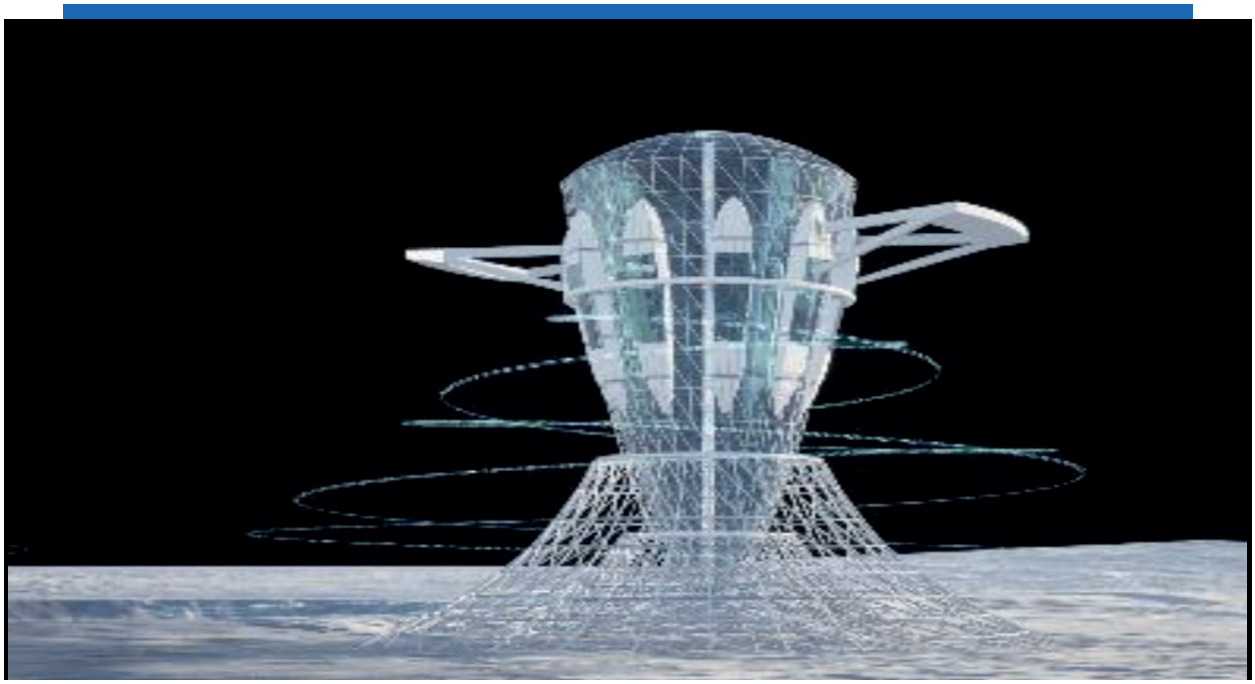
Gezegenlerin yörüngelerinin evrimi karmaşık bir süreçtir. Başlangıçta gezegenler genç ve sıcak Güneş'in etrafında dönen bir gaz ve toz diskinden oluşmuştur. Açısal momentumun korunumu olgusu, malzemenin dairesel ve aynı düzlemde olan yörüngelere yol açan bir düzlem oluşturmasına neden olmuştur.

Gezegenler büyüdükçe, protogezegensel disk içindeki etkileşimler, gezegenlerin içe ya da dışa doğru hareket ettiği yörünge göçlerine yol açmıştır. Eksantriklik ve eğimde önemli değişikliklere yol açan ve bazen protogezegenlerin Güneş Sistemi dışına fırlatılmasına neden olan yerçekimsel etkileşimler de olmuştur. Güneş'ten gelen gelgit kuvvetleri de yörüngeleri değiştirmiş olabilir. Güneş Sistemi oluşurken protoplanet fırlatmalarının oldukça yaygın olduğu düşünülse de, zaman zaman gök cisimleri bizi ziyaret etmiştir. Bu cisimlerin nadir olduğu ve uzak gezegen sistemleri hakkında değerli bir fikir verdiği görülmektedir. Oumuamua, 2017 yılında keşfedilmiş ve onaylanmış ilk yıldızlararası ziyaretçi olmuştur. Muhtemelen gaz çıkışı veya diğer yerçekimsel olmayan güçlerin neden olduğu uzun bir şekil ve olağandışı bir ivme sergilemiştir.

Yakın zamanda yayınlanan bir makale, böyle bir yıldızlararası ziyaretçinin gezegensel kuzenlerimizin yörüngelerindeki değişiklikleri yönlendirmiş olabileceğini öne sürmektedir. Makale Toronto Üniversitesi'nden Garett Brown liderliğindeki bir bilim ekibi tarafından kaleme alınmıştır. Gaz devlerinin eksantrikliğinin doğasını araştıran ekip, mevcut teorilerin gözlemleri açıklamasının pek mümkün olmadığını öne sürmektedir. Bunun yerine, Jüpiter'in 2 ila 50 katı kütleye sahip bir nesnenin Güneş Sistemi'nden geçmesinin daha olası bir neden olduğunu göstermektedirler. Makalede, perihelion mesafesi (Güneş'e en yakın mesafe) 20 astronomik birimden az ve hiperbolik aşırı hızı 6 km/s-1'den az olan bir nesnenin geçmesinin gözlemleri açıklayabileceği belirtilmektedir. Hesaplamalar, yıldızlararası bir ziyaretçinin bugün gördüğümüz yörüngeleri üretme ihtimalinin 100'de 1 olduğunu gösteriyor ki bu diğer teorilerden çok daha iyi bir ihtimaldir. Ziyaretçinin özellikleri için simülasyonlar ve yaklaşık değerler kullanan ekip, teorinin bugüne kadarki en makul teori olduğu sonucuna varmıştır.[63]

63 https://www.sciencealert.com/our-solar-systems-orbits-may-have-been-arranged-by-an-invading-planet

Japonya'dan Ay'da Yaşamı Gerçeğe Dönüştürmek İçin Araştırma



Bir Japon üniversitesi ve inşaat şirketi, insanların Ay'da Dünya'dakine benzer koşullar altında yaşamasını sağlayacak, yapay yerçekimi üretebilen bir Ay habitatı geliştirmek üzere araştırma ortaklığı kurmuştur. Kyoto Üniversitesi ve Kajima Corp, dönme yoluyla yerçekimi üreten paraboloid bir yapı olan "Neo Lunar Glass 'ın yer tabanlı bir prototipini 2030'lara kadar inşa etmeyi hedeflemektedir. Teknolojinin, mikro yerçekimine uzun süre maruz kalmanın insan vücudu üzerindeki kemik ve kas kaybı gibi olumsuz etkilerine ilişkin endişeleri gidermesi beklenmektedir.

Kyoto Üniversitesi'nde insan hayatta kalabilirliği konusunda ileri entegre çalışmalar profesörü olan ekip üyesi Yosuke Yamashiki, bu projenin önemli bir teknolojik sıçrama gerektirdiğini, ancak kendilerinin bunu başarmayı ve uzay kolonilerinin önünü açmayı hedeflediklerini açıklamıştır.

Lunar Glass yapısı yaklaşık 200 metre çapında ve 400 metre yüksekliğinde olacak ve 10.000 kişiyi barındırabilecektir2024 yılı içerisinde başlayan proje kapsamında öncelikle modeller ve bilgisayar simülasyonları aracılığıyla zorluklar tespit edilecektir. Kyoto Üniversitesi ve Kajima Aralık ayının başlarında tam teşekküllü ortak araştırmanın başladığını duyurduğunda 1:2000 ölçekli bir model tanıtılmıştır. Ayrıca nesnelerin yapay yerçekimi altındaki davranışlarını gösteren simülasyonlar da gerçekleştirilmiştir.[64]

64 https://japantoday.com/category/tech/japanese-team-launches-research-to-make-living-on-moon-reality

SAVUNMA SANAYİ

BAE'den, 5G Destekli İHA'lar

e&UAE, BAE Siber Güvenlik Konseyi (CSC) ile stratejik bir ortaklık kurarak BAE Drone'larını GITEX Global 2024'te tanıtacağını duyurmuştur. Çığır açan bu girişim, ülkenin İnsansız Trafik Yönetimi (UTM) alanında devrim yaratmaya hazırlanmaktadır. Bu son teknoloji dronlar, e&BAE'nin ultra hızlı, düşük gecikmeli 5G bağlantısından yararlanarak gerçek zamanlı tehdit algılama, önleme ve müdahale yetenekleri sağlayacak ve BAE'nin CSC sistemlerini önemli ölçüde güçlendirecektir.

CSC liderliğindeki girişim, operatörler ve devlet kurumları da dahil olmak üzere çok sayıda paydaş arasındaki süreçleri tek ve uyumlu bir platformda birleştirmeyi amaçlamaktadır. Bu uçtan uca çözüm, bulut hizmetlerini, platformları ve izleyicileri içermekte, düzenleyici ve güvenlik gereksinimlerine tam uyum sağlamakta ve dünya çapında kamu hizmetlerinin yönetimi için yeni bir ölçüt oluşturmaktadır. Bu proje, çeşitli devlet daireleri, operatörler ve diğer paydaşlar arasındaki karmaşık etkileşimleri tek ve birleşik bir platformda birleştirme hedefiyle küresel bir öncüdür.

Mevzuat ve güvenlik standartlarına sağlam bir şekilde uyulmasını sağlamak için e&UAE, bu çözümlerin belirlenen yönergelere göre doğrulanmasına yardımcı olacak ve tüm işlemlerin gerekli yasal ve güvenlik gerekliliklerine uygun olarak yürütülmesini sağlayacaktır.[65]

65 https://www.thefastmode.com/technology-solutions/37794-e-uae-cyber-security-council-launch-5g-powered-drones

Aselsan'ın Geliştirdiği "Dron Avcıları" Saha Expo'da

ASELSAN, milli imkanlarla geliştirdiği yeni nesil dron avcısı sistemlerinin tanıtımını ilk kez SAHA EXPO Uluslararası Savunma, Havacılık ve Uzay Sanayi Fuarı'nda gerçekleştirmiştir. Türkiye'nin ve Avrupa'nın en büyük sanayi kümelenmesi SAHA İstanbul tarafından Cumhurbaşkanlığı himayesinde organize edilen, 6 bakanlık ve Cumhurbaşkanlığı Savunma Sanayii Başkanlığının desteklediği, Anadolu Ajansının global iletişim ortağı olduğu SAHA EXPO Uluslararası Savunma, Havacılık ve Uzay Sanayii Fuarı İstanbul'da yapılmıştır.

*Şirketten yapılan açıklamaya göre, değişen askeri şartlara karşı harp sahasında sıkça kullanılan dron tehdidine karşı geliştirilen ASELSAN sistemleri, Mehmetçik'in gücüne güç katacak*tır. Dünyada giderek büyüyen bir sorun olan mini ve mikro dron tehdidine karşı geliştirilen ASELSAN çözümlerinin uluslararası arenada da büyük ilgi görmesi beklenmektedir. ASELSAN'ın İstanbul'da SAHA EXPO'da tanıttığı anti dron sistemleri arasında "KORKUT 25mm Yakın Hava Savunma Sistemi", "BUKALEMUN GNSS Aldatma Sistemi", "KANGAL FPV Anti-Drone Sistemi" ve "SEDA 100-Cuav Akustik Drone Tespit Sistemi" bulunmaktadır.

KORKUT 25, öncelikle zırhlı kara hedeflerine karşı geliştirilmiştir. Taktik araçlara entegrasyon için uyum sağlayan KORKUT 25, 4x4, 6x6 ve 8x8 tekerlekli veya paletli araçlara monte edilebilmekte ve kırsal ortamlardaki mini ve mikro insansız hava aracı (İHA) tehditlerini de etkisiz hale getirmektedir. Sistem, ASELSAN tarafından geliştirilen 25 milimetre parçacıklı mühimmatla harici sensörlerden bilgi alarak İHA tehditlerine karşı işlevsel ve fiziksel imha kabiliyetini yerine getirmektedir. Jiroskopla stabilize edilmiş yapısı, uzaktan komuta özelliği, yüksek çözünürlüklü kızılötesi kameraları, lazer mesafe bulucu, otomatik hedef tespit ve

takip fonksiyonu, yüksek atış hassasiyetine sahip gelişmiş otomatik balistik hesaplamasıyla KORKUT 25, tüm savaş şartlarına uygun tasarlanmıştır. Kapsamlı gözetleme, harici sensörlerle entegrasyon ve uzaktan kontrol yetenekleri sayesinde KORKUT 25, nişancının durumsal farkındalığını artırmakta ve İHA tehditlerinden kaynaklanan zafiyet saldırılarını da büyük ölçüde azaltmaktadır. KORKUT 25, hareket halindeyken mini ve mikro İHA tehditlerini tespit etme yeteneğine sahiptir.

BUKALEMUN sistemi de dron tehditlerine karşı, güvenlik güçlerinin taktik sahadaki gözü kulağı olacaktır. GNSS bantlarında aldatma yeteneğine sahip BUKALEMUN ile multi-GNSS bantlarında aldatma işlemi gerçekleştirilebilmektedir. Bu sınıfta bilinen ilk sistem olan BUKALEMUN ile statik ve dinamik senaryolar dahilinde görece uzun mesafelerden aldatma işlevi başarıyla gerçekleştirilebilmektedir.

ASELSAN'ın oyun değiştirici teknolojisiyle geliştirilen KANGAL FPV de askeri tesislerin, üslerin, devlet kurumlarının, konutlarının, tören alanlarının ve kontrol noktalarının mini İHA'lara karşı korunmasını sağlamaktadır. KANGAL, güvenlik güçlerinin araçlarına entegre edilerek, araçları olası risklere karşı korumaktadır.

Mini ve mikro İHA tehditlerini şehir ve kırsal ortamda etkisiz hale getirmek için geliştirilen İHTAR Sistemi, kritik tesislerin ve üs bölgelerinin korunması, sınır güvenliği, kamu güvenliği ve kalabalık organizasyonların korunmasında kullanılmaktadır. Üzerinde elektro-optik ve radar gibi çeşitli sensörlerin entegre çalıştığı İHTAR Sistemi'ne, SEDA 100-cUAV Sistemi de entegre edilerek mini/mikro İHA'ların tespiti için ilave yetenek kazandırılmıştır. SEDA 100-cUAV Sistemi, mikrofonlarla dinleme yaparak ortamda yer alan FPV dronlar dahil olmak üzere sabit ve döner kanatlı İHA tehditlerini farklı menzillerde tespit edebilmektedir. Sistem, muadillerine göre daha uzun menzillerde İHA tespiti yapabilmektedir.[66]

66 https://www.aa.com.tr/tr/ekonomi/aselsan-gelistirdigi-dron-avcilarini-saha-expoda-tanitti/3371271

Roketsan'dan Saha Expo'da 3 Yeni Ürün

Roketsan, SAHA EXPO'da bu yıl maliyet etkin yeni ürünleri olan PUSU, L-OMTAS ve LG-155'i tanıtmıştır. Roketsan Genel Müdürü Murat İkinci, SAHA EXPO'nun uluslararası katılımcılarıyla beraber Türk savunma sanayisini bir araya getiren en önemli etkinliklerden bir tanesi olduğunu söylemiştir. SAHA EXPO'da Roketsan olarak, ürünlerini ulusal ve uluslararası kullanıcılarla bir araya getirme fırsatı yakaladıklarına değinen İkinci şunları ilave etmiştir: "Bu sene SAHA EXPO'ya özellikle uluslararası katılımın çok yoğun olduğunu görüyoruz. Birçok delegasyon bizim standımızı ve diğer savunma sanayisi şirketlerini ziyaret ediyorlar. Bunların da çok güzel iş birliklerine vesile olacağını değerlendiriyorum."

İkinci, SAHA EXPO'da bu yıl 3 yeni ürünün tanıtımını gerçekleştirdiklerini belirterek, «PUSU, kamyon üstü güdümlü mühimmat atan sistemimiz. PUSU aslında asimetrik savaş ortamında özellikle hareketli alandaki kuvvetlerimiz için güdümlü mühimmat fırlatan bir platform olarak maliyet etkin bir çözüm oluşturuyor. Türk Silahlı Kuvvetlerinin de şu anda envanterinde olan ürünlerden bir tanesi. İkinci ürünümüz ise Roketsan'ın en önemli ürünleri arasında yer alan tanksavar ailesinin yeni bir üyesi olan, lazer güdümlü tanksavar füzemiz L-OMTAS. Orta menzilli tanksavar füzelerimizin lazer güdümlü olan versiyonu. L-OMTAS da hem maliyet etkin hem de 5,5 kilometreye kadar etkin vuruş kabiliyeti sunuyor." diye konuşmuştur.

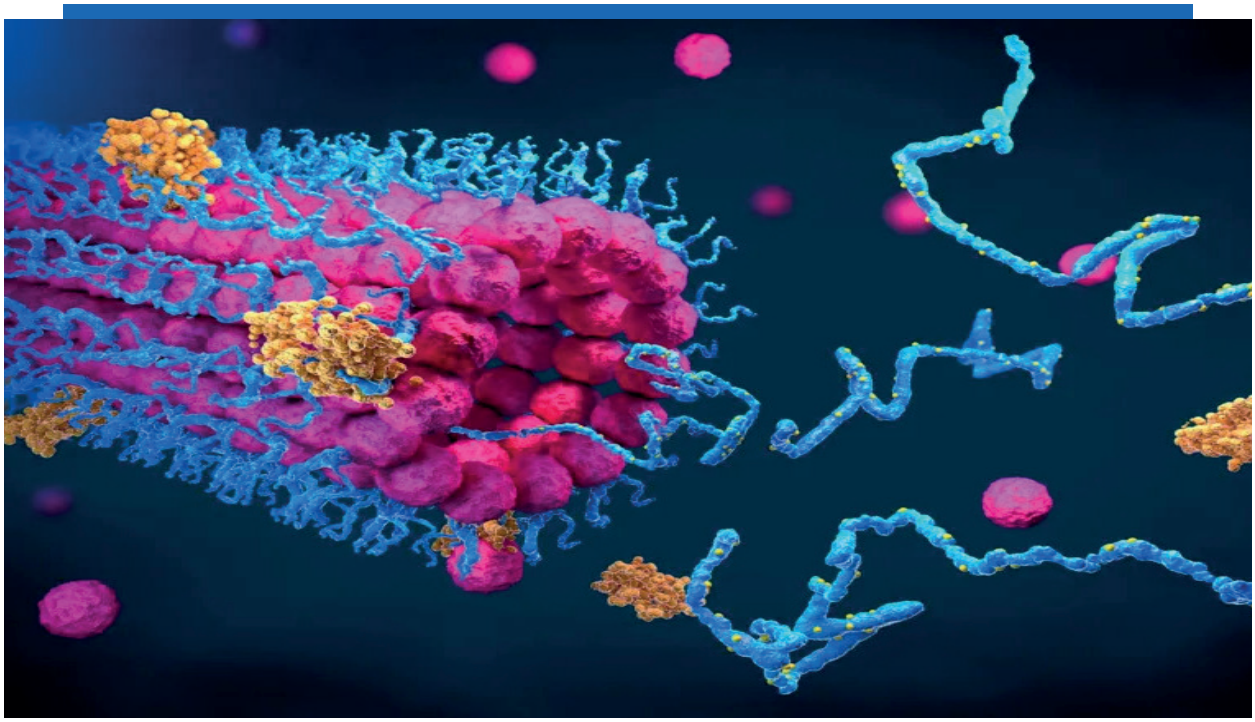
Lazer güdümlü 155'lik mühimmatlarını da fuarda görücüye çıkardıklarını belirten İkinci, "Bu ürünü, özellikle topçu birliklerinin 155'lik mühimmatlarının güdümsüz olanlarının yerine sahada maliyet etkin bir şekilde nokta hedef vurma kabiliyetini kazandıracak bir ürün olarak envanterimize kazandıracağız." yorumunu yapmıştır.

*İkinci, özellikle uluslararası alanda maliyet etkin ürünlerin pazar payının hızla arttığını gözlemlediklerini belirterek, maliyet etkin ürünlerin firmaların başarılarını direkt etkilediğini vurgula*mıştır.[67]

67 https://www.aa.com.tr/tr/gundem/roketsan-saha-expoda-3-yeni-urununu-tanitti/3370683

BİLİŞİM DÜNYASINDAN

Google DeepMind Patronuna Protein Buluşuyla Nobel Ödülü



İngiliz bilgisayar bilimcisi Profesör Demis Hassabis, yaşamın yapı taşları olan proteinler üzerine yaptığı "devrim niteliğindeki" çalışmalarıyla Nobel Kimya Ödülü'nü paylaşmaya hak kazanmıştır. 48 yaşındaki Profesör Hassabis, Google DeepMind'a dönüşen yapay zeka şirketinin kurucularındandır. Profesör Hassabis ile birlikte bu buluş üzerinde çalışan 39 yaşındaki Profesör John Jumper, ödülü 60 yaşındaki ABD'li Profesör David Baker ile paylaşmaktadır.

Proteinler yaşamın yapı taşlarıdır ve insan vücudundaki her hücrede bulunmaktadır. Proteinlerin daha iyi anlaşılması tıp alanında büyük atılımlara yol açmıştır. Antibiyotik direncini çözmede ve plastikleri ayrıştırabilen enzimleri görüntülemede kullanılmaktadır.

Prof. Hassabis ve Prof. Jumper, bilinen neredeyse tüm proteinlerin yapılarını tahmin etmek için yapay zeka kullanmış ve AlphaFold2 adlı bir araç geliştirmişlerdir. Proteinler, her biri benzersiz bir şekilde katlanan amino asit adı verilen yapı taşı zincirlerinden oluşmaktadır. Bilim insanları uzun süredir milyonlarca proteinin her birinin şeklini tahmin etmekte zorlanmaktaydı, ancak bu yapı insan vücudunda ne yaptığını yönlendirmektedir. Yapıyı anlamak, proteini nasıl hedefleyeceğimizi ve davranışını nasıl değiştireceğimizi bilmek için çok önemlidir, ki bu da tıpta çok önemlidir.

Nobel komitesi AlphaFold2'yi "tam bir devrim" olarak nitelendirmiş ve bu araç şu anda dünya çapında 200 milyon protein için kullanılmaktadır. İkili bu problem üzerinde çalışmaya

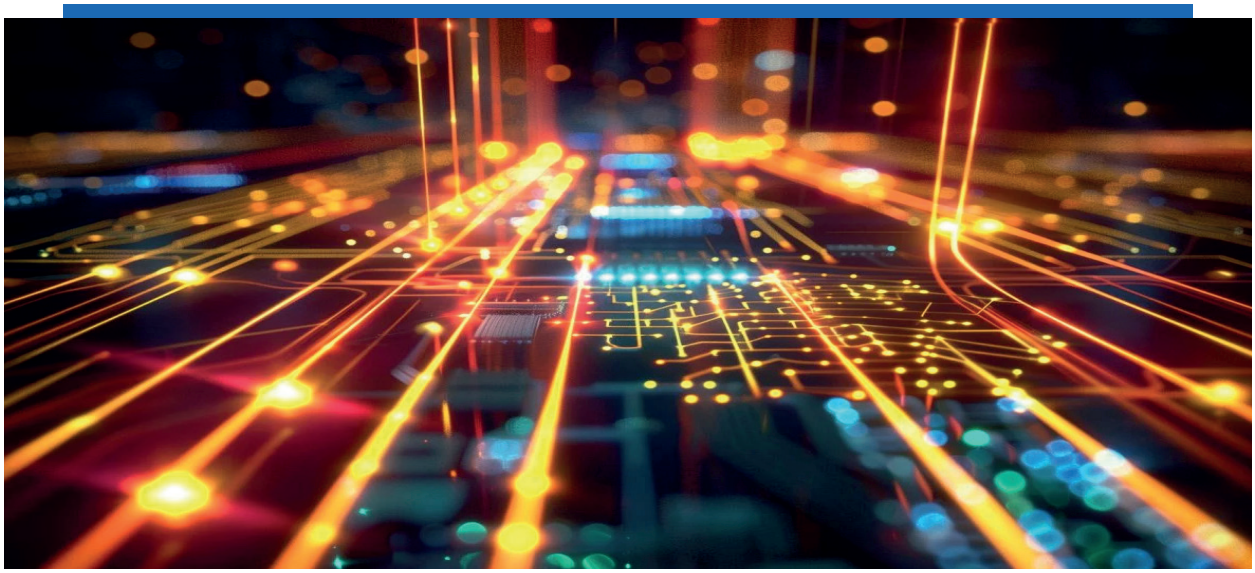
başlamadan önce, protein yapılarının sadece küçük bir kısmı çözülmüştür. İkili Nobel ödülünün yarısını almıştır. Diğer yarısı ise, komitenin "neredeyse imkânsız başarı" olarak nitelendirdiği yeni proteinlerin inşası için Prof. Baker'a verilmiştir.

2003 yılında Prof. Baker yeni bir protein tasarlamak için amino asitleri kullanarak ilaçlarda, aşılarda ve diğer araçlarda kullanılan yeni proteinlerin üretilmesine kapı aralamıştır. Kendisi de 1990'larda Rosette programını tasarlayarak protein yapılarını tahmin etmede bilgisayar yazılımlarını kullanmıştır. Seattle'daki Washington Üniversitesi'nde çalışan Prof. Baker, açıklamadan kısa bir süre sonra komiteye "çok heyecanlı ve çok onurlu" olduğunu söylemiştir.

Duyuru İsveç Kraliyet Bilimler Akademisi tarafından İsveç'in başkenti Stockholm'de düzenlenen bir basın toplantısıyla yapılmıştır. Kazananlar 11 milyon İsveç kronu (810,000 £) değerindeki ödül fonunu paylaşacaklardır. Prof. Baker ödülün yarısını alırken, kalan yarısı Prof. Hassabis ve Prof. Jumper'a verilecektir.[68]

68 https://www.bbc.com/news/articles/czrm0p2mxvyo

Foton Destekli Atılım: Gelecek için Hızlı, Güvenli ve Sürdürülebilir Telekom



ABD'de yeni bir çalışma, enerji tasarruflu bilgi işleme ve kapsamlı veri güvenliği sağlayabilecek teknolojileri ortaya çıkarmaktadır. Maryland Üniversitesi'nin yenilikçi araştırması, telekomünikasyon verilerini ışık kullanarak işleyen, enerji verimliliği sağlayan ve kuantum iletişim yoluyla bilgisayar korsanlığına karşı güvenliği güçlendiren bir cihaz sunmaktadır. Maryland Üniversitesi'ndeki (UMD) araştırmacılar tarafından yürütülen bu çalışmaya göre, gelişmiş bilgi işleme teknolojileri milyonlarca kişi için daha çevreci telekomünikasyon ve gelişmiş veri güvenliği sağlamaktadır. Minimum ışıkla bilgi işleme kapasitesine sahip yeni bir cihaz, enerji tasarruflu ve güvenli iletişimde devrim yapabilecektir. UMD Malzeme Bilimi ve Mühendisliği (MSE) Bölümü'nde yardımcı doçent olan You Zhou'nun ABD Enerji Bakanlığı (DOE) Brookhaven Ulusal Laboratuvarı'ndaki araştırmacılarla işbirliği içinde yürüttüğü bu proje, kısa süre önce Nature Photonics dergisinde vurgulanmıştır.

Telefon sinyalleri aracılığıyla bilgi göndermekten sorumlu cihazlar olan optik anahtarlar, iletim ortamı olarak ışığa ve işleme aracı olarak elektriğe dayanmakta ve verileri yorumlamak için ekstra bir enerji seti gerektirmektedir. Zhou tarafından tasarlanan yeni bir alternatif, telekomünikasyon ve hesaplama platformları için hız ve enerji verimliliğini artırabilecek tam bir iletime güç sağlamak için yalnızca ışık kullanmaktadır.

Bu teknolojinin ilk testleri önemli enerji iyileştirmeleri göstermiştir. Geleneksel optik anahtarlar bir iletişim iletimini sağlamak için 10 ila 100 femtojoule gerektirirken, Zhou'nun cihazı sadece onda bir ila bir femtojoule olan yüz kat daha az enerji tüketmektedir. Malzemenin "doğrusal olmayan tepki" olarak bilinen özelliği sayesinde az miktarda ışık kullanarak bilgi işlemeyi mümkün kılan bir prototip oluşturmak, araştırma grubunda yeni fırsatların önünü açmıştır. Zhou, "Güçlü doğrusal olmama özelliğini elde etmek beklenmedik bir şeydi ve bu da daha önce keşfetmediğimiz yeni bir yönü açtı: kuantum iletişimi" şeklinde konuşmuştur.

Cihazı oluşturmak için Zhou, Brookhaven Laboratuvarı'nda açık araştırma yapan bilim insanlarına birinci sınıf ekipmanlara ücretsiz erişim sunan bir DOE Bilim Ofisi kullanıcı tesisi olan Fonksiyonel Nanomalzemeler Merkezi'ndeki (CFN) Kuantum Malzeme Presi'ni (QPress) kullanmıştır. QPress, tek bir atom kadar ince katmanlara sahip kuantum malzemelerin sentezlenmesi için otomatik bir araçtır.

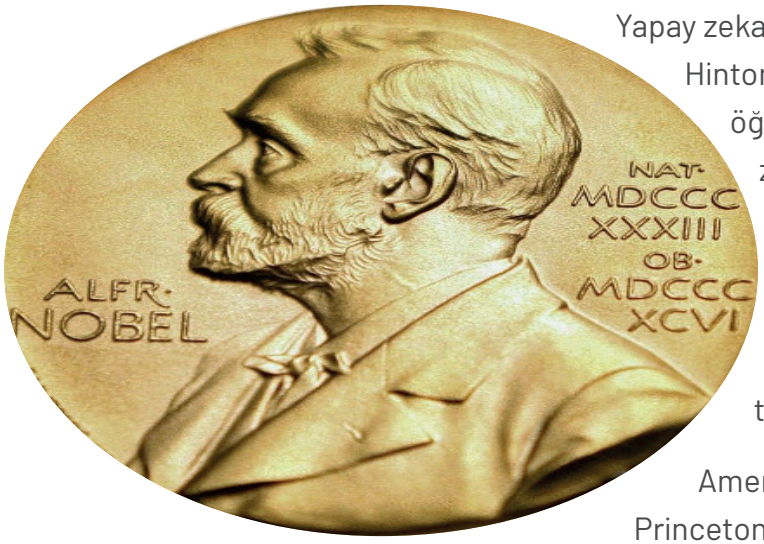
CFN Elektronik Nanomalzemeler Grubu'nda çalışan bir bilim insanı olan ortak yazar Suji Park "Zhou'nun grubuyla birkaç yıldır işbirliği yapıyoruz. Eksfoliyatör, kataloglayıcı ve istifleyici içeren QPress modüllerimizi en erken benimseyenlerden biri onlar. Özellikle, taleplerine göre uyarlanmış yüksek kaliteli eksfolye pullar sağladık ve malzemeleri için eksfoliyasyon koşullarını optimize etmek için yakın bir şekilde birlikte çalıştık. Bu ortaklık onların numune üretim sürecini önemli ölçüde geliştirdi." şeklinde açıklamalarda bulunmuştur.

Zhou'nun araştırma ekibi bir sonraki aşamada, veri güvenliği için umut verici bir alternatif sunan kuantum iletişimini mümkün kılmada temel bir zorluk olan enerji verimliliğini en küçük elektromanyetik enerji miktarına kadar artırmayı hedeflemektedir.

Artan siber saldırıların ardından, bilgisayar korsanlarına karşı kapsamlı bir koruma oluşturmak bilimsel bir ilgi odağı haline gelmiştir. Statista'nın yakın tarihli bir raporuna göre, geleneksel iletişim kanalları üzerinden iletilen veriler iz bırakmadan okunabilmekte ve kopyalanabilmektedir, bu da geçen yıl 350 milyon kullanıcı için binlerce ihlale mal olmuştur. Öte yandan kuantum iletişim, kuantum durumunu değiştirmeden ele geçirilemeyen ışığı kullanarak bilgiyi kodladığı için umut verici bir alternatif sunmaktadır. Zhou'nun malzemelerin doğrusal olmama özelliğini geliştirmeye yönelik yöntemi, bu teknolojileri mümkün kılmaya bir adım daha yaklaştırmaktadır.[69]

69 https://scitechdaily.com/photon-powered-breakthrough-speedy-secure-and-sustainable-telecom-for-the-future/

Yapay Zekâ Öncüleri John Hopfield ve Geoffrey Hinton'a Nobel Fizik Ödülü



Yapay zeka öncüleri John Hopfield ve Geoffrey Hinton, yapay sinir ağları ile makine öğrenimini mümkün kılan ve yapay zekada bugünün atılımlarına zemin hazırlayan keşifleri için 2024 Nobel Fizik Ödülü'nü kazanmışlardır. Ödül İsveç Kraliyet Bilimler Akademisi Genel Sekreteri Hans Ellegren tarafından Stockholm'de verilmiştir.

Amerika Birleşik Devletleri'ndeki Princeton Üniversitesi'nde araştırmalar yürüten Hopfield, 1982 yılında noktalar arasındaki değerleri belirleyerek, bunlar üzerinde çalışarak ve eksik değerleri güncelleyerek görüntülerdeki ve diğer veri türlerindeki örüntüleri koruyabilen ve yeniden oluşturabilen bir ağ oluşturmasıyla tanınmaktadır. Günümüzde Hopfield ağları olarak adlandırılan bu ağlar görüntüleri tanımak, hataları düzeltmek ve bilgisayar bilimlerindeki işlevleri optimize etmek için kullanılabilmektedir. 1985 yılında, Kanada'daki Toronto Üniversitesi'nde bilgisayar bilimcisi olan ve "yapay zekanın vaftiz babası" olarak bilinen Hinton, Hopfield ağını yeni bir model oluşturmak için kullanmıştır. Boltzmann makinesi olarak adlandırılan ağ, örneklerle beslendikten sonra verilerdeki özellikleri tanıyabilmekte ve bunu görüntülerdeki veya diğer desenlerdeki belirli öğeleri tanımlamak için kullanabilmektedir.

Nobel Fizik Komitesi Başkanı Ellen Moons, "Ödül sahiplerinin keşifleri ve icatları, örneğin tıbbi durumları teşhis ederken insanların daha hızlı ve daha güvenilir kararlar almasına yardımcı olabilecek makine öğreniminin yapı taşlarını oluşturmaktadır." açıklamasını yapmıştır. Gazetecilere konuşan Hinton, yapay zeka kaynaklı ilerlemelerin Sanayi Devrimi ile karşılaştırılabilir olacağını, ancak fiziksel güçte insanları aşmak yerine, entelektüel yetenekte insanları aşacağını söylemiştir.[70]

70 https://www.euronews.com/next/2024/10/08/john-hopfield-and-geoffrey-hinton-win-nobel-prize-in-physics-for-work-on-neural-networks

Dünyanın İlk Mobil İnme Ambulans Ünitesi Orta Doğu'da Hizmette

Kral Faysal Uzman Hastanesi ve Araştırma Merkezi (KFSHRC), Orta Doğu ve Kuzey Afrika bölgesinde İnme (felç) tedavisine adanmış ilk Mobil Ambulans Ünitesini tanıtmıştır. Bu yeni ünite, sağlık çalışanlarının nakil sırasında hastalara anında bakım sağlamasına olanak tanıyan ve iyileşme şansını önemli ölçüde artırabilen en son tıbbi teknolojiye sahiptir. İnme tedavisi sonuçlarını optimize etmek amacıyla mobil ünite, Suudi Kızılhaç Kurumu bir kolda güçsüzlük, yüz asimetrisi veya konuşma güçlüğü gibi ilgili semptomlar hakkında bildirim alır almaz devreye girmektedir. Ambulansta çalışan ekip bir vasküler nörolog, kritik bakım alanında uzmanlaşmış bir hemşire, bir paramedik ve bir tomografi teknisyeninden oluşmakta ve teşhis ve müdahaleleri yerinde gerçekleştirmektedir.

KFSHRC girişimi, inme semptomlarının başlamasından sonraki kritik ilk saatlerde gerekli bakımın sağlanmasını hızlandırmaya yönelik önemli bir adımdır. Bu yaklaşım sadece bakım kalitesini iyileştirmeyi değil, aynı zamanda bu tür tıbbi acil durumlarından muzdarip hastaların hayatta kalma oranlarını artırmayı da amaçlamaktadır. KFSHRC, Brand Finance tarafından yapılan 2024 sıralamasına göre dünyadaki 250 ana Akademik Tıp Merkezi arasında 20. sırada yer almasının yanı sıra Orta Doğu ve Afrika'daki en iyi hastane olarak sınıflandırılarak küresel sahnede öne çıkmaktadır. Hastane ayrıca Newsweek dergisine göre dünyanın en iyilerinden biri olarak kabul edilmiştir ve 2025 yılında en akıllı hastaneler listesinde yer almaktadır.[71]

71 https://globalhappenings.com/top-global-news/579236.html#google_vignette

Çin'de Beyin MR Verilerinin DNA Tabanlı Depolanmasında Çığır Açan Bir Gelişme

Tianjin Üniversitesi Sentetik Biyoloji Bilim Merkezi, Tianjin Huanhu Hastanesi ile işbirliği içinde DNA tabanlı veri depolama alanında büyük bir atılım gerçekleştirerek yenilikçi DNA Paleti kodlama şemasını tanıtmıştır. Bu yeni yöntem, beyin manyetik rezonans görüntüleme (MRI) verilerinin DNA'ya başarılı bir şekilde kodlanmasının yanı sıra kayıpsız kod çözme ve görüntüleme verilerinin 3D yeniden yapılandırılmasını sağlayarak gelişmiş tıbbi veri depolama teknolojilerinin geliştirilmesinin önünü açmaktadır. Bu atılımın gerçekleştiği çalışmanın sonuçları National Science Review'da yayımlanmıştır.

Beyin MR taramaları klinik tanı, cerrahi planlama ve tedavi değerlendirmesi için önemli bir araçtır. Ancak bu taramalar sırasında ortaya çıkan büyük miktardaki veri, uzun süreli depolama yöntemleri için önemli zorluklar teşkil etmektedir. Bu konu özellikle juvenil parkinson, epilepsi ve nörogenetik bozukluklar gibi hastalıklar için kritik önem taşımaktadır, çünkü bu gibi durumlarda ömür boyu veri birikimi ve analizi şarttır. Mevcut depolama ortamları, büyük ölçekli, uzun vadeli veri depolamaya yönelik yüksek talebi karşılamakta zorlanmaktadır.

Olağanüstü kararlılığa ve depolama yoğunluğuna sahip olduğu bilinen DNA, veri depolama için umut verici bir ortam olarak ortaya çıkmıştır. Tianjin Üniversitesi araştırma ekibi, 11,28 megabaytlık beyin MR verisini yaklaşık 250.000 DNA dizisine başarıyla kodlayarak baz başına 2,39 bitlik etkileyici bir veri yoğunluğu elde etmiştir. Sentetik DNA'nın tek iplikçikleri olan kodlanmış oligolar kuru toz formunda saklanır, sadece 3 mikrogram ağırlığındadır ve mevcut teknik standartlar altında 300'den fazla okuma işlemini desteklemektedir. Bu buluş, DNA'nın tıbbi veriler için uzun vadeli, verimli ve güvenli bir depolama ortamı olma potansiyelini ortaya koymaktadır.

Bu çalışma, DNA veri depolamanın pratik uygulamasına yönelik çok önemli bir adımı işaret etmekte, büyük miktarda tıbbi verinin güvenli bir şekilde depolanması için yeni bir teknik yol sunmakta ve DNA tabanlı depolama teknolojilerinin daha geniş çapta benimsenmesini hızlandırmaktadır.[72]

72 https://www.chinadaily.com.cn/a/202409/30/WS66fa0c40a310f1265a1c5ade.html

Genişbant İnternet Bağlantısında Lazer Kullanımı

Dünya çapında milyonlarca kullanıcının, internet omurgasına bağlanmasının ve sağlayıcının ağının bir eve veya binaya ulaşmasının son adımı olarak tanımlanan son mil sorunundan dolayı genişbant erişimine sahip olamadığı ifade edilmektedir. Birkaç yüz metreden birkaç kilometreye kadar uzanan bu kritik altyapı, arazideki zorluklar veya çok az sayıda kullanıcıya hizmet vermesi nedeniyle genellikle çok pahalı ya da inşa edilmesi zor olabilmekte ve bu durum kırsal bölgelerde daha büyük bir sorun olarak ortaya çıkmaktadır. Bu soruna bir çözüm olarak ise havadan veri aktarmak için lazerlerin kullanıldığı "serbest uzay optiği" (FSO) adı verilen bir teknoloji ortaya koyulmuştur. Ancak bu yenilikçi teknoloji, hava durumundan oldukça etkilenmekte, sis, yağmur, basit hava türbülansı bile sinyali bozmaya yetmektedir. Bu yüzden verici ve alıcı arasında sabit, doğrudan bir görüş hattı gerektirmekte ve dolayısıyla herhangi bir lisans veya düzenleme gerektirmemesi avantajına rağmen, FSO genişbant henüz ticari olarak kullanıma sunulamamaktadır.

Bu kapsamda, ABD merkezli Attochron şirketi, 20 yılı aşkın bir süredir üzerinde çalıştığı, bir alıcı ile verici içeren ve güvenlik kamerasına benzeyen ALTIS-7 adlı ana donanım ürününün düşük oranlı üretimine başladığını duyurmuştur. Şirket, ticari lansmana hazırlık olarak 2025 yılının başlarında üretimin artırılmasının planlandığını ve bu doğrultuda, telekom şirketi Lumen ve bir perakende şirketi ile ortaklık kurduğunu açıklamıştır.

Lazer bağlantısı ile saniyede 1,25 Gigabit hızla 1,5 milden fazla uzanılmış ve en hızlı fiber optik iş bağlantısıyla aynı seviyede olan 10 Gigabit'in biraz üzerinde bir azami hıza ulaşıldığı ifade edilmiştir. Bununla birlikte, genişbant erişiminde, son milin lazerlerle köprülenmesinin fiber optik kablo döşemeye kıyasla daha ucuz olduğu da belirtilmiştir. Lazer donanımlı Attochron paketi, 10 Gigabit bağlantı için 30.000 dolara mal olurken, fiber kablo altyapısının, uzun izin süreçleri gerektirmesinin yanı sıra özel bir bağlantı için 250.000 ila 1 milyon dolar arasında bir maliyete sahip olduğu ifade edilmektedir.[73]

73 https://edition.cnn.com/2024/10/09/tech/lasers-fso-internet-attochron-spc/index.html

Çin'de Kuantum Tekniğiyle Karanlık Maddenin Keşfi

Çinli bilim insanlarının liderliğindeki uluslararası bir ekip, evrenin en zor bulunan maddesini doğrudan araştırmak için en son kuantum teknolojisini kullanarak, algılama yeteneklerini önemli ölçüde geliştiren olağanüstü bir çalışma sergilemiştir.

Evrenin uçsuz bucaksız genişliğinde, en küçük toz zerresinden Dünya gibi devasa gök cisimlerine, hatta tüm galaksilere kadar değişen boyutlardaki görünür madde, kozmosun toplam kütlesinin yalnızca yaklaşık yüzde 5'ini oluşturmaktadır. Geriye kalan yüzde 95'in karanlık madde ve karanlık enerjiden meydana geldiği düşünülmektedir. Evrenimizin yapısını ve evrimini derinden etkileyen bu egzotik bileşenlerden karanlık madde bilim insanları tarafından hala tam olarak tanımlanamamıştır. Olası adaylar arasında zayıf etkileşimli büyük kütleli parçacıklar (WIMP'ler) ve aksionlar yer almaktadır. WIMP arayışları bugüne kadar görünmez maddeyi tanımlayamamışken, aksionlar özellikle ilgi çekici bir araştırma konusu olarak ortaya çıkmıştır.

Kuantum spin ve kuantum dolanıklık gibi inanılmaz özelliklerden yararlanan kuantum hassas ölçüm teknolojisi, düşük enerji seviyelerinin ultra hassas bir şekilde tespit edilmesini sağlayarak karanlık madde arayışında devrim niteliğinde bir yaklaşım sunmaktadır.

Çin Bilim ve Teknoloji Üniversitesi ve Berkeley Kaliforniya Üniversitesi'nden bilim insanları, kuantum spin etkileşimlerine dayalı süper hassas bir aksion dedektörü kurmak için polarize soygazdan yararlanmışlardır. Dedektör, etkileşim hassasiyetini geleneksel yöntemlere

kıyasla 145 kata kadar arttırmaktadır. Dahası, klasik manyetik alanların neden olduğu parazit için astronomik bir azalma elde ederek sahte sinyalleri önlemiştir. Ekip henüz aksion karanlık maddesinin kesin kanıtını keşfetmemiş olsa da, varsayımsal parçacıkların saklanıyor olabileceği teorik olarak tercih edilen bir kütle aralığı olan "aksion penceresi"ne doğru genişleyen nötron-nötron eşleşmesi üzerine şimdiye kadar bilinen en katı kısıtlamaları yerleştirmiştir.

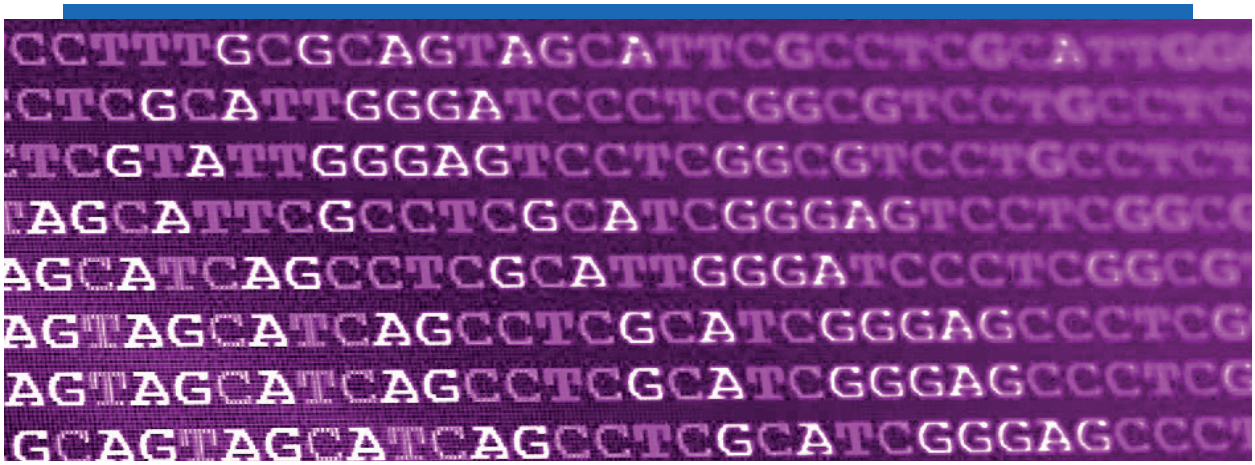
Physical Review Letters dergisinde kısa süre önce yayınlanan bir çalışmaya göre deney, önceki kısıtlamaları en az 50 kat iyileştirerek bu alanda yeni bir ölçüt belirlemiştir. Sonuçlar, kuantum teknolojisinin karanlık madde keşfi alanındaki geniş potansiyelini vurgulamakta ve sınır bilimini ilerletmede en son teknolojinin rolünü göstermektedir.

Dünya merkezli deneyin yanı sıra, ekibin lideri Peng Xinhua, 2023 yılında Çin'in uzay istasyonuna kuantum sensörleri yerleştirmek ve aksion arayışını desteklemek için uzay istasyonunun Dünya etrafındaki yüksek hızlı hareketini kullanmak amacıyla bir plan önermiştir.

Peng, bu çalışmanın hassas tıp için manyetik rezonans görüntülemenin doğruluğunu artırmak ve daha gelişmiş derin deniz keşiflerini mümkün kılmak gibi pratik uygulamalar için de önemli bir potansiyele sahip olduğunu söylemiştir.[74]

74 https://www.chinadaily.com.cn/a/202411/13/WS67341d3da310f1265a1cd1a2.html

Verileri Saklamada Yeni Bir DNA-Baskı Tekniği



Elektronik veri depolama sistemleri ne kadar verimli olursa olsun, doğanın kendi versiyonu olan DNA karşısında hiçbir şey yapamazlar. DNA'ya veri yazmaya yönelik yeni bir teknik matbaa gibi çalışmakta ve bunu herkesin yapabileceği kadar kolay hale getirmektedir. DNA'ya veri yazmak genellikle boncukları bir ipe dizmek gibi her seferinde bir harf sentezlemeyi içermektedir. Belirli bir DNA dizisinde bu harflerden ya da bazlardan milyarlarca olabileceği düşünüldüğünde bu oldukça yavaş bir süreçtir. Ancak yeni DNA baskı makinesi süreci büyük ölçüde hızlandırmaktadır. Ekip, hareketli yazı parçaları gibi çalışan, her biri 24 baz içeren 700 DNA zincirlerinden oluşan bir set oluşturmuştur. Bunlar istenen sıraya göre düzenlenebilecek ve daha sonra verilerini DNA şablon ipliklerine yazdırmak için kullanılabilecektir. Her seferinde bir bit yazmak yerine, bu baskı makinesi süreci reaksiyon başına aynı anda 350 bite kadar hızlandırmaktadır. Süreci basitleştirmek için veriler DNA'nın alışılagelmiş GCAT harflerine değil, ikili kodun tanıdık bir ve sıfırlarına kodlanmaktadır. Bu durumda, kimyasal işaretler bazı DNA zincirlerine eklenirken diğerlerine eklenmemiş; işaretli olanlar birleri, olmayanlar ise sıfırları temsil etmiştir. Ekip bu tekniği, eski bir Çin kaplanının 16.833 bitlik görüntüsü ve 252.500'den fazla bitten oluşan bir panda fotoğrafı da dahil olmak üzere görüntüleri depolayarak test etmiştir. Biraz ince ayar yapıldıktan sonra, verilerin yüzde yüzü standart DNA okuma yöntemleri kullanılarak kurtarılabilmiştir.

Kullanımının ne kadar basit olabileceğini göstermek için ekip 60 kişiyle bir deney gerçekleştirmiştir. Katılımcılar iDNAdrive adlı yazılım platformunu kullanarak seçtikleri metin parçalarını toplamda yaklaşık 5.000 bit olacak şekilde kodlamışlardır. Veriler yüzde 98,58 doğrulukla başarılı bir şekilde geri okunmuştur.

DNA veri depolamanın cazibesi açıktır. Sadece 1 cm^3 DNA'da 10 milyar Gigabayttan fazla veri depolanabileceği tahmin edilmektedir. Daha da iyisi, doğru koşullar altında saklanan bu veriler binlerce hatta milyonlarca yıl dayanabilmekte ve bu da onu harika bir arşiv sistemi haline getirmektedir. DNA'dan veri okumak nispeten hızlıdır, ancak yazmak en zor kısımdır.

Hareketli tip baskının icadı, ilk seri üretim metinlerin ortaya çıkmasını sağlamıştır. Kendi küçük pulları üzerindeki tek tek karakterler büyük bloklar halinde düzenlenerek hızlı bir şekilde çok sayıda kopya basılabiliyordu. Moleküler hareketli yazı tipinin ilham kaynağı, kendi hücrelerimizin verileri depolama ve işleme biçimidir. Vücudunuzdaki her hücre genomunuzun tamamını içermektedir. Çeşitli dokulardaki hücreleri farklılaştıran şey, epigenom adı verilen ekstra bir bilgi katmanıdır. DNA zincirleri hareketli yazı parçalarıdır ve boş DNA şablon iplikleri de kağıttır. Belirli bir diziye ihtiyaç duyulduğunda, karşılık gelen tuğlalar seçilmekte ve şablonla birlikte çözeltiye yerleştirilmektedir. Bir kez orada, zincirler DNA şablonu boyunca belirli bölgelere bağlanmaktadır. Son olarak mürekkep gelmektedir. Bir enzim, zincirlerdeki tüm metil gruplarını DNA şablonunun her bir parçasına kopyalamakta ve daha sonra, bir nano gözenek dizileme cihazı, depolanan dijital dosyaları yeniden oluşturmak için birler ve sıfırlar desenini okuyabilmektedir.

Zincirler şablon DNA ipliği üzerinde kendiliğinden bir araya geldiğinden, çok sayıda yazma işlemi parça parça değil bir kerede gerçekleşmektedir. Süreci hızlandırmak ve bilim insanı olmayanlar için erişilebilir kılmak, DNA'nın uygulanabilir bir veri depolama ortamı haline gelmesine yardımcı olabilecektir.[75]

75 https://www.sciencealert.com/a-new-dna-printing-technique-could-revolutionize-how-we-store-data

Katar'ın Bilgi Tabanlı Ekonomi Hedefi

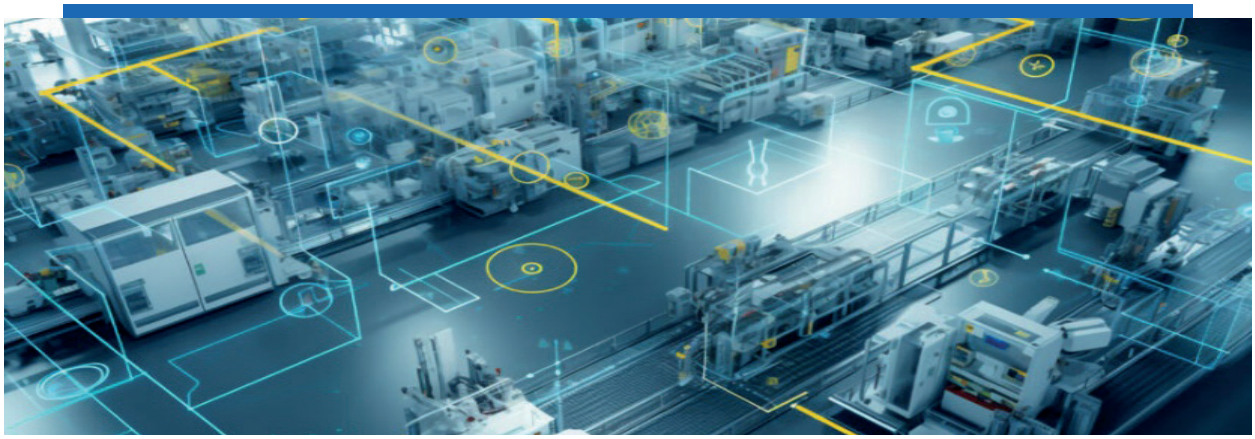
İletişim ve Enformasyon Teknolojileri Bakanı Muhammed bin Ali El-Mannai, Katar Devleti'nin Katar Ulusal Vizyonu 2030 çerçevesinde, teknoloji ve dijital dönüşüm etrafında dönen sürdürülebilir kalkınma hedefleri doğrultusunda bilgi tabanlı bir ekonomi kurma konusundaki kararlılığını teyit etmiştir. 18-19 Kasım tarihlerinde iki gün boyunca Doha'da düzenlenen M360 Orta Doğu ve Kuzey Afrika Konferansında Muhammed bin Ali El-Mannai şunları söylemiştir: "M360 Orta Doğu ve Kuzey Afrika Konferansı'na Doha'da ev sahipliği yapmak, Katar Devleti'nin bölgede dijital inovasyon ve iş birliği çabalarını teşvik etme konusundaki kararlılığının bir teyididir. Yapay zeka ve 5G ağları gibi en son teknolojileri benimseyerek ve etkili stratejik dijital ortaklıklar kurarak sürdürülebilir büyümeyi teşvik etme ve vatandaşlarımızın yaşam kalitesini iyileştirme yeteneğimize güveniyoruz. Konferans, Orta Doğu ve Kuzey Afrika bölgesindeki dijital geleceği tartışmak ve bunun geliştirilmesine katkıda bulunmak için etkili stratejiler geliştirmek için değerli bir platform sunuyor."

Mobil hizmetlerin bölge GSYİH'sine 360 milyar dolar katkı sağlayacağı yönündeki beklentiler ışığında, Ortadoğu ve Kuzey Afrika'da dijital ekonominin potansiyelini artırmak amacıyla düzenlenen konferansa, çok sayıda sanayi, teknoloji ve iletişim sektörü temsilcisinin yanı sıra çok sayıda hükümet yetkilisi katılmıştır.

Konferansta GSMA'nın Ortadoğu ve Kuzey Afrika bölgesindeki mobil ekonomiye ilişkin 2024 yılı raporu da yayımlanmıştır. Raporda, bölgede üretken yapay zekanın giderek daha fazla benimsendiği; telekom operatörlerinin müşteri deneyimini geliştirmek, ağ performansını iyileştirmek ve iş fırsatları için yeni ufuklar açmak amacıyla bu gelişmiş teknolojiye güvendiği ortaya konulmuştur. Konferansın açılışının ardından Ooredoo Katar ve GSMA'dan üst düzey yöneticilerden oluşan bir heyet, Ooredoo Katar, Katar Medya Şehri, Invest Katar, SAP ve Google gibi ana sergileri gezerek dijital dönüşüm çabalarını hızlandırmayı amaçlayan yenilikçi çözümler hakkında bilgi almışlardır.[76]

76 https://www.qna.org.qa/en/News%20Area/News/2024-11/18/0019-exchange-rates-in-qatar

Polonya'dan Yapay Zeka Hamlesi



Polonya, yapay zeka ve dijital dönüşümdeki son girişimleriyle önemli kazanımlar sağlamaktadır. Krakow'da "AI Factory"nin lansmanı ve Dijitalleşme Stratejisinin uygulanmasıyla ülke, modern, dijital olarak yönlendirilen bir ekonomi için güçlü bir temel oluşturmaktadır. Polonya, Krakow'daki Akademik Bilgisayar Merkezi CYFRONET AGH'de öncü bir "AI Fabrikası" kurmaya hazırlanmaktadır. Tesis, AI çözümlerinin geliştirildiği, test edildiği ve uygulandığı bir inovasyon merkezi olarak hizmet verecektir. Polonya Basın Ajansı'na (PAP) konuşan Dijital İşler Bakan Yardımcısı Dariusz Standerski'ye göre, AI Factory, Avrupa Komisyonu'nun desteğinden yararlanarak daha geniş Avrupa AI ekosistemi içinde iş birliğini teşvik etmeye odaklanacaktır. Geleneksel fabrikaların aksine, AI Factory, yapay zeka alanındaki ilerlemeleri yönlendirmek için Polonya'ya gereken bilgi işlem gücünü ve veri kaynaklarını sağlayarak, AI inovasyonu için son teknoloji bir platform görevi görecektir.

Polonya'nın son "Dijitalleşme Stratejisi", dijital dönüşüm için iddialı bir on yıllık yol haritası ortaya koymaktadır. Başbakan Yardımcısı ve Dijital İşler Bakanı Krzysztof Gawkowski tarafından tanıtılan bu plan, Polonya'nın dijital yeteneklerini 2035 yılına kadar yükseltmeyi amaçlamaktadır. Strateji, siber güvenliğe, bulut altyapısına ve kamu hizmetlerinin dijitalleştirilmesine daha fazla yatırım yaparak hem kamu hem de özel sektörde yapay zekanın kullanılmasına güçlü bir vurgu yapmaktadır. Polonya, bu yetenekleri geliştirerek Avrupa'da dijital dayanıklılıkta lider rolünü güçlendirmeyi amaçlamaktadır.

Polonya'nın iddialı AI girişimleri BT sektöründe önemli bir büyümeye yol açacaktır. Bu çabalar, Polonya'nın 2035 yılına kadar yapay zekayı işletmelerin %50'sine entegre etmek için çalışmasıyla yetenekli profesyonellere olan talep artacaktır. Aynı zamanda, bulut altyapısı ve siber güvenliğe yapılan yatırımlar bu alanlarda yeni fırsatlar oluşturacaktır. Avrupa AI ekosisteminin merkezi bir parçası olarak öngörülen AI Factory'nin, Avrupa genelindeki önde gelen teknoloji kuruluşlarıyla araştırma ve geliştirme ortaklıklarını teşvik ederek inovasyon ve iş birliğine yeni kapılar açması beklenmektedir. Bu girişimler Polonya'nın küresel profilini güçlendirmekte ve ülkeyi Avrupa'nın dijital ekonomisinde önemli bir oyuncu olarak konumlandırarak teknoloji sektöründe sürdürülebilir büyümenin önünü açmaktadır.[77]

77 https://doitinpoland.com/poland-advances-ai-with-new-innovation-hub-and-digitalization-strategy/

Esnek Anahtarlama İçin Gömülü eSIM'li LTE Cat 1bis Modülü

Entegre eSIM, esnek bağlantı yönetimi sağlamakta ve müşterilere kapsama alanı ve maliyet açısından en iyi ağa geçme olanağı vermektedir. Coğrafyadan bağımsız olarak daha hızlı dağıtım ve güvenilir bağlantı sunan SARA-R10001DE LTE modülü, varlık takibi, telematik, mikro mobilite, güneş teknolojisi, akıllı evler ve şehirler ve satış noktası gibi uygulamalarda birçok avantaj sunmaktadır.

Wireless Logic eSIM'de saklanan çoklu SIM profilleri, modülün otomatik olarak en iyi ağa bağlanmasını sağlamaktadır. Bu, modülün her zaman en iyi ağa bağlanacağına ve herhangi bir sorun ortaya çıktığında eSIM'in otomatik olarak farklı bir operatöre geçerek güvenilir bağlantıyı sürdüreceğine dair güven vermektedir. Yerleşik eSIM, SIM tedarikini yönetmek için harcanan zaman ve çabayı en aza indirdiği ve SIM tutucular gibi tamamlayıcı bileşenleri tedarik etme ihtiyacını ortadan kaldırdığı için müşteri lojistiğini basitleştirmektedir.

LTE küresel kapsama alanı sağlamak üzere tasarlanan SARA-R10001DE, eski 2G ve 3G cihazları için 4G LTE küresel kapsama alanına kolay bir geçiş yolu sağlamaktadır. U-blox LPWA Ürün Grubu Müdürü Samuele Falcomer "Dahili bağlantı özelliğine sahip yeni modülümüz, maliyet verimliliği sağlarken güvenilir bağlantıya ulaşmayı daha basit ve hızlı hale getirerek en iyi kullanıcı deneyimini sunmak için tasarlandı. Müşterilerin ayrı bir SIM, SIM tutucu ve ilgili bileşenleri satın almasına gerek kalmadığından, bağlantıyı ayrı olarak satın almaktan daha iyi finansal sonuçlar sunabilir. SARA-R10001DE modülü halihazırda profillenmiş bağlantı ile birlikte tedarik edildiğinden, müşterilerin yalnızca SIM Yönetimi aracılığıyla etkinleştirmesi yeterlidir." açıklamasında bulunmuştur.

Gömülü eSIM, zorlu ortamlarda güvenilir çalışma için sağlamlığı artırmaktadır. Bükülebilen ve bozulabilen plastik SIM'lerin aksine, eSIM bileşeni kalıcı elektrik temasını garanti etmek için standart bir elektronik bileşen gibi lehimlenmiştir.[78]

78 https://www.eenewseurope.com/en/lte-cat-1bis-module-with-embedded-esim-for-flexible-switching/

Yeniden Kullanılabilir Roketler

Eindhoven Teknoloji Üniversitesi'nde öğrencilerden oluşan Team VOID, telekomünikasyon ve uydular gibi uygulamalar için roketlerin yeniden kullanılabilirliğine odaklanmaktadır. Geleneksel roketler genellikle tek kullanımlıktır. Bu, uzay seyahatini pahalı ve çevre dostu olmayan hale getirmektedir. Eindhoven Teknoloji Üniversitesi'nde Ağustos 2023'te kurulan VOID, inşa edilecek roketlerinin mini bir versiyonunu tanıtmıştır.

Team VOID öğrencilerinin inşa ettiği henüz büyük ölçekli, parlak bir roket değildir, ancak geliştirmeleri devam etmektedir. Tanıtım etkinlikleri sırasında, roketin mini bir versiyonu olan Tapeti sergilenmiştir. Bu, bir roket motoru yerine pervanesi olan sözde bir "Hopper" dır.

Sadece sekiz üyeyle başlayan ekip, bir yılda 13 farklı ülkeden 27 azimli öğrenciden oluşan bir ekibe dönüşmüştür. Ekibin ortak hedefi uzay endüstrisini tamamen dönüştürmektir. Bu alandaki en büyük engellerden biri ise çoğu roketin yalnızca bir kez kullanılabilmesidir. Bu, her fırlatmadan sonra tamamen yeni bir roket inşa edilmesi gerektiği anlamına gelir ki bu hem zaman alıcı hem de maliyetli olmaktadır. Ayrıca tek kullanımlık roketlerin mevcut uygulaması çevre dostu olmaktan oldukça uzaktır. Pasifik Okyanusu'nda en az 263 uzay nesnesi bulunmaktadır. Öte yandan Team VOID farklı bir yol izlemekte ve yeniden kullanılabilir roketler tasarlamaktadır.[79]

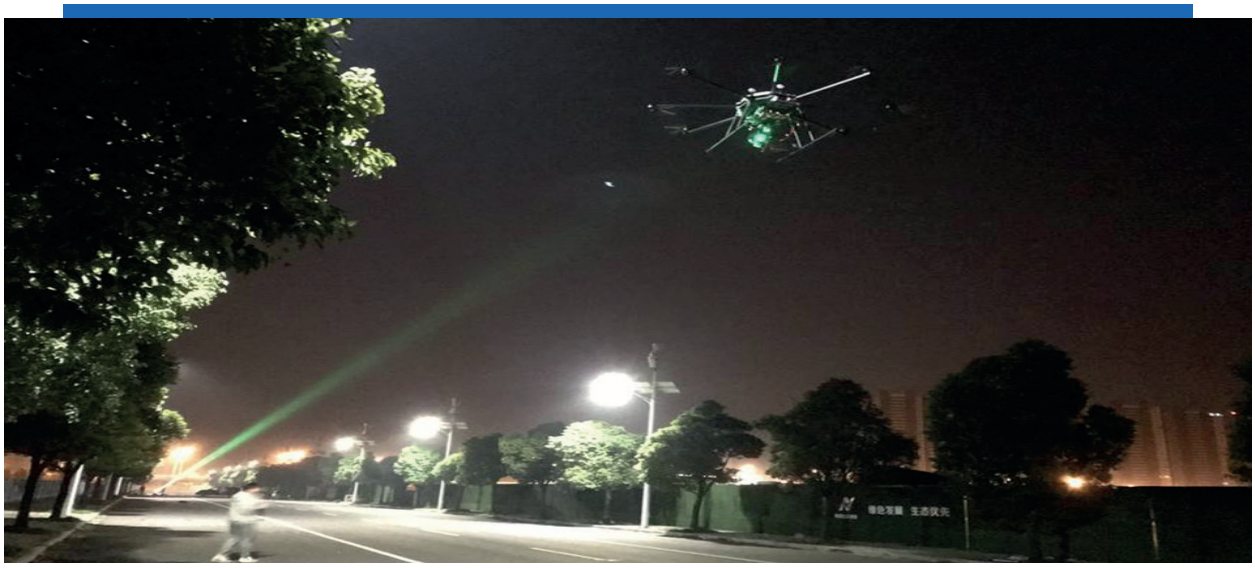
79 https://www.eenewseurope.com/en/team-void-designing-reusable-rockets/

Ecosia ve Qwant'tan Yeni Arama İndeksi

Alman Ecosia ve Fransız Qwant şirketleri yeni bir arama indeksi oluşturmak için ortaklık kurmuştur. İki Avrupa arama motoru şirketi, internet kullanıcılarına Avrupa'da bir arama alternatifi sunmak için yine Avrupa sınırları içerisinde altyapı inşa ettiklerini duyurmuştur. Avrupa Arama Perspektifleri (European Search Perspectives-EUSP) adı verilen altyapı Paris'te bulunmaktadır. 2025 yılında faaliyete geçecek olan arama indeksi hem Almanca hem de Fransızca olacaktır. Söz konusu platform ile, Avrupa'da dijital bağımsızlığın sağlanması ve yapay zeka altyapısı için bir temel oluşturulması hedeflenmektedir.[80]

80 https://www.euronews.com/next/2024/11/12/europes-answer-to-google-ecosia-and-qwant-partner-to-build-new-search-index

Çin'den Drone Üzerinde Dünyanın İlk Kuantum Şifreleme Deneyi



Çinli bilim insanları şehirlerarası, kıtalararası ve uzay da dahil olmak üzere çeşitli düzeylerde kuantum deneyleri gerçekleştirmişti. Şimdi de bir drone ile bu "kırılamaz" şifreleme teknolojisinin gerçek dünyada kullanılabileceği bir geleceğin önünü açacak bir buluşa imza atılmıştır.

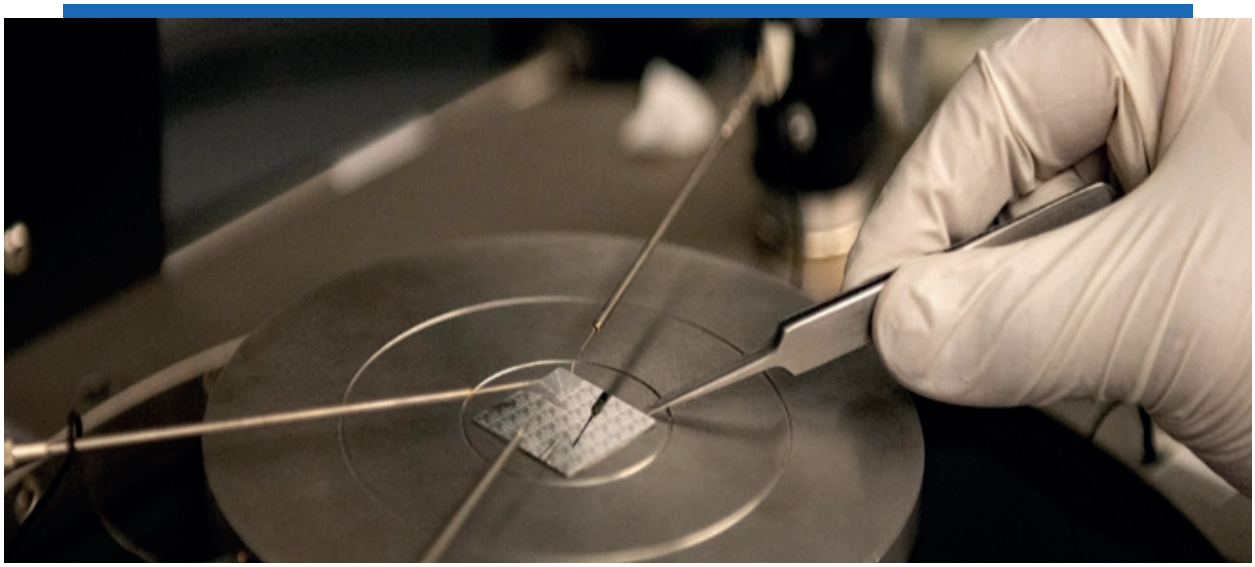
Nanjing Üniversitesi ve Çin Bilim ve Teknoloji Üniversitesi'nden araştırmacılar, bir drone platformuna dayalı kuantum anahtar dağıtımı (QKD) deneyini tamamlayarak küresel bir ilke öncülük etmişlerdir. Bu deney, drone gibi mobil platformların, tek fotonları son kullanıcılara doğrudan iletme kabiliyeti gerektiren daha pratik kuantum görevlerini yerine getirebileceğini göstermiştir.

QKD, kuantum mekaniğindeki, rastgele bilinmeyen bir kuantum durumunun bağımsız ve özdeş bir kopyasını oluşturmayı imkansız kılan fiziksel bir özelliğe dayanmaktadır. Böylece uzak kullanıcılar arasında şifreli mesaj alışverişi için "hacklenemez" bir yol sağlanmaktadır. Ekip, uçuş halindeki küçük bir çok rotorlu drone ile 200 metre mesafedeki bir yer istasyonu arasında düşük kayıplı, yüksek doğruluklu bir optik kuantum bağlantısı kurmuştur. Physical Review Letters dergisinde yayınlanan çalışmaya göre, deneyler hem gece hem de gündüz koşullarında yapılmış ve ortalama hata oranları sırasıyla yaklaşık yüzde 2,28 ve yüzde 3,86 olmuştur. Sonuçlar, pratik fotonik kuantum görevlerini yerine getirmek için drone platformlarının kullanılmasının fizibilitesini ve güvenilirliğini doğrulamaktadır.

Araştırmacılar, bir drone kullanarak gizli anahtar dağıtımı kabiliyetiyle, bir ağa doğru mobil düğümler arasındaki kuantum yaklaşımında gelişmiş güvenlik ile kablosuz iletişimin beklenebileceğini söylemektedir. Ayrıca gelecekte geniş alan QKD için yüksek irtifa sabit kanatlı dronlardan yararlanmayı ve sürekli, her yönlü mobil kuantum bağlantısı vaat etmeyi planlamaktadır.[81]

81 https://www.chinadaily.com.cn/a/202411/19/WS673c7da7a310f1265a1ce6a9.html

Veri Merkezlerini Soğutmada Kullanılabilecek Yeni Termal Malzeme



Dünyanın veri depolama taleplerini karşılamak para, enerji ve çevresel etki açısından maliyetlidir ancak yeni bir malzeme veri merkezlerinin soğutulması önemli ölçüde iyileştirebilecek ve aynı zamanda ev ve iş elektronik cihazlarını daha enerji verimli hale getirebilecektir. Şu anda, verileri tutan donanımı soğutmak için genellikle hantal ve yoğun enerji harcayan soğutma çözümleri kullanılmaktadır ve bu da toplam veri merkezi enerji kullanımının yaklaşık yüzde 40'ına (her yıl yaklaşık 8 Terawatt-saat) denk gelmektedir.
Austin'deki Teksas Üniversitesi ve Çin'deki Sichuan Üniversitesi'nden oluşan ekip, yeni organik termal arayüz malzemesi (TIM) sayesinde söz konusu 8 Terawatt-saatin yaklaşık yüzde 13'ünün azaltılabileceğini tahmin etmektedir. TIM, ısının aktif elektronik bileşenlerden uzaklaştırılma ve hava ya da suyun taşıması için bir soğutucuya kanalize edilme oranını önemli ölçüde artırmaktadır. Bu da fanlar ve sıvı soğutma gibi aktif soğutma teknolojilerine daha az ihtiyaç duyulması anlamına gelmektedir.

Austin'deki Texas Üniversitesi'nden malzeme bilimci Guihua Yu konuya ilişkin şunları söylemiştir: "Enerji yoğun veri merkezleri ve diğer büyük elektronik sistemler için soğutma altyapısının güç tüketimi hızla artıyor. Bu eğilim yakın zamanda ortadan kalkmayacak, bu nedenle kilovat seviyelerinde ve hatta daha yüksek güçte çalışan cihazların verimli ve sürdürülebilir bir şekilde soğutulması için oluşturduğumuz malzeme gibi yeni yöntemler geliştirmek kritik önem taşıyor."

Burada geliştirilen TIM, sıvı metal galinstan ve alüminyum nitrür parçacıklarının kolloidal bir karışımı olup, iki madde arasında herhangi bir sert sınır olmaksızın ısının geçmesine yardımcı olan bir gradyan arayüzü oluşturacak şekilde bir araya getirilmiştir. Deneysel bir laboratuvar test düzeneğinde TIM, önde gelen bir termal macuna kıyasla elektronik bir bileşenin her santimetrekaresinden güvenli bir şekilde aktarılabilen ısı miktarını iki katına çıkarırken

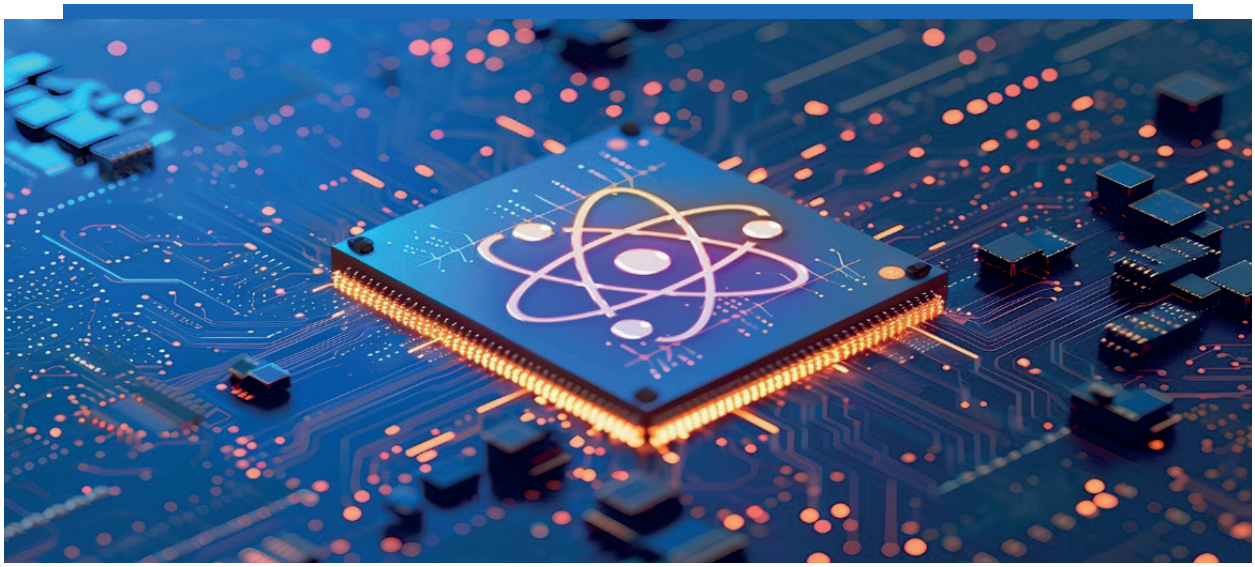
bileşenin genel sıcaklığını da düşürmeyi başarmıştır. Kurulum, aşırı ısınmaya karşı yaygın bir koruma olan bir soğutma pompası kullanmış ve TIM, pompanın enerji kullanımını yüzde 65 oranında azaltmıştır. Bu sadece küçük ölçekli bir örnektir, ancak malzemenin ısı aktarma potansiyelini göstermektedir.

Bir sonraki adım, malzemenin daha büyük sistemlerde ve daha çeşitli senaryolarda çalışmasını sağlamaktır ve araştırmacılar veri merkezi sağlayıcılarıyla ortaklık kurarak bunu gerçekleştirmeyi hedeflemektedir.

Analistler, büyük ölçüde yapay zekâ modellerinin artan talepleri nedeniyle 2028 yılında veri merkezi elektrik kullanımının 2023'tekinin iki katı olmasını beklemektedir. Bu da bilim insanlarının çözmek için çok çalıştığı gerçek bir enerji talebi sorununu ortaya çıkarmaktadır. Wu, malzemelerinin, veri merkezlerinden havacılığa kadar enerji yoğun uygulamalarda sürdürülebilir soğutma sağlayarak daha verimli ve çevre dostu teknolojilerin önünü açabileceğini söylemiştir. Araştırma Nature Nanotechnology dergisinde yayımlanmıştır.[82]

82 https://www.sciencealert.com/new-thermal-material-could-slash-data-center-cooling-demands

Çin'in İlk Kuantum Bilişim ve Tıbbi Veri Enstitüsü



Çin'de türünün ilk örneği olan Hefei Kuantum Hesaplama ve Tıbbi Veri Enstitüsü Anhui eyaletinin başkenti Hefei'de kurulmuştur. Anhui Kuantum Hesaplama Mühendisliği Araştırma Merkezi'ne göre, Hefei merkezli kuantum hesaplama şirketi Origin Quantum ve Bengbu şehrinden Bengbu Tıp Üniversitesi enstitüyü ortaklaşa kurmuştur. Merkezden yapılan açıklamaya göre enstitü, kuantum hesaplama yoluyla tıbbi verilerin güvenliğini ve uygulamasını güçlendirmeyi ve kuantum tıbbi algoritmalar üzerinde gerçek makine doğrulama araştırmaları yürütmeyi amaçlamaktadır.

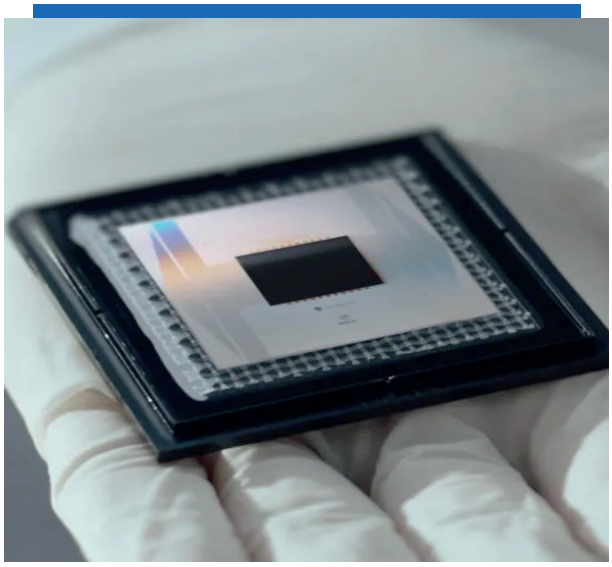
Bengbu Tıp Üniversitesi Başkan Yardımcısı Liu Hao, Çin'in tıbbi verilerinin, gelişimini ilerletmek için acilen yerel olarak geliştirilmiş ve kontrol edilebilir kuantum hesaplama gücüne ihtiyaç duyduğunu açıklamıştır. Enstitünün kurulmasının Çin'de kuantum bilişim ve tıbbi veri alanındaki araştırmaları teşvik edeceğini ve ilgili profesyonel yetenekleri yetiştireceğini söylemiştir.

Origin Quantum'un baş bilim adamı Guo Guoping, bu işbirliği sayesinde, kuantum bilişim ve tıbbi veriler alanında geleceğin hibrit yeteneklerini yetiştirmek için yeni yollar keşfetmeyi amaçladıklarını söylemiştir.

Bengbu Tıp Üniversitesi ve şirket, Origin Quantum tarafından geliştirilen süper iletken bir kuantum bilgisayar olan Origin Wukong'u kullanarak küçük molekül ilaç geliştirme çalışmalarını sürdürmektedir. Şirkete göre, bilgisayar bu yılın başlarında piyasaya sürüldüğünden beri 137 ülkeden kullanıcılar için yaklaşık 298.000 kuantum hesaplama görevini tamamlamıştır. Bengbu Tıp Üniversitesi, kuantum bilişimin tıpta kullanımını keşfetme konusunda Çin'de öncü olmuştur. Geçtiğimiz yıl Üniversite ve Origin Quantum, kuantum hesaplama teknolojisiyle meme hastalıkları için molibden hedef tespitinin verimliliğini artırarak, yerel olarak geliştirilen süper iletken kuantum bilgisayarların tıbbi araştırmalara ilk katılımını sağlamıştır.[83]

83 https://www.chinadaily.com.cn/a/202412/10/WS6757952ba310f1265a1d1ff2.html

Google'dan Akıllara Durgunluk Veren Kuantum Hesaplama Çipi



Google, şu anda dünyanın en hızlı süper bilgisayarlarının on septilyon - ya da 10,000,000,000,000,000,000,000 yıl - sürede tamamlayabileceği bir problemi beş dakikada çözdüğünü iddia ettiği yeni bir çipi tanıtmıştır. Bu çip, parçacık fiziği ilkelerini kullanarak akıllara durgunluk verecek kadar güçlü yeni bir bilgisayar türü geliştirmeye çalışan ve kuantum hesaplama olarak bilinen alandaki en son gelişmedir.

Google, "Willow" adını verdiği yeni kuantum çipinin önemli "atılımlar" içerdiğini ve "kullanışlı, büyük ölçekli bir kuantum bilgisayara giden yolu açtığını" bildirmiştir. Ancak uzmanlar Willow'un şimdilik büyük ölçüde deneysel bir cihaz olduğunu, yani çok çeşitli gerçek dünya sorunlarını çözebilecek kadar güçlü bir kuantum bilgisayarın hala yıllar - ve milyarlarca dolar - uzakta olduğunu söylemektedir.

Kuantum bilgisayarlar telefonunuzdaki ya da dizüstü bilgisayarınızdaki bilgisayardan temelde farklı bir şekilde çalışmaktadır. Sorunları geleneksel bilgisayarlardan çok daha hızlı çözmek için kuantum mekaniğinden - ultra küçük parçacıkların garip davranışlarından - yararlanmaktadırlar. Kuantum bilgisayarların eninde sonunda bu yeteneklerini yeni ilaçlar üretmek gibi karmaşık süreçleri büyük ölçüde hızlandırmak için kullanabilecekleri umulmaktadır. Ayrıca, örneğin hassas verileri korumak için kullanılan bazı şifreleme türlerini kırmak gibi kötü amaçlarla kullanılabileceğine dair korkular da bulunmaktadır.

Şubat ayında Apple, iMessage sohbetlerini koruyan şifrelemenin gelecekteki güçlü kuantum bilgisayarlar tarafından okunmasını engellemek için "kuantum geçirmez" hale getirildiğini duyurmuştur. Hartmut Neven, Willow'u geliştiren Google'ın Kuantum Yapay Zeka laboratuvarını yönetmekte ve kendisini projenin şef optimisti olarak tanımlamaktadır. BBC'ye Willow'un bazı pratik uygulamalarda kullanılacağını söylemiş, ancak şimdilik daha fazla ayrıntı vermeyi reddetmiştir. Ancak ticari uygulamaları gerçekleştirebilecek bir çipin on yılın sonundan önce ortaya çıkmayacağını belirtmiştir.

Başlangıçta bu uygulamalar kuantum etkilerinin önemli olduğu sistemlerin simülasyonu olacaktır. "Örneğin, ilaçların işleyişini anlamak ve ilaç geliştirmek için nükleer füzyon reaktörlerinin tasarımı söz konusu olduğunda, daha iyi araba aküleri geliştirmek için ve bunun gibi diğer bir çok ihtiyaç için uygun olacaktır".[84]

84 https://www.bbc.com/news/articles/c791ng0zvl3o

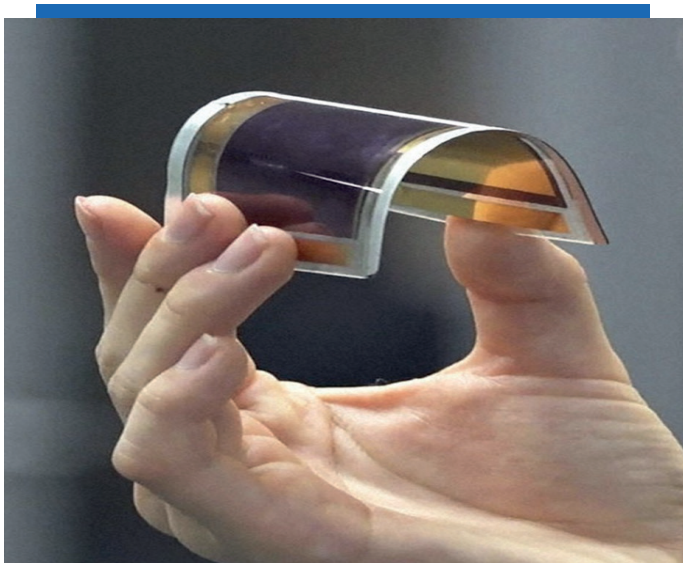
Katar ve İngiltere'den Ortak Yapay Zeka Araştırma Komisyonu

Birleşik Krallık ve Katar, Emir Şeyh Tamim bin Hamad Al-Thani'nin Birleşik Krallık'a gerçekleştirdiği devlet ziyareti çerçevesinde, her iki ülkeye de fayda sağlayacak yapay zeka konusunda Birleşik Krallık-Katar işbirliği için bir yol haritası oluşturmayı amaçlayan ortak bir Yapay Zeka (AI) araştırma komisyonu kurmuştur. Ortak çalışma, Londra Queen Mary Üniversitesi (QMUL) tarafından Katar'daki Hamad Bin Khalifa Üniversitesi (HBKU) ile ortaklaşa yürütülecektir. Çalışma, QMUL Dijital Çevre Araştırma Enstitüsü Etik, Teknoloji ve Toplum Profesörü ve Alan Turing Enstitüsü Etik ve Sorumlu İnovasyon Araştırmaları Direktörü David Leslie tarafından yönetilmektedir.

Proje, her iki ülkenin de yapay zeka alanında kaydettiği heyecan verici ilerlemeyi temel alacak ve ülkelerin yapay zeka ve teknoloji stratejileri doğrultusunda bu alandaki işbirliklerini geliştirmeleri için pratik ve iddialı yollar belirleyecek ve araştıracaktır. Ekosistem geliştirme, politika ve düzenleme, güvenlik ve uluslararası katılım yelpazesinde bir dizi alan araştırılacaktır. Proje, Katar Dışişleri Bakanlığı, Katar İletişim ve Bilgi Teknolojileri Bakanlığı (MCIT) YZ Komitesi, Katar Araştırma, Geliştirme ve İnovasyon Konseyi (QRDI) ve Doha'daki İngiliz Büyükelçiliği arasında bir işbirliği olarak tasarlanmış ve geliştirilmiştir. Proje, Birleşik Krallık hükümetinin Dışişleri, Milletler Topluluğu ve Kalkınma Ofisi bünyesindeki uluslararası programının bir parçası olan Körfez Strateji Fonu tarafından finanse edilmektedir. Katar Dışişleri Bakanlığı Tam Yetkili Bakanı Dr. Mariam Khalid Al Hamar da bu girişimin işbirliği yoluyla inovasyonu ilerletmek için önemli bir fırsat olduğunu belirterek, diyalog ve arabuluculukta küresel bir lider olan Katar'ın diplomasinin geliştirilmesi ve çatışmaların çözümünde işbirliğinin hayati öneminin farkında olduğunu söylemiştir.[85]

85 https://www.iloveqatar.net/news/technology/qatar-uk-artificial-intelligence-ai-research-comission

Japonya'dan 20 Nükleer Reaktöre Eşdeğer Yeni Nesil Güneş Enerjisi Hedefi



Japon hükümeti 2040 yılında ince ve bükülebilir perovskit güneş pilleriyle 20 nükleer reaktörün üretimine eşdeğer yaklaşık 20 gigawatt elektrik üretmeyi planlamaktadır. Japonya Sanayi Bakanlığı, Aralık ayında ülkenin revize edilmiş enerji planının taslağını açıklamış olup, yeni nesil güneş pillerini 2050 yılına kadar net sıfır emisyona ulaşmak için yenilenebilir enerji kaynaklarını genişletmenin anahtarı olarak belirlemeyi planlamaktadır.

Japonya, perovskit güneş pillerinin üretiminde kullanılan birincil malzeme olan iyodun küresel üretiminde Şili'den sonra ikinci büyük paya sahip olduğundan, ekonomik güvenliğini artırmaya yardımcı olacak istikrarlı bir tedarik için bağımsız bir tedarik zinciri oluşturabilecektir. Güneş panelleri, yıkıcı bir deprem ve tsunaminin tetiklediği 2011 nükleer felaketinden sonra Japonya'da hızla yayılmış ve Nisan 2024'e kadar olan dönemde ülkenin elektrik üretiminin yaklaşık yüzde 10'unu oluşturur hale gelmiştir. Ancak Japonya'da büyük geleneksel silikon bazlı güneş pillerini barındıracak çok fazla alan kalmamıştır. Perovskit güneş pilleri hafif ve bükülmeye veya bozulmaya karşı dayanıklı olduğundan, diğer yerlerin yanı sıra bina duvarlarına, pencerelere ve araba çatılarına yerleştirilebilmektedir.

Sekisui Chemical Co. gibi şirketler perovskit güneş pillerini ticarileştirmek için çalışıyor olsa da, zayıf hücre dayanıklılığı ve kısa ömür gibi hala aşılması gereken bir dizi zorluk olduğundan, teknolojinin tam teşekküllü olarak 2030'lara kadar tanıtılması beklenmemektedir.

Japonya'nın küresel güneş paneli üretimindeki payı, büyük devlet sübvansiyonları ile desteklenen güneş panelleri üreten Çinli üreticiler nedeniyle 2004 yılındaki yaklaşık yüzde 50 seviyesinden yüzde 1'in altına düşmüştür. Japon hükümeti, teknolojiyi önemli bir yerli yenilenebilir enerji olarak teşvik ettikten sonra gelecekte perovskit güneş pillerini ihraç etmeyi amaçlamaktadır.[86]

86 https://mainichi.jp/english/articles/20241201/p2g/00m/0bu/013000c

Kazakistan'da Yapay Zeka Destekli Kamu Güvenliği İçin Carpet CCTV

Teknolojinin şehirlerin emniyet ve güvenlik yönetimini giderek daha fazla şekillendirdiği bir dünyada, Kazakistan İçişleri Bakanlığı çığır açan "Carpet CCTV" projesiyle öne çıkmaktadır. Bu iddialı girişim, devasa bir gözetim ağını gelişmiş analitik ve yapay zeka ile birleştirerek kamu güvenliğinde odağı reaktif müdahalelerden proaktif önlemeye kaydıran bir sistem oluşturmuştur.

Geçtiğimiz dört yıl içinde Kazakistan'ın gözetim altyapısının kapsamı önemli ölçüde genişlemiştir. Kamera sayısı 40.500'den 1,3 milyona ulaşmıştır ve 313.000 kamera artık doğrudan polisin erişimine açıktır. Bu kameralar kilit alanları izlemek üzere stratejik olarak konumlandırılmış olup, kolluk kuvvetlerinin olayları gerçek zamanlı olarak tespit etme, önleme ve müdahale etme kabiliyetini artırmaktadır. Sistem etkinliğini şimdiden göstermiştir: 2024 yılının başından bu yana 8.200'den fazla suç tespit etmiş ve 7,1 milyon trafik ihlali kaydederek kamu güvenliği ve yol yönetiminde önemli gelişmeler sağlamıştır.

Bu dönüşümün merkezinde yapay zeka kullanımı yer almaktadır. Sistem, yüz tanıma, plaka algılama ve kalabalık izleme gibi en son teknolojileri entegre ederek, yetkililerin riskleri tırmanmadan önce ele almasına olanak tanıyan eyleme geçirilebilir bilgiler sağlamaktadır. Örneğin, yüz tanıma özellikleri, ilgili kişilerin gerçek zamanlı olarak tespit edilmesini sağlarken, yapay zeka destekli trafik izleme, yol güvenliğinin artırılmasına katkıda bulunmakta ve para cezaları yoluyla kamu geliri sağlamaktadır. Bu özellikler, sistemin pasif kayıt yapmanın ötesine geçerek suç önleme ve kent yönetimi için dinamik bir araca dönüşme yeteneğini vurgulamaktadır.

Bir milyondan fazla yüksek çözünürlüklü kamera tarafından üretilen muazzam veri hacminin yönetilmesi, iletişim ağlarında ve veri depolama altyapısında önemli yükseltmeler yapılmasını gerektirmiştir. Kamu ve özel kamera ağlarının entegrasyonu, veri paylaşımı ve yönetimi için birleşik bir yaklaşım gerektirirken, gizlilik endişeleri de vatandaşların güvenini sağlamak için sağlam düzenleyici çerçeveler gerektirmektedir. Stratejik planlama, kamu-özel sektör ortaklıkları ve şeffaf iletişimin bir araya gelmesiyle Bakanlık bu engelleri başarıyla aşarak diğer ülkeler için bir model oluşturmuştur.

Projenin en önemli başarılarından biri caydırıcı etki oluşturmasıdır. Kamu düzenini bozma gibi idari suçların keskin bir şekilde azaldığı, böylece güvenlik kameralarının görünür varlığının davranışları etkilediği ortaya çıkmıştır. Bu da teknolojinin sadece olaylara tepki vermek için değil, onları tamamen önlemek için de kullanılabileceğini göstermektedir. Ayrıca, video kanıtlarının kullanımı vaka çözüm oranlarını artırarak sistemin kolluk kuvvetlerinin etkinliği üzerindeki etkisini daha da sağlamlaştırmıştır.

*İleriye dönük olarak Kazakistan, coğrafi kapsamını genişleterek ve analitik yeteneklerini artırarak Carpet CCTV'nin başarısını geliştirmeyi planl*amaktadır. Yeni gelişmeler, gözetimin doğruluğunu ve kapsamını iyileştirmek için gelişmiş yapay zekadan yararlanmaya odaklanırken, aynı zamanda sivil özgürlükleri korumak için uyarlanabilir gizlilik önlemlerini de içerecektir. Bu ileri görüşlü yaklaşım, sistemin kamu güvenliği teknolojisinin ön saflarında yer almasını ve yenilik ile hesap verebilirliği dengelemesini sağlamaktadır.[87]

87 https://www.computerworld.com/article/3623120/kazakhstans-carpet-cctv-pioneering-the-future-of-ai-powered-public-safety.html