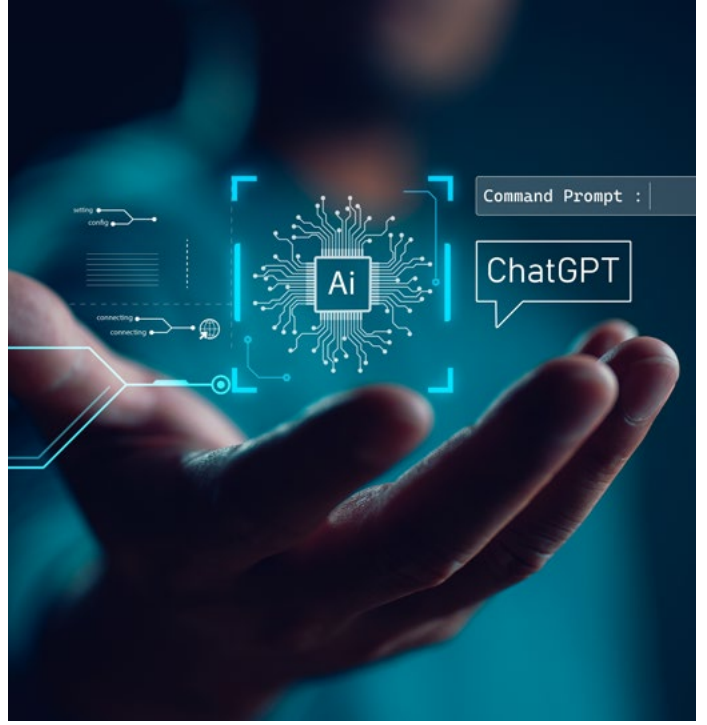


# ChatGPT ve Genel Olarak Yapay Zekânın Ulusal Güvenlik İçin Riskleri



Amerika Birleşik Devletleri (ABD) merkezli yapay zekâ araştırma şirketi OpenAI'nin diyalog konusunda uzmanlaşmış bir yapay zekâ (Artificial Intelligence -AI) sohbet robotu (chatbot) olan ChatGPT'yi (Chat Generative Pre-trained Transformer) 2022 yılının Kasım ayında kullanıma sunması, tüm dünyada yaşanan yapay zekâ çılgınlığını yeni boyutlara taşıdı. Makine öğrenmesi tekniklerini kullanan ChatGPT, insan konuşmalarını taklit etmenin ötesinde görevleri yerine getirebilen çok yönlü bir sohbet robotu olarak bilgisayar programları, müzik, tele-oyunlar ve kompozisyonlar yazabiliyor; test sorularını yanıtlayabiliyor, şiir ve şarkı sözleri yazabiliyor, bir Linux sistemini taklit ve bir sohbet odasını simüle edebiliyor, hatta oyun oynayabiliyor<sup>1</sup>.

İnsan benzeri konuşmalar yapmak, sorgu veya sorulara ayrıntılı yanıtlar üretmek için eğitilmiş olan ChatGPT aslında bir Geniş Dil Modelidir (Large Language Models -LLM). Başka bir deyişle, büyük veri kümelerinden elde edilen bilgilere dayanarak metin ve diğer içerikleri tanıyabilen, özetleyebilen, çevirebilen, tahmin edebilen ve üretebilen derin bir öğrenme algoritmasıdır.

14 Mart 2023'te OpenAI, GPT-4'ün lansmanını resmen duyurdu. İki sürüm arasındaki önemli bir fark, GPT-3.5 metinden metne (text to text) bir model iken, GPT-4'ün daha çok bir veriden metne (data to text) modeli olmasıdır. GPT-3.5 yaklaşık 3.000 kelimelik yanıtlarla sınırlı iken, GPT-4 25.000'den fazla kelimedenden oluşan yanıtlar üretebiliyor ve GPT-4'ün izin verilmeyen içerik isteklerine yanıt verme olasılığı sefine göre yüzde 82 oranında daha düşük. GPT-4 ayrıca daha fazla dil destekliyor ve geliştiricilerin AI'ın ayrıntı tarzına karar verebilmelerine izin veriyor. Şu anda, ChatGPT 3.5 2021'den sonraki dünya hakkında çok sınırlı bilgiye sahip ve bu nedenle son veya gerçek zamanlı olaylarla ilgili soruları cevaplayamıyor<sup>2</sup>.

## ChatGPT'nin Çalışma Tarzı

Temel olarak, LLM'ler, bir cümlede hangi kelimenin daha sonra geleceğini doğru bir şekilde tahmin etmek için büyük miktarda veri ile eğitiliyor. ChatGPT modelinin, kitaplardan, Wikipedia'dan, araştırma makalelerinden, web sitelerinden, diğer içerik biçimlerinden ve internetteki yazılardan elde edilen 570 GB'lık büyük bir veriyi içeren veritabanları kullanılarak eğitildiği söyleniyor. Sisteme girildiği bildirilen kelime sayısı ise yaklaşık 300 milyar.

İngilizce diline ek olarak ChatGPT, Fransızca, İspanyolca, Almanca ve Çince de dahil olmak üzere dünya çapında konuşulan 95 dili anlıyor. ChatGPT modeli yanlış bilgi, tekrarlar veya alışılmadık kelime ve kelime

<sup>1</sup> <https://tr.wikipedia.org/wiki/ChatGPT>

<sup>2</sup> <https://www.linkedin.com/pulse/national-security-cyber-risks-geopolitical-career-chatgpt-don-okereke/>

kombinasyonları üretebiliyor. Bunun nedeni olarak, ChatGPT gibi büyük dil modellerinin, akıcı ve tutarlı metinler üretmek için eğitilmiş olmakla beraber, her zaman bir insan tarafından yazılanlar kadar yaratıcı yanıtlar üretememeleri gösteriliyor<sup>2</sup>.

### **ChatGPT'nin Sıradışı İstatistikleri**

ChatGPT, 2023'ün Ocak ayında, yani sadece iki ay içinde 100 milyon aktif kullanıcı sayısına ulaşarak internet tarihinin en hızlı büyüyen çevrimiçi hizmeti oldu<sup>3</sup>. Üstelik similarweb'in web trafiği verilerine göre, uygulama 12 Ağustos 2023 itibarıyla 1,9 milyar sayfa ziyaretini aşmış durumda<sup>4</sup>. ABD en fazla sayıda ChatGPT kullanıcısına sahip ve toplamın yüzde 15,73'ünü oluşturuyor. Hindistan yüzde 7,10 ile ikinci sırada yer alıyor. 14 Mart 2023 itibarıyla Çin yüzde 16,58 ile 20'nci, Nijerya yüzde 12,24 ile 24'üncü, Güney Afrika ise yüzde 12,63 ile 41'inci sırada yer alıyor<sup>2</sup>. ChatGPT'nin ana şirketi OpenAI'nin piyasa değerinin yaklaşık 29 milyar dolar değerinde olduğu belirtiliyor<sup>5</sup>.

### **ChatGPT'nin Tetiklediği Rekabet**

ChatGPT viral hâle geldikten sonra, dünyanın dört bir yanındaki büyük teknoloji şirketleri üretken yapay zekâyı devreye almak için çalışmaya başladı. ChatGPT'nin piyasaya sürülmesinin arama motoru işini bozabileceği yönündeki spekülasyonların ardından Google'ın, kurucuları Sergey Brin ve Larry Page'i şirkete geri çağırdığı açıklandı<sup>6</sup>. Kısa bir süre sonra Google, Diyalog Uygulamaları için Dil Modeli (Language Model for Dialogue Applications -LaMDA) tarafından desteklenen Bard adı verilen deneysel bir AI destekli chatbot'u piyasaya sürdü. Google'ın, popüler Google Lens ve yeni çoklu arama özelliği de dahil olmak üzere arama özelliklerini geliştirmek için AI kullandığı söyleniyor. Google'ın ana şirketi Alphabet, arama motorunun yeni chatbot'u Bard'ın bir demo sırasında James Webb teleskobu hakkındaki bir soruyu yanlış yanıtlamasından sonra 163 milyar dolar değer kaybetti<sup>7</sup>. Öte yandan Google Deepmind, üzerinde çalıştığı Gemini adlı yeni araç ile OpenAI ile arasındaki üretken yapay zekâ yarışımı kızıştırıyor. Gemini'nin ChatGPT'den iki kat güçlü olacağı iddia ediliyor<sup>8</sup>.

Microsoft da kısa süre önce ChatGPT teknolojisini Microsoft 365 -Word, Excel, PowerPoint ve Outlook- ürün yelpazesine dahil etti. Apple, Meta (Facebook'un ana şirketi) ve Amazon, rekabette zor durumda kalmamak için üretken yapay zekâlarını kullanmaya devam ediyor. Microsoft Bing'in yanı sıra, Google'a kök söktüren diğer AI destekli arama motorları arasında Wolfram Alpha, You.Com, Perplexity AI, Andi, Metaphor ve Neeva yer alıyor<sup>2</sup>.

Çinli şirket Baidu da, kendi AI destekli chatbot'unu piyasaya sürmeye hazırlanıyor. Başka bir Çinli e-ticaret platformu olan Alibaba da ChatGPT tarzı DAMO (Discovery, Adventure, Momentum, and Outlook -Keşif, Macera, Momentum ve Görünüm) adlı AI dil modelini geçtiğimiz günlerde tanıttı<sup>2</sup>.

### **ChatGPT'ye Giden Yol**

Makinelerin insan dilini anlamalarına yardımcı olarak yazım denetimleri gibi basit görevleri yerine getirmelerini sağlayan günümüz Doğal Dil İşleme (Natural Language Processing -NLP) tekniklerinin temelini atan, yabancı dil belgelerinin çevirisini yapan programlar oldu.

Soğuk Savaş'ın sonlarına doğru AI güdümlü sistemler, bilgileri analiz ederek ve bunu tahminlerde bulunmak için kullanarak, olası terör hedeflerinin belirlenmesinde güvenlik kuruluşlarına yardımcı olmak amacıyla geliştirildi. Bu sistemler uzmanların görüntü analizi için karar vermelerini kolaylaştırmayı hedefliyor<sup>9</sup>.

3 <https://www.forbes.com/sites/cindygordon/2023/02/02/chatgpt-is-the-fastest-growing-ap-in-the-history-of-web-applications/>

4 <https://www.similarweb.com/website/chatgpt.com/#overview>

5 <https://techcrunch.com/2023/04/28/openai-funding-valuation-chatgpt/>

6 <https://www.nytimes.com/2023/01/20/technology/google-chatgpt-artificial-intelligence.html>

7 <https://www.theguardian.com/technology/2023/feb/10/google-v-microsoft-who-will-win-the-ai-chatbot-race-bard-chatgpt>

8 <https://shiftdelete.net/google-gemini-yapay-zeka>

9 <https://theconversation.com/intelligence-agencies-have-used-ai-since-the-cold-war-but-now-face-new-security-challenges-204320>

## ChatGPT Nasıl Yayıldı?

ChatGPT bir anda en popüler uygulamalar listesinde zirveye tırmanırken akademisyenlerden siyasi liderlere ve iş dünyasının önde gelen temsilcilerine kadar her kesimden farklı tepkiler alıyor. İsrail Cumhurbaşkanı Isaac Herzog, Şubat 2023'te bir konuşmasının açılış bölümünün ChatGPT tarafından yazıldığını açıkladı<sup>10</sup>. ChatGPT, Bill Gates ve İngiltere Başbakanı Rishi Sunak ile sorularını kendisinin hazırladığı bir röportaja da imza attı<sup>11</sup>.

2015 yılında ChatGPT'nin çatı şirketi OpenAI'ı kuran SpaceX'in ve Tesla'nın CEO'su ve Twitter'ın yeni sahibi Elon Musk da şu sıralar ChatGPT'ye rakip olacak "xAI" adında yeni bir AI girişimini dünyaya tanıtmakla meşgul<sup>12</sup>.

Bazı şirketler şimdiden ChatGPT ve Midjourney gibi AI programlarını kullanmayı bilen kişiler için iş ilanları vermeye başlamış durumda. Hatta ChatGPT kullanımı ders olarak okutulmaya başlandı. Arizona Eyalet Üniversitesinin Toplumda İnovasyonun Geleceği Fakültesinden (Arizona State University School for the Future of Innovation in Society)<sup>13</sup> Prof. Dr. Andrew Maynard, öğrencilerine ChatGPT'yi verimli şekilde kullanma konulu bir ders vermeye başladı. Prompt Engineering olarak adlandırılan bu derste öğrencilere, ChatGPT ve benzeri AI programlarından en iyi sonuçları almak için doğru komutların nasıl verileceği öğretiliyor<sup>14</sup>. ChatGPT kısa zamanda yetenekleri arasına arabuluculuğu da katmayı başardı. Alman yayın organı Berliner Zeitung ChatGPT'ye, Almanya Başbakanı Olaf Scholz adına Vladimir Putin ve Vladimir Zelensky'ye barış çağrısı yapan mektuplar yazdırdı ve ChatGPT Rusya ile Ukrayna arasında bir barış antlaşması taslağı hazırladı<sup>15</sup>.

Tabii birçok şirket de ChatGPT'ye karşı önlem almakta gecikmedi. Örneğin bazı çalışanlarının şirketin hassas verilerinin ve kodlarının yanlışlıkla ChatGPT'nin eline geçmesine yol açtığı Samsung, çalışanlarını ChatGPT'yi dikkatli kullanmaları konusunda uyardığını açıkladı. Samsung'un ardından Apple da çalışanlarının ChatGPT ve benzeri üretken yapay zekâ araçlarını kullanmalarını yasakladı. Apple ayrıca GitHub tarafından geliştirilen CoPilot'un da kullanımını yasakladı. Apple'ın ChatGPT'yi yasaklamasının sebebinin, kendi AI platformunu geliştiriyor olmasından kaynaklandığı belirtilirken, Samsung da ChatGPT'yi yasakladıktan sonra kendi AI platformunu kurmak için harekete geçti<sup>16</sup>. "Kuruluşlar için, herhangi bir çalışan ChatGPT'ye veri besledikçe risk yoğunlaşıyor" diyen CODE42 şirketinde CIO olarak görev yapan Jadee Hanson, Samsung olayını şöyle yorumluyor: "ChatGPT ve AI araçları inanılmaz derecede yararlı ve güçlü olabilir, ancak çalışanların ChatGPT'ye hangi verilerin yüklenmesinin uygun olup olmadığını anlamaları gerekir ve bilgi işlem ekiplerinin kuruluşun ChatGPT'ye ne gönderdiğine dair uygun görünürlüğe sahip olmaları gerekir. Yeni güçlü teknolojik gelişmelerle birlikte, kuruluşlarımızı korumak için anlamamız gereken riskler ortaya çıkıyor. Örneğin rekabetin şiddetli olduğu yarı iletken endüstrisinde, her türlü veri sızıntısı söz konusu şirket için felaket anlamına gelebilir."

## ChatGPT'nin Faydaları ve Dezavantajları

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, hazırladığı "Chatbot Uygulamaları ve ChatGPT Örneği" başlıklı bir raporla ChatGPT'nin faydalarını ve kısıtlarını değerlendirdi. Raporda, konuşmaları otomatikleştirerek verimliliği artırmak, geliştirilmiş doğruluk teknolojisi ve zaman içinde geliştirilebilir olması sayesinde yüksek maliyetli manuel güncellemelere olan ihtiyacı azaltarak sağlayacağı maliyet tasarrufu ChatGPT'nin faydaları arasında sayılıyor. ChatGPT'nin kısıtları ve dezavantajları ise yol açabileceği dezenformasyon tehlikesi ve yeteneklerinin henüz sınırlı olması olarak sıralanıyor<sup>17</sup>.

<sup>10</sup> <https://www.businessinsider.com/chatgpt-used-by-israeli-president-write-speech-at-cybersec-event-2023-2>

<sup>11</sup> <https://www.youtube.com/watch?v=fp6WHlq7qpg>

<sup>12</sup> <https://www.cnbc.com/2023/07/12/elon-musk-launches-his-new-company-xai.html>

<sup>13</sup> <https://www.top-mastersdegree.com/institutions/arizona-state-university-school-for-the-future-of-innovation-in-society>

<sup>14</sup> <https://tele1.com.tr/chatgpt-kullanimi-ders-olarak-okutulmaya-baslandi-888921/>

<sup>15</sup> <https://newsunrolled.com/world/215711.html>

<sup>16</sup> <https://www.tgrthaber.com.tr/teknoloji/apple-calisanlarina-chatgpt-yasaklandi-neden-2888751>

<sup>17</sup> [https://cbddo.gov.tr/SharedFolderServer/Genel/21.Chatbot-Uygulamas%C4%B1-ve-ChatGPT-%C3%96rne%C4%9Fi-Değerlendirme-Raporu.pdf](https://cbddo.gov.tr/SharedFolderServer/Genel/21.Chatbot-Uygulamas%C4%B1-ve-ChatGPT-%C3%96rne%C4%9Fi-De%C4%9Feri-Değerlendirme-Raporu.pdf)

Günümüzde bir çok ülkede sosyal medya üzerinden yürütülen mikropropaganda teknikleri politik destabilizasyon amaçlı olarak kullanılabilir. Bu tür mikropropaganda yöntemleri, içerisinde doğrular da bulunan ve bu nedenle tespiti zor olan yalan haberleri kamuoyu oluşturma amacıyla kullanılabilir. Bu kapsamda sivil toplumun bir etki aracı olarak kullanılmasından halkın devlete karşı güvenini sarsmaya ve isyanları teşvik etmeye kadar birçok amaç için kullanışlı bir yaklaşım olarak değerlendiriliyor. Mikropropagandalar, aynı anda farklı on binlerce propaganda haberini üreterek küçük hedef kitleleri sosyal medya üzerinden yönlendirebiliyor ve toplamda önemli bir etki yaratabiliyor. Bu büyüklükteki mikropropagandaların üretilmesinde çok sayıda insan gücü gerekiyor. Buna karşın ChatGPT ve benzeri akıllı metin üreticileri sayesinde kitleleri etkileyebilecek propaganda metinlerinin üretilmesi yakın gelecekte mümkün olabilecek.

Brexit ve ABD seçimlerindeki Cambridge Analytica deneyimine bakıldığında bir günde binlerce mikropropagandanın üretilerek iletişim araçları üzerinden hedef kitlelere yayıldığı biliniyor. Bu faaliyet ChatGPT yardımıyla çok daha hızlı ve geniş kapsamda gerçekleştirilebilirdi.

ChatGPT'nin ulusal güvenlik konusunda kötü amaçlarla kullanılması konusunda kendisi ile bir röportaj yaptık.

**Soru:** ChatGPT'nin milli güvenlik konusunda kötü amaçlı kullanımına dair riskler nelerdir?

**ChatGPT:** ChatGPT gibi yapay zekâ modellerinin milli güvenlik konusunda kötü amaçlı kullanımına dair bazı riskler şunlar olabilir:

- 1. Bilgi Toplama ve Analiz:** Kötü niyetli aktörler, ChatGPT'yi kullanarak sosyal medya ve diğer online platformlardan büyük miktarda bilgi toplayabilir ve analiz edebilirler. Bu bilgileri, hedeflenen kişilerin veya grupların davranışlarını, düşüncelerini veya zayıf noktalarını anlamak için kullanabilirler.
- 2. Sosyal Mühendislik:** ChatGPT, ikna edici konuşma yetenekleriyle, hedeflenen bireyleri veya grupları manipüle etmek için kullanılabilir. Kötü niyetli aktörler, sahte veya aldatıcı mesajlar oluşturarak insanları yanıltabilir ve istenmeyen eylemler yapmaya ikna edebilirler.
- 3. Propaganda ve Yalan Haber Yayma:** ChatGPT kullanılarak oluşturulan içerikler, propagandist amaçlar için kullanılabilir. Sahte haberler, yanıltıcı bilgiler veya aşırı ideolojileri yaymak için ChatGPT'yi kullanmak, kamuoyunu etkileyebilir ve iç karışıklıklara neden olabilir.
- 4. Siber Saldırıları:** Kötü niyetli aktörler, ChatGPT'yi kullanarak kişisel veri hırsızlığı, kimlik avı veya kötü amaçlı yazılımların yayılması gibi siber saldırılarda daha sofistike ve ikna edici taktikler kullanabilirler.
- 5. Hedeflenmiş Sosyal Mecralar ve Platformlarda Kötüye Kullanım:** ChatGPT, sosyal medya platformlarında veya forumlarda otomatik olarak sahte hesaplar veya sahte içerikler oluşturmak için kullanılabilir. Bu tür hesaplar, troller veya propagandacılar aracılığıyla halkın düşüncelerini manipüle edebilir.
- 6. Sosyal Huzursuzluk:** ChatGPT'yi kullanarak oluşturulan içerikler, insanlar arasında ayrışma, önyargı veya aşırılığı artırabilir, bu da toplumsal huzursuzluğa ve istikrarsızlığa neden olabilir.

Bu riskler, yapay zekâ teknolojilerinin milli güvenlik açısından olumsuz şekilde kullanılmasının potansiyel sonuçlarını yansıtır. Bu nedenle, yapay zekâ geliştiricileri, platform sağlayıcıları ve düzenleyiciler, bu tür riskleri azaltmak için etkili önlemler almalıdır. Düzenleme, eğitim, moderasyon ve diğer önlemler, yapay zekâ teknolojilerinin olumlu ve etik bir şekilde kullanılmasını sağlamak için önemlidir.

**Soru:** Kötü amaçlı ve milli güvenliği tehlikeye atabilecek mikropropaganda yöntemleri ve ChatGPT ile ilgili neler söylemek istersin?

**ChatGPT:** Kötü amaçlı ve milli güvenliği tehlikeye atabilecek mikropropaganda yöntemleri, ChatGPT gibi yapay zekâ modellerinin kullanımıyla birlikte daha sofistike hâle gelebilir. İşte bu konuda dikkate alınması gereken bazı noktalar:

- 1. Sahte Kimlikler ve Otomatik Üretim:** ChatGPT gibi araçlar, sahte kimlikler ve içerikleri otomatik olarak

oluşturmak için kullanılabilir. Bu, sosyal medya platformlarında, forumlarda veya diğer çevrimiçi mecralarda sahte hesaplar ve içerikler oluşturarak yanıltıcı veya manipülatif amaçlar için kullanılabilir.

**2. Bireyselleştirilmiş İletişim:** ChatGPT, kullanıcılarla bire bir iletişim kurabileceği için, hedeflenen bireylere veya gruplara özelleştirilmiş mesajlar göndermek için kullanılabilir. Bu, manipülatif içeriklerin daha etkili bir şekilde iletilmesini sağlayabilir.

**3. Dil ve İfade Kullanımı:** ChatGPT, insan gibi doğal dil kullanımına sahip olduğu için, duygusal dil veya ikna edici ifadelerle donatılmış içerikler üretmek için kullanılabilir. Bu tür içerikler, insanların düşüncelerini etkileyebilir ve istenmeyen davranışlara yol açabilir.

**4. Hızlı ve Yayılabilir İçerikler:** ChatGPT, büyük miktarda içeriği hızlı bir şekilde üretebilir. Bu, sahte haberler, spekülasyonlar veya yanıltıcı içeriklerin hızla yayılmasına ve toplumun tepkisini hızla etkilemesine yol açabilir.

**5. Sosyal Mecralarda Manipülasyon:** ChatGPT, sosyal medya platformlarında veya forumlarda manipülatif içerikler üretmek için kullanılabilir. Bu, insanların farkında olmadan manipüle edilmesine neden olabilir.

Bu riskleri yönetmek ve engellemek için şunlar yapılabilir:

**1. Düzenlemeler ve Yönergeler:** Platform sağlayıcıları, içerik üretimini düzenlemek ve kötü amaçlı kullanımı engellemek için kurallar ve yönergeler belirlemelidir.

**2. Doğruluk ve Kaynak Kontrolü:** Kullanıcılar, kendilerine iletilen bilgileri sorgulayarak doğruluklarını ve kaynaklarını kontrol etmelidir.

**3. Eğitim ve Farkındalık:** Kullanıcılar, manipülatif içerikler ve mikropropaganda yöntemleri konusunda eğitilmeli ve farkındalık kazanmalıdır.

**4. Moderasyon ve İzleme:** Platformlar, içerikleri izlemeli ve sahte hesapları veya yanıltıcı içerikleri tespit etmek için moderasyon mekanizmaları geliştirmelidir.

**5. Transparan Algoritmalar:** Sosyal medya platformları, algoritmalarını daha şeffaf bir şekilde açıklamalı ve kullanıcıların içeriklere nasıl maruz kaldığını anlamalarını sağlamalıdır.

Sonuç olarak, ChatGPT gibi yapay zekâ modellerinin potansiyel kullanım alanları geniş olsa da, bu teknolojilerin olumsuz amaçlarla kötüye kullanılma riskleri de vardır. Toplum, geliştiriciler ve platform sağlayıcıları, bu riskleri tanımak ve önlemek için işbirliği yapmalı ve ChatGPT'nin etik kullanımını teşvik etmelidir.

**Soru:** Cambridge Analytica'nın Brexit ya da ABD seçimlerinde kullandığı mikropropaganda yöntemlerinde ChatGPT de bir araç olarak kullanılsaydı sonuç ne olurdu?

**ChatGPT:** ChatGPT gibi yapay zekâ araçlarının mikropropaganda yöntemleriyle birleştirilmesi, propaganda ve manipülasyonun daha sofistike bir seviyede gerçekleşmesine olanak sağlayabilirdi. Bu, kampanyaların daha etkili ve geniş kapsamlı bir şekilde hedeflenen kişilere ulaşmasına ve toplumsal etkilerin artmasına yol açabilir. Bu tür bir kullanım, toplumun düşüncelerini etkileme ve demokratik süreçlere müdahale riskini artırabilir. Bu nedenle, etik ve sorumlu yapay zekâ kullanımı önemlidir ve platform sağlayıcıları, geliştiriciler ve düzenleyiciler, bu tür riskleri en aza indirmek için işbirliği yapmalıdır.

Ülkemizde sohbet robotları ve ChatGPT'nin faydalı amaçlarla kullanımı ile ilgili çeşitli akademik çalışmalara rastlamak mümkündür. Bu çalışmalar çoğunlukla eğitim, yabancı dil öğrenme, genel trendlerin yorumlanması, çeşitli konularda yapılan sohbetlerin sunulması vb. konulara odaklanmıştır. STM tarafından yapılan bir çalışmada, depremin hemen sonrasında atılan tweet'lerin yardım isteği, aciliyet, ihtiyaçlar gibi konularda sınıflandırılması konusunda yapay öğrenme modellerinin kullanabileceği bir etiketli veri seti sunulmuştur. Diğer taraftan ChatGPT ile ilgili olası milli güvenlik risklerine değinen bir çalışmaya rastlanmamıştır. Benzer şekilde YÖK tez merkezinde yapılan taramada da gelişmiş sohbet robotları ve ChatGPT'nin milli güvenlik risklerine yönelik bir çalışmaya rastlanmamıştır.



## ChatGPT ve Yapay Zekânın Savunma ve İstihbarat Alanında Kullanımı

ChatGPT'nin belki de en önemli etkisi savunma, istihbarat ve ulusal güvenlik alanlarında yaşanıyor. Kısa sürede yetenekleriyle tüm dünyada ilgi odağı olan ChatGPT'nin ülkelerin ulusal güvenliklerine yönelik ciddi tehditler oluşturduğuna dair dünya kamuoyunda giderek yayılan bir tartışma tetiklenmiş durumda. Siyaset ve iş dünyasındaki yaklaşımlara benzer şekilde, farklı ülkelerin savunma ve istihbarat yetkilileri de ChatGPT ile farklı bir boyuta ulaşan AI'nin kendi alanlarındaki etkileri konusunda farklı fikir ve öngörülere sahip görünüyor. Bir grup ChatGPT'den fayda sağlanacağına inanırken, diğer bir grup ise ChatGPT'nin çok ciddi güvenlik tehditlerine yol açacağını savunuyor. Örneğin, ABD Savunma Bakanlığı (DoD), insansız hava sistemlerinin yarattığı tehdidi önlemek için teknolojileri kullanan yeni bir görev gücü hakkında bir basın açıklaması yazmak için ChatGPT'yi görevlendirdi<sup>18</sup>. ABD Savunma Bilgi Sistemleri Ajansı (DISA) Direktörü Korgeneral Robert Skinner, Armed Forces Communications & Electronics Association International'ın (AFCEA)<sup>18</sup> düzenlediği bir konferanstaki açılış konuşmasının başında sesini klonlamak için üretken yapay zekâ kullandı. "Üretken yapay zekâdan korkmuyorum" diyen Skinner, üretici AI'dan yararlananların ve aynı zamanda ondan en iyi şekilde nasıl korunacaklarını anlayabilenlerin, avantaj sahibi olacağına inanıyor<sup>19</sup>. Skinner, bu teknolojiyi geliştirmeyi durdurma çağrılarında da şöyle yanıt veriyor: "Bunun hasım aktörlerle teknoloji yarışını nasıl etkileyeceğine bakmamız lazım. Yapmakta olduğumuz araştırmayı duraklatmanın hata olacağını düşünüyorum, çünkü düşmanlarımız bunu yapmayacak<sup>18</sup>."

ABD Merkezi İstihbarat Teşkilatı (CIA) Yapay Zekâ Direktörü Lakshmi Raman da, ChatGPT'yi teknolojiye bir dönüm noktası olarak tanımlarken, "Yeni ve yaklaşmakta olan teknolojilerden yararlanabileceğimiz yolları kesinlikle keşfetmemiz gerekiyor" görüşünü paylaşıyor<sup>20</sup>.

21'inci yüzyılın getirdiği olağanüstü teknolojik dönüşümler çağında dünya çapında ulusal ve uluslararası güvenlik alanında çalışan kuruluşlar, ele aldıkları bilgilerin doğruluğunun sağlanması için yenilikçi yollar bulmalarına yardımcı olmak için AI'ı kullanıyor. Bunun nedenlerinin başında, bütçe kısıtlamalarının, insani sınırlamaların ve artan bilgi seviyelerinin istihbarat kurumlarının politika yapımcılar için yeterince hızlı analiz üretmesini neredeyse imkânsız hâle getirmesi yatıyor.

2019 yılında ABD'nin istihbarat operasyonlarını denetleyen Ulusal İstihbarat Müdürlüğü, bilgisayarlarını kullanarak istihbarata katkıda bulunmak, CIA gibi kurumların büyük miktarda veriyi daha hızlı işlemesini sağlamak ve insan istihbaratı görevlilerinin diğer görevlerle daha fazla ilgilenmesini mümkün kılmak için tasarlanmış bir strateji olan "AIM Girişimi (The AIM Initiative A Strategy For Augmenting Intelligence Using Machines)"<sup>21</sup> adlı bir belge yayınladı. AI hâlihazırda istihbarat kurumlarının çok çeşitli kaynaklardan gelen çok miktarda veriyi işlemesine ve analiz etmesine yardımcı oluyor ve bunu insanlardan daha hızlı ve verimli bir şekilde yapıyor. AI, verilerdeki kalıpları tanımlayabiliyor ve insan istihbaratı görevlilerinin tespit etmesinin zor olabileceği anormallikleri de tespit edebiliyor. İstihbarat ajansları, internet üzerinden iletişim kurmak, siber saldırılara yanıt vermek ve ağlardaki olağandışı davranışları tanımlamak için kullanılan teknolojiye yönelik potansiyel tehditleri tespit etmek için de AI kullanabiliyor. AI bu sayede olası kötü amaçlı yazılımlara karşı harekete geçebiliyor ve daha güvenli bir dijital ortama katkıda bulunabiliyor.

Örneğin ChatGPT, Açık Kaynak İstihbaratı (Open-Source Intelligence -OSINT) araştırmalarında devrim yaratan inanılmaz derecede güçlü bir araç olarak değerlendiriliyor. ChatGPT, veri toplama, analiz etme ve çeşitli kaynaklardan gelen büyük miktarda yapılandırılmamış metin verisinden bilgi elde etme gibi tekrar eden görevleri otomatikleştirebilir ve böylece araştırmaları daha verimli ve etkili hâle getirebilir. Bu da,

18 <https://www.afcea.org/signal-media/chatgpt-we-trust>

19 <https://www.globalgovernmentforum.com/agencies-dont-have-the-tools-to-head-off-chatgpt-threat-to-national-security-warns-pentagons-ai-chief/>

20 <https://theintercept.com/2023/05/08/chatgpt-ai-pentagon-military/>

21 <https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf>

araştırmacıların bilgileri doğrulamak için gerçekten neyin önemli olduğuna odaklanmalarını sağlar. Ek olarak, ChatGPT sosyal ağ analizi, bireyler ve kuruluşlar arasında potansiyel bağlantılar oluşturmak için kullanılabilir. Örneğin, bir araştırmacı ChatGPT'ye çevrimiçi varlıklarına ve etkileşimlerine dayanarak bireyler ve kuruluşlar arasındaki bağlantıları bulması ve bunları listelemesi talimatını verebilir. Google Hacking olarak da bilinen Google Dorking, OSINT araştırmalarındaki dedektifler tarafından gelişmiş arama operatörlerini kullanarak internette belirli bilgileri aramak için kullanılan bir tekniktir. Bu teknik, araştırmacıların bir web sitesinin belirli bölümlerini aramasına veya arama sonuçlarını belirli bir dosya türüne daraltmasına olanak tanır. Araştırmalar, Birleşmiş Milletler barış operasyonlarında istihbarat ve analiz kuruluşları tarafından işlenen bilgilerin yüzde 80'inin halka açık bilgilerden veya genel olarak açık kaynaklı istihbarattan kaynaklandığını gösteriyor. Bu da OSINT'i diğer istihbarat disiplinlerine önemli ölçüde hâkim bir disiplin hâline getiriyor<sup>2</sup>.

### **ChatGPT'nin Ulusal Güvenliğe Yönelik Tehditleri**

AI, ağların siber saldırılardan korunmasına yardımcı olmak gibi amaçlarla kullanılırken, düşman birey veya kurumlar tarafından güvenlik açıklarına saldırmak, kötü amaçlı yazılım yüklemek, bilgi çalmak veya dijital sistemlerin kullanımını bozmak ve reddetmek için de kullanılabilir. Zira NATO Müttefik Dönüşüm Komutanlığı Siber Uzay Teknoloji Direktörü Alberto Domingo, AI siber saldırılarının kritik bir tehdit hâline geldiğine dikkat çekerek, katlanarak artan saldırıları azaltmak için uluslararası düzenlemeler yapılması çağrısında bulunuyor.

İngiliz iç istihbarat kurumu MI5 Genel Direktörü Ken McCallum da İngiltere'nin, ipuçları her zamankinden daha fazla parçalanmış verilerde gizlenmiş olan daha geniş ve daha karmaşık bir tehdit yelpazesine karşı karşıya olduğuna dikkat çekiyor. Örneğin; AI görüntüleri taramak, önceliklendirmek ve tehlikeli silahları tanımlamak için kullanılabilir. Bu bağlamda, MI5, "İngiltere'ye yönelik yeni anlayışlar sağlamak, ulusal güvenlik zorluklarıyla yüzleşmek ve bu zorlukları hafifletmek için AI ve veri bilimini uygulamayı" amaçlayan Alan Turing Enstitüsü ile ortaklık kuruyor<sup>9</sup>.

ChatGPT gibi AI uygulamalarının ülkelerin güvenliklerine yönelik benzersiz bir tehdit olduğunu düşünenler yasaklamalara varacak kadar sıkı tedbirler dahi öneriyor<sup>9</sup>. Özellikle Çin, Rusya, Afganistan, İran, Venezuela, Kuzey Kore gibi otoriter rejimler, internet kullanımını izlemek, jeopolitik ve ulusal güvenlik endişeleri nedeniyle ChatGPT kullanımını kısıtlamak için sansür ve gözetim uyguluyor. Çin bu grupta liderliği elinde tutuyor. Japonya'nın Nikkei haber servisi, Çinli teknoloji devleri Tencent ve Ant Group'a platformlarında ChatGPT hizmetlerini doğrudan veya dolaylı olarak kullanmamalarının söylendiğini, çünkü Pekin'de AI destekli chatbot'un kullanıcı sorgularına sansürsüz yanıtları konusunda artan bir alarm durumu olduğunu bildirdi<sup>2</sup>.

İtalya da kısa süre önce, bilgileri izinsiz kullanma kabiliyeti nedeniyle gizlilikle ilgili endişeleri gerekçe göstererek ChatGPT'nin en son sürümünü yasakladı. İngiltere'nin istihbarat, güvenlik ve siber güvenlik ajansı Hükümet İletişim Merkezinin (Government Communications Headquarters -GCHQ) bir kolu olan Ulusal Siber Güvenlik Merkezinden (National Cyber Security Centre -NCSC) siber güvenlik uzmanları, ChatGPT gibi akıllı sohbet robotlarının bir güvenlik tehdidi oluşturduğunu, çünkü hassas sorguların saldırıya uğrayabileceğini veya sızdırılabileceğini belirtiyor<sup>9</sup>. GCHQ, Microsoft ve Google gibi teknolojiyi kullanan şirketlerin chatbot'lara yazılan soruları okuyabildiğini söylüyor<sup>2</sup>.

Alman Hükümetinin Federal Veri Koruma ve Bilgi Özgürlüğü Komiseri Ulrich Kelber, Almanya'nın veri güvenliği endişeleri nedeniyle ChatGPT'yi engelleyerek İtalya'nın izinden gidebileceğini ve İtalya'dan bu konu hakkında bilgi talep ettiğini söyledi. Avrupa Birliği'nin de (AB) "Avrupa AI Yasası" olarak bilinen kanunlarla, AI'nın kritik altyapı, eğitim, kolluk kuvvetleri ve yargı sisteminde kullanımını büyük ölçüde kısıtlaması bekleniyor. Reuters'e göre, AB'nin bu konudaki taslak kanunu, ChatGPT'yi yüksek riskli uygulamalarda kullanılan genel amaçlı bir AI biçimi olarak görüyor. Yüksek riskli AI sistemleri, AB Komisyonu tarafından insanların temel haklarını veya güvenliğini etkileyebilecek sistemler olarak tanımlanıyor.

AI'ya dair yapılacak regülasyon planlarını açıklayan ülkelerden biri de İngiltere. ChatGPT'den ismen bahsetmeyen İngiltere'nin tasarısı, şirketlerin AI'ı ürünlerinde kullanırken izlemesi gereken güvenlik, şeffaflık, adalet, hesap verebilirlik ve itiraz edilebilirlik dahil olmak üzere bazı temel ilkelerin ana hatlarını belirliyor. İngiltere şu aşamada ChatGPT veya bu konuda herhangi bir AI için kısıtlamalar tasarlamıyor. Bunun yerine, şirketlerin AI araçlarını sorumlu bir şekilde geliştirmesini, kullanmasını ve kullanıcılara belirli kararların nasıl ve neden alındığı hakkında yeterli bilgi vermesini istiyor.

ChatGPT'ye yönelik somut bir yasak getirmese de genel olarak AI'nın risklerine karşı en etkili girişimlerde bulunan ülkelerin başında ABD geliyor. 2022'de ABD Başkanı Joe Biden, vatandaşları "Amerikan halkının haklarını tehdit eden" otomatik sistemlerden korumak için bir "AI Haklar Bildirgesi (AI Bill of Rights)" oluşturma planlarını açıklamıştı<sup>19</sup>. Bu çaba çerçevesinde ABD yönetimi, yapay zekânın risklerini azaltmak için yedi yeni ulusal yapay zekâ araştırma enstitüsüne 140 milyon dolar yatırım yapma planını duyurdu<sup>22</sup>.

Bu girişimlerin ardından ABD Başkan Yardımcısı Kamala Harris, Mayıs 2023'te AI'nın sorumlu gelişimini ve hükümetin özel sektörün AI etrafındaki riskleri azaltmasına yardımcı olma konusundaki rolünü tartışmak için teknoloji şirketleri Alphabet, Anthropic, Microsoft ve OpenAI'nın CEO'larıyla bir araya geldi. Beyaz Saray, toplantının Biden yönetiminin teknoloji hakkında uzmanlarla iletişim kurma ve AI ürünlerinin halka dağıtılmadan önce güvenli olmasını sağlama konusundaki geniş çabasının bir parçası olduğunu açıkladı<sup>23</sup>. Önümüzdeki aylarda, ABD Yönetim ve Bütçe Ofisi (The Office of Management and Budget -OMB), federal kurumlara AI araçlarının en iyi nasıl kullanılacağına dair rehberlik etmeyi de planlıyor.

ABD Kongre Üyesi Ted Lieu da 2023'ün Haziran ayında *New York Times*'ta "AI ve toplumu ilerletmeye devam edeceği inanılmaz yollar" hakkında bir makale yazsa da AI ve özellikle kontrolsüz ve düzensiz AI hakkında çok endişeli" olduğunu söylemekten geri kalmadı<sup>24</sup>.

AI teknolojisine gözetim getirmek için henüz herhangi bir resmi kanun tasarısı önerisinde bulunmayan ABD'nin Ulusal Bilim ve Teknoloji Enstitüsü, AI sistemlerini kullanan, tasarlayan veya dağıtan şirketlere riskleri ve potansiyel zararları yönetme konusunda rehberlik sağlayan ulusal bir çerçeve ortaya koydu. Ancak bu çerçeve gönüllülük esasına dayanıyor, yani firmalar kurallara uymadıkları için hiçbir sonuçla karşılaşmıyor<sup>25</sup>. Yine de ChatGPT ABD'de bazı eyaletlerde sınırlı düzeyde engellemelerle karşılaşılıyor. Örneğin New York City Eğitim departmanı öğrencilerin öğrenme süreci üzerindeki olası olumsuz etkileri nedeniyle AI tabanlı sohbet robotunu yasakladı<sup>26</sup>.

Ortadoğu Medya Araştırma Enstitüsü (Middle East Media Research Institute -MEMRI) İcra Direktörü Steven Stalinsky'ye göre ise sorun, "teröristlerin yapay zekâyı kullanıp kullanmayacağı değil, nasıl ve ne zaman kullanacağı meselesi". *Newsweek*'te yayınlanan yazısında Stalinsky, teröristlerin hâlihazırda teknolojiyi kullandıklarını belirtti: "Geçtiğimiz 10 yılda, MEMRI'nin Siber ve Terörizm Laboratuvarı tarafından yapılan araştırmalar, teröristlerin para toplamak için kripto para birimi ve iletişim için şifreleme dahil olmak üzere teknolojiyi nasıl kullandıklarını belgelediği gibi; insansız hava araçları ve kendi kendini yöneten bombalı araçlar da dahil olmak üzere bilgisayar korsanlığı ve silah sistemleri için AI unsurlarını ve sosyal yardım, askere alma ve saldırı planlama için robotları kullandıklarını da gösterdi<sup>27</sup>."

22 <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/>

23 <https://www.cnbc.com/2023/05/02/kamala-harris-to-hold-ai-meeting-with-google-microsoft-and-openai.html>

24 <https://www.nytimes.com/2023/01/23/opinion/ted-lieu-ai-chatgpt-congress.html>

25 <https://www.bloomberght.com/chatgpt-ye-hangi-ulke-ne-tavir-aldi-2329335/6>

26 <https://www.donanimhaber.com/chatgpt-ye-ilk-yasak-abd-den-geldi-okullarda-yasaklandi--159017>

27 <https://www.newsweek.com/terrorists-love-new-technologies-what-will-they-do-ai-opinion-1787482>



ABD Savunma Bakanlığının Dijital ve Yapay Zekâ Baş Sorumlusu Craig Martell ise, ChatGPT gibi üretken yapay zekâ sistemlerinin vatandaşları aldatma ve ulusal güvenliği tehdit etme potansiyelinden “ölümüne korktuğunu” söyleyecek kadar tedirgin. Martell, AI tarafından oluşturulan kampanyaların ABD vatandaşlarını etkilemek için kullanılabilirliğini ve ChatGPT’nin bugüne kadarki kullanımının, yaygın dezenformasyonu kolaylaştırmak için nasıl kullanılabilirliğini gösterdiğini söylüyor: “ChatGPT kendini akıcı ve otoriter bir şekilde ifade etmek için eğitildi. Yani, yanlış olsa bile buna inanıyorsunuz. Bu da dezenformasyon için mükemmel bir araç olduğu anlamına geliyor. Dezenformasyonun ne zaman olduğunu tespit edebilmek ve dezenformasyon olduğunda uyarabilmek için araçlara sahip değiliz ve bu araçlara gerçekten ihtiyacımız var. Bu mücadelede gerideyiz<sup>19</sup>.”

Martell’in dezenformasyon konusundaki endişeleri yersiz sayılmaz, zira ChatGPT’nin dezenformasyon kampanyaları ve siyasi müdahaleleri her zamankinden daha yaygın ve gerçekçi hâle getirebileceğine dair artan bir endişe var. ChatGPT’yi geliştiren OpenAI şirketinin CEO’su Sam Altman, AI teknolojisinin toplumu yeniden şekillendireceğini belirtiyor; ancak bunun büyük ölçekli dezenformasyon gibi gerçek tehlikelerle birlikte geldiğini de kabul ediyor.

Devlet dışı aktörlerin ve otoriter rejimlerin, ChatGPT’yi kamusal alanları zehirli unsurlarla kirletmek ve vatandaşların demokrasilere olan güvenini daha da zayıflatmak için kullanabileceğinden korkuluyor. Örneğin FBI Başkanı Christopher Wray, Temsilciler Meclisi İç Güvenlik Komitesi oturumunda, FBI’ın TikTok hakkında ulusal güvenlik endişeleri olduğunu dile getirerek Çin Hükümetinin milyonlarca ABD’li hakkında veri toplamak için popüler video paylaşım uygulamasını potansiyel olarak kullanabileceği konusunda uyarıda bulundu<sup>2</sup>.

AI, ChatGPT özelinde yanlış ama inandırıcı deepfake görüntüleri, videolar ve ses kayıtlarının yanı sıra metin üretebilir. Zira çevrimiçi yanlış bilgilendirme araştırma şirketi Newsguard’dan Gordon Crovits, ChatGPT’nin “İnternette şimdiye kadar bulunan yanlış bilgileri yaymak için en güçlü araç” hâline gelebileceği görüşünü paylaşıyor<sup>9</sup>.

ChatGPT’nin ulusal güvenlik için hem bir nimet hem de endişe kaynağı olabileceğini söyleyen Pentagon Savunma Müsteşarlığı ofisinde Güvenilir Yapay Zekâ ve Özerklik Baş Direktörü olan Kimberly Sablon, ChatGPT’nin istihbarat analizi veya bilgisayar kodu üretmek için kullanılabilirliğine dikkat çekiyor. Sablon bununla birlikte dikkat edilmesi gereken önemli tehditleri şöyle vurguluyor: “Kötü amaçlı kod, daha karmaşık kimlik avı e-postalarının yanı sıra dezenformasyon ve yanlış bilgilendirme kampanyaları ve derin sahtekârlıklar oluşturmak için de ChatGPT kullanılabilir.” Sablon, risklerinin yönetilebilmesi şartıyla bu tür chatbot’ların birçok Savunma Bakanlığı iş sürecini ve operasyonunu kolaylaştırmaya yardımcı olabileceğini, Pentagon’un takviye öğrenme alanında kendi adımlarını attığını belirtiyor: “Savunma İleri Araştırma Projeleri Ajansı (DARPA), Hava Savaşı Evrimi programında benzer makine öğrenmesi tekniklerini kullanarak, AI tarafından üretilen bir pilotu, ‘it dalaşı’nda bir insan pilota karşı yarıştırdı. Bunun gibi olaylar, bu alanda görmeye başladığımız atılımların harika örnekleridir ve eminim ki gelecekte bu atılımların çok daha fazlasını göreceğiz.”

İngiltere Savunma Bakanlığının Savunma İnovasyonu Direktörü John Ridge de ChatGPT’nin sunduğu tarzda yeniliklerin kesinlikle çok önemli olacağını belirterek, en iyi ChatGPT tipi yeteneklere sahip olanların, bir dizi nedenden dolayı baskın olacağına inandığını açıkladı<sup>28</sup>.

Dış Politika üzerine yazan Nicholas Welch ve Jordan Schneider’e göre ise, “AI chatbot’larının tehlikeleri arasında bilişsel savaşta bir araç hâline gelmek, uluslararası çatışmaları uzatmak, siber güvenliğe zarar vermek ve küresel dijital eşitsizliği şiddetlendirmek” yer alıyor<sup>2</sup>.

RAND Corporation Başkanı ve CEO'su Dr. Jason Matheny de, ulusal güvenlik endişeleri olarak gördüğü ana alanları şöyle özetliyor<sup>29</sup>:

- Teknolojiler, genellikle ulusal güvenlik çerçevelerimizin dışında kalan ticari kuruluşlar tarafından yönlendirilmektedir.
- Teknolojiler hızla ilerliyor, tipik olarak hükümet içindeki politikaları ve organizasyonel reformları geride bırakıyor.
- Teknolojilerin değerlendirilmesi, özel sektörde yoğunlaşan ve ulusal güvenlik için nadiren kullanılan uzmanlık gerektirir.
- Teknolojiler, iyi huylu kullanımı kötü amaçlı kullanımdan, kasıtlı kullanımı yanlışlıkla kötüye kullanımdan ayıran veya kesin olarak ilişkilendirmeye izin veren geleneksel istihbarat imzalarından yoksundur.
- AI'ın her şeyi değiştireceğini söylemek abartı değildir.

SlashNext CEO'su Patrick Harr ise bilgisayar korsanlarının ChatGPT'yi daha yüksek hacimli benzersiz hedefli saldırıları daha hızlı yapmak için kullandıklarını belirtiyor. Harr'a göre ChatGPT, siber suçluların kötü amaçlı yazılım algılama motorlarından bir adım önde olmak için sonsuz kod varyasyonları yapmalarını sağlıyor<sup>29</sup>:

“Chatbot'ların bugün başarılı olduğu iki alan var: kötü amaçlı yazılım ve iş e-postası uzlaşma (Business Email Compromise -BEC) tehditleri. BEC saldırıları, bir mağduru değerli finansal bilgiler veya veriler vermesi için sosyal mühendislik yapmaya yönelik hedefli girişimlerdir. Bu saldırıların başarılı olması için kişiselleştirilmiş iletiler gerekir. ChatGPT artık sonsuz varyasyonlarla toplu olarak iyi yazılmış, kişisel e-postalar oluşturabilir. Bu saldırıların hızı ve sıklığı artacak ve saldırganlar kullanıcı uzlaşmalarında ve ihlallerde daha yüksek bir başarı oranını sağlayacaktır. Zira 2023'ün ilk çeyreğinde bildirilen ihlal sayısında önemli bir artış yaşanmıştır.”

### **İnsan Ajan mı Yapay Zekâ Ajan mı?**

AI çok kapsamlı büyük veri analizi yeteneği sayesinde savunma ve istihbarat alanında kariyer basamaklarını hızla tırmanıyor. Ancak sahip olduğu çeşitli kırılabilirlikler, Soğuk Savaş sonrası dünyanın teknolojik ilerlemelerine rağmen, hâlâ insan ajanlara ve istihbarat görevlilerine ihtiyaç duyulduğu anlamına geliyor. AI'ın günümüzdeki en temel rollerinden biri, insanların şu anda yaptığı en çok zaman alan önemsiz analiz rollerini üstlenmektir. Ancak AI, istihbarat kurumlarının bir fotoğraftaki nesnelerin ne olduğunu anlamalarına izin verirken, insan istihbarat görevlileri bunların neden orada olduğunu söyleyebiliyor<sup>9</sup>.

Bir rapora göre, “AI ve otomasyon, şu anda Amerikan istihbarat elemanları tarafından yürütülen görevlerin yüzde 75'ini makul bir şekilde yerine getirebilecek. Yani drone'lardan, açık kaynaklı istihbarattan, keşif veya istihbarat uydularından ve dünyadaki diğer yayınlardan elde edilen jeo-uzamsal görüntüleri toplayan, analiz eden ve yorumlayan yapay zekâ analistler artık devrede”. CIA, memurlarının günlük işlerini ve kapsamlı casusluk görevlerini tamamlamalarına yardımcı olmak için sohbet robotlarını ve üretken yapay zekâ yeteneklerini kullanmayı araştıran kuruluşlardan biri. Bununla birlikte, yönetim ve bilişim teknolojileri danışmanlığı şirketi Booz Allen Hamilton'ın müdürü Patrick Biltgen, en azından şimdilik, AI'ın veya ChatGPT'nin aşama aşama yükseleceğini veya insan analistleri işsiz bırakacağını öngörmeyenlerden biri. “Bugün AI destekli raporlamanın çoğu çok kalıplaşmış ve insan analizi kadar inandırıcı değil” diyen Biltgen, ulusal güvenlik analizi için ChatGPT'nin “şimdiye kadar yazılmış tüm istihbarat raporları, tüm haber makaleleri ve tüm Wikipedia ile önceden eğitilmesi” gerektiğini iddia ediyor. “Bir tahmin makinesi yapabileceğinize inanmıyorum, ancak bir chatbot'un bana bir dizi olayın sonucu olarak, gerçekleşecek olası sonraki adımların bir listesini vermesi mümkün olabilir” diyor.

29 <https://www.csoonline.com/article/575153/ai-powered-chatbots-the-threats-to-national-security-are-only-beginning.html>

Stanford'daki Freeman Spogli Uluslararası Çalışmalar Enstitüsü ve Hoover Enstitüsünde kıdemli bir araştırmacı ve aynı zamanda HAI Uluslararası Güvenlik Yönlendirme Komitesi Başkanı olan Amy Zegart'a göre de insan zekâsı her zaman önemli olacak, ancak makine öğrenmesi insanlara daha iyi oldukları görevler için serbest zaman bırakabilir: "Uydular ve AI algoritmaları bir köprüdeki kamyon sayısını saymakta iyi olsa da, bu kamyonların ne anlama geldiğini size söyleyemezler. Başkalarının isteklerini, niyetlerini ve arzularını anlamak için insanlara ihtiyacınız var. İnsan analistleri bir köprüde kamyonları saymak için daha az zaman harcar. Çok büyük miktarda açık kaynaklı veri var, ancak bunları incelemek için AI'a ihtiyacınız var<sup>20</sup>".

ABD'nin önde gelen Coğrafi Konum İstihbaratı (Geospatial Intelligence -GEOINT) işleyicisi olan Ulusal Jeo-Uzamsal-İstihbarat Teşkilatının (National Geospatial-Intelligence Agency -NGA) Yeteneklerden Sorumlu Müdür Yardımcısı Phillip Chudoba da insan analistlerinin dünyayı yorumlamasına yardımcı olmak için ChatGPT'nin (veya benzeri bir AI'ın) tahmine dayalı metin yeteneklerini kullanmak arzusunda: "Bu uygulama, ordu ve istihbarat ajanslarına dünyada neler olup bittiğinin doğru bir resmini vermek için çok sayıda coğrafi bilgiyi (haritalar, uydu fotoğrafları, hava durumu verileri ve benzerleri) kullanmayı içeriyor."

Amerikan Bilim İnsanları Federasyonunda uzun süredir istihbarat topluluğu gözlemcisi olan Steven Aftergood, NGA'nın, insan analistleri ordusunun başa çıkabileceğinden daha fazla miktarda jeo-uzamsal bilgilerle dolu olduğuna dikkat çekerek, "İlk veri değerlendirme süreci otomatikleştirilebileceği veya yarı akıllı makinelere atanabildiği ölçüde, insanlar belirli aciliyet taşıyan konularla başa çıkmak için serbest bırakılabilir. Ancak burada önerilen şey, AI'ın bundan daha fazlasını yapabileceği ve insan analistlerinin kaçıracağı sorunları belirleyebileceğidir<sup>20</sup>".

### ChatGPT'nin Güvenlikle İlgili Faydalı Yanları

ChatGPT'nin ulusal güvenlik için riskleri hayli fazla olsa da bu teknoloji başta siber güvenlik alanında olmak üzere diğer büyük dil modelleri gibi, güvenliği artırıcı bir güç olarak da pekala kullanılabilir. Örneğin siber güvenlikte ChatGPT aşağıdaki şekillerde kullanılabilir<sup>2</sup>.

- **Kimlik avı algılama:** ChatGPT, kullanıcıları hassas bilgiler sağlamaları için kandırmak üzere tasarlanmış potansiyel olarak kötü amaçlı e-postaları veya mesajları tanımlamak ve işaretlemek için eğitilebilir.
- **Spam filtreleme:** ChatGPT, spam veya istenmeyen reklamlar gibi istenmeyen mesaj ve e-postaları otomatik olarak tanımlamak ve filtrelemek için kullanılabilir.
- **Kötü amaçlı yazılım analizi:** ChatGPT, virüsler ve truva atları gibi kötü amaçlı yazılımları otomatik olarak analiz etmek ve sınıflandırmak için kullanılabilir.
- **İzinsiz giriş algılama:** ChatGPT, kötü amaçlı IP adresleri veya olağandışı veri aktarımı modelleri gibi şüpheli ağ trafiğini otomatik olarak tanımlamak ve işaretlemek için kullanılabilir.
- **Güvenlik Açığı Değerlendirmesi:** ChatGPT, arabellek taşması saldırıları gibi güvenlik açıklarını bulmak ve bildirmek için yazılım kodunu otomatik olarak analiz etmek için kullanılabilir. 