

İLERİ TEKNOLOJİLER, ENFORMASYON MANİPÜLASYONU VE DEZENFORMASYON

Akın Ünver, Doç Dr Özyeğin Üniversitesi



GİRİŞ

Günümüzün teknolojik ortamı, bilginin yaratılma, tüketilme ve manipüle edilme biçiminde devrim yaratan benzeri görülmemiş gelişmelere tanık oldu. Gelişen teknolojiler, yapay zeka tarafından üretilen içeriğin gerçek ve uydurma arasındaki çizgiyi bulanıklaştırabilirdiği ve şüphelenmeyen kitleleri aldatmaya karşı savunmasız bıraktığı sofistike dezenformasyon kampanyalarının önünü açmıştır. Ünlü Cambridge Analytica skandalından ve Batı demokrasilerindeki seçimlere müdahale vakalarından bu yana, dijital iletişim yoluyla halkların kafasını karıştırmak ve nifak tohumları ekmek için tasarlanan teknolojiler hızla geliştiğinden, bu cephede çok şey oldu. Son yıllarda, Yapay Zeka (YZ), Üretken Çekişmeli Ağlar (GAN) ve derin sahtecilik alanlarındaki ilerlemeler sayesinde, Batı'da en çok çalışılan ülkelerin ötesinde, bilgi manipülasyonu ve bozulması için kullanılan teknoloji repertuarının giderek büyüdüğüne tanık olduk.

Örneğin, Brezilya'daki 2022 ulusal seçimleri, yapay zeka tarafından üretilen deepfake'lerin kötü niyetli kullanımıyla baltalanmıştır; burada yanlış bilgi yaymak için önde gelen adayları çeşitli skandal ve uzlaşmacı durumlara karışmış gösteren uydurma görüntüler ve videolar kullanılmıştır. ¹ Bu aldatmaca, adayların seslerini ve yüz ifadelerini doğru bir şekilde taklit etmek için gelişmiş yapay zeka ve sofistike düzenleme araçlarından yararlanılarak ustaca düzenlenmiş, son derece ikna edici, ancak halkın güvenini sarsan ve seçim ortamını çarpıtan tamamen hayali bir anlatı ekosistemine ait bir sonuç yaratmıştır. Myanmar'da askeri personel, Rohingya Müslüman azınlığına karşı nefret söylemi ve sahte haberler yaymak için Facebook'ta sistematik bir kampanya yürüttü. ² Kampanya, daha geniş bir kitleye ulaşmak için algoritmik güçlendirmeden yararlanarak yavaş yavaş Rohingya karşıtı içerik yayınlamaya başlayan görünüşte zararsız yaşam tarzı sayfaları oluşturmayı içeriyordu. Bu dezenformasyon, etnik temizlik eylemleriyle sonuçlanan bir düşmanlık atmosferine katkıda bulundu. Sonuç olarak, Facebook uluslararası eleştirilere maruz kaldı ve platformdaki nefret söylemi ve yanlış bilgilerle mücadele etmek için daha önemli çabalara yol açtı.

Dil ve lehçeler açısından zengin bir ülke olan Hindistan'da, Doğal Dil İşleme (NLP) yetenekleri siyasi tartışmaları geniş ölçekte manipüle etmek için kullanıldı. 2019-20 yılları arasında, rakip yapay zeka sistemleri, bölgeye özgü kültürel ve dilsel tonları dikkate alarak, ağırlıklı olarak Facebook'ta farklı bölgelere göre uyarlanmış dezenformasyon üretmek üzere özel olarak programlandı. ³ YZ, yerel lehçeler ve bölgesel bağlama mükemmel şekilde uyan, kültürel açıdan incelikli anlatılar kullandı. Bu taktik, bölgesel önyargılarla oynayarak ve uydurma haberleri yerel topluluklara daha gerçekçi ve ilişkilendirilebilir görünen bir şekilde sunarak endişe verici derecede etkili oldu. Rusya'daki daha sinsi bir örnekte, yapay zeka tabanlı

1 Vasconcellos, Paulo Henrique Santos, Pedro Diógenes de Almeida Lara, and Humberto Torres Marques-Neto. "Analyzing Polarization And Toxicity On Political Debate In Brazilian TikTok Videos Transcriptions." In Proceedings of the 15th ACM Web Science Conference 2023, pp. 33-42. 2023.
2 Mathew, Binny, Ritam Dutt, Pawan Goyal, and Animesh Mukherjee. "Spread of hate speech in online social media." In Proceedings of the 10th ACM conference on web science, pp. 173-182. 2019.
3 Bali, Aasita, and Prathik Desai. "Fake news and social media: Indian perspective." Media Watch 10, no. 3 (2019): 737-750.

bilgi manipülasyon sistemleri Ukrayna'daki kamuoyu duyarlılığını geniş ölçekte manipüle etmek için kullanıldı. ⁴ NLP tarafından desteklenen botların çeşitli sosyal medya platformlarında gerçek kullanıcıları taklit ettiğini ortaya çıkaran kapsamlı bir dezenformasyon kampanyası 2022'de gün ışığına çıkarıldı. Bu yapay zeka varlıkları kamuya açık tartışmalara katıldı, çatışmaları körükledi ve sahte haberler yayarak siyasi bölünmeleri yoğunlaştırdı ve Rusya'nın Ukrayna'yı ikinci kez işgali öncesinde toplumsal huzursuzluğu katkıda bulundu.

Filipinler'de Devlet Başkanı Rodrigo Duterte'nin 30 Haziran 2016'da göreve gelmesinden bu yana, özellikle yaygın sosyal medya platformu Facebook'ta devlet destekli dezenformasyon kampanyalarında belirgin bir artış yaşandı. ⁵ Hükümetin, sistematik olarak propaganda yaymak üzere büyük birey gruplarının ya da otomatik botların görevlendirildiği endişe verici bir strateji olan 'trol ordularını' harekete geçirdiği iddia ediliyor. Bunların başlıca hedefleri, kamuoyunun duygularını yönetim lehine yönlendirmek, muhalefeti itibarsızlaştırmak ve taciz etmek ve dikkatleri tartışmalı konulardan başka yöne çekmek gibi görünüyor. Bu dezenformasyon kampanyaları ne gelişigüzel ne de spontanedir. Karmaşık veri profillemesine dayanan içeriğin hedefli ve hesaplı bir şekilde yayılmasını içerirler. Bu kampanyaların odağında genellikle yönetimi eleştirenler ve aralarında haber kuruluşu Rappler'in Duterte yönetiminin dezenformasyon taktikleri ve iddia edilen yargısız infazları hakkında haber yapmaya başlamasından bu yana internet üzerinden taciz ve yasal tacizle karşı karşıya kalan insan hakları aktivisti Maria Ressa'nın da bulunduğu etkili muhalif isimler yer almaktadır. ⁶

Eş zamanlı olarak, dünya genelinde, Avustralya'da 2019'un sonlarından 2020'nin başlarına kadar meydana gelen feci orman yangınlarının ortasında, sosyal medya platformlarında bir yanlış bilgi dalgası yayıldı. ⁷ Bu yanlış bilgi, resmi raporların yangınların çoğunun yıldırımdan kaynaklandığını ve yalnızca %1'inin kasıtlı olarak çıkarıldığını belirtmesine rağmen, orman yangınlarının ağırlıklı olarak kundakçılar tarafından çıkarıldığını iddia ediyordu. Bu yanlış bilgi dalgası esas olarak, iklim değişikliği şüphecileri ve hükümet karşıtı gruplar da dahil olmak üzere duyarlı demografileri hedef almak için büyük veri profillemesine dayalı yanlış bilgileri stratejik olarak güçlendiren botlar ve troller tarafından yayıldı. Dahası, İsveç'te 2023 yazında Savunma Bakanlığı büyük ölçekli, otomatik bir bilgi manipülasyonu operasyonuna maruz kalmıştır. Bu operasyonda, Haziran ve Temmuz 2023'te meydana gelen bir dizi Kuran yakma olayını İsveç hükümetine mal etmek için deepfake teknolojisi (hiper-gerçekçi sahte görüntüler veya videolar yaratabilen sofistike yapay zeka) kullanıldı. Bu dezenformasyon kampanyasının büyüklüğü karşısında şaşkına dönen İsveç Savunma Bakanlığı, bu suçlamaları canlı olarak kontrol etmek ve çürütmek için organize bir karşı kampanya başlatmak zorunda

- 4 Stukal, Denis, Sergey Sanovich, Joshua A. Tucker, and Richard Bonneau. "For whom the bot tolls: A neural networks approach to measuring political orientation of Twitter bots in Russia." *Sage Open* 9, no. 2 (2019): 2158244019827715.
- 5 Ong, Jonathan Corpus, and Ross Tapsell. "Demystifying disinformation shadow economies: fake news work models in Indonesia and the Philippines." *Asian Journal of Communication* 32, no. 3 (2022): 251-267.
- 6 Tandoc, Edson C., Karryl Kim Sagun, and Katrina Paola Alvarez. "The digitization of harassment: Women journalists' experiences with online harassment in the Philippines." *Journalism Practice* 17, no. 6 (2023): 1198-1213.
- 7 Weber, Derek, Lucia Falzon, Lewis Mitchell, and Mehwish Nasim. "Promoting and countering misinformation during Australia's 2019-2020 bushfires: a case study of polarisation." *Social Network Analysis and Mining* 12, no. 1 (2022): 64.

kaldı. ⁸ Hükümet bu provokasyonlara karıştığını kesin bir dille reddederek bu tür manipülatif dijital taktiklerin karmaşıklığının ve potansiyel zararlarının altını çizdi.

Ancak teknoloji dezenformasyonun yükselişini körüklerken, potansiyel çözümlerin anahtarını da elinde tutuyor. Bir zamanlar dezenformasyon yaratıcıları tarafından kullanılan yapay zeka ve NLP artık tespit için güçlü araçlar olarak kullanılabilir. Makine öğrenimi ve veri analitiği, araştırmacılara ve doğruluk kontrol uzmanlarına büyük miktarda bilgiyi eleme ve dezenformasyonun izlerini ortaya çıkaran kalıpları ortaya çıkarma becerisi kazandırmaktadır. Örneğin, GPT destekli yapay zeka doğrulayıcılarının ortaya çıkışı, yapay zekanın iddiaları güvenilir kaynaklarla hızlı bir şekilde çapraz referanslamak ve gerçek zamanlı olarak yanlışları çürütmek için nasıl kullanılabileceğini göstermiştir. ⁹

Örneğin blok zinciri teknolojisinin dönüştürücü potansiyeli, içeriği yetkisiz değişikliklerden koruyarak ve kaynağını garanti altına alarak, kurcalamaya dayanıklı bilgi yayma yolunda umut verici bir yol sunmaktadır. Blok zincirinin kurcalamaya karşı dayanıklı yapısı, sunulan verilerin gerçek olmasını sağlayarak yanlış bilgilere karşı koymaya ve çevrimiçi bilgi kaynaklarına olan güveni artırmaya yardımcı olur. Araştırmacılar, ağları ve kullanıcı davranışlarını analiz ederek dezenformasyon kampanyalarını ve otomatik bot hesaplarının rolünü tersine mühendislikle çözebilir ve hedefe yönelik karşı stratejilerin geliştirilmesini sağlayabilir. Örneğin, 2016 Brexit referandumunun ardından araştırmacılar, yanıltıcı bilgiler yayan ve kamuoyu duyarlılığını manipüle eden kapsamlı bir Twitter bot ağı tespit etti. Bu organize kampanyanın ortaya çıkarılması daha sonra dezenformasyon yayılımının arkasındaki mekaniği anlamada ve bu tür koordineli çabaları bozmak için stratejiler geliştirmede etkili oldu. ¹⁰

- 8 Karlidag, Ilgin. 2023. "Sweden's Quran Burnings Put Freedom of Expression Law to Test." BBC News, July 27, 2023. <https://www.bbc.com/news/world-europe-66310285>.
- 9 Banas, John A., Nicholas A. Palomares, Adam S. Richards, David M. Keating, Nick Joyce, and Stephen A. Rains. "When machine and bandwagon heuristics compete: Understanding users' response to conflicting AI and crowdsourced fact-checking." *Human Communication Research* 48, no. 3 (2022): 430-461.
- 10 Nicoli, Nicholas, Soulla Louca, and Petros Iosifidis. "Social Media, News Media, and the Democratic Deficit. Can the Blockchain Make a Difference?." *tripleC: Communication, Capitalism and Critique* 20, no. 2 (2022).

DEZENFORMASYON, ENFORMASYON BASKILAMA ve DIŞ KAYNAKLI MÜDAHALELER

Dezenformasyon, yanlış bilgilendirme, kötü bilgilendirme, bilgi bastırma ve yabancı bilgi manipülasyonu ve müdahalesi (FIMI) olguları, dünya çapında toplumlar ve hükümetler için karmaşık zorluklar teşkil etmektedir. Farklı tanımları ve örtüşen etkileriyle propaganda, dezenformasyon ve yabancı müdahale gibi terimler, sıklıkla karıştırıldıkları veya birbirlerinin yerine kullanıldıkları için gerçek dünyadan örneklerle derinlemesine anlaşılmasını gerektirir.



Bilgi manipülasyonuna ilişkin mavi takım - kırmızı takım senaryosunu tasvir eden Avrupa Dış Eylem Servisi senaryosu. Kaynak: 1. EEAS Yabancı Bilgi Manipülasyonu ve Müdahale Tehditleri Raporu Ağ bağlantılı savunma için bir çerçeveye doğru. Şubat 2023
<https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf>

Bu terimlerden en eskisi olan propaganda, kapsamlı bir şekilde “önemli sembollerin manipülasyonu yoluyla kolektif tutumların yönetimi” olarak tanımlanmıştır.”¹¹, “Halkın bir girişim, fikir ya da grupla ilişkilerini etkilemek için olaylar yaratmaya ya da şekillendirmeye yönelik tutarlı ve kalıcı bir çaba”¹², “Bireyler ya da gruplar tarafından, önceden belirlenmiş amaçlar doğrultusunda diğer bireylerin ya da grupların görüşlerini ya da eylemlerini etkilemek üzere kasıtlı olarak tasarlanan görüş ya da eylem ifadesi”¹³, ve “Propaganda yapılan kişinin özgürce düşünmeden önce, propagandacının istediği tepkileri vermesini ikna teknikleriyle sağlamaya çalışan bir süreç”¹⁴.

Çin Komünist Partisi (ÇKP) tarafından kullanılan, söylemleri kontrol etmek ve kamuoyunu şekillendirmek için hem ülke içinde hem de uluslararası alanda

11 Lasswell, Harold D. “The theory of political propaganda.” American Political Science Review 21, no. 3 (1927): 627-631.

12 As cited in: Hobbs, Renee, and Sandra McGee. “Teaching about propaganda: An examination of the historical roots of media literacy.” Journal of Media Literacy Education 6, no. 2 (2014): 56-66.

13 Cantril, Hadley. “Propaganda analysis.” The English Journal 27, no. 3 (1938): 217-221.

14 Henderson, Edgar H. “Toward a definition of propaganda.” The Journal of Social Psychology 18, no. 1 (1943): 71-87.

kullanılan geniş propaganda mekanizmasını ele alalım. İçeride ÇKP, tüm devlet medya kuruluşları üzerinde sıkı bir kontrol sağlayarak parti söylemlerinin yayılmasını kolaylaştırmakta ve muhalefeti sansürlenmektedir. Ulusal gençleşme, sosyal ilerleme ve gelişmiş yaşam standartlarını kapsayan bir anlatı olan “Çin Rüyası”, ulusal gururu ve hükümetin gündemine desteği teşvik etmek için tasarlanmış bir örnektir. Dışarıda ise Çin, uluslararası imajını değiştirmek için küresel medya üzerindeki etkisini arttırmaktadır. Bunun çarpıcı bir örneği, küresel haberleri Çin bakış açısıyla sunan çok dilli bir küresel yayıncı olan Çin Küresel Televizyon Ağı’dır (CGTN). Ayrıca, Çin hükümeti dünya çapında “Konfüçyüs Enstitülerine” büyük yatırımlar yapmakta ve bu enstitüler hem kültürel organizasyonlar hem de yumuşak güç yansıtmak ve Çin’in olumlu imajını desteklemek için araçlar olarak hizmet vermektedir.¹⁵

Propagandanın bu denli kapsamlı kullanımı sayesinde ÇKP bir yandan ülke içinde kontrolü sağlarken bir yandan da uluslararası alanda algıları değiştirmeye çalışmakta ve böylece propagandanın kamusal ve siyasi manzaraları şekillendirmedeki yaygın rolünü vurgulamaktadır. Günümüz Kuzey Kore rejimi de propagandanın kullanımına örnek teşkil etmekte ve hükümet ülke içindeki tüm bilgiler üzerinde sıkı bir kontrol uygulamaktadır. Bu kontrol, halkın dış dünyaya, ülkenin liderliğine ve hakim siyasi ideolojiye ilişkin algılarını şekillendirmektedir.¹⁶

Dezenformasyon ise genellikle kısa vadeli kazançla ilişkilendirilir. Kasıtlı olarak yanıltıcı veya önyargılı bilgileri, manipüle edilmiş anlatıları veya gerçekleri ya da aldatmak, yanlış yönlendirmek veya kafa karıştırmak amacıyla yayılan yanlış bilgileri ifade eden bir terimdir.¹⁷ Genellikle zarar vermek, alıcıyı yanlış yönlendirmek veya bir kişi, kuruluş veya ülke hakkında yanlış algılar yaratmak amacıyla yanlış veya manipüle edilmiş bilgilerin kasıtlı olarak oluşturulmasını ve paylaşılmasını içerir. Dezenformasyon, sahte haberler, deepfakes veya yanıltıcı anlatılar gibi pek çok şekilde ortaya çıkabilir. Rusya ve Ukrayna arasında²⁰¹⁴ sonrası yaşanan çatışma dezenformasyonun modern bir örneğini teşkil etmektedir. Burada hem Rus devleti hem de vekilleri, durumun gerçekliğini maskeleyerek, Ukrayna hükümetini gayrimeşrulaştırmak ve Rusya’nın eylemlerini küresel toplum nezdinde haklı göstermek için dezenformasyonu yoğun bir şekilde kullanmıştır.¹⁸

Dezenformasyon siyasi alanla sınırlı değildir ve sağlıkla ilgili yanlışlıklar gibi siyasi olmayan tartışmalarda da ortaya çıkabilir. Örneğin, COVID-19¹⁹ salgını sırasında çoğu ülke sağlıkla ilgili yanlış bilgilerle mücadelede zorluklarla karşılaştı. Sosyal medya platformlarında virüs ve tedavisi hakkında söylentilerin, yanlış anlamaların ve yalanların yaygınlaşması paniğe, bilimsel olmayan çözümlerin yayılmasına ve halk sağlığı müdahalelerinin baltalanmasına yol açtı.¹⁹

- 15 Zhu, Yanling. “China’s ‘new cultural diplomacy’ in international broadcasting: branding the nation through CGTN Documentary.” *International Journal of Cultural Policy* 28, no. 6 (2022): 671-683.
- 16 Sukin, Lauren. “Why ‘cheap’ threats are meaningful: Threat perception and resolve in North Korean propaganda.” *International Interactions* 48, no. 5 (2022): 936-967.
- 17 Kapantai, Eleni, Androniki Christopoulou, Christos Berberidis, and Vassilios Peristeras. “A systematic literature review on disinformation: Toward a unified taxonomical framework.” *New media & society* 23, no. 5 (2021): 1301-1326.
- 18 Erlich, Aaron, and Calvin Garner. “Is pro-Kremlin disinformation effective? Evidence from Ukraine.” *The International Journal of Press/Politics* 28, no. 1 (2023): 5-28.
- 19 Grimes, David Robert. “Medical disinformation and the unviable nature of COVID-19 conspiracy theories.” *PLoS One* 16, no. 3 (2021): e0245900.

Yabancı veya devlet destekli kuruluşlar tarafından gerçekleştirilen bilgi manipülasyonunun çok yönlü ve benzersiz manzarasıyla boğuşurken, Yabancı Bilgi Manipülasyonu ve Müdahalesi (FIMI) kavramı daha popüler hale gelmeye başladı.²⁰ Bu terim, anlaşılması için temel özelliklerinin ve bunların gerçek dünya senaryolarındaki tezahürlerinin daha yakından incelenmesini gerektiren sayısız karmaşık olguyu kapsamaktadır. FIMI'nin belirleyici özelliği, yabancı kuruluşların veya hükümetlerin katılımıdır ve bu da onu bir ulusun sınırları içinde ortaya çıkabilecek geleneksel dezenformasyon veya yanlış bilgilendirme biçimlerinden ayırır. Bunun çarpıcı bir örneği 2017 yılında Avustralya'da yaşanan elektrik şebekesi krizi sırasında, Çin'in Avustralya'nın elektrik şebekesine müdahale ettiğine dair iddiaların ortaya atıldığı haberlerde görülebilir.²¹ Suçlamalar, panik ve kafa karışıklığı yaratmak için sosyal medya platformlarında dezenformasyon yayan ve nihayetinde Avustralya hükümetinin kritik altyapıyı sürdürme becerisine olan kamu güvenini zayıflatmayı amaçlayan Çinli kuruluşlara yöneltildi. Düzenlendiği iddia edilen kampanya, elektrik şebekesindeki arızanın boyutu ve nedeni hakkında yanlış anlatılar yaymanın yanı sıra hükümetin durumla başa çıkmadaki yetersizliğini abartmayı da içeriyordu. Bu olay, bilginin manipüle edilmesinde yabancı müdahalesinin açık bir örneğini sunmuş ve FIMI'nin ulusal güvenlik ve kamu güveni üzerindeki etkisini vurgulamıştır. FIMI için aynı derecede kritik olan bir diğer husus da jeopolitik saiklerle desteklenmesidir. Genellikle seçimleri etkilemek, anlaşmazlıkları körüklemek, toplumları istikrarsızlaştırmak veya hedef ülkelerdeki demokratik kurumları zayıflatmak gibi daha geniş jeopolitik amaçlara ulaşmak için bir araç olarak kullanılmaktadır. Bu husus, dış kaynaklı dijital kampanyaların kamuoyu duyarlılığını etkilemeye ve toplumsal bölünmeleri kışkırtmaya çalıştığı 2021 Uganda seçimlerinde açıkça görülmüştür.²²

Öncelikle kamuoyunu etkilemeyi amaçlayan geleneksel dezenformasyon ve yanlış bilgilendirme kampanyalarının aksine, FIMI özellikle yabancı ülkelerin yönetim ve siyasi süreçlerini hedef alır. Dahası, FIMI kampanyaları genellikle dış politika hedeflerini gerçekleştirmek için koordine edilen daha geniş stratejik çabaların bir parçasıdır. Genellikle dezenformasyon, siber saldırılar, sosyal medya manipülasyonu ve dijital iletişim kanalları ve ileri teknolojiler aracılığıyla güçlendirilen diğer psikolojik taktiklerin bir karışımını içerirler. Sosyal medya platformlarının hükümet yanlı mesajlarla doldurulmasını ve devleti eleştiren bireylerin taciz edilmesini içeren bir yaklaşım olan 'vatansever trolleme'nin, kamu söylemini ve algısını manipüle etmeye yönelik koordineli bir stratejinin parçası gibi görüldüğü Avustralya'daki şüpheli yabancı etki kampanyaları bunu iyi bir şekilde göstermektedir.

20 1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence, European External Action Service (EEAS), viewed 24 July 2023, <<https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf>>.

21 "China Accuses Australia and Canada of 'disinformation' over Jet Encounters." The Guardian, 7 June 2022, www.theguardian.com/world/2022/jun/07/china-accuses-australia-canada-jet-encounters.

22 Abrahamsen, Rita, and Gerald Bareebe. "Uganda's fraudulent election." Journal of Democracy 32, no. 2 (2021): 90-104.

İLERİ ENFORMASYON MANİPÜLASYONU TEKNOLOJİLERİ

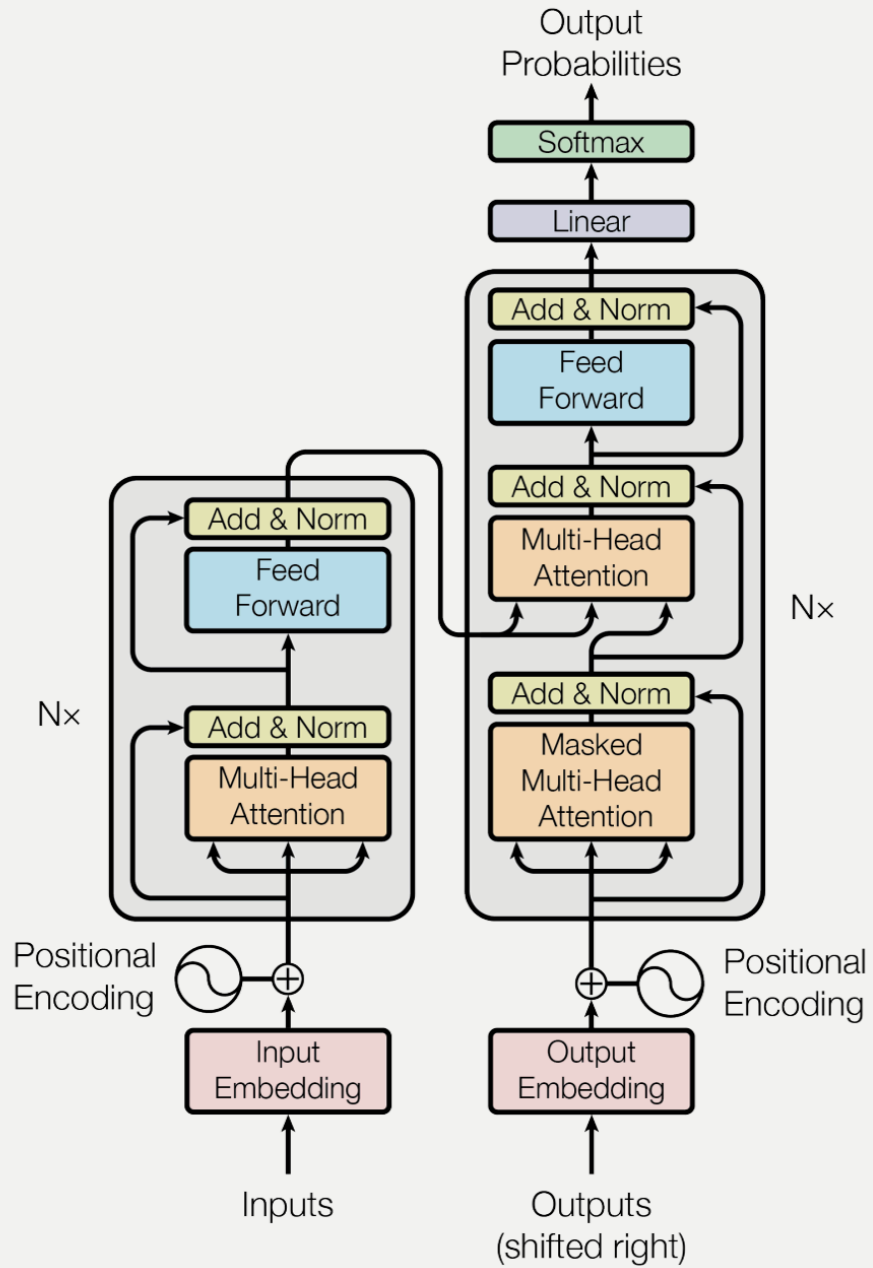
FIMI bağlamında, yeni teknolojiler, ister dezenformasyon yaymak, ister sosyal medyayı manipüle etmek, siber saldırılar düzenlemek veya diğer bilgi savaşı faaliyetlerinde bulunmak olsun, bilgi manipülasyonu hedeflerine ulaşmak için devlet aktörleri veya yabancı kuruluşlar tarafından gerçekleştirilen belirli eylemleri, kullanılan yöntemleri ve izlenen standart süreçleri kapsayan 'Teknikler, Taktikler ve Prosedürler' TTP'lerini güçlendirmektedir. Bu TTP'ler kamuoyu algısını etkilemek, anlatıları şekillendirmek ve jeopolitik çıkarları ilerletmek için daha geniş bir stratejinin parçasıdır. Yeni teknolojiler ve bunların FIMI TTP'leri üzerindeki etkileri üç ana başlık altında özetlenebilir: Yapay zeka tabanlı teknolojiler, sosyal medya ve algoritma tabanlı teknolojiler, deepfakes ve görsel-işitsel manipülasyon ve mikro hedefleme ve reklam tabanlı teknikler.

YAPAY ZEKA TABANLI TEKNOLOJİLER 1. YZ Tarafından Üretilen İçerik:

Gelişmiş yapay zekanın (AAI) gelişimi, her biri dış müdahale alanında önemli bir etkiye sahip olabilecek çok sayıda güçlü Yapay Zeka Tarafından Oluşturulan İçerik Üreticisinin (AI-GCG'ler) ortaya çıkmasını sağlamıştır.²³ Bunlar arasında kayda değer bir model, 100 trilyondan fazla makine öğrenme parametresine sahip müthiş bir dil modeli olan OpenAI'nin GPT-varyantlarıdır. GPT'lerin güçlü yetenekleri, deneme yazma, soruları yanıtlama, dilleri tercüme etme ve hatta insan benzeri bir akıcılık derecesiyle şiir yazma yeteneklerinde gösterilmiştir. Ancak bu teknoloji FIMI bağlamında iki ucu keskin bir kılıçtır. Örneğin, kötü niyetli bir devlet aktörü, milliyetçi duyguları körüklemek için tasarlanmış bir dizi sosyal medya paylaşımını yaymak için kullanarak, siyasi olarak yüklü bir açmaz sırasında bu teknolojiden yararlanabilir. Böyle bir kampanya mevcut gerilimleri artırabilir ve potansiyel olarak çatışmayı hızlandırabilir, bu da gelişmiş yapay zekanın bilgiyi manipüle etmek isteyenlerin elinde oluşturduğu potansiyel tehdidin altını çizer.

Bir diğer önemli model ise teknoloji devinin en gelişmiş dil modeli olan Microsoft'un Turing NLG'sidir (T-NLG). Yapay zeka, insan tarafından yazılmış içerikle kolayca karıştırılabilecek önemli metin paragrafları oluşturabilir. Bu durum, örneğin bir seçim sırasında yabancı bir kuruluşun T-NLG'yi kullanarak bir aday hakkında yanlış bilgilerle dolu makaleler yayınlayabileceği ve böylece kamuoyunu etkileyerek demokratik süreci baltalayabileceği potansiyel kötüye kullanıma kapı açıyor. Google'ın T5 (Metinden Metne Aktarım Dönüştürücüsü), esasen bir metin üreticisi olmasa da, potansiyel kötüye kullanım için mevcut araçlar dizisine eklenir. Çeviriden özetlemeye kadar bir dizi doğal dil işleme görevindeki esnekliği ve gücü, onu FIMI cephaneliğinde çok yönlü bir silah haline getirmektedir. Son olarak, Facebook'un Yapay Zeka araştırma grubu tarafından geliştirilen BART, Yapay Zeka Tarafından

Oluşturulan İçerik Oluşturucuların manzarasına bir katman daha ekliyor. Diziden diziye modellerin ön eğitimi için tasarlanmış bir denoising oto kodlayıcı olan BART, tutarlı ve yüksek kaliteli metinler üretebilir. Gelişmekte olan bir ülkede eşit olmayan veya yavaş bilgi yayılımının olduğu bir kriz, dış bir devletin BART destekli botları konuşlandırması, sosyal medya platformlarında söylentiler yayması ve böylece kafa karışıklığına neden olması ve zaten gergin olan durumu daha da istikrarsızlaştırması için bir fırsat sağlayabilir.



Dil dönüştürücü modellerinin genel bir akış şeması. Kaynak: Vaswani, Ashish, Shazeer, Noam, Parmar, Niki, Uszkoreit, Jakob, Jones, Llion, Gomez, Aidan N., Kaiser, Lukasz ve Illia Polosukhin. "Attention Is All You Need." ArXiv, (2017). Erişim tarihi 31 Temmuz 2023. /abs/1706.03762.

2. Metin Özetleme ve İçerik Manipülasyonu:

Doğal Dil İşleme'nin (NLP) evrimi, metin özetleme ve içerik manipülasyonu için sofistike tekniklerin geliştirilmesinin önünü açmıştır. Bu teknikler, kötü niyetli aktörler için yeni bir araç cephaneliği yaratarak FIMI'nin manzarasını önemli ölçüde değiştirmiştir. Soyutlayıcı özetleme bu alanda güçlü bir teknik olarak ortaya çıkmıştır. Bir metinden yalnızca en önemli cümleleri seçen muadili ekstraktif özetlemenin aksine, soyutlayıcı özetleme aynı bilgiyi iletmek için yeni cümleler oluşturur.²⁴

GPT'ler veya T5 gibi dil modelleri, orijinal içeriğin bağlamını ve duygusunu koruyan soyut özetler oluşturma konusunda uzmandır. Bununla birlikte, FIMI bağlamında, bu yetenek karmaşık konuların veya siyasi olayların yanıltıcı özetlerini oluşturmak için kullanılabilir. Örneğin, silahlı bir çatışmaya dahil olan harici bir devlet, soyutlayıcı özetlemeyi manipüle ederek anlatıları kendi lehine çevirebilir ve böylece savaşçıların moralini ve savaş alanı dinamiklerine ilişkin algılarını etkileyebilir. Soyutlayıcı özetlemenin yanı sıra, duygu manipülasyonu da kötüye kullanım için başka bir potansiyel yol sunar. Gelişmiş NLP modellerinin bir metnin genel içeriğini değiştirmeden duygusunu ince bir şekilde değiştirme yeteneği, dezenformasyon ekmeğe niyetli olanların elinde güçlü bir araçtır.²⁵

Dahası, modern NLP modelleri orijinal anlamı koruyarak cümleleri ve hatta tüm metinleri yeniden ifade etme veya yeniden yazma yeteneğine sahiptir. Bu işlev intihal tespiti veya metin sadeleştirme gibi görevler için faydalı olabilirken, dezenformasyon kampanyalarında istismara da kapı açmaktadır. Örneğin, iki kıyıdaş devlet arasındaki bir toprak anlaşmazlığı sırasında, harici bir varlık gerçek haber makalelerini ince bir yeniden ifade etme yoluyla manipüle edebilir, kamu algısını kendi bakış açısını destekleyecek şekilde çarpıtabilir ve izleyici maliyetlerine ve tırmanma modellerine katkıda bulunabilir. NLP'deki bir diğer kayda değer gelişme de bir metnin olgusal doğruluğunu otomatik olarak doğrulamayı amaçlayan otomatik doğruluk kontrolü tekniğidir. Ancak sofistike aktörler, teknik olarak doğru olsa da yanıltıcı veya bağlamından koparılmış içerikler üreterek bu sistemleri atlatmanın yollarını bulabilirler. Bu girişimler, bilginin son derece teknik ve kafa karıştırıcı hale gelebildiği afet ve acil durumlarda büyük hasara yol açacak ve yabancı aktörler tarafından geniş ölçekli manipülasyonun önünü açacaktır.

Bu gelişmiş tekniklerin ortaya çıkışı, kötü niyetli aktörlere bilgi manipülasyonu için sofistike araçlar sunarak FIMI TTP'lerinin potansiyel etkisini önemli ölçüde artırmıştır. Bu teknikler sadece gerçekçi içeriklerin değil, aynı zamanda hedef kitlenin önyargılarına ve beklentilerine bağlamsal ve duygusal olarak uyum sağlayan anlatıların oluşturulmasını sağlayarak dezenformasyonu daha ikna edici ve tespit edilmesi zor hale getirmektedir. Sonuç olarak, bu durum daha büyük sosyal ve siyasi etkiye yol açabilir ve bu gelişen tehditle mücadele etmek için yapay zeka

24 Winata, Genta Indra, Andrea Madotto, Zhaojiang Lin, Rosanne Liu, Jason Yosinski, and Pascale Fung. "Language models are few-shot multilingual learners." arXiv preprint arXiv:2109.07684 (2021).

25 Mathew, Leeja, and V. R. Bindu. "A review of natural language processing techniques for sentiment analysis using pre-trained models." In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 340-345. IEEE, 2020.

destekli tespit sistemleri, dijital okuryazarlık kampanyaları ve politika müdahaleleri dahil olmak üzere gelişmiş karşı önlemler geliştirmenin önemini vurgulamaktadır.

3. Otomatik Mütercim Algoritmalar ve Diller Arası Dezenformasyon:

NLP, sofistike dil çevirisi ve diller arası dezenformasyon tekniklerinin geliştirilmesiyle sonuçlanan önemli ilerlemeler kaydetmiştir. Bu gelişmeler, internetin yaygınlığı ve çok dilli kullanıcı tabanı göz önüne alındığında, FIMI taktikleri bağlamında büyük önem taşımaktadır. Bu alandaki en önemli gelişme Sinirsel Makine Çevirisi'dir (NMT).²⁶

Bunun mükemmel bir örneği, makine çevirisine yönelik uçtan uca öğrenme yaklaşımlarının öncüsü olan Google'ın Nöral Makine Çevirisi sistemidir. Bir cümleyi tek tek kelimelere veya kelime öbeklerine ayıran geleneksel çeviri sistemlerinin aksine, NMT tüm cümleleri çevirerek daha doğru ve akıcı çeviriler yapılmasını sağlar. Ancak, bu teknolojinin dezenformasyon yaymak için kötüye kullanılması göz ardı edilemez. Bir devlet aktörünün yanıltıcı bilgi veya propagandayı aynı anda birden fazla dilde çevirmek ve dağıtmak için NMT'yi kullandığı önemli bir jeopolitik olayı hayal edin. Bu potansiyel olarak kamuoyunu küresel ölçekte manipüle edebilir. Dahası, diller arası anlama için güçlü bir araç olan Çok Dilli BERT'in (mBERT) ortaya çıkışı manipülasyon potansiyelini derinleştirmiştir.²⁷ mBERT, farklı dillerdeki cümleler arasındaki anlamsal benzerlikleri anlamakta uzmandır; bu yetenek, aldatıcı amacını çeşitli dillerde koruyan dezenformasyonu yaymak için kullanılabilir. Kötü niyetli bir aktörün yanıltıcı sağlık tavsiyelerini çeşitli dillerde dolaşıma sokmak için mBERT'i kullandığı ve böylece farklı ülkelerde kafa karışıklığına ve potansiyel olarak zararlı davranışlara neden olduğu bir halk sağlığı krizi buna bir örnek olabilir.

NLP'deki bir başka son teknoloji gelişme olan sıfır atışlı çeviri, dezenformasyonun kapsamını önemli ölçüde genişletebilir. Facebook'un LASER veya OpenAI'nin GPT'leri gibi gelişmiş modellerde bulunan bu özellik, bir modelin eğitim sırasında görmediği dil çiftleri arasında çeviri yapmasını sağlar. Kötü niyetli aktörlerin elinde, daha az yaygın dillerde veya lehçelerde dezenformasyon yaymak, daha savunmasız veya dijital okuryazarlığı daha az olan nüfusları hedef almak için sıfır atışlı bir çeviri kullanılabilir. Etnik ve dinsel gerilimlerin yaşandığı Hindistan'ı ele alalım; burada bir dış varlık, yerel lehçelerde kışkırtıcı mesajlar yayarak şiddeti körüklemek için sıfır atışlı çeviriyi kullanabilir. Diller Arası Transfer Öğrenimi tekniği de FIMI alanında kendine yer bulmuştur.²⁸ Bu yöntem, başlangıçta başka bir dilde eğitilmiş bir model kullanılarak farklı bir dildeki metnin işlenmesini içerir. Bir dilde sahte haber üretmek ve daha sonra aynı modeli diğer dillerde benzer içerik üretmek için uyarlamak için kullanılabilir. Örnek bir senaryo, bir devlet aktörünün bu tekniği kullanarak katılımcı ülkelerin çevre politikaları hakkında yanlış bilgi yaydığı, potansiyel olarak anlaşmazlık tohumları ektiği ve uluslararası işbirliğini baltaladığı çekişmeli bir uluslararası iklim zirvesi olabilir.

26 Stahlberg, Felix. "Neural machine translation: A review." *Journal of Artificial Intelligence Research* 69 (2020): 343-418.

27 Pires, Telmo, Eva Schlinger, and Dan Garrette. "How multilingual is multilingual BERT?" *arXiv preprint arXiv:1906.01502* (2019).

28 Schuster, Sebastian, Sonal Gupta, Rushin Shah, and Mike Lewis. "Cross-lingual transfer learning for multilingual task oriented dialog." *arXiv preprint arXiv:1810.13327* (2018).

Özünde, bu gelişmiş yapay zeka çeviri teknikleri FIMI TTP'lerinin erişimini ve etkinliğini önemli ölçüde artırmaktadır. Dil engellerini ortadan kaldırarak dezenformasyon kampanyalarının küresel kitlelere ulaşmasını ve dilsel ve kültürel farklılıklardan yararlanmasını sağlarlar. Tekniklerdeki bu genişleme, dilsel çeşitliliği dikkate alan sağlam çok dilli dezenformasyon tespit stratejileri ve dijital okuryazarlık programları geliştirmenin aciliyetinin altını çizmektedir.

4. Duygusal Manipülasyon için Duygu Analizi:

Duygu analizinin FIMI alanına entegrasyonu, kullanılan taktiklerde endişe verici bir değişim getirmektedir. Genellikle fikir madenciliği olarak adlandırılan duygu analizi, bir metinde ifade edilen fikirleri tanımlamak ve kategorize etmek için kullanılan bir süreçtir. Bu teknik ağırlıklı olarak bir yazarın bir konuya ilişkin tutumunu (olumlu, olumsuz veya nötr) ayırt etmek için kullanılır. İnce Taneli Duygu Analizi olarak adlandırılan karmaşık bir duygu analizi yaklaşımı, temel pozitif, negatif veya nötr sınıflandırmaların ötesine geçer ve neşe, öfke, üzüntü ve daha fazlası gibi duyguları kapsar.

Google'ın BERT'i veya OpenAI'nin GPT'leri gibi son teknoloji modeller, ince taneli duygu analizi için uyarlanabilir.²⁹ FIMI ortamında, bu teknik devlet aktörleri tarafından belirli konulara veya gruplara yönelik korku veya öfke gibi belirli duyguları arttırmak için kullanılabilir ve bu da toplumsal kutuplaşmayı yoğunlaştırabilir. Yabancı bir kuruluşun seçmenler arasında öfke ve bölünmeyi kışkırtmak için bu tekniği kullanabileceği çekişmeli bir seçimi düşünün. Öte yandan, Unsur Tabanlı Duygu Analizi (ABSA), genel içerikten ziyade bir metindeki belirli yönler veya niteliklerle ilgili duygu analizine odaklanır.³⁰ Bu teknik, bir durumun ya da bireyin belirli yönlerini hedef alarak kamuoyu duyarlılığını orantısız bir şekilde etkileyebilir ve bu da kamuoyu manipülasyonuna giden açık bir yoldur. Örnek vermek gerekirse, yabancı bir aktör bir halk sağlığı krizi sırasında ABSA'yı kullanarak hükümetin kriz yönetimi yaklaşımına karşı halkın hoşnutsuzluğunu artırabilir ve böylece anlaşmazlık ve huzursuzluğu körükleyebilir.

Tekrarlayan Sinir Ağları (RNN'ler) ve Evrimsel Sinir Ağları (CNN'ler) gibi Derin Öğrenme tekniklerinin ortaya çıkışı, duygu analizinin doğruluğunu önemli ölçüde artırmıştır.³¹ Ancak bu yöntemler, kamuoyunda belirli duygusal tepkileri tetiklemek üzere uyarlanmış içeriklerin oluşturulması ve yayılması yoluyla duygusal manipülasyonu optimize etmek için de kullanılabilir. Yabancı bir aktörün bu teknikleri kullanarak bir tarafa sempati, diğer tarafa ise düşmanlık uyandıran mesajlar üretmesi ve bunun sonucunda kamuoyunu etkilemesi ve potansiyel olarak diplomatik sonuçları etkilemesi uluslararası bir askeri çatışma için örnek olabilir.

29 Mathew, Leeja, and V. R. Bindu. "A review of natural language processing techniques for sentiment analysis using pre-trained models." In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 340-345. IEEE, 2020.

30 Nazir, Ambreen, Yuan Rao, Lianwei Wu, and Ling Sun. "Issues and challenges of aspect-based sentiment analysis: A comprehensive survey." IEEE Transactions on Affective Computing 13, no. 2 (2020): 845-863.

31 Lim, Wootae, Daeyoung Jang, ve Taejin Lee. "Konvolüsyonel ve tekrarlayan sinir ağları kullanarak konuşma duygusu tanıma." 2016 Asya-Pasifik sinyal ve bilgi işleme derneği yıllık zirvesi ve konferansı (APSIPA), s. 1-4. IEEE, 2016.

Son olarak, Çok Modlu Duygu Analizi, duygu tahmin doğruluğunu artırmak için metin, ses ve video gibi girdileri birleştiren gelişmiş bir tekniktir.³² Bu teknik, içeriğin genellikle birden fazla moda yayıldığı sosyal medya ortamlarında özellikle güçlüdür. FIMI perspektifinden bakıldığında, bir devlet aktörü, toplumsal bozulmayı amaçlayan duygusal olarak yankı uyandıran, çok yönlü dezenformasyon kampanyaları oluşturmak için bu tekniği kullanabilir. Örneğin, tartışmalı bir ticaret anlaşmasına ilişkin müzakerelerin ortasında, yabancı kuruluşlar çok modlu duygu analizini kullanarak kamuoyunun duygularını anlamaya karşı yönlendirebilir ve böylece politika sonuçlarını etkileyebilir.

Özetle, bu gelişmiş duygu analizi teknikleri, halkın duygularını artıran bir hassasiyet ve bağımlılıkla manipüle ederek FIMI taktiklerinin etkisini önemli ölçüde artırma potansiyeline sahiptir. Bu tür dezenformasyonun neden olduğu duygusal yapı ve kutuplaşma, etkilerine karşı koymada önemli zorluklar ortaya çıkarmakta ve böylece bu gelişen tehditlerle mücadele etmek için gelişmiş tespit tekniklerinin, kamu eğitimi girişimlerinin ve kapsamlı düzenlemelerin geliştirilmesi gerekliliğinin altını çizmektedir.

5. Dil Modeli Mikro-Ölçek Ayarı:

Dil Modeli İnce Ayarı tekniklerinin kullanımı sayısız NLP uygulamasında artış göstermektedir. Bu süreç, önceden var olan modellerin belirli veri kümeleri üzerinde uyarlanarak belirli görevler için daha uygun hale getirilmesini ve dil modellerinin verimliliğinin ve etkinliğinin önemli ölçüde artırılmasını içerir. Bununla birlikte, bu gelişmeler aynı zamanda özellikle FIMI alanında kötüye kullanım için yeni yollar açmaktadır.

Bu alandaki gelişmiş teknikler arasında Alana Özgü İnce Ayar bulunmaktadır. Bu yaklaşım, bir modelin belirli bir alandaki veriler üzerinde ince ayar yaparak o alandaki metni daha iyi anlamasını ve üretmesini sağlar.³³ Siyasi söylem üzerinde ince ayar yapılmış bir model düşünün; ikna edici siyasi propaganda üretmede daha etkili olacaktır. FIMI ile uğraşan bir devlet aktörü, daha ikna edici ve bağlama uygun dezenformasyon üretmek için hedef ülkenin dili ve kültürel yönleri üzerine bir modele ince ayar yapabilir.

Bir diğer taktik ise, yanıltıcı veya taraflı çıktılar üretmek için bir modelde ince ayar yapmayı içeren Adversarial Fine-Tuning'dir.³⁴ Bir FIMI senaryosunda, bu teknik bir devlet aktörü tarafından içerik denetleme algoritmalarından geçecek şekilde tasarlanmış dezenformasyon yaratmak için kullanılabilir. Siyasi bir kriz sırasında, otomatik denetim sistemlerini harekete geçirmeden etnik gerilimleri kışkırtan anlatılar üretmek için düşmanca ince ayar kullanılabilir. Bu, tüm sosyal

32 Soleymani, Mohammad, David Garcia, Brendan Jou, Björn Schuller, Shih-Fu Chang ve Maja Pantic. "Çok modlu duygu analizi üzerine bir araştırma." *Image and Vision Computing* 65 (2017): 3-14.

33 Cui, Yin, Yang Song, Chen Sun, Andrew Howard, and Serge Belongie. "Large scale fine-grained categorization and domain-specific transfer learning." In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 4109-4118. 2018.

34 Chen, Tianlong, Sijia Liu, Shiyu Chang, Yu Cheng, Lisa Amini, and Zhangyang Wang. "Adversarial robustness: From self-supervised pre-training to fine-tuning." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 699-708. 2020.

6. Bağlamsal Analiz ve Taklitçilik:

Yapay zeka alanındaki, özellikle de Bağlamsal Analiz ve Taklitçilik teknikleri alanındaki gelişmelerin çeşitli alanlarda derin etkileri olmuştur. Bu araçlar özellikle NLP alanında önemli bir rol oynamaktadır. Bu gelişmeler yeni olasılıkların önünü açarken, özellikle FIMI alanında kötüye de kullanılabilir.

En gelişmiş yapay zeka modelleri, Bağlamsal Varlık Tanıma olarak bilinen bir yetenekle donatılmıştır. Esasen, bu modeller bir metin parçasında geçen kişiler, kuruluşlar ve yerler gibi varlıkların içinde bulunduğu bağlamı kavrayabilir.³⁷ Örneğin, "Apple yeni bir ürün çıkardı" cümlesinde, bu modeller bağlama dayanarak "Apple"ı bir meyve değil, bir teknoloji şirketi olarak tanımlayacaktır. Ne yazık ki, bu incelikli anlayış, FIMI senaryolarında, devam eden konuşmalara veya tartışmalara sorunsuz bir şekilde uyan dezenformasyonu özelleştirmek ve böylece yanlış anlatıları daha ikna edici hale getirmek için kullanılabilir. Örneğin, ²⁰¹⁹ Amazon Yağmur Ormanları orman yangınları sırasında, çevre STK'ları tarafından kasıtlı olarak yakıldığını öne süren manipüle edilmiş anlatılar, bağlamsal olarak sosyal medya tartışmalarına eklenmiş ve yanlış anlatının daha fazla yayılmasına ve kabul edilmesine yol açmıştır.³⁸

Aynı zamanda, YZ modelleri Bağlamsal Taklitçiliğe izin veren bir karmaşıklık derecesine ulaşmıştır. Bu modeller belirli kaynakların ya da bireylerin tarzını, tonunu ve bağlamsal nüanslarını taklit edebilir.³⁹ Bir FIMI senaryosunda bu durum, görünüşte güvenilir kişi veya kurumlardan kaynaklanan yanlış beyan veya makalelerin yaratılmasıyla sonuçlanabilir. Bu durum Myanmar, Malezya ve Endonezya gibi ülkelerde görülmüş, önde gelen politikacıları taklit eden YZ tarafından üretilen ifadeler yayılmış ve seçim dönemlerinde seçmenler arasında yaygın bir kafa karışıklığına ve güvensizliğe neden olmuştur.⁴⁰ Son olarak, bu YZ modelleri gelişmeye devam ettikçe, Bağlamsal Adaptasyon yeteneklerini göstermeye başlıyorlar. Çıktılarını farklı bağlamlara uyacak şekilde ayarlayabilir, esnekliklerini ve taklit yeteneklerini geliştirebilirler. Bu özellik, FIMI'de dezenformasyonu farklı platformlara, kültürlere veya demografik özelliklere uyarlamak ve etkinliğini artırmak için kullanılabilir. Örneğin, Güney Çin Denizi'nde devam eden bölgesel anlaşmazlıklar sırasında, yerel dillere ve kültürel nüanslara göre uyarlanmış dezenformasyon anlatıları, bölgesel gerilimleri alevlendirmek için kullanılmış ve bu gelişmiş yapay zeka teknolojilerinin kötüye kullanıldığında potansiyel tehlikelerini ortaya koymuştur.⁴¹

37 Cucchiarelli, Alessandro, and Paola Velardi. "Unsupervised named entity recognition using syntactic and semantic contextual evidence." *Computational Linguistics* 27, no. 1 (2001): 123-131.

38 de Moraes, Rodrigo Fracalossi. "Demagoguery, populism, and foreign policy rhetoric: evidence from Jair Bolsonaro's tweets." *Contemporary Politics* 29, no. 2 (2023): 249-275.

39 Hess, Ursula, and Agneta Fischer. "Emotional mimicry: Why and when we mimic emotions." *Social and personality psychology compass* 8, no. 2 (2014): 45-57.

40 Tan, Netina. "Electoral management of digital campaigns and disinformation in East and Southeast Asia." *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 214-239.

41 Nguyen, Dennis, and Erik Hekman. "A 'new arms race'? Framing China and the USA in AI news reporting: A comparative analysis of the Washington Post and South China Morning Post." *Global Media and China* 7, no. 1 (2022): 58-77.

SOSYAL MEDYA PLATFORMLARI VE ALGORITMA TABANLI TEKNOLOJİLER

Son on yılda sosyal medya platformları dezenformasyonu hızla yayma güçlerini ortaya koymuştur. Algoritmik beslemeler, doğruluğuna bakılmaksızın sansasyonel veya ilgi çekici içeriğe öncelik verebilir ve potansiyel olarak yanlış bilginin viral yayılımına katkıda bulunabilir. Sosyal medya platformları ve algoritmaları dezenformasyon ve FIMI ortamının şekillenmesinde önemli bir rol oynamaktadır. Bu platformlar ve algoritmalarındaki teknik gelişmeler, aldatıcı içeriğin hızla yayılmasını ve güçlendirilmesini sağlayarak, kamuoyunu manipüle etmek isteyen kötü niyetli aktörler için onları güçlü araçlar haline getirmiştir. İşte bunların etkilerine dair genişletilmiş bir analiz:

1. Algoritmik Dezenformasyon / Programlamalı Propaganda:

İçeriği yaymak ve teşvik etmek için sosyal medya platformu algoritmalarından yararlanan güçlü bir teknik olan Algoritmik Güçlendirme, dezenformasyonun yayılmasında temel bir rol oynamaktadır. Bu tekniğin önemi, kötü niyetli aktörleri erişim alanlarını genişletmek ve etkilerini artırmak için araçlarla donattığı için FIMI ortamında özellikle belirgin hale gelmektedir. Bu alanda sayısız sofistike taktik gelişmiştir.

Bu taktiklerden biri olan Mikro Hedefleme, demografik profillerine, ilgi alanlarına veya davranış kalıplarına göre belirlenen belirli kullanıcı gruplarına odaklanır.⁴² Dezenformasyonun stratejik kullanımı, etkilenme olasılığı en yüksek olan bireylere özel mesajlar iletmek için mikro hedeflemeden yararlanır. Bu taktiğin dikkat çekici bir örneği, mikro hedefleme iddialarının ortaya çıktığı²⁰¹⁶ Brexit kampanyası sırasında ortaya çıkmıştır. Belirli seçmen grupları, Birleşik Krallık'ın Avrupa Birliği'nden ayrılmasının sonuçlarıyla ilgili olarak, mali tasarruflarla ilgili abartılı iddialardan göçmenlik kontrolüyle ilgili asılsız iddialara kadar değişen yanıltıcı bilgilere maruz bırakılmıştır.⁴³

Dijital ortam aynı zamanda Sosyal Botların ve Cyborg'ların yaygın kullanımına da tanık oldu. Sosyal botlar, sosyal medyada kullanıcılarla ya da diğer botlarla etkileşime giren otomatik hesaplardır; siborglar ise otomatik faaliyeti insan jirdisiyle harmanlayan hesapları temsil etmektedir.⁴⁴ Bu varlıklar, içerikle etkileşime girerek dezenformasyonun erişimini artırmak için kullanılır; bu da sosyal medya algoritmalarını kandırarak içeriğin popüler olarak algılanmasına ve daha geniş bir alana yayılmasına yol açabilir. Fransa'da 2022 yılında yapılan cumhurbaşkanlığı seçimleri sırasında, sosyal botların seçim sahtekarlığı ile ilgili yanlış anlatıları güçlendirmek, belirsizliği ve siyasi gerginliği artırmak için kullanıldığı bildirilmiştir.⁴⁵

42 Barbu, Oana. "Advertising, microtargeting and social media." *Procedia-Social and Behavioral Sciences* 163 (2014): 44-49.

43 Šimunjak, Maja. *Tweeting Brexit: social media and the aftermath of the EU referendum*. Routledge, 2022.

44 Gorwa, Robert, and Douglas Guilbeault. "Unpacking the social media bot: A typology to guide research and policy." *Policy & Internet* 12, no. 2 (2020): 225-248.

45 Shahid, Wajih, Yiran Li, Dakota Staples, Gulshan Amin, Saqib Hakak, and Ali Ghorbani. "Are you a cyborg, bot or human?—a survey on detecting fake news spreaders." *IEEE Access* 10 (2022): 27069-27083.

Bir başka teknik olan Hashtag Zehirlenmesi (ya da ele geçirme), dezenformasyon yaymak için trend olan hashtag'leri birlikte kullanmayı içerir.⁴⁶ Bu, kötü niyetli aktörlerin içeriklerini daha geniş, şüphelenmeyen bir kitleye göstermelerine olanak tanır. 2022'deki Çin COVID protestoları sırasında Çin hükümeti, protesto içeriklerini yaymak ve dikkati protestoyla ilgili hashtag'leri takip eden veya kullanan kullanıcılardan uzaklaştırmak için hashtag'leri ele geçirmekle suçlanmıştı⁴⁷. Deepfake Amplifikasyonu önemli bir zorluk olarak ortaya çıkmıştır. Yapay zeka ile oluşturulan hiper-gerçekçi videolar olan Deepfake'ler, özellikle içerik tartışmalı veya sansasyonel olduğunda, sosyal medya aracılığıyla yaygın bir şekilde yayılabilir ve algoritmalar tarafından teşvik edilebilir. Avustralya'da 2023 yılında yapılan federal seçimler sırasında, önde gelen bir adayın deepfake videosu geniş çapta paylaşılmış ve seçmenler arasında kafa karışıklığına ve güvensizliğe yol açarak deepfake teknolojisinin kötüye kullanıldığında potansiyel zararlarını ortaya koymuştur.⁴⁸

Son olarak, Etkileşim Yemleme, içeriğin beğeniler, paylaşımlar ve yorumlar gibi kullanıcı etkileşimini teşvik etmek için hazırlandığı ve potansiyel olarak algoritmik güçlendirme ile sonuçlanan bir tekniktir.⁴⁹ Dezenformasyon sansasyonel ya da bölücü içeriklerle eşleştirildiğinde güçlü tepkilere yol açabilir ve sonuç olarak daha hızlı yayılabilir. Bu taktik, 2023'te Nijerya'da yapılan genel seçimlerde açıkça görülmüş, yanlış bilgiler genellikle duygu yüklü veya sansasyonel içeriklerle eşleştirilerek etkileşimi artırmayı ve böylece erişimini büyütmeyi amaçlamıştır.⁵⁰

2. Kişiselleştirilmiş İçerik Sunumu:

Sosyal medya algoritmaları, her bir kullanıcının tercihleri ve davranış kalıplarıyla uyumlu içerikleri düzenlemek üzere tasarlanmıştır. Bu kişiselleştirilmiş içerik sunumu, genellikle kullanıcıların mevcut inanç ve ideolojilerini yansıtan bilgilerin sunulmasına yol açmakta ve böylece yankı odaları olarak adlandırılan dijital bir ortamı teşvik etmektedir. Bu seçici bilgi sunumu, teyit önyargılarını güçlendirebilir ve bireyleri kendi bakış açılarına uygun dezenformasyona karşı daha duyarlı hale getirebilir. Sosyal medya platformlarında içeriği belirli kişi veya gruplara göre uyarlamak için kullanıcı verilerinden yararlanan Kişiselleştirilmiş İçerik Sunumu yaygın bir tekniktir.

Genellikle kullanıcı katılımını ve deneyimini geliştirmek için kullanılsa da, FIMI için de manipüle edilebilir. Mikro Hedefleme ve Davranışsal Profillemeye gibi teknikler bu alanda özellikle güçlü araçlardır. Daha önce de belirtildiği gibi mikro hedefleme, demografik özelliklerine, ilgi alanlarına veya çevrimiçi davranışlarına

46 VanDam, Courtland, and Pang-Ning Tan. "Detecting hashtag hijacking from twitter." In Proceedings of the 8th ACM Conference on Web Science, pp. 370-371. 2016.

47 China accused of flooding social media with spam to crowd out protest news. The Guardian. 4 Dec 2022. <https://www.theguardian.com/world/2022/dec/04/china-accused-of-flooding-social-media-spam-covid-protests>

48 Vasist, Pramukh Nanjundaswamy, and Satish Krishnan. "Deepfakes: an integrative review of the literature and an agenda for future research." Communications of the Association for Information Systems 51, no. 1 (2022): 14.

49 Zhang, Wanjiang Jacob, Jingjing Yi, and Hai Liang. "I cue you liking me: Causal and spillover effects of technological engagement bait." Computers in Human Behavior (2023): 107864.

50 Nigerian elections 2023: False claims and viral videos debunked. BBC Africa. 28 February 2023. <https://www.bbc.com/news/world-africa-64797274>

göre belirli gruplara belirli içeriklerin sunulmasını içerir.⁵¹ Bir kullanıcının çevrimiçi davranışlarından ayırt edilen kalıplar aracılığıyla kapsamlı profiller oluşturan bir yöntem olan davranışsal profillemeye ile birleştirildiğinde etkinliği artar. Bu profiller daha sonra bireysel kullanıcılar ya da gruplar arasında güçlü bir yankı uyandıran yüksek hedefli dezenformasyonun sunulmasını sağlar. Örneğin, 2019'daki Tayland genel seçimleri sırasında, belirli demografik gruplara göre uyarlanmış yanıltıcı anlatılar yayarak seçmenlerin duygularını etkilemek için mikro hedefleme taktiklerinin kullanıldığına dair raporlar vardı.⁵²

Uyarlanabilir Haber Kaynağı Algoritmaları bir başka kritik yönü temsil etmektedir. Sosyal medya platformları tarafından kullanılan bu algoritmalar, bir kullanıcının haber akışını geçmiş davranışlarına, ilgi alanlarına ve etkileşimlerine göre özelleştirir. Bu, kullanıcıların öncelikle önceden var olan bakış açılarını güçlendiren içeriğe maruz kaldıkları "filtre baloncuklarının" oluşmasına yol açabilir. Böyle bir ortam dezenformasyonu güçlendirmek için istismar edilebilir. Dezenformasyon hayaleti, Yapay Zeka Tarafından Oluşturulan Kişiselleştirilmiş İçerik üzerinde de belirmektedir. Gelişmiş yapay zeka modellerinin ortaya çıkmasıyla, daha önce görülmemiş ölçekte kişiselleştirilmiş dezenformasyon yaratmak mümkün. Her bir içerik parçası, belirli bir kullanıcının ilgi alanlarına, önyargılarına ve inançlarına hitap edecek şekilde titizlikle uyarlanabilir ve bu da onu önemli ölçüde daha ikna edici hale getirir. Henüz bununla ilgili büyük ölçekli bir jeopolitik olay kapsamlı bir şekilde rapor edilmemiş olsa da, bu durum gelecekteki potansiyel risklerle birlikte ortaya çıkmakta olan bir endişe alanını temsil etmektedir. Deepfake Kişiselleştirme ek bir karmaşıklık katmanı getirmektedir. Kişiselleştirme, özellikle deepfake'lerin ortaya çıkmasıyla birlikte metinlerin ötesine geçerek görüntü ve videoları da kapsayabilir.⁵³ Deepfake'ler tanıdık figürleri taklit edecek ya da kullanıcının inançları veya korkularıyla uyumlu senaryolar yaratacak şekilde uyarlanabilir. Örneğin, 2023 Arjantin genel seçimleri sırasında, uydurma senaryolara dahil olan siyasi adayların deepfake'leri geniş çapta yayılmış, önemli ölçüde kafa karışıklığına ve yanlış bilgilendirmeye neden olmuştur.⁵⁴

3. Mikro Hedefleme ve Kitle Segmentasyonu:

Sosyal medya platformları, sofistike algoritmalarıyla, içeriğin farklı kullanıcı gruplarına hassas bir şekilde iletilmesini kolaylaştıran bir özellik olan mikro hedeflemeyi mümkün kılmıştır. Bu özellik, kullanıcı deneyimini geliştirmede ve pazarlama stratejilerini kolaylaştırmada faydalı olmakla birlikte, özellikle FIMI alanında potansiyel kötüye kullanımı da barındırmaktadır. Kötü niyetli aktörler, hedeflenen demografik gruplar arasında dezenformasyon yaymak, kamuoyunu stratejik olarak etkilemek ve toplumsal bölünmeleri istismar etmek için bu özelliği kullanabilir.

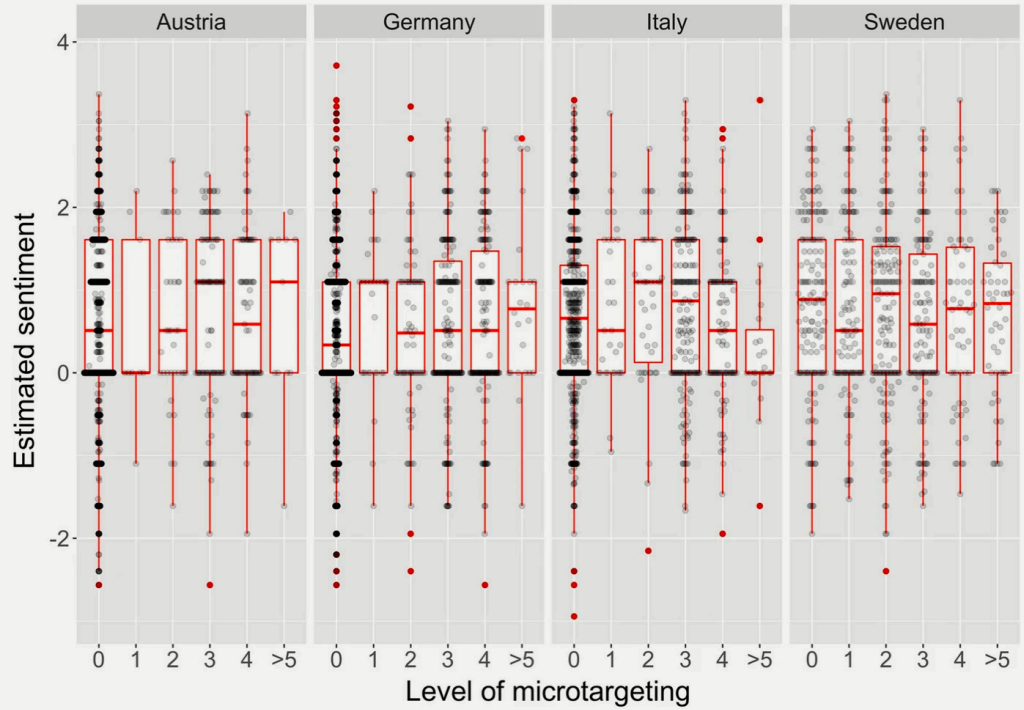
51 Schäwel, Johanna, Regine Frener, and Sabine Trepte. "Political microtargeting and online privacy: A theoretical approach to understanding users' privacy behaviors." *Media and Communication* 9, no. 4 (2021): 158-169.

52 Wanless, Alicia, and Michael Berk. "The audience is the amplifier: Participatory propaganda." *The Sage handbook of propaganda* (2020): 85-104.

53 Khan, Ihtiram Raza, Saman Aisha, Deepak Kumar, and Tabish Mufti. "A Systematic Review on Deepfake Technology." *Proceedings of Data Analytics and Management: ICDAM 2022* (2023): 669-685.

54 Riera, Ariel, and Laura Sommer. "Using fact checking to improve information systems in Argentina." *The political quarterly* 91, no. 3 (2020): 600-604.

Mikrohedefleme ve Kitle Segmentasyonu, farklı bireylere veya gruplara özel içerik sağlayarak bu konuda çok önemli teknikler olarak hizmet vermektedir. Bu alanda özellikle etkili bir yöntem, sosyal medya kullanıcılarının ayrıntılı profillerinin oluşturulmasını içeren Psikografik Profillemedir.⁵⁵ Bu profiller çevrimiçi davranışlar, ilgi alanları, tutumlar ve hatta kişilik özellikleri de dahil olmak üzere bir dizi veriyi içermektedir. Bu tekniğin önemli bir uygulamasının 2016 ABD Başkanlık Seçimleri sırasında Cambridge Analytica tarafından gerçekleştirildiği iddia edilmektedir. Ancak benzer taktikler dünyanın başka yerlerinde de rapor edilmiştir. Örneğin, 2018'deki Brezilya Başkanlık Seçimleri ya da 2019'daki İspanya seçimleri sırasında, psikografik profillemenin kişiye özel siyasi reklamlar yoluyla seçmen davranışını etkilemek için kullanıldığı iddia edilmiştir.⁵⁶



Psikografik profilleme, bilgi manipülasyonunu belirli ülkelere uyarlamak için kullanıldığında en iyi sonucu verir. Bununla birlikte, çok fazla mikro hedefleme azalan getiriler yaratır. Kaynak: López Ortega, A. Mikro hedefli kampanya mesajları daha olumsuz ve çeşitli mi? Avrupa seçim kampanyalarındaki Facebook reklamlarının analizi. *Eur Polit Sci* 21, 335-358 (2022). <https://doi.org/10.1057/s41304-021-00346-6>

Bir diğer önemli teknik olan Coğrafi Mikro Hedefleme, içeriğin kullanıcıların coğrafi konumlarına göre uyarlanmasına olanak tanır. Hindistan'da 2019 yılında yapılan genel seçimlerde, bölgesel gerilimleri kıskırtmak ve oy verme davranışını etkilemek için coğrafi hedefli yanlış bilgilerin kullanıldığına dair iddialar ortaya çıkmıştır. Bu durum özellikle halihazırda yerel huzursuzluklara veya siyasi anlaşmazlıklara sahne olan bölgelerde daha belirgindi.

55 Bakir, Vian. "Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting." *Frontiers in Communication* 5 (2020): 67.

56 Baviera, Tomás, Lorena Cano-Orón, and Dafne Calvo. "Tailored messages in the feed? Political microtargeting on Facebook during the 2019 General Elections in Spain." *Journal of Political Marketing* (2023): 1-20.

Davranışsal Hedefleme, gelecekteki davranışları tahmin etmek ve potansiyel olarak etkilemek için bir bireyin çevrimiçi tıklama kalıpları, arama geçmişi ve sayfa ziyaretleri gibi geçmiş davranışlarına ilişkin verileri kullanan bir başka yöntemdir. Nijerya’da 2019 yılında yapılan genel seçimler sırasında, davranışsal hedeflemenin siyasi içerikleri duyarlı bireylere yaymak, toplumsal bölünmeleri artırmak ve seçmen duyarlılığını kutuplaştırmak için kullanıldığı bildirilmiştir. Yapay Zeka, mikro hedeflemenin hassasiyetini büyük ölçüde artırma potansiyeline sahiptir.

Yapay Zeka ile Geliştirilmiş Mikro Hedefleme, büyük veri kümelerini analiz etmek için yapay zeka kullanır ve son derece hassas kitle segmentasyonuna ve daha verimli mikro hedeflemeye olanak tanıyan incelikli kalıpları tanımlar. Bu tekniğin FIMI’de yaygın kullanımı kapsamlı bir şekilde belgelenmemiş olsa da, bu tür büyük ölçekli, yüksek hedefli dezenformasyon kampanyalarının yarattığı potansiyel risk göz ardı edilemez. Son olarak, Benzer Kitle Hedefleme, tipik olarak mevcut destekçilerden veya istenen bir hedef gruptan oluşan bir “tohum” kitle profili oluşturmayı ve ardından bu profile benzeyen kullanıcıları bulmak ve hedeflemek için sosyal medya algoritmalarından yararlanmayı içeren bir tekniktir.

Başlangıçta bir pazarlama aracı olsa da, dezenformasyon için duyarlı bireylerin belirlenmesi ve hedeflenmesi yoluyla siyasi istismar potansiyeli endişe kaynağı haline gelmiştir. Örneğin, 2022’deki Kenya genel seçimleri sırasında, belirli demografik gruplara dezenformasyon dağıtmak için Benzer Kitle Hedeflemenin kullanıldığına dair iddialar ortaya çıkmıştır. Bu gelişmiş teknikler, son derece hedefli ve etkili dezenformasyon kampanyaları için potansiyelin altını çizmekte ve veri kullanımında daha fazla şeffaflık, gizlilik konusunda daha sıkı düzenlemeler ve halk arasında kapsamlı dijital okuryazarlık eğitiminin gerekliliğini vurgulamaktadır.

4. Otomatik Bot Hesapları:

Bu hesaplar, hızlı ve ekonomik bir şekilde hacimli içerik üretme kapasiteleri nedeniyle sosyal medya manipülasyonunda temel bir araçtır. Bu botlar, içerik yayınlamak ve paylaşmaktan kullanıcıları takip etmeye ve onlarla arkadaş olmaya kadar çeşitli görevleri yerine getirmek üzere programlanabilmektedir. Kamusal söylemi çarpıtmak, dezenformasyonu yaymak ve bölücü mesajları güçlendirmek için kullanılmışlardır. Uygulamalarının incelikleri ve potansiyel zararları, birkaç gelişmiş tekniğin araştırılmasıyla incelenebilir.

İçerik Amplifikasyon Botları bu tekniklerden biridir. Bu botlar, belirli içerik veya mesajları sosyal medya platformlarında geniş çapta yaymak için tasarlanmıştır. Temel olarak paylaşımları retweetleyerek, beğenerek ya da paylaşarak görünürlüklerini ve algılanan popülerliklerini artırır. Bunun çarpıcı bir örneği 2016 Kolombiya Barış Referandumu sırasında görüldü. Burada, içerik güçlendirme botları kutuplaştırıcı anlatıları ve yanlış bilgileri yaymak için kullanılmış, böylece kamusal

söylemi çarpıtmış ve hükümetin FARC isyancılarıyla yaptığı barış anlaşmasını reddeden dar oylama sonucunu potansiyel olarak etkilemiştir.⁵⁷

Sybil Botları başka bir örnek sunmaktadır. Adını çoklu kişilik bozukluğu teşhisi konulan Sybil Dorsett'in ünlü vakasından alan bu botlar, sosyal ağlarda birden fazla sahte kimlik oluşturur. Dezenformasyonu yaygın bir şekilde yayabilir, bir mesajı gerçekte olduğundan daha popülermiş gibi gösterebilir ve bir kullanıcının takipçi sayısını yapay olarak şişirebilirler. Bu manipülasyon, 2019'daki Güney Afrika genel seçimleri sırasında Sybil botlarının kamu duyarlılığını ve söylemini manipüle etmek için kullanıldığı ve sosyal medya platformlarındaki siyasi konuşmaları çarpıttığı açıktı.

Sosyal Botlar başka bir otomatik hesap kategorisini oluşturur. İnsan kullanıcılarla arkadaşlık kurarak ya da onları takip ederek etkileşime girerler ve böylece onların sosyal ağlarına erişim sağlarlar. Bu noktadan hareketle dezenformasyonu doğrudan bu ağlara sokabilirler. Filipinler'de 2016 başkanlık seçimleri sırasında sosyal botların kullanımı rapor edilmiştir. Bu botlar sosyal ağlara sızmış ve bölücü içerikler yayarak oldukça kutuplaşmış bir siyasi ortama katkıda bulunmuştur. Influencer Botlar ise etkili sosyal medya kullanıcılarıyla etkileşime girer. Amaçları bu etki sahiplerini kendi dezenformasyonlarını yaymaya ikna etmektir. 2019'daki Endonezya genel seçimleri sırasında, influencer botları yanıltıcı mesajları yaymak için yerel influencer'ları hedef aldı ve kamuoyunun kutuplaşmasına katkıda bulundu.⁵⁸ Son olarak, tek bir varlık tarafından kontrol edilen bot ağları olan Botnet'ler, mesajları veya dezenformasyonu daha etkili bir şekilde koordine etme ve yayma potansiyeline sahiptir. Bu teknik, 2020 Tayvan genel seçimleri sırasında, Twitter'ın yanlış bilgi ve dezenformasyon yayarak kamu söylemini bozmaya çalışan önemli bir botnet'i dağıttığı sırada kullanılmıştır.⁵⁹

Bu teknikler, botların artan karmaşıklığını ve FIMI operasyonlarında potansiyel kötüye kullanımlarını vurgulamaktadır. Bu tehdidin ele alınması teknolojik, düzenleyici ve eğitici girişimleri içeren çok yönlü bir yaklaşım gerektirmektedir. Giderek dijitalleşen bir dünyayla karşı karşıya olduğumuz için, bu aldatıcı taktikleri anlamak ve bunlarla mücadele etmek, kamusal söylemin ve demokratik süreçlerin bütünlüğünü korumak için daha da önemli hale gelmektedir.

- 57 Gallego, Jorge, Juan D. Martínez, Kevin Munger, and Mateo Vásquez-Cortés. "Tweeting for peace: Experimental evidence from the 2016 Colombian Plebiscite." *Electoral Studies* 62 (2019): 102072.
- 58 Uyheng, Joshua, and Kathleen M. Carley. "Characterizing bot networks on Twitter: An empirical analysis of contentious issues in the Asia-Pacific." In *Social, Cultural, and Behavioral Modeling: 12th International Conference, SBP-BRIMS 2019, Washington, DC, USA, July 9-12, 2019, Proceedings* 12, pp. 153-162. Springer International Publishing, 2019.
- 59 Uyheng, Joshua, and Kathleen M. Carley. "Computational analysis of bot activity in the Asia-Pacific: A comparative study of four national elections." In *Proceedings of the international AAAI conference on web and social media*, vol. 15, pp. 727-738. 2021.

5. Sosyal Mühendislik ve Tıklama Yemi Taktikleri:

Kötü niyetli aktörler, kullanıcıları dezenformasyonla etkileşime girmeye ikna etmek için sosyal mühendislik ve tıklama tuzağı taktiklerinden yararlanır. Akılda kalıcı başlıklar, duygu yüklü görseller ve aldatıcı bilgiler kullanarak tıklama oranlarını artırmayı ve böylece dezenformasyonun görünürlüğünü ve etkisini büyütmeyi hedefler. Sosyal mühendislik ve tıklama tuzağı stratejileri, dezenformasyonu yaymak, anlaşmazlıkları körüklemek ve kamuoyunu etkilemek için insan merakını, önyargılarını ve güvenini kullandıklarından, sosyal medya manipülasyonu dünyasındaki en ustaca taktiklerden bazılarını temsil etmektedir.

Kimlik avı kampanyaları, genellikle meşru bilgi talepleri veya tıklama istemleri gibi görünen yanıltıcı mesajların gönderildiği popüler bir sosyal mühendislik biçimi olarak hizmet eder. Bu taktikler genellikle hassas verilere erişmek için kullanılsa da, dezenformasyon yaymaya veya güvenilir ağlara kötü amaçlı içerik enjekte etmeye de yardımcı olabilirler. Bunun bir örneği, başarılı bir kimlik avı kampanyasının önde gelen adayın ekibinden hassas belgelerin sızmasına yol açarak önemli bir kesinti ve siyasi skandalı tetiklediği 2018'deki Meksika genel seçimleri sırasında yaşandı.⁶⁰

Bir başka teknik de sahte kişilikler yaratmak ya da gerçek kişi veya kuruluşların kimliğine bürünmektir. Bu, kötü niyetli aktörlere dezenformasyon kampanyaları için güvenilirlik görüntüsü verir. Bu durum, Nijerya'da 2019 yılında yapılan genel seçimler sırasında Twitter'ın Nijerya vatandaşı gibi davranan ancak aslında yabancı bir dezenformasyon operasyonunun parçası olan bir hesap açını tespit edip kaldırmasıyla gözlemlenmiştir.⁶¹ Kötü niyetli aktörler, kullanıcıların katılımını ve dezenformasyon paylaşma olasılığını artırmak için genellikle duyguları istismar eder ve öfkeyi körükler. Bu teknik, duygu yüklü ve yanıltıcı içeriğin sosyal medya platformlarında yoğun bir şekilde paylaşıldığı, toplumsal bölünmeleri derinleştirdiği ve hararetli kamuoyu tartışmalarını körüklediği 2018 Malezya genel seçimleri sırasında açıkça görülmüştür.

Clickbait başlıklar ve aldatıcı başlıklar, dikkat çekmek ve tıklamaları kışkırtmak için kullanılan bir başka yaygın stratejidir ve genellikle kullanıcıları hikayenin gerçek özümüyle hiçbir ilgisi olmayan veya önemli ölçüde çarpıtılan içeriğe yönlendirir. Bu taktik, 2019'daki İsrail yasama seçimleri sırasında yoğun bir şekilde kullanıldı ve kullanıcıları yanlış veya aldatıcı bilgilerle dolu web sitelerine yönlendirerek kamusal söylemi önemli ölçüde çarpıttı.⁶² Pretexting, kullanıcıları bilgi vermeleri, bağlantılara tıklamaları veya içerik paylaşmaları için kandırmak amacıyla makul bir bahane veya senaryo oluşturulmasını içeren başka bir tekniktir. 2020 Covid-19 salgını sırasında, bu yöntem İran ve Brezilya da dahil olmak üzere çok sayıda ülkedeki dezenformasyon kampanyalarında bariz bir şekilde görüldü. Kriz, hastalık, hastalığın kökenleri ve tedavileri hakkında yanlış bilgi yaymak için bir bahane

60 Mexico election: Concerns about election bots, trolls and fakes. BBC Monitoring. 30 May 2018. <https://www.bbc.com/news/blogs-trending-44252995>
61 Oyeboode, Oladapo, and Rita Orji. "Social media and sentiment analysis: the Nigeria presidential election 2019." In 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 0140-0146. IEEE, 2019.
62 Mourão, Rachel R., and Craig T. Robertson. "Fake news as discursive integration: An analysis of sites that publish false, misleading, hyperpartisan and sensational information." *Journalism studies* 20, no. 14 (2019): 2077-2095.

olarak kullanılmış, kamuoyunda kafa karışıklığına yol açmış ve etkili halk sağlığı müdahalelerini engellemiştir.⁶³

Bu taktikler, FIMI kampanyalarında sosyal mühendislik ve tıklama tuzağı stratejilerinde kullanılan gelişmiş ve çeşitli yöntemleri vurgulamaktadır. Bu tehditlere karşı koymak için, bu taktikler hakkında kamu eğitimi, gelişmiş dijital okuryazarlık ve sofistike tespit ve azaltma araçlarının geliştirilmesi ve konuşlandırılması dahil olmak üzere bütünsel bir yaklaşım gereklidir.

DERİN YANILTMA (DEEPAKES) VE GÖRSEL-İŞİTSEL MANİPÜLASYON

Deepfakes, izleyicileri yanıltmak amacıyla videoları, görüntüleri veya sesleri inandırıcı bir şekilde değiştirmek için yapay zekayı kullanır. Ses manipülasyonu teknolojileri, kulağa son derece gerçek gelen sahte sesler üreterek gerçek ses kayıtlarının sahtelerinden ayırt edilmesini zorlaştırabilir. Deepfakes ve ses manipülasyonu, dezenformasyon kampanyalarının cephaneliğinde güçlü araçlar olarak ortaya çıkmıştır. Bu teknolojiler kötü niyetli aktörlerin son derece gerçekçi ve aldatıcı içerikler oluşturmaya olanak tanıyarak gerçek ve manipüle edilmiş bilgileri ayırt etmeyi giderek zorlaştırmaktadır.

1. Video Manipülasyonu Olarak Deepfake:

Deepfake ve video manipülasyon tekniklerinin ortaya çıkışı, sosyal medya manipülasyonu alanında giderek artan bir zorluk teşkil etmektedir. Bu sofistike teknolojiler, kamuoyu duyarlılığını büyük ölçüde etkileyebilecek inanılmaz derecede gerçekçi sahte medyanın üretilmesini sağlar. "Deepfake" terimi, video ve ses içeriğini gerçekmiş gibi göstermek için oluşturabilen veya değiştirebilen yapay zeka tabanlı teknoloji ile ilişkilidir. Bu teknoloji, gerçek görüntülerden öğrenerek, bir kişiyi gerçekte hiç yapmadığı bir şeyi söylerken ya da yaparken gösterebilen inandırıcı bir sahte üretebilir. Bunun çarpıcı bir örneği, 2021 Peru genel seçimleri sırasında, adayların deepfake videolarının geniş çapta yayılması, kafa karışıklığına neden olması ve video içeriğinin doğruluğu hakkında sorulara yol açması sırasında meydana geldi.⁶⁴ Güney Kore'deki 2023 başkanlık seçimleriyle ilgili bir başka olayda, bazıları adayları kışkırtıcı ve yanlış ifadeler kullanırken gösteren birkaç deepfake yayınlandı. Bu olaylar seçmenlerin kafasını karıştırmaya hizmet etmiş ve normal seçim söylemini bozmuştur.⁶⁵

Video sahtekarlıkları, yapay zeka ve makine öğreniminin, özellikle de derin öğrenme tekniklerinden yararlanılarak gerçekleştirilen sofistike bir uygulamasıdır. Özünde

63 Ceron, Wilson, Mathias-Felipe de-Lima-Santos, and Marcos G. Quiles. "Fake news agenda in the era of COVID-19: Identifying trends through fact-checking content." *Online Social Networks and Media* 21 (2021): 100116.

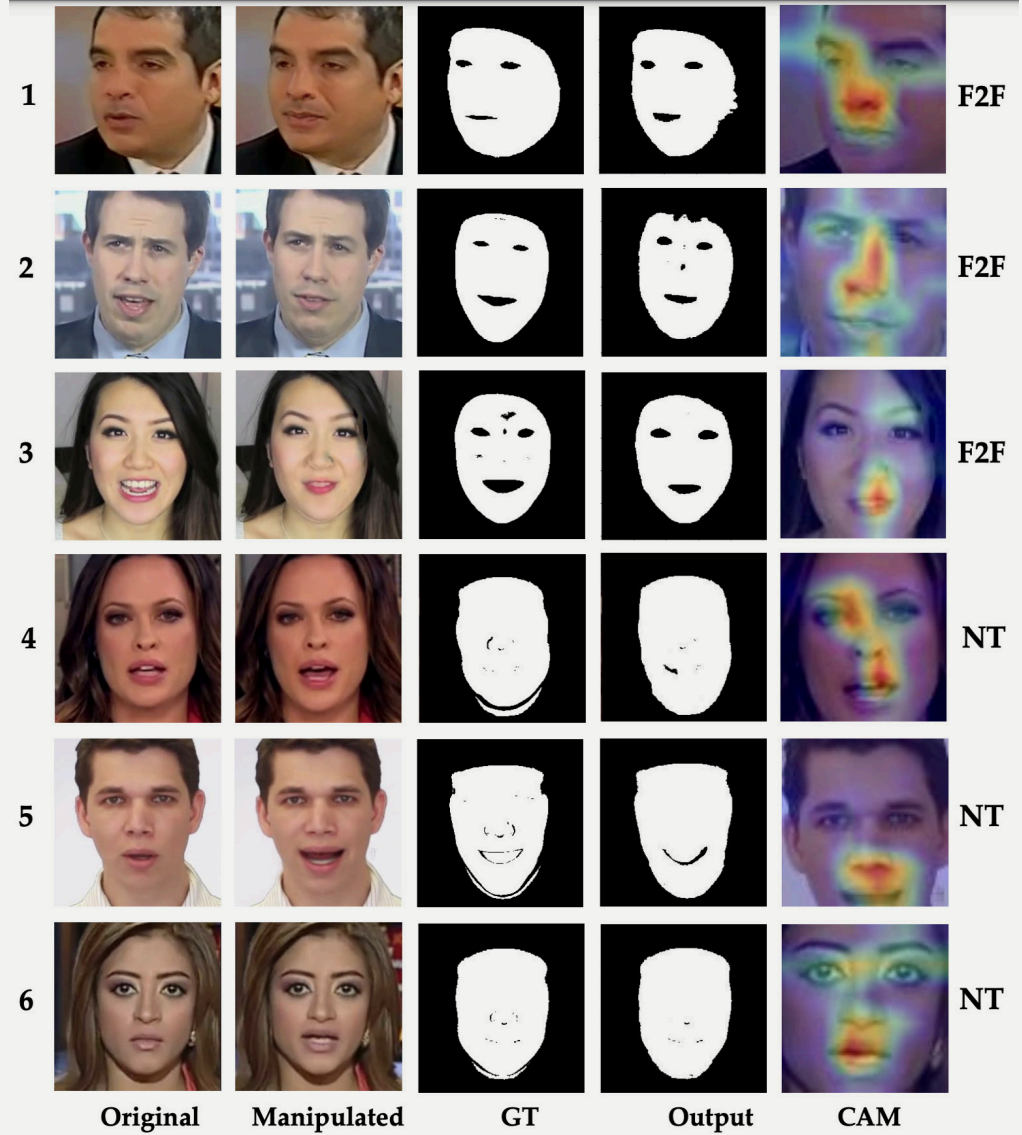
64 Pashentsev, Evgeny, and Darya Bazarkina. "Malicious Use of Artificial Intelligence and Threats to Psychological Security in Latin America: Common Problems, Current Practice and Prospects." In *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, pp. 531-560. Cham: Springer International Publishing, 2023.

65 Pashentsev, Evgeny. "The Malicious Use of Deepfakes Against Psychological Security and Political Stability." In *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, pp. 47-80. Cham: Springer International Publishing, 2023.

deepfake'ler, videodaki bir kişi ya da nesnenin aslında söylemediği ya da yapmadığı bir şeyi söylüyormuş ya da yapıyormuş gibi görünmesini sağlamak amacıyla video içeriğini manipüle etmek ve değiştirmek için derin sinir ağlarının kullanılmasının sonucudur. "Deepfake" terimi "derin öğrenme" ve "sahte" kelimelerinin birleşiminden oluşmaktadır. Bir deepfake video oluşturma süreci birkaç temel adımı içerir. Başlangıçta, bir deepfake yaratıcısının, genellikle hedef bireyin veya nesnenin büyük miktarda video görüntüsünü içeren eğitim verilerini toplaması gerekir. Bu veriler, hedefin görsel ve işitsel özelliklerini öğrenmekten ve taklit etmekten sorumlu olan derin bir sinir ağını eğitmek için temel oluşturur. Video sahteciliği oluşturmada kullanılan temel teknoloji, üretken düşman ağlarıdır (GAN'lar).

GAN'lar iki ana bileşenden oluşur: bir üretici ve bir ayırt edici. Üretecin görevi sahte içerik üretmek, ayırtıcının görevi ise gerçek ve sahte içeriği ayırt etmektir. Her iki bileşen de rekabetçi bir öğrenme sürecine girerek birlikte çalışır. Eğitim süreci, GAN'ı hedef bireyin gerçek video verileriyle besleyerek başlar ve jeneratör sahte videolar üretmeye başlar. Başlangıçta, üretilen bu videolar düşük kalitededir ve gerçek olanlardan kolayca ayırt edilebilir. Ayırtıcı daha sonra gerçek ve üretilmiş videoların bir karışımı üzerinde eğitilerek bunlar arasında ayırım yapmayı öğrenir.

Zamanla, üretici daha ikna edici sahteler yaratma becerisini geliştirir ve ayırt edici ince farklılıkları tespit etmede daha becerikli hale gelir. Bu yinelenmeli eğitim süreci, üretici, ayırt edicinin gerçek olanlardan ayırt etmesi zor olan sahte videolar üretene kadar devam eder. Bu noktada deepfake yaratıcısı, gerçek gibi görünen ikna edici video içeriği üretebilen iyi eğitilmiş bir modele sahip olur. Belirli bir deepfake video oluşturmak için, eğitilmiş modele yeni ses veya yüz hareketleri gibi girdiler verilir ve model bunlara karşılık gelen sahte video kareleri üretir. Örneğin, amaç videodaki bir kişinin söylemediği bir şeyi söylemesini sağlamaksa, deepfake modeli hedef bireyin orijinal yüz ifadelerini ve hareketlerini korurken istenen sesle beslenebilir. Üreteç daha sonra dudakları ve yüz özelliklerini yeni ses girdisiyle eşleşecek şekilde hizalayan video kareleri üreterek ikna edici bir deepfake video elde eder.



Birinci ve ikinci sütunlar sırasıyla orijinal görüntüleri ve manipüle edilmiş görüntüleri göstermektedir. Üçüncü sütundaki siyah ve beyaz görüntüler, ikili GT maskelerine karşılık gelmektedir. Face2Face (satır 1,2,3) ve Neural-Textures (satır 4,5,6) veri kümesinden manipüle edilmiş görüntüler için tahmin edilen maskeler (sütun 4) ve oluşturulan CAM'ler (sütun 5). Kaynak: Mazaheri, Ghazal ve Amit K. Roy-Chowdhury. "Yüz ifadesi manipülasyonlarının tespiti ve lokalizasyonu." IEEE/CVF Winter Conference on Applications of Computer Vision Bildiriler Kitabı içinde, s. 1035-1045. 2022.

2. Ses Manipülasyonu ve Ses Sentezi:

Metin-konuşma (TTS) sentezi ve ses klonlama gibi ses manipülasyon teknikleri, insan konuşmasını yakından taklit eden sentetik seslerin yaratılmasında devrim yaratmıştır. TTS teknolojisi, yazılı metni doğal insan tonlamasını ve ritmini yakından yansıtan konuşmaya dönüştürür. Ses klonlama teknolojisi ise nispeten az miktarda örnek ses verisine dayanarak belirli bir bireyin sesini kopyalar. Yapay zekanın ilerlemesi, ses manipülasyonu ve ses sentezi teknolojilerinde bir devrim yarattı.

Sonuç olarak, artık hiper-gerçekçi ve çoğu zaman ayırt edilemeyen sahte ses içeriği üretmek mümkün.

Özellikle ses klonlama, en önemli gelişmelerden biri olarak öne çıkıyor. Bu teknoloji, bir kişinin benzersiz sesini doğru bir şekilde kopyalamak için yapay zekayı kullanıyor. Yapay zeka sistemi, kişinin konuşma örneğiyle eğitildikten sonra, klonlanmış sesle yeni diyaloglar oluşturabilir ve orijinal kişinin hiç söylemediği kelimeleri söyleyebilir.⁶⁶ Bu teknolojinin kötüye kullanım potansiyelinin endişe verici bir göstergesi, 2019 yılında Euler Hermes Group'un Alman CEO'su Rüdiger Kirsch'in bir dolandırıcılığın kurbanı olmasıyla görüldü. Kirsch, amirinin sesini ikna edici bir şekilde taklit eden bir ses klonlama yapay zekası tarafından kandırılarak önemli miktarda para transfer etti. Bu tür olaylar, hızla gelişen bu teknolojik tehditlerle acilen mücadele edilmesi gerektiğinin altını çizmektedir.⁶⁷

Metinden sese sentezleme, bu alandaki bir diğer önemli yapay zeka ilerlemesidir. Bu teknoloji yazılı metinleri sözlü kelimelere dönüştürerek kulağa son derece doğal ve insan benzeri gelen ses içerikleri ortaya çıkarır. Potansiyel kullanım alanları arasında ikna edici sahte radyo yayınları veya telefon görüşmeleri oluşturmak ve dezenformasyon için yeni bir platform sağlamak yer alıyor. Örneğin, 2023'te Nijerya genel seçimleri sırasında, yanlış bilgi yayan sahte radyo yayınları iddiaları ortaya çıktı, ancak TTS teknolojisinin kullanımı kesin olarak kanıtlanmadı, bu da bu girişimlerin gerçekleştirilmesinden sonra bile doğrulanmasının sorunlu doğasına işaret ediyor.⁶⁸

Video deepfakelerine benzer şekilde, ses 'deepfakeleri' de belirli bir bireyin sesini taklit etmek için makine öğrenimi modellerini kullanır. Ses klonlama ve ses sahteciliği arasındaki fark genellikle gelişmişlik ve gerçekçilik seviyesinde yatar; ses sahteciliği genellikle daha ikna edici bir taklit sunar. Gerçek zamanlı ses sahteciliğinin ortaya çıkışı özellikle önemli bir tehdit oluşturmaktadır.

Teknolojik gelişmeler, Filipinler'de 2022 yılında yaşanan ve bir politikacının sesinin canlı bir radyo programı sırasında taklit edilerek yaygın bir kafa karışıklığına ve tartışmaya neden olduğu olayda olduğu gibi, canlı konuşmalar sırasında başka birinin kimliğine bürünmeyi mümkün kılmıştır. Bu teknikler potansiyel olarak gerçek zamanlı siyasi senaryolarda tahribat yaratabilir, dolandırıcılığı mümkün kılabilir veya sosyal mühendislik saldırılarını yönlendirebilir. Ses manipülasyon tekniklerinin sürekli ilerlemesi, FIMI operasyonlarında potansiyel kötüye kullanımlarını vurgulamaktadır. Yaygın kullanılabilirlikleri göz önüne alındığında, sağlam tespit mekanizmaları geliştirmeye, güvenlik protokollerini iyileştirmeye ve bu aldatıcı uygulamaların potansiyeli ve etkileri konusunda halkı eğitmeye acil ihtiyaç vardır.

66 Almutairi, Zaynab, and Hebah Elgibreen. "A review of modern audio deepfake detection methods: challenges and future directions." *Algorithms* 15, no. 5 (2022): 155.

67 Pashentsev, Evgeny. "The Malicious Use of Deepfakes Against Psychological Security and Political Stability." In *The Palgrave Handbook of Malicious Use of AI and Psychological Security*, pp. 47-80. Cham: Springer International Publishing, 2023.

68 Bola Tinubu's Nigeria election win: The rigging claims of Peter Obi and Atiku Abubakar. BBC Africa. 1 March 2023. <https://www.bbc.com/news/world-africa-64802490>

HEDEFLEMELİ REKLAMCILIK VE MİKROHEDEFLEME

Hedefli reklamcılık ve mikro hedefleme, dijital reklamcılık ortamını yeniden şekillendiren iki etkili pazarlama stratejisini temsil etmekle birlikte, aynı zamanda FIMI'nin amaçları doğrultusunda da kullanılmaktadır. Bu teknikler, belirli demografik özelliklere, bireylere veya niş gruplara kişiselleştirilmiş reklam içeriği sunmak için çeşitli dijital platformlardan toplanan büyük miktarda tüketici verisinden yararlanır. Bu teknik metinde, teknolojik temelleri, veri analizi yöntemlerini ve kullanılan algoritmaları inceleyerek hedefli reklamcılığın ve mikro hedeflemenin arkasındaki karmaşık mekaniği araştıracağız.

1. Veri Toplama ve Kullanıcı Profili Oluşturma:

Hedefli reklamcılık, ayrıntılı kullanıcı profilleri oluşturmak için kapsamlı veri toplamaya dayanır. Sosyal medya platformları ve diğer çevrimiçi hizmetler, kullanıcıların demografik özellikleri, ilgi alanları, davranışları ve tercihleri hakkında bilgi toplayarak reklamverenleri bireysel kullanıcılar hakkında bilgilendiren zengin bir veri seti oluşturur.

Sosyal medya platformları, özellikle veri bilimi tekniklerinin karmaşıklığının artmasıyla birlikte, veri toplama ve kullanıcı profili oluşturmanın merkezi haline gelmiştir. Günlük etkileşimler ve etkileşimlerden muazzam miktarda veri toplanmakta ve bu veriler daha sonra kapsamlı kullanıcı profilleri oluşturmak için gelişmiş veri bilimi metodolojileri kullanılarak işlenmekte ve analiz edilmektedir. Bu profiller, kötüye kullanıldığında, Yabancı Bilgi Manipülasyonu ve Müdahalesi (FIMI) için güçlü araçlar olarak hizmet edebilir.

İşte bazı gelişmiş tekniklere ve bunların FIMI Taktikleri, Teknikleri ve Prosedürleri (TTP'ler) üzerindeki etkilerine genel bir bakış

- **Metadata Analizi:** Meta veriler veya veriler hakkındaki veriler, kullanıcı davranışları ve tercihleri hakkında çok şey ortaya çıkarabilir. Örneğin, paylaşımların zamanı ve sıklığı, coğrafi konum verileri ve paylaşım için kullanılan cihaz türü, kullanıcı alışkanlıkları ve tercihleri hakkında değerli bilgiler sunar. Örneğin, meta veriler 2019 Kanada Federal Seçimleri sırasında çok önemli bir rol oynamıştır. Kullanıcıların coğrafi konum verilerinin ayrıntılı analizi, yabancı aktörler tarafından oy verme davranışlarını etkilemek üzere tasarlanmış kişiselleştirilmiş siyasi içeriklerle belirli demografik grupları belirlemek ve hedeflemek için kullanılmıştır.
- **Sosyal Ağ Analizi (SNA):** SNA, bireyler arasındaki ilişkileri görselleştirme ve analiz etme yöntemidir. Bireylerin birbirleriyle nasıl bağlantı kurduklarını ve etkileşime girdiklerini inceleyerek grup dinamikleri çıkarılabilir, etkili bireyler belirlenebilir ve bilgi akışı kalıpları tespit edilebilir. Bu teknik, 2020 yılında Amerika Birleşik Devletleri'ndeki

Black Lives Matter protestoları sırasında bölücü söylemleri güçlendirmek için çeşitli aktörler tarafından kullanılmış ve mevcut toplumsal bölünmeleri siyasi kazanç için istismar etmiştir.

- **Makine Öğrenimi ve Yapay Zeka Analitiği:** Gelişmiş algoritmalar, büyük miktarda veriyi işlemek ve analiz etmek, kalıpları, eğilimleri ve korelasyonları tanımlamak için kullanılır. Bu sayede son derece hassas kullanıcı segmentasyonu, davranış tahmini ve içerik kişiselleştirmesi yapılabilmektedir. Örnek olarak, oy tercihlerini tahmin etmek ve özelleştirilmiş siyasi reklamlar sunmak için makine öğrenimi modellerinin kullanıldığı Japonya'daki 2021 genel seçimleri gösterilebilir.
- **Duygu Analizi:** Bu, sosyal medya paylaşımlarının ardındaki duyguları analiz etmek için Doğal Dil İşleme (NLP) kullanılmasını içerir. Belirli konulara veya varlıklara yönelik kamuoyu duyarlılığını anlayarak, aktörler bu duyguları istismar eden mesajlar tasarlayabilirler. 2020 Hong Kong protestoları sırasında, duygu analizi yabancı aktörler tarafından hoşnutsuzluğu körüklemek ve siyasi gerilimi arttırmak için kullanıldı.
- **Psikografik Profil Oluşturma:** Bu, insanları tutumlarına, isteklerine ve diğer psikolojik kriterlerine göre sınıflandırmayı içerir. 2020 Tayland siyasi protestoları sırasında, psikografik profilleme yabancı aktörler tarafından memnuniyetsizliği körüklemek ve siyasi gerilimi tırmandırmak için kullanıldı.

Bu gelişmiş tekniklerin FIMI TTP'leri üzerindeki etkisi derindir. Bireylerin davranışlarını büyük ölçekte anlama, tahmin etme ve manipüle etme yeteneği, dış ilişkilere müdahale etmek veya kamuoyunu etkilemek isteyenler için güçlü araçlar sunmaktadır. Bu durum, veri gizliliği düzenlemelerinin iyileştirilmesi, karşı önlemlerin geliştirilmesi ve kamuoyunun verilerinin nasıl kullanılabileceği konusunda eğitilmesi için sürekli çaba sarf edilmesini gerektirmektedir.

2. Algoritmik Hedefleme ve Reklam Yerleştirme:

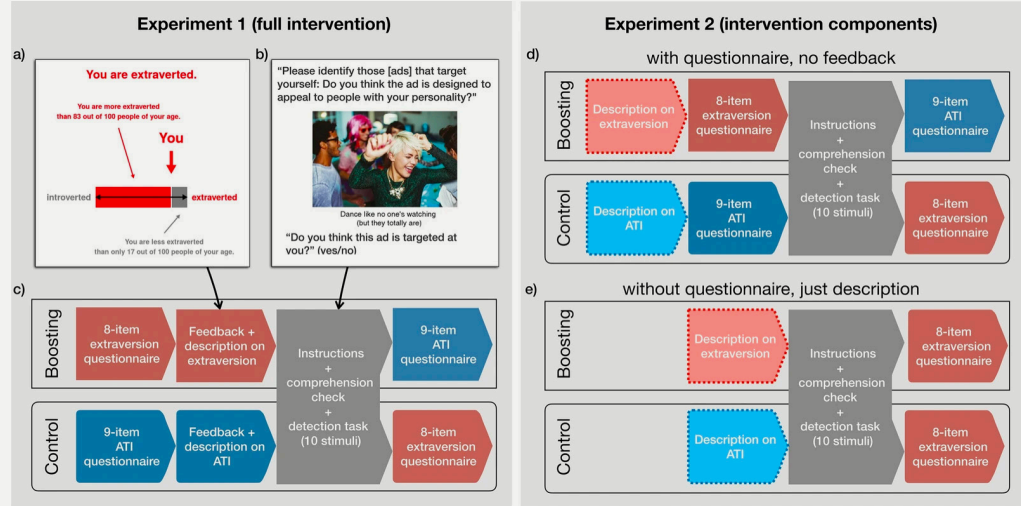
Gelişmiş algoritmalar, her bireye gösterilecek en uygun içeriği belirlemek için kullanıcı profillerini ve davranışlarını analiz eder. Bu algoritmalar, kişiselleştirilmiş reklamlar sunmak için konum, tarama geçmişi ve etkileşim kalıpları gibi faktörleri dikkate alır. Sosyal medyada algoritmik hedefleme ve reklam yerleştirme, bilgi manipülasyonu ve bastırma üzerinde önemli etkileri olan ve hızla gelişen bir alandır:

- **Benzer Kitle Hedefleme,** bilinen bir kullanıcı grubuna benzerlikleri nedeniyle belirli bir mesaja açık olabilecek potansiyel yeni kullanıcıları belirlemek için kullanılan güçlü bir araçtır. Bu teknik, 2016 Brexit referandumu sırasında, çeşitli siyasi kuruluşların mevcut destekçilerini yansıtan bireylere erişimlerini genişletmek için benzer kitle hedeflemeyi kullandıklarında dikkate değer bir etkinlikle kullanıldı. Bu, kampanya mesajlarını güçlendirdi ve etkilerini pekiştirdi. Benzer bir şekilde, Hindistan'daki 2019

genel seçimleri sırasında bazı siyasi partiler, potansiyel destekçilerine ulaşmak için Facebook gibi platformlarda bulunan geniş kullanıcı verilerinden yararlanarak seçmen tabanlarını genişletmek için benzer kitle hedeflemesinden yararlandı.

- Reklam Yerleşimi için Tahmine Dayalı Analitik, geçmiş verilere dayanarak gelecekteki sonuçları tahmin etmek için makine öğrenimi ve istatistiksel algoritmalarından yararlanır. Reklamverenler, maksimum etki için hangi reklamların hangi kullanıcılara hangi zamanlarda gösterilmesi gerektiğini belirleyerek reklam yerleşimlerini optimize etmek için tahmine dayalı analitikten yararlanır. Seçmenlerin korkularını ve önyargılarını istismar etmek üzere tasarlanmış hiper-hedefli reklamlar sunmak için tahmine dayalı analitiğin kullanıldığı iddia edilen 2018 Brezilya başkanlık seçimleri aydınlatıcı bir örnektir. Benzer şekilde, 2020 Güney Kore yasama seçimleri sırasında, kampanya mesajlarını farklı demografik gruplara göre uyarlamak ve reklamların etkisini en üst düzeye çıkarmak için tahmine dayalı analitik kullanılmıştır.
- Gerçek Zamanlı Teklif (RTB), reklam envanterinin anlık bir açık artırma yoluyla gösterim başına işlem gördüğü programatik reklamcılığın ayrılmaz bir bileşenidir. Bu, hassas mikro hedefleme ve verimli reklam yerleşimi sağlar. RTB, 2019 Avustralya federal seçimleri sırasında kapsamlı bir şekilde kullanıldı ve kampanyalar bu özellikten yararlanarak önemli seçmen gruplarını hedefleyen reklam alanları için rekabetçi teklifler verdi.
- Davranışsal Hedefleme, görüntülenen sayfalar, arama sorguları ve tıklanan bağlantılar dahil olmak üzere kitleleri çevrimiçi davranış kalıplarına göre segmentlere ayıran bir stratejidir. Bu teknik, kişiselleştirilmiş siyasi reklamların çevrimiçi davranışlarına göre belirli oy bloklarına sunulduğu 2020 Tayvan başkanlık seçimleri öncesinde kullanılmıştır. Benzer şekilde, 2021 İsrail genel seçimleri sırasında, belirli demografik gruplara yönelik yüksek düzeyde hedeflenmiş siyasi mesajlar sunmak için davranışsal hedefleme kullanılmıştır.
- Mikro hedefleme genellikle, belirli kullanıcılara yönelik reklamlar olan ve genel halk tarafından görülemeyen Karanlık Reklamların kullanımını içerir. Bu reklamları oluşturmak için kullanıcıların çevrimiçi davranışlarını, ilgi alanlarını ve demografik özelliklerini inceleyen gelişmiş yapay zeka ve makine öğrenimi algoritmaları kullanılmaktadır. Bu tekniklerin Yabancı Bilgi Manipülasyonu ve Müdahalesi (FIMI) Taktikleri, Teknikleri ve Prosedürleri (TTP'ler) üzerinde önemli etkileri vardır, çünkü son derece özelleştirilmiş dezenformasyon kampanyalarının oluşturulmasını sağlarlar. Karanlık reklamların daha geniş kamu incelemesinden korunarak gizlice dolaşıma sokulması, bireylerin ve grupların ince bir şekilde manipüle edilmesine olanak tanır. Özellikle, 2020 Myanmar genel seçimleri sırasında, karanlık reklamlar çeşitli aktörler tarafından bölücü siyasi mesajları yaymak için kullanıldı ve incelemeyi atlamak için sınırlı görünürlükten yararlandı.
- A/B Testi ve İçerik Optimizasyonu, hangisinin en iyi yanıtı verdiğini belirlemek için içeriğin farklı sürümlerini karşılaştırmayı içerir. Mikro hedefleme, ayrıntılı düzeyde

A/B testine ve etkileşimi en üst düzeye çıkarmak için içeriğe ince ayar yapılmasına olanak tanır. Dijital pazarlama dünyasında sıklıkla kullanılan bu yöntemler, FIMI Taktikleri, Teknikleri ve Prosedürleri (TTP'ler) bağlamında dikkate değer uygulamalara sahiptir. Aktörler, A/B testi ve içerik optimizasyonunu kullanarak dezenformasyon kampanyalarının etkinliğini artırabilir. Örneğin, 2018 Meksika genel seçimleri sırasında, A/B testi çeşitli aktörler tarafından siyasi mesajlarını rafine etmek ve seçmen katılımını en üst düzeye çıkarmak için kullanılmıştır.



Son yıllarda anket deneyleri ile profil oluşturma tekniklerinden yararlanan çok sayıda mikro hedefleme optimizasyon çalışması yapılmıştır. Kaynak: Lorenz-Spreen, P., Geers, M., Pachur, T. ve diğerleri. İnsanların mikro hedefli reklamları tespit etme becerilerinin artırılması. *Sci Rep* 11, 15541 (2021). <https://doi.org/10.1038/s41598-021-94796-z>

TÜRKİYE'DE DEZENFORMASYON EKOSİSTEMİ

Türkiye'deki dezenformasyon ekosistemine ilişkin kapsamlı bir analiz daha önce EDAM tarafından yayımlanmıştı.⁶⁹ Son yıllarda Türkiye, bilgi ortamında dezenformasyonun yaygınlaşmasıyla mücadele etmektedir. Dijital teknolojilerin ve sosyal medya platformlarının yükselişi, yanlış anlatıların, yanıltıcı içeriklerin ve manipülatif propagandanın erişimini ve etkisini artırarak demokrasinin dokusunu tehdit ediyor. Türkiye'nin dezenformasyon ekosisteminin labirentinde, modern iletişim kanallarının zayıflıklarından faydalanan çeşitli rahatsız edici aldatıcı içerik türleri gelişmiştir. Üzerinde oynanmış görüntüler, manipüle edilmiş videolar ve değiştirilmiş ses kayıtlarını içeren manipüle edilmiş medya, gerçekliği çarpıtmak ve yanlış anlatılar üretmek için akıllıca hazırlanmıştır. Gelişmiş düzenleme araçları ve deepfake teknolojisi, faillerin son derece ikna edici dezenformasyon yaratmalarını sağlayarak ortalama bir kullanıcının gerçek ve manipüle edilmiş içerik arasında ayırım yapmasını zorlaştırmıştır. Dezenformasyon, Türkiye'de bir iletişim anomalisi olmaktan ziyade, hem muhalefet hem de hükümet kanalları tarafından sistematik olarak kullanılan bir siyasi iletişim biçimidir.

Yanlış iddialar ve komplo teorileri dezenformasyon kampanyalarında stratejik bir rol oynamakta, insanların duygularını sömürmekte ve toplumsal fay hatlarını istismar etmektedir. Psikolojik hedefleme ve mikro segmentasyon tekniklerinin kullanımı, belirli hedef kitlelerde yankı uyandırmak için dezenformasyon anlatılarının şekillendirilmesinde yaygın hale gelmiştir. Örneğin, 2016 darbe girişiminin ardından, belirli demografik gruplar arasında korku ve öfkeyi kışkırtmak için sosyal medya platformları aracılığıyla hem hükümet yanlısı hem de hükümet karşıtı duyguların yanlış anlatıları yayılmış, bu da kutuplaşmanın ve toplumsal huzursuzluğun artmasına yol açmıştır.⁷⁰ Çevrimiçi trollemenin yükselişi ve koordineli dezenformasyon kampanyalarının yaygınlaşması belki de sorunun en sinsi yönleri. İyi organize olmuş gruplar ya da bireyler, eşi benzeri görülmemiş bir hız ve ölçekte yanlış anlatıları yaymak için sosyal medyadan yararlanmaktadır. Otomasyon ve sosyal medya botlarının kullanımı dezenformasyonu güçlendirerek kısa bir süre içinde milyonlarca kullanıcıya ulaşmasını sağlar. Bu kampanyalar genellikle sosyal medya platformlarındaki algoritmik önyargılardan yararlanarak daha yüksek etkileşim sağlayan sansasyonel ve bölücü içeriklere öncelik vermekte ve aldatıcı anlatıların yayılmasını istemeden de olsa kolaylaştırmaktadır.⁷¹

Türkiye’de 2023 yılında yapılacak seçimler öncesinde dezenformasyon önemli bir endişe kaynağı olarak ortaya çıktı. Hem Cumhurbaşkanı Recep Tayyip Erdoğan hem de muhalefet lideri Kemal Kılıçdaroğlu birbirlerini aldatıcı taktikler uygulamakla suçladılar. Bir örnekte, bir mitingde Kılıçdaroğlu’nun yasaklı PKK üyeleriyle aynı çizgide olduğu izlenimi veren bir video montajı gösterildi.⁷² Kılıçdaroğlu, Erdoğan’ın ekibi tarafından işe alınan ‘yabancı hackerları’ seçim öncesinde rakiplerini itibarsızlaştırmak için deepfake içerik hazırlamakla suçladı.⁷³ Dezenformasyon kullanımı sosyal medya platformlarında yoğunlaştı ve her iki taraf da birbirlerine karşı suçlamalarda bulundu. Türkiye parlamentosu ‘sahte haberlerin’ yayılmasını suç sayan bir yasayı kabul etti, ancak eleştirmenler bu yasanın gazeteciler ve eleştirel sesler üzerinde ‘caydırıcı bir etkiye’ yol açtığını savunuyor. Hem hükümet hem de muhalefet saflarından sosyal ağlarda ve toplantılarda yayılan manipüle edilmiş görüntüler ve kırılmış ya da bağlamından koparılmış içerik telaşı. Sahte kampanya broşürleri de kullanılmış, Kılıçdaroğlu’nun ekibinden olduğu iddia edilen bir broşürde Suriye’den askerlerin çekileceği ve PKK’ya karşı askeri operasyonların durdurulacağı vaat edilmiştir.⁷⁴

Dikkate değer bir başka vaka çalışması da Türkiye’nin Suriye’deki çatışmaya müdahil olduğu dönemde dezenformasyonun yayılmasıdır.⁷⁵ Çatışma boyunca, çeşitli aktörler kendi gündemlerini ilerletmek için sosyal medya platformlarını

- 70 Akgül, Harun Güney. “Fake news as a tool of populism in Turkey: The Pastor Andrew Brunson case.” *Polish Political Science Review* 7, no. 2 (2019): 32-51.
- 71 Furman, Ivo, and Asli Tunc. “The end of the Habermassian ideal? Political communication on Twitter during the 2017 Turkish constitutional referendum.” *Policy & Internet* 12, no. 3 (2020): 311-331.
- 72 “Disinformation Adds Dark Note to Pivotal Turkish Election.” *France 24*, 12 May 2023, www.france24.com/en/live-news/20230512-disinformation-adds-dark-note-to-pivotal-turkish-election. Accessed 3 Aug. 2023.
- 73 “Turkey’s Opposition Accuses Russia of Interfering in Elections.” *Al Jazeera*, 12 May 2023, www.aljazeera.com/news/2023/5/12/turkeys-kilicdaroglu-accuses-russia-of-interfering-in-elections. Accessed 3 Aug. 2023.
- 74 Ioannou, Demetrios. “Deepfakes, Cheapfakes, and Twitter Censorship Mar Turkey’s Elections.” *Wired*, 26 May 2023, www.wired.com/story/deepfakes-cheapfakes-and-twitter-censorship-mar-turkeys-elections/. Accessed 3 Aug. 2023.
- 75 Salem, Fatima K. Abu, Roaa Al Feel, Shady Elbassuoni, Mohamad Jaber, and May Farah. “Fa-kes: A fake news dataset around the syrian war.” In *Proceedings of the international AAAI conference on web and social media*, vol. 13, pp. 573-582. 2019.

kullandılar, kamuoyu duyarlılığını manipüle ettiler ve politika kararlarını etkilediler. Suriyeli mülteci krizi, kamuoyunu etkilemeye ve mülteci karşıtı duyguları körüklemeye çalışan dezenformasyon kampanyaları ile Türkiye’de tartışmalı bir konu haline geldi. Mültecileri suç faaliyetleriyle ilişkilendiren ve onları ev sahibi ülkeye ekonomik bir yük olarak gösteren yanlış anlatılar yayıldı. Ayrıca, mültecilerle ilgili olaylara ilişkin sansasyonel ve uydurma hikayeler geniş çapta paylaşılarak Türk toplumunun farklı kesimleri arasındaki bölünmeleri derinleştirdi ve gerilimleri artırdı.

Suriye’deki çatışma sırasında yürütülen dezenformasyon kampanyaları da siyasi çıkarlara hizmet etmek için terörist grupları belirli bir ışık altında göstermeye çalışmıştır. Anlatılar faillere göre değişmekle birlikte, bazı gruplar belirli terör örgütlerinin faaliyetlerini küçümsemeyi veya diğerlerinin oluşturduğu tehdidi abartmayı amaçlamıştır. Ayrıca, sahte haberlerin ve tık tuzağı makalelerin yayılması, hassas siyasi olaylar veya seçimler sırasında dezenformasyon sorununa önemli ölçüde katkıda bulunmuştur. Fırsatçı aktörler, doğruluklarına bakılmaksızın yalnızca yüksek düzeyde etkileşim yaratmak için tasarlanmış sansasyonel hikayelerden ve tıklanmaya değer başlıklardan yararlandılar. Örneğin, seçim dönemlerinde, siyasi adaylar, partiler ve olası sonuçlar hakkında yanlış hikayeler, kafa karışıklığı yaratmak, güvensizlik tohumları ekmek ve seçmenlerin tercihlerini manipüle etmek için kasıtlı olarak yayıldı. Suriye çatışması veya mülteci yönetimi ile ilgili kritik politika kararları sırasında, politika yapımcıları ve kamuoyunu etkilemek için dezenformasyon kampanyaları yürütülmüştür.⁷⁶

Türkiye’deki yabancı devlet kaynaklı dezenformasyon kampanyaları, çeşitli ülkelerin Türk siyasetini, toplumunu ve uluslararası ilişkilerini etkilemeye çalıştığı birkaç önemli vaka ile endişe verici bir eğilim haline gelmiştir. Bilgi savaşındaki uzmanlığıyla bilinen Rusya, Türkiye’de dezenformasyon kampanyaları yürütme konusunda özellikle aktif olmuştur. Öne çıkan vakalardan biri, Rusya’nın Türkiye’nin Suriye’deki askeri müdahalesi ve bölgedeki diğer aktörlerle ilişkileri hakkındaki söylemleri şekillendirme girişimlerini içeriyordu. Rusya’nın devlet kontrolündeki medya kuruluşları ve sosyal medya botları kamuoyunu etkilemek, Türkiye karşıtı duyguları körüklemek ve Türkiye’nin bölgesel girişimlerini baltalamak için yanıltıcı içerikler yaydı. Bu kampanyalar, Türkiye’nin Suriye’deki eylemlerine ilişkin algıları manipüle etmeyi ve ülkeyi küresel sahnede olumsuz bir şekilde göstermeyi amaçlamıştır.

Türkiye ile Avrupa Birliği (AB) arasındaki gerginlik dönemlerinde Türk hükümeti, Avrupa ülkelerini Türkiye’de kamuoyunu ve karar alma mekanizmalarını etkilemek amacıyla dezenformasyon kampanyaları yürütmekle suçlamıştır.⁷⁷ Türkiye ile Avrupalı ortakları arasında anlaşmazlık yaratmak ve AB’yi Türk kamuoyunun gözünde olumsuz göstermek için yanlış anlatılar ve yanıltıcı bilgiler yayıldığı iddia edilmiştir. Örneğin, Yunanistan ve Türkiye’nin uzun bir bölgesel rekabet geçmişi vardır ve dezenformasyon gerilimi arttırmak için kullanılmıştır. Bazı durumlarda,

76 Yerlikaya, Turgay, and Seca Toker Aslan. "Social Media and Fake News in the Post-Truth Era." *Insight Turkey* 22, no. 2 (2020): 177-196. Filibeli, Tirşe Erbaysal, and Can Ertuna. "Sarcasm beyond hate speech: Facebook comments on Syrian refugees in Turkey." *International journal of communication* 15 (2021): 24.

77 Please see Heinrich Böll Stiftung Project on homegrown EU disinformation: <https://eu.boell.org/en/homegrown-disinformation>

Yunanistan'a atfedilen ve Türkiye'nin Ege Denizi ve Kıbrıs'taki eylemlerini çarpıtmayı ve Türkiye'yi saldırgan olarak göstermek için kamuoyu algısını manipüle etmeyi amaçlayan dezenformasyon kampanyaları Türk hükümeti tarafından vurgulanmıştır.⁷⁸ Bu kampanyalar Yunanistan içinde ve uluslararası gözlemciler arasında Türkiye karşıtı duyguları körüklemeyi amaçlamıştır.

Türk-Amerikan ilişkileri ve Türkiye'nin NATO içindeki konumu da kamuoyunun algısını şekillendirmek ve Türk politikalarını etkilemek amacıyla yabancı dezenformasyon kampanyalarının hedefi olmuştur. Bazı durumlarda devlet kaynaklı dezenformasyon Türkiye ile NATO müttefikleri arasında güvensizlik yaratmaya ve Türkiye içinde ittifaka verilen desteği zayıflatmaya çalışmıştır. Türkiye'nin bölgesel güvenlikteki rolünü zayıflatmak ve ülkeyi tartışmalı bir müttefik olarak göstermek için yanlış söylemler yayılmıştır.⁷⁹ Bölgesel çatışma dönemlerinde, özellikle de Azerbaycan ve Ermenistan'ın dahil olduğu Dağlık Karabağ sorunuyla ilgili olarak, hem AB hem de Ermenistan'dan veya sempatanlarından kaynaklanan dezenformasyon kampanyaları Türkiye'yi hedef almıştır. Türkiye'nin bölgedeki rolünü şeytanlaştırmak ve Türkiye karşıtı duyguları körüklemek için yanlış anlatılar yayılmıştır⁸⁰. Bu kampanyalar, Ermenistan'ın çıkarlarını ilerletmek ve Türkiye'nin imajını zedelemek için tarihi şikayetleri ve jeopolitik gerilimleri istismar etmeyi amaçlamıştır. İran ve Türkiye'nin karmaşık ilişkileri vardır ve İran kaynaklı dezenformasyon kampanyaları Türk kamuoyunu etkilemeyi ve İran'ın bölgedeki eylemlerine ilişkin algıları şekillendirmeyi amaçlamıştır. Türkiye'nin bölgesel etkisini zayıflatmak ve Türkiye'nin politikalarını olumsuz göstermek için yanlış anlatılar kullanılmıştır. Bu kampanyalar iki ülke arasında nifak sokmak için dini ve mezhepsel farklılıkları istismar etmeye çalışmıştır.

Otomatik hesaplar ve troller, sosyal medya platformlarını belirli bakış açılarını güçlendiren ve alternatif perspektifleri zayıflatan aldatıcı içeriklerle doldurarak bu kampanyalarda etkili bir rol oynadı. Spesifik bir vakada, Türkiye Büyük Millet Meclisi'nde yeni bir mülteci politikasına ilişkin kritik bir tartışma sırasında, koordineli bir dezenformasyon kampanyası sosyal medya platformlarını yanıltıcı istatistikler, mülteci suçlarına ilişkin yanlış hikayeler ve uydurma kamuoyu muhalefeti hesaplarıyla doldurdu. Bu kampanya, yeni politikaya karşı kamuoyu duyarlılığını etkilemeyi ve hükümetin mülteci krizini ele alışını itibarsızlaştırmayı amaçlıyordu. Dezenformasyon sadece demokratik süreci sekteye uğratmakla kalmadı, aynı zamanda toplumsal bölünmeleri derinleştirdi ve halkın kurumlara olan güvenini aşındırdı.⁸¹

Türkiye'nin dezenformasyon ekosisteminin arkasındaki aktörleri anlamak, oyundaki güdülerini ve stratejilerini kavramak için hayati önem taşımaktadır. Başlıca failer arasında, anlatıyı kontrol etmek, muhalefeti bastırmak veya kamuoyunu kendi lehlerine şekillendirmek için dezenformasyon kampanyalarını kullanabilen devlet

78 Markham, Lauren, and Lydia Emmanouilidou. "How Free Is the Press in the Birthplace of Democracy?" The New York Times, 26 Nov. 2022, www.nytimes.com/2022/11/26/business/greece-journalists-surveillance-predator.html.

79 Bernstein, Jonas. "US Dismisses Russian Allegations of Turkey's Involvement in Trading IS Oil." VOA, 2 Dec. 2015, www.voanews.com/a/russia-claims-to-have-proof-turkey-involved-in-is-oil-trade/3084253.html. Accessed 3 Aug. 2023.

80 Atanesyan, Arthur. "Media framing on armed conflicts: limits of peace journalism on the Nagorno-Karabakh conflict." Journal of intervention and statebuilding 14, no. 4 (2020): 534-550.

81 Saka, Erkan. Social media and politics in Turkey: A journey through citizen journalism, political trolling, and fake news. Lexington Books, 2019.

aktörleri yer almaktadır. Siyasi gruplar da rakiplerini zayıflatmak, seçmenleri etkilemek ve muhalifleri itibarsızlaştırmak için dezenformasyonu kullanarak önemli bir rol oynamaktadır. Genellikle karanlık odaklar tarafından finanse edilen sosyal medya botları ve trolleri, belirli mesajları güçlendirmede ve hem hükümet yanlısı hem de hükümet karşıtı görüşlere yaygın destek olduğu yanlışlamasını yaratmada etkili olmaktadır. Dahası, yabancı aktörler Türk siyasetini etkilemek, nifak tohumları ekmek ve bölgedeki çıkarlarını ilerletmek için dezenformasyon kampanyaları yürütmektedir.⁸²

Yaygın dezenformasyon ekosistemiyle etkin bir şekilde mücadele etmek için Türkiye, sorunun çeşitli yönlerini ele alan kapsamlı bir dizi proaktif önlem alabilir. İlk olarak, dezenformasyon ve hükümet sansürü arasındaki ilişkiyi kabul etmek çok önemlidir. Araştırmalar, dezenformasyonun hükümetlerin serbest bilgi akışını bastırdığı ortamlarda gelişme eğiliminde olduğunu göstermiştir. Dezenformasyonla geniş ölçekte mücadele edebilmek için açık ve özgür bir bilgi ekosistemini teşvik etmek elzemdir. Bu da medya özgürlüğünün güvence altına alınmasını, gazetecilerin haklarının korunmasını ve farklı bakış açılarının sansür veya misilleme korkusu olmadan ifade edilebileceği bir ortamın teşvik edilmesini gerektirir. Bağımsız medyanın ve doğruluk kontrol kuruluşlarının güçlendirilmesi, demokratik değerleri korurken dezenformasyonla mücadeleye daha fazla katkıda bulunabilir.

İkinci olarak, bağımsız doğruluk kontrol kuruluşlarının teşvik edilmesi ve desteklenmesi, bilgilerin doğrulanması ve yanlış iddiaların çürütülmesinde çok önemlidir. Doğruluk kontrol kuruluşları, medya kuruluşlarının ve kamuya mal olmuş kişilerin dezenformasyon yaymaktan sorumlu tutulmasında çok önemli bir rol oynamaktadır. Doğruluk kontrol kuruluşları halka doğru ve güvenilir bilgi sağlayarak medya okuryazarlığının geliştirilmesine yardımcı olur ve vatandaşların güvenilir kaynaklar ile aldatıcı içerikler arasında ayırım yapabilmelerini sağlar. Üçüncü olarak, dezenformasyona karşı daha sıkı politikalar uygulamak için sosyal medya platformlarıyla işbirliği şarttır. Bu platformlar aldatıcı içeriğin yayılması için önemli savaş alanları haline gelmiştir ve teknoloji şirketleri yanlış anlatıların erişimini sınırlandırmada çok önemli bir rol oynamaktadır. Sağlam içerik denetleme mekanizmalarının ve şeffaf algoritmaların uygulanması, dezenformasyonun virallliğini azaltmaya yardımcı olabilir, böylece viral olma ve daha geniş bir kitleye ulaşma olasılığı azalır.

Ayrıca, medya sahipliğinde şeffaflığın sağlanması, taraflı habercilik ve propagandanın etkisini azaltmak için hayati önem taşımaktadır. Medya sahiplik yapıları açıklandığında, kamuoyu tükettikleri bilgilerdeki potansiyel önyargıları daha iyi değerlendirebilir. Bu şeffaflık daha fazla hesap verebilirliği teşvik eder ve vatandaşların güvendikleri haber kaynaklarının güvenilirliği hakkında bilinçli kararlar vermelerine yardımcı olur. Son olarak, sınır ötesi dezenformasyon kampanyalarının ve yabancı müdahalelerin ele alınmasında uluslararası işbirliğinin

teşvik edilmesi büyük önem taşımaktadır. Dezenformasyon tehditleri genellikle ulusal sınırları aşar ve uluslar arasındaki işbirliği çabaları bu tür zorluklara karşı kolektif direnci güçlendirebilir. NATO'nun ortak dezenformasyon izleme ve ilişkilendirme mekanizmaları gibi girişimler dezenformasyon kaynaklarının belirlenmesine ve eşgüdümlü kampanyalara etkili bir şekilde yanıt verilmesine yardımcı olabilir.

SONUÇ

İleri teknolojilerin dezenformasyon ve bilgi manipülasyonu üzerindeki etkisine ilişkin bu teknik incelemenin sonunda, bu teknolojilerin küresel jeopolitik üzerindeki çok yönlü etkisine dair derin bir farkındalık ortaya çıkmaktadır. Makine Öğrenimi (ML), Derin Öğrenme (DL) ve Yapay Zekanın (AI) ortaya çıkışı, dezenformasyon sorunlarını hem şiddetlendirebilen hem de hafifletebilen yeni bir güçlü çift kullanımlı teknoloji çağını başlatmıştır. Bu rapor, karmaşık makine öğrenimi modelleriyle üretilen sentetik medya olan derin sahtelerin yarattığı artan tehdidi ve bunların toplumsal huzursuzluğu ateşleme, medyaya olan güveni aşındırma ve jeopolitik manzaraya nüfuz ederek çatışmaları tırmandırma potansiyelini araştırmıştır. Derin sahteciliklerin karmaşıklığı, bunların tespit edilmesini giderek zorlaştırmakta ve gerçek dünyada ciddi sonuçları olan uydurma içeriklerin yayılmasına yol açabilmektedir. Bu kötü niyetli araçlar, bir kişinin benzerliğini manipüle edilmiş sesle birleştirerek gerçek gibi görünen videolar oluşturabilir ve toplumda kafa karışıklığına ve kutuplaşmaya neden olabilir.

Devlet ve devlet dışı aktörler, kamuoyu algısını manipüle etmek, siyasi muhalifleri itibarsızlaştırmak ve uluslar arasında gerginliği körüklemek için derin sahtekarlıklardan faydalanarak dezenformasyon kampanyalarının etkisini artırabilir. Rapor ayrıca, sosyal medya platformlarında ve diğer dijital kanallarda bilgi tüketiminin şekillendirilmesinde yapay zeka güdümlü algoritmaların rolüne ışık tutmuştur. Bu algoritmaların karmaşık tasarımı, kullanıcıların öncelikle önceden var olan inançlarıyla uyumlu içeriğe maruz kaldıkları yankı odalarını istemeden de olsa teşvik etmektedir. Bilginin bu şekilde filtrelenmesi, bireylerin farklı perspektiflerden izole edildiği bilgi silolarına yol açarak dezenformasyonun kontrolsüz bir şekilde yayılmasını sağlayabilir. İçerik önerilerini etkileşimi en üst düzeye çıkaracak şekilde uyarlayan bu algoritmalar, istemeden de olsa mevcut önyargıları güçlendirebilir ve toplumsal bölünmeleri şiddetlendirebilir.

Dezenformasyon alanında ileri teknolojilerin yarattığı zorluklar zorlu olsa da, rapor aynı zamanda yapay zeka ve makine öğreniminin bu sorunlarla mücadeledeki potansiyelini de vurgulamaktadır. Yapay zeka destekli araçlar dezenformasyon kalıplarını tespit etmek ve analiz etmek için kullanılabilir, böylece derin sahte ve diğer aldatıcı içeriklerin hızlı bir şekilde tanımlanmasını sağlar. Araştırmacılar ve doğruluk kontrolörleri, gelişmiş veri analitiğinden yararlanarak medyadaki anormallikleri ve tutarsızlıkları tespit edebilir ve dezenformasyon kampanyalarının etkisini azaltabilir. Buna ek olarak, blok zinciri teknolojisi, içerik kaynağının değişmez ve şeffaf bir kaydını sağlayarak, kullanıcıların paylaşılan bilgilerin doğruluğunu

doğrulamasına olanak tanıyarak bilginin gerçekliğini sağlama konusunda umut vaat etmektedir. Bununla birlikte, gelişmiş teknolojilerin sorumlu bir şekilde kullanılması, potansiyel risklerin ve istenmeyen sonuçların dikkatli bir şekilde değerlendirilmesini gerektirir. Rapor, bu tür teknolojilerin kullanımını yönetmek ve kötü niyetli aktörlerin dezenformasyon yaymak için bu araçlardan yararlanmasını önlemek için sıkı düzenleyici çerçevelerin gerekliliğini vurgulamaktadır.

Dezenformasyonun ulus ötesi doğasını ele almak için, ülkelerin şeffaflık, hesap verebilirlik ve bilgi bütünlüğünü teşvik eden uyumlu politikalar oluşturmak için birlikte çalışmasıyla uluslararası işbirliği çok önemlidir. Teknolojinin iki ucu keskin bir kılıç olduğunun bilincinde olan rapor, gerçek bilgileri dezenformasyondan ayırt etme konusunda bireyleri güçlendirmek için dijital okuryazarlık girişimlerinin öneminin altını çizmektedir. Kullanıcıları eleştirel düşünme becerileri ve medya okuryazarlığı ile donatarak, toplumlar dijital gerçekliklerin manipülasyonuna karşı direnç oluşturabilir. Kamusal farkındalık kampanyaları ve eğitim programları yoluyla bireyler aldatıcı içeriği ayırt etmeye ve bilinçli kararlar almaya daha iyi hazırlanabilir.

Sonuç olarak, ileri teknolojilerin dezenformasyon, bilgi manipülasyonu ve jeopolitik üzerindeki etkisi geniş kapsamlı ve çok yönlüdür. Bu zorlukların ele alınması, hükümetler, teknoloji şirketleri, araştırmacılar ve sivil toplumdaki ortak bir çaba gerektirmektedir. Yapay zeka, makine öğrenimi ve blok zincirinin potansiyelinden sorumlu bir şekilde yararlanarak, sağlam düzenleyici çerçeveler ve dijital okuryazarlık girişimleriyle birlikte, demokrasinin ve kamusal söylemin temellerini koruyarak daha güvenli ve bilinçli bir bilgi ortamına giden yolu açabiliriz. Bu kapsamlı araştırma, gelişen dezenformasyon ortamının inceliklerini anlamaya ve bu karmaşık ve sürekli değişen tehdide karşı etkili stratejiler oluşturmaya yönelik bir basamak görevi görmektedir.

Ekonomi ve Dış Politika
Arařtırmalar Merkezi

edam

Adres : Hare Sokak NO:16 AKATLAR 34335 İstanbul/Türkiye

Telefon : +90 212 352 18 54

Faks : +90 212 351 54 65

E-Posta : info@edam.org.tr