İletişim
Kuram ve Araştırma
Dergisi

Sayı Vol. 66, Bahar Spring, (2024)
https://dergipark.org.tr/tr/pub/ikad
DOI » https://doi.org/10.47998/ikad.1339733

Dijital Propagandanın Yeni Bir Versiyonu: Ukrayna-Rusya Savaşı Örneğinde Deepfake Dokümanlar Üzerine Bir Analiz

A New Version of Digital Propaganda: An Analysis on Deepfake Documents on the Case of Ukraine-Russia War

Başak AKMEŞE* **Raci TAŞCIOĞLU****

Araştırma Makalesi Research Article

Başvuru Received: 10.08.2023 ■ Kabul Accepted: 14.03.2024

ÖZ

Algoritmik görsel ve işitsel manipülasyon olarak da tanımlanan deepfake dokümanları, bireylerin tahrif edilmiş bilgilerinin kendi rızası dışında medyaya servis edilmesini mümkün hale getirmiştir. Başlı başına sahte olan bilgiler toplumda dezenformasyon ve propaganda aracına dönüşebilmektedir. Savaş dönemi propaganda faaliyetlerinin konu edinildiği bu araştırmada, deepfake dokümanların dijital propaganda bağlamında nasıl kullanıldığının ortaya konulması amaçlanmaktadır. Bu açıdan deepfake dokümanların ilk kez bir savaş ortamında propaganda amaçlı kullanılması ve dijital propagandanın yeni bir versiyonu olarak hayata geçirilmesi bu araştırmayı hem önemli hale getirmekte hem de özgün kılmaktadır. Bu araştırmada, Ukrayna-Rusya savaşı sürecinde deepfake dokümanlarının dijital propaganda aracı olarak nasıl ve hangi amaçla kullanıldığı ele alınmıştır. Dijital ortamda kullanılan deepfake dokümanları ile ilgili ülke devlet başkanları ve halkının mücadelesi betimleyici bir yaklaşımla analiz edilmektedir. Bu araştırma çerçevesinde, olasılıksız örnekleme yöntemlerinden kolayda örnekleme yöntemiyle belirlenen dört deepfake dokümanı incelenmiştir. Araştırmanın sonucunda; Rusya'nın siber saldırılarına maruz kalan Ukrayna'nın deepfake dokümanları neticesinde olası propagandalar için halkını önceden uyardığı, hızlı dönüşlerle karşı saldırılarda bulunduğu tespit edilmiştir. Elde edilen bulgulara göre, Ukrayna'nın deepfake dokümanları ile karşı saldırılara geçtiği, videolarda daha çok Putin'i itibarsızlaştıracak içerikler geliştirdiği gözlenmiştir. Dolayısıyla araştırmada bilgi çağında kullanılan, propaganda araçlarının yeni bir versiyonu olan deepfake dokümanlarının savaşın gidişatına kısa süreli de olsa etki ettiği ortaya koyulmaktadır.

Anahtar Kelimeler: Propaganda, Dijital Propaganda, Dezenformasyon, Manipülasyon, Deepfake Dokümanı, Ukrayna-Rusya Savaşı.

ABSTRACT

Deepfake documents which are also defined as algorithmic visual and auditory manipulation, have made it possible to provide the media with fake information from individuals the falsified information of individuals to the media without their consent. Information that is fake on its own can turn into a disinformation and propaganda tool in the society. The first use of propaganda purposes for the first time in a war environment makes this research important. In this research, how and for what purpose deepfake documents have been used as a digital propaganda tool during the Ukraine-Russia war has been discussed. The struggle of the heads of state and their people against the deepfake documents used in the digital environment is analyzed with a descriptive approach. Within the framework of this research, four deepfake documents determined by convenience sampling method, one of the non-probability sampling methods, were examined. As a result of the research, it has been determined that Ukraine, which has been exposed to cyber-attacks from Russia, warned its people in advance of possible propaganda as a result of deepfake documents, and took quick turns and counter-attacks. According to the findings, it was observed that Ukraine launched counter-attacks with deepfake documents and developed content that would discredit Putin in videos. This study includes the originality of handling deepfake documents as a new version of digital propaganda in the war environment. It is revealed that deepfake documents, which are a new version of propaganda tools used in the information age, have a short-term effect on the course of the war.

Keywords: Propaganda, Digital Propaganda, Disinformation, Manipulation, Deepfake Document, Ukraine-Russia War.

Giriş

İnsan, doğası gereği öğrendikçe ve bilgiye ulaştıkça gelişmekte ve değişmektedir. Günlük yaşam pratikleri içerisinde öğrenme ve bilgi sahibi olabilme süreçlerinde zaman, hayat koşulları gibi pek çok unsur insanları doğruluğunu teyit etmeden başka bilgi kaynaklarına güvenmeye zorlamaktadır. Haliyle insan, duygular ve kişisel deneyimler yanında ampirik kanıtlar/veriler toplayarak elde edilen bilgilere de inanma eğilimi gerçekleştirebilir. Günümüzün önemli bilgi kaynaklarından biri olan ve aynı zamanda bilgiye erişimi giderek kolaylaştıran internet ortamında kişisel günlük yaşam pratikleri ile bilgiye ulaşmak beraberinde birçok zorluğu da getirmektedir. Şöyle ki, edinilen profil ile zaman geçirilen internet platformlarında her kullanıcı kendisine ait verilerin dijital izini bırakmaktadır. Algoritmalar bu dijital izler üzerinden analitik hesaplamalar yapmakta, birbirleriyle ayrışan farklı profillerin bağ kurmalarını engelleyici izolasyon ortamı oluşturmaktadır. Kutuplaşmaya neden olan algoritmalar "yankı odası etkisi" ile bireyleri propagandaya açık hale getirebilmektedir. Bu yöntemle çalışan yapay zekâ güdümlü argümanlar, teknolojik ilerlemeyi dijital propaganda aracı haline getirebilmektedirler. Bu dijital propaganda araçlarından en önemlisi de deepfake dokümanlarıdır. Deepfake dokümanları; insanların yapmadıklarını yapmış, söylemediklerini söylemiş gibi gösterilebilmektedir. Bu uygulamalarla insanlar, sosyolojik, psikolojik, etik ve siyasi açıdan etkilenerek güven duygularının zedelendiği, düşüncelerinin yanlış yöne çekildiği bir süreçten geçebilmektedirler.

Bu araştırmada, dijital propagandanın yeni versiyonu deepfake dokümanlarının Ukrayna-Rusya savaş ortamındaki kullanım nitelikleri incelenmiştir. Söz konusu araştırma, deepfake konusunda ortaya çıkan bilimsel literatüre ve deepfake'lerle ilgili halka açık haber makalelerine dayanmaktadır. Bu bağlamda, araştırmada yerli ve yabancı olmak üzere 43 haber makalesi ve 78 bilimsel literatür incelenmiştir. Devam eden savaşa dair dört "deepfake dokümanı" incelenmiştir. İncelemeler sonucunda deepfake dokümanları ile ilgili yazılı ve görsel materyal, malzemeler ve grafikler araştırmaya dâhil edilmiştir.

Thalen (2022), çalışmasında süregelen savaşta yaşanan bilgi savaşının bir parçası olan deepfake dokümanlarını ilk üst düzey sahtekarlık olarak tanımlamıştır. Bu açıdan deepfake dokümanlarının savaşın seyrine etkisi olup olamayacağı araştırılmış, savaş ortamında kullanılan deepfake dokümanları ile ülke devlet başkanları ve halkının mücadelesi, savaşa etkileri ve savaştaki tepkileri incelenmiştir. Her iki ülke vatandaşlarının "deepfake dokümanlarına" savaştan önce de ilgilerinin olduğu gözlenmiştir. Araştırmada Rusya'nın siber saldırılarına maruz kalan Ukrayna'nın deepfake dokümanları neticesinde olası propagandalar için halkını önceden uyardığı, hızlı dönüşler alıp karşı saldırılarda bulunduğu tespit edilmiştir. Ukrayna'nın deepfake dokümanları ile karşı saldırılara geçtiği, videolarda daha çok Putin'i itibarsızlaştıracak içerikler geliştirdiği gözlenmiştir. Ukrayna tarafından oluşturulan deepfake videolarının YouTube ve Google gibi platformlarda yayında kalma sürelerinin çok az olduğu belirlenmiştir. Rusya tarafında ise Ukrayna devlet televizyonunu ve internet sitesini hackleyerek yayınladıkları "deepfake dokümanı" dışında herhangi bir bulguya ulaşılamamıştır. Ukrayna ve devlet başkanına yönelik yayınlanan tek deepfake'in de sosyal mecralarda silinmesi araştırmanın sınırlılıklarındandır.

Yapılan literatür çalışmasında deepfake dokümanlarına ilişkin değerli çalışmalara rastlanılmıştır. İlgili literatürde rastlanılan başlıca çalışmalar şunlardır: Deepfake argümanını 'dezenformasyon' olarak inceleyen çalışmalar; (Bennett vd., 2018, ss. 122-139; Temir, 2020, ss. 1009-1024; Whyte, 2020, ss. 199-217). 'Algoritmalar üzerinden deepfake uygulamalarının tespitine yönelik çalışma; (Korkmaz ve Alkan, 2021), reklam anlatısı olarak deepfake uygulamaları ile ilgili çalışma; (Acar & Tanyıldızı, 2022, ss. 78-99), bilgi savaşı, dezenformasyon aracı olarak deepfake'i konu alan çalışma; (Hartmann & Giles, 2020, ss. 233-250), Zelenskyy'nin 'deepfake videosunun sahte oluşunu tespit etmek' için yüz özelliklerinin ve jestsel özelliklerinin incelendiği çalışma; (Boháček, & Farid, 2022, ss. 1-6), deepfake sahtekarlıklarının sosyal etkisini inceleyen çalışma; (Hancock & Bailenson, 2021, ss. 149-152), deepfake farkındalığını

inceleyen çalışma; (Cochran & Napshin, 2021, ss. 164-172), söylemsel olarak deepfake sorununu inceleyen çalışma; (Brooks, 2021, ss. 159-163), deepfake'i algılamaya ve deepfake'in eksikliklerini belirlemeye odaklanan çalışma; (Dolhansky vd., 2020, ss. 1-11), şeklinde sıralamak mümkündür.

Savaş ortamında servis edilen deepfake dokümanlarını her iki ülke perspektifinden değerlendiren ve savaşta propaganda aracı olarak inceleyen hemen hiçbir çalışmaya rastlanılmamıştır. Bu araştırmada, deepfake dokümanlarının savaş ortamında dijital propagandanın yeni bir versiyonu olarak ele alınması araştırmanın önemini ve özgünlüğünü oluşturmaktadır.

Dijital Propaganda Tanımı

"Propaganda", "toplumsal ve politik değerleri aktarma girişimi" anlamına gelir (Kenez, 1985, s. 4). Bir tür manipülasyon olarak da tanımlanan propagandanın dijital platformlara evrilmesi ile dijital propagandadan bahsedilmektedir. Ali Efendioğlu'na (2020) göre "dijital propaganda, "kamuoyunu bilinçli bir şekilde manipüle etmek için tasarlanmış, internet, bilgisayar ve mobil cihaz uygulamalarıdır; dijital iletişim ekipmanlarının, veri arşivlerin ve yapay zekanın, bir propaganda kampanyası oluşturmak için kullanılmasıdır". Dijital propaganda, yabancı kaynaklı literatürde hesaplamalı propaganda olarak ifade edilmektedir. Woolley ve arkadaşlarına (2018) göre ise dijital propaganda, "internet üzerinden ortaya çıkan bir siyasi manipülasyon biçimidir". Dijital propagandayı, "sosyal medya platformlarının, otonom aracıların, algoritmaların ve kamuoyunu manipüle etmekle görevli büyük verilerin bir araya getirilmesi olarak tanımlamaktadırlar" (2018, ss. 3-249). Dijital propaganda, krizler veya seçimler sırasında kasıtlı olarak kamuoyunu manipüle etmek için tasarlanmış internet, bilgisayar ve mobil cihazlarda insanlarla etkileşim kurmak veya bir kampanya yürütmek için insan kullanıcılara ek olarak makinelerin kullanılması anlamına gelmektedir (Neyazi, 2020).

"Bir terim olarak, hesaplamalı propaganda, yanıltıcı bilgileri sosyal medya platformları üzerinden kasıtlı olarak dağıtmak için algoritmaların, otomasyonun ve insan küratörlüğünün kullanılması olarak tanımlanabilir. Hesaplamalı propagandanın amacı, üçüncü taraf aktörlerin gündemine ve çıkarlarına hizmet etmek için kamuoyunu manipüle etmektir" (Bilgi University Website, 2021).

Hesaplamalı propaganda insanların yeni icat ettiği teknolojilerdendir. Bu yeni teknolojilerin ve bu teknolojilerin izin verdiği yeni davranışların sosyal medya kesişiminden doğan olasılıkları fark ederek gerçekleştirdikleri makinelerdir. Sosyal medyada kaybetme, öfke, korku ve özlem duyguları da dahil olmak üzere pek çok sebepten ötürü bir şeyler paylaşılabilir. Bu nedenle hesaplamalı propagandanın dijital çağda demokrasi üzerindeki potansiyel olarak tehlikeli etkileriyle mücadele etmek için, bunun hem nasılına hem de nedenine odaklanılması gerekmektedir (Frank, 2018).

İletişim, özelliklerine göre zamanla çeşitlere ayrılmış ve bu çeşitlilik iletişimin kullanım alanlarına göre farklı araç-gereçlere ihtiyaç duyulmasına neden olmuştur (Özdemir ve Taşcıoğlu, 2022, s. 67). Dolayısıyla dijital iletişimin büyük kısmı artık insanlar arasında değil, cihazlar arasında, insanlar hakkında, nesnelerin interneti üzerinden gerçekleşmektedir. Politik aktörler, kamuoyunu manipüle etmek için girişimlerde, özel mülk algoritmalar biçimindeki teknolojik vekilleri ve yarı otomatik sosyal aktörleri -siyasi robotlar- kullanmaktadırlar. Bu araçlar bir açıdan insan kontrolü için yapı iskelesi, oluşturabilirler. Diğer açıdan, etkileşim ve organizasyon üzerinde böyle bir kontrol sağlamak için çalışma biçimleri, onları inşa edenler için bile tahmin edilemez olabilir. Bu nedenle, çağdaş politik iletişimi ve genel olarak modern iletişimi anlamak için artık algoritmalar ve otomasyon politikaları araştırılmalıdır (Woolley ve Howard, 2016, ss. 3-18).

Dijital Propaganda Türleri

Brown (2018), propaganda türlerini; "duygusal, conative ve bilişsel propaganda" şeklinde bir ifade etmektedir.

Duygusal Propaganda: "Geniş kitlelerce, üyelerinin yeterince bilgilendirilmiş, rasyonel, yansıtıcı yargılarını engelleyecek şekilde duyguları harekete geçirmeye yönelik organize girişimdir".

Conative Propaganda: "Geniş kitlelerce, üyelerinin yeterince bilgilendirilmiş, rasyonel, yansıtıcı muhakemesini engelleyecek şekilde arzulara hitap etme amaçlı organize girişimdir".

Bilişsel Propaganda: "İletişim yoluyla, geniş bir kitledeki inançları, üyelerinin yeterince bilgilendirilmiş, rasyonel, yansıtıcı yargılarını atlatacak şekilde şekillendirmeye yönelik organize girişimdir" olarak tanımlanabilir (2018, ss. 194-218).

Propagandayı farklı açıdan inceleyen Lock ve Ludolph (2020), internette yürütülen propagandanın özelliklerini inceledikleri çalışmalarında halkla ilişkilerin nerede durup propagandanın nerede başladığı dair araştırmalar yaptıkları görülmektedir. Bu bağlamda çevrimiçi örgütsel propagandaya ilişkin, dijital örgütsel propagandayı beş aşamada incelemektedirler. Bu beş aşama şu şekilde sıralanmaktadır: propagandayı kim kullanıyor, hangi kanallarda, hangi medya kullanılıyor, propaganda stratejisinin amaçları nelerdir ve hangi bağlamlarda gerçekleştiğidir. Çevrimdışı ortamın aksine, çevrimiçi propaganda yapan kuruluşlar kimliklerini gizlemezler ve tutumları değiştirmek amacıyla öncelikli olarak (potansiyel) takipçilerine hitap ederler.

Dijital propagandanın pek çok unsuru vardır ve zamanla literatürde birtakım tekniklerle ortaya çıkmaktadır:

Şekil 1

Dijital Propaganda Unsurları (European. P.R.S, 2018)

Bot *(Robot 'un Kısaltması): "Sosyal medyada bir kullanıcı gibi etkileşim kurmak üzere programlanmış otomatik bir hesaptır. Dezenformasyon amacıyla, meşru olmayan robotlar belirli anlatıları öne sürmek, yanıltıcı mesajları çoğaltmak ve çevrimiçi ifadeleri çarpıtmak için kullanılabilir".*

Troller: *"Diğer kullanıcıları taciz etmek veya tartışmalara yol açmak için bölücü içerik yayınlamak için bazen devlet aktörleri tarafından desteklenen insan çevrimiçi aracılardır".*

Makine Güdümlü İletişimler (Madcom): *"Metin, ses ve video içeriği oluşturmak için yapay zekayı (AI) makine öğrenimiyle birleştirir ve mesajları bireysel kullanıcıların kişiliklerine ve geçmişlerine göre uyarlamayı kolaylaştırır. Örneğin, MADCOM kullanıcıları çevrimiçi tartışmalara dahil etmek veya hatta insanları trolllerle tehdit emek için yapay olmayan dil işletim sistemlerini kullanabilirler".*

Yemleme Kancası: *"Hedefe alınan kimlikler (hedefli kimlik avı), virüslü ekleri veya bağlantıları olan e-postalar, gizli bilgilere erişmek için kişi veya kuruluşlara gönderilmektedir. Bağlantıyı veya eki açarken, kötü amaçlı yazılım yayınlanır veya alıcı, alıcının bilgisayarına bulaşan kötü amaçlı yazılımın bulunduğu bir web sitesine yönlendirilir".*

Dağıtılmış Hizmet Reddi (Ddos): *"DDOS saldırılarında, hedeflenen web sitelerine aşırı yüklenerek ve dondurularak büyük miktarda bilgi gönderilir. Bir ülkeye karşı bilinen ilk koordineli siber savaşta, Estonya'daki bir Sovyet savaş anıtının kaldırılması sokak protestolarına sebep olmuştur, ardından hükümeti, bankaları, telekomünikasyon şirketlerini, internet servis sağlayıcılarını ve medya kuruluşlarını haftalarca felç eden DDoS saldırıları da dahil olmak üzere siber saldırılar düzenlenmiştir".*

Nesnelerin interneti (IoT): *"Kaba kuvvet saldırılarında bu cihazların güvenliği genelde zayıftır".*

Politik Botlar: *"Çoğu zaman sahte takipçiler, halı saha hesapları veya çorap kuklaları olarak bilinir birçok türü vardır".*

Dijital propaganda çabalarının üç ana unsuru; "bot" -otomatik hesaplar-, "trol" ve "sahte" -kafa karışıklığı yaymak için gerçek hesapları taklit eden web siteleri veya sosyal medya hesapları- olarak ifade edilebilir. Bunlar Şekil-1 de daha detaylı ifade edilmiştir (European. P.R.S, 2018).

Bir başka dijital propaganda türü de dijital oyunlardır. Dijital oyunlar geniş kitlelere ulaşabilen, eğlence sektöründe ticari amaçlarla hareket edilen ve bu doğrultuda düşünce mesajının paylaşılması amacı gütmektedirler. "Özellikle senaryo modu içeren tek kişilik savaş oyunları, oyun kullanıcılarının ve üretimin genel ki düşüncelerinin propagandasını yapmak maksadıyla kullanılmaktadır" (Kahraman & Fidan, 2022).

Dijital Propagandanın Uygulama Alanları

Başta sosyal medya olmak üzere bloglar, forumlar ve katılım ve tartışma içeren diğer web sitelerinde yürütülmektedir. Bu tür propaganda, genellikle yapay zekâ ve makine öğrenimi gibi ileri teknolojiler tarafından oluşturulan ve kontrol edilen veri madenciliği ve algoritmik botlar aracılığıyla yürütülmektedir (D'Alessio, 2021). Sosyal medya, nüfusta önemli bir değişikliği etkileme gücüne sahiptir. Sosyal medya aracılığıyla, dünyanın her yerinden insanlar bağlantı kurabilir ve görüşlerini paylaşabilir. Bununla birlikte, bu sosyal alan artık hileli, müstehcen, sahte ve etkili medyanın sızması nedeniyle enfekte olmuştur (2021, ss. 3-5). Bir UNESCO raporuna göre, sahte haber ve derin sahte içeriklerin yaygınlığı, sahte propaganda yayma potansiyeline sahip olması nedeniyle siyasi ve sosyal huzursuzluğa yol açabilir. Sosyal medyaya güven, yeni ortaya çıkan bir sorundur ve buna acilen çözüm bulunması gerekmektedir. Sahte haberleri ve derin sahtekarlıkları tespit eden yaklaşımlar hakkında bazı araştırmalar yapılsa da sosyal medya platformlarında yayınlanan bu derin sahtekarlıkların kaynağının belirlenmesi önemli ve nispeten bilinmeyen bir zorluktur (Narayan vd., 2022, ss. 2858-2867).

DeepFake Dokümanlarının Tanımı ve Tarihsel Süreci

Deepfake kelimesi, "derin öğrenme" ve "sahte" terimlerini birleştiren bir yapay zekâ biçimidir (Shao, 2022; Mitra, 2020; Norman, 2022). Derin öğrenme, "yapay zekanın bir alt kümesidir" ve öğrenebilen ve kendi başına akıllı kararlar verebilen algoritma düzenlemelerini ifade eder. Bu tür dijital içerik oluşturmak için kullanılan teknolojiye, "deepfake" denilmektedir. Deepfake, gerçek gibi görünen fabrikasyon görüntüler ve sesler veren, gelişmiş yapay zekâ tarafından üretilen manipüle edilmiş videoları veya diğer dijital temsilleri ifade etmektedir (Shao, 2022). Schick'a (2020) göre, derin sahteleri, "ya yapay zekâ tarafından manipüle edilen ya da tamamen oluşturulan medya -resimler, ses ve video dahil-" olan sentetik medyanın habis bir tezahürü olarak tanımlamıştır (Esselink, 2021, ss. 5-93).

> "Aldatan yapay zekâ olarak bilinen deepfake teknolojisi, adını yapay zekanın bir biçimi olan derin öğrenmeden almaktadır. Derin sahte yapay zekada, kendilerine büyük veri kümeleriyle ilgili sorunları nasıl çözeceklerini öğreten derin öğrenme algoritmaları, sahtenin gerçek gibi görünmesini sağlamak için videolar, resimler ve diğer dijital içeriklerdeki yüzleri değiştirmek için kullanılmaktadır. Deepfake içeriği, birbiriyle rekabet eden iki algoritma kullanılarak oluşturulmaktadır. Algoritmalardan ilkine jeneratör, diğerine de ayrımcı denilmektedir. Oluşturucu, sahte dijital içeriği oluşturduktan sonra ayrımcıdan içeriğin gerçek mi yoksa yapay mı olduğunu bulmasını istemektedir. Ayrımcı, içeriği gerçek veya sahte olarak doğru bir şekilde tanımladığında, bir sonraki derin sahtekarlığı iyileştirmek için bu bilgiyi oluşturucuya iletmektedir. Bir araya getirildiğinde, bu iki algoritma GAN adı verilen üretken bir rakip ağ oluşturmaktadır. Bu ağ sayesinde sahte görüntüler üretmek için bir dizi algoritma kullanılmaktadır" (Great Learning ,2022); (Cervantes, 2021).

Sinir ağları ilk olarak 1943'te kavramsallaştırılmıştır (Galloway, 2022). Deepfake uygulamalarının temelini atan akademisyenler incelendiğinde bu uygulamaların, süreç içerisinde gelişimi hakkında çıkarımda bulunabilir. 1997'de Christoph Bregler, Michele Covell ve Malcolm Slaney tarafından yazılan bir makale neticesinde bazı film stüdyolarının yapabileceklerini temelde otomatikleştiren "Video Yeniden Yazma Programı" geliştirilmiştir. Bu programla, yüzleri yorumlayan, metinden sesi

sentezleyen ve 3B alanda dudakları modelleyen eski çalışmalar temel alınarak oluşturulmuştur. Dönem itibariyle tüm çalışmaları bir araya getiren ve inandırıcı canlandırmaları sağlayan arayüz oluşu ve yüz canlandırmayı tamamen otomatikleştiren ilk sistem olması nedeniyle önemlidir. Bu program ses çıkışından yeni yüz animasyonlarını sentezleyebilmektedir (Song, 2019; Norman, 2022).

Deepfake uygulamaları, bir videoda veya video gibi görüntüleme cihazlarında bir kişinin yüzünü başka biriyle değiştirme olanağı sunmaktadır. Bu tür videoları oluşturan teknolojik yapılar, performansını sürekli iyileştirmek için kurgulanmıştır. Özellikle sahte derin içerikli videoları oluşturan algoritmalar öğrenerek ve taklit etmeye devam ederek videoları iyileştirmektedir. Bu sayede deepfake uygulamalarıyla bireyin yüz ifadeleri, jestleri, sesi ve varyasyonları onları daha gerçekçi hale gelmektedir. Bunlara birinci nesil yapay zekâ teknolojisi örneği diyebiliriz. "Birinci nesil yapay zekâ teknolojisinin bazı örnekleri, Apple'ın Siri'si, Amazon'un Alexa'sı, Google'ın Nest öğrenme termostatı ve Pandora'nın otomatik müzik tavsiye hizmetleridir. Bu yazılım programları, konuşulan dili kullanarak sorguları ve istekleri tanımlayan ve bir veri tabanından alınan yanıtlarla yanıt veren makine öğrenimi teknolojisini kullanmaktadır. Algoritma, bir kişinin yeterli video ve sesiyle yola çıktığında, yalnızca sahte videoyu oluşturmakla kalmaz, aynı zamanda kişinin aslında söylemediği şeyleri de söylemesini sağlayabilir". Sonuç olarak, bu videolar, çıplak gözle bakıldığında gerçek videolardan ayırt edilemeyecek oranda profesyonel videolar haline gelmektedir" (Maras, 2017, s. 7).

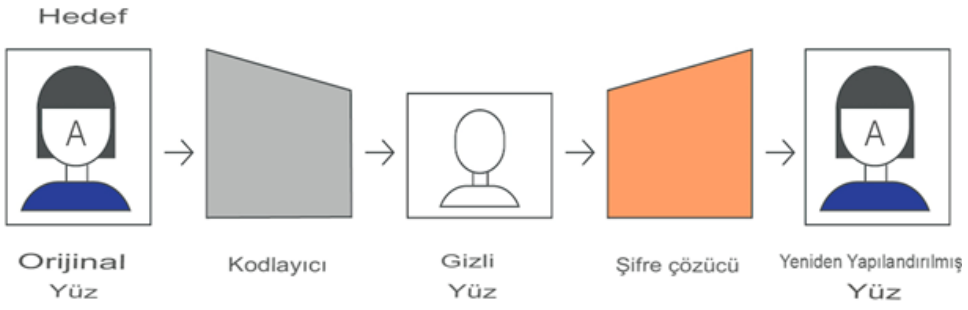
Deepfake uygulamalarına ilişkin pek çok yazılımlara rastlanılmaktadır. İnternet ortamlarında bu tür yazılımlara pek çok kişinin erişebilmesi ve kullanabilmesi nedeniyle -duyulan endişe ve merak doğrultusunda- herkesin kullanımına açık olan bu manipülasyon araçlarının nasıl yapıldığına ilişkin bazı çalışmalara da rastlanılmıştır. Bunlardan biri de Şekil-2'de yer alan ve deepfake uygulamalarının nasıl yapıldığına ilişkin çalışmadır.

Şekil-2'de deepfake uygulamasına yönelik yapılan çalışmada değişiklik boyutunun kodlayıcı ve şifre çözücü aracılığıyla gerçekleştirildiği görülmektedir. Kodlayıcı bir yüzün görüntüsünü almakta ve onu "gizli yüz" olarak da bilinen düşük boyutlu bir temsile sıkıştırmaktadır. Kod çözücü daha sonra bu gösterimi alıp yüzü orijinal biçimine göre işlemi yineleyerek yeniden yapılandırmaktadır (Gov.Uk, 2019).

Yeniden yapılandırılan yüz sentetik işlemi medya teknolojisinde manipülasyon aracı haline gelebilmektedir. Şekil-2'dekine benzer yazılımlarla daha farklı manipülasyon biçimleri oluşturulabilir.

Şekil 2

Deepfake Uygulaması (Gov.Uk, 2019)



Deepfake Dokümanlarının Kullanım Alanları ve Örnekleri

"Bir kişinin deepfake videosunu yapmak için, içerik oluşturucuların bir bilgisayarının, imajını ve sesini manipüle etmeye çalışılan "hedefin" ve "kaynağın" çok sayıda videosunun olması gerekmektedir. İçerik oluşturucuların hedefte olan kişinin sesini veya görüntüsünü işlemesi gerekmektedir. Hedefe aldığı kişinin söylemesini istediği kelimeleri veya yapmasını istediği eylemi modelleyen sistem, bunu başarmak için kanıtlara bakar, örüntüler bulur ve ardından bu örüntüyü yeni bilgilere uygulayarak "bir sorunu çözmeye çalışan bir insan beyni gibi" bir tür yapay sinir ağları kullanır" (Galloway, 2022).

Bilgisayarla görme ve yapay zekâ gelişmeye devam ettikçe, insan görüntü sentezindeki ilerlemeler nedeniyle çoğu kişinin mevcut görüntüleri ve videoları kaynak görüntülere veya videolara, "üretken çekişmeli ağ" olarak bilinen bir makine öğrenimi tekniği ile aktarılmasını sağlamaktadır. Bu bağlamda deepfake uygulamaları sahte videolar aracılığıyla siyasi veya pornografik amaçlarla kullanılmayı mümkün kılmaktadır (Norman, 2022).

Deepfake içerikleri, pornografik veya politik amaçla bir kişinin rızası olmadan imajını ve sesini kullanarak zorbalık yaşatmak için kullanılabilir. Çevrimiçi işitsel/görsel sahtekarlıklar son teknolojik ve yazılımsal gelişmelerin aracılığıyla, tüketici seviyesindeki kullanıcılar tarafından ucuz, hızlı ve tespit edilemeyen video sahtekarlığının oluşturulmasını mümkün kılmaktadır (Fletcher, 2018, ss. 455-471).

2019'da "derin sahte ürünlerin gelişen yeteneklerini ve tehditlerini araştıran" Amsterdam merkezli Deeptrace Şirketi, internet ortamında dolaşan yaklaşık 15.000 deepfake hakkında bir çalışma yayınlamıştır. Çalışmada %96'sının pornografik olduğunu ve %99'unun da ünlü kadın yüzlerinin kullanıldığı tespit edilmiştir (Celebrtiy, 2021). Bu şekilde dijital görüntülerin kullanımı arttıkça, dijital görüntü sahteciliği yaratma araçları ve teşviki de artmaktadır. Buna göre, görüntü değişikliklerini ve sahte görüntüleri tespit edebilen adli dijital görüntü tekniklerine büyük bir ihtiyaç duyulmaktadır (Stamm & Liu, 2010).

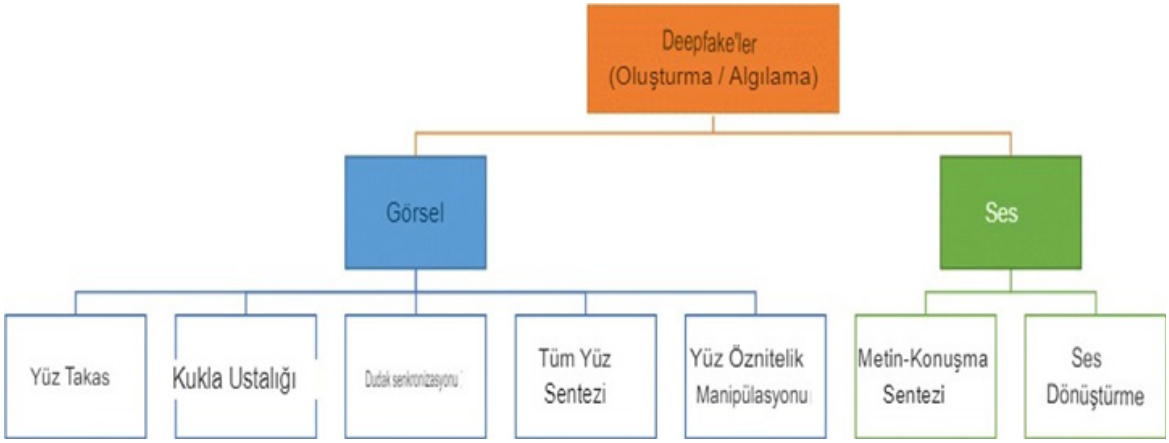
Masood ve arkadaşları (2022, s. 4), deepfake dokümanlarını aşağıdaki türlerde kategorize etmektedirler:

a. Yüz değiştirme,
b. Dudak senkronizasyonu,
c. Kukla ustası,
d. Yüz sentezi ve öznitelik manipülasyonu,
e. Yapay sahtekarlıklar.

Şekil-3'de Masood ve arkadaşları (2022, ss. 1-53), deepfake dokümanları için yapmış oldukları sınıflandırmalarında yüz takası dudak senkronizasyonu ve kukla ustalığı aşamalarının ağırlıkla üstünde durmaktadırlar. Yüz takas videoları çoğunlukla eğlence amaçlı kullanılsa da giderek daha gerçekçi ve ayırt edilemez hale gelen sahte videolar, finansal dolandırıcılık, güven krizi vb. dahil olmak üzere büyük potansiyel güvenlik risklerinde oluşmasına neden olmaktadır (Wang vd., 2022). Yüz değiştirme için kullanılan deepfake

Şekil 3

Deepfake Dokümanlarının Sınıflandırılması (Masood vd., 2022)



uygulamalarında, hedefte olan kişinin sahte bir videosunu oluşturmak için kaynak kişinin yüzü bir kurbanın yüzüyle değiştirilmektedir. Yüz odaklı deepfake uygulamaları genellikle ünlü bir kişiyi, rıza dışı pornografide, halkın gözünde itibarını zedelemek için hiç görünmedikleri senaryolarda, göstererek hedef alınabilmektedir. Dudak senkronizasyonuna dayalı uygulamalarda, hedef kişinin dudaklarının hareketi, belirli bir ses kaydıyla tutarlı hale getirilecek şekilde manipüle edilmektedir. Böylece kurban kayıtta ne varsa söylüyormuş gibi görünmektedir. Kukla ustası sürecin de ise; bu uygulamalarla hedef kişinin göz hareketi, yüz ifadesi, kafa hareketi gibi ifadelerini taklit eden video oluşturulmasına olanak sağlamaktadır" ifadelerine yer vermektedirler.

Deepfake materyali tanımlamak ve tespit etmek için, işlem sırasında ortaya çıkan kusurlar dikkat çekmektedir. Çıplak gözle de görülen bu kusurlar "Manuel algılama" olarak da ifade edilebilir. Deepfake videolar oluştururken fark edilen kusurlar şunlardır:

- Yüzün etrafındaki çift çeneler veya hayalet kenarlar.
- Aşırı bulanıklık karşılaştırması zor hedef ve diğer yüz dışı bölgeler.
- Yüzün kenarında ve cilt tonunda bir değişiklik.
- Yüzde çift kaş veya çift kenar.
- Yüz kısmen eller veya başka şeyler tarafından engellenir.
- Videoda titreme veya bulanıklık görülebilir.

Bu kusurlar daha çok deepfake videoların yaratıcıları tarafından gereken süreyi kısaltmak için köşeleri kestiği için üretilir ve bu durumda videolarda kalite düşürebilmektedir (Botha & Pieterse, 2020).

Deepfake'in kullanım alanlarının ve kullanım amaçlarının çoğalması ile birlikte sosyal medyada, çevrimiçi ortamlarda çok sayıda yapay, sahte videoya rastlamak mümkün hale gelmiştir. Bu bağlamda deepfake'lerle ilgili bilimsel literatür ve halka açık haber makalelerinin taranması sonucunda deepfake uygulamalarının farklı örnekleri ile karşılaşılmıştır:

Deepfake Örnekleri

Var Olmayan Figürler veya Hayvanlar

Şekil-4'de Barbie bebek figürünün, Günther and The Sunshine Girls'ün "ding dong song" şarkısını söylediği deepfake video içeriğindeki ekran resimleri gösterilmektedir. Video içeriğinde gözler, dudaklar ve baş bölgesi hareketlendirilmiştir. Barbie bebek müziğin ritmine göre dudaklarını oynatmakta ve hareket etmektedir.

Şekil-5'te insan yüzünün hayvana, hayvan yüzünün de insana dönüştürüldüğü bir uygulamadan alınan ekran resimleri görülmektedir.

Şekil 4

Barbie Bebek Deepfake (Boredpanda, 2021)

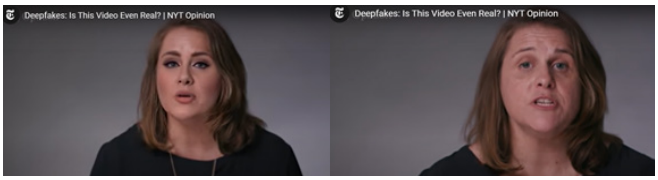
Şekil 5

Yüz Dönüştürücü Deepfake (Kucher, 2020);(Baki, 2021)

Yüz Takas Yolu ile Yapılan Deepfake

Şekil 6

Yüz Takas Yoluyla Deepfake Uygulaması (Cervantes, 2021).



Ekran alıntısının gösterildiği Şekil-6'da videonun ilk 30 saniyesinde, çevrimiçi manipülasyon uzmanı Claire Wardle, Adele olarak lanse edilmektedir. 30 saniyeden sonra kendi gerçekçi görünümü ile videoya devam etmektedir.

Mem'ler

Şekil 7

Nicholas Cage- Lois Lane Manipülasyonu (Netlingo, 2022)

Şekil-7'de "Çelik Adam" filminin bir sahnesi alınmış ve baş rol oyuncusu Lois Lane karakterinin yüzü yerine mizah amacı ile Nicholas Cage'in yüz montajı yapılmıştır. Filmdeki sahnenin orijinal hali ile kıyaslandığında yüz takası yapıldığı açıkça fark edilmektedir.

Geçmişte Konuşulanların Yeniden Canlandırılması

Şekil 8

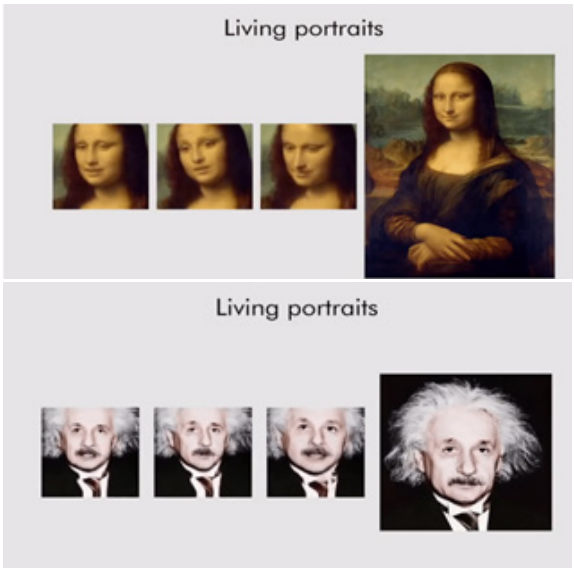
Obama Röportajının Manipülasyonu (Moran, 2020)

Şekil-8'de Obama'nın gençlik yıllarında vermiş olduğu röportajda kullandığı ifadelerin yer aldığı, dudak senkronizasyonu yardımıyla günümüzde ki görünümüne uyarlanarak hazırlanan deepfake video içeriğinin ekran alıntısı gösterilmektedir. Obama'nın geçmişte verdiği röportaj güncel görüntüsü ile yeniden oluşturularak servis edilmiştir.

Nostalji Aracı Deepfake'ler

Şekil 9

Mona Lisa ve Einstein Portre Deepfake Uygulaması (Sagar, 2019)



Şekil-9'da Leonardo Da Vinci'nin, 'Mona Lisa' adlı eseri Lisa del Giocondo ve Einstein portresinin kullanılması ile üretilmiş video içeriğinden alınan ekran resimleri görülmektedir. Konuşan kafa veri setleriyle çalışılan videolarda Mona Lisa ve Einstein'ın göz kırptığı, kafalarını hareket ettirdikleri ve konuştukları görülmektedir.

Siyasi Deepfake'ler

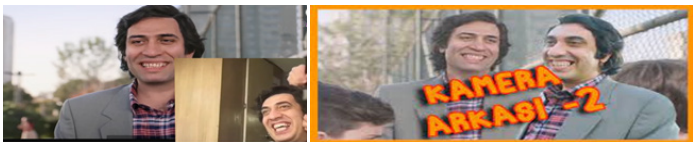
Şekil 10

Kim Jong'un Dudak Senkronizasyonuyla Çekilmiş Deepfake Videosu (Bickerton, 2020)

Şekil-10'da Kim Jong'un dudak senkronizasyonuyla çekilmiş deepfake videosundan elde edilen ekran alıntısı gösterilmektedir. Bu video Amerika'da yapılan seçimlere yönelik manipülasyon amaçlı olarak çekilmiştir. Söz konusu ekran alıntısının sergilendiği videoda, Kim Jong-un Amerikan seçimlerine yönelik "Demokrasi kırılgan bir şey. İnanmak istediğinden daha kırılgan. Seçim başarısız olursa demokrasi olmaz. Hiçbir şey yapmak zorunda değilim. Bunu kendinize yapıyorsunuz. İnsanlar bölünmüş durumda. Oy verme bölgeleriniz manipüle edildi. Oy verme yerleri kapanıyor, bu yüzden milyonlar oy kullanamıyor. Demokrasinin çökmesi zor değil. Tek yapman gereken hiçbir şey yapmamak" ifadelerini kullanmıştır (Bickerton, 2020).

Tam Vücut Takası Olan Deepfake'ler

Şekil 11
Kemal Sunal'ın Ziraat Bankası Reklamı (Youtube, 2022)



Şekil-11'de Ziraat Bankası'nın reklam yüzü olarak Kemal Sunal'ı kullandığı reklam içeriğine ait ekran alıntısı ve kamera arkası görüntüsü yer almaktadır. Reklamda Sunal'ı canlandıran kişiye yapay zekâ yardımıyla kafa hareketleri, mimikleri, kas hareketleri aktarılmıştır. Söz konusu reklamda deepfake uygulaması yüz ve hareket ile sınırlandırılmış, dublaj noktasında deepfake uygulanmamıştır.

Şekil 12
Paris Hilton'un Tom Cruise İle Videosundan Kareler (Khanrah, 2022)

Şekil-12'de Paris Hilton'un deepfake ile yapılmış Tik Tok videosundan kareler görüntülenmektedir. Video içeriğinde Hilton, Tom Cruise ile sevgili olduklarına ve beraber yaşadıklarına dair izlenim yaratmaktadır. Video yayınlandıktan sonra bir içerik geliştiricisi Cruise'un taklitçisi olan Miles Fisher ile bir video paylaşmış ve videonun deepfake olduğu anlaşılmıştır. Bu bağlamda ileri boyutta sahtekarlık içeren bu tür videolar için Westerlund (2019) deepfake ile ilgili şu tür ifadelere yer vermektedir;

> "Deepfake hobisi olan topluluklar, yabancı hükümetler ve çeşitli aktivistler gibi siyasi oyuncular, dolandırıcılar gibi diğer kötü niyetli aktörler, televizyon şirketleri gibi meşru aktörler olmak üzere en az dört ana deepfake üreticisi türü vardır. Üreticilerin bu sahtekarlıkları oldukça viral olup, sosyal medya platformları aracılığıyla hızla yayılma eğilimindedir. Bu durum, onları dezenformasyon için etkili bir araç haline getirmektedir" (2019, s. 41).

Ukrayna-Rusya Savaşı Özelinde Deepfake Doküman Analizi

Araştırmanın Metodolojisi

Bu araştırma nitel yönteme dayalı olarak doküman analizi ile gerçekleştirilmiştir. Diğer bir ifadeyle, yazılı ve görsel deepfake dokümanlar betimleyici bir yaklaşımla incelenmiştir.

Araştırmanın Konusu

Bu araştırmada, dijital propagandanın yeni bir versiyonu olan deepfake uygulamasının, Ukrayna-Rusya savaşı özelinde kamuoyunu yanlış bilgilendirmek ve manipülasyon amacıyla kullanımı analiz edilmektedir.

Araştırmanın Amacı ve Önemi

Bu araştırmada, Ukrayna-Rusya savaş sürecinde dijital propagandanın yeni bir versiyonu olan deepfake dokümanların nasıl ve hangi amaçla hazırlandığının betimleyici bir yaklaşımla incelenmesi amaçlanmaktadır. Araştırmada 2 Mart'ta Ukrayna Kara Kuvvetlerinin Resmi Facebook hesabından Rusya'nın Ukrayna'ya yönelik deepfake videosu yayınlayabileceği duyurusunun üzerine, ülke vatandaşlarının bu konu hakkında tepkisi ölçülmek istenmiştir. Bu açıdan araştırmada hem deepfake videolarına ilişkin her iki ülke vatandaşlarının eğilimleri hem de kullanılan deepfake videolarının yarattığı etkinin ölçülmesi amaçlanmaktadır. Bu araştırmanın önemi, savaş ortamında yeni nesil teknolojinin özellikle de yapay zekânın dezenformasyon ve manipülasyon amacıyla nasıl kullanıldığını genel hatlarıyla ortaya koyacak olmasıdır. Daha önce farklı alanlarda kullanım örneklerine rastlanan

deepfake dokümanların ilk kez bir savaş sürecinde kullanılmış olması bu araştırmanın özgünlük kaynağını oluşturmaktadır.

Araştırmanın Kapsam ve Sınırlılıkları

Araştırmanın kapsamı savaşın başladığı 24 Şubat 2022 tarihinden, araştırmanın yapıldığı zamana -17 Aralık 2022- kadar geçen süredeki deepfake dokümanlarını içermektedir. Bu dokümanlar Putin'in itibarını sarsacak nitelikte, sosyal medya mecralarında yayınlanan videolardan oluşmaktadır. Zelenskyy'i hedef alan sadece bir adet deepfake videosuna rastlanılmıştır. Bu video Ukrayna devlet kanalının ve internet sitesinin hacklenmesiyle yayınlanmıştır. Bu bağlamda videonun geniş kitlelere ulaşması hedeflenmiştir.

Dijital sosyal medya ve içerik sağlayıcılarında dolaşıma giren Zelenskyy'e ait deepfake dokümanı, Google, YouTube ve Facebook gibi en çok kullanılan platformlardan kısa süre içerisinde kaldırılmıştır. Rusya'nın hazırladığı dokümanlara Amerikan ve Avrupa sermayesinin kontrolünde olan platformlarda yer verilmediği tespit edilmiştir. Bu durum Ukrayna'nın hazırladığı bu tür dokümanların hedef kitlelere ulaşılabilirliğini Rusya'ya karşın artırmıştır. Araştırmanın sınırlılıkları, Ukrayna'ya yönelik yapılan deepfake videolarının, Ukrayna açısından savaşın seyrine olumsuz etkisi nedeniyle Google, YouTube gibi platformlardan kaldırılmış olmasıdır. Bir diğer sınırlılık ise, videoların çoğunun her iki ülkenin ana dillerinde servis edilmesidir.

Araştırmanın Yöntemi

Bu araştırma, deepfake uygulamaları üzerine yapılan literatür çalışmalarının ve halka açık haber makalelerinin analizlerini kapsamaktadır. Analiz konusu deepfake uygulamaları ile ilgili yazılı ve görsel doküman, grafikler araştırmaya dâhil edilmiştir. Bowen'a (2009) göre doküman analizi, "hem basılı hem de elektronik (bilgisayar tabanlı ve İnternet üzerinden iletilen) materyalleri gözden geçirmek veya değerlendirmek için sistematik bir prosedür" olarak tanımlanmıştır (ss. 27-40). Bowen, doküman analizi için kullanılan belgeleri; gündemler, yoklama kayıtları, toplantı tutanakları, kılavuzlar, kitaplar, broşürler, günlükler, notlar, haritalar, çizelgeler, gazeteler, basın yayınları, program önerileri, başvuru formları ve özetleri, radyo ve televizyon programı metinleri, organizasyonel veya kurumsal raporlar, anket verisi ve çeşitli kamu kayıtları olarak çeşitlendirmiştir (ss. 27-28). Bu araştırmada savaşa dahil olan ülkelerin bu uygulamalara olan yaklaşımı ve yönetimi konusunda bilgi edinilmek istenmiştir. Bu kapsamda devam eden savaşla ilgili dört deepfake videosu incelenmiştir.

Araştırma Soruları

1. Deepfake dokümanlarının dijital propaganda stratejisi açısından amaçları nelerdir ve hangi bağlamlarda kullanılmışlardır?
2. Ukrayna-Rusya arasında karşılıklı uygulanan dijital propaganda faaliyetlerinin ortak noktaları ve ayrıştıkları yönler nelerdir?
3. Savaş sürecinde deepfake dokümanları aracılığı ile uygulanan dijital propaganda türleri, teknikleri ve kuralları açısından nasıl hazırlanmıştır?

Araştırmanın Evren ve Örneklemi

Araştırma kapsamında, ulusal/uluslararası kamuya açık haber makaleleri, sosyal medya platformları ve internet haber sayfaları evreninden, olasılıksız örnekleme yöntemlerinden kolayda örnekleme yöntemiyle belirlenen dört deepfake dokümanı incelenmiştir. Bu yöntemde amaç, "İsteyen herkesin örneklem içerisine ve örnekleme dahil edilmesidir. Bu süreç denek bulma işlemi belirlenen örneklem hacmine ulaşılıncaya kadar devam eder" (Ural & Kılıç, 2011).

Araştırmanın Bulguları ve Yorumlanması

24 Şubat 2022 tarihinden itibaren Rusya, Ukrayna'da bir savaş yürütmektedir. Devam eden Rusya-Ukrayna savaşı, İkinci Dünya Savaşı'ndan bu zamana kadar kamuoyuna yansımış Avrupa'daki en belirgin çatışma niteliğindedir. İkinci dünya savaşından günümüze kadar gelişen ve değişen savaş teknolojileri ile birlikte bu savaşın sadece sahada değil aynı zamanda dijital ortamlarda da sürdürüldüğü görülmektedir. Zira, savaş

Şekil 13

Ukrayna Silahlı Kara Kuvvetlerinin Resmi Facebook Hesabından Deepfake Uyarısı

sırasında oluşturulan pek çok video görüntüsü manipüle edilerek kamuoyuna servis edilmiştir. Bu bağlamda, deepfake uygulamalarıyla hazırlanan çok sayıda video, araştırma bulgularında dijital propaganda unsuru taşıyıp taşımadıklarına göre incelenmiştir.

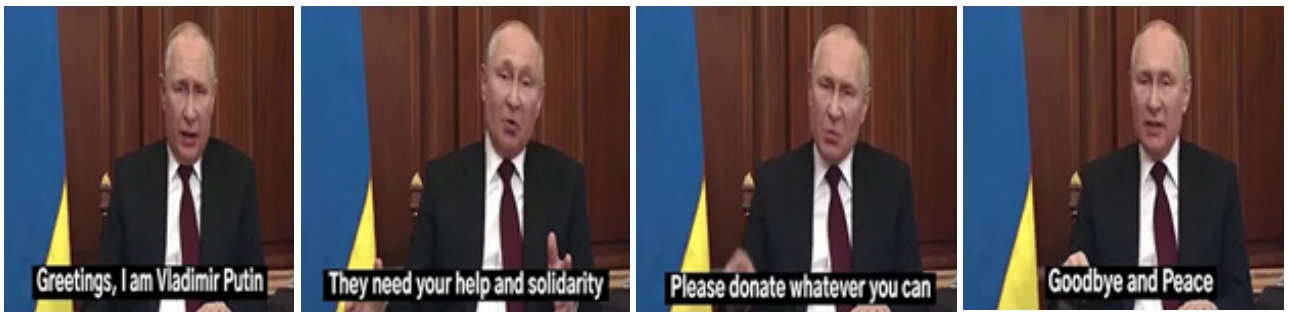
Şekil-13'de Rusya-Ukrayna arasında başlayan savaş ortamında, Ukrayna Kara Kuvvetlerinin resmi Facebook hesabından 2 Mart 2022 tarihinde yayınlanan bildirinin ekran görüntüsü yer almaktadır. Söz konusu açıklamada Rusya'nın Ukrayna'ya yönelik deepfake videosu yayınlayabileceği duyurulmuştur. Dijital ortamda yayınlanan bu duyuru, savaş ortamında başlaması muhtemel deepfake uygulamalarına karşı alınan tedbir mahiyetindeki ilk açıklama olmuştur.

Ukrayna Kara Kuvvetlerinin Resmi Facebook sayfasından yapılan açıklamayla Rusya'nın deepfake dokümanları ile Ukrayna halkının moral ve motivasyonunu bozmasının, halkın endişeye sokulmasının önüne geçilmek istenmiştir. Bu duyuru ile aynı gün Youtube'da Putin'in dünyaya seslendiğini gösteren, ekran alıntılarının Şekil-14'de gösterildiği bir başka deepfake dokümanı yayınlanmıştır.

Videoda, Putin'in konuşmalarının YouTube'da altyazılı olarak verildiği görülmektedir. Konuşmada "Selamlar ben Putin önemli bir mesajım var. Acımasız ve suçlu işgalime karşı Ukrayna ile dayanışma içinde olun, lütfen Ukrayna'ya yardım etmek için elinizden geleni yapın" ifadelerine yer verilmektedir.

Şekil 14

Putin'in Dünyaya Seslendiği DeepFake Videosu (Youtube, 2022)



2 Mart 2022 tarihinde YouTube'da yayınlanan, Putin'in dünyaya seslendiği deepfake dokümanının görüntü manipülasyonu yönüyle incelenmeksizin, mesajın içeriği nedeniyle sahte olduğu kolaylıkla anlaşılmaktadır. Kayıtta, kendini suçlu hisseden bir devlet başkanının savaş açtığı ülke için yardım istediği görülmektedir. Video içeriğindeki bu söylem ve arka plandaki Ukrayna bayrağının görüntüsü, söz konusu deepfake dokümanının Ukrayna ya da Ukrayna yanlıları tarafından oluşturulduğunun açık göstergesidir.

Devam eden savaş sürecinde, ülke vatandaşlarını etkileyebilecek iki önemli deepfake dokümanı yayınlanmıştır. Bunlardan ilkinde 16 Mart 2022 tarihinde Ukrayna Devlet Başkanı Volodymr Zelenskyy Ukrayna halkına silah bırakma, ikincisinde ise 17 Mart 2022 tarihinde Rusya Devlet Başkanı Putin barış ilanı duyurusu yapmıştır (Reuters, 2022).

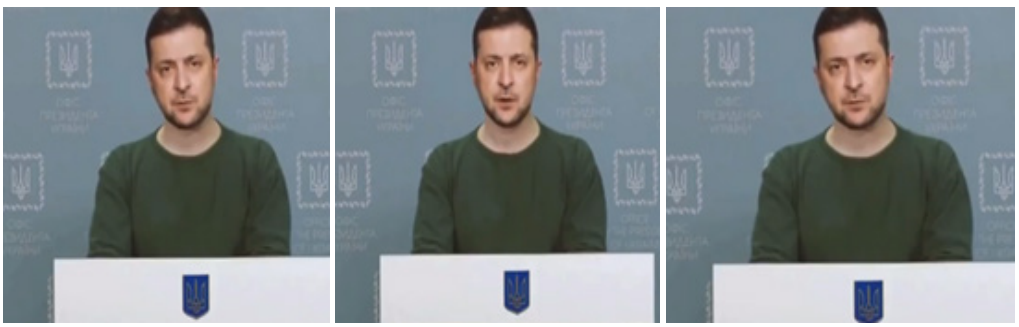
16 Mart 2022 tarihinde Ukraine 24 televizyon kanalının ve internet sitesinin hacklenmesi ile birlikte yayınlanan, deepfake olduğu anlaşılan video içeriğinin ekran alıntıları Şekil-15'te gösterilmektedir. Doğrulama web sitesi Verify, bu videonun Zelenskyy'nin önceki basın toplantılarındaki hareketsiz görüntülerini kaynak olarak kullanan yapay zekâ tarafından oluşturulduğunu doğrulamıştır (Arab News, 2022).

Şekil-15'te ekran görüntülerinin sunulduğu video içeriğinde Zelenskyy; "Sevgili Ukraynalılar! Sevgili savunucular! Başkan olmak o kadar kolay değildi. Zor kararlar vermek zorundayım. İlk başta Donbas'ı iade etmeye karar verdim. İşe yaramadı. Sadece daha da kötüleşti. Çok daha kötü. Artık yarın yok. En azından bende. Ve şimdi sana veda etmeye karar verdim. Silahlarınızı bırakmanızı ve ailelerinizin yanına dönmenizi tavsiye ederim. Bu savaşta ölmemelisin. Sana yaşamanı tavsiye ediyorum ve ben de aynısını yapacağım" ifadelerini kullanmaktadır. Videonun görsel manipülasyon içerip içermediğine ilişkin inceleme yapıldığında, arka fonda seslerin gelmesi, Zelenskyy'nin baş bölgesi ile gövdesinin orantısız oluşu gibi ipuçlarına rastlanılmaktadır.

Reuters tarafından servis edilen haberde (2022) söz konusu deepfake uygulamasının amacına ulaşamadığı belirtilmiştir. Ukraynalı yetkililerin hazırlanan senaryo hakkında halkını daha önceden uyarması, sosyal medya kanallarında Zelenskyy'nin bizzat kendisinin videoyu anında yalanlayışı, video kalitesinin düşük oluşu deepfake uygulamasının başarısız olmasının sebepleri olmuştur. Sahte videonun ardından ekran resimleri gösterilen Şekil-16'da Ukraine 24 televizyon kanalında ve sosyal medya platformlarında Zelenskyy'nin telefon kamerasıyla çektiği bir video yayınlamıştır. Videoda Zelenskyy, Ukrayna'nın aslında teslim olmadığını ve deepfake videoda öne sürülen iddiaların asılsız olduğunu ifade etmektedir.

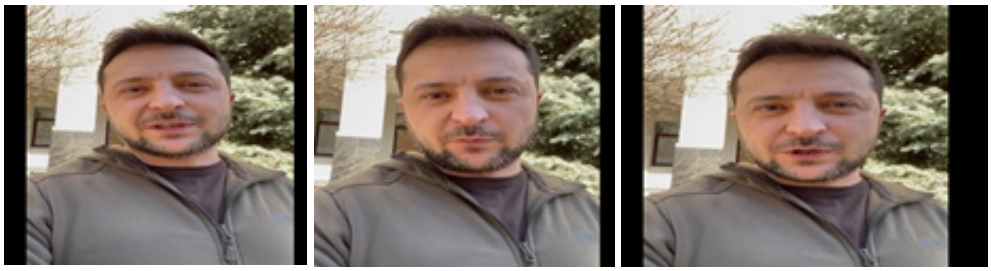
Şekil 15

Zelenskyy'nin Ukraine 24 Televizyon Kanalının ve İnternet Sitesinin Hacklenmesinin Ardından Yayılan Deepfake Uygulaması (Cole, 2022)



Şekil 16

Zelenskyy'nin Deepfake Videodaki Söylemlerini Twitter da Yalanladığı Video Görüntüsü



Zelenskyy, Şekil-16'daki video gönderisinde Ukraynalıları teslim olmaya çağırdığı iddialarını yalanlayıp, Ukrayna'da olduğunu ve ülkesini koruduğunu ifade etmektedir. Videonun çevirisine göre Zelenskyy "Silah bırakmayı teklif ettiğim son çocukça provokasyona gelince. Sadece Rusya Federasyonu ordularına silah bırakmayı ve eve dönmeyi teklif edebilirim. Ve biz zaten evdeyiz. Toprağımızı, topraklarımızı çocuklarımızı ve ailelerimizi savunuyoruz. Ve kesinlikle silahlarımızı bırakmayacağız. Zafere kadar" ifadelerine yer vermektedir (Cole, 2022).

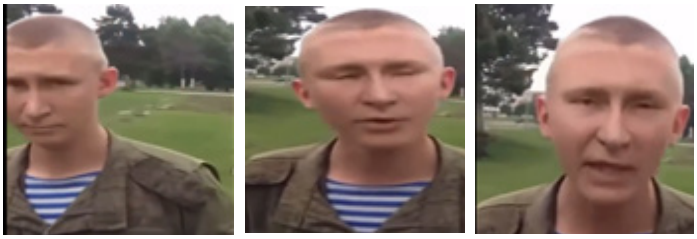
Savaş devam ederken Putin'e benzerliği ile dikkat çeken bir üniformalı askerin, Şekil-17'de ekran resimlerinin sunulduğu deepfake videosu sosyal medya platformlarında dolaşmaya başlamıştır.

Videoda Rus üniformalı kişiye "83. Tugay neden bu kadar yetersiz besleniyor?" sorusu sorulmakta, askerin ise "Biliyorsun, Sergey, bu konuyu daha önce ele aldım ve tekrar söyleyeceğim, sadece 83. Tugaya bakarsak, Rus Hava Kuvvetleri genelinde resmin tamamını göremiyoruz" cevabına yer verilmektedir. Bu videoyu görüntü manipülasyonu yönüyle incelemeden de Putin'e benzerliği olan kişinin çok zayıf ve yaşının küçük olduğu açıkça anlaşılmaktadır. Putin'in yüz özelliklerinin başka bir yüzün üzerine yerleştirildiği ve görüntü kalitesinin düşük olduğu bu videoda konuşan kişi, Putin'in sesine ve yüzüne sahipmiş gibi görüntülenmektedir. Newsweek'in (2022) gerçek kontrolü yazısında, askerin fiziksel özelliklerinin ve vücut yapısının Rusya Devlet Başkanı'nınkine benzemediği, videonun ilk olarak 2021 yılında, Ukrayna çatışmasından önce çevrimiçi olarak yayınlandığı belirtilmektedir. Söz konusu deepfake 'in birkaç versiyonu YouTube'da ve Rus sosyal medya platformu VK'da yer almaktadır. Aslında bu video Rusya'nın 2022 yılında Ukrayna'yı işgalinden çok önce sosyal medyada da dolaşmaya başlamıştır. Savaşla beraber tekrar gündeme getirilmiştir **(**Kaonga, 2022).

Şekil-18'de 17 Mart 2022 tarihinde servis edilen, içeriğinde Putin'in barış ilan ettiği ifadeleri yer alan, deepfake dokümanına ait ekran alıntıları görülmektedir.

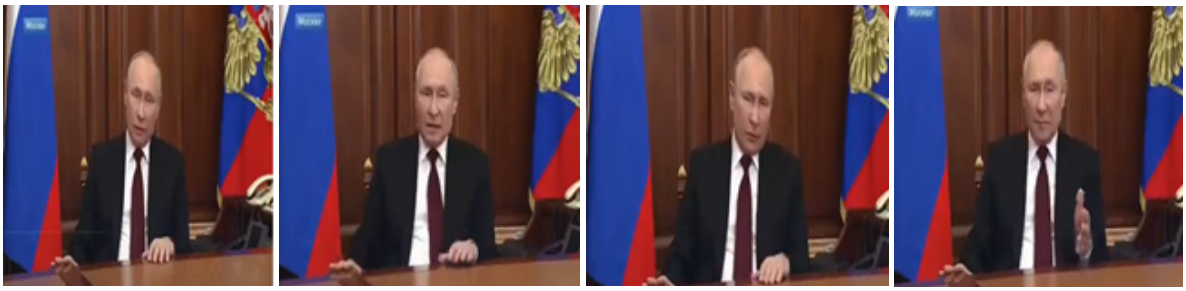
Şekil 17

Putin'in Asker Deepfake Videosundan Kareler (Kaonga, 2022)



Şekil 18

Putin'in Barış İlan Ettiğine İlişkin Deepfake Videosundan Kareler (Reuters, 2022)



Reuters'e göre (2022) söz konusu içerik, 1 Şubat 2022 tarihinde Kremlin tarafından yayınlanan Putin'e ait gerçek bir videonun manipüle edilmesiyle oluşturulmuştur. Putin Ukrayna ile barışı sağlamayı başardığını ve Ukrayna içinde bir Cumhuriyet kurularak Kırım'ın bağımsızlığının yeniden tesis edildiğini ilan etmektedir. "Rus askeri, hayattayken silahlarınızı bırakın ve evinize gidin!" ifadelerinin yer aldığı videoda mat bir görüntünün varlığı ve ağız yapısında kaymalar olduğu gözlemlenmiştir. Kukla ustası olarak gerçekleştirilen deepfake videosunun gerçekçi ve orijinal videolardan ayrılamayacak kadar başarılı olduğu görülmektedir (Butler, 2022).

Verify, web sitesinde video kaydının 21 Şubat 2022 tarihine ait olduğunu doğrulamaktadır. Şekil-19'daki ekran resimleri incelendiğinde Putin'in el hareketlerinin, duruşunun, giydiği takım elbisenin, taktığı kravatın ve sergilenen arka planın her iki videoda da aynı olduğu görülmektedir. İki video arasındaki tek fark sestir. Yapılan ses analizi, sahte videodaki sesin Putin'in 21 Şubat 2022 tarihinde yayınlanan videosundaki orijinal sesinden farklı olduğunu göstermektedir. Verify, düzenlenen sesin kaynağını doğrulayamamış, Rusça ve İngilizce transkripsiyonu ararken hiçbir arama sonucuna ulaşamamıştır.

Savaş ortamında ilk kez kullanılan deepfake'ler, savaş ilan eden ülkelerin halkı ve basın organlarının gündeminde olmuştur. Hedef kitlesinde oluşturduğu algılar ile savaşın gidişatını etkileyecek kadar güçlü bir propaganda faaliyetine sahip bu uygulamalarla birlikte savaşın dijital platformlara taşındığı görülmektedir.

Tüm bu araştırmaların sonucunda elde edilen bulgularla Tablo-1 ve Tablo-2 oluşturulmuştur. Literatür taramalarını ve haber makalelerini de sentezleyerek oluşturulan, Ukrayna-Rusya savaşı sırasında uygulanan propagandaların ortak ve ayrıştıkları noktaları içeren tablo aşağıda sunulmaktadır.

Geleneksel propaganda türlerinin Ukrayna-Rusya deepfake'leri bazında dijital propagandaya entegrasyonu Tablo-1'de gösterilmektedir. Ukrayna'ya yönelik yapılan deepfake dokümanı sahası bakımından dış, konusu bakımından askeri, kaynakları bakımından beyaz ve gri, kullanışı

Şekil 19

Putin'in Deepfake Videosunun Verfiy Analizi (Jones, 2022)

Tablo 1

Geleneksel Propaganda Türlerinin Ukrayna-Rusya Deepfake'leri Bazında Dijital Propagandaya Entegrasyonu

Deepfake Dokümanlarının Muhatabı Olan Ülke	**Sahası Bakımından Yapılan Propaganda Türü**	**Konusu Bakımından Yapılan Propaganda Türü**	**Kaynakları Bakımından Yapılan Propaganda Türü**	**Kullanışı Bakımından Propaganda Türü**
Ukrayna	-Dış Propaganda	-Askeri Propaganda	-Beyaz Propaganda	-Taktik Propaganda -Karşı Propaganda -Takviye Amaçlı Propaganda
Rusya	-Dış Propaganda	-Askeri Propaganda	-Beyaz Propaganda -Gri propaganda	-Stratejik ve Taktik Propaganda

bakımından taktik, karşı ve takviye amaçlı propaganda olarak kategorilere ayrılmıştır.

Dış propagandanın amacı, uluslararası platformlarda kendi uluslarını ön plana çıkarmak için faaliyet yürütmektir (Karaca & Çakı, 2018, ss. 75-114). Askeri propagandanın amacı, rakip tarafın motivasyonunu bozmak veya yok etmek için hedef kitleyi etkileyebilecek her yolu kullanmaktır. Stratejik propaganda daha çok ileride oluşabilecek muhtemel savaş durumlarına hazırlık için planlanmaktadır. Dolayısıyla stratejik propaganda, kitlelerin eğilimlerine göre ön plana çıkmakta, sürekli tekrar yöntemi ile hafızalara kazınmakta böylece doğrudan ihtiyaçlara hitap ederek beyinleri yıkamaktır (Leblebitozu, 2022). Beyaz propagandanın amacı kaynağın güvenilir olmasıyla birlikte hedef kitlenin propaganda karşısında alternatif bir çözüm düşünmemesini sağlamaktır (Bektaş, 2013, ss. 5-272). Gri propagandanın belirsiz veya açıklanmayan bir kaynağı veya amacı vardır (Wikipedia, 2023). Ukrayna tarafından hazırlanan deepfake dokümanlarının başarısı bünyesindeki uzman personelinin ve gelişmiş bilişim sektörünün yanı sıra siber savunma ve siner saldırı faaliyetleri için batıdan destek almasının rolü büyük olmuştur. Bu yönüyle sahası bakımından kullanılan propaganda türü için gri propaganda kullanıldığı da ifade edilebilir. Taktik propaganda ise stratejik propagandaların daha küçük çaplı olan şekli olarak kısa vadede hemen sonuç almak için uygulanmaktadır. Bu bağlamda düşmanın zayıf noktaları taktik stratejilerle etkin olarak değerlendirilmektedir. Takviye amaçlı propaganda da ise işgal edilen yerlerin yeniden teşkilatlanmasında ve yeni sahalarda direnişle karşılaşmamak için halkın her türlü ihtiyaçları giderilmeye çalışılmaktadır. Bu sayede sistemli bir şekilde hoparlörlerle halka rahatlatıcı mesajlar verilmekte ve çeşitli kitle iletişim araçları etkin bir şekilde kullanılmaktadır (Tarhan, 2003, ss. 51-52).

Araştırma kapsamında literatür taramaları, haber makaleleri ve deepfake dokümanları incelenmiştir. Sentezlenen bilgilerle Ukrayna-Rusya savaşı sırasında yapılan dijital propaganda türlerinin, manipüle edilmiş mesajları iletme yönünden ortak ve ayrıştıkları yönlerini içeren tablo aşağıda sunulmaktadır.

Tablo 2

Dijital Propaganda Tekniklerinin (Görsel-İşitsel Manipülasyon) Ukrayna-Rusya Deepfake'leri Bazında Karşılaştırılması

Dijital Propagandaya Maruz Kalan Ülke	**Dijital Propaganda Türü**	**Dijital Propaganda Uygulanış Çabası**	**Kategorize Edilen Deepfake Doküman Türü**	**Kullanılan Özel Teknikler**
Ukrayna	-Bilişsel Propaganda	-Dağıtılmış Hizmet Reddi (Ddos Uygulaması)	-Dudak Senkronizasyonu -Ses Dönüştürme	-Lider Kullanımı -İzleyicide Yankı Uyandırma -Karşı Saldırı
Rusya	-Bilişsel Propaganda -Conative Propaganda	-Politik Botlar	-Dudak Senkronizasyonu -Ses Dönüştürme -Kukla Ustası	-Lider Kullanımı -İzleyicide Yankı Uyandırma

Tablo-2'ye göre Ukrayna'ya yönelik yapılan deepfake 'de Ukraine 24 televizyon kanalının hacklenmesi, kanala Ddos uygulaması yapıldığını göstermektedir. Zelenskyy'nin görüntüsünün yer aldığı videoda dudak senkronizasyonu yöntemiyle ve sesiyle manipülasyon oluşturulduğu gözlemlenmiştir. Rusya'nın siber saldırıları karşısında Ukrayna'nın deepfake dokümanları neticesinde olası propagandalar için halkını önceden uyardığı, hızlı dönüşlerle karşı saldırılarda bulunduğu söylenebilir. Ukrayna dijital platformlarda psikolojik savaşı yenebilmek için bilişsel propaganda türünü, dijital ortamda güç dengesini ayakta tutabilmek içinse conative propaganda türünü kullanmıştır. Rusya'ya yönelik yapılan deepfake'lerde hedefin yüz ifadeleri ve baş hareketlerinin aynı kaldığı, hedef kişinin yüz ifadelerinin ve baş hareketlerinin yönlendirildiği görülmektedir. Bu türe "kuklacı" senaryosu da denir çünkü kuklanın kimliği korunurken, ifadeleri bir usta -kaynak- tarafından yönlendirilir (Bernaciak & Ross, 2022).

Sonuç ve Öneriler

24 Şubat 2022 tarihinde başlayan Rusya-Ukrayna savaşında her iki taraf da çatışma süresince yaygın dezenformasyon üretmişlerdir. Bununla birlikte, Ukrayna çatışması bağlam dışında çekilmiş fotoğraflardan, yalanları teşvik etmek için yapay teknolojiler kullanan, dijital olarak manipüle edilmiş filmlere kadar birçok dezenformasyon biçimi için verimli bir zemin olmuştur (Dhyani, 2022). Bu açıdan deepfake dokümanı oluşturmadaki son gelişmeler, deepfake'i daha gerçekçi ve yapımı daha kolay hale getirmektedir. Gerçekliğinin ayırt edilmesi zor olan deepfake, potansiyel tehditlerle mücadele etmek için deepfake algılama yöntemleri gerektiren ulusal güvenlik, demokrasi, toplum ve mahremiyetimize yönelik önemli bir tehdit olmuştur (Zhang, 2022, ss. 6259-6276). Gerçekçi dijital insanlar yaratmanın demokratikleşmeye olumsuz etkileri olduğu gibi, görsel efektlerdeki uygulamalar, dijital avatarlar, Snapchat filtreleri, sesini kaybedenlerin seslerini oluşturma veya film bölümlerini yeniden çekmeden güncelleme yapabilme gibi deepfake'lerin pek çok olumlu kullanımları da vardır (Nguyen vd., 2022, s. 2).

Dolayısıyla deepfake uygulamalarına telefonlara yüklenen aplikasyonlarla ulaşımının kolaylığı ve video oluşturma aşamalarının çok fazla nitelik gerektirmediği gibi etkenler, daha çok kişinin, bu tür içerikler üretmesinin önünü açmıştır. Başlangıçta eğlence amacıyla kullanılan uygulama, teknolojinin ilerlemesiyle siber güvenliği etkileyecek nitelikte, yapay zekâyı da kullanarak orijinal görünen sahte videolar üretilmesine olanak sağlamıştır. Videolar çoğunlukla görüntülerin manipülasyon yöntemiyle değiştirilip kişinin yapmadığını yapmış, söylemediğini ise söylemiş gibi gösterebilmektedir. Söz konusu uygulamalar bazı kesimler için birçok avantaj ve kolaylık barındırdığı gibi telafisi mümkün olmayan veya bedeli ağır olan sonuçlara da neden olabilmektedir. Yoğun dezenformasyon ve propaganda amacıyla düzenlenen içerikler bazen kişiye özgü hak ihlallerine bazen de ülkeler arası diplomatik ilişkilerde sarsıcı etkilere sebebiyet verebilir. Bu tür uygulamalar daha çok gördüklerinize ve duyduklarınıza inanamayacağınız etkiler yaratabilmesi nedeniyle sosyolojik açıdan değerlendirildiğinde güven duygusunun azalmasına neden olabilir. Güven kargaşası savaş ortamındaki propagandanın ana unsuru haline gelebilir. Bu bağlamda deepfake dokümanlarını yeni nesil dijital propaganda faaliyetlerinin yeni bir versiyonu olduğunu söylemek mümkündür.

"Son dönemin en önemli iletişim olgularından biri olan internet, küresel düzeyde ana iletişim araçlarından biri durumuna gelmiştir" (Ün & Türkal, 2018). Bu sayede yakın gelecek için, ilerleyen teknoloji ile deepfake uygulamalarının aynı seyirde gelişmesiyle servis edilen deepfake video içeriklerinin orijinal video içeriği olup olmadığı anlaşılmayacak seviyelere gelebilir. Söz konusu uygulamalar ile oluşturulan içeriklerin doğruluğunun teyit edilmesi gerekmektedir. Zira bu içerikler, uluslararası diplomatik ilişkileri olumsuz etkileme potansiyeline sahiptir. Çatışmaları alevlendirebilir, video içeriği şeklindeki kanıtların hukuki açıdan gerçekliğinden şüphe edilebilir, bankacılık ve miras işlemlerinde telafisi güç sonuçlar doğurabilir, insanların medyaya olan güveni sarsılabilir, yanlış bilgiler aracılığıyla provokasyona neden olarak "öfkeli kamuoyu"

oluşturabilir, seçimleri manipüle edebilir. Halihazırda Ukrayna-Rusya özelinde, savaşan iki ülkenin hazırladığı bu uygulamalara; her iki tarafın da hazırlıklı oluşu ve bilişim altyapılarının yeterliliği nedeniyle bu uygulamaların savaşın seyrine herhangi bir etkisi olmadığı tespit edilmiştir. Bu nedenle olası propaganda eylemleri sonuçsuz kalmıştır.

Bu araştırmada Rusya'nın siber saldırılarına maruz kalan Ukrayna'nın deepfake dokümanları neticesinde olası propagandalar için halkını önceden uyardığı, hızlı dönüşler alıp karşı saldırılarda bulunduğu sonucuna varılmıştır. Ukrayna'nın deepfake dokümanları ile karşı saldırılara geçtiği, videolarda daha çok Putin'i itibarsızlaştıracak içerikler geliştirdiği gözlenmiştir. Ukrayna'nın maruz kaldığı deepfake dokümanlarının olumsuz sonuçlarından en az şekilde etkilenmesinde, Ukrayna Silahlı Kuvvetleri bünyesindeki uzman personelinin ve gelişmiş bilişim sektörünün yanı sıra siber savunma ve siber saldırı faaliyetleri için batıdan destek almasının rolü büyük olmuştur.

Bu araştırma; deepfake dokümanları üzerine yapılacak araştırmalarda kuruluşlara, siyasetçilere ve medyaya alanları ile ilgili bilgilerin doğruluğunu teyit etmelerine ve değerlendirmelerine yardımcı olacaktır. Deepfake'in kötüye kullanımlarından dolayı mağdur olabileceklerin ise bu uygulamaları daha iyi anlamalarını ve kötü niyet okumalarını daha iyi yapmalarını sağlayacaktır.

Gelecek dönemler için duyulan endişeler arasında bu uygulamaların daha ileri boyutta mahkemelerde delil, siyasi sabotaj, terör propagandası, şantaj, piyasa manipülasyonu ve sahte haberler, intikam pornosu, zorbalık, sahte video için giderek daha fazla kullanılacağı üzerinedir (Maras & Alexandrou, 2019). Dolayısıyla gelecek araştırmalarda teknik imkanların gelişmesiyle birlikte bu uygulamaların daha gerçekçi ve profesyonel yapılacağı düşünülerek deepfake dokümanlarına ilişkin farklı çalışmalar yapılabileceği tahmin edilmektedir.

Kaynaklar

Acar, H. M., & Tanyıldızı, N. İ. (2022). Reklamda yapay zekâ kullanımı: Ziraat Bankası# sen hep gülümse reklam filminde deepfake uygulamasının görsel anlatıya etkisi. Kastamonu İletişim Araştırmaları Dergisi, (8), 78-99.

Aliefendioğlu, M. (2020). Dijital propaganda. .

Arab News. (2022). Zelenskyy deepfake video goes viral, reflecting troubling new wave of disinformation. https://www.arabnews.com/node/2044866/spa/page_view_ti ming/aggregate.

Baki, O. (2021,). İnsan ile hayvan yüzleri arasında dönüşüm yapabilen yapay zekâ. https://www.webtekno.com/insan-ile-hayvan-yuzleri-arasinda-donusum-yapabilen-yap ay-zeka-h91471.html.

Bektaş, A. (2013). Kamuoyu, iletişim ve demokrasi. İstanbul: Bağlam Yayıncılık.

Bennett, W. Lance., and Steven Livingston. (2018). The disinformation order: disruptive communication and the decline of democratic ınstitutions. European Journal of Communication 33(2): 122–139. https://doi.org/10.1177/0267323118760317.

Bernaciak & Ross. (2022,1 Mayıs). How easy is it to make and detect a deepfake? https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake.

Bickerton, J. (2020). Kim Jong-un' delivers urgent us election warning – 'not hard for democracy to collapse'. https://www.express.co.uk/news/world/1348410/Kim-Jong-un-news-North-Korean-leader-US-election-deepfake-Donald-Trump-Joe-Biden-on.

Bilgi University Website. (2021). Global politics in the age of computational propaganda online conference. https://www.bilgi.edu.tr/en/event/10386/global-politics-in-the-age-of-computational-propaganda-online-conference/.

Boháček, M., & Farid, H. (2022). Protecting President Zelenskyy against deep fakes. *ArXiv preprint arXiv:2206.12043*. https://doi.org/10.48550/arXiv.2206.12043.

Boredpanda. (2021). New app creates deepfakes of lip-synced pictures, and ı used ıt to have a laugh (13 Pics). https://www.boredpanda.com/digital-art-singing-pictures-pop-culture-characters-wombo aiidreley/?utm_source=google&utm_medium=organic& utm_cam paign.

Botha, J., & Pieterse, H. (2020). Fake news and deepfakes: A dangerous threat for 21st century information security. In *ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited* (s. 57).

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9(2),* 27-40.

Brahm, E. (2006). Propaganda. https://www.beyondintractability.org/essay/ propaganda.

Brooks, C. F. (2021). Popular discourse around deepfakes and the interdisciplinary challenge of fake video distribution. *Cyberpsychology, Behavior, and Social Networking*, *24*(3), 159-163.

Brown, É. (2018). Propaganda, Misinformation, and the epistemic value of democracy. *Critical Review, 30(3-4),* 194-218.

Butler. (2022). Putin declares peace with Ukraine in debunked deepfake video. https://www.indy100.com/news/putin-peace-ukraine-deepfake-video.

Celebrtiy. (2021). What is a deepfake and how are they made? https://celebrity.land/what-is-a-deep-fake-and-how-are-they-made/.

Cervantes, E. (2021). What is deepfake? Should you be worried? .

Cochran, J. D., & Napshin, S. A. (2021). Deepfakes: awareness, concerns, and platform accountability. *Cyberpsychology, Behavior, and Social Networking*, *24*(3), 164-172.

Cole, S. (2022). Hacked news channel and deepfake of Zelenskyy surrendering ıs causing chaos online. https://www.vice.com/en/article/93bmda/hacked-news-channel-and-deepfake-of-zelenskyy-surren dering-is-causing-chaos-online.

D'Alessio, F. A. (2021). Computational propaganda: challenges and responses. *Academia Letters*, 2. http://dx.doi.org/10.20935/AL3468.

Dhyani, A. (2022). Rise of deep-fakes in Russia – Ukraine conflict. https://thekootneeti.in/2022/11/01/rise-of-deep-fakes-in-russia-ukraine-conflict/.

Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., & Ferrer, CC (2020). The deepfake detection challenge (dfdc) dataset. *arXiv preprint arXiv:2006.07397*. https://doi.org/10.48550/arXiv.2006.07397.

Esselink. J. (2021). *Deepfakes and extreme beliefs. An ethical assessment.* (Master's Thesis, Amsterdam).

European Parliamentary Research Service. (2018). Computational propaganda techniques. https://www.europarl.europa.eu/regdata/etudes/atag/2018/628284/eprs_ata (2018)628284_en.pdf.

European Parliament Research Service. (2018). Computational propaganda techniques. https://epthinktank.eu/2018/10/22/computational-propaganda-techniques.

Fletcher, J. (2018). Deepfakes, artificial ıntelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal*, *70*(4): 455–471. Project Muse, https://doi.org/10.1353/tj.2018.0097.

Fletcher, J. (2018). Deepfakes, artificial ıntelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal*, *70*(4): 455–471. Project Muse, https://doi.org/10.1353/tj.2018.0097.

Frank, A. (2018). Computational propaganda: bots, targeting and the future. .

Galloway, M. (2022). Deepfakes may use new technology, but they're based on an old idea. https://www.popsci.com/technology/deepfakes-history-museum-exhibit/.

Gov.Uk. Web. (2019). Snapshot paper- deepfakes and audiovisual disinformation. https://www.gov.uk/government/publications/cdei-publishes-its-first-series-of-three-snapshot-papers-ethical-issues-in-ai/snapshot-paper-deepfakes-and-audiovisual-disin formation.

Great Learning (2022). All you need to know about deepfake aıhttps://www.mygr eatlearning.com /blog/all-you-need-to-know-about-deepfake-ai/.

Hancock, J. T., & Bailenson, J. N. (2021). The social impact of deepfakes. *Cyberpsychology, Behavior, and Social networking*, *24*(3), 149-152.

Hartmann, K., & Giles, K. (2020). The next generation of cyber-enabled information warfare. In *2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, ss. 233-250). IEEE.

Jones, K. (2022). Want something verified? No, the video of Russian President Vladimir Putin announcing peace isn't real. 9341555fd0.

Kahraman, İ., & Fidan, Z. (2022). Yeni bir propaganda mecrası olarak dijital oyunlar. *TRT Akademi*, *7*(16), 852-887. https://doi.org/10.37679/trta.1139103.

Karaca, M., & Çakı, C. (2018). *İletişim ve propaganda*. Eğitim Yayınevi.

Kaonga, G. (2022). Fact check: does video show 'Putin's double' fighting on Ukraine frontline? https://www.newsweek.com/vladimir-putin-ukraine-front-lines-deep-fake-video-fact-check-russia-1751468.

Kenez, P. (1985). *The birth of the propaganda state: Soviet methods of mass mobilization, 1917-1929*. Cambridge: Cambridge University Press.

Khanrah, A. (2022). DeepFake video: are Tom Cruise and Paris Hilton dating? https://therecenttimes.com/news/deep-fake-video-are-tom-cruise-and-paris-hilton-dating

Korkmaz, Ş., & Alkan, M. (2021). Derin öğrenme algoritmalarını kullanarak deepfake video tespiti. *Politeknik Dergisi*, 1-1. https://doi.org/10.2339/politeknik. 1167225.

Kucher, D. (2020). Artificial intelligence. https://www.somagnews.com/artificial-intelligence-can-transform-human-animal-faces/.

Leblebitozu. (2022). Propaganda nedir? Propaganda çeşitleri, propaganda teknikleri nelerdir? http://www.leblebitozu.com/propoganda-nedir-propoganda-cesitleri-propoganda-teknikleri-nelerdir/?

Lock, I., & Ludolph, R. (2020). Organizational propaganda on the Internet: A systematic review. *Public Relations Inquiry*, *9*(1), 103-127. https://doi.org/10.1177/ 204 6147X19870844.

Maras, M. H. (2017). Social media platforms: Targeting the 'found space'of terrorists. *Journal of Internet Law*, 21(2), 3-9.

Maras, M.H. ve Alexandrou, A. (2018). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. The International. *Journal of Evidence & Proof*, 23(3), 255-262. https://doi.org/10.1177 /1365712718807226.

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2022). Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, 1-53. https://doi.org/10.1007/s10489-022-03766-z.

Mitra G,2020 What exactly are deepfakes and how do they work? https://www.expresscomputer.in/features/what-are-deepfakes-and-how-do-they.

Moran, M. (2020). Deepfake videos to make up '90% of online content' in just five years. https://www.dailystar.co.uk/news/latest-news/artificial-intelligence-created-deepfake-videos-22761685.

Narayan, K., Agarwal, H., Mittal, S., Thakral, K., Kundu, S., Vatsa, M., & Singh, R. (2022). Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (cvpr) workshops, 2022, ss. 2858-2867.

Netlingo. (2022). Deepfake. https://www.netlingo.com/word/deepfake.php.

Neyazi, T. A. (2020). Digital propaganda, political bots and polarized politics in India. *Asian Journal of Communication*, *30(1),* 39-57, http://dx.doi. org.10.1080 /012929 86.2019.1699938.

Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., ... & Nguyen, C. M. (2022). Deep learning for deepfakes creation and detection: A survey. *Computer Vision and Image Understanding*, *223*, 103525. https://doi.org/10.1016/j.cviu.2022.103525

Norman, J. (2022). Video Rewrite, Origins of Deepfakes. https://www.historyofinformation.com/detail.php?id=4792.

Özdemir, Ö. C., & Taşcıoğlu, R. (2022). Kurumsal iletişimde sosyal medya kullanımı: Cumhurbaşkanlığı İletişim Başkanlığı üzerine bir inceleme. *Karadeniz Uluslararası Bilimsel Dergi*, *1(53),* 65-81.

Reuters. (2022). "Fact check-doctored video appears to show Putin Announcing Peace." https://www.reuters.com/article/factcheck-putin-address-idusl2n2vk1cc .

Sagar, R. (2019). Artificial ıntelligence brings Mona Lisa to life using gans. https://analyticsindiamag.com/artificial-intelligence-brings-mona-lisa-to-life-using-gans/ .

Schick, Nina. (2020). Deepfakes and the ınfocalypse: What you urgently need to know [Kindle version] (London UK: Octopus Publishing Group).

Shao, G. (2022). What 'deepfakes' are and how they may be dangerous. .

Song, D. (2019). A short history of deepfakes. https://medium.com/@songda/a-short-history-of-deepfakes-604ac7be6016.

Stamm, M. and Liu, K. (2010). Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Transactions on Information Forensics and Security, 5(3), pp.492-506. http://dx.doi.org /10.1109/TIFS.2010.2053202.

Tarhan, N. (2003). Psikolojik savaş. İstanbul: Timaş Yayınları.

Temir, E. (2020). Deepfake: New era in the age of disinformation & end of reliable journalism. *Selçuk İletişim*, *13*(2), 1009-1024.

Thalen, M. (2022). Hackers drop deepfake of Zelenskyy ordering troops to surrender on Ukrainian news site. https://www.dailydot.com/debug/hackers-zelenskyy-deepfake-surrender-ukraine-war/.

Ural, A ve Kılıç, İ. (2011). Bilimsel araştırma süreci ve SPSS ile veri analizi. 3. baskı. Ankara: Detay.

Ün, H. & Türkal, İ. (2018). Kurumsal iletişim bağlamında yükseköğretim kurumlarının sosyal medya kullanımları: Üniversitelerin Youtube kanallarını kullanımları üzerine bir inceleme. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *22*(Özel Sayı 3), 2811-2833.

Wang, J., Sun, Y., & Tang, J. (2022). Lisiam: localization invariance siamese network for deepfake detection. *IEEE Transactions on Information Forensics and Security*, *17*, 2425-2436.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, *9*(11). ss. 39-52. .

Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy*, *5*(2), 199-217. http://dx.doi.org/10.1080/23738871.2020.1797135.

Wikipedia. (2023). Propaganda. https://en.wikipedia.org/wiki/Propaganda.

Woolley, S. C., & Howard, P. N. (2016). Political communication, computational propaganda, and autonomous agents: Introduction. *International Journal of Communication*, *10*.

Woolley, S. C., & Howard, P. N. (2018). Introduction: computational propaganda worldwide. *computational propaganda: Political parties, politicians, and political manipulation on social media*, 3-18. https ://doi.org/10.1093/oso/9780190931407.003.0 001.

Youtube. (2022). Kemal Sunal reklamı nasıl çekildi? Yapımcıları anlatıyor. Kamera arkası/2. deepfake. https://www.youtube.com/watch?v=t9DbUAaJr9M .

Youtube. (2022). Putin deepfake: #standwithukraine. https://www-youtube-com.translate.goog/ watch?

Zhang, T. (2022). Deepfake generation and detection, a survey. *Multimedia Tools and Applications*, *81*(5), 6259-6276.

Extended Abstract

This study examines the characteristics of the usage of deepfake documents, which is the new version of digital propaganda, in the atmosphere of the Ukraine-Russia war. This research is based on the emerging scientific literature on deepfake as well as the publicly available news articles about deepfakes. Within this framework, 43 local and foreign news articles and 78 scientific literature articles were analysed during the research. Four "deepfake documents" on the ongoing war were examined. As a result of the research, written and visual materials and graphics related to deepfake documents were included in the research.

Since 24 February 2022, Russia has been at war with Ukraine on the latter's territory. The ongoing war between Russia and Ukraine has been the conflict taking the highest public attention in Europe since the Second World War. In parallel with the developing and changing technologies of war since the Second World War, it is observed that this war is not only being fought on the battlefield but also in the digital media. As a matter of fact, many video footages created during this war were manipulated and made available to the public. In this context, a large number of videos created with deepfake applications were examined during the research in order to find out whether they contain digital propaganda elements. This study analyzes the use of deepfake applications, which are a new form of digital propaganda, to misinform and manipulate public opinion in the context of the war between Ukraine and Russia.

Deepfake documents, also defined as algorithmic visual and auditory manipulation, have made it possible to provide fake information about individuals to the media against their will. Information that is false in itself can become a tool of disinformation and propaganda in society. This study focuses on wartime propaganda activities and aims to show how deepfake documents are

used for the purpose of digital propaganda. In this respect, this study is important and original as the deepfake documents are used for the first time for propaganda purposes in a war environment as a new version of digital propaganda. This study analyses how and for what purpose deepfake documents were created as a digital propaganda tool during the Ukraine-Russia war. It uses a descriptive approach to examine the struggle of the heads of state and the people of the relevant countries using deepfake documents in the digital environment. Within the framework of this research, four deepfake documents identified through convenience sampling, one of the non-probability sampling methods, were analyzed. As a result, it was found that Ukraine, which was exposed to Russian cyberattacks, warned its people in advance about the potential propaganda based on deepfake documents and quickly launched a counter-attack in return. The findings demonstrated that Ukraine launched counter-attacks using deepfake documents and developed video content intended to discredit Putin in particular.

Factors such as the easy access to deepfake applications via apps installed on phones and the fact that the video creation stages do not require much qualification have enabled more people to produce such content. Originally, the application was used for entertainment purposes, but as technology has advanced, it has become possible to use artificial intelligence to produce fake videos that appear to be genuine, which compromises cybersecurity. Videos can often be manipulated to make it appear as if people did what they did not do and said what they did not say. While these practices offer many advantages and conveniences for some people, they can also lead to irreparable or costly consequences. Content organized for the purposes of intense disinformation and propaganda can sometimes lead to violations of individual rights and sometimes have a devastating impact on diplomatic relations between countries. From a sociological perspective, such practices can lead to a decline in the sense of trust, as they can create the impression of mistrust. Mistrust can become a key element of propaganda in an atmosphere of war. In this context, one may argue that deepfake documents represent a new version of new-generation digital propaganda activities.

In the near future, alongside the development of deepfake applications with the advancement of technology, it may be impossible to tell whether the deepfake video content served is original video content or not. It is necessary to verify the accuracy of the content created with such applications. This is because such content has the potential to negatively affect international diplomatic relations. They can exacerbate conflicts, cast doubt on the legal authenticity of evidence in the form of video content, have irreparable consequences for banking and inheritance transactions, undermine people's trust in the media, provoke "angry public opinion" through propaganda using misinformation, and manipulate elections. In the case of the Ukraine-Russia conflict, it was found that these applications prepared by the two warring countries had no impact on the course of the war, as both sides were prepared and their information infrastructure was sufficient in this respect. Possible propaganda activities could therefore not lead to success.

The study concluded that Ukraine, exposed to cyberattacks by Russia, warned its people in advance about possible propaganda based on deepfake documents, reacted quickly, and launched counter-attacks. It was observed that Ukraine launched counter-attacks using deepfake documents and developed video content primarily aimed at discrediting Putin. Ukraine was only slightly affected by the negative consequences of the deepfake documents it was exposed to, as Ukrainian armed forces had experienced personnel, an advanced IT sector, and has been supported by the West in cyber defense and cyber-attacks.

This research will help organizations, politicians, and the media to verify and assess the accuracy of the information in their fields while conducting research on deepfake documents. Considering

the fact that these applications will be made more realistic and professional with the development of technical possibilities, it is estimated that various studies can be conducted on deepfake documents in the future.

Yazar Bilgileri

Author details

*(Sorumlu Yazar **Corresponding Author**) Atatürk Üniversitesi İletişim Fakültesi, basakavci8@msn.com, Orcid: 0000-0003-4528-2833

**Prof. Dr., Atatürk Üniversitesi İletişim Fakültesi, tascio@atauni.edu.tr, Orcid: 0000-0003-2917-295X

Katkı Oranı

Author Contribution Percentage:

Birinci yazar % 50 First Author % 50

İkinci yazar % 50 Second Author % 50

Destekleyen Kurum/Kuruluşlar **Supporting-Sponsor Institutions or Organizations:**

Herhangi bir kurum/kuruluştan destek alınmamıştır. None

Çıkar Çatışması

Conflict of Interest

Herhangi bir çıkar çatışması bulunmamaktadır. None

Kaynak Göstermek İçin

To Cite This Article

Akmeşe, B. & Taşçıoğlu, R. (2024). Dijital propagandanın yeni bir versiyonu: Ukrayna-Rusya savaşı örneğinde deepfake dokümanlar üzerine bir analiz. *İletişim Kuram ve Araştırma Dergisi*, (66), 116-139. https://doi.org/10.47998/ikad.1339733