



T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GAZETECİLİK ANA BİLİM DALI

**TROL ORDULARI VE DİJİTAL PROPAGANDA: UKRAYNA-RUSYA SAVAŞI
ÖRNEĞİNDE TROL HESAPLARIN ROLÜ VE STRATEJİLERİ**

YÜKSEK LİSANS TEZİ

Uğur DURMAZ

Danışman

Doç. Dr. Nida Sümeyya ÇETİN

MALATYA- 2025

ONUR SÖZÜ

Doç. Dr. Nida Sümeyya Çetin'in danışmanlığında yürütmüş olduğum ***Trol Orduları Ve Dijital Propaganda: Ukrayna-Rusya Savaşı Örneğinde Trol Hesapların Rolü Ve Stratejileri*** başlıklı çalışmamda, bilimsel etik ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını, yararlanılan eserlerin kaynakçada gösterilenler olduğunu, bu eserlere atıf yapılarak yararlanılmış olunduğunu belirtir ve onurumla tasdik ederim.

Uğur DURMAZ

TEŞEKKÜR

Yüksek lisans sürecim boyunca, geçirmiş oldukları deprem felaketine rağmen benimle sabır, samimiyet ve nezaketle ilgilenen başta danışmanım sayın Doç. Dr. Nida Sümeyya Çetin hanımefendi olmak üzere jüri üyelerim Doç. Dr. Dilar Diken Yücel ile Doç. Dr. Hasan Altincik ve eğitimime katkı sağlayan tüm hocalarıma en içten teşekkürü bir borç bilirim. Emektar aileme de teşekkürlerimi sunarken çalışmamı terörle mücadelede kaybettiğimiz aziz şehitlerimizin hatırasına ithaf ederim.



TROL ORDULARI VE DİJİTAL PROPAGANDA: UKRAYNA-RUSYA SAVAŞI ÖRNEĞİNDE TROL HESAPLARIN ROLÜ VE STRATEJİLERİ

ÖZET

21. yüzyılın başlarından itibaren gündelik hayatta yer almaya başlayan dijital teknolojilerin hızlı bir şekilde gelişmesi ve yaygınlaşması, pek çok alanda olduğu gibi propaganda faaliyetlerinde de köklü bir değişime neden olmuştur. Dijital çağ, devletler ve toplumlar arasındaki çatışmalarda yeni bir cephe açmış, sosyal medya platformları ve dijital iletişim araçları propaganda faaliyetlerinin merkezi haline gelmiştir. Bu propaganda faaliyetlerinde, belirli bir amaç ve hedef doğrultusunda genellikle dezenformasyon yaymak, toplumsal algıyı manipüle etmek ve kamuoyunu yönlendirmek amacıyla oluşturulan sahte veya anonim sosyal medya hesapları ciddi bir rol üstlenmektedir. Yaygın kullanımıyla 'trol' olarak anılan bu hesaplar, özellikle kriz ve savaş dönemlerinde propaganda aracı olarak etkin şekilde kullanılmaktadır. 24 Şubat 2022'de Rusya'nın Ukrayna'ya saldırması ile başlayan Ukrayna ve Rusya arasındaki çatışmanın propaganda ayağındaki trol hesaplar oldukça aktif bir rol oynamıştır. Çalışmada, Ukrayna ve Rusya'nın sosyal medyada yürüttükleri, trol hesaplar üzerinden şekillenen dezenformasyon kampanyaları, propaganda ve bilgi savaşları incelenmiştir. Çalışma kapsamında, Rusya-Ukrayna savaşı sırasında aktif olarak kullanılan trol hesapların, X platformundaki paylaşımları içerik analizi yöntemi ile incelenerek, paylaşımlarda kullanılan içerik türleri ve kullanılan dil analiz edilmiştir. Araştırma, iki ülkenin dijital propaganda stratejilerini ve trol hesapların propaganda faaliyetlerinde oynadığı rolü değerlendirerek, modern dönemdeki çatışma ortamlarında, dijital propagandanın da güçlü bir üstünlük aracı haline geldiğini ortaya koymayı amaçlamaktadır. Çalışmada, 1 Ocak 2024 – 1 Ocak 2025 tarihleri arasında paylaşılan 60 adet X (Twitter) paylaşımı, amaçlı örnekleme seçilerek nicel ve nitel içerik analizi metotlarıyla incelenmiştir. Sonuç olarak incelenen trol hesapların farklı ülkeleri destekliyor olmalarına rağmen oransal olarak aynı türden propaganda içeriklerine başvurdukları tespit edilmiştir. Güven zedeleme, korku yaratma ve aşağılama gibi söylemlerin, trol paylaşımlarında sık sık kullanıldığı anlaşılmıştır.

Anahtar Sözcükler: Troller, Dijital Propaganda, Ukrayna, Rusya, Sosyal Medya.

TROLL ARMIES AND DIGITAL PROPAGANDA: THE ROLE AND STRATEGIES OF TROLL ACCOUNTS IN THE CASE OF THE UKRAINE-RUSSIA WAR

ABSTRACT

The rapid development and proliferation of digital technologies, which have started to take place in daily life since the beginning of the 21st century, have caused a radical change in propaganda activities as in many other areas. The digital age has opened a new front in conflicts between states and communities, and social media platforms and digital communication tools have become the center of propaganda activities. In these propaganda activities, fake or anonymous social media accounts, which are generally created to spread disinformation, manipulate social perception and direct public opinion in line with a specific purpose and goal, play a serious role. These accounts, commonly referred to as 'trolls', are effectively used as propaganda tools, especially in times of crisis and war. Troll accounts have played a very active role in the propaganda leg of the conflict between Ukraine and Russia, which began with Russia's attack on Ukraine on February 24, 2022. The study examines the disinformation campaigns, propaganda and information wars carried out by Ukraine and Russia on social media, shaped by troll accounts. Within the scope of the study, the posts of troll accounts actively used during the Russia-Ukraine war on the X platform were examined using the content analysis method, and the types of content and language used in the posts were analyzed. The research aims to evaluate the digital propaganda strategies of the two countries and the role played by troll accounts in propaganda activities, and to reveal that digital propaganda has become a powerful tool of superiority in modern conflict environments. In the study, 60 X (Twitter) posts shared between January 1, 2024 and January 1, 2025 were selected with a purposeful sample and examined using quantitative and qualitative content analysis methods. As a result, it was determined that the troll accounts examined resorted to the same types of propaganda content proportionally, despite supporting different countries. It was understood that discourses such as undermining trust, creating fear and humiliation were frequently used in troll posts.

Keywords: Trolls, Digital Propaganda, Ukraine, Russia, Social Media.

İÇİNDEKİLER

ONUR SÖZÜ.....	ii
TEŞEKKÜR.....	iii
ÖZET.....	iv
ABSTRACT.....	v
İÇİNDEKİLER.....	vi
TABLolar, GRAFİKLER VE GÖRSELLER LİSTESİ.....	x
EKLER.....	xi
GİRİŞ.....	1
BİRİNCİ BÖLÜM.....	5
DİJİTAL PROPAGANDA VE TROLL ORDULARI: KAVRAMSAL VE KURAMSAL ÇERÇEVE.....	5
1.1. PROPAGANDA, TARİHSEL GELİŞİMİ VE DİJİTAL PROPAGANDA KAVRAMI.....	5
1.2. TROL ORDULARI: TANIMI, YAPISI VE İŞLEYİŞİ.....	8
1.2.1.Trol Orduları.....	10
1.2.2.Trol Hesapların Türleri ve Özellikleri.....	12
1.2.2.1. Provokasyon Trolleri.....	13
1.2.2.2. Sosyal Mühendislik Trolleri.....	14
1.2.2.3. Siyasi Troller.....	14
1.2.2.4. Tıklama-Reklam Trolleri.....	15
1.2.2.5. Hiciv, Mizah Ve Alaycı Troller.....	16
1.2.3.Trol Ordularının Organizasyonel Yapısı ve Finansman Kaynakları.....	16
1.2.3.1. Organizasyonel Yapı.....	16
1.2.3.2. Finans Kaynakları.....	18

1.3. BİLGİ SAVAŞLARI VE SİBER OPERASYONLAR.....	19
1.3.1. Bilgi Savaşlarının Uluslararası İlişkilerdeki Yeri.....	20
1.3.2. Siber Operasyonların Askeri ve Siyasi Boyutları.....	22
1.4. DİJİTAL PROPAGANDA VE TROL HESAPLARIN TOPLUMSAL ETKİLERİ.....	24
1.4.1. Kamuoyu Manipülasyonu ve Algı Yönetimi.....	24
1.4.2. Toplumsal Kutuplaşma ve Güven Erozyonu.....	26
1.5. UKRAYNA-RUSYA SAVAŞI'NIN DİJİTAL BOYUTU.....	27
1.5.1. Savaşın Tarihsel ve Politik Arka Planı.....	28
1.5.2. Dijital Propaganda ve Trol Hesapların Savaştaki Rolü.....	29
1.5.2.1. Rusya'nın Dijital Propaganda Stratejileri.....	30
1.5.2.1.1. Devlet Destekli Trol Faaliyetleri.....	31
1.5.2.1.2. Dezenformasyon Kampanyaları.....	32
1.5.2.1.3. Siber Saldırıları ve Bilgi Savaşları.....	33
1.5.2.2. Ukrayna'nın Dijital Karşı Stratejileri.....	35
1.5.2.2.1. Sivil Siber Direniş ve Dijital Aktivizm.....	36
1.5.2.2.2. Doğrulama Platformları ve Karşı-Propaganda Mekanizmalar.....	38
İKİNCİ BÖLÜM.....	40
SOSYAL MEDYADA DİJİTAL PROPAGANDA: TROL FAALİYETLERİ, KAMUOYU ÜZERİNDE ETKİLERİ VE FAALİYETLERE YÖNELİK KARŞI STRATEJİLER.....	40
2.1. SOSYAL MEDYADA TROL ORDULARININ STRATEJİLERİ.....	40
2.1.1. Yapay Kamuoyu (Astroturfing).....	40
2.1.2. Zaman Ve Örgütlenme Açısından Koordineli Saldırıları.....	42

2.1.3. Hashtag Kampanyaları ve Bilgi Kirliliği.....	44
2.1.4. Deepfake ve Manipülatif Görsel İçerikler.....	45
2.1.5. Mizah Üzerinden Yürütülen Faaliyetler.....	46
2.2. ALGORİTMALARIN VE YAPAY ZEKÂNIN ROLÜ.....	48
2.2.1. Sosyal Medya Algoritmalarının Propaganda İle İlişkisi.....	48
2.2.2. Bot Hesapların Tespiti ve Engellenmesi.....	50
2.2.3. Yapay Zekâ Destekli Propaganda Araçları.....	52
2.3. KAMUOYU ALGISI VE TEPKİSİ.....	54
2.3.1. Dijital Propagandanın Toplum Üzerindeki Etkileri.....	54
2.3.2. Kamuoyu Manipülasyonu ve Kutuplaşma.....	56
2.3.3. Bilgi Kirliliğine Karşı Farkındalık Çalışmaları.....	57
ÜÇÜNCÜ BÖLÜM.....	59
UKRAYNA-RUSYA SAVAŞINDA TROL HESAPLARIN ROLÜ VE STRATEJİLERİ.....	59
3.1. ARAŞTIRMANIN AMACI VE ARAŞTIRMA YÖNTEMİ.....	59
3.1.1. İki Aşamalı Akış Teorisi.....	60
3.2. EVREN VE ÖRNEKLEM.....	62
3.3. BULGULAR VE VERİLERİN ANALİZİ.....	63
3.3.1. Nicel İçerik Analizi.....	64
3.3.2. Nitel İçerik Analizi.....	70
3.3.2.1. Rusya Yanlısı @Blackdiammon Paylaşımlarının Nitel İçerik Analizi.....	70
3.3.2.2. Rusya Yanlısı @Alex_Oloyede2 Paylaşımlarının Nitel İçerik Analizi.....	73
3.3.2.3. Rusya Yanlısı @GeromanAT Paylaşımlarının Nitel İçerik Analizi.....	76

3.3.2.4. Ukrayna Yanlısı @Maks_NAFO_FELLA Paylaşımlarının Nitel İçerik Analizi.....	77
3.3.2.5. Ukrayna Yanlısı @Heroiam_Slava Paylaşımlarının Nitel İçerik Analizi....	79
3.3.2.6. Ukrayna Yanlısı @GloOuD Paylaşımlarının Nitel İçerik Analizi.....	81
3.4. TARTIŞMA.....	84
SONUÇ VE ÖNERİLER.....	89
KAYNAKÇA.....	93
İNCELENEN PAYLAŞIMLARIN İNTERNET ADRESLERİ.....	108



TABLÖLAR, GRAFİKLER VE GÖRSELLER LİSTESİ

Tablo 1.....	64
Tablo 2.....	65
Tablo 3.....	66
Tablo 4.....	67
Tablo 5.....	68
Tablo 6.....	69
Tablo 7.....	84
Tablo 8.....	86
Grafik 1.....	84
Grafik 2.....	85
Grafik 3.....	86
Grafik 4.....	86
Görsel 1.....	70
Görsel 2.....	71
Görsel 3.....	72
Görsel 4.....	73
Görsel 5.....	73
Görsel 6.....	74
Görsel 7.....	75
Görsel 8.....	76
Görsel 9.....	77
Görsel 10.....	77
Görsel 11.....	78
Görsel 12.....	79
Görsel 13.....	79
Görsel 14.....	80
Görsel 15.....	81
Görsel 16.....	81

Görsel 17.....	82
Görsel 18.....	83

EKLER

EK-1.....	112
EK-2.....	116
EK-3.....	121
EK-4.....	125
EK-5.....	130
EK-6.....	135

GİRİŞ

21. yüzyılın başlarından itibaren dijital teknolojilerin hızlı bir şekilde gelişmesi, insan yaşamının her alanını ciddi şekilde değiştirmiştir. Özellikle internet teknolojisinin ortaya çıkışı ve hızla yaygınlaşması ve sosyal medya platformlarının popülerleşmesi, küresel ölçekte bilgi akışını hızlandırarak kitleler ve farklı toplumlar arasındaki iletişimi büyük ölçüde etkilemiştir.

Günümüzde enformasyona erişim ve yayılım süreçlerinin eskisine göre çok daha hızlı, yaygın ve çeşitli olması da toplumda ciddi değişimlere sebep olmuştur. Bu durum, yalnızca sivil kitleler arasında değil, devletler ve diğer aktörler arasında da yeni fırsatlar ve meydan okumalar yaratmıştır. Özellikle savaş ve çatışma durumlarında dijital teknolojiler, geleneksel propaganda araçlarının ötesine geçerek dijital propagandanın ve dolaylı olarak siber savaşın etkili birer unsuru haline gelmiştir (Arslan & Ebre, 2021, s. 4). Toplumsal boyutta bu durum, propagandanın yayılım alanını genişletmiş ve manipölasyon yönünü kuvvetlendirmiştir.

Son dönemde yaşanan gelişmelerle birlikte dijital dünyanın en önemli kavramlardan biri haline gelen siber savaş, fiziksel savaşın yerini alan veya ona ek yürütölen bir çatışma biçimi olarak bilgi ve iletişim teknolojilerini stratejik bir silah olarak kullanmaktadır. Devletler ve örgütler, siber saldırılar yoluyla kritik altyapılara zarar verebilmekte, düşmanlarını dijital kabiliyet olarak zayıflatılabilmekte ve bilgi sistemlerine sızarak rakiplerine karşı üstünlük kurabilmektedir. Bu yeni nesil savaş yöntemi, yalnızca teknik açıdan değil, psikolojik ve politik açıdan da etkili bir silah olarak kabul edilmektedir. Siber savaşın en önemli bileşenlerinden biri ise dijital propagandadır. İçinde bulunduğumuz modern çağda bilgi, en güçlü savaş araçlarından biri haline gelmiştir ve dijital propaganda, hedef kitlelere yanlış bilgi yayarak ya da bilgiyi manipöl ederek kamuoyunu etkilemeyi amaçlamaktadır. Bu süreçte, özellikle sosyal medya platformları üzerinden kasıtlı olarak yayılan yanlış haberler ve dezenformasyon; hedef toplumları bölmek, kutuplaştırmak ve karşı tarafın itibarını zedelemek için kullanılmaktadır (Sepili, 2020, s. 100). Bu durum ise dijital propagandayı tüm yönleri ile anlamayı ve stratejileri yorumlamayı zorunlu kılmaktadır.

Dijital propaganda kavramı, internetin ve dijital teknolojilerin yaygınlaşmasıyla birlikte şekillenen bir kavramdır. İnternetin, özellikle web 2.0 teknolojisinin 2000'li yılların başında ortaya çıkışıyla birlikte dijital medya araçları ve sosyal medya platformları propaganda amaçlı kullanılmaya başlanmıştır. Bu gelişme, bilgi akışının hızlanması ve kitlelerle doğrudan iletişim kurulabilmesi sayesinde, propagandanın dijital ortamlarda daha etkin ve geniş kitlelere ulaşacak şekilde yapılmasına olanak tanımıştır. Dijital propaganda, geleneksel medyanın sınırlı erişim ve tek yönlü iletişim yapısını aşarak, geniş kitlelere anlık ve çift yönlü bir etkileşim imkânı sunmaktadır. Bu süreç propagandayı, yalnızca devletlerin veya 'kanaat önderlerinin' tekeline bırakan bir yapıdan çıkararak bireylerin, örgütlerin ve tüm sosyal medya kullanıcılarının da etkin bir aktör haline gelmesine yol açmıştır.

Siber uzaydaki propaganda akışının kitleler üzerindeki etkileri de kuşkusuz büyük ve güçlü olmaktadır (Şenkardeş, 2023, s. 150). Dünya üzerindeki sıcak çatışma bölgeleri mercek altına alındığında dijital propagandanın, çatışmaların tarafları arasında oldukça ilgi gördüğü ve aktif şekilde bir savaş aracı olarak kullanıldığı görülmektedir. Özellikle Rusya-Ukrayna savaşı, bu yeni nesil savaşın ve dijital propaganda yöntemlerinin en çarpıcı örneklerinden biri olarak karşımıza çıkmaktadır. 2022 yılında Rusya'nın Ukrayna'ya başlattığı saldırı, savaşın sadece fiziksel alanlarda değil, aynı zamanda dijital ve psikolojik alanlarda da sürdüğünü açıkça ortaya koymuştur. Rusya, siber saldırılar ve dijital propaganda yoluyla Ukrayna'nın altyapısına zarar vermek ve halkın moralini bozmak amacıyla çeşitli stratejiler uygulamıştır. Rusya'nın dezenformasyon kampanyaları, Ukrayna halkının güvenini sarsmayı ve uluslararası kamuoyunu yanıltmayı hedeflemiştir. Özellikle sosyal medya platformları üzerinden yayılan sahte haberler, kamuoyunu yanıltmak ve karşı tarafa yönelik algıyı değiştirmek için etkili bir araç olarak kullanılmıştır (Paltacı, 2022, s. 12). Ukrayna ise bu süreçte sosyal medya kampanyaları ile dünya kamuoyuna sesini duyurmuş, Rusya'nın saldırılarını ve işgallerini uluslararası toplum nezdinde kınamaya yönelik bir strateji izlemiştir. Ukrayna Devlet Başkanı Volodimir Zelenski, bu süreçte sosyal medyanın etkin kullanımını hem Ukrayna halkını birleştirmek hem de dünya liderlerini harekete geçirmek amacıyla kullanmıştır. Ukrayna'nın sosyal medya stratejisi, savaşın psikolojik boyutunda önemli bir zafer olarak değerlendirilmiştir. Zelenski'nin Twitter ve Instagram gibi platformlar

üzerinden yaptığı paylaşımlar, dünya kamuoyunu Ukrayna'nın yanında yer almaya teşvik etmiştir (Bayram, 2022, s. 81).

Dijital propagandanın önemli bir unsuru olup dezenformasyon kampanyalarının ve bilgi savaşlarının merkezinde yer alan trol hesaplar da sosyal araştırmalara ciddi şekilde konu olmaya başlamıştır. Trol hesapların kökenleri, internetin ilk yıllarına, özellikle 1990'ların başında çevrimiçi forumlar ve haber gruplarına kadar uzanmaktadır. 'Trol' terimi, internet kültüründe başlangıçta, bir tartışma ortamında kasten karışıklık yaratmak amacıyla yanıltıcı veya saldırgan mesajlar gönderen kullanıcıları tanımlamak için kullanılmıştır (Mercimek vd., 2015, s. 70). Bu dönemde trollük, daha çok bireysel ve eğlence amaçlı bir eylemken; 2000'lerin başından itibaren sosyal medya platformlarının yaygınlaşmasıyla birlikte, trol hesaplar daha organize ve etkili bir dijital manipülasyon aracı haline gelmiştir. 2010'lu yıllardan sonra ise özellikle devlet destekli trol faaliyetleri ve 'trol orduları' dikkat çekmeye başlamıştır. Bu hesaplar, kriz ve savaş anlarında devreye sokularak, propaganda faaliyetlerinin etkisini artırmakta ve bilgi operasyonlarının etkinliğini sağlamaktadır. Ukrayna ve Rusya arasında 2014 yılında Kırım'ın ilhakı ve Donbas bölgesindeki çatışmalarla başlayan ve 2022 yılında geniş çaplı bir askeri saldırı ile yeni bir aşamaya evrilen kriz, dijital propagandanın ve trol faaliyetlerinin etkin bir şekilde kullanıldığı bir örnek olarak dikkat çekmektedir (Uyaniker, 2018, s. 142). Özellikle Rusya, trol fabrikaları olarak bilinen yapılar aracılığıyla, sosyal medyada geniş çaplı dezenformasyon ve manipülasyon kampanyaları yürütmektedir. Bu trol fabrikalarının en bilinen örneklerinden biri olarak Internet Research Agency (IRA) gösterilmekte, dijital propaganda ve trol hesapların organizasyonunda merkezi bir rol oynadığı iddia edilmektedir. Rusya'nın bu yapılar aracılığıyla Twitter ve Facebook gibi platformlarda yaydığı içerikler, Ukrayna'daki çatışmanın algısını uluslararası kamuoyu nezdinde şekillendirmeyi hedeflemektedir. Ukrayna ise, Rusya'nın bu dijital saldırılarına karşı dijital savunma ve karşı-propaganda stratejileri geliştirmiştir. Özellikle Ukrayna'nın sosyal medya kampanyaları ve siber savunma operasyonları, dijital savaşın iki yönlü ve dinamik bir yapıda sürdüğünü göstermektedir. Ukrayna, sosyal medya platformlarını etkili bir şekilde kullanarak uluslararası kamuoyunu mobilize etmeye, yaşanan gelişmeler hakkında bilgi yaymaya ve kendi halkının moralini yüksek tutmaya çalışmıştır (Silverman & Kao, 2022).

Rusya-Ukrayna savaşı süresince, her iki taraf da kamuoyunu yönlendirmek, kendi stratejilerini ve politikalarını meşrulaştırmak ve karşı tarafı itibarsızlaştırmak amacıyla dijital propagandayı ve siber teknolojileri etkin biçimde kullanmıştır. Sosyal medya, özellikle savaşın gidişatını etkileyen önemli bir propaganda aracı haline gelmiş, bu platformlar üzerinden yayılan haberler ve görseller, savaşın psikolojik, stratejik ve politik boyutlarını güçlendirmiştir (Akmeşe & Taşcıoğlu , 2024, s. 125-126). Sosyal medya üzerinden yayılan bilgi ve dezenformasyonun yayılma hızı, geleneksel medya araçlarına göre çok daha hızlıdır. Bu nedenle, savaş esnasında kamuoyunun yönlendirilmesi ve düşman tarafların psikolojik olarak zayıflatılması gibi stratejilerde, dijital platformlar kilit bir rol oynamaktadır. Sosyal medyada yayılan görüntüler, açıklamalar ve yorumlar, yalnızca ülkeler arası rekabetin değil, aynı zamanda bireylerin algı savaşının da bir parçası olmuştur.

Rusya-Ukrayna savaşında, sosyal medya üzerinden yürütülen dijital propaganda faaliyetlerinin incelenmesi ve dijital propaganda faaliyetlerinin ciddi bir öznesi olan sosyal medya trolleri hakkında çıkarımlarda bulunulması, çalışmanın ana amacını oluşturmaktadır. Yapılan incelemelerle, sosyal medya trollerine dair elde edilen bulgular sayesinde literatüre katkı yapmak hedeflenmektedir. Belirtilen hedef doğrultusunda, nitel araştırma yöntemlerinden birisi olan içerik analizi yöntemi kullanılarak X paylaşımlarında tespit edilen ifadeler ve materyaller, düşünce kalıpları ve propaganda stratejileri yorumlanmıştır.

BİRİNCİ BÖLÜM

DİJİTAL PROPAGANDA VE TROLL ORDULARI: KAVRAMSAL VE KURAMSAL ÇERÇEVE

Günümüzün değişen ve gelişen teknolojilerinin bir sonucu olarak propaganda kavramı da dönüşüme uğramış, geleneksel yapısının ötesine geçerek dijital bir hal almıştır. Bu süreç içerisinde propaganda üretimi de iletişim araçlarını elinde bulunduran küçük bir kesimin tekelinden kurtularak, kamuoyunun çok ciddi bir bölümü tarafından üretilip yayılabilir duruma gelmiştir. Yaşanan gelişmeler, daha demokratik bir toplumun zeminini hazırlamak için etkili bir fırsat olarak görülse de beraberinde pek çok etik tartışmayı da getirmiştir.

1.1. Propaganda, Tarihsel Gelişimi ve Dijital Propaganda Kavramı

Siyasi ve toplumsal söylemlerde genişçe yer bulan ‘propaganda’ terimi, antik çağlardan günümüze kadar binlerce yıllık bir tarihe sahip önemli kavramlardandır. Propaganda, özü gereği insanların davranışlarını ve tutumlarını etkilemek maksadıyla sistematik şekilde yayılan bilgi, fikir veya görüşlerden oluşmaktadır. Kavramın kendisi, Latince’de ‘yeni fidanlar dikmek’, ‘yeni bilgiler üretmek ve yaymak’ anlamına gelen ‘propagare’ kökünden oluşmuştur (Qualter, 1980, s. 257). Sadece bu etimolojik bilgi bile propagandanın ‘üretmek’ ve ‘yaymak’ üzerine kurulu olduğunu açıklamaktadır. Genellikle olumsuz çağrışımlarla ilişkilendirilse de propagandanın hem iyi niyetli hem de kötü niyetli pek çok amaç için kullanılabileceğini belirtmek önemlidir. Gerçekleştirilenlere yarar sağlaması için genel olarak duygusal çağrılar, manipülasyonlar ve etkili hitabet gibi tekniklerle hedef üzerine yönlendirilen propagandalar, birçok biçimde sunulabilmektedir. Yazılı materyaller, konuşmalar, filmler ve sanat eserleri, modern çağdaki sosyal medya içerikleri, propagandayı sunum biçimlerinin başlıcalarındandır (Karakuş, 2021, s. 464-466).

Antik medeniyetlere kadar uzanan kullanımıyla propaganda, ilk olarak Antik Mısır’daki firavunların, diktirdikleri hiyeroglif anıtlarda göze çarpmaktadır. Yönetim haklarını ilahi varlıklardan aldıklarını iddia eden firavunlar, bu iddialarını Mısır halkı karşısında sürekli dile getirmişlerdir. Firavuna ait söylemleri güçlendirmek ve saltanatını meşrulaştırarak kalıcı kılmak için bu dönemde yaptırılan, bugün bile dünya harikası

sayılan anıtsal yapıtlar ve sanat eserleri propagandanın ilk örneklerindendir. Yine önemli antik medeniyetlerden olan Yunan ve Roma kültürlerinde ise propaganda, günümüzdeki kullanımına daha yakın biçimde retorik ve hitabetler aracılığıyla yapılmıştır. Özellikle, mübalağalar kullanarak duygulara hitap eden hatipler ve şairler, kamuoyunu şekillendirmede önemli bir rol oynamıştır. Demosthenes ve Cicero gibi hatipler, bu dönemdeki önemli ‘propaganda üreticileri’dir (Gürgen, 1990, s. 136). Türk kültürüne ait keşfedilen ilk propaganda metinleri ise Orhun Kitabeleri olarak karşımıza çıkmaktadır. MS. 8. yüzyılın başlarına dayandığı düşünülen bu kitabelerdeki metinler, bugün dahi Türkleri manevi olarak etkilemektedir.

Orta Çağ’a gelindiğinde ise bu dönem boyunca devletleri etkisi altına alan, dogmatik düşünceler, mezhepsel ve dinsel söylemler, temel propaganda materyallerini oluşturmuştur. Avrupa özelinde bakıldığında zaman karanlık bir dönem olarak tarihe geçen Orta Çağ’da, din adamlarının kendi tekelinde olan halka karşı dini bir propaganda aracı olarak aktif şekilde kullandıkları görülmektedir. Orta Çağ’da başlayan Haçlı Seferleri’nin de ana propaganda kaynağını dini öğeler oluşturmaktadır. Keza bu dönemde Haçlı Seferleri’ne karşı koymak isteyen İslam dünyası da yine ‘din için yapılan savaş ve cihat’ vurguları ile Müslüman halka yönelik aktif bir propaganda yürütmüşlerdir. Avrupa açısından ‘aydınlanma çağı’ olarak nitelendirilen Rönesans dönemi ve reform hareketlerinde ise propaganda açısından tarihi bir gelişme yaşanmıştır. Johannes Gutenberg’in 15. yüzyılın ortalarında matbaayı icat etmesi, bilgi ve fikirlerin yayılmasını kökten değiştirerek yeni bir dönemin kapılarını aralamıştır. Bu teknolojik ilerleme, kitapların, broşürlerin ve gazetelerin seri üretimine olanak tanıyarak propagandanın yayılımını ve dolayısıyla etkilerini önemli ölçüde artırmıştır (Qualter, 1980, s. 257-261).

‘Tüm savaşları bitirecek’ denilen Birinci Dünya Savaşı patlak verdiğinde, propaganda tarihinde yeni ve ciddi bir dönüm noktası başlamıştır. Bu dönemde hükümetler, içeride morali korumak ve düşmanı demoralize etmek için özel propaganda ajansları kurmuşlardır. Savaş bittikten sonra Anadolu’nun kurtuluşu için verilen milli mücadelede Mustafa Kemal Atatürk’ün talimatıyla kurulan Anadolu Ajansı da aslında propaganda üretmek ve düşman ülkeler tarafından yapılan dezenformasyonları önleyerek halka doğru bilgi ulaştırmak amacıyla kurulmuştur (Çağlak, 2023, s. 2903). Yine Birinci Dünya Savaşı döneminde basılı materyaller ana propaganda araçları olarak karşımıza çıkmaktadır. İkinci Dünya Savaşı dönemine gelindiğinde ise görece daha da dijitalleşen

dünyada basılı materyallere kıyasla radyo, bu dönemin ana propaganda aracı olmuştur. Bu dönemde ülke sınırlarına konuşlandırılmış devasa hoparlör sistemleri ve siyah-beyaz sinema filmleri de kamuoyunu etkilemede oldukça başarılı olan propaganda araçları olmuştur. Propagandanın kitleler üzerindeki etkilerinin en net şekilde görüldüğü İkinci Dünya Savaşı yıllarında propaganda bakanlıkları ve bilgi yayma merkezleri dahi kurulmuştur. Bu dönemin en etkili propaganda mekanizması Nazi rejimi yönetimindeki Almanya'da işlemiştir (Çakı, 2018, s. 64). Günümüz dünyasında uygulanan propaganda faaliyetlerin, Nazi Almanya'sında yaygın olarak kullanılmış olan propaganda çalışmalarından yola çıkarak geliştirilmiş olduğu söylenebilir.

Teknolojik gelişmelerin ve kısmi çatışmaların eşliğinde Soğuk Savaş dönemi başladığında propaganda, Amerika Birleşik Devletleri ile Sovyetler Birliği arasındaki ideolojik savaşta önemli bir silah haline gelmiştir. Her iki süper güç de kendi ideolojilerini tanıtmak ve rakiplerini itibarsızlaştırmak için radyo, film ve edebiyat gibi çeşitli medya araçlarını kullanmıştır. Ayrıca her iki ulus da uzay araştırmalarını, genel teknolojik üstünlüklerini ve ideolojik başarılarını propaganda olarak aktif biçimde kullanmıştır. 21. yüzyılın başlarından itibaren teknoloji dünyasında yaşanan dijital devrim ve internetin yükselişi ise propagandayı daha önce hiç görülmemiş bir değişime uğratarak kavram için yepyeni bir dönemin başlangıcı olmuştur. Bu dönemde almış olduğu biçim ile geleneksel muadillerine göre daha yaygın ve karşı konulması daha zor bir duruma gelen propaganda, hayatın her alanında varlığını göstermeye başlamıştır (Balel, 2024, s. 42). Çevrimiçi platformlar bu noktada taşıyıcı ve yayıcı konumda rol almışlardır.

Çevrimiçi platformların ve sosyal medyanın yaygınlaşması, bilginin yayılma biçimini yeniden şekillendirmiş ve doğal olarak propaganda alanında da köklü değişikliklere sebep olmuştur. Gazetelere, basılı yayınlara, televizyona ve radyoya dayanan geleneksel propaganda biçimlerinin aksine, 21. yüzyılın başlarından itibaren günlük hayata giren dijital medya araçlarının bir sonucu olarak propaganda benzeri görülmemiş bir hızda üretilip yayılır hale gelmiştir. Bu hızlı dağıtım sürecine paralel olarak kitleler üzerinde etkisi de artan propagandanın aynı ölçüde karmaşıklığı da artmış, küresel ölçekte siyasi manzaraları, toplumsal hareketleri ve kamu algısını etkilemiştir (Özer, 2019, s. 18). Belli güç erklerinin tekelinden alınarak, dijital medya araçlarına sahip olan herkesin üretebileceği bir konuma erişen propaganda, her zamankinden daha çok demokrasiye ve toplumsal hak arayışlarına hizmet etmiş fakat bir o kadar da kamuoyu aleyhine

dezenformasyonlar ve bilgi manipölasyonlarının üretilmesini sağlamaya aracı olmuştur. Özellikle sosyal medya sistemlerine entegre yapay zekânın önü alınamayan yükselişi ile birlikte propagandanın gelecekteki durumu çok daha öngörülemez bir hal almaktadır.

1.2. Trol Orduları: Tanımı, Yapısı ve İşleyişi

21. yüzyılın başlarından itibaren, bireylerin ihtiyaç ve taleplerine göre şekillenen iletişim ve haberleşme teknolojileri sayesinde, insanlar artık çok daha geniş kitlelerle iletişim kurabilmekte, kendi iletilerini aktarabilmekte ya da başka iletilere rahatça erişebilmektedirler. Özellikle mobil cihazların ve akıllı telefonların yaygınlaşması ile internete erişimin oldukça kolay bir hale gelmesi, bilgiye erişim noktasında zaman ve maliyet açısından ciddi imkanlar sağlarken; içerik çeşitliliği, dağıtım ve erişim kolaylığı gibi avantajlar, sosyal medyanın bir kitle iletişim aracı olarak kullanılmasına zemin hazırlamıştır. İletişim tarihinin insanlık kadar eskiye dayandığı göz önüne alındığında, sosyal medya ağlarının son derece kısa bir sürede yaygınlaşması, geleneksel medyaya bambaşka bir boyut kazandırmıştır (Sönmezer & Büyükbaykal, 2024, s. 758). Sosyal medyadaki temel mantık, kullanıcıların oluşturdukları kişisel profiller aracılığıyla diğer kullanıcılar ya da diğer kullanıcılar tarafından oluşturulan içerikler ile etkileşime girebilmeleridir. Bu etkileşim bireylerin bilgi edinme, sosyalleşme ya da kendini geliştirme gibi ihtiyaçlarını karşılamak amacıyla yapılır ve günümüz dünyasında oldukça yaygındır.

Dünya çapında pek çok sivil toplum kuruluşuna ve yarı resmi kuruma hizmet veren araştırma şirketi Statista'nın yapmış olduğu bir araştırma, sosyal medyanın dünya üzerindeki yaygınlığını gözler önüne sermektedir. Statista'nın 2025 yılı Şubat ayında yaptığı bir araştırmaya göre küresel çapta internet kullanıcısı olan kişi sayısı 5,56 milyarı bulurken; sosyal medya kullanan kişi sayısı ise 5,24 milyara dayanmaktadır. Aynı veriler ışığında dünya nüfusunun yüzde 67,9'u interneti kullanırken; dünya nüfusunun yüzde 63,9'unun ise sosyal medya kullanıcısı olduğu görülmektedir (Petrosyan, 2025). Sosyal medyanın böylesine geniş bir kullanım kitlesinin bulunması, söz konusu mecraayı kötü emeller doğrultusunda kullanıma da açık hale getirmektedir. Siber zorbalık, yasadışı faaliyetler ve görüşmeler, dezenformasyon üretmek ve yaymak, fikri mülkiyet gibi alanlarda yapılan hırsızlıklar, nefret söylemi, trolleme ve taciz bu kötü emellerden bazılarıdır.

Sosyal medya alanını art niyet doğrultusunda kullanma hususunda, günümüzde en çok dikkati çeken kavramlardan birisi ‘trolleme’ kavramıdır. Trolleme, sosyal medyada açılan hesaplar aracılığıyla, şaka, şüphe uyandırma ya da tartışma yaratma gibi yöntemlerle insanları etkileme biçimidir. ‘Trollenen’ bireyler eğlendirilip düşünmeye sevk edilebilecekleri gibi ironik ifadelerle rahatsız edilerek, yanıltılarak ve hedef gösterilerek de bu deneyimi yaşayabilirler (Anadolu Ajansı, 2023).

“Trolleme” kavramının kökeni, internet öncesi döneme kadar uzansa da bugünkü anlamıyla ilk ortaya çıkışı 1990’lı yılların başına, internet forumlarının ve özellikle ilk çevrim içi tartışma platformlarının kullanımına dayanmaktadır. Bu forumlarda, kullanıcıları ‘trolleyen’ diğer kullanıcılara ise ‘trol’ adı verilmiştir. ‘Trol’ adı, yalnızca sosyal medya platformlarının gelişmesiyle birlikte günlük hayatta kullanılan bir tanım değildir; kavramın tarihi mitolojiye kadar uzanmaktadır. Kelimenin kökeni, İskandinav mitolojisindeki ‘insana benzeyen, kötü niyetli, aldatıcı, hain ve büyülü’ varlıklara dayanmaktadır (Wilbur, 1958). İskandinav mitolojisine göre troller, iyi insanlara kötülük yapmak üzere yaratılmış, yeryüzüne çıkmadan mağaraların karanlık derinliklerinde büyü ve benzeri işlerle uğraşan varlıklardır. Kült haline gelmiş eserleriyle tanınan yazar John Ronald Reuel Tolkien de İskandinav mitolojisinden esinlendiği trolleri kurgusal karakterler olarak eserlerine taşımış ve onları güneş ışığı gördüğü zaman taşa dönüşen varlıklar olarak tasvir etmiştir. Günümüzdeki kullanımı ise daha ziyade sosyal medya alanına indirgenmiş olup, sahte kimlikler ile profiller oluşturan ve belli art niyetler doğrultusunda faaliyetler yürüten kişiler ‘trol’ olarak nitelendirilmektedir.

Eski mit anlatılarından yola çıkarak bugünkü sosyal medya trolleri arasında bağlar kurmak mümkündür. Sosyal medya trolleri, hedef aldıkları kullanıcılara ya da gruplara kötülük yapmak için kendi gerçek kimliklerini açık etmeyerek ‘karanlıkta’ durmakta ve belirlenen amaç kapsamında dijital saldırıya hazır halde beklemektedirler. Troller, çevrim içi tartışma gruplarında, herhangi bir somut kanıta dayanmayan iddialarla diğer üyelerle etkileşime girerek tartışma yaratır ya da mevcut tartışmaları amacından saptırarak, grubun dikkatini dağıtırlar, insanları rahatsız ederek kışkırtmaya çalışırlar. Bunlar, konuşulan konularla doğrudan ilgisi olmayan, yalnızca diğer katılımcılara hakaret etmek ve onları küçük düşürmek amacıyla mesajlar paylaşan kişilerdir. Trollük, çoğu zaman çevrimiçi bir diğer olumsuz davranış biçimi olan siber zorbalıkla karıştırılsa da ikisi farklı kavramlardır. Karışıklık yaratma ya da aldatmaya dayalı hareketler trolleme ile

ilişkilendirilirken, siber zorbalık bu özelliklerle tanımlanamaz. Her iki durumda da saldırınlık söz konusudur fakat siber zorbalık daha farklı bir karaktere sahiptir. Siber zorbalıkta failer çoğunlukla mağdurlarını gerçek hayatta tanır ve zarar verici eylemler genellikle belirli kişilere doğrudan yöneltilir (Kayaduman, 2020, s. 4). Trollerin davranışları göz önüne alındığında, trol kullanıcıların kişisel olarak kendilerini zeki, üstün ya da eğlenceli göstermek istedikleri ve başkalarının kafasını karıştırarak, sinirlendirerek kendilerini tatmin ettikleri anlaşılmaktadır. Bazı araştırmalar, yoğun trol davranışı gösteren bireylerin yüksek düzeyde psikopatik eğilimler, empati yoksunluğu, pişmanlık duymama gibi özellikler taşıyabileceğini göstermiştir (Yetkin, 2019, s. 61). Fakat sosyal medyanın sağladığı olanaklar sayesinde gizlice, serbestçe ve oldukça etkili biçimde hareket eden bu trol kullanıcılar, kısa zamanda resmi ya da resmi olmayan oluşumlar tarafından da kullanılmaya başlanmıştır. Keyif alma ve şahsi amaçlar için bireysel olarak yapılan trollük faaliyetleri artık belli kesimlerin amaçları için sistematik ve büyük gruplar halinde yürütölmeye başlanmıştır.

1.2.1. Trol Orduları

Sosyal medyadaki trol kullanıcıların yürüttüğü faaliyetler, hükümetlerin, bazı örgütlerin ve istihbarat servislerinin de dikkatini çekmiştir. ‘Kamuoyu desteğini almadan ayakta duramayacakları’ gerçeğinden hareketle kitlelere hâkim olma çabası ve algıyı yönetme istekleri olan bu oluşumlar, iletişim teknolojilerindeki gelişmeleri takip ederek kitleleri şekillendirmek için stratejiler geliştirmektedirler. Bu doğrultuda geleneksel medyanın, yerini büyük ölçüde sosyal medyaya bırakması ile birlikte mecra değişikliğine giden resmi ya da sivil grup ve oluşumlar, ‘piyon’ değişikliğine de giderek sosyal medyada trol orduları kurmaya başlamışlardır (Yetkin, 2019, s. 52). 'Trol orduları', belli kişi ya da gruplar hakkında yalan haber yaymaktan, belirli bir tarafı desteklemeye veya iftira atmaya kadar, sistematik şekilde çalışan, çok sayıda sahte sosyal medya hesabı ve bu hesapları yöneten ‘klavye savaşçıları’ olarak tanımlanabilir. Sıradan trol bireylere kıyasla trol orduları, genelde belli bir ücret karşılığında çalışan ve sayıları zaman zaman on binler ile ifade edilen yapılardır.

Kamuoyunu şekillendirme ve onu istenilen yönde ikna etme çabaları, geleneksel medyanın hakim olduğu dönemlerde radyo, televizyon, gazete ve basılı materyaller gibi iletişim araçları ile sağlanmış, dolayısıyla günümüze kıyasla ciddi ölçüde sınırlı bir etki

bırakmıştır. Bu dönemde belli çıkar grupları ile anlaşmalar sağlanarak, bazı kanaat önderleri ile bağlantı kurularak veya resmi propaganda kanalları aracılığıyla algı yönetimi faaliyetleri sürdürülmüştür. Fakat sosyal medyanın günlük yaşamda aktif şekilde kullanılması ile birlikte tek elden yönetilebilen ve oldukça ucuza mal olan sistematik trol orduları, resmi ya da sivil olarak algı yönetimi yapan oluşumların bir numaralı tercihi haline gelmiştir (Mercimek vd., 2015, s. 70).

Dünya üzerinde her ülkede görülebilecek trol ordularının ilk örneklerinin Rusya’da ortaya çıktığı söylenebilir. Rusya, 2003 yılına kadar uzanan ve kamuoyunda ‘trol fabrikaları’ ya da ‘trol çiftlikleri’ olarak bilinen yapılar aracılığıyla dijital propaganda çalışmaları yürütmüştür. Bu faaliyetler, özellikle 2014 yılında Kırım’ın ilhakı sürecinde ve sonrasında daha görünür hale gelmiştir. Özellikle Rus devlet kurumları tarafından açıkça istihdam edilen trol orduları, Kremlin’in çıkarları doğrultusunda ülkedeki siyasi gündemi şekillendirmek için sosyal medyada aktif olarak yorum yapmakta ve içerik yayınlamaktadırlar (Yetkin, 2019, s. 65). St. Petersburg merkezli İnternet Araştırma Ajansı (Internet Research Agency-IRA), Rus trol ordusunun en iyi belgelenmiş örneklerinden birisidir. 2013 yılında kurulan IRA, hem yerel hem de uluslararası kitleleri etkilemeyi amaçlayan bir dizi faaliyette bulunmuştur. Ajans, sahte sosyal medya hesapları oluşturan, yanıltıcı içerikler üreten ve Facebook, Twitter ve Instagram dahil olmak üzere çeşitli sosyal medya platformlarında koordineli kampanyalar yürüten çok sayıda kişiyi istihdam etmektedir. IRA’nın faaliyetlerinin ardındaki temel motivasyon, ulusal ve uluslararası arenadaki siyasi söylemi Rusya’nın çıkarları lehine şekillendirmektir. Bu doğrultuda Rus jeopolitik hedefleriyle uyumlu olan siyasi adayların veya anlatıların parlatılması, Batılı ülkeler tarafından yayımlanan çeşitli rapor, iddia ve kampanyalara yönelik düşmanlığın körüklenmesi gibi birtakım faaliyetler IRA tarafından aktif biçimde yürütülmektedir. IRA genellikle hedef ülkelerdeki ya da gruplardaki sosyal bölünmeleri, fikir ayrılıklarını istismar etmeye çalışarak ırk, göç ve ulusal kimlik gibi tartışmalı konuları büyütür. Ajans, taraflar arasında troller vasıtasıyla kasıtlı olarak anlaşmazlıklar yaratarak toplumsal uyumu zayıflatmayı ve kurumlara olan güveni baltalamayı amaçlar. Trol ordularının aktif biçimde kullanımı sayesinde, geleneksel olmayan dijital algı yönetimi taktiklerini kullanarak stratejik hedeflere askeri çatışma olmadan ulaşmak amaçlanır. Bu da aslında Rusya’nın hibrit savaş stratejilerinden birisidir (Mueller, 2019, s. 22-26).

Çin Halk Cumhuriyeti'nde de sayıları 500 bin ila 2 milyon arasında değiştiği iddia edilen '50 Cent Army' takma adlı bir trol ordusunun varlığından söz edilmektedir. Hükümet tarafından finanse edilen bu yapının, isimlerini, kendilerine ödenen 50 Cent'lik paradan aldıkları iddia edilmektedir. '50 Cent Partisi' adıyla da anılan bu yapı hakkında pek çok akademisyen, gazeteci ve aktivist, sosyal medyadaki politik tartışmalarda Çin hükümetini savunarak algı yaratmaya çalıştıklarını belirtmektedir. Nisan 2017'de yayımlanan bir Harvard araştırmasına göre bu trol ağının tamamı mükemmel biçimde koordine edilmiş gerçek insanlardan oluşmaktadır, incelemelerde 'bot hesap' izine rastlanmamıştır (King vd., 2017, s. 484-485). Çin'in son yıllarda yapay zekâya yönelik yatırımları ve dijital atılımları göz önünde tutulduğu zaman böyle bir trol ağının varlığı ciddi bir iddiadır. Sayıları bu denli çok olan bir yapı ile sosyal medya platformlarında çok hızlı bir şekilde gündem oluşturabilir ya da mevcut gündem değiştirilebilir.

Çin ve Rusya gibi ülkelerin yanı sıra Suudi Arabistan'da 'Elektronik Sinekler' adıyla kurulan trol ordusu (Anadolu Ajansı, 2018), İsrail desteğiyle, Gazze-İsrail çatışmasıyla ilgili dünya kamuoyunu şekillendirmek için dezenformasyon yapan Shirion Collective yapısı (Wilson, 2024) ve Hindistan'da Hindistan Halk Partisi (BJP) adıyla faaliyet yürüten siyasi partiye ait trol ordusu gibi örnekler de mevcuttur (Chaturvedi, 2016).

1.2.2. Trol Hesapların Türleri ve Özellikleri

Troller genel olarak, özellikle etkileşimin yoğun ve bilgi akışının hızlı olduğu Twitter gibi sosyal medya platformlarında, bilgi dezenformasyonu yaparak kitleleri yönlendirme, kasıtlı muhalefet etme ve küfür, hakaret, ırkçı ya da cinsiyetçi içeriklerle dijital ortamda kargaşa yaratma eğilimindedirler. Trolleme davranışları, içerik, taktik, motivasyon ve etkiler açısından oldukça çeşitlilik gösterir. Bu nedenle hem tanımlamalar hem de algılar ve verilen tepkiler farklılık gösterebilir. Genellikle çevrimiçi topluluklar üzerinde olumsuz etkiler yaratan sıra dışı davranışlar olarak tanımlanan trolleme faaliyetleri; grupları aşağılamak, küçük düşürmek, itibarsızlaştırmak, damgalamak ve etiketlemek gibi zarar verici amaçlar taşır. Bununla birlikte, ideolojik saiklerle yönlendirilen bazı trolleme türlerinin, sosyal sorunlara ya da toplumsal ve politik olarak marjinalleştirilmiş grupların dikkatini çekmeye yönelik bir amaç taşıdığı da görülmektedir (Kayaduman, 2020, s. 7).

Çevrimiçi ortamlarda sergilenen trol davranışlarına yönelik olarak, farklı sınıflandırmalar yapılmaktadır.

1.2.2.1. Provokasyon Trolleri

Provokasyon trolleri, çevrimiçi platformlarda kasıtlı olarak insanları sinirlendirmek kutuplara ayırmak ve tartışmaları alevlendirmek amacıyla kışkırtıcı içerikler paylaşan sosyal medya kullanıcılarıdır. Bu troller çoğunlukla gerçek kimliklerini belli etmemek için anonim isimler ve sahte isimler kullanır. Bu trollerin genel amaçları doğrudan hakaret etmekten ziyade hedef kitleyi duygusal olarak harekete geçirecek şekilde düşünülmüş mesajlarla toplulukları bölmek ve kaos ortamı yaratmaktır. Genel olarak toplumda var olan dini, etnik, ideolojik vb. ‘fay hatlarını’ tetikleyici cümlelerle kırmaya çalışırlar. Böylelikle bir çatışma ortamı yaratmış olurlar (Mercimek vd., 2015, s. 68).

Provokasyon trolllerinin paylaşımlarında duygusal sömürülere sık sık rastlanır. Hedef alınan kişi ya da kitlenin duygusal yönleri ve değer verdikleri hassas konuları istismar edilerek kullanıcıların öfkeleri, korkuları ve hüzneleri gibi hassas noktaları tetiklenir. Provokasyon trolleri yalan ve çarpıtmalardan da oldukça fazla yararlanır. Özellikle doğruluğu şüpheli içerikler dolaşıma sokularak kasıtlı bir bilgi kirliliği oluşturulur ve bu sayede toplumda birtakım provokasyonlar yaratılmak istenir. Bu tarz içerik üreten trollerin bazı çıkar gruplarınca finanse edildiği sıklıkla iddia edilmektedir. Türkiye açısından bakacak olduğumuzda özellikle seçim dönemlerinde ya da toplumsal olaylar sırasında provokatif içeriklerin yaygınlaşması, bu tür trol faaliyetlerinin toplumsal çapta sorunlar yaratmak istediği görülmektedir. Bu tip trollerin dünya çapında en çok ses getiren eylemlerinden bazıları ABD’de yaşanmıştır. Rusya merkezli IRA, 2016 ABD başkanlık seçimleri döneminde Amerikan kamuoyunu provokatif paylaşımlar ve kutuplaştırıcı söylemler aracılığıyla ciddi ölçüde etkilemiştir. Yine geçtiğimiz yıllarda ABD’de, ırkçı olduğu iddia edilen polis memurları tarafından öldürülen George Floyd olayı sonrası Birleşik Devletler’de ciddi sokak protestoları başlamıştır. Bu protestolarda IRA etkisi sıklıkla dile getirilmektedir (Scotland vd., 2024, s. 3-4). Irkçılığın her zaman olduğu ABD’de, George Floyd olayı ile beraber alışılmışın dışında bu denli bir toplumsal patlamanın yaşanması gerçekten ilgi çekicidir ve IRA etkisi iddialarını güçlendirmektedir.

1.2.2.2. Sosyal Mühendislik Trolleri

Sosyal mühendislik trolleri, çevrimiçi platformlarda insan psikolojisinden faydalanarak hedeflerini manipüle eden kişilerdir. Genellikle doğrudan saldırgan ya da kışkırtıcı içeriklerden kaçınırlar; bunun yerine güven oluşturarak, inandırıcı bir anlatı kurarak ve insanları adım adım ikna ederek hedeflerine ulaşırlar. Bu troller, teknik becerilerden ziyade psikolojik analiz ve ikna stratejilerine dayalı yöntemlerle hareket ederler. Bu trollerin amacı yalnızca bireylere yönelik bilgi çalma ve manipüle etme eylemi değil, aynı zamanda toplum mühendisliği de yapmaktır. Belli bir gruba, topluluğa ya da kamuoyuna yönelik aşamalı bir şekilde işletilen ve hedef grubu şekillendirmeyi amaçlayan eylemler toplum mühendisliğinin kapsamındadır (Kayaduman, 2020, s. 6).

Sosyal mühendislik trolleri, özellikle seçim dönemlerinde, salgın gibi kriz zamanlarında ve savaş ortamlarında aktif hâle gelmektedir. Yakın geçmişimizdeki COVID-19 pandemisiyle birlikte sosyal medyada kendini doktor ya da bu alandaki kanaat önderi gibi tanıtarak, topluma yararlı bilgiler verdiğini iddia eden manipülatif kişiler aslında halk sağlığına yönelik ciddi bir tehdit oluşturmuştur. Bir dönem, aşı karşıtı hesaplar tarafından paylaşılan ‘aşılar ile insan vücuduna mikroçipler yerleştirilerek beyinler ele geçiriliyor’ gibi iddialar, toplumun çıkarınaymış gibi lanse edilmiş ve aslında toplum sağlığına ciddi bir saldırı olmuştur (BBC News Türkçe, 2021).

Sosyal mühendislik trollerini diğer trol türlerinden ayıran en önemli özellik, çatışmadan ziyade ikna ve hedefin rızası ile yönlendirme üzerinden çalışmalarınıdır. Bu da onları daha tehlikeli ve tespit edilmesi güç hâle getirmektedir.

1.2.2.3. Siyasi Troller

Yeni dijital teknolojilerin gelişmesiyle birlikte, geleneksel propaganda yöntemlerinin yerini alan karmaşık yöntemlerin son dönemdeki önemli bir aktörü troller olmuştur. Siyasi troller, bireysel olarak ya da organize yapılar içinde hareket ederek çevrim içi platformlarda belirli bir ideolojiyi, bir siyasi partiyi ya da devlet politikasını desteklemeyi; buna karşıt görüşleri ise itibarsızlaştırmayı amaçlayan faaliyetler yürütmektedir. Siyasi troller söz konusu olduğunda, sadece resmi ya da legal oluşumlar ile sınırlı kalmamakta; terör örgütleri ve suç örgütlerinin de siyasi alandaki savunuculuğunu üstlenen troller bulunmaktadır (Kayaduman, 2020, s. 9).

Siyasi troller; sosyal medya, forumlar ve haber sitelerinin yorum bölümleri gibi alanlarda sistematik, ideolojik ve manipölasyon içeren içerikler paylaşan kişilerdir. Bu kişilerin hedefi yalnızca provokasyon ya da tartışma çıkarmakla sınırlı değildir; aynı zamanda toplumun algısını yönlendirmek, siyasi rakipleri değersizleştirmek ve kamuoyunu belli bir düşünce doğrultusunda şekillendirmek gibi stratejik hedefler taşırlar. Bu özellikleriyle siyasi troller, sıradan kullanıcılar olmaktan çok, dijital propaganda sürecinin aktif bir parçası hâline gelmişlerdir. Siyasi trol faaliyetleri yalnızca bireysel düzeyde değil, kimi zaman devlet destekli ya da partiler tarafından organize edilen yapılar hâlinde yürütülmektedir (Assardo, 2023). Özellikle daha önce de bahsedilen, Rusya’da ‘trol fabrikaları’ olarak adlandırılan ve profesyonel şekilde yönetilen yapılar, bu tür faaliyetlerin en bilinen örneklerinden biridir. Bu yapılar yalnızca içerik üretimiyle değil, sosyal medya algoritmalarını manipüle etmek, koordineli etkileşim sağlamak ve sahte kamuoyu oluşturmak gibi tekniklerle de çalışırlar. Türkiye’de de neredeyse tüm siyasi partiler, rakiplerine ait bir trol grubu olduğunu iddia etmekte ve bu yapılar aracılığıyla kamuoyunun kendi aleyhlerine manipüle edildiğini ifade etmektedirler.

1.2.2.4. Tıklama-Reklam Trolleri

Dijital medyadaki tanıtım ve pazarlama olanaklarının büyümesi ve popülerleşmesiyle birlikte, reklam verenlerin rekabet sahasına dönüşen sosyal medyada ‘tıklama trolleri’ önemli bir yere sahiptir. Sosyal platformlarda öne çıkmak isteyen bazı çevreler, kullanıcıların tıklama reflekslerini suistimal eden bir yöntem geliştirerek tıklama trollerinden faydalanmaktadırlar. Bu tür troller, içerik üretiminde dürüstlükten uzaklaşarak yalnızca ‘tıklanma’ (click) odaklı manipölatif başlıklar ve paylaşımlar yaparak trafik, gelir ve dikkat kazanmaya çalışırlar. Reklam veren ve tıklama trollerinin karşılıklı kar-çıkâr ilişkisine dayanan bu sistemin işleyişinde özellikle sosyal platformlarda popüler olan hesaplar tercih edilmektedir. Tıklama trolleri, genellikle gerçekte olduğundan çok daha çarpıcı gösterilen içerikler üretirler. Amaçları, kullanıcıları verilen bağlantıya ya da reklama tıklamaya ikna etmektir. Özü itibarıyla reklamcılık sektörüne ait olup toplumu provoke etmek gibi bir niyetleri yoktur (Kayaduman, 2020, s. 10).

1.2.2.5. Hiciv, Mizah ve Alaycı Troller

Sosyal medya kültürü, yapısı gereği çoğu zaman ironik, esprili ve kışkırtıcı bir nitelik taşır. Sosyal medya platformlarında, haber sitelerinin yorum bölümlerinde ya da forumlarda karşılaşılan bazı paylaşımlar yalnızca eğlence amacıyla yapılmaz; aynı zamanda toplumsal, siyasal veya kültürel normlara yönelik bir eleştiri ya da yönlendirme de barındırabilir. Bu tür içeriklerin ardındaki kullanıcılar, genellikle ‘hiciv, mizah ve alaycı trol’ olarak tanımlanır. Bu troller, mizahı aldatmacayla birleştirerek, doğrudan değil dolaylı yollarla hedef kitlelerini etkilemeyi amaçlarlar. Hiciv ve mizah temelli troller çoğu zaman zararsız gibi algılansa da, özellikle düşük medya okuryazarlığına sahip bireyler üzerinde bilgi kirliliğine neden olabilir ve yanlış kanaatlerin oluşmasına yol açabilir. Bununla birlikte, bu tür trollerin söylemleri kimi zaman sınırları aşarak ayrımcı veya toksik bir mizaha dönüşebilir. Örneğin, cinsiyetçi ya da ırkçı içerikler, ‘ifade özgürlüğü’ kisvesi altında sosyal medyada dolaşıma sokulabilir. Bu da sosyal medyadaki diğer kullanıcıları olumsuz anlamda etkiler (Kayaduman, 2020, s. 11).

1.2.3. Trol Ordularının Organizasyonel Yapısı ve Finans Kaynakları

Belli bir amaç doğrultusunda hareket eden ve sistematik planlar dahilinde faaliyet yürüten trol ordularının, başına buyruk ve doğaçlama bir biçimde davranması beklenemez. Ayrıca bu yapıların herhangi bir sermaye olmadan kontrol altında tutulabileceği de düşünülemez. Kamuoyunu şekillendirmede günümüzün önemli figürleri haline gelme potansiyeli olan trol ordularının işlevsel ve sürekli olabilmesi için belli bir düzen ile oluşturulmuş ve ast-üst ilişkisine dayalı bir organizasyonel şemasının yanı sıra bu organizasyonun devamlılığını sağlayacak bir sermaye akışı da gereklidir.

1.2.3.1. Organizasyonel Yapı

Dijital çağda bilgi, basit bir iletişim aracı olmanın ötesine geçerek stratejik bir silaha dönüşmüştür. Sosyal medya platformları başta olmak üzere, forumlar, tartışma platformları ve haber siteleri artık yalnızca bireylerin iletişim kurduğu alanlar değil; aynı zamanda bilgi savaşlarının yürütüldüğü, farklı manipülasyon taktiklerinin uygulandığı ve psikolojik operasyonların sahnelendiği dijital cepheler hâline gelmiştir. Bu görünmeyen savaşın en etkili aktörlerinden biri ise trol ordularıdır. Devlet destekli ya da belli bir çıkar odakları tarafından finanse edilen, organize yapılar altında faaliyet gösteren bu gruplar,

bireysel trollerden farklı olarak belirli bir hiyerarşi içinde çalışır. Trol orduları görev paylaşımı, stratejik planlama ve eşgüdüm içinde hareket ederek sistematik dijital operasyonlar yürütürler (Ayeb & Bonini, 2024, s. 7-8).

Günümüzde pek çok ülkenin resmi makamları, farklı isimlerdeki yapılar aracılığıyla ‘sosyal medyada kendi trol ordularını’ oluşturmakla itham edilse de bu tarz iddiaların resmi düzeyde üstlenildiği ya da kabul edildiğine tanık olunmamıştır. Bu durum, resmi anlamda bir trol ordusunun işleyişi ve organizasyonunun tanımına engel olmakta, resmi olarak bu yapının nasıl bir hiyerarşik şema ile açıklanacağını konusunda soru işaretleri doğurmaktadır. Bu yüzden trol ordularının organizasyonel şeması ile ilgili fikir edinmek için ‘itirafçıların’ yorumlarından faydalanılmış ve trol ordusu kurmakla itham edilen yapıların organizasyon şeması açık kaynaklardan ulaşılabilen veriler ile incelenmiştir.

İngiltere kaynaklı haber ajansı BBC’nin 2017 tarihli araştırmasında, Brezilya’daki bir halkla ilişkiler firması için çalışan trolün itiraflarına yer vermiştir. ‘Pedro’ takma adını kullanan bu trol, aralarında siyasetçilerin de olduğu firma müşterilerine hizmet veren bir trol takımının üyesiydi. Pedro’nun ve trol takımının ayda kişi başı 360 dolar ücret karşılığında çeşitli sosyal medya platformlarındaki trollük faaliyetlerine değinilen araştırma yazısında Pedro, takımının hiyerarşik ve organizasyonel yapısına dair ipuçları vermektedir. Pedro, bir koordinatör gözetiminde olduklarını aktarırken, sistemli trol yapılarının aslında hiyerarşik bir düzen ile örgütlendiği anlaşılmaktadır. Yapıyı koordine eden kullanıcı, troller üzerindeki denetimi sıkı tutmakta ve bir ‘süpervizör’ görevi görmektedir. Kavram olarak süpervizör, bir şirket ya da kurumda, çalışanlarına uymaları gereken talimatları vermekte ve talimatların uygulanışını denetlemektedir. Dolayısıyla Pedro takma adlı kullanıcının ifadelerine göre ast-üst ilişkisi ile kurulu olan trol yapısı, belli emirleri yerine getirerek tam anlamıyla planlı ve sistematik şekilde çalışmaktadır. Yapı içinde görev alanların, işe başlarken sahte bilgiler ile oluşturulmuş bir sosyal medya hesabı aldıkları ve bu hesabı ilk olarak etkin ve inandırıcı biçimde kullandıkları anlaşılmaktadır. Bunun için genellikle birkaç ay boyunca düzenli olarak içerik paylaşımı yapar, gündelik hayata dair gönderilerle hesapların gerçek bir kullanıcıya ait olduğu izlenimini yaratmaya çalışırlar. Amaç, bu hesapları doğal bir görünüme kavuşturarak ilerideki propaganda faaliyetleri için hazır hâle getirmektir (Gragnani, 2017).

Rusya merkezli The Moscow Times gazetesinin haberine göre eski IRA çalışanı olduklarını iddia eden Lyudmila Savchuk ve Olga Maltseva adındaki iki trol, tartışmalı Rus ajansına dair önemli bilgiler vermişlerdir. IRA'nın işleyişine değinen itirafçı troller, bu birimde 12'şer saatlik mesailer ile çalıştıklarını, her gün 200 yorum ve 20 haber yazısı yazarak limitlerini doldurduklarını açıklamışlardır. IRA'nın organizasyonel şemasını da açıklamalarla çizen troller, burada farklı konularda yazan ve farklı web sitelerini hedefleyen birçok trol ekibinin varlığından söz etmektedirler. Açıklananlardan hareketle Rusya'nın 'trol ordusu' olduğu belirtilen IRA 'karargahında' askeri örgütlenmeye benzer biçimde alt mangalar oluşturulduğu anlaşılmaktadır. Bu da Rusya'nın trol ordusunu nasıl bir ciddiyet ve nizamla hazırladığını göstermektedir. The Moscow Times'ın haberine göre bu troller, IRA'nın o dönem Ukrayna'da yaşanan çatışmalar ve ABD seçimlerine atanan departmanları olduğunu da iddia etmişlerdir. Yine yapılan açıklamalar, trol ordularında çalıştırılmak üzere devşirilen kişilerin 'başka çareleri olmadıkları' için bu işi yaptıklarını göstermektedir. İtirafçı çalışanlar, üniversiteden mezun olduktan sonra iş bulamamış ve o dönem ödemeleri gereken borçları olan kişilerdir. Çevrelerindeki bazı kişilerin de bu işle uğraştıklarını görünce işe başvurmuşlar ve mülakatı geçerek trol ordusunda çalışmaya başlamışlardır. Günlük kotalarını doldurduklarında ve iyi işler çıkarttıkları zaman aldıkları ödüllerle birlikte her ay 80.000 – 90.000 rublelik bir kazançlarının olduğunu dile getirmişlerdir (Davies K. M., 2017). Bahsi geçen dönemde Rusya'daki asgari ücretin 7.500-7.800 ruble olduğu dikkate alındığında (BirGün, 2017). IRA'nın oldukça motive edici bir ücret ile çalışanlarını trollüğe teşvik ettiği görülmektedir.

1.2.3.2. Finans Kaynakları

Pek çok ülkede trol faaliyetleri, doğrudan ya da dolaylı biçimde devlet kurumlarının finansal desteğiyle yürütülmektedir. Özellikle Rusya, Çin ve İran bu ülkelere örnek olarak gösterilmektedir. Fakat burada özellikle belirtilmesi gereken nokta, şu ana kadar bu ülkelerin hiçbiri bahse konu trol faaliyetlerine dair resmi bir açıklama yapmamış; haklarında verilen bilgi, 'delil' ve iddialar, sivil kuruluşlar ya da farklı ülkelerin resmi makamlarınca açıklanmıştır. Devletlerin direkt olarak açıklamadığı ve finanse etme iddialarını kabul etmediği bu konuda IRA, yine çarpıcı bir örnek olarak karşımıza çıkmaktadır. IRA, öldüğü zamana kadar Yevgeni Prigojin'in komutası altında olmuştur. Rusya devlet başkanı Vladimir Putin'e yakınlığıyla bilinen Prigojin, IRA'yı kendisinin kurduğunu söylemiş ve CNN'e göre ABD seçimlerine müdahil olduğunu da

itiraf etmiştir. Rusya'nın en önemli kişileri arasında gösterilen Prigojin, IRA'yı finanse etmektedir. Burada, Rusya'nın resmi makamlarının Prigojin aracılığıyla IRA'yı finanse etme olasılığının çok yüksek olduğu anlaşılmaktadır. Böylece resmi makamların hem iç hukukta hem de uluslararası hukukta sorumluluğu olmayacak ve paravan kişiler aracılığıyla, resmi makamlara hizmet eden bir yapı rahatça finanse edilecektir (Krever & Chernova, 2023). IRA örneğinden de anlaşılabacağı üzere bu tarz büyük trol ordularının en önemli finans kaynaklarından bir tanesi, ilgili devletlerdir.

Sistemli şekilde çalışan trol gruplarının finans kaynakları, türleriyle paralel olmaktadır. Sözelimi politik troller belli siyasi oluşumlar tarafından finanse edilirken, reklam trolleri bağlı oldukları özel şirket tarafından finanse edilmektedirler. Özellikle çok takipçisi olan sosyal medya hesapları, belli bir ücret ya da ürün karşılığında reklam trollüğü yapmaktadırlar. Provokasyon trolleri gibi art niyetli yapıların ise ülkelerin gizli servislerinden tutun da terör örgütlerine kadar karanlık bir finans kaynakları olduğu bilinmektedir. Bu karanlık finans kaynakları da bazı araçlar kullanarak ödeme yapmakta ve daha çok kripto varlıklar üzerinden finans işlemlerini yürüttükleri tahmin edilmektedir. Özellikle şifreli olması ve takip edilememesi sebebiyle kripto ödemeler, bu organizasyonları küresel bir tehdit hâline getirmektedir (Robinson, 2020). Trol ordularını analiz ederken, amaçlarını anlamak için yalnızca mesajlarına değil, bu mesajları mümkün kılan finansal arka plana da bakmak gerekmektedir.

1.3. Bilgi Savaşları ve Siber Operasyonlar

Yeni yüzyılın başından itibaren 'savaş' kavramı, yalnızca fiziksel çatışmalarla sınırlı olmaktan çıkmıştır. Devletler, örgütler ve bireyler arasındaki güç mücadeleleri giderek dijital mecralara taşınmış; siber operasyonlar ve bilgi savaşları, bu yeni dönemin en görünmeyen fakat en etkili silahları hâline gelmiştir. Sınırların bulanıklaştığı, düşman figürlerinin net biçimde tanımlanamadığı bu modern savaş biçimleri, yalnızca teknik yetkinliklerle değil aynı zamanda psikolojik, sosyolojik ve stratejik analiz yeteneğiyle de yürütülmektedir.

Bilgi savaşı, çoğunlukla devletler veya örgütler gibi aktörlerin, hedef kitlenin algılarını, tutumlarını ve davranışlarını yönlendirmek amacıyla bilgi üzerinde manipülasyon yapmasıyla ortaya çıkan bir mücadele biçimidir. Bu süreçte gerçek bilgiler çarpıtılır, yanlış bilgiler kasıtlı olarak yayılır ve toplumun karar verme süreçleri hedef

alınır. Günümüz bilgi savaşları; dezenformasyon, propaganda, bilgi sızıntıları ve sosyal medya üzerinde algı yönlendirme gibi çeşitli yöntemlerle yürütülmektedir. Geleneksel savaşlardan temel farkı ise fiziksel değil, zihinsel hâkimiyet kurma amacını taşımasıdır. Yani bu savaş biçiminde eli silah tutan askerlerden çok; kitlelerin algısını yönlendirecek olan ‘profesyonellere’ ihtiyaç duyulmaktadır. Siber operasyonlar ise bir bilgisayar sistemini, ağı ya da dijital altyapıyı hedef alarak hasar verme, veri çalma veya kontrolü ele geçirme amacı güden faaliyetleri kapsamaktadır. Bu operasyonlar hem askeri hem de sivil alanlarda yürütülebilir. Casusluk, siber sabotaj, fidye yazılımları aracılığıyla yapılan korsanlık gibi çeşitli alt dallara ayrılan siber operasyonlara artık yeni bir alt alan olarak sistematik trol saldırıları da eklenebilmektedir. Genel olarak bu tür operasyonlar, askeri birliklerden ziyade küçük hacker grupları ya da devlet destekli dijital birlikler tarafından yürütüldüğü için kimlik tespiti zor, sorumlu tutmak ise neredeyse imkânsızdır (Erdoğan, 2020, s. 15).

1.3.1. Bilgi Savaşlarının Uluslararası İlişkilerdeki Yeri

Tarih boyunca dünya üzerinde binlerce medeniyet kurulmuş ve bu medeniyetler kendi aralarında tıpkı bugün olduğu gibi her zaman bir çekişme yaşamıştır. Üstünlük kurmak ve kendi çıkar hedeflerini gerçekleştirmek için yapılan bu çekişmelerde asker gücü ve ekonomik zenginlik kadar bilgi de stratejik bir unsur olmuştur. Medeniyetler, uygarlıklar, devletler ve gruplar, varlıklarını devam ettirebilmek adına rakipleri hakkında bilgi edinmeyi kıymetli bulmuş, bu sayede her türlü mücadeleye nasıl hazırlanacağını öngörürken aynı zamanda rakibin maddi-manevi gücünü nasıl kıracakları hakkında da stratejiler geliştirmişlerdir.

Dijital çağın hızla gelişen iletişim teknolojileri ile birlikte devletler arasındaki mücadele biçimlerinin köklü değişiklikler geçirmesi, bilgiye verilen değeri daha da arttırmış ve bilgi savaşlarını her alanda görünür kılmıştır. Bu dönüşümle birlikte, ‘bilgi savaşları’ kavramı uluslararası ilişkilerde merkezi bir konuma yerleşmiş, modern çağdaki devletlerin dış politikalarını etkileyen görünmez bir güç biçimi olarak ortaya çıkmıştır. Bilgi savaşları, yalnızca doğru veya yanlış bilgiyi yaymak ya da rakip hakkında istihbarat toplamaktan ibaret değildir; aynı zamanda hem teknik hem de psikolojik araçların bir arada kullanıldığı, çok katmanlı bir mücadele biçimidir. Günümüzde dezenformasyonlar, psikolojik hareketler ve algı operasyonları, sosyal medya manipülasyonları ve siber

saldırıları gibi başlıca yöntemleri bulunan bilgi savaşlarının örnekleri de oldukça fazladır (Geneş & Taydaş, 2024, s. 5-6).

Kökleri görece yakın tarihlere dayanan Çin-Tayvan gerilimi, özellikle son dönemde bilgi savaşları açısından dikkate değer bir örnek teşkil etmektedir. 1949 yılında Çin İç Savaşı'nın komünistlerin üstünlüğüyle sona ermesinin ardından, milliyetçi Kuomintang partisi yönetimi Tayvan'a çekilmiş ve burada Çin Cumhuriyeti adı altında yönetimini sürdürmeye devam etmiştir. Çin Halk Cumhuriyeti ise Tayvan'ı kendi topraklarının ayrılmaz bir parçası olarak görmekte ve 'tek Çin' politikası çerçevesinde Tayvan'ın bağımsızlık iddialarını kesin bir şekilde kabul etmemektedir (Çakı & Fidan, 2020, s. 185). Bu doğrultuda iki ülke arasında zaman zaman uluslararası arenada da tepkilere sebep olan askeri tatbikatlar yapılmakta ve gerilim tırmandırılmaktadır. Yakın geçmişe kadar askeri güç ile arttırılan bu gerilimler yeni bir boyuta taşınarak artık bilgi savaşları aracılığıyla gerçekleşmektedir. Tayvan yönetimi, Çin'in halkı 'kutuplara ayırmak' amacıyla Tayvan'a karşı dezenformasyonu artırmak için yapay zekâdan yararlandığını açıklamıştır. Tayvan parlamentosuna sunulan resmi raporda, 2025 yılının ilk aylarında, yarım milyondan fazla 'tartışmalı mesaj' tespit edildiği ve bu mesajların daha çok Facebook ve TikTok platformlarında yayınlandığı vurgulanmıştır. Raporda, özellikle yapay zekâ vurgusu yapılarak, 'Çin Komünist Partisi tarafından tartışmalı mesajların üretilmesi ve yayılmasında yapay zekâ araçlarının kullandığı da görüldü' denilmiştir. Çin yönetimi ise bu iddialara bir cevap vermemiştir (Reuters, 2025).

Yıllardır süren ve 7 Ekim 2023 tarihinden itibaren katlanarak devam eden Filistin-İsrail çatışmasının da askeri ve taktik savaşın yanında dijital mecralara sıçramış bir bilgi savaşı boyutu vardır. 7 Ekim tarihinde Hamas militanlarının İsrail tarafına düzenlediği saldırılar sonrasında başlatılan geniş çaplı askeri operasyonlar ve sivil ölümleri, dünya çapında büyük ses getirmiştir. Çatışmalar sürerken taraflar arasında başlayan dezenformasyon savaşları, geniş kitlelere de hızla sıçramış ve sosyal medya kullanıcıları da taraf duruma gelmiştir. Sosyal medyada yayılan ve 'Refah Mülteci Kampı'na İsrail Saldırısı' başlığıyla verilen bazı görüntülerin yanlış olduğu kanıtlanmış, bu görüntülerin İsrail'e yapılan bir saldırıdan alındığı anlaşılmıştır (Reuters, 2024). Öte yandan İsrail tarafının sivil bölgeleri vurması sonucu hayatını kaybeden insanları belgeleyen görüntüleri yalanladığı da süreç boyunca görülmektedir. Fakat bazı ölümler, sadece

sosyal medya hesaplarından yayınlanan içeriklerle değil, uluslararası kuruluşlarca da belgelenebilmiştir (Bartholomew, 2025).

Tüm bu bilgi savaşlarında dikkati çeken hususlar, yaşanan olayların yerel boyuttan hızla çıkıp küresel boyutlara ulaşabilmesidir. Tarafların iddiaları ve ispatları, kısa sürede destek ya da karşıt düşünceleri bulabilmekte ve savaş bambaşka bir boyuta taşınmaktadır.

1.3.2. Siber Operasyonların Askeri ve Siyasi Boyutları

Tarihin erken dönemlerinden itibaren ağırlıklı olarak kara ve denizlerde sürdürülen savaşlar, 20. yüzyılın başlarından itibaren havacılık teknolojisinde yaşanan ilerlemelerle birlikte gökyüzünü de bir savaş sahasına dönüştürmüştür. 1950'li yıllardan itibaren ise küresel güçlerin rekabeti ve iki kutuplu dünya düzeninin getirmiş olduğu çekişmeler, savaşları bu kez uzaya taşımıştır. 21. yüzyıla gelindiğinde ise hızla gelişen dijital teknolojiler ve bilgi sistemlerindeki dönüşüm, siber ortamın da bir çatışma alanı olarak tanımlanmasına yol açmıştır. Günümüzde siber ortamda yürütülen mücadeleler, 'beşinci savaş alanı' olarak tanımlanmakta ve diğer tüm alanlardaki savaşlara kıyasla giderek daha fazla stratejik bir önem kazanmaktadır (Polat, 2020, s. 138).

Siber savaşlar kapsamında düzenlenen siber operasyonlar, devletlerin askeri ve siyasi güç tanımlarını yeniden şekillendiren, uluslararası ilişkilerdeki dengeleri yeniden düzenleyen ve geleneksel savaş stratejilerini köklü biçimde dönüştüren dijital saldırı biçimleridir. Bilgisayar sistemleri, iletişim altyapıları ve dijital veri akışı üzerinden gerçekleştirilen bu tür operasyonlar, günümüzde yalnızca savunma stratejilerinin temel bileşeni hâline gelmekle kalmamış, aynı zamanda diplomatik gerilim ve çatışmalarda da belirleyici bir faktör olarak yavaş yavaş öne çıkmaktadır. Modern devletlerin stratejik kurumları ve askeri ittifaklar bu alana ciddi yatırımlar yapmaya başlamış ve çeşitli savunma stratejileri geliştirmişlerdir (Baştan & Çoban, 2024, s. 1206-1207).

Türkiye Cumhuriyeti'nin resmi istihbarat örgütü olan Millî İstihbarat Teşkilatı (MİT), kendi bünyesinde Siber İstihbarat Başkanlığı kurmuş ve siber tehditlere karşı daha kapsamlı savunmalar yapabilmek adına ciddi adımlar atmıştır (Aksan, 2023). Yine Türkiye'nin üyesi olduğu Kuzey Atlantik Antlaşması Örgütü (NATO), Siber Savunma Mükemmeliyet Merkezi kurarak bu alana önemli bir bütçe ayırmıştır. Yeni istihbarat ve siber savaş doktrinlerine yönelik düzenli tatbikatlar ve eğitimler düzenleyen örgüt,

modern askeri stratejilerin önemli bir parçası konumuna gelmiştir (NATO's Strategic Warfare Development Command, 2023).

Keşif, istihbarat toplama, kritik dijital altyapılara yönelik sabotajlar ve psikolojik harekât gibi işlevler üstlenen siber operasyonlar, askeri anlamda ciddi bir stratejik saldırı olarak ön plana çıkmaktadır. Bu alanda faaliyet gösteren devlet destekli hacker grupları ya da bizzat orduların siber operasyon birimleri, düşman kuvvetlerin iletişim ağlarını bozabilmekte, stratejik dijital altyapıları zedeleyebilmekte veya sahte bilgi akışları oluşturarak savaşın seyrini değiştirebilmektedirler. 2007 yılında bir NATO üyesi olan Estonya'ya yönelik düzenlenen siber saldırı, bu alandaki dönüm noktalarından biri olmuştur. Rus hackerlerin düzenlediği siber saldırıda, Estonya'da 13 gün süreyle dijital altyapı, haberleşme ve bankacılık sistemlerinde ciddi sorunlar meydana gelmiştir (Habertürk, 2007). Yaşanan gelişmeden sonra NATO, Estonya'nın Başkenti Tallinn'de Siber Savunma Mükemmeliyet Merkezi'ni kurmuştur.

Siber operasyonlar, yalnızca askeri stratejilerde değil, aynı zamanda devletlerin dış politika araçları arasında da önemli bir yer edinmiştir. Seçim süreçlerine müdahale etmek, kamuoyunu manipüle etmek ya da devlet kurumlarının itibarını zedelemek gibi girişimler, dijital teknolojiler sayesinde hem daha ulaşılabilir hâle gelmiş hem de izlenmesi ve engellenmesi güçleşmiştir. Bu durum, ülkelerin iç işlerine karışmayı kolaylaştıran yeni bir dış politika pratiği olmuştur. Ayrıca siber saldırılar, devletler açısından örtülü mesaj iletmenin modern bir aracı hâline de gelmiştir. Bir ülkenin finansal sistemine ya da enerji altyapısına yönelik gerçekleştirilen dijital saldırılar, geleneksel diplomatik söylemler yerine tehditkâr bir dil kullanmanın yeni ve etkili bir yolu olarak öne çıkmaktadır. Bu tür eylemlerle devletler, doğrudan çatışmaya girmeden karşı tarafa güç gösterisinde bulunmakta, tepkilerini ölçmekte ve stratejik sınırlarını zorlamaktadır. Yakın geçmişte Türkiye'de yaşanan, 'kişisel verilerin çalındığı' iddialarının resmi makamlarca doğrulanması, bu anlamda ciddi siber operasyonlardan birisi olarak görülmektedir (Oksijen Gazetesi, 2024).

Sonuç olarak, siber operasyonlar, yalnızca dijital altyapılara zarar vermekle kalmayan, aynı zamanda devletlerin stratejik planlamalarında ve dış politikalarında etkili rol oynayan güçlü bir unsur haline gelmiştir. Bu nedenle, ülkeler sadece fiziksel güvenlik değil, dijital güvenlik açısından da kendilerini korumaya almak; aynı zamanda

uluslararası iş birlikleri geliştirerek bu yeni tehdit biçimine karşı ortak refleksler oluşturmak zorundadır. Günümüz dünyasında savaşlar artık yalnızca demir yığını silahlarla değil, bilgisayar tuşlarıyla da etkili biçimde yapılmaktadır.

1.4. Dijital Propaganda ve Trol Hesapların Toplumsal Etkileri

Dijital çağın iletişim alanındaki en dikkat çekici değişimlerinden biri, bilginin dolaşımındaki hız ve etkinin artmasıyla birlikte kamuoyunun şekillenme süreçlerinin çevrimiçi mecralara taşınmasıdır. Geleneksel medyanın sınırlarını aşan bu yeni ortam, propaganda tekniklerinin de dönüşmesine yol açmıştır. Artık daha hızlı, hedef kitlesine doğrudan ulaşabilen ve manipülasyona açık bir propaganda biçimi olan dijital propaganda öne çıkmaktadır. Dijital propaganda, sosyal medya platformları, çevrimiçi forumlar, bloglar ve dijital haber kaynakları üzerinden belirli görüşleri yaymayı ve toplumun algısını istenilen yönde şekillendirmeyi amaçlayan bir propaganda şeklidir. Geleneksel propagandadan farklı olarak, bu tür propaganda yöntemleri tek yönlü bir aktarım yerine etkileşime açık, katmanlı ve daha güçlü bir ikna mekanizması sunar. Kullanıcıların içerikle doğrudan temas kurabildiği bu yapı, propaganda sürecini daha dinamik ve etkili hale getirmektedir. Oxford Üniversitesi profesörlerinden Philip N. Howard ve Samuel C. Woolley'e göre 'dijital propaganda', kitlelerin görüşlerini şekillendirmek amacıyla sosyal medya platformları, algoritmalar ve otomasyon teknolojileri yoluyla yapılan stratejik iletişim manipülasyonudur (Woolley & Howard, 2017, s. 4-6). Bu yeni propaganda biçiminin uygulanmasındaki en etkili araçlardan biri ise planlı ve organize bir şekilde faaliyet gösteren trol hesaplar olmuştur. Bu hesaplar, yalnızca bireysel çıkışlarla değil; belirli ideolojik, siyasi ya da stratejik hedeflere yönelik hareket ederek, dijital kamuoyunu yönlendirme gücüne sahiptir. Dezenformasyon yayarak ve yapay tartışmalar başlatarak belli bir gündemin dijital platformlarda baskın hale gelmesini sağlarlar. Tüm bu dijital propaganda faaliyetlerinin ise kitleler üzerinde ciddi biçimde olumsuz etkileri olabilir.

1.4.1. Kamuoyu Manipülasyonu ve Algı Yönetimi

Türk Dil Kurumu'na göre 'seçme, ekleme ve çıkarma yoluyla bilgileri değiştirme' anlamı taşıyan manipülasyon kavramı (Türk Dil Kurumu Sözlüğü, tarih yok). Özellikle iletişim ve medya bağlamında, bireylerin ya da toplulukların düşünce, tutum ve davranışlarını belirli bir yöne sevk etmek amacıyla bilginin planlı ve kasıtlı biçimde şekillendirilmesi olarak tanımlanabilir. Bu süreçte bilgi, hedef kitlenin algısını

etkileyecek biçimde değiştirilerek kimi zaman eksik sunulur, kimi zaman bağlamından kopararak anlamı değiştirilir ya da duygusal tepkiler uyandıracak şekilde yeniden kurgulanır. Amaç, alıcının mesajı belirli bir şekilde yorumlamasını sağlamak ve istenilen etkiyi yaratmaktır. Kamuoyu manipülasyonu ise geniş kitlelerin düşünce ve tutumlarını bilinçli olarak etkileme ya da yönlendirme sürecidir. Bu süreçte temel amaç, kitlelerin kararlarını manipüle edecek şekilde bilgi vermek, bilgi saklamak ya da çarpıtmaktır. Genellikle siyasi kampanyalarda, kriz anlarında ya da toplumsal olaylarda devreye girer. Manipülasyon, çoğunlukla bireylerin fark etmeden içine çekildiği bir süreçtir ve karar alma mekanizmalarını etkilemektedir. Algı yönetimi ise belirli olay ya da durumun toplum tarafından nasıl algılanacağını şekillendirmeye yönelik stratejik iletişim uygulamalarını kapsamaktadır. Manipülasyonla benzer yönleri olsa da algı yönetiminde mutlaka açık bir yalan ya da doğrudan bilgi çarpıtması olmayabilmektedir. Bunun yerine, bilgi seçimi, duygusal çerçevelendirme ve anlatının bağlamını değiştirme gibi yollarla gerçeklik algısı üzerinde kontrol kurmak hedeflenmektedir (Kimberly, 2003, s. 302-306).

Trol hesaplar tarafından yapılan dijital propaganda çalışmalarında, kamuoyu manipülasyonu ve algı yönetimine sıkça başvurulmaktadır. Trol orduları ve bot hesaplar üzerinden yürütülen kampanyalarda sosyal medyada yapay gündemler oluşturmak, kasıtlı yanlış ve sansasyonel bilgiler yaymak, aleyhteki olumsuz bir gelişmeyi gölgelemek için dikkati lehteki konulara odaklandırmak, bazı bilgilerin vurgulanıp diğerlerinin görmezden gelinmesiyle algıyı istenilen yöne çekmek gibi pek çok taktik kullanılmaktadır. Konuya Türkiye özelinde baktığımız zaman, ‘suç işlemek amacıyla örgüt kurmak’, ‘cinsel istismar’, ‘cinsel saldırı’ gibi suçlardan 8 bin 463 yıl hapis cezası alan suç örgütü lideri Adnan Oktar’ın sosyal medyadaki trol ağı, zaman zaman ciddi kamuoyu manipülasyonları yapmıştır. Ağdaki trol hesaplar, çeşitli sosyal medya platformlarında dikkat çekici içerikler ile yapay gündemler oluşturarak Adnan Oktar’ı ‘aklamaya’ çalışırken, oluşturdukları gündemleri ‘popüler’ göstermek maksadıyla bot hesapları da etkin şekilde kullanmışlardır. Gerekli takipler sonrasında yakalanan sorumlular çeşitli cezalara çarptırılmıştır (İhlas Haber Ajansı, 2023). Ancak dolaşıma sokulan manipülatif içeriklerin aksi ispatlansa dahi bu, kitleler tarafından yanlış bilgi kadar ilgi çekmemekte ve geniş kitlelere nüfuz edememektedir. Massachusetts Teknoloji Enstitüsü (MIT)’nin 2018 yılında yapmış olduğu bir araştırma bu konu hakkında önemli detaylara yer vermektedir. MIT araştırmacıları Soroush Vosoughi, Deb Roy ve Sinan

Aral'ın yürüttüğü kapsamlı bir çalışmada, 2006 ile 2017 yılları arasında X'te (eski adıyla Twitter) yayılan 126.000 tweet incelenmiştir. Yaklaşık 3 milyon kullanıcı tarafından toplamda 4.5 milyon kez paylaşılan bu içeriklerin analizin sonucunda yanlış bilgilerin, doğru bilgilere kıyasla yüzde 70 oranında daha fazla paylaşıldığı ve kitlelere ulaşma hızının doğru haberlere kıyasla 6 kat daha fazla olduğu ortaya çıkmıştır. Söz konusu araştırma, yanlış bilgilerin yayılmasında bot hesaplardan ziyade gerçek kullanıcıların daha etkili bir rol oynadığını ortaya koymuştur. Yalan içeriklerin genellikle daha ilgi çekici ve şaşırtıcı bulunması, kullanıcıların bu tür bilgileri paylaşma motivasyonunu artırmaktadır (Dizikes, 2018). Dijital çağda yürütülen manipölasyonlar ve toplumsal algı yönetimi konularında ciddi çıkarımlarda bulunmamızı sağlayan araştırma, yalan haberlerin hızlı yayılmasının, sadece bireysel değil, toplumsal düzeyde de ciddi sorunlara yol açabileceğini göstermektedir. Bu nedenle hem bireysel ölçekte hem toplumsal ölçekte hem de resmî kurumlarca bu konuda bilinçli ve sorumlu davranılmasının, sağlıklı bir enformasyon akışının oluşturulması için hayati önemde olduğu anlaşılmaktadır.

1.4.2. Toplumsal Kutuplaşma ve Güven Erozyonu

Kutuplaşma, bireylerin ya da toplumsal grupların düşünsel, siyasal veya kültürel alanlarda karşıt görüşlerde keskin bir şekilde ayrışmalarını ifade etmektedir. Bu ayrışma zamanla ortak değerleri aşındırabilmekte ve toplumsal diyalog kanallarını kapatabilmektedir. Her toplumda farklı derecelerde görülebilecek olan kutuplaşma ancak belirli bir eşiğin üzerine çıktığında, toplumsal barış ve güvenlik için ciddi tehditler oluşturabilmektedir (Bilgiç, 2014, s. 164)

Sosyal medya ortamlarında yapılan trol odaklı manipölasyonlar, toplumsal yapının temelinde ciddi çatlaklara yol açmaktadır. Bu tür faaliyetler, bireyler arası güven ilişkisini zayıflatırken, kutuplaşmayı da besleyerek ortak paydada buluşulmasını zorlaştırmaktadır. Etik değerlerden uzak şekilde yapılan partizan propagandalar, hedef birey veya grupları aşağılamak, onlara iftiralar atmak ya da onları toplumsal dışlanma tehlikesiyle karşı karşıya bırakma amacı gütmektedir. Bu tür içerikler, bireyler veya gruplar arasında nefreti körüklemekte ve toplumlarda derinleşen kutuplaşmanın bir sebebi olarak karşımıza çıkmaktadır. Bu kutuplaşmanın yalnızca siyasal ya da ideolojik farklarla sınırlı kalmayacağı, aynı zamanda kültürel, dini ve etnik farklılıklar etrafında da derinleşebileceği düşünülmektedir. Sosyal medyada hedef alınan gruplar, kendilerini

dışlanmış, tehdit altında ve güvensiz hissedebilmekte, bu durum ise toplumsal dayanışmayı zedeleyerek daha geniş çaplı çatışmaların ortaya çıkmasına neden olabilmektedir (Guess vd., 2021, s. 3-5). Myanmar'ın Arakan eyaletinde Müslüman vatandaşlara yönelik baskı ve şiddet olayları sonrasında binlerce insan yaşamını yitirmiş, yüzbinlerce insan ise göç etmek zorunda kalmıştır. Uluslararası Af Örgütü, yaşananları insanlık suçu olarak görmüş ve sorumluların yargılanmasını istemiştir (BBC News Türkçe, 2018). Yaşanan olaylarla ilgili 2018 yılında yayımlanan bir Birleşmiş Milletler raporu, sosyal medyanın yapılan katliamlar üzerindeki ciddi etkisini göstermektedir. Raporda, bölgede yaşayan farklı etnik grupların ayrışmasında ve birbirlerine karşı düşmanlık beslemesinde sosyal medyanın önemli bir etken olduğu; sosyal medya özelinde de Facebook'un bölgedeki çatışmalarda ciddi etkisi olduğu vurgulanmıştır. Farklı etnik gruplara karşı nefretin yayılmasına sebep olan Facebook, yeterli önleyici adımları atmamış ve etkisiz olmuştur. Raporda, Facebook gönderileri ve mesajlarının toplumda ayrımcılık ve şiddete yol açma derecesinin, bağımsız ve kapsamlı bir şekilde incelenmesi gerektiği vurgulanmıştır (Human Rights Council, 2018, s. 11-12). Facebook da Myanmar'daki sosyal medya hizmetinin 'şiddeti teşvik', 'kışkırtma' gibi amaçlarla kullanılmasını engelleyemediğini kabul etmiştir. Facebook'un siparişi üzerine hazırlanan bağımsız bir raporda, platformun insan hakları ihlallerinin yaygınlaşmasına 'uygun ortam' yarattığı belirtilmiştir (BBC, 2018).

Sosyal medya aracılığıyla ciddi bir potansiyel teşkil eden bu tehdidin önlenmesi sadece teknik müdahalelerle değil; medya okuryazarlığını artıran eğitim politikaları, şeffaflık ilkesine dayalı yönetim anlayışı, toplumsal farkındalık ve sağlam yasal çerçevelerin eş zamanlı uygulanmasıyla mümkün olabileceği düşünülmektedir. Aksi halde, dijital ortamda ortaya çıkan bu ayrışmalar, toplumsal dokunun uzun vadeli bütünlüğünü tehdit edebilecektir.

1.5. Ukrayna-Rusya Savaşı'nın Dijital Boyutu

Tarihsel bağlamda Ukrayna ve Rusya arasında uzun yıllardır yaşanan çatışmalar, hak talepleri ve sınır anlaşmazlıklarının bir sonucu olarak 24 Şubat 2022 tarihinde Rusya'nın 'özel askeri operasyon' şeklinde tarif ettiği geniş çaplı bir savaşa dönüşmüştür. Birçok devletin 'Rusya'nın Ukrayna'yı işgali' olarak tanımladığı ve karşı çıktığı bu gelişme, yalnızca geleneksel askeri unsurların değil; aynı zamanda dijital araçların,

algoritmaların ve savaşlarının da yoğun şekilde kullanıldığı hibrit bir savaş modelini ortaya koymuştur. Bu süreçte sahadaki çatışmalar kadar sosyal medyada yürütülen bilgi savaşları, bot ve trol hesaplarla yapılan manipülasyonlar ve siber saldırılar da savaşın ayrılmaz bir parçası haline gelmiştir.

1.5.1. Savaşın Tarihsel ve Politik Arka Planı

Tarih boyunca Ukrayna, Rusya ile ciddi biçimde dini, kültürel ve dilsel benzerlikler taşıyan bir ülke olmuştur. İki ülkenin halkının da Slav kökenli oluşu, bu benzerlikleri daha da güçlendiren bir faktör olmuştur. Ancak değişen siyasi ve ideolojik yönelimler, zaman içerisinde kurulan farklı ittifaklar ve toplum zemininde ayrışmaya başlayan halklar iki ülke arasındaki ilişkilerin zaman zaman ciddi biçimde bozulmasına yol açmıştır. 1654'te Pereyaslav Antlaşması ile Ukrayna'nın bir kısmının Rusya egemenliğini isteyerek Ruslara katılması, toplumsal anlamda ayrışmanın ciddi bir boyutu olarak karşımıza çıkarken Çarlık Rusya ve Sovyetler Birliği döneminde Ukrayna halkına sürekli baskılar yapıldığı görülmüştür. İlk başlarda 'korumacı' bir tavır takınan Rusya'nın Ukrayna'ya yönelik ilişkilerini 'sömürgeci' bir şekle bürümesi Ukraynalıların sık sık isyan etmesine sebep olmuştur (Aydın, 2015, s. 37).

Sovyetler Birliği'nin 1991 yılında dağılması, Rus siyasi zihniyetinde derin bir kırılma noktası olmuştur. Yıllardır bölge ülkelerini kendi himayesi altında tutarak ABD karşısında yeni bir kutup ve güç dengesi yaratan birliğin dağılmasıyla 15 ülke bağımsızlık kazanmış, bunlardan birisi de Ukrayna olmuştur. Bağımsız bir ülke olarak, Rusya ile kurmuş olduğu ikili ilişkilerde zaman zaman yumuşamalar yaşansa da Ukrayna, üzerinde Rus baskısını her zaman hissetmiştir. Sovyetler Birliği'nin dağılmasıyla birlikte Rus siyasi zihniyetinde yaşanan kırılma özellikle Vladimir Putin'in liderliğinde ulusal gururun yeniden inşasıyla telafi edilmek istenmiştir. Putin, bu dönemi '20. yüzyılın en büyük jeopolitik felaketi' olarak nitelendirerek, Rusya'nın eski nüfuz alanlarını yeniden kazanmayı hedefleyen bir dış politika anlayışı geliştirmiştir. Bu anlayış doğrultusunda Ukrayna hem tarihi bağları hem de jeostratejik konumu nedeniyle Putin için çok daha özel bir önem kazanmış; özellikle 2004 Turuncu Devrimi ile başlayan Ukrayna'nın Batı ülkelerine entegrasyon süreci, Kremlin tarafından doğrudan bir tehdit olarak değerlendirilmiştir. Ukrayna'nın Avrupa ve NATO ile yakınlaşmasına karşı çıkan Rusya, 2014'te Kırım'ı ilhak etmiş ve Ukrayna'nın Donbas bölgesinde silahlı faaliyetlere

başlayan ayrılıkçı grupları destekleyerek Ukrayna'yla dolaylı bir çatışmaya girmiştir (Abdumaminova & Ayhan, 2024, s. 33). 2022'nin şubat ayında ise Rusya, Ukrayna'nın NATO'ya katılacağı iddialarını da gerekçe göstererek Donbas'a kapsamlı bir 'özel askeri operasyon' başlattığını duyurmuştur (Anadolu Ajansı, 2022). İlk başta Donbas ile sınırlı gösterilen bu operasyon, kısa sürede topyekûn bir işgal girişimine dönüşmüştür. Geline nokta itibariyle her iki tarafın da kayıpları yüzbinler ile açıklanırken, savaşın başlamasından itibaren 14,5 milyondan fazla Ukraynalı ülkesini terk etmek zorunda kalmış, her iki ülke de ciddi ekonomik kayıplar vererek çıkmaza sürüklenmiştir (Anadolu Ajansı, 2022).

Dolaylı olarak 2014 yılında başlayan ve 2022'de tam ölçekli konvansiyonel savaşa dönüşen Rusya-Ukrayna savaşı, yalnızca iki ülke arasında değil; aynı zamanda Avrupa'nın güvenliği ve uluslararası düzenin geleceği açısından da derin etkiler yaratmış, dünya ekonomisini ise birçok yönden olumsuz olarak etkilemiştir. İki ülkenin halkı arasındaki çatlak ve düşmanlık ise ciddi boyutlara ulaşmıştır.

1.5.2. Dijital Propaganda ve Trol Hesapların Savaştaki Rolü

Rusya-Ukrayna savaşında sahadaki askeri mücadelenin yanında sosyal medya üzerinden yürütülen propaganda savaşı da kitleler üzerinde ciddi etkiler yaratmakta ve modern çağın dolaylı mücadele biçimleri hakkında çıkarımlar yapılmasını sağlamaktadır. Bu kapsamda Rusya ve Ukrayna'nın sosyal medya üzerinden yürüttükleri propaganda stratejilerini anlamak oldukça önemlidir. Araştırma kapsamında Rusya tarafının trol faaliyetleri de dahil olmak üzere Ukrayna'ya yönelik sistematik bir algı savaşı yürüttüğü gözlemlenirken; Ukrayna tarafının daha çok savunma stratejileri benimsediği ve Rusya'nın algı operasyonlarına karşı uluslararası toplumda destek toplamak istediği anlaşılmıştır. Bu doğrultuda Ukrayna tarafı teyit platformlarına büyük önem verirken Batılı ülkeler ve askeri oluşumlardan da aktif şekilde destek almıştır. Ayrıca Ukrayna tarafında resmi olmamakla birlikte sivil kişilerin gönüllü gruplar kurarak Rusya tarafından gelen algı operasyonları ve dezenformasyonlara karşı sosyal medyada mücadele ettiği ve bu mücadelede karşı trol faaliyetlerinin de olduğu tespit edilmiştir.

1.5.2.1. Rusya'nın Dijital Propaganda Stratejileri

Propaganda, Rusya'nın tarihsel gelişiminde hem iç yönetimi sağlamlaştırmak hem de dış politikadaki hedeflerini desteklemek amacıyla sıklıkla başvurduğu temel araçlardan biri olmuştur. Çarlık rejiminden başlayarak Sovyetler Birliği döneminde ideolojik bir devlet politikası haline gelen propaganda, modern Rusya'da ise dijital teknolojilerin sunduğu imkanlarla daha sofistike ve yaygın bir yapıya bürünmüştür. Bu dönüşüm hem kitle iletişim araçlarının evrimi hem de küresel iletişim ağlarının genişlemesiyle doğrudan ilişkilidir.

Çarlık Rusyası'nda propaganda, dönemin sosyo-politik ihtiyaçlarına göre şekillenmiş, Ortodoks Kilisesi, bu propagandada ciddi bir rol üstlenmiştir. Çar'ın tanrısal yetkiyle donatıldığı fıkri halk arasında yaygınlaştırılarak otoritenin sağlamlaştırılmaya çalışması bunun önemli bir göstergesidir. Ayrıca bu dönemde Rusya'nın, Bizans ve Roma'nın varisi olduğu iddiası da Rus halkında tarihsel ve dini bir aidiyet duygusu yaratmayı hedeflemiştir. 1917 Ekim Devrimi'nden sonra Bolşeviklerin Rusya'da kontrolü ele geçirmesi ve Sovyetler Birliği'nin kurulmasıyla Rus propagandası, tarihinin en sofistike dönemlerinden birine başlamıştır. Kurulan istihbarat örgütleri ve ilgili devlet kurumlarıyla, Sovyetler Birliği içindeki ülke halklarını mobilize etmek, kontrol altında tutmak ve hasım ülkelere yönelik karalama kampanyaları yürütmek için propaganda çalışmalarına büyük önem verilmiştir. Geleneksel medya aletlerinden faydalanan bu dönemde, psikolojik savaşa ve kültürel propagandaya da sıkça başvurulmuş, iki kutup arasında seçim yapmak zorunda kalan devletlerden destek almak amaçlanmıştır (Kowal vd., 2016, s. 28).

Sovyetler Birliği'nin dağılmasından birkaç sene sonra, 2000 yılında Rusya yönetimini devralan Vladimir Putin döneminde propaganda, yalnızca geleneksel medya araçlarıyla değil; aynı zamanda dijital teknolojilerle de desteklenen çok katmanlı bir stratejiye dönüşmüştür. Sovyet döneminden devralınan anlayış, internetin sunduğu yeni imkanlarla yeniden yapılandırılmıştır. Devlet destekli medya organları, uluslararası kamuoyuna yönelik İngilizce içerikler üretirken, Rus kamuoyuna yönelik olarak da milliyetçi söylemler, dış tehdit algısı ve tarihsel travmalar ön plana çıkarılmıştır. 2014'teki Kırım ilhakı sırasında sosyal medyada yürütülen bilgi operasyonları, Rusya'nın dijital propaganda kapasitesini ortaya koymuştur. Yerel halkın desteğini göstermek,

Ukrayna yönetimini gayrimeşru göstermek ve Batı kamuoyunda kafa karışıklığı yaratmak amacıyla pek çok manipülatif video ve haber devreye sokulmuştur. 2016 ABD başkanlık seçimlerinde ise bu strateji uluslararası bir boyut kazanmıştır. IRA gibi yapılar aracılığıyla, Amerikalı seçmenlerin kutuplaşmasını artırmaya ve belirli adaylara destek sağlamaya dönük içerikler üretilmiş, bunlar sosyal medya platformlarında yaygınlaştırılmıştır. Bu dönemde bot hesaplar, sahte haber portalları ve organize trol faaliyetleri üzerinden yürütülen propaganda çalışmaları, dezenformasyonun küresel bir tehdit haline gelmesinin en dikkat çekici örneklerinden biri olmuştur (Kowal vd., 2016, s. 29).

1.5.2.1.1. Devlet Destekli Trol Faaliyetleri

Devlet destekli trol faaliyetleri, genellikle belli bir devletin kurum ya da kuruluşları tarafından istihdam edilen veya sözleşmeli olarak çalıştırılan, sahte sosyal medya hesapları oluşturan ve yöneten grupların, sosyal medyada yürüttükleri manipülasyon faaliyetleridir. Bu faaliyetler, yanlış bilgi yaymak, belirli anlatıları güçlendirmek ve hedef alınan düşmanlara karşı tacizde bulunmak için kullanılmaktadır. Özel işyerlerinde çalışan ya da bireysel olarak trol faaliyetleri yürütenlere kıyasla çok daha sistematik ve daha güçlü imkanlara sahip olan bu trol grupları, özellikle günümüz dijital dünyasında tam anlamıyla bir ‘modern propaganda faaliyeti’ yürütmektedir.

Rusya’nın devlet destekli trol ağları, şu anda dünyadaki en etkili ‘dijital propaganda’ ve ‘bilgi savaşı’ mekanizmalarından birisi olarak öne çıkmaktadır. Bu yapılar hem ülke içinde kamuoyunu yönlendirmek hem de uluslararası arenada dezenformasyon stratejileri yürütmek amacıyla etkili bir araç olarak kullanılmaktadır. 2013 yılında Rus araştırmacı gazetecilerin bulgularıyla trol faaliyetleri yürüttüğü ortaya çıkartılan IRA, Rusya’nın ‘devlet destekli trol ağı’ iddialarında en çok adı geçen kuruluş olmuştur. Bahsi geçen yapının bünyesinde oluşturulan organizasyon şemasında ‘yorumcular birimi’, ‘blog yazarları birimi’, ‘gazeteciler’, ‘sosyal medya uzmanları birimi’, ‘hızlı tepki birimi’ gibi bölümlerin olduğu iddia edilmektedir. Bu iddiaların doğru olduğu düşünüldüğünde IRA’nın oldukça kapsamlı ve planlı bir işleyişi olduğu göze çarpmakta, yapı içerisinde ‘gazeteci’ sıfatındaki kişilerin de yer aldığı anlaşılmaktadır. İlk kurulduğu dönemde ağırlıklı olarak Rusça içerikler üreten ve ana hedefinin Rusya’nın iç siyaseti olduğu belirtilen IRA kurulduktan 1 yıl sonra 2014’te, İngilizce içerikler de üretmeye başlamış

ve hedefleri arasına Batı ülkelerini de koymuştur. 2014'te Rusya tarafından Kırım'ın ilhak edilmesinde hem Rus kamuoyunu hem de dünya kamuoyunu ikna etmeye yönelik olarak aktif şekilde çalışan IRA merkezinde, alanında uzman isimlerin çalışanlara iç ve dış siyaset hakkında bilgi verdikleri, hedefteki ülkelerin ya da grupların sosyolojik zaafaları, ses getirme potansiyeline sahip olayları gibi konularda detaylı olarak sunumlar yaptıkları belirtilmektedir (Nimmo & Toler, 2018). 2016 ABD Başkanlık Seçimleri'ne müdahale ettiği iddialarıyla tanınan IRA özellikle, 2022'de başlayan Rusya-Ukrayna Savaşı ve muhalif Rus politikacı Boris Nemtsov suikasti gibi kritik dönemlerde Rus hükümetinin 'dezenformasyon operasyon merkezi' olmuştur. ABD Senatosu İstihbarat Komitesi'nin 2020'de yayınladığı rapora göre, IRA, sosyal medya üzerinden dezenformasyon yayarak ABD seçmenlerini etkilemeye çalışmış ve bu çalışmalar, toplumsal bölünmeleri artırarak iç karışıklığı hedeflemiştir (U.S. Department of Justice).

1.5.2.1.2. Dezenformasyon Kampanyaları

Rusya, sadece trol fabrikaları ile dezenformasyon yapmakla kalmamış aynı zamanda devlet destekli, yurtiçi ve yurtdışı yayın yapan televizyon kanallarını da bir propaganda aleti olarak kullanmıştır. Russia Today (RT), Sputnik News, Sovyetler Birliği Telgraf Ajansı (TASS), Russia-1 gibi kanallar devlet tarafından desteklenmekte ve yalnızca televizyonda değil sosyal medya gibi mecralarda da yayın yaparak Rus Hükümeti'nin dijital propagandasını yürütmektedirler. Ulusal ve uluslararası kamuoyunu etkilemek için sistematik çabalar harcayan bu kanallar, farklı ülke temsilcilikleri aracılığıyla Rusya hakkında olumlu haberler hazırlayarak, faaliyet yürüttükleri ülkelerde algı çalışmaları yapmaktadırlar (Paul & Matthews, 2016, s. 7-10).

Rusya'nın, dezenformasyon kampanyalarını, Türkçe'ye 'yalan yangını hortumu' ya da 'yalanların şelalesi' olarak çevrilen 'firehose of falsehood' yöntemiyle yürüttüğü görülmektedir. İlk olarak ABD kaynaklı RAND Corporation'un yayınladığı bir raporda değinilen bu yöntemin temel stratejisi, yüksek hacimli, sürekli, hızlı, çok kanallı ve tekrarlayıcı bilgi akışına dayanmaktadır. Devlet tarafından desteklenen resmi haber kanalları başta olmak üzere uygulanan bu strateji, yaşanan gelişmelere hızlı tepki verme ve sürekli olarak benzer mesajları tekrarlama üzerine kuruludur. Gerçeklikten bağımsız olarak, olaylar hakkında hükümet lehine hızla yorumlar yapılır ve bu yorumlar sürekli olarak tekrarlanır. Böylece, hedef kitlenin ilk izlenimlerini şekillendirmeyi ve bu

izlenimlerin pekiştirilmesi amaçlanır (Paul & Matthews, 2016, s. 4-6). Buna benzer bir yöntemin İkinci Dünya Savaşı sırasında Nazi Almanyası'nda gözlemlendiği de bilinmektedir. Adolf Hitler'in propagandadan sorumlu bakanı Joseph Goebbels tarafından sık sık dillendirilen propaganda tekniği 'her yerde her zaman her an propaganda' ilkesi üzerine kuruluydu. Bu, propaganda mesajlarının kitleler tarafından daha kolay kabul edilmesini sağlıyor, mesajları daha tanıdık ve inandırıcı hale getiriyordu.

Rusya kaynaklı olarak hazırlanan ve ciddi bir dezenformasyon örneği olan bazı 'deepfake' (derin-sahte) içerikler de son dönemde oldukça dikkat çekmektedir. Genelde video içeriklerine yapılan manipölasyonlar ile içerikteki suratları farklı suratlarla değiştirme işlemi olan deepfake, son dönemde pek çok tanınmış kişinin maruz kaldığı bir dezenformasyon yöntemidir. 2022 yılında başlayan Rusya-Ukrayna savaşında, Ukrayna devlet başkanı Volodimir Zelenski'ye yönelik yapılan bir deepfake video içeriğinde, Zelenski'nin ordusuna 'silah bırakın' çağrısı yaptığı görülmektedir. Tartışmalara neden olan video Ukrayna tarafınca hızla yalanlanmış fakat sosyal medyada ciddi şekilde etkileşim almıştır (Burgess, 2022).

1.5.2.1.3. Siber Saldırıları ve Bilgi Savaşları

Siber saldırılar ve bilgi savaşları birbirinden farklı iki alan olsa da aslında birbirleriyle bağlantıları bulunmaktadır. Siber saldırılar, dijital sistemlere yetkisiz erişim sağlanarak bilgiye zarar verme, verileri ele geçirme ya da sistem işleyişini bozma amacı taşıyan kasıtlı ve planlı müdahalelerdir. Bu tür saldırılar, bireylerden devletlere kadar geniş bir yelpazede ciddi güvenlik tehditleri yaratmaktadır. Bilgi savaşı ise rakip aktörler karşısında psikolojik, stratejik ve operasyonel üstünlük elde etmek amacıyla bilgi ve iletişim teknolojilerinin sistematik biçimde kullanıldığı çok boyutlu bir mücadele biçimidir. Bu kapsam, siber saldırılar gibi dijital yöntemleri de içerebilir ve hem askeri hem de sivil hedeflere yönelik olarak uygulanabilmektedir. Rusya, trol orduları aracılığıyla yürüttüğü sistematik dezenformasyon faaliyetleri kadar siber saldırılar ve bilgi savaşları düzenleme potansiyeli ve altyapısı açısından da dünyadaki güçlü bir örnek olarak karşımıza çıkmaktadır (Topçu, 2022, s. 26).

Özellikle 2000'li yıllardan itibaren Rusya, siber güvenlik alanında stratejik adımlar atan ve bu alana erken dönemde yatırım yapan öncü devletlerden biri olmuştur.

Sovyetler Birliđi'nin dađılmasının ardından Rusya, teknolojik gelişmelerle birlikte geleneksel istihbarat yöntemlerini dijital yeteneklerle harmanlama yoluna gitmiştir. Bu stratejik evrim, Rusya'nın yalnızca konvansiyonel deđil, aynı zamanda siber alanda da 'asimetrik savaş' tekniklerini benimseyerek küresel ölçekte tehdit oluşturan bir aktöre dönüşmesini sağlamıştır. Devlet destekli hacker grupları, resmi kurumlar ve sosyal mühendislik uygulamaları, Rusya'nın siber saldırılar ve bilgi savaşlarındaki etkinliğini arttıran birer faktör olarak karşımıza çıkmaktadır (Topçu, 2022, s. 29).

Rusya'nın en büyük istihbarat teşkilatı olan Rus Ana İstihbarat Müdürlüğü (GRU)'nün, siber saldırılar kapsamında 'ana karargâh' görevi gördüğü düşünülmektedir. ABD Federal Soruşturma Bürosu (FBI)'nin aktardığı bilgilere göre GRU ajanları, uluslararası ölçekte zararlı yazılım dağıtımı yapmakta ve siber saldırılar düzenlemektedir. Bu ajanların kimlik hırsızlığı, korunan bilgisayarlara siber saldırılar ile zarar vermek ve dolandırıcılık yapmak gibi dar kapsamlı suçlar işlemenin yanında; kritik altyapı saldırıları, siyasi seçimlere müdahale ve uluslararası sabotajlar gibi geniş ölçekli suçları işledikleri de iddia edilmiştir (FBI, 2020).

GRU'nun, özellikle uluslararası alanda düzenlemiş olduğu siber saldırılarda genel olarak ABD ve Ukrayna'nın hedef alındığı görülmektedir. 2017 yılında gerçekleştirilen NotPetya Saldırısı, dünya çapında büyük ses getirmiştir. Microsoft Windows tabanlı sistemleri hedef alan NotPetya, kötü amaçlı bir yazılım türüdür. Bu yazılım ilk olarak 2017'de kullanılmış ve Ukrayna'yı hedef alan önemli bir küresel siber saldırıda kullanılmıştır (IKosmos, 2020). Ukrayna'daki bankalar, enerji şirketleri ve hükümet sistemlerini hedef alan bu saldırı, küresel çapta da etki etmiş ve Maersk, Merck gibi şirketlere 1 milyar dolarlık bir zarar vermiştir. GRU ajanlarının düzenlediği siber saldırılar ABD Adalet Bakanlığı raporlarına da yansımış ve Ukrayna, Fransa, Gürcistan gibi ülkelerde yapılan seçimlere müdahale edildiği belirtilmiştir. Söz konusu raporda, GRU'nun geniş siber saldırı faaliyetleri kapsamında Ukrayna'da elektrik kesintilerine neden olan 'KillDisk' ve 'Industroyer' saldırısı ile 2018 Pyeongchang Kış Olimpiyatları'na yönelik yapılan ve binlerce bilgisayarı bozan 'Olympic Destroyer' saldırısına da yer verilmiştir (U.S. Department of Justice, 2020).

1.5.2.2. Ukrayna'nın Dijital Karşı Stratejileri

Rusya'nın, Ukrayna'ya karşı yıllardır süren saldırıları 2022 yılında geniş kapsamlı, aynı zamanda Rusya'nın dijital kapasitesini de sahaya sürdüğü hibrit bir savaşa evrilmiştir. Ukrayna, bu saldırılar karşısında çeşitli silah sistemlerinden oluşan savunma teknolojilerinden ziyade siber savunma teknolojileri ile de önlemler almaya mecbur kalmıştır. Hem siber saldırılarla hem de yoğun dezenformasyon kampanyalarıyla mücadele etmek zorunda kalan Ukrayna, dijital savunma konusunda batılı ülkelerden aktif şekilde destek alarak Rusya'ya karşı koymaya çalışmıştır.

Rusya'nın siber saldırılarına ve dezenformasyon üzerine kurulu stratejilerine yönelik uluslararası kurum ve kuruluşlarla iş birliği yürüten Ukrayna, NATO, Avrupa Birliği ve ABD gibi aktörlerle yaptığı ortak çalışmalar sayesinde dijital savunma kapasitesini önemli ölçüde artırmıştır. Rus saldırılarına karşı teknik destek, kapasite geliştirme, mali yardım ve çok yönlü stratejileri içeren iş birliğinde ABD, Ukrayna'ya siber savunması için doğrudan ve dolaylı olarak milyarlarca dolarlık yardım sağlamıştır. 2022'de ABD Kongresi, Ukrayna'ya 40 milyar dolarlık bir yardım paketini kabul etmiş ve bu paket içerisinde siber güvenlik altyapısını destekleyen fonlar da yer almıştır. Amerika Birleşik Devletleri Siber Komutanlığı (USCYBERCOM), Ukrayna'ya yönelik siber tehditler karşısında aktif rol üstlenmiş; gerçek zamanlı tehdit istihbaratı paylaşımı yoluyla Rusya kaynaklı dijital saldırıların etkisiz hale getirilmesine katkı sağlamıştır. Bu iş birliği ABD açısından, yalnızca Ukrayna'yı savunma amacıyla değil, aynı zamanda Rusya'nın siber faaliyetlerinin tespiti ve önlenmesi açısından da stratejik bir öneme sahiptir. Fakat 2024 ABD'de yapılan seçimler sonrası ülke yönetimine gelen Donald Trump, Ukrayna-Rusya savaşına diplomatik yollarla çözüm bulunması hedefi doğrultusunda, ABD'nin Rusya'ya karşı yürüttüğü siber operasyonları sonlandırma kararı almıştır (Nigrelli, 2025).

Dünyanın en önemli askeri organizasyonlarından birisi olarak NATO, Rusya-Ukrayna savaşını çok yakından takip eden diğer bir aktördür. NATO Genel Sekreteri Jens Stoltenberg, Rusya-Ukrayna savaşının başladığı ilk aylarda, NATO'nun Ukrayna için siber güvenlik ve gerekli teknik ekipman yardımı yapma kararı aldığını açıklamıştır. Bu kararın temel sebebinin Ukrayna'ya yönelik olası kimyasal, biyolojik ve nükleer saldırıları önlemek olduğunu açıklayan Stoltenberg, bu yardımların yalnızca savunma

amaçlı olacağının altını çizmiştir (Anadolu Ajansı, 2022). NATO'ya bağlı olan İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi (CCDCOE), yapılan siber yardımın merkezinde yer almıştır. Her yıl düzenli olarak tatbikatlar düzenleyen CCDCOE, uzmanlar aracılığıyla Ukraynalı yetkililere eğitimler vermiş ve danışmanlık faaliyetleri de yürütmüştür. Ukrayna Milli Güvenlik ve Savunma Konseyi (NSDCU) direktörü Nataliya Tkachuk, bu iş birliği sayesinde NATO ülkelerinin siber tehditlerle ilgili daha detaylı tecrübe edeceklerini savunmuş ve Ukrayna'nın bu tecrübe için oldukça uygun bir saha olduğunu vurgulamıştır. Aslında Tkachuk'un bu açıklamaları Rus siber saldırılarının boyutunu ve oluşturdukları tehdidi de dolaylı olarak göstermiştir.

Rusya-Ukrayna savaşının başladığı andan itibaren ciddi askeri yardımlar yapan diğer bir kuruluş da AB olmuştur. AB, siber savaş konusunda özellikle dezenformasyon ve trollere yönelik çalışmalara odaklanarak Rusya'nın medyadaki manipülatif faaliyetlerini ve trol ordularını bertaraf etmeye çalışmıştır. Bu kapsamda AB, çeşitli medya okuryazarlığı eğitimleri vererek toplumdaki farkındalığı arttırmış, siber savunma sistemlerini uzun vadede kapasite geliştirmek ve hibrit tehditlerle mücadele etmek gibi alanlarda geliştirmek için faaliyetler yürütmüştür. Avrupa devletleri başta olmak üzere yürütülen bağış kampanyaları kapsamında oluşturulan Tallinn Mekanizması ile de Ukrayna'ya siber güvenliğini sağlamak ve daha da iyileştirmek için para toplanmıştır (Antoniuk, 2023).

Ukrayna'nın kendi bünyesinde kurmuş olduğu Ukrayna Devlet Özel İletişim Servisi (SSSCIP) gibi birimler siber savunma konusunda faaliyetler yürütse de Rusya'nın siber kabiliyeti yanında güçsüz kalmaktadır. Özellikle 2022'de Rusya ile başlayan savaş sonrasında Ukrayna'nın siber savunması genel olarak batılı devletler ve batılı askeri yapılar tarafından düzenlenmiştir.

1.5.2.2.1. Sivil Siber Direniş ve Dijital Aktivizm

Rusya'nın, Ukrayna'yı topyekûn işgal girişimini başlattığı 'özel askeri operasyonuna' ilk günden itibaren sivil vatandaşlar da karşı koymuş ve Rus askerlerine şehirlerini vermeme konusunda direnmişlerdir. Medyada geniş yer bulan Ukraynalı siviller, Rusya tarafına karşı taktiksel olarak üstün olamasalar da işgalci birliklere psikolojik olarak baskılar yaşatmışlar, moral olarak güç kaybettirmişler ve uluslararası çapta ise Ukrayna lehine bir izlenim oluşturmuşlardır. Yer yer Rus birlikleri ile sokak

çatışmalarına da dönen sivil direniş, dijital dünyaya da yansımıştır. Ukrayna'nın askeri olarak Rusya'ya karşı yürüttüğü siber savunma stratejilerinden farklı olarak Ukraynalıların sivil siber direnişi ve dijital aktivizmi de dikkat çekmektedir (Hollanda Hükümeti, 2024).

Sivil siber direniş, bireylerin ve sivil toplum aktörlerinin dijital araçlar yoluyla otoriter ya da işgalci güçlere karşı yürüttükleri direnç faaliyetlerini ifade eder. Bu faaliyetler, 'hackleme' girişimleri ya da siber savunma stratejileri gibi teknik uygulamaları içerebilir. Dijital aktivizm ise sosyal medya ve internet tabanlı platformlar üzerinden farkındalık oluşturma, kamuoyu mobilizasyonu sağlama ve siyasi değişim talep etme amacı güden eylemler bütünüdür. Her iki strateji de dijital çağın toplumsal mücadele biçimlerini dönüştürmüş ve bireylerin çevrimiçi alanda kolektif hareket kapasitesini artırmıştır (Tuna & Türkölmez, 2023, s. 214).

Rusya'nın 2022 yılında başlayan işgal girişimiyle Ukraynalı yazılımcılar, aktivistler ve sıradan vatandaşlar, dijital beceri ve olanaklarını kullanarak Rusya'nın dezenformasyon kampanyalarına karşı koymak, devlet kurumlarını savunmak ve uluslararası kamuoyunu harekete geçirmek adına birçok dijital eylemde bulunmuşlardır. Ukrayna resmi birimleri bu süreçte, düzensizliğin önüne geçmek ve daha sistematik eylemler gerçekleştirmek amacıyla 'gönüllü ordular' geliştirmiştir (Schulze & Kerttunen, 2023, s. 4-6). Bunlardan bir tanesi olan Ukrayna Bilişim Teknolojileri Ordusu (ITAU), Ukrayna Savunma Bakanlığı ile iş birliği içinde olan ve gönüllü hackerlardan meydana gelen bir 'dijital direniş' grubudur. Hem Ukraynalı hem de uluslararası gönüllülerden oluşan bu yapı, Rus devlet kurumlarına, finans kuruluşlarına ve medya organlarına yönelik siber saldırılar düzenlemektedir. Amaçları arasında web sitelerini çökertmek, bilgi sızdırmak ve Rus dijital altyapısında kesintiler yaratmaktır. ITAU, Telegram üzerinden organize edilmekte ve gönüllülere saldırı yapılacak hedeflerin listesi bu platform üzerinden iletilmektedir. Bu örnek, sivil siber direnişin bir devlet çatısı altında organize edilerek hibrit savaşın bir parçası haline gelebileceğini göstermesi bakımından dikkat çekicidir (Council on Foreign Relations, tarih yok). Ayrıca Ukraynalı dijital aktivistler, ülkede yaşanan durumları sosyal medya vasıtasıyla aktif olarak yaymakta ve mücadeleleri için destek toplamaya çalışmaktadırlar.

Dijital çağda sivil direniş, geleneksel eylem biçimlerinin çevrimiçi mecralara taşınmasıyla yeni bir boyut kazanmıştır. Artık protestolar yalnızca sokaklarda değil, sosyal medya kampanyaları, hashtag hareketleri ve dijital eylemler yoluyla da gerçekleştirilmektedir. Bu yeni direniş biçimi, daha geniş kitlelere ulaşma, sansürü aşma ve uluslararası farkındalık yaratma açısından önemli avantajlar sunmaktadır. Ancak bu süreç aynı zamanda yeni etik ve hukuki tartışmaları da beraberinde getirmiştir. Özellikle yürütülen hacker faaliyetleri, gibi dijital eylemler, bazı ülkelerce yasa dışı kabul edilmekte, siber saldırılarla bireylerin ya da kurumların hedef alınması tartışmalara neden olmaktadır. Yine bu konuda Ukrayna yanlısı trol faaliyetler de tartışma konusu olmakta ve ‘mağdur durumda olmaları trollük yapmalarını haklı kılar mı’ sorusunu akıllara getirmektedir.

1.5.2.2.2. Doğrulama Platformları ve Karşı-Propaganda Mekanizmaları

Yaşadığımız yüzyılda dijital içeriklerin hızla üretilip paylaşılması, doğru bilgi kadar yanlış bilginin yayılmasına da sebep olmuştur. Bu durum, dijital bilgi ortamını karmaşıktırılmış, kamuoyunun sağlıklı bilgiye ulaşmasını zorlaştırmış ve doğru olan bilgilere de şüphe ile bakılmasına sebep olmuştur. Özellikle savaş ve çatışma dönemlerinde rakip ülkelerin birbirlerine karşı kullandığı propaganda faaliyetlerinin bir parçası olarak bilinçli şekilde dolaşıma sokulan yanlış bilgiler, büyük kitleleri hedef aldığı için ciddi sonuçlar doğurabilmektedir. Bu bağlamda, doğrulama/teyit platformları, bilgi kirliliğine karşı önemli bir savunma mekanizması olarak öne çıkmaktadır. Söz konusu platformlar, kamuoyunun yanıltılmasını engellemeyi, bilgi güvenini yeniden tesis etmeyi ve demokratik süreçlerin şeffaf biçimde işlemesine katkı sunmayı amaçlamaktadır.

Ukrayna, Rusya ile yaşadığı mücadelede yanlış bilgilerin etkisini azaltmak ve kamuoyunu doğru bilgilendirmek için teyit platformlarından oldukça yararlanmıştır. Hem saldırı altındaki taraf olması hem de rakibi Rusya’nın köklü propaganda stratejileri ve yapıları olması sebebiyle Ukrayna, kendi kamuoyuna karşı moral vermek için de teyit platformlarına büyük önem vermiştir. Bu kapsamda Ukrayna kaynaklı Stop Fake, Vox Check, Ukraine Facts, Fact Check Ukraine gibi platformlar ön plana çıkmaktadır.

Ukrayna’daki teyit platformlarının büyük çoğunluğu devletten bağımsız olarak genellikle akademisyenler, gazeteciler ve sivil toplum aktörlerinden oluşan uzman ekiplerce oluşturulmuştur. Tarafsızlık ve şeffaflık ilkeleri doğrultusunda yapılandırılan bu

platformlar hem yerel kamuoyuna hem de uluslararası kitlelere ulaşmak için Ukraynaca, Rusça ve İngilizce başta olmak üzere çok dilli şekilde hizmet vermektedir (Baptista, Roca, Gradim, & Loureiro, 2023, s. 29). Bu oluşumların devlete ait muadilleri ise bizzat Ukrayna'nın resmî kurumlarınca hazırlanmış olan Dezenformasyonla Mücadele Merkezi (CCD) ve Stratejik İletişim ve Bilgi Güvenliği Merkezi (CSCIS)'dir. Ottawa Üniversitesi'nden Profesör Paul Robinson ise Ukrayna'nın 'teyit' platformlarını taraflı bulduğunu dile getirmiş ve adı geçen platformların, kendi görüşleriyle uyuşmayan her haberi ve görüşü 'dezenformasyon' olarak nitelediğini iddia etmiştir. Robinson, bu platformların çoğunlukla nesnel araştırmalar yapan bağımsız araştırmacılardan oluşmadığını ve Avrupa Birliği ülkeleri tarafından fonlanarak yayın yaptıklarını savunmuştur (Robinson P. , 2021).

Ukrayna'daki resmi ve sivil teyit platformları, bilgi güvenliğinin sağlanmasında önemli bir rol üstlenmektedir. Ancak, doğrudan savaşın taraflarından biriyle ilişkili oldukları için 'mutlak tarafsızlık' içinde hareket ettikleri konusunda şüpheler oluşmaktadır. Öte yandan, Rusya'nın ise bu doğrulama girişimlerini hedef alarak onların güvenilirliğini sarsmaya yönelik organize bir karşı propaganda stratejisi yürüttüğü düşünülebilir. Bu çerçevede, enformasyon savaşı yalnızca dijital içeriklerin değil, algıların ve güvenin de hedef alındığı karmaşık ve çok boyutlu bir mücadele alanı olarak görülmektedir.

İKİNCİ BÖLÜM

SOSYAL MEDYADA DİJİTAL PROPAGANDA: TROL FAALİYETLERİ, KAMUOYU ÜZERİNDE ETKİLERİ VE FAALİYETLERE YÖNELİK KARŞI STRATEJİLER

Sosyal medyanın gelişimi ve günlük hayata girmesiyle birlikte dünya çapında ciddi bir iletişim devrimi yaşanmıştır. Kitleler arasında hızla yaygınlaşan sosyal medya platformları aracılığıyla insanlar arası iletişimde mekan ve zaman kısıtı büyük ölçüde ortadan kalkmıştır. Bu teknolojiler aynı zamanda kitlelerin bilgiye ulaşma hızını da ciddi ölçüde etkilerken, bilginin doğruluğu konusunda büyük tartışmalara ve belirsizliklere de sebep olmuştur. Özellikle son dönemde literatüre girmeye başlayan sosyal medya trolleri ise bu dönemin önemli aktörleri olarak karşımıza çıkmaktadır.

2.1. Sosyal Medyada Trol Ordularının Stratejileri

Günümüzde sosyal medya, yalnızca bireyler arasındaki iletişimi kolaylaştıran bir mecra olmaktan çıkarak, devletler ve siyasi aktörler için etkili bir propaganda ve manipülasyon aracı haline gelmiştir. Bu süreçte, ‘trol orduları’ olarak tanımlanan organize yapılar, kamuoyunun algısını şekillendirmek, muhalif görüşleri bastırmak ve belirlenen siyasi gündemleri desteklemek amacıyla sistematik stratejiler geliştirmekte ve uygulamaktadır.

2.1.1. Yapay Kamuoyu (Astroturfing)

Dijital çağda kitleleri yönlendirmek için kullanılan etkili bir strateji olarak astroturfing kavramı da karşımıza çıkmaktadır. Terim, ilk kez 1985 yılında ABD’li senatör Lloyd Bentsen tarafından kullanılmıştır. Bentsen, sigorta sektörünün, halktan gelen doğal bir destekmiş gibi görünen mektupları hedef alarak yaptığı manipülasyonu eleştirmiş, ‘‘Bir Teksaslı, gerçek halk desteğini (grassroots) Astroturf’tan (yapay çim) ayırt edebilir’’ demiş ve bu kavramı dile getirmiştir (Şahin, 2023). ‘Astroturfing’ stratejisi, sahte bir halk desteği görüntüsü oluşturarak, gerçek bir toplumsal hareket yaratma amacı gütmektedir. Araştırmacı Edward Walker’a göre astroturfing, ‘kurumsal veya politik aktörler tarafından finanse edilen, ancak halk tabanlı olduğu izlenimi verilen stratejik girişimler’dir (Walker & Le, 2023, s. 189-191). Bu tür organize kampanyalar, toplumu manipüle etmek ve bireylerin algısını değiştirmek amacıyla özellikle sosyal medya

platformlarında yaygın bir şekilde uygulanmaktadır. Son yıllarda ise trol orduları, astroturfing yöntemini dijital propaganda ve bilgi savaşlarının önemli bir bileşeni olarak kullanmaktadır.

Psikolog Dr. Robert Cialdini'nin 'sosyal kanıt' teorisine göre bir kişi, belirli bir durumda nasıl davranması gerektiğini bilmiyorsa, başkalarının davranışlarını gözlemleyerek kendi davranışını şekillendirmektedir. Özellikle belirsizlik anlarında insanlar, çevrelerindeki tepkilerini ve eylemlerini doğru davranışın göstergesi olarak kabul ederler. Robert Cialdini tarafından dile getirilen bu görüşe, propaganda ve reklamcılık gibi alanlarda bireylerin yönlendirilmesi için sıkça başvurulmaktadır (Bozkanat & Göksu, 2020, s. 87). Bu bağlamda çevrimiçi ortamda ve özellikle sosyal medya platformlarında siyasi partiler, şirketler ya da çıkar grupları, asıl amaçları doğrultusunda, kamuoyunun kendiliğinden ortaya koyduğu bir fikir veya desteği yaratıyormuş gibi sahte paylaşımlar düzenlemektedirler. Bot hesaplar ve trol ağları üzerinden geniş kitlelere yayılan mesajlarla 'organik çoğunluk illüzyonu' oluşturmayı hedefleyerek astroturfing yöntemi devreye sokulmaktadır. Sosyal medyada, bir ürün ya da politika hakkında, gerçeği yansıtmayan çok sayıda olumlu yorum yapılabilen veya belirli bir görüşün geniş kitlelerce desteklendiği algısı yaratılabilmektedir. Bu tür yapay etkileşimler, sosyal medya platformlarının geri bildirim sistemlerinden de yararlanarak, gerçekte mevcut olmayan bir destek ağı izlenimi yapmakta ve bireylerde sahte bir 'sosyal onay' algısı oluşturabilmektedir. Beğeni, paylaşım, yorum sayısı, içerik izlenme oranları veya trend başlıklar gibi ölçülebilir göstergelerin fazlalığı bu süreçte kilit rol oynamaktadır. Örneğin, Facebook'ta bir gönderinin aldığı beğeni ve yorum sayıları, YouTube'daki izlenme rakamları ya da Twitter'daki trend konular, kullanıcılarda bu içeriklerin popüler ve güvenilir olduğu algısını oluşturmaktadır. İnsanlar, bu tür 'sosyal kanıt' işaretlerini 'başkaları zaten bunu onaylamış' biçiminde yorumlayarak etkileşim gösterme eğilimindedir. Çevrim içi platformlarda bu eğilimi desteklemek için 'milyonlarca kişi izledi' veya 'geniş destek gördü' gibi ifadelerle pazarlama da yapılmaktadır (Buchanan, 2020).

2019–2020 arasında hukuki tartışmalar ve talepler sebebiyle ortaya çıkan Hong Kong protestoları sırasında, Çin hükümetine yakın trol grupları sosyal medyada yoğun bir astroturfing faaliyeti yürütmüştür. Bu gruplar, Hong Kong'daki muhalif sesleri bastırmak ve Çin'in politikalarını desteklemek amacıyla organize bir şekilde içerik

üretmişlerdir. Haziran 2020’de Twitter, Hong Kong karşıtı mesajlar ve ABD’yi itibarsızlaştırmaya yönelik içerikler yayan 150 binden fazla hesabı platformdan kaldırmıştır. Bu hesapların çoğunun, ‘50 Cent Partisi’ olarak bilinen trol ordusunun bir parçası olduğu iddia edilmiştir. Çin devlet medyası ise zaman zaman bu sahte hesapların paylaşımlarını haberleştirerek, geleneksel medya yoluyla sosyal kanıt etkisini güçlendirmiştir (Kharpal, 2020). Sözgelimi, sahte hesaplarca yayılan #HongKong etiketleri Twitter’da trend olduğunda, birçok gerçek kullanıcı bu konunun doğal olarak popülerleştiğini düşünerek etkileşime geçmiş, böylece aslında az sayıda aktör tarafından desteklenen görüşler, geniş kitlelerce meşru algılanmaya başlanmıştır.

2.1.2. Zaman ve Örgütlenme Açısından Koordineli Saldırıları

Sosyal medyada zamana ve örgütlenmeye dayalı koordineli saldırılar, trol ordularının birçok sahte hesap ve duruma göre bot hesaplar da kullanarak, eş zamanlı şekilde belirli hedeflere yönelik organize saldırılar gerçekleştirmelerini ifade eder. Planlı olarak kullanılan bu yöntem, yanlış bilgiyi daha geniş ölçekte yayabilme, gerçek bilgilerin görünürlüğünü azaltma, eleştirileri susturma gibi amaçlara yönelik başarılar kazanabilmektedir. Bireysel trol eylemlerinden çok daha etkili olan koordineli saldırılar, sosyal medya kullanıcıları üzerinde astroturfing etkisi yapabilmektedir (Assardo, 2023).

Koordineli saldırılarda belli zamanlara göre ve örgütlü biçimde yapılan eylemler hem sosyal medya algoritmalarını etkilemekte hem de kamuoyunda istenilen algıyı oluşturmakta kritik bir rol oynamaktadır. Zamanlama stratejileri, sosyal medyanın işleyiş dinamikleri dikkate alınarak kurgulanmaktadır. Özellikle kullanıcıların en yoğun çevrimiçi olduğu saatler, gündem oluşturma faaliyetleri için özellikle tercih edilmektedir. Bu dönemlerde yapılan yoğun içerik akışı, sosyal medya platformlarındaki algoritmaların ‘trend içerik’ sinyallerini tetikleyerek, mesajların daha geniş kitlelere ulaşmasına olanak tanır. Bunun yanı sıra, kriz anları, seçim süreçleri ya da toplumsal hassasiyetlerin yüksek olduğu olaylar, koordineli saldırıların yürütülmesi için özellikle seçilmektedir çünkü bu dönemlerde yapılan müdahaleler, kamuoyu algısını etkilemede daha etkili olabilmektedir (Ferrara vd., 2016, s. 98). Trol gruplarında görülen örgütlenme stratejisi ise koordineli saldırıların başarısında kritik bir rol oynar. Bu tür ağlar ya hiyerarşik ya da hücresel yapılar temelinde organize edilmektedir. Hiyerarşik sistemlerde, merkezde bir komuta noktası bulunmakta ve buradan sahte ya da yönlendirilmiş hesaplara belirli talimatlar

iletilmektedir. Hücresel örgütlenme modelinde ise, daha küçük ve bağımsız gruplar birbirleriyle uyumlu hareket etmektedir ve böylece faaliyetlerin tespit edilmesi daha güç hale gelmektedir. Saldırıların koordinasyonu ise çoğunlukla özel iletişim platformları olan Telegram, WhatsApp veya Discord gibi kanallar üzerinden sağlanmaktadır. İletişim kanalları üzerinden, önceden hazırlanmış mesaj şablonları, kullanılacak etiketler ve paylaşım zamanlamaları gibi detaylar aktarılır. Hedef alınacak kişi ya da konu hakkında yapılacak yorumların tonu, dili ve vurguları dahil ayrıntılı şekilde örgütlü bir plan yapılır. Böylece dışarıdan bakıldığında farklı bireylerden geliyormuş gibi görünen içerikler, aslında merkezi bir stratejinin parçası olarak ortaya çıkmakta ve daha inandırıcı olmaktadır (NATO Strategic Communications Centre of Excellence, 2021).

Trol ordularının zaman ve örgütlenme stratejileri ile kitleleri manipüle etme eylemlerinin çarpıcı bir örneği 2017’de yapılan Fransa Başkanlık seçimlerinin ikinci turuna kısa bir süre kala yaşanmıştır. Seçimlerde Cumhurbaşkanı aday olan Emmanuel Macron, açıklama yaparak seçim kampanyasına ilişkin çok sayıda belge ve raporun bir siber saldırı sonucu çalındığını kamuoyuna duyurmuştur. Çalınan bu belgeler internette dolaşıma sokulmuş ve bazı gruplar tarafından organize olarak özellikle kara propaganda yapmak maksadıyla sosyal medyada kullanılmıştır. Avrupa Konseyi’nin 2019 tarihli bir raporunda, bu saldırının Fransa dışındaki bir ülkeden gerçekleştirildiği vurgulanmıştır. Aynı raporda farklı bir olaya da değinilerek Birleşik Krallık’ın AB üyeliğine ilişkin referandumunda da benzer bir olaya tanık olunduğu belirtilmiştir. Kamuoyunda ‘Brexit’ olarak anılan Birleşik Krallık’ın AB’den ayrılması sürecinde, seçime 48 saat kala sosyal medyada 156 bin 252 Rus hesabın, 45 binden fazla ‘Brexit’ mesajı yayınladığı tespit edilmiştir. Bununla birlikte devlet destekli Rus ajansları RT ve Sputnik de bu referandum hakkında, AB karşıtı duygular içeren çok sayıda haber yayınlamıştır. Raporda, RT ve Sputnik’in, özellikle X’te daha fazla erişime sahip olduğu da belirtilmiştir (Doublet, 2019, p. 13). Özellikle Fransa’daki olay, siber saldırı ekiplerinin ve trol gruplarının da belli bir koordinasyon içerisinde çalışarak seçimleri hedef aldıklarını ve kamuoyunu manipüle etmeye çalıştıklarını göstermektedir. AB Konseyi raporundan aktarılan her iki olayda da trol ağlarının, yapılacak olan seçimlerden çok kısa bir süre önce dezenformasyon çalışmalarına başlamaları, zamanlama stratejisi açısından kritik bir göstergedir. Kamuoyunun kırılmaya daha yatkın olduğu ve görüş ayrılıklarının daha keskin olduğu

seim zamanları, propaganda ve dezenformasyon faaliyetlerinin en fazla yrtldė zamanlardır.

2.1.3. Hashtag Kampanyaları ve Bilgi Kirliliėi

Oxford Szlė’ne gre ‘hashtag’, sosyal medya platformlarında bir kelime ya da ifadenin bařına ‘#’ iřareti eklenerek oluřturulan bir etikettir. Hashtagler, ieriklerin belirli konular altında toplanmasını, kolayca bulunmasını ve ilgili temalar etrafında tartiřmaların organize edilmesini mmkn kılmaktadır (Oxford English Dictionary, 2014). Hashtag kullanımı, Amerikalı teknoloji yazarı ve Twitter kullanıcısı Chris Messina’nın 2007’de attıėı bir tweetle ortaya ıkmıřtır. Messina, sosyal medyada paylařılan ieriklerin daha kolay gruplanabilmesi iin ‘kare’ (#) sembolnn kullanılmasını nermiřtir. Bařlangıta bu fikir Twitter ynetimi tarafından fazla ciddiye alınmamıř olsa da aynı yıl ABD’de meydana gelen byk bir yangın sırasında bir kullanıcının tm gnderilerinde ‘#SanDiegoFire’ etiketini kullanmasıyla hashtag kavramı dikkat ekmiřtir. Bylece, yangınla ilgili geliřmeler Twitter zerinde bu etiket altında toplanmıř ve hashtaglerin paylařım organizasyonu iin ne kadar etkili olabileceėi somut bir řekilde grlmřtr. Twitter, bu olaydan birka yıl sonra hashtaglerin iřlevselliėini artırmak iin nemli bir adım atmıř ve kullanıcıların, artık bir hashtage tıklayarak, o etiketi ieren tm tweetlere kolayca ulařabilmelerini saėlamıřtır. 2010 yılında ise platform, hakkında en fazla tweet atılan konuları ‘trend konular’ olarak sınıflandırmıř ve popler konuları grnr hale getirmiřtir. Bu zellik, hashtag kullanımının hızla yaygınlařmasına ve sosyal medyada nemli bir ierik organizasyon aracı haline gelmesine katkı saėlamıřtır (řahin, 2024). İlk olarak Twitter’da kullanılmaya bařlanan hashtag, bugn hemen hemen her sosyal medya platformunda aynı iřlevde kullanılmaktadır. Bu kullanım iřlevi ve hashtag kampanyaları, trol faaliyetlerinin de nemli bir aracı konumundadır. Trol grupları, belirli hedefler doėrultusunda yrttkleri dezenformasyon kampanyalarını desteklemek amacıyla hashtaglerden aktif ve sistemli bir řekilde yararlanmaktadır. Belirli bir hashtagi ne ıkarmak iin binlerce trol ya da bot hesap aracılıėıyla eř zamanlı ierik paylařımı yapılmakta ve bu ierikler oėunlukla benzer, tekrar eden mesajlardan oluřmaktadır. Hashtagler aracılıėıyla bu mesajların birok farklı kullanıcı tarafından paylařıldıėı izlenimini vermek, belirli bir grřn ya da bilginin, toplumun geniř bir kesimi tarafından benimsendiėi algısını oluřurmaktadır. Bu yntem de sosyal kanıt etkisini devreye sokarak bireylerin grup davranıřına uyum gsterme eėilimini artırmaktadır. Trol grupları,

seçtikleri hashtagler altında sahte belgeler, çarpıtılmış haberler ve manipülatif içerikler de paylaşarak bilgi kirliliğini artırmakta ve böylece doğru bilgiler görünmez hale getirilebilmektedir (Aytekin vd., 2023, s. 25-26).

2019'un son aylarında başlayarak kısa sürede dünyayı etkisi altına alan COVID-19 pandemisi, küresel bir sağlık krizi olmanın ötesinde, aynı zamanda geniş çaplı bir infodemiye de yol açmıştır. İngilizce 'information' (bilgi) ve 'epidemic' (salgın) kelimelerinin birleşiminden türetilen 'infodemi' kavramı, COVID-19 pandemisi sırasında sıkça kullanılan terimlerden biri olmuştur. Bu kavram hem doğru hem de yanlış bilgilerin hızla yayılmasını tanımlamaktadır. Dünya Sağlık Örgütü (DSÖ) infodemiye, 'doğru veya yanlış her türlü bilginin dolaşımının, bireylerin güvenilir bilgi kaynaklarına ulaşmasını ve doğru rehberlik almasını güçleştiren bir durum' olarak tanımlamış ve salgının ilk dönemlerinde, kamu sağlığını tehdit eden yanlış bilgilerin ve komplo teorilerinin virüs kadar hızlı yayıldığını da vurgulamıştır (World Health Organization, 2020). Özellikle sosyal medya platformlarında öne çıkan bazı hashtagler, bu dezenformasyon akımlarının odak noktası haline gelmiştir. Trol ağları, bu hashtagler aracılığıyla yanlış bilgilerin yayılmasını hızlandırmış ve halkın, sağlık önlemlerine olan güvenini ciddi ölçüde sarsmıştır. Çeşitli komplo teorileri ile aşı karşıtlığını arttıran ve salgın önlemlerine karşı toplumda ciddi bir tepki doğuran trollerin yaymış oldukları manipülatif içeriklerin Twitter'da, doğrulanmış kaynaklardan gelen içeriklere göre daha yüksek oranda etkileşim aldığı da ortaya çıkmıştır (Cinelli vd., 2020, s. 6-7).

2.1.4. Deepfake ve Manipülatif Görsel İçerikler

Sosyal medyada ve çevrimiçi kanallarda dezenformasyon yalnızca yazılı içeriklerle sınırlı kalmayıp, giderek daha fazla görsel ve işitsel araçlar üzerinden yürütülmektedir. Özellikle trol ağlarının devreye soktuğu deepfake videolar ve görseller ile manipüle edilmiş materyaller dijital ortamda, güvenlikten etîge; siyasal istikrardan birlik ve beraberliğe kadar pek çok alanda tehdit oluşturmaktadır. Görsellerin insan algısı üzerindeki güçlü etkisi de bu içeriklerin kamuoyu manipölasyonunda etkili bir araç olarak kullanılmasına neden olmakta ve deepfake içerikleri daha da tehlikeli hale getirmektedir (Pennycook vd., 2020). Deepfake terimi, 'deep learning' (derin öğrenme) ve 'fake' (sahte) kelimelerinin birleşiminden türetilmiştir. Aslında bir yapay zekâ teknolojisi olan deepfake, bir kişinin yüzünü, sesini veya mimiklerini başka bir kişinin bedenine dijital

olarak monte ederek sahte video ve ses içerikleri üretme imkânı sağlamaktadır. Genellikle Generative Adversarial Networks (GAN) gibi gelişmiş, görsel üretici yapay zekâ modelleri kullanılarak oluşturulan bu sahte içerikler, her geçen gün daha gerçekçi hale gelmektedir (Kietzmann vd., 2020). Sosyal medya trolleri için ciddi bir dezenformasyon stratejisi haline gelen deepfake içerikler manipüle etme, toplumsal ayrışmayı körükleme, hedefteki kişi ya da grubu itibarsızlaştırma ve komplo teorilerini besleme gibi pek çok amaçla dolaşıma sokulmakta ve koordineli biçimde kitlelerde gerçek algısı yaratmaya çalışmaktadırlar. Üstelik bu teknoloji sadece sıradan vatandaşları değil, üst düzey bürokratları da aldatabilecek kadar risk taşımaktadır. Ben Cardin vakası, bu bağlamda örnek bir vakadır. 2024 yılı Ocak ayında ABD Senatörü Ben Cardin'in katıldığı çevrimiçi bir görüşmede, karşısındaki kişinin Ukrayna'lı bir yetkili olduğu öne sürüldü. Görüşme sırasında, 'Uzun menzilli füzelerin Rus topraklarına gönderilmesini destekliyor musunuz? Cevabınızı bilmem gerekiyor' gibi sorular soruldu. Bu durumdan şüphelenen Ben Cardin, durumu yetkililere bildirdi. Daha sonra bu kişinin gerçek bir insan olmadığı, deepfake teknolojisi kullanılarak oluşturulmuş sahte bir figür olduğu ortaya çıkmıştır. Görüşmenin içeriği kamuoyuyla paylaşılmassa da olay resmi makamlarca doğrulanmış ve Amerikalı yetkililer, söz konusu olayın 'Rusya ile bağlantılı kişiler tarafından gerçekleştirilen üst düzey bir dezenformasyon girişimi' olduğunu ifade etmiştir. Bu olay, devlet düzeyinde dahi gerçekleştirilebilen yapay içerik manipülasyonlarının ulaştığı noktayı ve deepfake teknolojisinin potansiyelini açıkça göstermektedir (NBC News, 2024).

Facebook, Twitter, TikTok ve Youtube gibi platformlar, açık şekilde manipüle edildiği tespit edilen içerikleri kaldırma politikası benimsemişlerdir. Bu politika kapsamında gerçek kullanıcıların şikayetleri incelenmekte ve otomatik tespit algoritmaları geliştirilmektedir. Fakat tespit algoritmaları hala kusurlu çalışmakta ve deepfake dolaşıma sokan kişi ya da gruplar, içerikleri platform politikalarına uygun hale getirerek sistemleri aşabilmektedirler (Chesney & Citron, 2019, s. 1768).

2.1.5. Mizah Üzerinden Yürütülen Faaliyetler

İnsan yaşamının evrensel ve temel bir parçası olan mizah, tarih boyunca yalnızca eğlence amacıyla değil, aynı zamanda psikolojik ve sosyolojik ihtiyaçları karşılamak için de önemli bir araç olmuştur. Mizah, bireyin ruh sağlığını korumasına yardımcı olmanın

yanı sıra, toplumsal ilişkileri pekiştirme, otoriteye karşı dolaylı direniş sergileme, zihinsel esneklik kazanma ve biyolojik düzeyde iyi olma hâlini destekleme gibi çok yönlü işlevler üstlenir. Mizah, tarihsel süreçte yalnızca bireysel ya da toplumsal rahatlama aracı olarak değil, aynı zamanda güçlü bir propaganda ve ikna yöntemi olarak da işlev görmüştür. Özellikle savaş ve kriz dönemlerinde mizah; düşmanı alaya alarak itibarsızlaştırma, kolektif duyguları yönlendirme, ulusal morali artırma ve kitleleri belirli düşünce ve eylemlere ikna etme gibi çok katmanlı amaçlarla stratejik biçimde kullanılmıştır (Coşkun, 2013, s. 41). 21. yüzyıldaki dijital dönüşümle birlikte mizah, özellikle sosyal medyanın temel bileşenlerinden biri olmuş, aynı zamanda propaganda amacı taşıyan mizah da sosyal medya platformlarına taşınarak dijital bilgi savaşlarının temel araçlarından biri haline gelmiştir. Mizah içerikli paylaşımlar hem kolay yayılabilirliği hem de duygusal etkileşim yaratma gücü sayesinde, toplumsal algıların şekillendirilmesinde etkili bir ‘enformasyon silahı’ olarak kullanılmaktadır. Bu yönüyle mizah, trollerin de kamuoyunu şekillendirmek ya da dezenformasyon yaratmak için aktif biçimde kullandığı bir strateji haline gelmiştir.

Troller, mizahın masum ve zararsız algısından faydalanarak organize kampanyalar aracılığıyla parodi videolar, memler ve ironik gönderiler üretir. Bu tür içerikler çoğunlukla sadece ‘komik’ ya da ‘günlük eğlence’ olarak değerlendirilse de aslında belirli ideolojik ya da politik mesajlar içerir. Akademik araştırmalar, bu tarz mizahi paylaşımların hedef kitlede eleştirel süzgeç devreye girmeden tüketildiğini ve bu nedenle propaganda etkilerinin daha güçlü olabileceğini ortaya koymaktadır. Mizahın bu yönü, özellikle genç kullanıcılar arasında etkili bir algı yönetimi aracına dönüşmektedir. Mizah stratejilerine bakıldığında zaman trollerin, kışkırtıcı içerikler ürettikleri, dezenformasyonu mizah aracılığıyla çekici hale getirdikleri, mizahi bir dil kullanarak ciddi içerikleri geçiştirdikleri ve kitlelerde öfke, alay veya kin gibi kuvvetli duygular uyandırmak için mizah kullandıkları görülmektedir (Nieuburt, 2021, s. 3). Rusya-Ukrayna savaşında, Ukrayna tarafından çok sık şekilde kullanılan kamikaze dronların sansürsüz görüntülerinden, komik fon sesleriyle ve yorumlarla video kolajları oluşturulduğu görülmektedir. Bu videoları milyonlarca kişi izlemekte ve yorum yaparak sözde mizaha dahil olmaktadır. Bir insanın son anlarının bu denli ‘gülünç’ bulunarak savaşın ve yer yer tartışmalı askeri taktiklerin mizahi bir dille işlenmesi, trollerin mizah stratejilerine güçlü bir örnek olarak karşımıza çıkmaktadır. Benzer şekilde farklı ırklardaki insanları temsil

eden deęerler üzerinden alaycı bir tutum ile yapılan mizahlar da ayrışmayı ve önyargıyı körüklemektedir. Son dönemde oldukça popüler hale gelen ‘Hint sokak lezzetleri’, ‘Asya yemek kültürü’ gibi mizah amacıyla yapıldığı öne sürülen videolar bu bağlamda önemli birer örnektir. Hijyenik olmayan şartlar altında üretilen gıda maddelerinin videolarına maruz kalan sosyal medya kullanıcıları, tümevarım mantığıyla mizaha konu olan ülkenin tamamında hijyen sorunu olduğunu düşünebilmektedir.

2.2. Algoritmaların ve Yapay Zekânın Rolü

Sosyal medya algoritmaları, kullanıcıların platformlarda gördüğü içerikleri filtreleyen ve sıralayan yazılım sistemleridir. Bu algoritmalar; beğeniler, paylaşımlar, izleme süresi, yorumlar gibi kullanıcı etkileşimlerini analiz ederek, bireye en çok ilgi göstereceğı içerikleri sunmayı amaçlamaktadır. Böylece kullanıcıların platformda daha fazla zaman geçirmesi sağlanır. Yapay zekâ teknolojileri, günümüz sosyal medya algoritmalarının temel yapıtaşı haline gelmiştir. Bu sistemler, hangi içeriklerin kullanıcıyı daha uzun süre platformda tutacağını öngörebilmekte ve içerik akışını buna göre şekillendirmekte, böylece her kullanıcıya özgü, kişiselleştirilmiş bir içerik grubu sunmaktadır (Açıkalin & Canbey, 2022, s. 4-5).

2.2.1. Sosyal Medya Algoritmalarının Propaganda İle İlişkisi

Belirli bir sorunu çözmek ya da belirli bir hedefe ulaşmak amacıyla izlenen aşamalı yönergeler bütününe ‘algoritma’ denilmektedir. Özellikle dijital çağ ile birlikte günlük hayatta daha fazla adı geçen algoritma kavramı, yalnızca bilgisayar teknolojileriyle sınırlı kalmayıp, gündelik yaşamda da birçok süreçte karşımıza çıkmaktadır (Torun, 2021).

Sosyal medya platformları, algoritmaların en görünür ve etkili şekilde uygulandığı dijital ortamlardan biridir. Bu platformlarda sistemler, kullanıcının hangi içerikle ne kadar süre etkileşim kurduğunu, hangi paylaşımları beğendiğini veya kimlerle iletişimde bulunduğunu sürekli olarak takip etmektedir. Bu analizler sonucunda ise kullanıcıya özgü içerikler sunulmaktadır. TikTok, Instagram, Facebook, YouTube ve X gibi uygulamalar, kullanıcıların platformda daha fazla vakit geçirmesini sağlamak amacıyla kişiselleştirilmiş akışlar oluşturmakta ve bu süreçte, yapay zekâ destekli teknolojiler olan makine öğrenmesi ve doğal dil işleme yöntemlerinden yararlanmaktadırlar. Böylece

sosyal medya, yalnızca bilgi paylaşımı yapılan bir mecra olmaktan çıkmakta; bireyleri yönlendiren, düşünsel eğilimleri şekillendiren güçlü bir mekanizmaya dönüşmektedir. Kimi zaman kamuoyunu etkileme aracı olarak da devreye giren algoritmalar politik kampanyalar, ticari pazarlama stratejileri ya da dijital propaganda faaliyetleri için de uygun bir strateji konumundadır. Bu çerçevede, sosyal medya algoritmaları yalnızca teknik birer yapı değil, aynı zamanda bireylerin düşünce kalıplarını etkileyebilecek dijital strateji araçları olmaktadır (Açıkalın & Canbey, 2022, s. 5).

Algoritmaların kitleler üzerinde kurabileceği etkiyi gören propaganda üreticileri çeşitli yöntemlerle bundan istifade etmektedir. Kullanıcıların çevrim içi etkileşimlerinden yola çıkarak ilgi alanlarını, davranış örüntülerini ve hatta siyasi yönelimlerini çözümleyebilen algoritmalar, propaganda yapan taraflar için her şeyden önce bir analiz ve çıkarım yöntemidir. Günümüzde ciddi miktarda kullanıcıyı içinde barındıran dijital alanlarda kitlelerin isteklerini ve hassas noktalarını gösteren algoritmalarla dayanarak hangi kitlelere nasıl yaklaşılabileceği ve nasıl stratejiler ile destek alınabileceği öngörülebilmektedir. Diğer taraftan algoritmalar, çeşitli yöntemler kullanılarak istenilen yöne de çevrilebilir ki bu da kitleleri manipüle etmek ve istenilen yönde propagandaya maruz bırakmak için etkili bir strateji olarak karşımıza çıkmaktadır. Sosyal medya algoritmaları, yapıları gereği çevrimiçi platformlarda fazla etkileşim alan popüler içerikleri, sosyal medya kullanıcılarının karşısına çıkartma mantığıyla çalışmaktadırlar. Bu da algoritmaları, bir takım bot hesaplar ya da organize trol grupları gibi faaliyetler aracılığıyla manipüle etmenin yolunu açmaktadır. Kitlelere bildirilmek istenen mesajların dijital ortamda sahte etkileşimler ile ‘popüler’ gibi gösterilmesi, algoritmaların bu mesajları kullanıcıların karşısına çıkartma olasılığını arttırmaktadır. Böylece sosyal medya kullanıcılarının ne düşündükleri kontrol edilemese bile ne hakkında düşünecekleri kontrol edilmiş olmaktadır (Yetkin, 2019, s. 63). Algoritmaları belli bir doğrultuda yönlendirmenin diğer bir yolu ise belli ücretler karşılığında sosyal medya platformlarına reklam verilmesidir. Bu işlemde sosyal medya platformları, propaganda üreticilerden aldıkları ücretin miktarına orantılı olarak verilen reklamları ön plana çıkartmakta ve diğer kullanıcıların görmesini sağlamaktadır. Bu durumlarda fazla bir etkileşim olmasa dahi yazılımsal arka plan sayesinde algoritmalar şekillendirilebilmekte, verilen ödeme kapsamında belli bir propagandanın reklamı yapılabilir. 2020 yılında yapılan ABD Başkanlık seçimlerinde Donald Trump, seçim kampanyasına yönelik olarak propaganda

reklamları için Facebook’a toplamda 110 milyon dolar harcamış; rakibi Joe Biden ise yaklaşık olarak 100 milyon dolar harcayarak Facebook’a siyasi reklamlarını vermiştir. Bu rakamların yalnızca Facebook verileri olduğu düşünüldüğünde siyasilerin, özellikle seçim dönemlerinde sosyal medya platformlarına ciddi bütçeler ayırarak reklam verdikleri anlaşılmaktadır (Sofuoğlu, 2020). Öte yandan sosyal medya algoritmaları kullanıcıların belli bir düşünce kalıbına sıkışmasına ve dolaylı yoldan radikalleşmesine de sebep olmaktadır. Kullanıcıların dijital davranışlarını temel alarak içerik sunan algoritmalar, bilgi çeşitliliğini teşvik etmek yerine, bireyleri benzer görüşlerin tekrarlandığı ve farklı bakış açılarına kapalı kalan ‘yankı odalarına’ sürükleyebilmektedir. Yankı odası kavramı, benzer düşünce ve inançlara sahip bireylerin, karşıt görüşlerle karşılaşmadan yalnızca kendi fikirlerini pekiştiren içeriklerle etkileşime geçtiği kapalı iletişim alanlarını tanımlamaktadır. Sosyal medya platformları açısından irdelendiğinde yankı odaları, algoritmaların kullanıcı tercihlerine göre içerik filtrelemesiyle oluşmaktadır. Filtrelenen içerikler kapsamında bazı düşünceler daha da güçlenmekte ve kullanıcılara yalnızca kendi inançlarını doğrulayan bilgileri sunulmaktadır. Bu durum, bireylerin farklı bakış açılarına erişimini engelleyerek çok yönlü düşünme yetisini zayıflatmakta, kullanıcı çevrimiçi ortamda sürekli olarak desteklenen fikirlerini mutlak doğru olarak benimseyebilmektedir (Anadolu Ajansı, 2023).

2.2.2. Bot Hesapların Tespiti ve Engellenmesi

Bot hesaplar, çevrimiçi platformlarda insan davranışlarını taklit edecek şekilde tasarlanmış otomatik ya da yarı otomatik yazılımlardır. Bu tür hesaplar, belirli kurallara dayalı algoritmalarla içerik paylaşabilmekte, yorum yapabilmekte, gönderileri beğenebilmekte ya da dijital gündemi yönlendirmeye çalışabilmektedirler. Bazı botlar yalnızca bilgi yayımı amacıyla kullanılırken, bir kısmı ise sistematik biçimde dezenformasyon üretmek, propaganda yürütmek veya dijital ortamda manipülasyon gerçekleştirmek üzere organize edilmektedir. Her iki biçimde de bot hesaplar, sosyal medyada algıyı yönlendirmenin ve kitleleri etkilemenin bir aracı olmaktadır. Bu yüzden bu tür hesapların özellikle dezenformasyon yapılan durumlarda tespit edilmesi ve etkisizleştirilmesi, kamuoyunun yararına olacaktır.

Bot hesapların, gerçek bir kullanıcıdan ayırt edilebilir bazı yanları bulunmaktadır. Öncelikle bot hesaplarda kullanılan profil fotoğrafları çoğu zaman stok görsellerden ya

da başka kişilere ait görüntülerden alınmaktadır. Bu durum basit bir tersine görsel arama yöntemiyle tespit edilebilmektedir. Fakat gelişen yapay zekâ teknolojileriyle birlikte gerçekçi ve özgün insan görselleri oluşturmak bu tespit yöntemini zaman içinde etkisiz kılabilme potansiyeline sahiptir. Profil fotoğrafı olarak hiçbir görselin bulunmaması veya kullanıcıya dair bilgi vermeyen çizim ve benzeri görsellerin yer alması da bu hesapların sahte olabileceğine dair önemli birer işarettir. Diğer bir bot tespit yöntemi ise, hesap ismini incelemektir. Pek çok bot hesap, kullanıcı adlarında rastgele oluşturulmuş harf ve rakam kombinasyonlarını kullanmaktadır. Bu tür hesaplarda genellikle bir isimden sonra gelen uzun sayı dizileri, anlamsız şekilde sıralanmış harf ve rakam kümeleri ya da dört haneli standart sayılar sıkça görülmektedir. Örneğin, ‘mehmet8885372’ ya da ‘xj92lk8qzr01’ gibi adlar, kişisellikten uzak yapılarıyla bu hesapların sahte olabileceğine dair önemli ipuçları sunmaktadır. Takipçi ve takip edilen sayıları arasındaki dengesizlik, bot hesapları tespit etmede önemli bir göstergedir. Örneğin, çok sayıda kişiyi takip eden ancak neredeyse hiç takip edilmeyen ya da tam tersi şekilde, binlerce takipçisi olup kimseyi takip etmeyen hesaplar şüphe uyandırabilir. Çünkü bazı bot hesaplara ‘popüler’ gözükmeleri için takipçi satın alınabilmektedir. Ayrıca, takip eden ve takipçi sayılarının olağan dışı biçimde eşit ya da birbirine çok yakın olması da bu hesapların belli bir otomasyonla oluşturulmuş olabileceğine dair ipuçları sunabilmektedir. Bir hesabın paylaşımlarında dilin yapay ya da alışılmadık bir şekilde kullanılması, cümle yapılarının garip ya da akıcılıktan uzak olması, içeriğin otomatik sistemler tarafından üretildiğine işaret edebilir. Bunların yanı sıra aynı hesapta birden fazla dilde paylaşımlar yapılması, sistematik bir zaman aralığında aynı site bağlantılarının yer aldığı paylaşımların sürekli olarak tekrarlanması, paylaşımların hesap takipçileriyle orantılı biçimde etkileşim alması gibi ipuçları da bot hesap tespitinde işe yaramaktadır (Özgür, 2021).

Otomatik olarak oluşturulan bot hesapların sadece tespiti yeterli olmamakta, bulunduğu sosyal medya platformundan kaldırılması da gerekmektedir. Bot hesapların kaldırılmasına yönelik olarak platformlar, algoritmalarını ve altyapılarını sürekli olarak güncellemekte, bunun yanı sıra kullanıcılardan da ‘geri bildirim’ sistemiyle yardım almaktadır. Bazı sosyal medya platformları, sahte hesapların yayılmasını önlemek amacıyla şüpheli profillerden telefon numarası, e-posta adresi veya kimlik doğrulaması gibi ek güvenlik adımları talep etmektedir. Bu şartları sağlayamayan hesaplar süreli ya da süresiz olarak askıya alınmaktadır. Twitter, Elon Musk tarafından satın alınmadan önce

yaptığı bir açıklamada her gün yaklaşık 1 milyon bot hesabı tespit ederek sildiğini açıklamıştır (Ortutay, 2022). Musk'ın satın almasından sonra ise X platformu, sahte hesapları sistematik şekilde silmeye devam etmiş ve uzun süre oturum açmayan hesapların da kaldırılacağı açıklanmıştır (Euro News, 2023). Meta şirketi çatısında olan Instagram ve Facebook ise, bot hesapları takip eden algoritmaların yanı sıra açılan hesaplarda özellikle gerçek isimlere dikkat etmektedir (Facebook, tarih yok).

2.2.3. Yapay Zekâ Destekli Propaganda Araçları

Geleneksel propaganda biçimlerinin dijital ortama taşınmasıyla birlikte, yapay zekâ destekli teknolojiler propaganda süreçlerinin hem hızını hem de etkinliğini önemli ölçüde artırmıştır. Otomatik içerik üretimi, hedef kitleye özel mesajların oluşturulması, deepfake gibi görsel manipülasyon teknikleri ve sosyal medya botlarının kullanımı, bilgi manipülasyonunu daha gelişmiş ve algılanması güç bir boyuta taşımaktadır.

Yapay zekâ, makinelerin insan benzeri düşünme, öğrenme, karar verme ve problem çözme yetenekleri kazanarak bu yetenekleri birtakım işlevlerde kullanan teknolojileri tarif etmektedir. İlk kez 1956 yılında John McCarthy tarafından kavramsallaştırılan yapay zekâ, günümüzde sadece teorik bir tartışma alanı olmaktan çıkmış; savunmadan sağlığa, medyadan kamu yönetimine kadar birçok sektörde aktif olarak kullanılmaya başlanmıştır (Russell & Norvig, 2016). İlk kullanım ve testlerinde basit mantık yürütme programları aracılığıyla satranç oyununa entegre edilen yapay zekâ teknolojisine sahip makineler, yıllar içerisinde geçirdikleri ciddi değişiklikler ile bugün hayatın her alanına yayılmış sistemler olarak karşımıza çıkmaktadırlar. Sağlık hizmetleri, finansal analizler, navigasyon, gözetim ve tespit, kişiye özel içeriklerinin geliştirilmesi gibi birçok alanda karar süreçlerini hızlandırmak ve farklı fikirler sunmak için kullanılan yapay zekâ, propaganda ve kamuoyunun algısını yönetmek için de aktif şekilde kullanılmaktadır. Yapay zekânın bu işlevinde ise dijital çağın vazgeçilmez birer parçası haline gelen sosyal medya platformları birer 'dijital kamusal alan' görevi görmektedir (Bustanur vd., 2022). Yapay zekâ teknolojileri propaganda alanında kullanılarak kamuoyunu yönlendirmek için çeşitli algoritmalarla donatılmaktadır. Bu algoritmalarından dikkat çeken ve kamuoyu üzerinde etkisi kanıtlanmış olan doğal dil işleme (NLP) teknolojisi, belirli hedef kitlelere yönelik içerikleri özelleştirerek propaganda içeriklerini kullanıcı profillerine uygun şekilde şekillendirebilmektedir. Bu durum, siyasi alandan

halkla ilişkiler ve reklamcılık alanına; askeri alanlardan istihbari alanlara kadar pek çok yerde etkili algı yönetimi çalışmalarını mümkün kılmaktadır.

Yapay zekâ, etkili biçimde analiz yeteneklerini kullanarak daha iyi çalışabilmek için hedef kitlenin büyüklüğüne paralel olarak çok geniş bir veri yelpazesine ihtiyaç duymaktadır. Kitleler hakkında elde edilen veriler, algoritmalar aracılığıyla hızla analiz edilmekte, işlenmekte ve çok kısa bir süre içerisinde hedefe yönelik olarak oluşturulan fikir ve planlar ortaya çıkmaktadır. Burada, çevrimiçi kullanıcıların dijital ayak izlerinden elde edilen psikografik veriler, kilit rol oynamaktadır. Bireylerin kişilik özellikleri, yaşam tarzları, sosyal statüleri, ilgi alanları, aktiviteleri, düşünce biçimleri ve tutumları gibi psikografik veriler incelenerek, hedefteki kitle gruplandırılmakta ve hedef kitleyi daha derinlemesine anlayarak, ona özel stratejiler geliştirmek için kullanılmaktadır (Survey Monkey, tarih yok). Günümüzde bazı sosyal medya platformları, kullanıcılarının verilerini belli ücretler karşılığında bazı şirketlere satmak ya da siber saldırılara karşı yeterince koruyamamakla suçlanmaktadır. Yakın tarihte bu suçlama ile karşı karşıya kalan Facebook, özellikle seçim süreçlerindeki analiz ve veri toplamalarıyla bilinen İngiltere kaynaklı danışmanlık şirketi Cambridge Analytica'ya birtakım verileri dolaylı olarak satmak ile suçlanmıştır. Cambridge Analytica ile aynı çatı altında bulunan Strategic Communication Laboratories (SCL) şirketi tarafından 2014 yılında yaklaşık 87 milyon Facebook kullanıcısının psikografik verilerinin kullanıcılardan habersiz olarak alındığı ve Cambridge Analytica'ya iletildiği, buradan da çeşitli Amerikalı siyasetçilere bu verilerin satıldığı tespit edilmiştir. Facebook yönetimi bu durumdan kendisinin de mağdur olduğunu iddia etmiş ve 'kişisel verileri satma' ithamlarını reddetmiştir. Ele geçirilen verilerin çeşitli algı yönetimi çalışmalarında kullanılmasının yanı sıra 2016 yılında ABD'de Donald Trump'ın başkanlık kampanyasında ve Birleşik Krallık'taki Brexit referandumunda da kişiye özel propaganda içerikleri oluşturmak amacıyla kullanıldığı ortaya çıkmıştır (Davies H. , 2015).

Cambridge Analytica skandalının ardından ABD Federal Ticaret Komisyonu (FTC), Facebook'a 5 milyar dolarlık para cezası verdiğini açıklamıştır. Bu açıklama sonrasında Facebook'un hisse senetlerinde yüzde 1.2'lik bir düşüş yaşanırken Cambridge Analytica ise iflas etmiştir. (Independent Türkçe, 2019). Bu skandal ile birlikte sosyal medya kullanıcılarının verilerini izinsiz olarak almak ve kullanmak, yakın tarihin en sansasyonel veri skandallarından birisi olmuştur. Cambridge Analytica örneğinde de

görüldüğü üzere kullanıcıların dijital izlerinden elde edilen veriler, yapay zekâ algoritmalarına entegre edilerek seçmen davranışları öngörülme ve yönlendirilmeye çalışılmıştır.

2.3. Kamuoyu Algısı ve Tepkisi

Dijital çağda kamuoyu, geleneksel medyanın tek yönlü ve sınırlayıcı yapısından uzaklaşarak, daha hızlı değişen, katılımcı fakat aynı zamanda manipülasyona daha açık dolayısıyla daha kırılğan bir forma evrilmiştir. Özellikle sosyal medya platformlarında gerçekleştirilen dijital propaganda ve trol faaliyetleri, bireylerin düşünme biçimlerini, algı süreçlerini ve verdikleri tepkileri doğrudan etkilemektedir. Sistematik olarak yayılan dezenformasyon, yapay gündemler ve ayırıştırıcı dil, toplumsal ortak gerçeklik algısını bozmakta; insanları duygusal ve politik açıdan yönlendirmeye çalışarak yanlış bilgilendirmeye açık hale getirmektedir (Acar, 2023, s. 7). Dijital manipülasyonlara maruz kalan kamuoyu radikalleşme, güvensizlik ve duyarsızlaşma gibi tepkiler verebilmektedir. Dijital mecralarda sürekli benzer ideolojik içeriklerle karşılaşan bireylerde, farklı düşüncelere karşı hoşgörüsüzlük gelişebilmekte ve kendi görüşlerini mutlak doğru olarak kabul eden sert tutumlar ortaya çıkabilmektedir. Trol faaliyetlerinin artması ve yanlış bilgilerin yaygınlaşması ise bireylerin bilgi kaynaklarına olan güvenini zayıflatmakta ve bu durum, hakikate karşı genel bir güvensizlik ortamı doğurmaktadır. Ayrıca sürekli değişen gündem ve bilgi yoğunluğu, bireylerde belli düzeyde bir duyarsızlaşmaya sebep olarak toplumsal olaylara karşı ilgisizliğe ve kayıtsızlığa yol açabilmektedir (Lewandowsky vd., 2012, s. 124).

Sosyal medyada karşılaşılan tüm bu durumlar neticesinde kamuoyu, dijital aktivizme yönelmekte, teyit platformları oluşturmakta, hashtag ve tepki kampanyaları gerçekleştirmekte ve doğru bilgiye erişmek için bağımsız platformlar ya da kaynaklar aramaktadır.

2.3.1. Dijital Propagandanın Toplum Üzerindeki Etkileri

Kitleleri etkilemeyi ve yönlendirmeyi hedefleyen propaganda, geçmişte ağırlıklı olarak kampanyalar, broşürler, afişler ve geleneksel medya araçlarıyla yürütülmekteyken bugün dijitalleşmenin etkisiyle, propaganda faaliyetlerinin büyük bölümü çevrimiçi platformlara taşınmıştır. 21. yüzyılın getirdiği yeni dijital medya ortamı, propaganda

faaliyetlerinin erişim alanını ve etkisini önemli ölçüde artırmıştır. Artık yalnızca siyasi partiler veya aktörler değil, sosyal medya kullanıcılarının tamamı belirli fikirleri yayma ve kitleleri etkileme potansiyeline sahiptir. Böylece propaganda, merkezi otoritelerin tekelinden çıkarak, herkesin katılım sağlayabileceği bir dijital eylem biçimine dönüşmüştür. Bununla bağlantılı olarak ise zaten siyasiler ile özdeşleşen ve kamuoyunda ‘güvenilmez’ bir izlenim bırakan propaganda kavramı, daha karmaşık bir hale bürünmüş ve hakkında yapılan araştırmaların daha da genişletilmesine neden olmuştur.

Son dönemlerde gerçekleştirilen çeşitli akademik çalışmalar, özellikle sosyal medya aracılığıyla yayılan dijital propagandanın seçmen davranışları üzerinde belirgin bir etki yarattığını ortaya koymaktadır. Bu bağlamda, dijital platformlarda yürütülen propaganda çalışmalarının, geleneksel medyaya kıyasla seçmen tercihlerini daha fazla etkilediği görülmektedir. Hedef kitleye hızlı ve etkili biçimde ulaşmanın daha kolay olması, propaganda içeriklerinin bireysel olarak kullanıcıya aktarıldığında daha rahat anlaşılması, viral olan içeriklerin daha fazla görünümü ve yayılımının algoritmalar aracılığıyla hızlı bir şekilde gerçekleşmesi gibi avantajlar, bu etkinin temelini oluşturmaktadır. Bunun yanında denetim ve sansür gibi faktörlerin en az düzeyde olması da dijital platformlarda uygulanan propaganda stratejilerini, geleneksel platformlardakilere göre daha etkili yapmaktadır. Avrupa Komisyonu Ortak Araştırma Merkezi (JRC) tarafından 2020 yılında yayınlanan bir raporda, genç yaş grubu başta olmak üzere günümüzde pek çok bireyin siyasi içerikli haberlere ulaşmak için geleneksel medya yerine sosyal medya platformlarını tercih ettiği belirtilmiştir. Bu durum da sosyal medya algoritmalarının dolaylı olarak kamuoyu algısını şekillendirmede ne kadar önemli bir rol üstlendiğini göstermektedir. Raporda, özellikle seçim dönemlerinde dolaşıma giren yanlış bilgiler ve kutuplaştırıcı içeriklerin, bireylerin kısa vadeli oy tercihlerini etkileyebildiği belirtilmekte ancak bu etkilerin uzun vadeli ideolojik yönelimler üzerinde kalıcı bir değişim yaratıp yaratmadığının henüz kesin şekilde anlaşılamadığı bildirilmektedir (Lewandowsky vd., 2012, s. 111-112). Türkiye ekseninde yapılan bir başka çalışmaya göre ise özellikle Twitter ve Facebook’un, siyasal katılımı teşvik eden, politik ilgi ve bağlılığı artıran etkili mecralar haline geldiği görülmüştür. Siyasi aktörler, bu dijital araçları seçmenlere doğrudan ulaşmak ve mesajlarını yaymak amacıyla yoğun şekilde kullanmaktadır. Siyasal gelişmeleri sosyal medya üzerinden takip eden bireylerin oy kullanma eğilimlerinin daha yüksek olduğu; özellikle kararsız seçmenlerin, seçim

dönemlerinde dijital içeriklerden daha fazla etkilendiği gözlemlenmektedir. Genç bireyler, sosyal medyada sıkça etkileşimde bulundukları siyasetçileri daha kolay hatırladıkları için, bu platformlar üzerinden kurulan iletişim, siyasal yönelimler ve oy verme davranışları üzerinde belirleyici olabilmektedir. Güven ilişkisi kurulan kişilerin yaptığı siyasal paylaşımlar, bireylerin siyasi görüşlerini de etkileme potansiyeline sahiptir. Öte yandan, sosyal medya kullanımı, sandığa gitme eğiliminde olmayan ya da siyasi süreçlere karşı ilgisiz kalan seçmenleri harekete geçirebilmekte, özellikle Z kuşağı gibi genç seçmen grupları için geleneksel siyasal iletişim yöntemlerine kıyasla daha cazip ve etkili bir iletişim kanalı olarak öne çıkmaktadır. Elde edilen bulgular, siyasal açıdan incelendiğinde dijital propagandanın yalnızca bilgi paylaşımını sağlamadığını; aynı zamanda seçmen davranışlarını yönlendirme kapasitesine sahip, stratejik bir siyasal etki aracı olarak işlev gördüğünü de ortaya koymaktadır (Yanık, 2024, s. 84).

2.3.2. Kamuoyu Manipülasyonu ve Kutuplaşma

Sosyal medyanın yapısal dinamikleri, algoritmalara dayalı içerik sunum mekanizmaları ve kullanıcı etkileşim alışkanlıkları, kullanıcıların yanlış ya da yanıltıcı bilgilere sistematik biçimde maruz kalmasına zemin hazırlamaktadır. ABD merkezli düşünce kuruluşu Pew Research Center (PRC)'in araştırmasına göre kullanıcılar, sosyal medya platformlarında sıkça yanlış bilgiyle karşılaştıklarını ifade etmişlerdir ve bu yüzden, dijital teknolojilerin toplumsal yapılar üzerindeki olumsuz etkilerine daha fazla inanmaktadırlar. Bu kullanıcılar, teknolojinin yanlış bilgileri yayarak bireyleri manipüle etmeyi kolaylaştırdığını, sosyal medya platformlarının yerli siyasetçiler tarafından manipülasyona açık hale geldiğini ve yabancı aktörlerin seçim süreçlerine müdahale etme riskini artırdığını düşünmektedir. Ayrıca, dijital iletişimin, halk tabanındaki siyasi görüşler arasındaki kutuplaşmayı derinleştirdiğine ve sosyal medya üzerinden edindikleri haber ve bilgilerin, diğer kaynaklara kıyasla daha fazla nefret söylemi içerdiğine inanmaktadırlar (Silver, 2019). ABD merkezli farklı üniversitelerden araştırmacıların bir araya gelerek yaptıkları bir araştırmada ise çeşitli ideolojik düşüncelerin uç noktalarında konumlanan sosyal medya kullanıcılarının yanlış bilgilere inanma olasılığının daha yüksek olduğu ve bu kullanıcıların dezenformasyona daha erken maruz kaldığı ortaya konulmuştur (Iyer, 2024). Cambridge Üniversitesi'nden araştırmacılar tarafından yapılan bir diğer çalışmada, sosyal medyada negatif tonda yazılmış olan haberlerin daha yüksek paylaşım oranlarına sahip olduğu ortaya çıkmıştır. Bulgular, medya kuruluşlarının

etkileşimi artırma amacıyla içeriklerinde olumsuz dile yönelme eğiliminde olabileceklerini göstermiştir. Araştırmaya göre, sosyal medya kullanıcıları ise negatif içeriklere daha fazla ilgi göstermekte ve bu tür içeriklerin hem etkileşimi daha fazla olmaktadır hem de daha geniş kitlelere ulaşmaktadır (Watson vd., 2024, s. 2).

2.3.3. Bilgi Kirliliğine Karşı Farkındalık Çalışmaları

Son yıllarda dijital propaganda faaliyetlerinin kamuoyu manipülasyonu ve toplumsal kutuplaşma üzerindeki etkileri, sosyal bilimciler ve medya araştırmacıları tarafından yoğun biçimde incelenen bir mesele haline gelmiştir. Dijital iletişim ve bilgi teknolojilerinin hızla yaygınlaşmasıyla birlikte sosyal medya, bireylerin haber alma süreçlerinde başat kaynaklardan biri haline gelmiştir. Ancak bu dönüşüm, bilgi kirliliği, dezenformasyon ve kamuoyu manipülasyonu gibi ciddi sorunları da beraberinde getirmiştir. Özellikle siyasi kampanyalarda şeffaflıktan uzak dijital propaganda yöntemlerinin kullanılması, halkın doğru bilgiye erişimini zorlaştırmakta ve toplumsal kutuplaşmayı derinleştirmektedir. Bu bağlamda, bilgi kirliliğine karşı geliştirilen farkındalık çalışmaları, demokratik toplumların sürdürülebilirliği açısından hayati bir rol oynamaktadır.

Bilgi kirliliği ile mücadele stratejileri temel olarak bireysel önlemler ve kurumsal önlemler olarak ikiye ayrılmaktadır. Bilgi kirliliğine karşı bireylerin alabileceği kişisel önlemler, dijital okuryazarlık becerilerinin artırılmasıyla birlikte, alınan bilgilerin kaynağını sorgulama, içerikleri çapraz kaynaklarla doğrulama ve duygusal tepkilerle değil eleştirel düşünceyle hareket etme alışkanlıklarını kapsamaktadır. Aynı zamanda, sosyal medyada karşılaşılan içerikleri paylaşmadan önce doğruluğunu kontrol etmek, dezenformasyonun yayılmasını engellemek açısından bireysel düzeyde önemli bir adım olarak görülmektedir (Siberay, tarih yok). Bilgi kirliliği ile mücadelede alınacak bireysel önlemlerin etki alanı kişiye özel olacağı için bu alanda atılacak kurumsal adımlar, farkındalığı geniş kitlelere ulaştırmakta kritik bir rol oynamaktadır. Özellikle eğitim kurumları, medya kuruluşları, teknoloji şirketleri ve sivil toplum örgütleri tarafından hayata geçirilen stratejiler, kamuoyunun dezenformasyona karşı bilinçlenmesini sağlamakta ve dijital ortamda bilgiye eleştirel bakış geliştiren bireyler yetiştirmeye katkıda bulunmaktadır. Bu kurumların sunduğu eğitim programları, doğrulama araçları

ve farkındalık kampanyaları, toplumsal düzeyde bilgi kirliliğine karşı kolektif bir direnç oluşturulmasında önemli rol oynamaktadır.

Birleşmiş Milletler Eğitim, Bilim ve Kültür Kurumu (UNESCO), modern toplum için doğru bilginin vazgeçilmez bir değerde olduğunu açıklamıştır. Bu yüzden bilgiye erişimin önemine vurgu yapan UNESCO, bu doğrultuda farkındalık çalışmaları yürüten aktif bir uluslararası örgüttür. UNESCO, bilgi kirliliğine karşı mücadelenin en etkili yollarından biri olarak medya okuryazarlığı eğitimine dikkat çekmektedir. Kurumun periyodik olarak güncellediği ‘Media and Information Literacy Curriculum’ adlı rehberde, bu eğitimin ulusal eğitim programlarına entegre edilmesi gerektiği ifade edilmektedir. Bu kapsamda özellikle genç bireylere yönelik geliştirilen programlar, yanlış bilgiyi ayırt etme, teyit yöntemlerini kullanma gibi temel yetkinliklerin kazandırılmasını hedeflemektedir (UNESCO, tarih yok). Avrupa Birliği ile koordineli biçimde çalışan Belçika merkezli EU DisinfoLab da uluslararası alanda hizmet veren güçlü bir dezenformasyonla mücadele örgütü olarak öne çıkmaktadır. Kuruluş, bilgi kirliliğinin demokratik değerlere ve toplumsal bütünlüğe yönelik tehditlerini tespit etmeyi ve bu tehditlerle mücadele etmeyi amaçlamaktadır (EU DisinfoLab, 2025). Bu kuruluşların yanı sıra daha yerel olan birçok dezenformasyonla mücadele oluşumu da bilgi kirliliğine yönelik toplumsal farkındalık için çalışmalar yapmaktadır. İngiltere merkezli Full Fact, ülkedeki siyasi söylemlerden sosyal medya içeriklerine kadar birçok farklı alanda gerçek zamanlı bilgi doğrulama çalışmaları yürütmektedir. Bu kuruluş aynı zamanda gazetecilere, akademisyenlere ve halka yönelik olarak, veri okuryazarlığı ve dezenformasyonla mücadele konularında eğitim programları düzenlemektedir (Full Fact, tarih yok). Güney Afrika merkezli doğrulama faaliyetleri yürüten Africa Check ise Afrika bölgesindeki sorunlara odaklanarak özellikle sağlık, eğitim, ekonomi ve siyaset gibi temel alanlarda dolaşıma giren yanlış bilgileri analiz etmekte ve çürütmeye çalışmaktadır. Afrika’da yoğun olarak kullanılan WhatsApp ve Facebook gibi platformlara özel bir önem veren kuruluş, bölgedeki yerel dilleri de içine alan kapsamlı çalışmalarla daha fazla insana ulaşmayı hedeflemektedir (Africa Check, 2022).

ÜÇÜNCÜ BÖLÜM

UKRAYNA-RUSYA SAVAŞINDA TROL HESAPLARIN ROLÜ VE STRATEJİLERİ

Çalışmanın bu bölümünde, Ukrayna ve Rusya arasında yaşanan çatışmaların X platformundaki trol hesaplar tarafından nasıl işlendiği içerik analizi yöntemiyle incelenerek sosyal medya trolllerinin propaganda stratejileri hakkında çıkarımlarda bulunulmuştur. Elde edilen bulgular doğrultusunda bir sonuç kısmı yazılarak dijital çağda değişen propaganda stratejileri üzerine genel bir değerlendirme yapılmış ve dezenformasyon ile nasıl mücadele edileceği hususunda önerilerde bulunulmuştur.

3.1. Araştırmanın Amacı ve Araştırma Yöntemi

Geniş bir tarihsel döneme yayılan propaganda faaliyetleri, belli teknolojik gelişmeler ve olaylarla kritik değişimlerden geçerek günümüze kadar ulaşmıştır. Bu değişimlerin en güncel hali olarak karşımıza çıkan dijital propaganda faaliyetleri, bilimsel araştırmaların propaganda faaliyetleri hakkında yeni inceleme alanı olmuştur. Bu doğrultuda, Rusya-Ukrayna savaşında, sosyal medya üzerinden yürütülen dijital propaganda faaliyetlerinin incelenmesi ve dijital propaganda faaliyetlerinin ciddi bir öznesi olan sosyal medya trolleri hakkında çıkarımlarda bulunulması, çalışmanın ana amacını oluşturmaktadır. Yapılan incelemelerle, sosyal medya trolleriine dair elde edilen bulgular sayesinde literatüre katkı yapmak hedeflenmektedir.

Belirtilen amaç doğrultusunda, nitel araştırma yöntemlerinden birisi olan içerik analizi yöntemi kullanılarak X paylaşımlarında tespit edilen ifadeler ve materyaller, düşünce kalıpları ve propaganda stratejileri yorumlanmıştır. İçerik analizi, çeşitli belgeler, yazılı metinler ve dokümanlar üzerinde, belirli sistematik kurallar çerçevesinde gerçekleştirilen bir araştırma yöntemidir. Bu yöntem, nitel araştırma kapsamında yer almaktadır ve amacı nesnel, ölçülebilir ve doğruluğu teyit edilebilir bilgilere ulaşmaktır (Karataş, 2015, s. 70).

Nitel araştırmalarda ilk olarak 16. yüzyılda kullanılmaya başlanan içerik analizi, o dönemde gazetelerde geçen dini söylemlerin ne ölçüde yer aldığını tespit etmek için uygulansa da günümüz anlamında içerik analizi, ilk olarak 20. yüzyıl başlarında çalışmalarda yer almaya başlamıştır. 1930'lu yıllarda Harold Laswell ve çalışma

arkadaşları, içerik analizi yöntemine başvurarak çeşitli araştırmalar yürütmüşlerdir. 1960'lı yıllarda ise gelişen teknolojiler ile içerik analizi yöntemi, bilgisayar programlarına entegre edilerek daha fazla verinin incelenmesine ve daha az hata payı ile bulguların değerlendirilmesine yaramıştır. Bilimsel araştırmalarda sıklıkla tercih edilen bir yöntem haline gelen içerik analizi, günümüzde özellikle sosyal bilimler alanında pek çok dalda güvenilir bir yöntem olarak kullanılmaktadır. İletişim bilimine katkıları ile tanınan düşünür John Fiske, 'İletişim Çalışmalarına Giriş' adlı eserinde içerik analizinden bahsederken, 'iletilerin açık olan içeriğinin nesnel ölçülebilir ve doğrulanabilir bir açıklamasını yapabilmek amacıyla kullanılmaktadır' ifadelerini kullanmıştır. Kitle iletişim araçlarına yönelik yürüttüğü çalışmaları ile tanınan Bernard Berelson ise içerik analizini tanımlarken 'objektifliğe' vurgu yaparak, 'iletişimin açıklanan içeriğinin yansız, sistematik sayısal tanımlarını yapan bir araştırma tekniği' ifadelerini kullanmaktadır (Metin & Ünal, 2022, s. 276-277). Çalışmanın yöntemi olarak belirlenen içerik analizinde, seçilen konuya yönelik bulguların detaylı bir analizi yapılmaktadır. Bu sayede araştırmaya konu olan örneklemdaki genel yönelimler tespit edilmekte ve elde edilen araştırma sonuçları, gelecekte yapılması planlanan aynı bağlamdaki çalışmalar için güvenilir bir kaynak olabilmektedir.

3.1.1. İki Aşamalı Akış Teorisi

Medyanın ve kitle iletişim araçlarının nasıl bir mantıkla çalıştığını, kitleler üzerinde nasıl bir etkiye sahip olduğunu ve siyasi tercihler üzerindeki payını araştırmak için Paul Lazarsfeld, Bernard Berelson ve Hazel Gaudet tarafından 1944 yılında yapılan The People's Choice (Halkın Seçimi) çalışması, kitle iletişim araçları ve etkileri açısından literatürdeki öncü araştırmalardan birisidir. Araştırma sonucunda ortaya konulan 'iki aşamalı akış' tezi, iletişim alanında 'sınırlı etkiler dönemini' başlatmıştır. Kitle iletişim araçlarının, kitleler üzerindeki etkisinin sanılanın aksine oldukça sınırlı olduğu savunulan bu dönemdeki kuramlar, medyanın insanları doğrudan değil dolaylı olarak etkilediğini ve kitlelerin, medya aracılığıyla verilen mesajlara karşı oldukça seçici davrandığını savunmuştur. Medya mesajlarının kitleleri doğrudan etkilediğini varsayan önceki modellerin aksine, bu teori daha ayrıntılı bir etki sürecinden bahsetmekteydi. Verilen mesajın iki ayrı aşamada aktığını öne süren yaklaşıma göre, mesaj kitle iletişim araçlarından ilk olarak kanaat önderlerine; ardından da kanaat önderlerinden daha geniş bir kitlelere yayılıyordu. Bu model, sosyal medyanın ve kanaat önderlerinin kamuoyunu

şekillendirmede önemli bir rol oynadığı günümüz dijital çağında da geçerliliğini korumaktadır (Aytekin, 2020, s. 27).

İki aşamalı akış modeline göre, mesajların hedef kitleye ulaşmasında kanaat önderleri merkezi bir rol oynamaktadır. Kitle iletişim araçları tarafından iletilen mesajlar, doğrudan geniş kitlelere değil, önce kanaat önderlerine ulaşır. Kanaat önderleri, aldıkları bu mesajları kendi yorum ve bakış açılarıyla şekillendirip dönüştürerek, etkiledikleri gruplara iletirler. Bu süreçte mesajın içeriği, kanaat önderinin yorumuna göre değişebileceğinden, mesajı son olarak alan kitle, aslında doğrudan değil, kanaat önderinin filtresinden geçmiş haliyle mesajı almış olur. Kanaat önderi bu süreçte bir nevi eşik bekçisi görevi görmektedir.

Lazarsfeld, Berelson ve Gaudet'in çalışmalarını yürüttükleri dönemde kitle iletişim araçları olarak yer alan televizyon, gazete, radyo, dergi gibi geleneksel medya araçları bugün yerini ciddi ölçüde sosyal medya ve internet teknolojilerine bırakmış ve aslında 'kanaat önderi' kavramı da buna paralel olarak ciddi bir değişim getirmiştir. 'İki aşamalı akış' modelinin ortaya çıktığı yıllarda 'kanaat önderi' sıfatı genel olarak siyasetçilere, din adamlarına ve bazı sivil toplum kuruluşları gibi taraflara verilmekteydi. Günümüz dijital çağında ise bu sıfat, bahsi geçen tarafları aşarak içerik üreticilerine, sosyal medya fenomenlerine, sosyal medyada çok takipçisi olan kişi ve gruplara kadar çok geniş bir küme için kullanılmaktadır. Günümüzde dijital ortamda etkin olan kişi ve gruplar, yerel çevrelerin yanı sıra küresel ölçekte etki yaratmakta, kitleleri etraflarında toplamakta ve onları şekillendirebilmektedir (Güz & Demirtaş, 2020, s. 3). Bu durum toplumlar için, 'doğru ve objektif bilgilere hızlıca ulaşabilme' açısından demokratik bir kapı aralarken, sahte bilgiler ve dezenformasyonlar ile oldukça tehlikeli bir hale gelebilme potansiyeline de sahiptir. İnsanlar, sosyal mecralarda ciddi beğeni ve etkileşim almış kanaat önderlerini takip etmeyi ve benimsemeyi tercih ettikleri zaman, aslında algoritmalar aracılığıyla dijital olarak manipüle edilebileceklerini, bazı kişi ve grupların 'botlar' aracılığı ile ciddi etkileşim manipülasyonları yapabileceklerini unutmamalıdır.

Çalışma kapsamında belirlenen araştırma soruları şu şekildedir;

- Rusya-Ukrayna savaşı bağlamında trol hesaplar aracılığıyla yapılan dijital propaganda, bilgi ve iletişim teknolojilerini modern çatışma süreçlerinde nasıl stratejik bir silah haline getirmektedir?

- Dijital propaganda, modern çatışma süreçlerinde geleneksel propaganda yöntemlerinden nasıl farklılaşmaktadır ve bu değişim kamuoyu üzerinde ne tür etkiler yaratmaktadır?
- Rusya-Ukrayna savaşı sırasında trol hesaplar, dezenformasyon stratejilerini nasıl kullanmakta ve bu stratejiler kamuoyu algısını nasıl şekillendirmektedir?
- Sosyal medya platformlarında yayılan dezenformasyon ve bilgi akışı, geleneksel medya araçlarına göre ne kadar hızlı ve etkili olmaktadır ve bu durum kamuoyunun algısını nasıl etkilemektedir?

3.2. Evren ve Örneklem

Bu çalışmanın evrenini, Rusya-Ukrayna savaşında sistematik olarak trol faaliyeti yürüten X hesapları oluşturmaktadır. Henüz yeni bir alanda yapılan bu çalışmanın konusu ve ana kapsamı dolayısıyla literatür taramasında, kabul gören net bir ‘trol’ tanımına rastlanamamıştır. Bu yüzden çeşitli raporlar, teyit platformları ve makalelerden edinilen bilgilerin derlenmesiyle trol hesapların tespitinde kullanılacak olan 7 madde geliştirilmiştir. Bu maddeler, birlikte şu şekilde sıralanmaktadır:

- Trol hesaplar, sosyal medyada normal bir kullanıcıya göre belirgin şekilde daha fazla zaman geçirmekte ve daha fazla paylaşım yapmaktadır (Bradshaw & Howard, 2019, s. 8).
- Trol hesapların sosyal medya profillerindeki ‘biyografi’ kısmı genel olarak ideolojik birtakım söylemler barındırmakta, ziyaretçileri belli internet adreslerinde yönlendirmekte ya da tamamen boş olmaktadır (Seferoğlu & Doğan, 2017, s. 894).
- Trol hesapların sosyal medya profil resimlerinde stok görseller, tanınmış kişilerin fotoğrafları ya da ideolojik unsurlar gibi hesabı yöneten gerçek kişiyi ifşa etmeyecek görseller kullanılmaktadır (NATO Strategic Communications Centre of Excellence, 2021).
- Trol hesaplar belli kamusal ya da özel tanınmış figürler ile çok fazla etkileşime girmektedir (Bradshaw & Howard, 2017).
- Trol hesaplar, paylaşımlarında saldırgan bir dil kullanmakta, kutuplaştırıcı söylemlere başvurmakta ve hakarete varan içerikleri dolaşıma sokmaktadır (Assardo, 2023).

- Trol hesaplar, dezenformasyon içeren paylaşımlar yapmaktadır (Assardo, 2023).
- Trol hesaplar, sürekli aynı konuda paylaşım yapmaktadırlar (Bradshaw & Howard, 2017).

Belirtilen ifadeler doğrultusunda ve Rusya-Ukrayna savaşı konusu çerçevesinde çalışmanın evreni belirlenmiştir. Çalışmanın güvenilirliği açısından, sayılan maddelerdeki kriterlerin hepsini karşılayan X hesapları dikkate alınmıştır. Bu noktada, trol olmayan kullanıcıların da bu maddelerden herhangi birini ya da birkaçını zaman zaman uygulayabileceği gerçeği göz ardı edilmemiş ve bundan kaynaklı bir hatanın önüne geçmek için kriterlerin hepsine birden uyan hesaplar belirlenmiştir. Kriterleri karşılayan hesapların tamamını incelemek zor olacağı için, belirlenen X hesapları içerisinde 6 adet hesap amaçlı örneklem ile seçilmiş ve 1 Ocak 2024 ile 1 Ocak 2025 tarihleri arasındaki paylaşımları incelenmiştir. Belirtilen süre aralığında, farklı aylarda yapılan paylaşımlardan amaçlı örneklem ile seçimler yapılmıştır. Aynı hesaplara ait farklı aylarda yapılan paylaşımların sürekli aynı konuda ve doğrultuda olması da belirlenen trol hesap kriterlerine uyum açısından önem arz etmektedir. Rusya-Ukrayna savaşında taraflara eşit yaklaşmak ve her iki tarafın lehine paylaşım yapan hesapların stratejilerini değerlendirmek için 3 Rusya yanlısı hesap, 3 Ukrayna yanlısı hesap incelenmiştir.

3.3. Bulgular ve Verilerin Analizi

Çalışma kapsamında elde edilen veriler nicel ve nitel içerik analizi yöntemleri ile incelenmeden önce, sosyal medya trollerinin paylaşım içerikleri, incelemede kullanılacak kategorileri oluşturmak üzere sıralanmıştır. Bu kategoriler; saldırgan dil, kutuplaştırıcı dil, dezenformasyon, aşağılama, korku yaratma, düşmanlaştırma, güven zedeleme, gerçekliği çarpıtma ve Deepfake içerik üretimi olarak belirlenmiştir. Çalışma bulgularındaki ifade ve materyallerin yapıları, bu kategorilere göre değerlendirilerek Rusya-Ukrayna savaşındaki trollerin propaganda stratejileri hakkında çıkarımlar yapılmıştır.

Nicel ve nitel içerik analizi ile yapılan incelemenin sonuçları, tablolar ve grafikler halinde verilmiştir. İncelenen hesaplar arasında @Blackdiammon, @Alex_Oloyede2 ve @GeromanAT Rusya yanlısı bir tutum sergilerken; @Maks_NAFO_FELLA, @Heroiam_Slava ve @GloOuD hesapları Ukrayna yanlısı bir tutum sergilemiştir. Hesap analizleri yapılırken yazılı içerikler Türkçe'ye çevrilerek incelenmiştir.

3.3.1. Nicel İçerik Analizi

Çalışmanın bu bölümünde Rusya ve Ukrayna yanlısı trol hesapların paylaşımları, nicel içerik analizi yöntemi ile analiz edilmiştir.

Twit Numarası	Paylaşım Tarihi	Yorum/Retweet/Beğeni Sayısı	Paylaşım İçeriği	Görsel Materyal
Twit 1	30.01.2024	4/2/25	Deepfake İçerik, Güven Zedeleme	Resim
Twit 2	27.02.2024	0/1/12	Aşağılama	Resim
Twit 3	31.03.2024	56/134/681	Aşağılama, Korku Yaratma,	Video
Twit 4	26.04.2024	146/39/417	Aşağılama, Dezenformasyon, Güven Zedeleme	Resim
Twit 5	26.05.2024	226/40/661	Aşağılama	Kullanılmamış
Twit 6	30.06.2024	28/118/303	Güven Zedeleme, Kutuplaştırıcı Dil	Video
Twit 7	21.07.2024	7/9/50	Aşağılama, Güven Zedeleme	Kullanılmamış
Twit 8	21.08.2024	3/15/117	Saldırgan Dil, Korku Yaratma	Video
Twit 9	30.09.2024	18/48/455	Gerçekliği Çarpıtma, Kutuplaştırıcı Dil	Resim
Twit 10	14.10.2024	12/7/135	Korku Yaratma, Güven Zedeleme	Kullanılmamış

Tablo 1: Rusya Yanlısı @Blackdiammon Hesabının Paylaşım Tarihleri, Etkileşim Türü ve Oranları, Paylaşım İçerikleri ve Görsel Materyal Kullanımı

Tablo 1’de, Rusya yanlısı @Blackdiammon adlı X hesabının daha çok aşağılama ve güven zedelemeye yönelik paylaşımlar yaptığı görülmektedir. Hesabın paylaşımlarında deepfake içeriğe, dezenformasyona, saldırgan dile ve gerçekliği çarpıtmaya oransal olarak çok daha az yer verilirken düşmanlaştırıcı içeriklerin paylaşılmadığı görülmüştür. Kullanıcı, incelenen 10 paylaşımında görsel materyal olarak 4 kez resim, 3 kez video kullanmış; 3 kez ise paylaşımlarını herhangi bir görsel materyal kullanmadan dolaşıma sokmuştur. Kullanıcının paylaşımlarındaki etkileşim oranları ise değişkenlik göstermektedir. İncelenen paylaşımlar arasında en fazla etkileşim alan gönderide video kullanılmış ve aşağılama ile korku yaratmaya yer verilmiştir. En az etkileşim alan gönderi ise resim içeren bir aşağılama paylaşımıdır.

Twit Numarası	Paylaşım Tarihi	Yorum/Retweet/Beğeni Sayısı	Paylaşım İçeriği	Görsel Materyal
Twit 1	25.01.2024	560/363/1.825	Kutuplaştırma, Güven Zedeleme, Korku Yaratma	Resim
Twit 2	24.02.2024	907/520/3.794	Aşağılama, Saldırgan Dil	Resim
Twit 3	29.03.2024	1.081/1.602/4.707	Gerçekliği Çarpıtma, Dezenformasyon, Güven Zedeleme, Korku Yaratma,	Video
Twit 4	25.04.2024	165/74/774	Aşağılama, Güven Zedeleme	Resim
Twit 5	10.05.2024	316/101/1.329	Aşağılama	Resim
Twit 6	25.06.2024	62/112/651	Dezenformasyon, Güven Zedeleme	Resim
Twit 7	12.07.2024	507/1.632/11.500	Aşağılama, Gerçekliği Çarpıtma	Resim
Twit 8	07.08.2024	629/362/2.044	Kutuplaştırıcı Dil, Aşağılama, Düşmanlaştırma, Güven Zedeleme	Resim
Twit 9	22.09.2024	93/75/657	Aşağılama, Korku Yaratma, Saldırgan Dil, Gerçekliği Çarpıtma	Kullanılmamış
Twit 10	08.10.2024	73/124/860	Düşmanlaştırma, Korku Yaratma, Dezenformasyon.	Resim

Tablo 2: Rusya Yanlısı @Alex_Oloyede2 Hesabının Paylaşım Tarihleri, Etkileşim Türü ve Oranları, Paylaşım İçerikleri ve Görsel Materyal Kullanımı

Tablo 2’de, Rusya yanlısı @Alex_Oloyede2 adlı X hesabının daha çok aşağılama ve güven zedelemeye yönelik paylaşımlar yaptığı görülmektedir. Hesabın paylaşımlarında saldırgan dile, kutuplaştırıcı dile ve düşmanlaştırmaya oransal olarak daha az yer verilirken, deepfake içeriklerin paylaşılmadığı görülmüştür. Kullanıcı, incelenen 10 paylaşımında görsel materyal olarak 8 kez resim, 1 kez video kullanmış; 1 kez ise paylaşımlarını herhangi bir görsel materyal kullanmadan dolaşıma sokmuştur. İncelenen paylaşımlar arasında en fazla etkileşim alan gönderide resim kullanılmış ve aşağılama ile gerçekliği çarpıtmaya yer verilmiştir. En az etkileşim alan gönderi ise resim içeren bir dezenformasyon ve güven zedeleme paylaşımıdır.

Twit Numarası	Paylaşım Tarihi	Yorum/Retweet/Beğeni Sayısı	Paylaşım İçeriği	Görsel Materyal
Twit 1	31.01.2024	189/313/2.292	Aşağılama, Dezenformasyon, Korku Yaratma, Düşmanlaştırma	Kullanılmamış
Twit 2	29.02.2024	5/9/121	Aşağılama, Düşmanlaştırma, Gerçeği Çarpıtma	Kullanılmamış
Twit 3	30.03.2024	107/100/863	Dezenformasyon, Aşağılama, Güven Zedeleme,	Kullanılmamış
Twit 4	30.04.2024	73/255/1.664	Aşağılama, Güven Zedeleme, Korku Yaratma	Video
Twit 5	31.05.2024	77/278/1.842	Dezenformasyon, Korku Yaratma, Aşağılama, Saldırgan Dil, Güven Zedeleme	Kullanılmamış
Twit 6	28.06.2024	12/24/243	Aşağılama, Dezenformasyon	Kullanılmamış
Twit 7	29.07.2024	44/95/640	Gerçeği Çarpıtma, Düşmanlaştırma	Kullanılmamış
Twit 8	31.08.2024	21/70/416	Gerçeği Çarpıtma, Güven Zedeleme	Kullanılmamış
Twit 9	31.10.2024	24/43/941	Güven Zedeleme, Aşağılama, Saldırgan Dil, Düşmanlaştırma	Kullanılmamış
Twit 10	30.11.2024	5/83/615	Gerçeği Saptırma, Güven Zedeleme	Kullanılmamış

Tablo 3: Rusya Yanlısı @GeromanAT Hesabının Paylaşım Tarihleri, Etkileşim Türü ve Oranları, Paylaşım İçerikleri ve Görsel Materyal Kullanımı

Tablo 3'te, Rusya yanlısı @GeromanAT adlı X hesabının daha çok aşağılama ve güven zedelemeye yönelik paylaşımlar yaptığı görülmektedir. Hesabın paylaşımlarında en az saldırgan dil kullanıldığı görülmüş; deepfake içeriklerin ve kutuplaştırıcı dilin kullanılmadığı tespit edilmiştir. Kullanıcı, incelenen 10 paylaşımında görsel materyal olarak 1 kez video kullanırken, hiç resim kullanmamış; 8 paylaşımında ise herhangi görsel materyale yer vermemiştir. İncelenen paylaşımlar arasında en fazla etkileşim alan gönderide görsel materyal kullanılmamış ve paylaşımın aşağılama, dezenformasyon, korku yaratma ve düşmanlaştırma içerdiği tespit edilmiştir. İncelenen paylaşımlar arasında kullanıcının en az etkileşim alan gönderisinde ise görsel materyal kullanılmazken paylaşımın gerçekliği çarpıtma, düşmanlaştırma ve aşağılama içerdiği görülmüştür.

Twit Numarası	Paylaşım Tarihi	Yorum/Retweet/Beğeni Sayısı	Paylaşım İçeriği	Görsel Materyal
Twit 1	29.02.2024	23/71/848	Korku Yaratma, Güven Zedeleme	Video
Twit 2	30.03.2024	4/28/315	Korku Yaratma, Güven Zedeleme	Video
Twit 3	30.04.2024	8/44/485	Korku Yaratma, Güven Zedeleme	Video
Twit 4	31.05.2024	12/26/363	Korku Yaratma, Güven Zedeleme	Video
Twit 5	30.06.2024	15/115/1.025	Korku Yaratma, Güven Zedeleme	Video
Twit 6	31.07.2024	51/142/1.688	Dezenformasyon, Deepfake İçerik, Aşağılama	Resim
Twit 7	31.08.2024	10/193/1.662	Korku Yaratma, Güven Zedeleme	Resim-Video
Twit 8	30.09.2024	14/207/2.030	Korku Yaratma, Güven Zedeleme	Video
Twit 9	31.10.2024	7/84/910	Korku Yaratma, Güven Zedeleme	Video
Twit 10	31.12.2024	22/113/1.326	Korku Yaratma, Güven Zedeleme	Video

Tablo 4: Ukrayna yanlısı @Maks_NAFO_FELLA Hesabının Paylaşım Tarihleri, Etkileşim Türü ve Oranları, Paylaşım İçerikleri ve Görsel Materyal Kullanımı

Tablo 4’te, Ukrayna yanlısı @Maks_NAFO_FELLA adlı X hesabının daha çok korku yaratma ve güven zedelemeye yönelik paylaşımlar yaptığı görülmektedir. Hesabın paylaşımlarında deepfake içeriğe, dezenformasyona, düşmanlaştırmaya ve aşağılamaya oransal olarak çok daha az yer verilirken; gerçekliği çarpıtma, kutuplaştırıcı dil ve saldırgan dile hiç yer verilmediği görülmüştür. Kullanıcı, incelenen 10 paylaşımında görsel materyal olarak 8 kez video, 1 kez resim, 1 kez ise hem resim hem video kullanmıştır. İncelenen paylaşımlar arasında en fazla etkileşim alan gönderide video kullanılmış ve korku yaratma ile güven zedelemeye yer verilmiştir. En az etkileşim alan gönderi ise videolu bir paylaşımdır. Paylaşım, korku yaratma ve güven zedeleme içeriklidir.

Twit Numarası	Paylaşım Tarihi	Yorum/Retweet/Beğeni Sayısı	Paylaşım İçeriği	Görsel Materyal
Twit 1	30.01.2024	8/78/886	Korku Yaratma, Aşağılama, Güven Zedeleme	Video
Twit 2	28.02.2024	0/11/98	Korku Yaratma, Aşağılama, Güven Zedeleme	Video
Twit 3	31.03.2024	5/27/143	Aşağılama	Resim
Twit 4	30.04.2024	6/26/211	Korku Yaratma, Aşağılama, Güven Zedeleme	Video
Twit 5	31.05.2024	16/44/404	Korku Yaratma, Aşağılama, Güven Zedeleme	Video
Twit 6	29.06.2024	8/35/298	Güven Zedeleme, Dezenformasyon	Resim
Twit 7	31.07.2024	2/30/321	Korku Yaratma, Aşağılama, Güven Zedeleme, Kutuplaştırma	Video
Twit 8	29.08.2024	1/19/115	Korku Yaratma, Aşağılama, Güven Zedeleme, Gerçeği Saptırma	Video
Twit 9	28.09.2024	4/57/404	Korku Yaratma, Aşağılama, Güven Zedeleme,	Video
Twit 10	29.10.2024	0/28/117	Deepfake İçerik, Aşağılama, Korku Yaratma	Video

Tablo 5: Ukrayna yanlısı @Heroiam_Slava Hesabının Paylaşım Tarihleri, Etkileşim Türü ve Oranları, Paylaşım İçerikleri ve Görsel Materyal Kullanımı

Tablo 5’te, Ukrayna yanlısı @Heroiam_Slava adlı X hesabının daha çok karşıt tarafı aşağılamaya yönelik paylaşımlar yaptığı görülmektedir. Hesabın paylaşımlarında oransal olarak en az kutuplaştırıcı dil, gerçekliği çarpıtma, deepfake içerik ve dezenformasyon kullanıldığı tespit edilmiştir. Düşmanlaştırma ve saldırgan dile ise incelenen paylaşımlar arasında rastlanmamıştır. Kullanıcı, incelenen 10 paylaşımında görsel materyal olarak 8 kez video kullanırken, 2 kez ise resim kullanmıştır. İncelenen paylaşımlar arasında en fazla etkileşim alan gönderide görsel materyal olarak video kullanılmış, içerikte korku yaratma, aşağılama ve güven zedeleme tespit edilmiştir. En az etkileşim alan gönderinin görseli de video olarak tespit edilmiş, bu paylaşımında da korku yaratma, aşağılama ve güven zedeleme ifadelerine yer verilmiştir.

Twit Numarası	Paylaşım Tarihi	Yorum/Retweet/Beğeni Sayısı	Paylaşım İçeriği	Görsel Materyal
Twit 1	31.01.2024	30/294/3.256	Korku Yaratma, Güven Zedeleme,	Video
Twit 2	26.02.2024	4/5/163	Dezenformasyon	Kullanılmamış
Twit 3	29.03.2024	44/150/1.303	Aşağılama, Korku Yaratma, Güven Zedeleme	Video
Twit 4	30.04.2024	14/237/2.369	Aşağılama, Korku Yaratma, Güven Zedeleme	Video
Twit 5	28.05.2024	26/212/1.553	Güven Zedeleme, Korku Yaratma	Video
Twit 6	29.06.2024	368/467/4.497	Saldırgan Dil, Gerçeği Saptırma, Korku Yaratma, Güven Zedeleme	Video
Twit 7	30.07.2024	30/173/1.581	Aşağılama, Güven Zedeleme, Korku Yaratma	Video
Twit 8	30.08.2024	160/1.077/9.537	Güven Zedeleme, Korku Yaratma, Kutuplaştırıcı Dil	Video
Twit 9	30.09.2024	9/78/690	Güven Zedeleme, Korku Yaratma, Aşağılama	Video
Twit 10	31.10.2024	38/230/1.813	Güven Zedeleme, Korku Yaratma, Aşağılama, Gerçeği Saptırma	Video

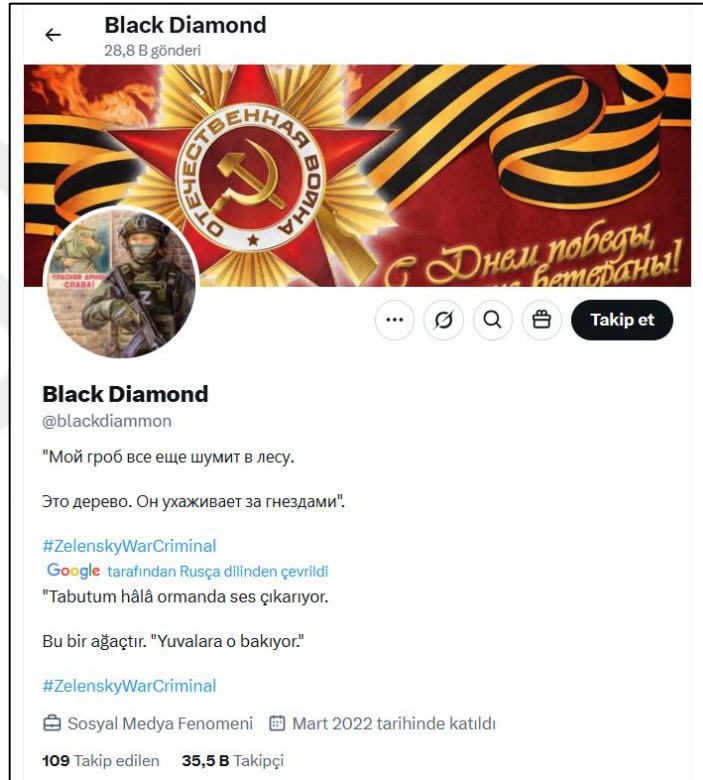
Tablo 6: Ukrayna yanlısı @GloOuD Hesabının Paylaşım Tarihleri, Etkileşim Türü ve Oranları, Paylaşım İçerikleri ve Görsel Materyal Kullanımı

Tablo 6’da Ukrayna yanlısı @GloOuD adlı X hesabının daha çok korku yaratma ve güven zedelemeye yönelik paylaşımlar yaptığı görülmektedir. Hesabın paylaşımlarında kutuplaştırıcı dile, dezenformasyona ve saldırgan dile oransal olarak çok daha az yer verilirken; düşmanlaştırmaya ve deepfake içeriklere yer verilmediği saptanmıştır. Kullanıcı, incelenen 10 paylaşımında görsel materyal olarak 9 kez video kullanmış, hiç resim kullanmamış; bir paylaşımını ise herhangi bir görsel materyal kullanmadan dolaşıma sokmuştur. İncelenen paylaşımları arasında en fazla etkileşim alan gönderisinde video kullanan hesap, bu paylaşımında güven zedeleme, korku yaratma ve kutuplaştırıcı dile yer vermiştir. En az etkileşim alan gönderisi ise görsel materyal içermezken dezenformasyon içerikli bir paylaşımıdır.

3.3.2. Nitel İçerik Analizi

Çalışmanın bu bölümünde Rusya ve Ukrayna yanlısı trol hesapların paylaşımları, nitel içerik analizi yöntemi ile bütüncül bir biçimde analiz edilmiştir. İncelenen hesapların profilleri de çalışmaya dahil edilmiş ve her hesap için üç adet paylaşım nitel içerik analizi çerçevesinde yorumlanmıştır.

3.3.2.1. Rusya Yanlısı @Blackdiammon Paylaşımlarının Nitel İçerik Analizi



Görsel 1. @Blackdiammon Hesabının X Profili

@Blackdiammon hesabının profilinde açıkça ideolojik öğeler ve sloganlar dikkat çekmektedir. Mart 2022 tarihinde X platformuna katılan hesap 29 bine yakın paylaşım yapmıştır. Kullanıcı, incelenen paylaşımlarında genel olarak aşağılama ve güven zedeleme içeriklerine yer vermiştir.



Görsel 2: @Blackdiammon Hesabına Ait İncelenen ‘8’ Numaralı Twit

Gönderilerinin büyük çoğunluğunda görsel materyale yer verdiği görülen hesabın sansürsüz şiddet içeriklerine de yer verdiği görülmekte, böylece hem Ukrayna kamuoyunu hem de sahadaki Ukrayna askerlerini korkutmak istediği anlaşılmaktadır. Görsel 2’de verilen video içeriğinde kullanıcı, Ukrayna Ordusu’na ait bir askeri aracın Ruslar tarafından patlayıcı ile imha edildiği bir video yayınlamıştır. Videoda Ukrayna tarafına ait askeri aracın kasıtlı ya da kasıtsız bir şekilde bir köpeği ezdiği görülmektedir. Drone kamerasına yansıyan görüntülerde köpek ezildikten kısa bir süre sonra araç vurulmaktadır. @Blackdiammon hesabı yazılı olarak ‘Ukrayna’ya ait bir kamyon, Kursk bölgesindeki Rubanşçina Köyü’nde bir köpeğe çarptı ve zırhlı araçla birlikte bir Lancet tarafından anında imha edildi’ ifadelerini kullanmış ve görüntülerde yaşananları anlatmıştır. Son kısımda ise küfürlü bir ifadeye de yer vererek ‘kimsenin onları özlemeyeceğini’ söylemiş ve Ukrayna askerlerini şeytanlaştıran bir dil kullanmıştır. Videonun hassas görüntüler içermesi Ukrayna tarafı üzerinde psikolojik anlamda olumsuz bir etki bırakacak niteliktedir ve karşı tarafa yönelik ‘kötüleyici’ bir algı yaratma amacıyla olduğu görülmektedir.



Görsel 3: @Blackdiammon Hesabına Ait İncelenen ‘4’ Numaralı Twit

Görsel 3’teki gibi Rusya ve Rus ordusunu yücelten paylaşımlarıyla birlikte @Blackdiammon hesabının Ukrayna tarafına umutsuzluk aşılayacak paylaşımlar yaptığı da dikkat çekmektedir. Görsel 3’te kullanıcı, ‘Ukrayna kaybediyor ve bu konuda yapabileceğiniz hiçbir şey yok’ ifadelerini kullanarak Rus olduğu anlaşılan bir asker görseli paylaşmıştır. Görseldeki askerin etrafında efektif bir şekilde dumandan oluşan bir ‘Z’ işareti vardır. Bu işaret Ukrayna-Rusya savaşında Rusları sembolize eden bir figür haline gelmiş hem propaganda amacıyla hem de savaş alanındaki Rus askerleri ayırt ederek ‘dost ateşini’ önlemek için kullanılmıştır (BBC News Türkçe, 2022). Görseldeki Rus askerinin tam donanımlı bir imaj yaratması da dikkati çekmektedir. Bu imaj ile ‘caydırıcı’ ve ‘savaşa hazır’ algısı yaratılmak istenmiştir. Yazılı ifadede geçen Ukrayna’nın ‘kaybettiği ve çözümün olmadığı’ iması ise karşı tarafa yönelik bir korku yaratma amacı taşımakta ve psikolojik olarak olumsuz bir etki bırakmayı amaçlamaktadır.

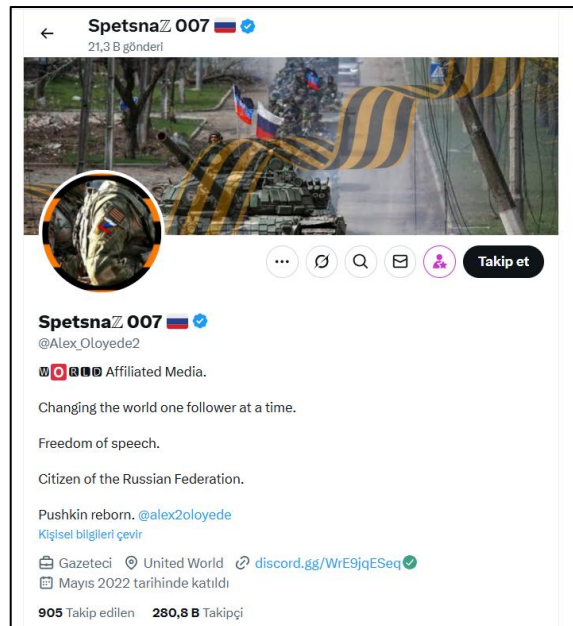
Ayrıca hesap, Görsel 4’te olduğu gibi deepfake teknolojisini kullanarak Zelenski’yi ve eşini suçlu göstermeye de çalışmıştır. Görselde, Ukrayna Devlet Başkanı Volodimir Zelenski ile eşi Olena Zelenska, bir masadaki büyük miktar paranın baş ucunda oturmaktadır. Görsel başka bir kullanıcının twiti alıntılanarak verilmiştir. Görece fazla etkileşim almayan bu paylaşımdaki görselin orijinal hali ise tersine görsel arama yöntemi ile bulunmuş, Zelenski ve eşinin yerinde ABD’li profesyonel boksör Floyd Mayweather olduğu tespit edilmiştir. Yazılı metin kullanılmayarak paylaşılan görsel ile Rusya-

Ukrayna Savaşı'ndan, Ukrayna'nın 'seçkin' sınıfı ve siyasetçilerinin kâr elde ettikleri algısı yaratılmaya çalışılmıştır.



Görsel 4: @Blackdiammon Hesabına Ait İncelenen '1' Numaralı Twit

3.3.2.2. Rusya Yanlısı @Alex_Oloyede2 Paylaşımlarının Nitel İçerik Analizi



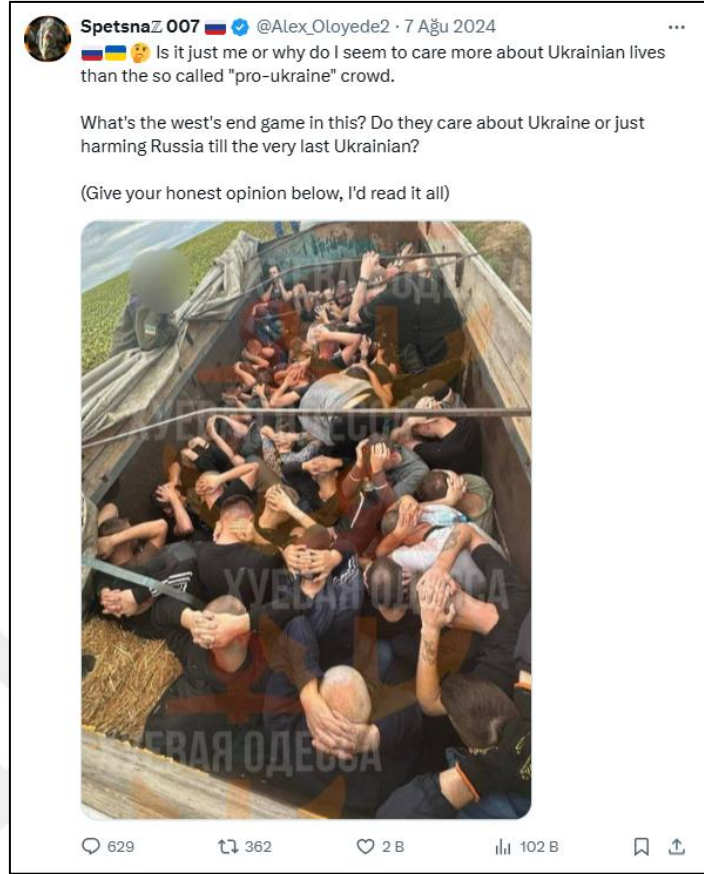
Görsel 5. @Alex_Oloyede2 Hesabının X Profili

@Alex_Oloyede2 hesabının Mayıs 2022’de X platformuna katıldığı görülmekte ve 21 binin üzerinde paylaşım yaptığı görülmektedir. Kullanıcı profiline bakıldığı zaman ideolojik öğelerin varlığı dikkat çekmektedir. Ayrıca hesabın, profilini ziyaret edenleri farklı bir adrese yönlendirmek için bir bağlantı bıraktığı da görülmektedir.



Görsel 6. @Alex_Oloyede2 Hesabına Ait İncelenen ‘2’ Numaralı Twit

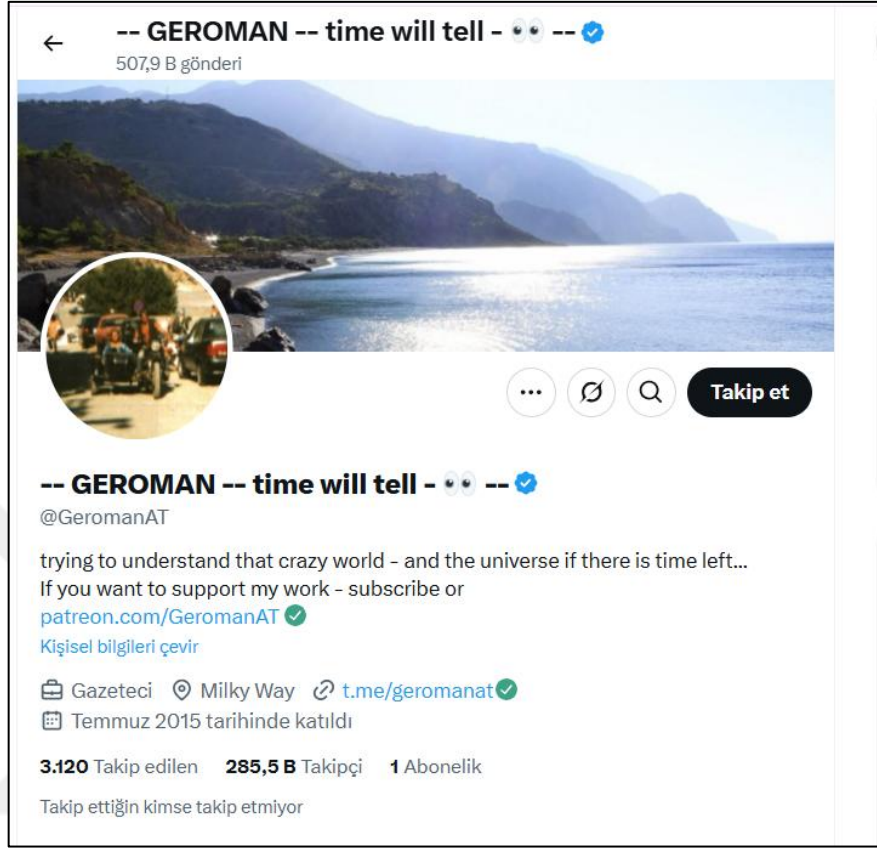
@Alex_Oloyede2 adlı kullanıcı paylaşımlarında büyük çoğunlukla aşağılayıcı içeriklere yer vermiştir. Görsel 6’da anlaşılabileceği üzere paylaşımlarda Ukrayna’nın milli değerlerine küfredildiği görülürken aynı zamanda Ukrayna tarafına yönelik, savaşın sebebinin kendi yöneticileri ve uluslararası destekçileri olduğu algısı da yaratılmak istenmiştir. Bu paylaşımında kullanıcı, Ukrayna bayrağı üzerinde aşağılayıcı biçimde bir küfür kullanarak ‘Ukrayna’ya, Zelenskiy’e ve diğer Nazilere ne söylemek istersiniz?’ sorusu ile diğer sosyal medya kullanıcılarını yorum yapmaya teşvik etmeye çalışmıştır. Kullanıcının bir milletin milli değerlerine aşağılayıcı bir dille yaklaşmasının yanı sıra Ukrayna tarafını ‘Nazi’ olarak da tanımlaması, kitleler üzerinde Ukrayna’ya yönelik olumsuz bir algı bırakmak istediğine işaret etmektedir. Çünkü ‘Naziler’ olarak nitelendirilen Alman Hükümetinin ve devlet başkanlarının adı soykırım suçu ile anılmakta ve dünyanın pek çok ülkesinde kamuoyu tarafından Naziler olumsuz bir biçimde anılmaktadır.



Görsel 7. @Alex_Oloyede2 Hesabına Ait İncelenen ‘8’ Numaralı Twit

Görsel 7’de olduğu gibi bazı paylaşımlarında ise ‘Ukraynalılara üzüldüğü’ algısı yaratmaya çalışan kullanıcı, Ukrayna kamuoyuna Zelenski yönetimi tarafından ‘yalan söylendiğini’ de iddia etmiştir. Kullanıcının Görsel 7’deki paylaşımında bir kamyon kasasında yer alan ve tamamı erkeklerden oluşan onlarca kişinin yer aldığı bir görsel verilmiştir. Görselde kamyonun kenarında Ukrayna peçi takan bir kişi durmakta ve kasadaki kişiler ise ‘teslim olma’ pozisyonunda durmaktadırlar. @Alex_Oloyede2 bu kişilerin Ukraynalı olduklarını iddia etmiştir. Yapılan araştırma sonrasında bu kişilerin askere gitmek istemeyen kaçaklar oldukları ve Ukraynalı görevliler tarafından yakalandıkları anlaşılmıştır (Enovosty, 2024). Paylaşımında ise @Alex_Oloyede2 adlı kullanıcı bu kişilere Ukraynalılardan ve Batı ülkelerinden daha fazla üzüldüğünü belirtmiştir. Bu doğrultuda kullanıcının Ukrayna tarafında, ‘Rusya merhametlidir’ algısı yaratmaya çalıştığı anlaşılmaktadır. Batılı ülkelerin Ukrayna’yı ‘umursamadıkları’ iddiası da yazı olarak sunulurken diğer sosyal medya kullanıcılarına fikirlerini belirtmeleri yönünde bir not da paylaşımında verilmiştir.

3.3.2.3. Rusya Yanlısı @GeromanAT Paylaşımlarının Nitel İçerik Analizi



Görsel 8. @GeromanAT Hesabının X Profili

@GeromanAT hesabının Temmuz 2015'te X platformuna katıldığı görülmekte ve 508 bine yakın paylaşım yaptığı anlaşılmaktadır. Kullanıcı profiline bakıldığı zaman ziyaretçileri bir bağlantı aracılığıyla hayran bağış sayfasına yönlendirmek istediği görülmektedir.

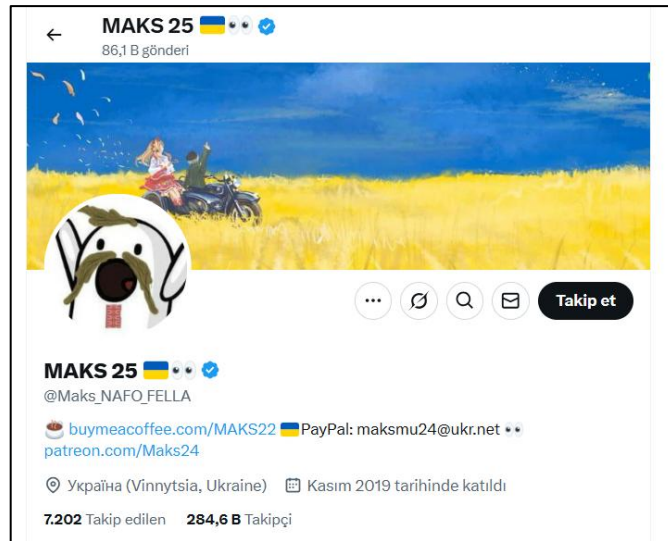
Paylaşımlarında daha çok aşağılayıcı içeriklere yer verdiği görülen kullanıcının Rusya-Ukrayna savaşında NATO ve Batı ülkelerini doğrudan suçladığı ve propagandasını Ukrayna üzerinden adı geçen yapılara karşı yürüttüğü de tespit edilmiştir. Görsel 9'da 'NATO Ukrayna'da şimdi daha hızlı kaybediyor' ifadesini kullanan kullanıcı, savaşın sadece Ukrayna-Rusya savaşı olmadığı algısını yaratarak Rusya'nın Ukrayna'da aslında NATO ile savaştığı mesajını vermiştir. Bu savaşı 'NATO'nun kaybettiğini' söyleyen kullanıcı, NATO ve Ukrayna saflarının 'başsız tavuklar gibi panik halinde olduklarını ve aptalca hareket ettiklerini' belirtmiştir. Kullanıcının, gücüne vurgu yapmak amacıyla

Rusya'nın sadece Ukrayna ile savaşmadığı buna rağmen savaşı kazandığı algısını yaratmak istediği anlaşılmaktadır. Bu tarz söylemlerin Ukrayna kamuoyunda ve ordusunda olumsuz bir etki bırakılabileceği gibi NATO müttefiki ülkelerin kitlelerini de etkileme potansiyeli olduğu söylenebilir. Ayrıca kullanıcı, paylaşımlarının büyük bölümünde görsel materyale yer vermemiş, yazılı yorumlar halinde gönderilerini oluşturmuştur.



Görsel 9. @GeromanAT Hesabına Ait İncelenen '1' Numaralı Twit

3.3.2.4. Ukrayna Yanlısı @Maks_NAFO_FELLA Paylaşımlarının Nitel İçerik Analizi



Görsel 10. @Maks_NAFO_FELLA Hesabının X Profili

@Maks_NAFO_FELLA hesabının profilinde ideolojik ögeler olduğu görülmekte ve ziyaretçileri farklı internet sayfalarına yönlendiren bağlantılar bulunmaktadır. Kasım 2019 tarihinde X platformuna katılan hesap 86 binin üzerinde paylaşım yapmıştır.

Kullanıcı, incelenen paylaşımlarında genel olarak korku yaratma ve güven zedeleme içeriklerine yer vermiştir. Gönderilerinin büyük çoğunluğunda görsel materyale yer veren hesap, gönderilerinin çoğunda sansürsüz şiddet içeriklerine de yer vermiştir. Bu doğrultuda Görsel 11’de olduğu gibi sahadaki Rusya aleyhine savaş görüntülerinin sunulduğu paylaşımların Rusya tarafına yönelik bir propaganda malzemesi olduğu anlaşılmaktadır. Kullanıcı bu paylaşımında savaş alanında öldürülen Rus askerlerinin görüntülerini video olarak sansürsüz biçimde paylaşmış ve görüntülerin Ukrayna’nın Avdiivka şehri yakınlarında çekildiğini yazmıştır. Sansürsüz şiddet görüntülerinin ve hassas içeriklerin insan psikolojisi üzerindeki etkisi düşünüldüğünde paylaşımın Rus Ordusu ve Rus kamuoyunda olumsuz bir etki yaratacağı anlaşılmaktadır. Ayrıca görüntülerde yer alan ölü sayısı da ‘güç’ algısı yaratmak açısından etkili bir noktadır.



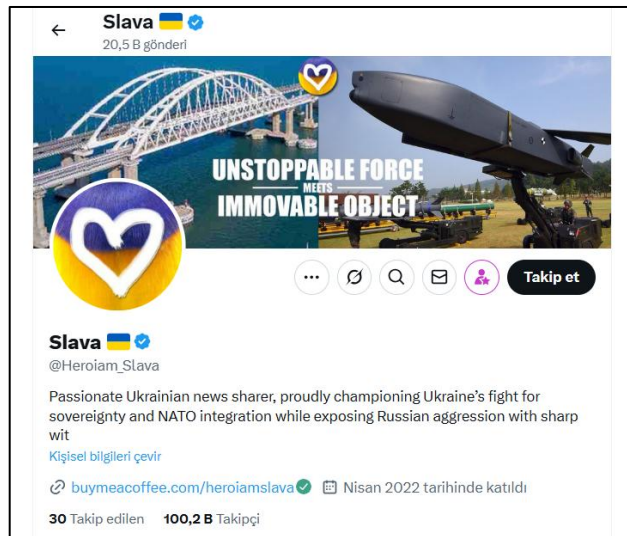
Görsel 11. @Maks_NAFO_FELLA Hesabına Ait İncelenen ‘1’ Numaralı Twit

Ukrayna ordusunu yücelten paylaşımlar yapan kullanıcının, deepfake içerik ürettiği de görülmektedir. Deepfake içeriğe örnek olarak Görsel 12’deki ‘koruma zırhlı helikopter’ paylaşımı gösterilebilecektir. Rusya, düşmana ait patlayıcı yüklü dronların tank ve zırhlı araçlara direkt olarak temas etmemesi ve böylece saldırı etkisinin azalması amacıyla Görsel 12’deki gibi ‘koruyucular’ yapmaktadır (Erbaş, 2023). Buradan hareketle Rusların helikopterlere de aynı tarzda koruyucular yapacağı manipülasyonu ironik bir dille sunulmuş ve alaycı bir tavırla bu paylaşım dolaşıma sokulmuştur.



Görsel 12. @Maks_NAFO_FELLA Hesabına Ait İncelenen ‘6’ Numaralı Twit

3.3.2.5. Ukrayna Yanlısı @Heroiam_Slava Paylaşımlarının Nitel İçerik Analizi



Görsel 13. @Heroiam_Slava Hesabının X Profili

@Heroiam_Slava hesabının profilinde ideolojik ögeler olduğu görülmekte ve ziyaretçileri farklı internet sayfalarına yönlendiren bağlantılar bulunmaktadır. Nisan 2022 tarihinde X platformuna katılan hesap 20 binin üzerinde paylaşım yapmıştır.

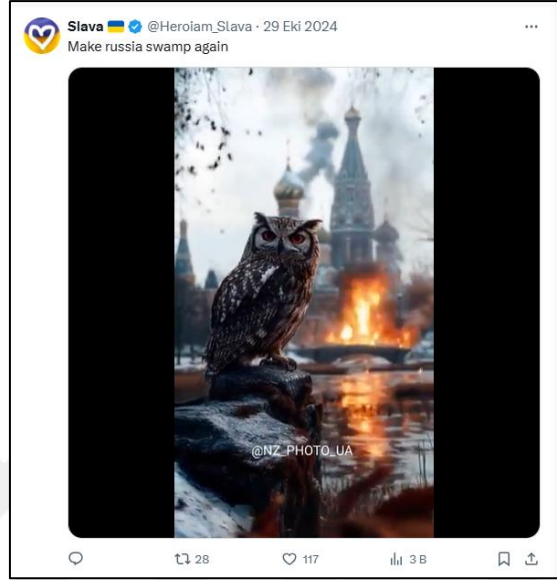


Görsel 14. @Heroiam_Slava Hesabına Ait İncelenen ‘5’ Numaralı Twit

Kullanıcı, incelenen paylaşımlarında genel olarak aşağılama içeriklerine yer vermiştir. Bunlardan birisi olan Görsel 14’teki paylaşımında @Heroiam_Slava, kamikaze dron tarafından vurulmaya çalışılan bir Rus askerinin panik anlarına ait bir videoyu paylaşmıştır. ‘Rus işgalci korkuyla saldırı tüfeğini drona fırlattı ve bir kaçış oyunu başladı’ notuyla dolaşıma sokulan twitte asker ‘işgalci’ olarak nitelendirilmiş ve aslında ölümü ‘haklılaştırılmaya’ çalışılmıştır. Metinde geçen ‘korkuyla’ vurgusu ise Ukrayna tarafına yönelik bir ‘güç’ imajı yaratmaya yöneliktir. Ayrıca bu hassas anlar bir ‘oyun’ olarak nitelendirilmiş ve alaycı bir dil ile sansürsüz görüntüler verilmiştir. Tüm bunlar Rusya tarafında ciddi motivasyon kırıklığına sebep olabilecektir.

Gönderilerinin büyük çoğunluğunda görsel materyale yer veren hesap, gönderilerinin ciddi bir kısmında sansürsüz şiddet içeriklerine de yer vermiştir. Bu şiddet görüntüleri savaş alanında Rusya aleyhine gelişen olayların aşağılayıcı bir dil ile verilmesiyle dolaşıma sokulmuştur. Ukrayna ordusunu yücelten paylaşımlar yapan

kullanıcının, deepfake içerikler ürettiği de görülmektedir. Görsel 15'teki paylaşımında deepfake teknolojisini kullanarak Rusya'yı sembolize eden yapıların ve Rus şehirlerinin yıkıldığını video ile tasvir eden kullanıcı bu paylaşımıyla Rus milli değerlerine saldırmıştır.



Görsel 15. @Heroiam_Slava Hesabına Ait İncelenen '10' Numaralı Twit

3.3.2.6. Ukrayna Yanlısı @GloOouD Paylaşımlarının Nitel İçerik Analizi



Görsel 16. @GloOouD Hesabının X Profili

@GloOouD hesabının profilinde ideolojik ögeler olduğu görülmekte ve ziyaretçileri farklı internet sayfalarına yönlendiren bağlantılar bulunmaktadır. Haziran 2022 tarihinde X platformuna katılan hesap 22 bine yakın paylaşım yapmıştır.



Görsel 17. @GloOouD Hesabına Ait İncelenen ‘7’ Numaralı Twit

Kullanıcı, incelenen paylaşımlarında genel olarak korku yaratma ve güven zedeleme içeriklerine yer vermiştir. Görsel 17’de @GloOouD, dron saldırısı ile bir Rus tankının imha edildiği görüntüleri paylaşmıştır. Sansürsüz olarak verilen görüntülerde şiddetli bir patlama olduğu izlenmekte ve kullanıcı bu duruma alaycı bir atıf yaparak ‘Mürettebat hayatta kaldı mı’ sorusunu sormaktadır. Paylaşım Rusya tarafında korku etkisi yaratacak niteliktedir.

Gönderilerinin genelinde görsel materyale yer veren hesap, yaptığı paylaşımların çoğunda sansürsüz şiddet içeriklerine de yer vermiştir. Bu şiddet görüntüleri savaş alanında Rusya aleyhine gelişen olaylardan oluşmaktadır. Görüntüler, Rusya kamuoyuna ve ordusuna yönelik güçlü bir propaganda potansiyeline sahiptir. Görsel 18’deki paylaşımda yer alan metinde bu görüntüleri bir başka Rus askerinin çektiği ve ‘Burası kardeşlerimizin hiçbir topçu hazırlığı yapılmadan anlamsız saldırılara gönderildiği

cehennem yeridir' ifadelerini kullandığı iddia edilmiştir. Fakat videoda herhangi bir konuşmanın geçmediği anlaşılmaktadır. Kullanıcı burada ölen askerlerin 'Ukrayna mevzilerine anlamsız şekilde saldırdıklarını' belirtmiş ve bu savaşın Rusya tarafı için 'sonu olmayan' ve 'anlamsız' bir savaş olduğu imasını yapmıştır. Dolayısıyla motivasyon kırmak için böyle bir söylem kullanıldığı anlaşılmaktadır. Gönderide yer alan metnin sonunda ise videoda 'tüm ölülerin olmadığı' belirtilerek ölen asker sayısının daha fazla olduğu ima edilmiştir. Bu durum da Rusya tarafında olumsuz psikolojik etkiler yaratmaya yöneliktir.



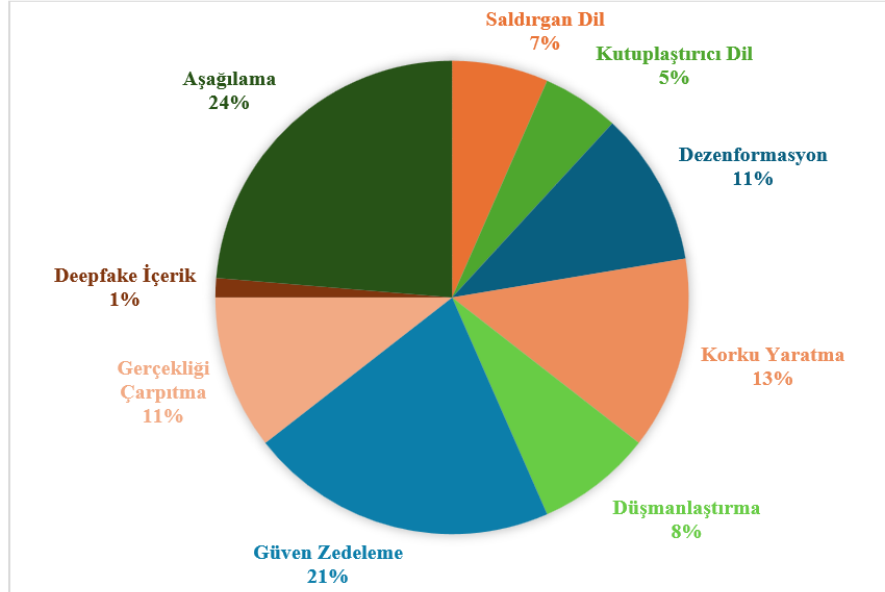
Görsel 18. @GloOuD Hesabına Ait İncelenen '8' Numaralı Twit

3.4. Tartışma

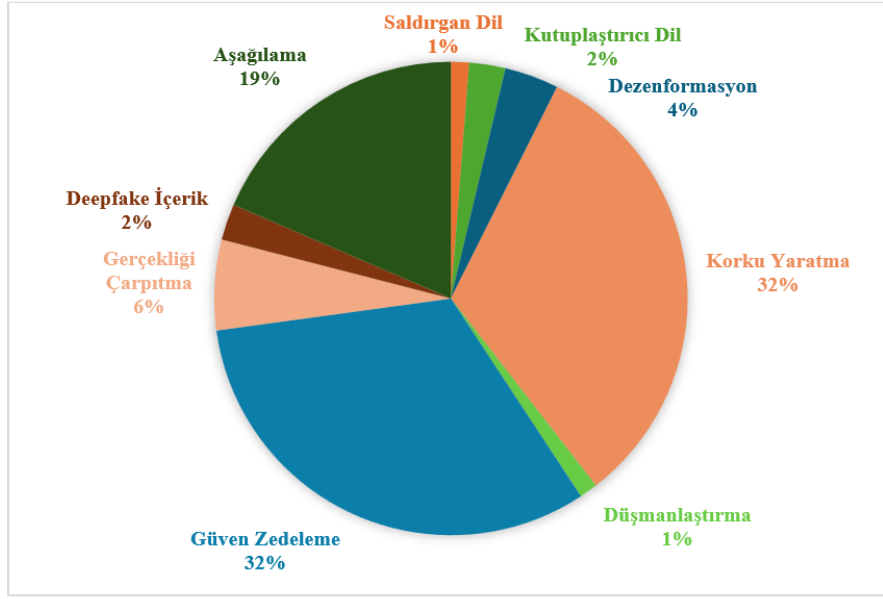
Çalışmanın bu kısmında, araştırmaya uygulanan nicel ve nitel içerik analizi sonucunda elde edilen bulgular karşılaştırmalı olarak değerlendirilmiş ve Ukrayna ile Rusya yanlısı olduğu tespit edilen trollerin genel davranışları bulgular doğrultusunda tartışılmıştır. Bu kapsamda ilk olarak nicel veri bulguları karşılaştırmalı bir şekilde değerlendirilmiş; ardından ise nitel içerik analizi bulguları karşılaştırmalı biçimde ele alınmıştır. Ayrıca çalışmanın araştırma soruları da bulgular ışığında bu bölümde değerlendirilmiştir.

	Ukrayna Yanlısı	Rusya Yanlısı
Saldırgan Dil	1	5
Kutuplaştırıcı Dil	2	4
Dezenformasyon	3	8
Aşağılama	15	18
Korku Yaratma	26	10
Düşmanlaştırma	1	6
Güven Zedeleme	26	16
Gerçekliği Çarpıtma	5	8
Deepfake İçerik	2	1

Tablo 7: Rusya ve Ukrayna Yanlısı Troll Hesapların Paylaşımlarında Kullandıkları İçerikler



Grafik 1: Rusya Yanlısı Troll Hesapların Paylaşımlarında Kullandıkları İçeriklerin Yüzdelik Oranları



Grafik 2: Ukrayna Yanlısı Trol Hesapların Paylaşımlarında Kullandıkları İçeriklerin Yüzdelik Oranları

Tablo 7’de Rusya ve Ukrayna yanlısı trol hesapların paylaşımlarının içerik oranları toplanmış, Grafik 1 ve Grafik 2’de ise ayrı ayrı bu oranların yüzdelik oranları sunulmuştur. Bulgulara göre Rusya yanlısı trollerin gönderilerinde yüzde 24 oranıyla en çok aşağılama yer almaktadır. Bunu yüzde 21 oranında güven zedeleme ve yüzde 13 oranında korku yaratma içerikleri takip etmektedir. Rusya yanlısı trollerin gönderilerinde en az oranda tespit edilen içerik yüzde 1 oranıyla deepfake içeriklerdir.

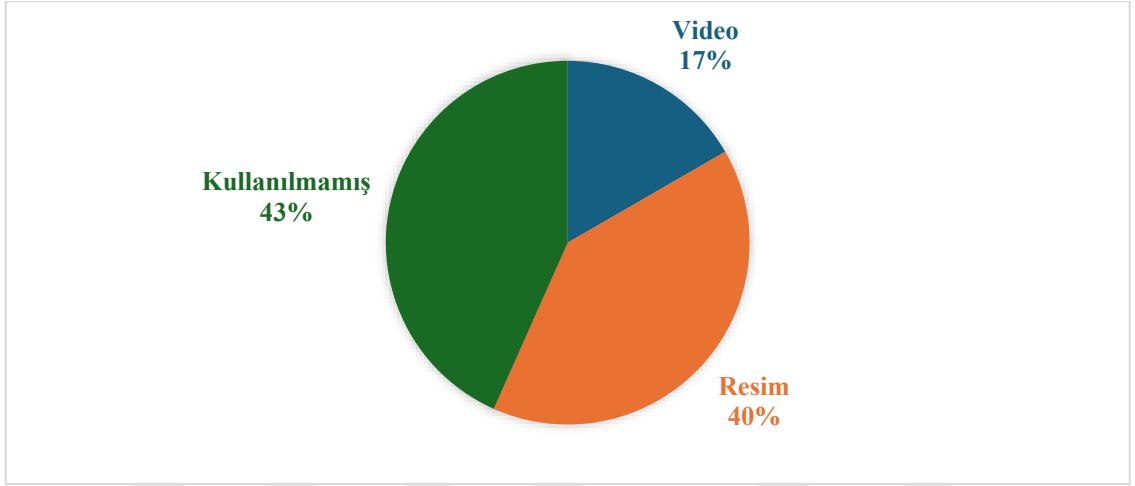
Tablo ve grafik verilerine dayanarak Ukrayna yanlısı hesapların paylaşımlarında yüzde 32 oranıyla aynı düzeyde güven zedeleme ve korku yaratma içeriklerinin olduğu tespit edilmiştir. Bu oranı takiben paylaşımların yüzde 19 oranında aşağılama ve yüzde 6 oranında gerçekliği çarpıtıcı içerik barındırdığı görülmüştür. Ukrayna yanlısı hesapların gönderilerde en az kullandıkları içerikler ise saldırgan dil ve düşmanlaştırma olarak kayda geçmiştir.

Karşılaştırmalı bir yaklaşım ile yüksek oranlar incelendiğinde, Ukrayna yanlısı trollerin güven zedeleyici ve korku yaratıcı içerikleri Rusya yanlısı trollere göre daha fazla paylaştığı tespit edilmiştir. Rusya yanlısı troller ise gönderilerinde Ukrayna yanlısı trollere kıyasla daha fazla aşağılayıcı içerik kullanmıştır. Oransal olarak Rusya tarafı en

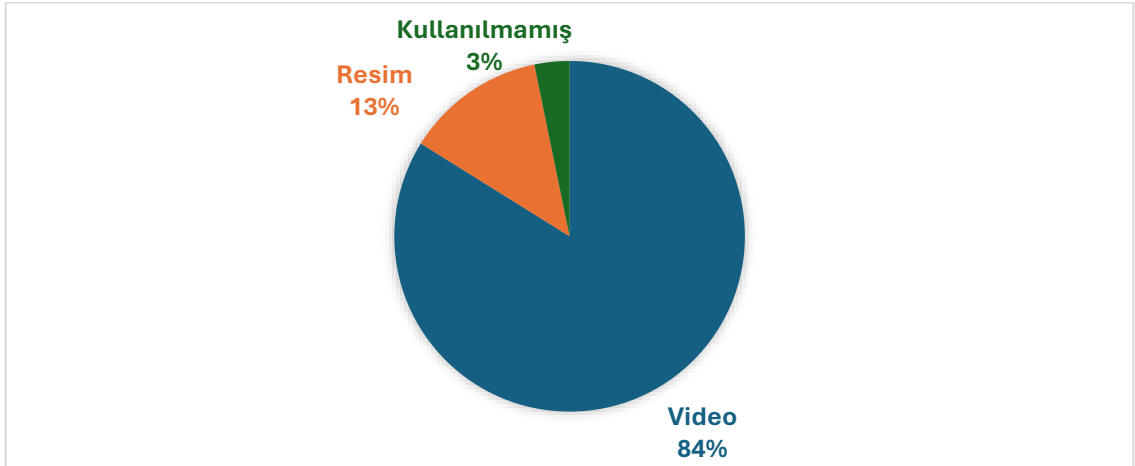
az deepfake içeriklere yer verirken; Ukrayna tarafının paylaşımlarında en az kullanılan içeriklerin düşmanlaştırma ve saldırgan dil olduğu görülmüştür.

Görsel Materyal	Ukrayna Yanlısı	Rusya Yanlısı
Video	26	12
Resim	4	5
Kullanılmamış	1	13

Tablo 8: Rusya ve Ukrayna Yanlısı Trol Hesapların Paylaşımlarında Kullandıkları Görsel Materyaller



Grafik 3: Rusya Yanlısı Trol Hesapların Paylaşımlarında Kullandıkları Görsel Materyallerin Yüzde Oranları



Grafik 4: Ukrayna Yanlısı Trol Hesapların Paylaşımlarında Kullandıkları Görsel Materyallerin Yüzde Oranları

Tablo 8’de Rusya ve Ukrayna yanlısı trol hesapların paylaşımlarında kullanılan görsel materyal sayıları toplanmış, Grafik 3 ve Grafik 4’te ise ayrı ayrı bu rakamların yüzdelik oranları sunulmuştur. Bulgulara göre Rusya yanlısı trollerin gönderilerinde görsel materyaller önemli ölçüde kullanılmamıştır. Yüzde 40 oranıyla resim; yüzde 17 oranıyla ise videolu paylaşımlar yapılmıştır. Ukrayna yanlısı trollerin paylaşımlarında ise yüzde 84 oranında video kullanıldığı görülmektedir. Bu gönderilerde yüzde 13 oranında resim kullanılırken yüzde 3 oranında herhangi bir görsel materyal kullanılmamıştır.

Araştırmaya uygulanan nitel içerik analizinin sonuçları karşılaştırmalı şekilde değerlendirildiğinde, Ukrayna yanlısı trol hesapların paylaşımlarında ciddi ölçüde şiddet içerikleri olduğu görülmüştür. Savaş sahasındaki hassas görüntüler bu içeriklerin neredeyse tamamını oluşturmakta ve herhangi bir sansür uygulanmadan verildiği görülmektedir. Rusya yanlısı trol hesapların paylaşımlarında bu tarz içeriklerin daha az olduğu görülürken, bu hesapların genel olarak Ukrayna tarafını ‘küçük gören’ paylaşımlar yaptıkları ve savaşın tarafı olarak Batı ülkeleri ile NATO’yu da gösterdikleri tespit edilmiştir. Öte yandan Rusya yanlısı trol hesapların içeriklerindeki duygusal ve yumuşak söylemin daha çok Ukrayna’daki sivil halka yönelik olduğu görülürken; Ukrayna tarafı aynı söylemi Rus askerlere karşı kullanmıştır. Burada ortaya çıkan farktan da anlaşılacağı üzere Rusya tarafı düşman tarafın kamuoyunu ‘kazanmak’ isterken Ukrayna tarafı sahada savaşan askerlerin motivasyonlarını kırarak pes ettirmek istemektedir.

Çalışmada elde edilen bulgular kapsamında araştırma soruları değerlendirildiğinde, günümüzde yürütülen savaş ve çatışma stratejilerinde dijital propagandadan aktif biçimde faydalandığı ortaya konulmuştur. Sosyal medya trolllerinin, materyal olarak herhangi bir silahın kullanılmadığı bu strateji biçiminin dijital aktörlerinden olduğu görülmüş ve üretilen propaganda içeriklerinde rakip tarafın kamuoyu, ordusu, devlet yetkilileri ve savaşın dolaylı aktörlerinin de hedef alındığı tespit edilmiştir. Kamuoyu desteği alamayan hiçbir savaşın başarılı olamayacağı tezi düşünüldüğü zaman, sanal ortamda uygulanan dijital propaganda biçimlerinin, savaş sahasına dolaylı fakat güçlü bir etkisi olduğu anlaşılmaktadır.

İçinde bulunduğumuz yüzyıl ile birlikte gelişmeye başlayan ve hızla popülerleşen dijital propaganda taktikleri, geleneksel propaganda stratejilerine kıyasla verilmek istenen mesajı neredeyse zaman ve mekân sınırı olmadan kitlelere ulaştırmaktadır. Bu

durum kitleleri geleneksel medyaya göre daha fazla etkilemekte ve propagandanın amacına ulaşmasına katkı sağlamaktadır. Öte yandan dijital araçların sağlamış olduğu içerik biçimleri ve bu içerikleri sunuş şekilleri de oluşturulan propaganda mesajlarının amacına ulaşması için güçlü bir çarpan olarak karşımıza çıkmaktadır.

Rusya-Ukrayna savaşındaki trol hesapların, paylaşımlarında çeşitli dezenformasyon stratejileri kullandıkları görülmüştür. Deepfake içerikler, yanlış yönlendirme ile yapılan manipülasyonlar ve olmayan iddiaları gerçek gibi vererek yapılan dezenformasyonların belli miktarlarda etkileşim aldıkları gözlemlenmiş ve sosyal medya kullanıcılarının dikkatlerini çektiği anlaşılmıştır. İncelemeler doğrultusunda dezenformasyon içerikli paylaşımların büyük bölümünün sansasyonel özellikler taşıması ise kitlelerin algısını şekillendirmekte güçlü bir etki yaratacağına işaret etmektedir.

İnternet ortamında dolaşıma sokulan sansasyonel içerikler, insanları duygusal biçimde uyarmakta ve böylece ciddi etkileşimler kazanmaktadırlar. Sosyal medya trolleri ise genel olarak bu durumu hedef alıp içerikler üretmekte ve geniş kitlelere yaymaktadırlar. Heyecan yaratan bu içerikler insanların paylaşma ve etkileşime girme motivasyonunu arttırarak içeriklerin viral olmalarına ve daha fazla görünürlük kazanmalarına sebep olmaktadır. Bu durum da sosyal medya platformlarını, geleneksel medyaya göre çok daha hızlı ve etkili birer propaganda yayma aracına dönüştürmektedir. Fazla etkileşim alan içerikleri ise kullanıcılar için daha ilgi çekici olmakta ve algıları istenen doğrultuda şekillendirmektedirler.

SONUÇ VE ÖNERİLER

Propagandanın insanlık tarihi içerisindeki yeri ve önemi geçmişten bugüne kadar artarak gelmiş ve aynı şekilde artarak devam etmektedir. Bu süreç boyunca teknolojik gelişmelere bağlı olarak değişen propaganda yapıları ve farklılaşan propaganda taktikleri günümüz koşullarında büyük ölçüde dijitalleşerek tarihinin en yoğun dönemini yaşamaktadır. Tarih boyunca her devletin, psikolojik üstünlük başta olmak üzere, kitleleri ikna etmek ve yönetmek gibi amaçlarla kullandığı propaganda, dünya savaşları döneminde oldukça sistematik bir şekilde uygulanmış ve propaganda üreticileri bu kavramın değerini yakından anlama fırsatı bulmuştur. 2000’li yılların başlarından itibaren günlük hayata giren internet teknolojileri ve akabindeki yıllarda kullanımı hızla yayılan akıllı telefonlar ve sosyal medya teknolojileri ile birlikte propaganda, yepyeni bir soluk kazanmış, aynı zamanda çok daha komplike bir yapıya bürünmüştür. Kitlelerin fikirlerini dile getirebildiği, yapılan toplantılar ve buluşmalar aracılığıyla sosyalleşebildiği kamusal alanlar, modern çağın sosyal medya teknolojileri ile önemli ölçüde dijitalleşmiş ve bilgiye erişim hızında ciddi gelişmeler yaşanmıştır. Öte yandan bu gelişmeler bilgi güvenilirliğine de gölge düşürerek sosyal medya platformlarında ciddi ölçülerde bilgi kirliliğine sebep olmuştur.

Modern toplumun ‘dijital kamusal alanı’ haline gelen sosyal medya platformları, başta siyasi yapılar olmak üzere propaganda üreten ve bunu kitlelere yayan her kesimin de ilgisini çekmiş ve kitleleri yönlendirebilmek adına özellikle bu mecralara yatırım yapılmaya başlanmıştır. Bu yatırımların bir parçası da çalışmanın ana konusunu oluşturan troller olmuştur. Trollük faaliyetleri bireysel yapılabildiği gibi daha sistematik ve koordinasyonlu bir şekilde, belli gruplar halinde de yapılmakta ve özellikle son dönemde devletler ve siyasi aktörlerin sosyal medya piyonları olarak karşımıza çıkmaktadır. Algıyı yönetmek, kitleleri manipüle etmek, sosyal medya üzerinden belirlenen hedeflere planlı ve koordineli saldırılar düzenlemek gibi farklı görev tanımları olan trollerin bazı devletler tarafından özellikle bu iş için eğitildikleri ve ücretli çalışanlar olarak görev yaptıkları da zaman zaman raporlanmıştır. Bu devletler arasında gösterilen Rusya, 2022 yılında Ukrayna’ya yönelik ‘özel askeri operasyon’ adı altında bir saldırı ve işgal girişimini başlatmış, bu girişim çerçevesinde sahada silahlı mücadele veren askeri ordunun yanında sosyal medya üzerinden çeşitli taktiklerle mücadele eden trol ordusunu da devreye sokmuştur. Trol orduları aracılığıyla yürütülen algı ve dezenformasyon çalışmaları

kapsamında Ukrayna kamuoyunun direncini kırmak amaçlanırken, dünya kamuoyuna dönük olarak da Ukrayna aleyhine propaganda yapılmıştır. Buna bir cevap olarak Ukrayna tarafında da sistematik trol grupları oluşmaya başlamış ve sosyal medyadaki çeşitli platformlar, Rusya ile Ukrayna'nın troller aracılığı ile yürüttükleri bir propaganda savaş alanına dönüşmüştür. Bu durum, iki ülkenin savaşı konusunda müthiş bir bilgi kirliliğine sebep olurken aynı zamanda sahada yürütülen savaşla ilgili etikten uzak, sayısız içeriğin de internet üzerinde dolaşıma sokulmasına yol açmıştır.

Çalışma kapsamında tespit edilerek incelenen trol hesapların farklı ülkeleri destekliyor olmalarına rağmen oransal olarak aynı türden propaganda içeriklerine başvurdukları tespit edilmiştir. Güven zedeleme, korku yaratma ve aşağılama söylemleri, her iki ülkenin sempatzanı olan troller tarafından en çok kullanılan yöntemler olmuştur. Bu noktada özellikle Ukrayna yanlısı trol hesapların, işgalci olarak gördükleri Rusya aleyhine sansürlü ve etik dışı materyalleri paylaşımları dikkat çekicidir. Ukrayna, sahadan servis edilen Rus askerlerinin ölüm görüntülerini aşağılayıcı bir tavırla sosyal medyada servis etmiş ve Rusya kamuoyu üzerinde moral bozukluğu, hükümete ve orduya güvensizlik ve korku gibi olumsuz etkileri yaratmaya çalışmıştır. Öte yandan Ukrayna yanlısı hesaplar, zaman zaman Rusya tarafının gerçekleştirdiği savaş suçlarını da paylaşarak uluslararası kamuoyunun desteğini almak istemiş ve Ukrayna kamuoyunu bu duruma karşı birlik olmaya teşvik etmeye çalışmışlardır. Ayrıca savaş boyunca Ukraynalı gönüllüler tarafından 'bilgi kirliliğine karşı' oluşturulduğu iddia edilen 'North Atlantic Fellas Organization' (NAFO) topluluğuna mensup kişilerin de trol davranışlar sergiledikleri ve hem manipülatif hem de etik dışı paylaşımlar yaptıkları tespit edilmiştir. Bu da faydalı bir amaç doğrultusunda sosyal medyada oluşturulan yapıların, kuralsız yapıları sebebiyle ana amaçlarının tam tersi yönüne sapabileceklerini göstermektedir.

Araştırma kapsamında incelenen Rusya yanlısı trol paylaşımlarında ise Ukrayna halkından ziyade Zelenski yönetiminin ve uluslararası camiada Ukrayna'ya aktif biçimde destek veren ülkelerin daha çok hedef alındığı tespit edilmiştir. Ukrayna'ya yönelik geniş çevrelerce 'işgal' girişimi olarak nitelendirilen hareketin meşru bir zemine oturtulması için Rusya yanlısı trollerin aktif biçimde propaganda yaptıkları anlaşılmıştır.

Sosyal medya trollerinin saldırgan yapıları ve etik değerlerden uzak tutumları, lehine paylaşımlar yaptıkları ülkelerin sosyal medyada propaganda açısından ellerini

güçlendirirken, kamuoyu açısından çok ciddi tehditleri beraberinde getirmektedir. Bu tehditler arasında hedef alınan kitlelerde büyük infiale sebep olacak hareketlerin tetiklenmesi, paylaşım yapılan konular ile ilgili sağlıklı veri ve bilgilere ulaşamaması ve doğru bilgilerin gölgede kalması, kitlelerin sistematik algı yönetimi ile haksız tarafları desteklemeleri gibi durumlar gösterilebilir. Bu yüzden tarihi yakın geçmişe kadar uzanan sosyal medya trollerine yönelik ulusal ve uluslararası çapta hızlı önlemler alınması zaruri bir durum haline gelmiştir.

Sosyal medya platformları trollerin tespiti ve engellenmesinde ana unsurlardan biri olarak karşımıza çıkmaktadır. Bu doğrultuda çeşitli platformlar tarafından yapılan çalışmalar olmasına rağmen algoritmaların mantığı gereği çok etkileşim alan paylaşımlar, içeriği sorgulanmaksızın sosyal medyada hızlı ve görünürlüğü daha da artarak yayılmaktadır. Dolayısıyla sosyal medya platformları, dezenformasyon ve etik dışı paylaşımlar konusunda radikal kararlar alarak algoritmalarındaki bu sorunu düzeltebilirler. Ayrıca sosyal medya platformlarının bu konuda daha tarafsız bir tutum sergilemeleri de kamuoyunun güvenilir ve sağlıklı bilgiye erişebilmesi için ciddi öneme sahiptir. Bu konuda Ukrayna-Rusya savaşında X platformunun sahibi Elon Musk, Ukrayna tarafına açıkça destek vermiştir. Bu şekilde savaşın bir öznesine destek veren sosyal medya platformlarına uluslararası yapılar aracılığıyla ciddi yaptırımların uygulanması, ilgili platformların politikaları üzerinde ciddi etkiler oluşturabilecektir.

Troller ve sosyal medya üzerinden yayılan dezenformasyonlar ile mücadelede teyit platformları bir diğer önemli hususu oluşturmaktadır. Fakat sivil kuruluş ya da kişilerce oluşturulan teyit platformlarından ziyade Birleşmiş Milletler gibi uluslararası birimler tarafından kurulacak olan teyit platformları, kitleler nezdinde daha güvenilir olacaktır. Çünkü sivil kişi ve kuruluşlar tarafından kurulan teyit platformlarının bulgularına, ispatlar dahilinde bile olsa kuşkuyla yaklaşılabilecektir.

Sosyal medyada her geçen gün daha fazla yayılan trollere ve olumsuz içeriklerine yönelik olarak alınabilecek güçlü bir önlem de bireylerin medya okuryazarlığı alanında farkındalık kazanması ve bunu çocukluk yıllarından itibaren devam ettirmesidir. Bu bağlamda resmi yapılara düşen görev, ilkokul çağlarından itibaren ciddi ve objektif bir kapsam ile medya okuryazarlığı eğitiminin verilmesi, yetişkin bireyler için de çeşitli kurslar ya da eğitimler ile bu eğitimin günümüz şartlarına ve yeniliklerine uygun biçimde

sunulmasıdır. Bunun yanı sıra tüm sosyal medya kullanıcılarının özellikle sansasyonel olan içeriklere yönelik kısa ve hızlı biçimde bir doğrulama araştırması yapmaları ve karşılaştıkları içerikleri, bu aşamanın ardından değerlendirmeleri de büyük önem arz etmektedir. Kullanıcıların, teyit edemedikleri paylaşımları yaymamaları ve içeriğin durumuna göre ilgili platformlara ya da resmi makamlara bildirmelerinin daha doğru olacağı da unutulmamalıdır.



KAYNAKÇA

- Abdumaminova, Z., & Ayhan, N. (2024). Medyatik Mücadele: Kırım'ın İlhakı Üzerine Rusya ve Ukrayna Perspektifleri. *Journal of Turkic Civilization Studies*, 5(1), s. 21-49.
- Acar, O. (2023). Siyasal Propaganda Bağlamında Sosyal Medya ve Kamuoyu. *Uluslararası Politik Araştırmalar Dergisi*, 9(3), s. 1-14.
- Açıkalın, Ş. N., & Canbey, M. (2022). Post-Truth Bağlamında Sosyal Medya. *İletişim Kuram ve Araştırma Dergisi*, 1(51), s. 1-11.
- Akmeşe , B., & Taşcıoğlu , R. (2024). Dijital Propagandanın Yeni Bir Versiyonu: Ukrayna-Rusya Savaşı Örneğinde Deepfake Dokümanlar Üzerine Bir Analiz. *İletişim Kuram ve Araştırma Dergisi*(66), s. 116-139.
- Arslan, G., & Ebren, Ö. (2021). Yeni Medya Ve Siyasal İletişim. *Uluslararası Medeniyet Çalışmaları Dergisi*, 6(1), s. 1-8.
- Aydın, M. (2015). Tarih Boyunca Türkiye-Ukrayna İlişkileri. *Güneydoğu Avrupa Araştırmaları Dergisi*(28), s. 31-44.
- Ayeb, M., & Bonini, T. (2024). It Was Very Hard for Me to Keep Doing That Job”: Understanding Troll Farm’s Working in the Arab World. *Social Media+ Society*, 10(1), s. 1-10.
- Aytekin, Ç. (2020). İki Aşamalı Akış Kuramı Bağlamında Instagram’daki Ünlü Destekçiler Üzerine Bir Örnek Olay Çalışması. *İletişim Çalışmaları Dergisi*, 6(1), s. 23-46.
- Aytekin, Ç. (2020). İki Aşamalı Akış Kuramı Bağlamında Instagram’daki Ünlü Destekçiler Üzerine Bir Örnek Olay Çalışması. *İletişim Çalışmaları Dergisi*, 6(1), s. 23-46.
- Aytekin, Ç., Gulmammadzada, U., & Aghayev, H. (2023). Covid-19 Aşı Karşıtlığı Tutumunda Çok Yüksek Etkileşime Sahip Trollerin Ortak Özelliklerini Belirlemeye İlişkin Bir Araştırma. *Türkiye İletişim Araştırmaları Dergisi*(42), s. 19-38.

- Balel, C. (2024). Savaş Haberlerinin Bir Propaganda Aracı Olarak Kullanımına İlişkin Eleştirel Bir Çalışma: 2003 Irak Savaşı Örneği. *Florya Chronicles of Political Economy*, 10(1), s. 37-68.
- Baptista, P., Roca, R., Gradim, A., & Loureiro, M. (2023). The Disinformation Reaction to the Russia-Ukraine War. *An International Journal of Pure Communication Inquiry*, 11(1), s. 27-48.
- Baştan, Y., & Çoban, F. (2024). Rus Dış Politikasında Siber Müdahale Yöntemi Olarak Dezenformasyon Operasyonları. *Yönetim Bilimleri Dergisi*, 22(53), s. 1205-1230.
- Bayram, Y. (2022). Dış Politik Olaylarda Siyasal Liderlik Stillerinin Medyada İnşası Üzerine Bir Analiz Denemesi: Vladimir Putin-Volodimir Zelenski Örneği. *İletişim ve Diplomasi*(9), s. 73-95.
- Bilgiç, M. S. (2014). Türkiye’de Kimlikler Arası Kutuplaşmanın Sosyal Mesafe Üzerinden Ölçümü ve Toplumsal Güvenliğe Etkisi. *Bilge Strateji Dergisi*, 6(11), s. 163-205.
- Bozkanat, E., & Göksu, O. (2020). Siyasette İknayı Robert B. Cialdını Üzerinden Okumak. *Öneri Dergisi*, 15(53), s. 77-104.
- Bradshaw, S., & Howard, P. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. University of Oxford.
- Bradshaw, S., & Howard, P. (2019). *The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation*. Oxford Üniversitesi.
- Bustanur, Hafizi, K., & Yuhelman, N. (2022). Analysis Of The Filter Bubble Algorithm In The Search For. *Jurnal Teknologi Dan Open Source*, 5(2), s. 136-141.
- Chaturvedi, S. (2016). *I Am A Troll: Inside the Secret World of the BJP's Digital Army*. Juggernaut Books.
- Chesney, B., & Citron, D. (2019). Deep Fakes: A Looming Challenge For Privacy, Democracy, And National Security. *Boston University School of Law*, 107, s. 1752-1820.

- Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C. M., Brugnoli, E., Schmidt, A. L., . . . Scala, A. (2020). The Covid-19 Social Media Infodemic. *Nature*, 10(1), s. 1-10.
- Coşkun, G. E. (2013). Propagandada Mizah Ve İroninin Yeri, Örnek: Michael Moore Sinemasi. *Doktora Tezi*. İstanbul.
- Çağlak, A. (2023). Milli Mücadele Dönemi Propaganda Çalışmalarında Kurumlararası Koordinasyon. *Ordu Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Araştırmaları Dergisi*, 13(3), s. 2895-2914.
- Çakı, C. (2018). Mitinglerin Propagandadaki Rolü: Nürnberg Mitingleri'ne Ait Fotoğrafların Göstergebilimsel Analizi. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, 5(1), s. 59-79.
- Çakı, C., & Fidan, Y. (2020). Çin Propagandasında Çin-Tayvan İlişkilerinin Sunumu: Mao Zedong Dönemi Üzerine Bir İnceleme. *Istanbul Gelisim University Journal of Social Sciences*, 7(1), s. 185-202.
- Doublet, M. (2019). *Disinformation And Electoral Campaigns*. Council of Europe.
- Erdoğan, K. (2020). Siber operasyonlar ve Jus Ad Bellum. *Yüksek Lisans Tezi*. İstanbul.
- Geneş, M., & Taydaş, O. (2024). Dezenformasyon ile Algı Yaratmak ve Bilgi Kontrolü: İsrail-Filistin Savaşı Örneği. *İletişim ve Diplomasi* (12), s. 5-24.
- Guess, A., Barbera, P., Munzert, S., & Yang, J. (2021). The Consequences Of Online Partisan Media. *Proceedings of the National Academy of Sciences*, 118(14), s. 1-8.
- Gürgen, H. (1990). Propaganda. *Kurgu Dergisi*, 8(2), s. 135-157.
- Güz, N., & Demirtaş, Z. G. (2020). Yeni Medya Çağında Siyasi Konuşma ve Kanaat Önderliği: 24 Haziran Cumhurbaşkanlığı Seçimi Örneği. *Yeni Medya Dergisi*(7), s. 1-19.
- Hansen, F. S. (2017). *Russian Hybrid Warfare: A Study Of Disinformation*. DIIS Report.
- Human Rights Council. (2018). *Report Of The Independent International Fact-Finding Mission On Myanmar*. Human Rights Council.

- Karakuş, M. (2021). Gelenekselden Dijitale Propaganda Araçlarının Dönüşümü. *Selçuk İletişim Dergisi*, 14(1), s. 462-491.
- Karataş, Z. (2015). Sosyal Bilimlerde Nitel Araştırma Yöntemleri. *Manevi Temelli Sosyal Hizmet Araştırmaları Dergisi*, 1(1), s. 62-80.
- Kayaduman, A. C. (2020). Sosyal Medya Trolllerinin Motivasyonu Ve Trolleme Çeşitleri Üzerine Bir İnceleme. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(32), s. 1-14.
- Kietzmann, J., Lee, L., McCarthy, I., & Kietzmann, T. (2020). Deepfakes: Trick or Treat? *Business Horizons*, 63(2), s. 135-146.
- Kimberly, E. (2003). Organizational Perception Management. *Research In Organizational Behavior*, 25, s. 297-332.
- Kıng, G., Pan, J., & Roberts, M. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review*, 111(3), s. 484-501.
- Kowal, P., Malicki, J., & Gawin, D. (2016). The Wars of Russia. *Warsaw East European Review*, 6, s. 25-30.
- Lewandowsky, S., Ecker, U., Seifert, C., Schwarz, N., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science In The Public Interest*, 13(3), s. 106-131.
- Mercimek, B., Yaman, N. D., Kelek, A., & Odabaşı, H. F. (2015). Dijital Dünyanın Yeni Gerçeği: Troller. *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, 6(1), s. 67-77.
- Metin, O., & Ünal, Ş. (2022). İçerik Analizi Tekniği: İletişim Bilimlerinde ve Sosyolojide Doktora Tezlerinde Kullanımı. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 22(Özel Sayı), s. 273-294.
- Mueller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. U.S. Department of Justice.
- NATO Strategic Communications Centre of Excellence. (2021). *Robotrolling*. NATO Strategic Communications Centre of Excellence.

- Niebuurt, J. T. (2021). Internet Memes: Leaflet Propaganda Of The Digital Age. *Frontiers in Communication*, 5, s. 1-14.
- Özer, N. P. (2019). Propagandada Yöntemler, Araçlar Ve Bir Propaganda Modeli Olarak; Herman Ve Chomsky Propaganda Modeli. *Kritik İletişim Çalışmaları Dergisi*, 1(1), s. 15-30.
- Paltacı, B. M. (2022). Ukrayna-Rusya Savaşı Bağlamında Siber Güvenlik Ekosistemi'Nde Yaşanan Gelişmeler Ve Değerlendirmeler. *Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi*, 2(2), s. 1-19.
- Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model. *Rand Corporation*, 2(7), s. 1-16.
- Pennycook, G., Bear, A., Collins, E., & Rand, D. (2020). The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Headlines Increases Perceived Accuracy of Headlines Without Warnings. *Management Science*, 66(11), s. 4944-4957.
- Polat, D. (2020). Nato'Nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi*, s. 135-158.
- Qualter, T. (1980). Propaganda Teorisi ve Propagandanın Gelişimi. *Ankara Üniversitesi SBF Dergisi*, 35(1), s. 255-307.
- Russell, S., & Norvig, P. (2016). *Artificial Intelligence A Modern Approach*. Pearson.
- Schulze, M., & Kerttunen, M. (2023). Cyber Operations İn Russia'S War Against Ukraine: Uses, Limitations, And Lessons Learned So Far. *SWP Comment*(23), s. 1-9.
- Scotland, J., Thomas, A., & Jing, M. (2024). Public Emotion And Response İmmmediately Following The Death Of George Floyd: A Sentiment Analysis Of Social Media Comments. *Telematics and Informatics Reports*(14), s. 1-7.
- Seferoğlu, S. S., & Doğan, D. (2017). Sosyal Medyanın Karanlık Yüzleri Trollerle İlgili Bir İnceleme. *Eğitim Teknolojileri Okumaları*, s. 887-915.

- Seppli, M. (2020). Dijital Diplomasinin Karanlık Tarafı: Online Propaganda Ve Aşırılıkçılık Karşıtlığı. *İzmir Katip Çelebi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 3(1), s. 98-102.
- Silver, L. (2019). *Misinformation And Fears About Its Impact Are Pervasive In 11 Emerging Economies*. Pew Research Center.
- Sönmezer, Z., & Büyükbaykal, A. C. (2024). Dijital Medya ve Teknolojinin Kolektif Kullanımı. *Turkish Online Journal of Design Art and Communication*, 14(3), s. 753-762.
- Stephan, L., Laura, S., David, G., Ralph, H., Jim, W., Stefanie, E., . . . Mark, L. (2020). *Technology And Democracy: Understanding The Influence Of Online Technologies On Political Behaviour And Decision-Making*. Publications Office of the European Union.
- Şenkardeş, İ. Ç. (2023). Merkeziyetsiz Kamusal Alan: Metaverse Bağlamında Kamusal Alanı Yeniden Düşünmek. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*(76), s. 149-159.
- Topçu, S. H. (2022). Rusya Federasyonu'nun Siber Güvenlik Stratejisi: Kırım Örneği. *Uluslararası İlişkiler Çalışmaları Dergisi*, 2(1), s. 19-35.
- Tuna, P. C., & Türkölmez, O. (2023). Yeni Toplumsal Hareketler ve Dijital Aktivizm. *Kamu Yönetimi ve Politikaları Dergisi*, 4(2), s. 211-240.
- U.S. Department of Justice. (tarih yok). *Report Of The Select Committee On Intelligence United States Senate Russian Active Measures Campaigns And Interference In The 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure With Additional Views*. U.S. Department of Justice.
- Uyaniker, H. B. (2018). Kırım Sorunundan Donbas Savaşına Rusya-Ukrayna Uzlaşmazlığı. *Karadeniz Araştırmaları Dergisi*, 15(59), s. 137-168.
- Walker, E., & Le, A. (2023). Poisoning the Well: How Astroturfing Harms Trust in Advocacy Organizations. *Social Currents*, 10(2), s. 184-202.

- Watson, J., Linden, S., Watson, M., & Stillwell, D. (2024). Negative Online News Articles Are Shared More To Social Media. *Scientific Reports*, 14(1), s. 1-10.
- Wilbur, T. (1958). Troll, An Etymological Note. *University of Wisconsin Press*, 30(3), s. 137-139.
- Woolley, S., & Howard, P. (2017). *Computational Propaganda Worldwide: Executive Summary*. Oxford Üniversitesi.
- World Health Organization. (2020). *Managing The Covid-19 Infodemic Call For Action*. World Health Organization.
- Yanık, H. (2024). Sosyal Medyanın Türk Seçmeninin Bilgilenme Ve Oy Verme Davranışındaki Etkisi. *Muhafazakar Düşünce Dergisi*, 20(67), s. 74-102.
- Yetkin, B. (2019). Dijitalleşen Siyasal İletişimde Bilişimsel Propaganda: Botlar. *Atatürk İletişim Dergisi*(16), s. 51-72.

İNTERNET KAYNAKLARI

- 1Kosmos. (2020). *What Is NotPetya? Biggest Modern Cyberattack in History?* 03 17, 2025 tarihinde 1kosmos.com: <https://www.1kosmos.com/security-glossary/notpetya/> adresinden alındı
- Africa Check. (2022). *What We Do?* 04 12, 2025 tarihinde Africa Check: <https://africacheck.org/what-we-do> adresinden alındı
- Aksan, S. (2023). *Mit'Ten Kritik Adım: Siber İstihbarat Başkanlığı Kuruldu*. 03 09, 2025 tarihinde TRT Haber: <https://www.trthaber.com/haber/gundem/mitten-kritik-adim-siber-istihbarat-baskanligi-kuruldu-782199.html> adresinden alındı
- Anadolu Ajansı. (2018). *Suudi trollerin hedefinde sadece muhalifler değil müttefikler de var*. 03 01, 2025 tarihinde Anadolu Ajansı: <https://www.aa.com.tr/tr/dunya/suudi-trollerin-hedefinde-sadece-muhafifler-degil-muttefikler-de-var-/1336263> adresinden alındı
- Anadolu Ajansı. (2022). *14,5 milyondan fazla Ukraynalı savaş nedeniyle ülkelerinden ayrıldı*. 03 13, 2025 tarihinde Anadolu Ajansı: <https://www.aa.com.tr/tr/dunya/14->

5-milyondan-fazla-ukraynali-savas-nedeniyle-ulkelerinden-ayrildi/2753294
adresinden alındı

Anadolu Ajansı. (2022). *NATO Genel Sekreteri Stoltenberg: Ukrayna'ya siber güvenlik ve ekipman yardımı yapma kararı aldık*. 03 18, 2025 tarihinde Anadolu Ajansı: <https://www.aa.com.tr/tr/dunya/nato-genel-sekreteri-stoltenberg-ukraynaya-siber-guvenlik-ve-ekipman-yardimi-yapma-karari-aldik/2544641> adresinden alındı

Anadolu Ajansı. (2022). *Rusya Devlet Başkanı Putin Donbas'a özel askeri operasyon kararı aldı*. 03 13, 2025 tarihinde Anadolu Ajansı: <https://www.aa.com.tr/tr/dunya/rusya-devlet-baskani-putin-donbasa-ozel-askeri-operasyon-karari-aldi/2512311> adresinden alındı

Anadolu Ajansı. (2023). *Trolleme nedir?* 02 28, 2025 tarihinde Anadolu Ajansı: <https://www.aa.com.tr/tr/teyithatti/aktuel/trolleme-nedir/1815722#:~:text=Trolleme%2C%20sosyal%20medyada%20a%C3%A7%C4%B1lan%20hesaplar,%2C%20%C5%9Fa%C5%9F%C4%B1rt%C4%B1r%C5%9F%C4%B1r%20ve%20yan%C4%B1lt%C4%B1r> adresinden alındı

Anadolu Ajansı. (2023). *Yankı Odası Nedir?* 04 01, 2025 tarihinde Anadolu Ajansı: <https://www.aa.com.tr/tr/teyithatti/blog/yanki-odasi-nedir/1815399> adresinden alındı

Antoniuk, D. (2023). *Ukraine Signs Agreement To Join Nato Cyber Defense Center*. 03 18, 2025 tarihinde The Record: <https://therecord.media/ukraine-signs-agreement-to-join-nato-cyber-defense-center> adresinden alındı

Assardo, L. (2023). *Investigating Digital Threats: Trolling Campaigns*. 03 04, 2025 tarihinde Global Investigative Journalism Network: <https://gijn.org/resource/investigating-digital-threats-trolling-campaigns/> adresinden alındı

Bartholomew, J. (2025). *First Thing: Postmortems Of Rescue Workers Killed By Israeli Troops In Gaza Show 'Gunshots To Head And Torso'*. 03 08, 2025 tarihinde The Guardian: <https://www.theguardian.com/us-news/2025/apr/17/first-thing->

postmortems-of-rescue-workers-killed-by-israeli-troops-in-gaza-show-gunshots-to-head-and-torso adresinden alındı

BBC. (2018). *Facebook admits it was used to 'incite offline violence' in Myanmar*. 03 12, 2025 tarihinde BBC: <https://www.bbc.com/news/world-asia-46105934> adresinden alındı

BBC News Türkçe. (2018). *Af Örgütü: Myanmarlı komutanların Arakanlı Müslümanlara yaptıkları insanlığa karşı suç*. 03 12, 2025 tarihinde BBC News Türkçe: <https://www.bbc.com/turkce/haberler-dunya-44627455> adresinden alındı

BBC News Türkçe. (2021). *Covid aşılarıyla ilgili komplo teorileri neler, bilim insanları bunları nasıl çürütüyor?* 03 04, 2025 tarihinde BBC News Türkçe: <https://www.bbc.com/turkce/haberler-dunya-55172316> adresinden alındı

BBC News Türkçe. (2022) *Rusya'Nın Ukrayna İşgali: 'Z' Harfi Ne Anlama Geliyor ve Nasıl İşgale Desteğin Sembolü Oldu?* 06 06, 2025 tarihinde BBC News Türkçe: <https://www.bbc.com/turkce/haberler-dunya-60657547> adresinden alındı.

BirGün. (2017). *Rusya'da asgari ücrete yüzde 26 zam*. 03 06, 2025 tarihinde BirGün: <https://www.birgun.net/haber/rusya-da-asgari-ucrete-yuzde-26-zam-167450> adresinden alındı

Buchanan, T. (2020). *Why Do People Spread False Information Online? The Effects Of Message And Viewer Characteristics On Self-Reported Likelihood Of Sharing Social Media Disinformation*. 03 23, 2025 tarihinde Plos One: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0239666> adresinden alındı

Burgess, S. (2022). *Ukraine War: Deepfake Video Of Zelenskyy Telling Ukrainians To 'Lay Down Arms' Debunked*. 03 16, 2025 tarihinde Sky News: <https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789> adresinden alındı

Council on Foreign Relations. (tarih yok). *Ukrainian IT Army*. 03 20, 2025 tarihinde Council on Foreign Relations: <https://www.cfr.org/cyber-operations/ukrainian-it-army> adresinden alındı

- Davies, H. (2015). *Ted Cruz Using Firm That Harvested Data On Millions Of Unwitting Facebook Users*. 04 04, 2025 tarihinde The Guardian: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> adresinden alındı
- Davies, K. M. (2017). *Revealed: Confessions of a Kremlin Troll*. 03 06, 2025 tarihinde The Moscow Times: <https://www.themoscowtimes.com/2017/04/18/revealed-confessions-of-a-kremlin-troll-a57754> adresinden alındı
- Dizikes, P. (2018). *Study: On Twitter, False News Travels Faster Than True Stories*. 03 11, 2025 tarihinde MIT News: <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308> adresinden alındı
- Enovosty. (2024). *An Entire Company Of Ukrainians Fleeing To Transnistria Was Detained In The Odessa Region*. 06 06, 2025 tarihinde Enovosty: https://enovosty.com/uk/news-ukr/news_society-ukr/full/0708-na-odeshhini-zatrimali-cilu-rotu-ukrainsiv-yaki-tikali-do-pridnistrovy adresinden alındı
- Erbaş, A. (2023). *Rusya'nın İHA'lara Karşı Yeni Savunma Sistemine Sahip Tankları Görüldü*. 06 08, 2025 tarihinde Defence Türk: <https://www.defenceturk.net/rusyanin-ihalara-karsi-yeni-savunma-sistemine-sahip-tanklari-goruldu> adresinden alındı
- EU DisinfoLab. (2025). *We Fight Disinformation Because We Fight For Democracy*. 04 12, 2025 tarihinde EU DisinfoLab: <https://www.disinfo.eu/we-fight-disinformation-because-we-fight-for-democracy/?tztc=1> adresinden alındı
- Euro News. (2023). *Twitter'De Uzun Süredir Aktif Olmayan Hesaplar Kalici Olarak Silinecek*. 04 01, 2025 tarihinde Euro News: <https://tr.euronews.com/2023/05/08/twitterde-uzun-suredir-aktif-olmayan-hesaplar-kalici-olarak-silinecek> adresinden alındı
- Facebook. (tarih yok). *Facebook'ta İzin Verilen Adlar*. 04 01, 2025 tarihinde Facebook: https://www.facebook.com/help/229715077154790/?locale=tr_TR adresinden alındı

- FBI. (2020). *Gru Hackers' Destructive Malware And International Cyber Attacks*. 03 17, 2025 tarihinde Federal Bureau of Investigation: <https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks> adresinden alındı
- Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The Rise of Social Bots. *Communications of the ACM*, 59(7), s. 96-104.
- Full Fact. (tarih yok). *Who We Are*. 04 12, 2025 tarihinde Full Fact: <https://fullfact.org/about/> adresinden alındı
- Gragnani, J. (2017). *Brezilyalı sosyal medya trollerinin gizli dünyası*. 03 06, 2025 tarihinde BBC News Türkçe: <https://www.bbc.com/turkce/haberler-dunya-42339450> adresinden alındı
- Habertürk. (2007). *İlk Siber Savaş*. 03 09, 2025 tarihinde Habertürk: <https://www.haberturk.com/dunya/haber/23642-ilk-siber-savas> adresinden alındı
- Hollanda Hükümeti. (2024). *Donors Accumulate 200 Million Euros For Ukraine'S Resilience In Cyberspace*. 03 18, 2025 tarihinde Government Of The Netherlands: <https://www.government.nl/documents/diplomatic-statements/2024/12/20/tallinn-mechanism> adresinden alındı
- İhlas Haber Ajansı. (2023). *Adnan Oktar Suç Örgütünün Sosyal Medyadaki Troll Ordusuna Operasyonda Yeni Detaylar*. 03 11, 2025 tarihinde İhlas Haber Ajansı: <https://www.ihb.com.tr/haber-adnan-oktar-suc-orgutunun-sosyal-medyadaki-troll-ordusuna-operasyonda-yeni-detaylar-1166185> adresinden alındı
- Independent Türkçe. (2019). *Facebook'A 5 Milyar Dolarlık Tarihi Ceza*. 04 04, 2025 tarihinde Independent Türkçe: <https://www.indyturk.com/node/54816/haber/facebook%E2%80%995-milyar-dolarl%C4%B1k-tarihi-ceza> adresinden alındı
- Iyer, P. (2024). *New Studies Shed Light on Misinformation, News Consumption and Content Moderation*. 04 07, 2025 tarihinde Tech Policy Press: <https://www.techpolicy.press/new-studies-shed-light-on-misinformation-news-consumption-and-content-moderation/> adresinden alındı

- Kharpal, A. (2020). *Twitter Takes Down China-Linked Accounts Spreading Disinformation On Hong Kong And Coronavirus*. 03 24, 2025 tarihinde CNBC: <https://www.cnbc.com/2020/06/12/twitter-takes-down-china-linked-accounts-spreading-disinformation.html> adresinden alındı
- Krever, M., & Chernova, A. (2023). *Wagner Chief Admits To Founding Russian Troll Farm Sanctioned For Meddling In Us Elections*. 03 07, 2025 tarihinde CNN: <https://edition.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html> adresinden alındı
- NATO's Strategic Warfare Development Command. (2023). *NATO Centres of Excellence – Cooperative Cyber Defence (CCD COE)*. 03 09, 2025 tarihinde NATO's Strategic Warfare Development Command: <https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe/> adresinden alındı
- NBC News. (2024). *Sen. Ben Cardin Says He Was Targeted By Apparent Deepfake Call*. 03 27, 2025 tarihinde NBC News: <https://www.nbcnews.com/politics/congress/ben-cardin-targeted-apparent-deep-fake-call-dmytro-kuleba-rcna172776> adresinden alındı
- Nigrelli, C. (2025). *Us To Halt Offensive Cyber Operations Against Russia: Reports*. 03 17, 2025 tarihinde Straight Arrow News: <https://san.com/cc/us-to-halt-offensive-cyber-operations-against-russia-reports/> adresinden alındı
- Nimmo, B., & Toler, A. (2018). *How They Did It: The Real Russian Journalists Who Exposed the Troll Factory in St. Petersburg*. 03 15, 2025 tarihinde Global Investigative Journalism Network: <https://gijn.org/stories/real-russian-journalists-exposed-troll-factory-st-petersburg/> adresinden alındı
- Oksijen Gazetesi. (2024). *Bakan Uraloğlu Doğruladı: 85 Milyonun Kimlik Bilgileri Çalındı*. 03 09, 2025 tarihinde Oksijen Gazetesi: <https://gazeteoksijen.com/turkiye/bakan-uraloglu-dogruladi-85-milyonun-kimlik-bilgileri-calindi-222721> adresinden alındı
- Ortutay, B. (2022). *Twitter says it removes 1 million spam accounts a day*. 04 01, 2025 tarihinde Associated Press: <https://apnews.com/article/elon-musk-twitter-inc->

technology-misinformation-social-media-e9fa93bc9132a4adf8535a8a34bebec9
adresinden alındı

Oxford English Dictionary. (2014). *Hashtag*. 03 26, 2025 tarihinde Oxford English Dictionary:
https://www.oed.com/dictionary/hashtag_n?tab=meaning_and_use&tl=true#301493073 adresinden alındı

Özgür, E. (2021). *Bot Hesaplar Nasıl Tespit Edilir?* 04 01, 2025 tarihinde Teyit.org:
<https://teyit.org/teyitpedia/bot-hesaplar-nasil-tespit-edilir> adresinden alındı

Petrosyan, A. (2025). *Number Of Internet And Social Media Users Worldwide As Of February 2025*. 02 28, 2025 tarihinde Statista:
<https://www.statista.com/statistics/617136/digital-population-worldwide/> adresinden alındı

Reuters. (2024). *Fact Check: Photo Shows Israeli City Of Sderot In 2023, Not 2024 Rafah Strikes*. 03 08, 2025 tarihinde Reuters: <https://www.reuters.com/fact-check/photo-shows-israeli-city-sderot-%092023-not-2024-rafah-strikes-2024-05-13/> adresinden alındı

Reuters. (2025). *Taiwan Says China Using Generative Ai To Ramp Up Disinformation And 'Divide' The Island*. 03 08, 2025 tarihinde Reuters:
<https://www.reuters.com/world/asia-pacific/taiwan-says-%09china-using-generative-ai-ramp-up-disinformation-divide-island-2025-04-08/> adresinden alındı

Robinson, P. (2021). *Is Everyone A Russian Agent Now?* 03 22, 2025 tarihinde Russia Today:
<https://www.rt.com/russia/541563-western-media-russian-agent/> adresinden alındı

Robinson, T. (2020). *Russian troll farms and the \$1 million in crypto used to influence US elections: Four Compliance Takeaways from Blockchain Insights*. 03 07, 2025 tarihinde Elliptic: <https://www.elliptic.co/blog/four-compliance-takeaways-from-blockchain-insights-one-million-russian-troll-farms-influence-us-election> adresinden alındı

- Siberay. (tarih yok). *Sanal Ortamda Bilgi Kirliliği*. 04 10, 2025 tarihinde Siberay: <https://www.siberay.com/bilgi-kirliligi> adresinden alındı
- Silverman, C., & Kao, J. (2022). *Infamous Russian Troll Farm Appears to Be Source of Anti-Ukraine Propaganda*. 03 12, 2025 tarihinde ProPublica: <https://www.propublica.org/article/infamous-russian-troll-farm-appears-to-be-source-of-anti-ukraine-propaganda> adresinden alındı
- Sofuoğlu, Y. (2020). *Trump Ve Biden Seçim İçin Facebook Sayfalarına Ne Kadar Para Harcadi?* 04 01, 2025 tarihinde İndependent Türkçe: <https://www.indyturk.com/node/266656/d%C3%BCnya/trump-ve-biden-se%C3%A7im-i%C3%A7in-facebook-sayfalar%C4%B1na-ne-kadar-para-harcad%C4%B1> adresinden alındı
- Survey Monkey. (tarih yok). *Psikografik Segmentasyon Nedir?* 04 04, 2025 tarihinde Survey Monkey: <https://tr.surveymonkey.com/market-research/resources/what-is-psychographic-segmentation/> adresinden alındı
- Şahin, Z. (2023). *Astroturfing Nedir?* 03 23, 2025 tarihinde Teyit.org: <https://teyit.org/teyitpedia/teyit-sozluk-astroturfing-nedir> adresinden alındı
- Şahin, Z. (2024). *Uluslararası Hashtag Günü: Sosyal Medya Etiketleri Ve Bilgi Ekosistemine Etkisi*. 03 26, 2025 tarihinde Teyit.org: <https://teyit.org/teyitpedia/uluslararasi-hashtag-gunu-sosyal-medya-etiketleri-ve-bilgi-ekosistemine-etkisi> adresinden alındı
- Torun, C. (2021). *Algoritma Nedir, Nerelerde Kullanılır?* 03 29, 2025 tarihinde TÜBİTAK Bilim Genç: <https://bilimgenc.tubitak.gov.tr/algoritma-nedir> adresinden alındı
- Türk Dil Kurumu Sözlüğü. (tarih yok). *Manipülasyon*. 03 11, 2025 tarihinde Türk Dil Kurumu Sözlüğü: <https://sozluk.gov.tr/> adresinden alındı
- U.S. Department of Justice. (2020). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. 03 17, 2025 tarihinde U.S. Department of Justice:

<https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and> adresinden alındı

UNESCO. (tarih yok). *Media And Information Literacy Curriculum - E-Version*. 04 10, 2025 tarihinde UNESCO: <https://www.unesco.org/mil4teachers/en/curriculum> adresinden alındı

Wilson, J. (2024). *Revealed: The Tech Entrepreneur Behind A Pro-Israel Hate Network*. 03 01, 2025 tarihinde The Guardian: <https://www.theguardian.com/world/article/2024/jun/29/daniel-linden-shirion-collective-pro-israel-palestine-hate> adresinden alındı



İNCELENEN PAYLAŞIMLARIN İNTERNET ADRESLERİ

Rusya Yanlısı @Blackdiammon Hesabına Ait İncelenen Paylaşımların Bağlantı Adresleri

Twit 1: <https://x.com/blackdiammon/status/1752186612321231051>

Twit 2: <https://x.com/blackdiammon/status/1762267847827571054>

Twit 3: <https://x.com/blackdiammon/status/1774279229049282697>

Twit 4: <https://x.com/blackdiammon/status/1783861818282152441>

Twit 5: <https://x.com/blackdiammon/status/1794762519816319241>

Twit 6: <https://x.com/blackdiammon/status/1807459625073086527>

Twit 7: <https://x.com/blackdiammon/status/1814807324197859455>

Twit 8: <https://x.com/blackdiammon/status/1826137282279305235>

Twit 9: <https://x.com/blackdiammon/status/1840620388180525398>

Twit 10: <https://x.com/blackdiammon/status/1845866750597898327>

Rusya Yanlısı @Alex_Oloyede2 Hesabına Ait İncelenen Paylaşımların Bağlantı Adresleri

Twit 1: https://x.com/Alex_Oloyede2/status/1750565632976826850

Twit 2: https://x.com/Alex_Oloyede2/status/1761331690998309180

Twit 3: https://x.com/Alex_Oloyede2/status/1773671891611377993

Twit 4: https://x.com/Alex_Oloyede2/status/1783594450352054752

Twit 5: https://x.com/Alex_Oloyede2/status/1788883745501478914

Twit 6: https://x.com/Alex_Oloyede2/status/1805688676489609717

Twit 7: https://x.com/Alex_Oloyede2/status/1811527068363989317

Twit 8: https://x.com/Alex_Oloyede2/status/1820989614322029042

Twit 9: https://x.com/Alex_Oloyede2/status/1837603353401970911

Twit 10: https://x.com/Alex_Oloyede2/status/1843484152563409145

Rusya Yanlısı @Geromanat Hesabına Ait İncelenen Paylaşımların Bağlantı Adresleri

Twit 1: <https://x.com/GeromanAT/status/1752791246341365851>

Twit 2: <https://x.com/GeromanAT/status/1763216258345189758>

Twit 3: <https://x.com/GeromanAT/status/1773987854806372451>

Twit 4: <https://x.com/GeromanAT/status/1785358757934805460>

Twit 5: <https://x.com/GeromanAT/status/1796510525754613905>

Twit 6: <https://x.com/GeromanAT/status/1806712905250828729>

Twit 7: <https://x.com/GeromanAT/status/1817945006306398266>

Twit 8: <https://x.com/GeromanAT/status/1829786248380141696>

Twit 9: <https://x.com/GeromanAT/status/1852013713181569457>

Twit 10: <https://x.com/GeromanAT/status/1862834988082770092>

Ukrayna Yanlısı @Maks_Nafo_Fella Hesabına Ait İncelenen Paylaşımların Bağlantı Adresleri

Twit 1: https://x.com/Maks_NAFO_FELLA/status/1763275711966519405

Twit 2: https://x.com/Maks_NAFO_FELLA/status/1774117847851041164

Twit 3: https://x.com/Maks_NAFO_FELLA/status/1785379867564921272

Twit 4: https://x.com/Maks_NAFO_FELLA/status/1796536908522344886

Twit 5: https://x.com/Maks_NAFO_FELLA/status/1807163383499686227

Twit 6: https://x.com/Maks_NAFO_FELLA/status/1818694793876410405

Twit 7: https://x.com/Maks_NAFO_FELLA/status/1829798053701718331

Twit 8: https://x.com/Maks_NAFO_FELLA/status/1840801497531007160

Twit 9: https://x.com/Maks_NAFO_FELLA/status/1852046021385470274

Twit 10: https://x.com/Maks_NAFO_FELLA/status/1874053475702804527

Ukrayna Yanlısı @Heroiam_Slava Hesabına Ait İncelenen Paylaşımların Bağlantı Adresleri

Twit 1: https://x.com/Heroiam_Slava/status/1752397706494869559

Twit 2: https://x.com/Heroiam_Slava/status/1762877110572474418

Twit 3: https://x.com/Heroiam_Slava/status/1774341418330316911

Twit 4: https://x.com/Heroiam_Slava/status/1785263114662941095

Twit 5: https://x.com/Heroiam_Slava/status/1796435346861015339

Twit 6: https://x.com/Heroiam_Slava/status/1807047294698569944

Twit 7: https://x.com/Heroiam_Slava/status/1818562581436457139

Twit 8: https://x.com/Heroiam_Slava/status/1829062721788113237

Twit 9: https://x.com/Heroiam_Slava/status/1840086566804566028

Twit 10: https://x.com/Heroiam_Slava/status/1851176058235523221

Ukrayna Yanlısı @Glooud Hesabına Ait İncelenen Paylaşımların Bağlantı Adresleri

Twit 1: <https://x.com/GloOuD/status/1752647497661440185>

Twit 2: <https://x.com/GloOuD/status/1762156322894553174>

Twit 3: <https://x.com/GloOuD/status/1773657069276557709>

Twit 4: <https://x.com/GloOuD/status/1785182723444719753>

Twit 5: <https://x.com/GloOuD/status/1795454604575982050>

Twit 6: <https://x.com/GloOuD/status/1807095089073627332>

Twit 7: <https://x.com/GloOuD/status/1818280420490068249>

Twit 8: <https://x.com/GloOuD/status/1829585562808033767>

Twit 9: <https://x.com/GloOuD/status/1840729403568853393>

Twit 10: <https://x.com/GloOuD/status/1852052533621170538>

EKLER

EK-1: Rusya Yanlısı @Blackdiammon Hesabının İncelenen Paylaşımları

Twit 1:



Twit 2:



Twit 3:



Twit 4:



Twit 5:



Twit 6:



Twit 7:



Twit 8:



Twit 9:



Twit 10:



EK-2: Rusya Yanlısı @Alex_Oloyede2 Hesabının İncelenen Paylaşımları

Twit 1:



Twit 2:



Twit 3:

Spetsnaz 007   @Alex_Oloyede2 · 29 Mar 2024

 Kids below 18 riding to their deaths...

With the sharp decline in men, women were conscripted to fill in the gaps, but that doesn't seem to be enough.

This is where your tax goes, we will be forced to do our jobs and the blood is on the hands of the west and Zelensky.



1 B 1 B 4 B 309 B

Okuyucular, insanların bilmek isteyebileceğini düşündükleri içerikler ekledi

These are students of the Ivan Bohun Military High School. They do not have status of a serving soldier. The age of military service in Ukraine is 18-60 years of age. Children are not being sent to the war.

The school website: kvl.mil.gov.ua
The law on military duties and military service: zakon.rada.gov.ua/laws/show/2232...

Bu size yardımcı oldu mu? **Değerlendir**

Bağlam, X uygulamasını kullanan kişiler tarafından yazılır ve başkaları tarafından Yardımcı Oldu olarak değerlendirildiğinde görüntülenir. [Daha fazlasını keşfet.](#)

Twit 4:

Spetsnaz 007   @Alex_Oloyede2 · 25 Nis 2024

 F-16 just dropped in Ukraine.

Months of talking about F-16 non-stop and this is all you have to show? Pathetic.



165 74 774 35 B

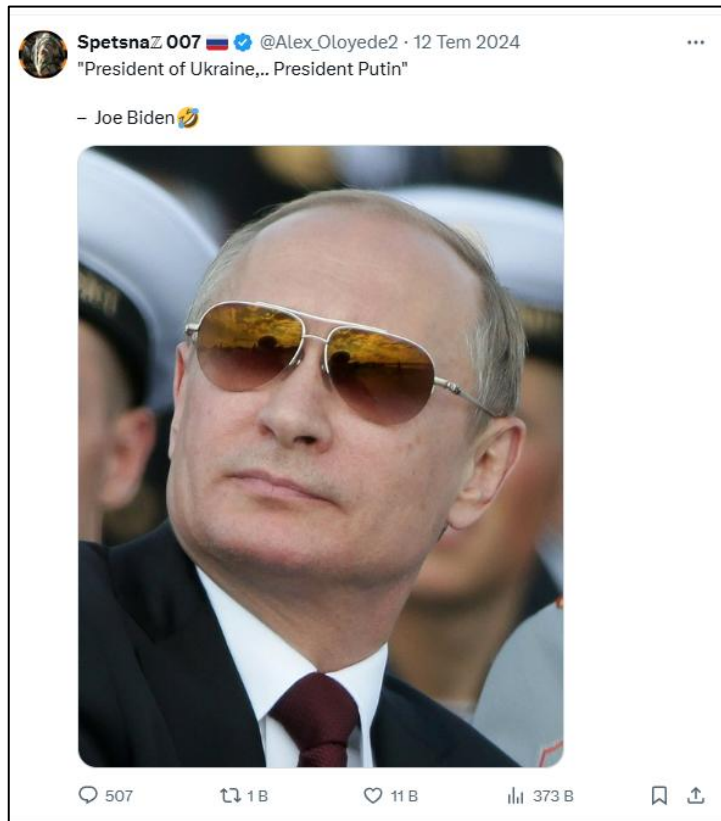
Twit 5:



Twit 6:



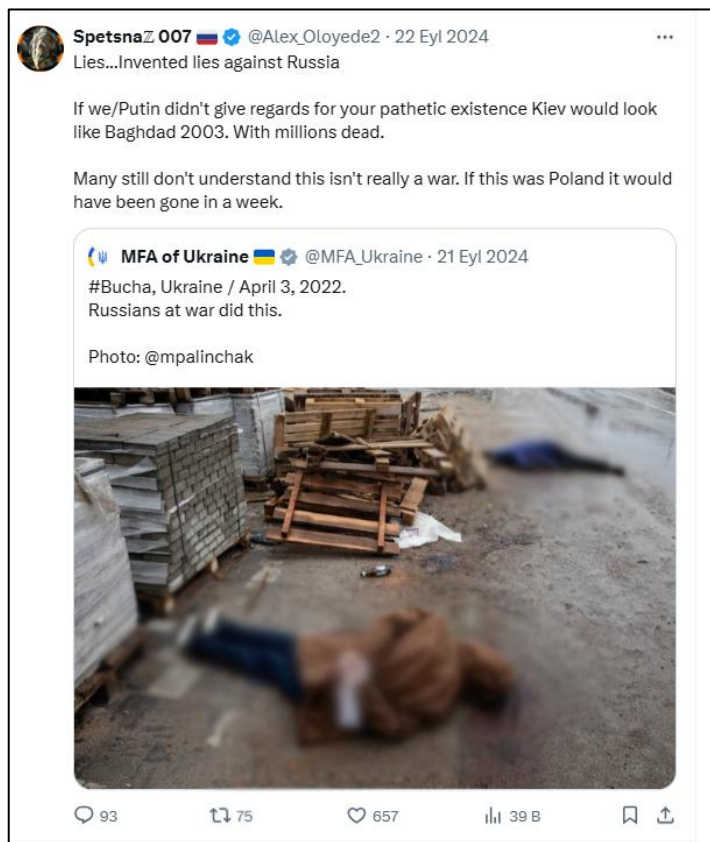
Twit 7:



Twit 8:



Twit 9:



Twit 10:



EK-3: Rusya Yanlısı @GeromanAT Hesabının İncelenen Paylaşımları

Twit 1:



Twit 2:



Twit 3:



Twit 4:



Twit 5:



Twit 6:



Twit 7:



Twit 8:



Twit 9:



Twit 10:



EK-4: Ukrayna Yanlısı @GloOouD Hesabının İncelenen Paylaşımları

Twit 1:



Twit 2:



Twit 3:



Twit 4:

 **Clooud** |  
@GloOuD

 Strike Drones Company of the 47th Mech. Brigade destroys  Russian T-72B3 tank.

«The Avdiivka direction is one of the most difficult. Our unit destroys assault groups and their equipment every day. Thanks to FPV drones, most of the assault actions in the area of responsibility of our brigade are contained.»
[Gönderiyi çevir](#)



ÖÖ 8:41 · 30 Nis 2024 · **88,5 B** Görüntüleme

14 237 2 B 36

Twit 5:

 **Clooud** |  
@GloOuD

Precision drone-dropped munition on TWO  Russian soldiers by  Ukrainian «Peacky Blinders» group.

Hearing the drone, they simply froze and a powerful munition immediately struck them..
[Gönderiyi çevir](#)



ÖS 4:58 · 28 May 2024 · **51 B** Görüntüleme

26 212 1 B 34

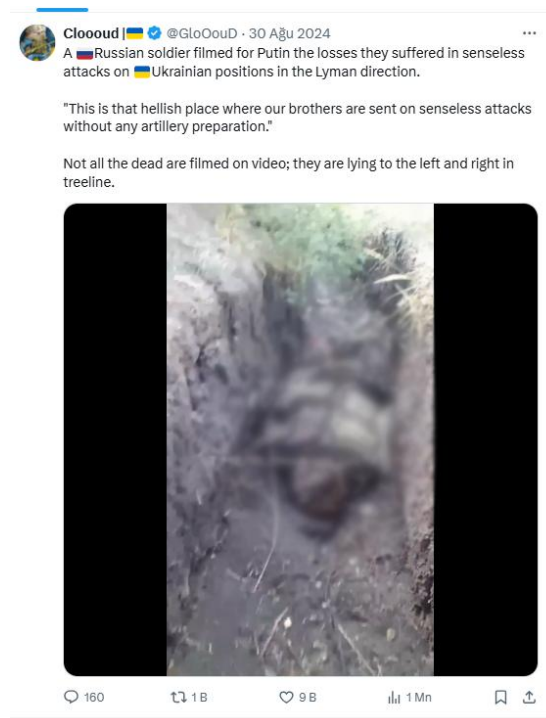
Twit 6:



Twit 7:



Twit 8:



Twit 9:



Twit 10:



Cloodud |  

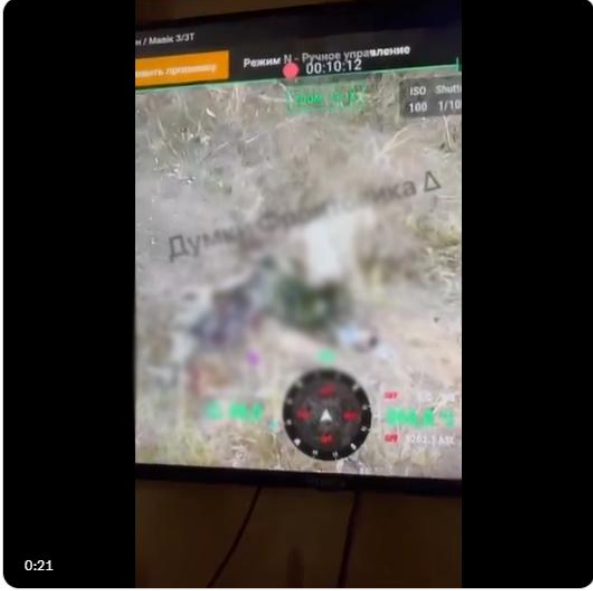
@GloOuD

Abone ol ...

Russian invader loots things left over from his comrade...

Even here, the Russians manage to steal... They don't even think about evacuating their fallen comrade.

[Gönderiyi çevir](#)



ÖS 9:18 · 31 Eki 2024 · **128,9 B** Görüntüleme

 38

 230

 1 B

 64



EK-5: Ukrayna Yanlısı @Heroiam_Slava Hesabının İncelenen Paylaşımları

Twit 1:

 **Slava**  
@Heroiam_Slava

Abone ol ...

⚡ Fireworks from a Russian machine gunner
[Gönderiyi çevir](#)



ÖS 9:25 · 30 Oca 2024 · **18,1 B** Görüntüleme

8 78 886 9

Twit 2:

 **Slava**  
@Heroiam_Slava · 28 Şub 2024

Run Ivan, run, to the Russia !



0:04

 **Slava**  
@Heroiam_Slava · 28 Şub 2024

Oops, i drop something. Found it.



0:19

11 98 9 B

Twit 3:



Twit 4:



Twit 5:



Twit 6:



Twit 7:

Slava  
@Heroiam_Slava

Operators of the 3rd Brigade's FPV drones reduce russo vehicles and livestock of the Lavrov tribe

[Gönderiyi çevir](#)



ÖÖ 11:21 · 31 Tem 2024 · 6.025 Görüntüleme

2 30 321 6

Twit 8:

Slava  
@Heroiam_Slava · 29 Ağu 2024

Russo fighters tired laying around "sleeping"



Нена в кого спитати дорогу

TikTok
@lalk430...

1 19 115 6 B

Twit 9:

 **Slava**    @Heroiam_Slava Abone ol ...

 Through good negotiations, the Russian  'visitors' made the right decision to surrender. 7 of them came out of the landing.

It was just a catch. As soon as the pilots began to leave with the Russo-occupiers, the Russian army launched a valiant attack, at their own.

A few of them were accurately mowed down - not all of them got into the good hands of our brigade...

[Gönderiyi çevir](#)



ÖS 8:49 · 28 Eyl 2024 · **15,9 B** Görüntüleme

4 57 404 8

Twit 10:

 **Slava**   @Heroiam_Slava · 29 Eki 2024 ...

Make russia swamp again



@NZ_PHOTO_UA

28 117 3 B

EK-6: Ukrayna Yanlısı @Maks_NAFO_FELLA Hesabının İncelenen Paylaşımları

Twit 1:



Twit 2:



Twit 3:

 **MAKS 24**  
@Maks_NAFO_FELLA

🔥🔥 Strike group "ACHILLES" hit enemy equipment in Ocheretyne direction:

- 1 BMP-3;
- 1 BMP-2;
- 1 T-72 tank;
- 1 car;
- 2 soldiers dead;
- 1 soldier wounded.



ÖS 9:45 · 30 Nis 2024 · 18,2 B Görüntüleme

8 44 485 3

Twit 4:

 **MAKS 24**   @Maks_NAFO_FELLA · 31 May 2024
Russians in Vovchansk 🇷🇺 18



12 26 363 30 B

Twit 5:



Twit 6:



Twit 7:

 **MAKS 24** 🇺🇦 🇷🇺 @Maks_NAFO_FELLA · 31 Ağu 2024

💣🔥 Russian convoy and crossing were destroyed in the Kursk region!



10 193 1 B 43 B

Twit 8:

 **MAKS 24** 🇺🇦 🇷🇺 @Maks_NAFO_FELLA

💣🔥 Part of the work on the destruction of the Russians in Vovchansk by 57th OMPBr.

! ~100 killed, ~25 wounded, 16 MTLB and 1 BMP-2 destroyed!

[Gönderiyi çevir](#)



ÖS 8:10 · 30 Eyl 2024 · **74,3 B** Görüntüleme

14 207 2 B 46

Twit 9:



MAKS 24 🇺🇦 🇷🇺 @Maks_NAFO_FELLA · 31 Eki 2024

...

👊 The 95th ODSHBr repelled the Russian assault and once again eliminated a group of marines from the Russian 155th brigade in Kursk region.



💬 7

↻ 84

❤ 910

📊 37 B

🔖 ⬆

Twit 10:



MAKS 24 🇺🇦 🇷🇺 @Maks_NAFO_FELLA · 31 Ara 2024

...



💬 22

↻ 113

❤ 1 B

📊 45 B

🔖 ⬆