T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İSTİHBARAT ÇALIŞMALARI ANABİLİM DALI
İSTİHBARAT PROGRAMI

YAPAY ZEKÂ TABANLI ALGORİTMA ÇAĞINDA ÖRTÜLÜ OPERASYONUN ANALİZİ: CAMBRIDGE ANALYTICA ÖRNEĞİ

YÜKSEK LİSANS TEZİ

TUĞÇE SENA KARA
1920106104

TEZ DANIŞMANI: DOÇ. DR. GÜNGÖR ŞAHİN

İSTANBUL
NİSAN 2023

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İSTİHBARAT ÇALIŞMALARI ANABİLİM DALI
İSTİHBARAT PROGRAMI

YAPAY ZEKÂ TABANLI ALGORİTMA ÇAĞINDA ÖRTÜLÜ OPERASYONUN ANALİZİ: CAMBRIDGE ANALYTICA ÖRNEĞİ

YÜKSEK LİSANS TEZİ

TUĞÇE SENA KARA
1920106104

TEZ DANIŞMANI: DOÇ. DR. GÜNGÖR ŞAHİN

İSTANBUL
NİSAN 2023

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İSTİHBARAT ÇALIŞMALARI ANABİLİM DALI
İSTİHBARAT PROGRAMI

YAPAY ZEKÂ TABANLI ALGORİTMA ÇAĞINDA ÖRTÜLÜ OPERASYONUN ANALİZİ: CAMBRIDGE ANALYTICA ÖRNEĞİ

YÜKSEK LİSANS TEZİ

TUĞÇE SENA KARA
1920106104

Tezin Enstitüye Verildiği Tarih: 05.05.2023
Tezin Savunulduğu Tarih : 05.04.2023

Tez Oy birliği ile başarılı bulunmuştur.

	Unvan Ad Soyad	İmza
Tez Danışmanı	Doç. Dr. Güngör ŞAHİN	
Jüri Üyeleri	Doç. Dr. Ali Burak DARICILI	
	Dr. Öğr. Üyesi Barış ATEŞ	

İSTANBUL
NİSAN 2023

ÖZGÜNLÜK RAPORU

Tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve ç) Sonuç kısımlarından oluşan toplam 124 sayfalık kısmına ilişkin, 28/03/2023 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı % 5'tir.

Uygulanan filtrelemeler:

1- Kaynakça hariç

2- Alıntılar hariç

3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü Lisansüstü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Usul ve Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Tuğçe Sena KARA
05.04.2023

ETİK BEYAN

Millî Savunma Üniversitesi Enstitüleri Dönem Projesi ve Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan kurallara uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir; aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bu tezdeki düşünce, görüş, varsayım, sav veya tezler bana aittir; Millî Savunma Bakanlığı ve Millî Savunma Üniversitesi ve Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü sorumlu tutulamaz.

Tuğçe Sena KARA
05.04.2023

Sevgili babamın aziz hatırasına ithaf olunur.

ÖNSÖZ ve TEŞEKKÜR

Yıllar evvel kıymetli babamın, internet ortamı ve sosyal medyanın bir dezenformasyon alanı olduğu ve bu platformlardan ulaşılan bilgilere septik yaklaşılması gerektiği yönündeki nasihatleri, konuya dair bende bir ilgi ve merak uyandırmıştı. Uluslararası İlişkiler alanında lisans eğitimi aldığım sıralar patlak veren Arap Ayaklanması hâdiseleri ile konuya siyaset bilimi perspektifinden aşina olsam da, derinlemesine bir araştırmaya yüksek lisans eğitimime kadar girişmemiştim. Bu çalışmada konunun dinamiklerine gerek teknik gerekse sosyal boyutlardan yaklaşarak mevcut durumu ortaya koyup bir öngörü perspektifi sundum. Konuya yıllar öncesinden öngörülü yaklaşımı ile bana ışık olan sevgili babama minnettarım.

Çalışmamda bana sağladığı motivasyon ve sunduğu akademik katkılarından dolayı Saygıdeğer tez danışmanım Doç. Dr. Güngör ŞAHİN'e sonsuz teşekkürlerimi sunarım. Ayrıca, Atatürk Stratejik Araştırmalar ve Lisanüstü Eğitim Enstitüsü İstihbarat Programı Arş. Gör. Kaan KILIÇ nezdinde tüm akademik kadroya ve enstitü personeline, ders dönemimde kendilerinden çok şey öğrendiğim kıymetli hocalarıma, hayatımın en zorlu dönemine denk gelmiş olmasına karşın eğitim hayatımın en güzel dönemini geçirdiğim Millî Savunma Üniversitesi'nin her bir personeline ve bu süreçte desteklerini esirgemeyen aileme en içten teşekkürlerimi sunarım.

İstanbul; Nisan 2023 Tuğçe Sena KARA

İÇİNDEKILER

Sayfa

ÖZGÜNLÜK RAPORU
ETİK BEYANI
İTHAF
TEŞEKKÜR VE ÖNSÖZ
İÇİNDEKİLER ..... **vii**
TABLOLAR LİSTESİ ..... **ix**
ŞEKİLLER LİSTESİ ..... **x**
SEMBOL LİSTESİ ..... **xi**
KISALTMALAR ..... **xii**
TÜRKÇE ÖZ ..... **xiii**
İNGİLİZCE ÖZ (ABSTRACT) ..... **xiv**
1. GİRİŞ **1**
2. KAVRAMSAL ÇERÇEVE **9**
2.1. Algoritma ve Yapay Zekâ 9
2.2. Büyük Veri: Analiz ve Analitik 13
2.3. Siber Uzay ve Siber İstihbarat 18
2.4. Psikografi 26
2.5. Sosyal Medya Analitiği 30
3. ÖRTÜLÜ OPERASYONLAR **37**
3.1. Örtülü Operasyonun Tanımlanması 38
3.2. Makul İnkâr Edilebilirliği Destekleyen Caydırıcı Unsurlar 39
3.3. Örtülü Operasyon Türleri 44
3.3.1. Paramiliter Örtülü Operasyonlar 46
3.3.2. Ekonomik Örtülü Operasyonlar 47
3.3.3. Siyasi Örtülü Operasyonlar 48
3.4. Örtülü Operasyonlarda Propagandanın Yeri ve Propaganda Türleri 49
3.5. Dış Kaynaklı Seçim Müdahaleleri ve Askerî Darbeler 53
4. CAMBRİDGE ANALYTİCA VAKASI **57**
4.1. SCL ve Cambridge Analytica 58
4.2. Cambridge Analytica ve Siyasi Kampanya Yöntemleri 63
4.2.1. Büyük Verinin Kullanımı 65
4.2.2. Sosyal Medyanın Kullanımı 67
4.2.3. Psikografinin Kullanımı 69
4.3. 2016 ABD Başkanlık Seçimlerine Müdahalelerin Yargılama Süreci 71
5. SOSYAL MEDYADA ÖRTÜLÜ OPERASYONUN ANALİZİ **75**
5.1. İstihbarat Analizi ve Bilişsel Tuzaklar 75
5.2. Stratejik İstihbarat 76
5.3. Sosyal Medyada Örtülü Operasyon 81
5.4. Rakip Hipotezlerin Analizi (Analysis Of Competing Hypotheses – ACH) 82
5.4.1. Rakip Hipotezlerin Analizi (ACH) Metodolojisi 83
5.4.2. Rakip Hipotezlerin Analizi (ACH) Uygulaması 84
5.4.3. ACH Genel Değerlendirmesi 96
5.5. Analitik Hiyerarşi Süreci (Analytical Hierarchy Process- AHP) 98
5.5.1. Analitik Hiyerarşi Süreci (AHP) Metodolojisi 99
5.5.2. Sosyal Medyada Örtülü Operasyonun Analitik Hiyerarşi Süreci (AHP) ile Analizi 103
5.6. Analiz Sonucu 116
6. SONUÇ VE ÖNERİLER **118**

KAYNAKÇA 124
ÖZGEÇMİŞ..... 139

TABLOLAR LİSTESİ

Tablo 2.1 : Kategorize Edilmiş Yapay Zekâ Tanımları 11
Tablo 5.1 : ACH Analiz Sorusu ve Hipotezler 85
Tablo 5.2 : Bilgi 1 ACH Matrisi 87
Tablo 5.3 : Bilgi 2 ACH Matrisi 88
Tablo 5.4 : Bilgi 3 ACH Matrisi 89
Tablo 5.5 : Bilgi 4 ACH Matrisi 90
Tablo 5.6 : Bilgi 5 ACH Matrisi 90
Tablo 5.7 : Bilgi 6 ACH Matrisi 91
Tablo 5.8 : Bilgi 7 ACH Matrisi 93
Tablo 5.9 : Bilgi 8 ACH Matrisi 94
Tablo 5.10 : Bilgi 9 ACH Matrisi 94
Tablo 5.11 : Bilgi 10 ACH Matrisi 94
Tablo 5.12 : Bilgi 11 ACH Matrisi 95
Tablo 5.13 : ACH Genel Değerlendirme Matrisi 96
Tablo 5.14 : AHP Kriterlerin Önem Dereceleri ve Nicel Değerleri 99
Tablo 5.15 : *n* Sayıda Kritere Göre Rassal Endeks Değerleri 102
Tablo 5.16 : Kriterlere İlişkin İkili Karşılaştırma Matrisi 107
Tablo 5.17 : Kriterlere İlişkin Normalizasyon Matrisi 107
Tablo 5.18 : Kriterlere İlişkin Öz Vektör Tablosu 108
Tablo 5.19 : Kriterlere İlişkin Özdeğer Tablosu 109
Tablo 5.20 : Kriterlere İlişkin En Büyük Özdeğer Hesaplanması 109
Tablo 5.21 : Erişim İmkânı İçin Seçeneklerin Karşılaştırılması 110
Tablo 5.22 : Erişim İmkânı İçin Normalize Edilmiş Seçenekler Matrisi, Öz Vektör, Öz Değer ve En Büyük Öz Değer 111
Tablo 5.23 : Etki İmkânı İçin Seçeneklerin Karşılaştırılması 112
Tablo 5.24 : Etki İmkânı İçin Normalize Edilmiş Seçenekler Matrisi, Öz Vektör, Öz Değer Ve En Büyük Öz Değer 112
Tablo 5.25 : Makul İnkâr Edilebilirlik İçin Seçeneklerin Karşılaştırılması 113
Tablo 5.26 : Makul İnkâr Edilebilirlik İçin Normalize Edilmiş Seçenekler Matrisi, Öz Vektör, Öz Değer Ve En Büyük Öz Değer 114
Tablo 5.27 : AHP Karar Matrisi 115
Tablo 5.28 : Seçeneklerin Önem Dereceleri 115

ŞEKİLLER LİSTESİ

Sayfa

Şekil 2.1 : Sekiz Katmanlı Siber Uzay Modeli 19
Şekil 2.2 : CITP Analtik Çerçevesi 24
Şekil 3.1 : Mark Lowenthal Örtülü Eylem Merdiveni 45
Şekil 5.1 : AHP Problemi Hiyerarşik Yapı 104
Şekil 5.2 : AHP Analiz Sonucu 116

SEMBOLLER LİSTESİ

λ	: Lambda Sembolü
Σ	: Toplam Sembolü
λ_{max}	: En büyük Özdeğer
n	: Kriter sayısı
m	: Alternatif Sayısı
x_{ij}	:i. Kriterinin j. Ölçütüne Göre Puanı
y_{ij}	**:** Normalize Edilmiş İkili Karşılaştırma Matrisi
S	: Öz vektör
s_i	: i. Kriterin Ağırlığı
s_{ij}	: i Kriterinin j Seçeneği Açısından Önem Ağırlığı
t	: Tutarlılık Sembolü
t_i	: i. Kriterin Tutarlılığı
CE	: Uyum Endeksi
RE	: Rassal Endeks
CE	: Tutarlılık Oranı
W	: Kriterlerin Ağırlıkları
D	: Karar Matrisi
A	: Alternatiflerin Nihai Öz Vektörü
A_i	: Alternatiflerin i. Kriter İçin Karşılaştırılması

KISALTMALAR

9/11	**:** 11 Eylül 2001 Saldırıları
AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
ACH	**:** Analysis of Competing Hypotheses (Rakip Hipotezlerin Analizi)
AHP	**:** Analytic Hyerarchy Process (Analitik Hiyerarşi Süreci)
AIMS	**:** Advanced Impact Media Solutions (Gelişmiş Medya Etki Çözümleri)
API	**:** Application Programming Interface (Uygulama Programlama Arayüzü)
AWS	**:** Amazon Web Services
BREXIT	**:** British Exit (Birleşik Krallık'ın Avrupa Birliğinden Ayrılması)
CFR	**:** Council on Foreign Relations
ÇHC	**:** Çin Halk Cumhuriyeti
CIA	**:** Central Intelligence Agency (Merkezi İstihbarat Teşkilatı)
GSM	**:** Global System for Mobile Communications (Küresel Mobil İletişim Sistemi)
HUMINT	**:** Human Intelligence (İnsan İstihbaratı)
I & W	**:** Indicators and Warnings (Göstergeler ve Uyarılar)
IBM	**:** International Business Machines (Uluslararası İş Makineleri)
IRA	**:** Internet Research Agency (İnternet Araştırmaları Ajansı)
IoT	**:** Internet of Things (Nesnelerin İnterneti)
NATO	**:** North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
NIST	**:** National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
SCL	**:** Strategic Communication Laboratories (Stratejik İletişim Laboratuvarları)
SOCMINT	**:** Social Media Intelligence (Sosyal Medya İstihbaratı)
YSA (ANN)	**:** Yapay Sinir Ağları (Artificial Neural Networks)
YZ (AI)	**:** Yapay Zekâ (Artificial Intelligence)
WWW	**:** World Wide Web (Dünya Çapında Ağ)

ÖZ

Yapay Zekâ Tabanlı Algoritma Çağında Örtülü Operasyonun Analizi: Cambridge Analytica Örneği

Tuğçe Sena KARA

Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü

İstanbul, Nisan 2023

Devletler, özellikle İkinci Dünya Savaşı'nın yarattığı yıkım nedeniyle konvansiyonel ve nükleer savaşlardan kaçınılan Soğuk Savaş döneminde, diplomasinin de yetersiz kaldığı durumlarda örtülü operasyonları dış politika hedeflerini gerçekleştirmede üçüncü bir seçenek olarak değerlendirmişlerdir. Örtülü operasyonun temel kavramsal özellikleri makul inkâr edilebilirlik olarak ifade edilen, eylemin izinin sponsora atfedilemeyecek şekilde gerçekleştirilmesi ve siyasi, paramiliter yahut ekonomik bir etki yaratmasıdır. Günümüzde üssel bir hızla gerçekleşen dijitalleşme sürecinin bir sonucu olan büyük veri ve yapay zekâ uygulamaları, bir etki yaratma konusunda teknoloji gücünü elinde bulunduran tarafı oldukça avantajlı bir konuma getirmiştir. Siber uzayın ontolojik olarak anonimlik ve gizliliği destekleyen bir yapıda olmasının yanı sıra, web 2.0 dönemi ile internet iletişiminin düalist bir yapıya bürünmesinin bir ürünü olan sosyal medya, makul inkâr edilebilirliği destekleyen modern bir örtülü operasyon zemini olmuştur. Söz konusu gelişmeler, yapay zekâ ile sosyal medyada örtülü operasyonun analiz edilmesi ihtiyacını doğurmuştur.

Bu bilgiler doğrultusunda bu çalışmada, yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olup olamayacağı sorunsalı analiz edilmiştir. Çalışmada Cambridge Analytica vakası örnek vaka olarak seçilmiştir. Elde edilen bulgular perspektifinde öngörüler ortaya konularak stratejik istihbarat analizi yapılmıştır. Analiz, Richards Heuer'in, Karl Popper'ın yanlışlanabilirlik ilkesi perspektifinden geliştirdiği Rakip Hipotezler Analizi (ACH) ile elde edilen subjektif bilgilerin; çok kriterli karar verme tekniklerinden biri olan ve optimal seçim hesaplamalarında kullanılan Analitik Hiyerarşi Süreci (AHP) ile nicelleştirilmesi ile gerçekleştirilmiştir. Analiz sonucunda, yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabileceği sonucuna ulaşılmıştır. Sonuç olarak elde edilen bulgulara yönelik öneriler sunulmuştur.

Anahtar Sözcükler: Yapay Zekâ, Sosyal Medya, Cambridge Analytica, Örtülü Operasyon, Stratejik İstihbarat Analizi.

Bilim Kodu	**:** 92432, 114111, 117105
Sayfa Sayısı	**:** xiv + 139
Tez Danışmanı	**:** Doç. Dr. Güngör ŞAHİN

ABSTRACT

Analysis of Covert Operation in the Age of Artificial Intelligence Based Algorithm: The Cambridge Analytica Case

Tuğçe Sena KARA

Turkish National Defense University Atatürk Strategic Studies and Graduate Institute

Istanbul, April 2023

States regarded covert operations as a third option for achieving their foreign policy objectives, particularly during the Cold War, due to the devastation caused by the Second World War, when avoiding conventional and nuclear wars, and diplomacy was insufficient. The primary conceptual characteristics defining a covert operation are; the conduct of the act in such a way as to deny knowledge of or responsibility of the sponsor, which is conveyed as plausible deniability, and the effect of the operation in a political, paramilitary, or economic manner. Big data and artificial intelligence applications, which are the result of the exponentially accelerating digitalization process, have put in a very advantageous position those who holding the technological power in terms of ability to wield effect. In addition to the ontological structure of cyberspace, which supports anonymity and secrecy, social media, a product of the dualist structure formed by the transformation of the web 2.0 era and internet communication, has become a modern covert operation ground that supports plausible deniability. Such situations brought in the need of analyzing covert operations in social media utilizing artificial intelligence tools.

This study examines, in light of these facts, whether artificial intelligence can become the primary element of covert operations in social media in the near future. The Cambridge Analytica experience has been selected as the case study for this investigation. In light of the revealed findings, strategic intelligence analysis was conducted by making predictions. The analyze have been carried out obtained subjective informations which based on Analysis of Competing Hypotheses (ACH), developed by Richards Heuer from the perspective of Karl Popper's falsifiability principle; it was conducted by quantifying with the Analytical Hierarchy Process (AHP), one of the multi-criteria decision-making techniques that utilizing for optimal selection calculations. As a result of the analysis, it has been concluded that, in the near future, artificial intelligence may be the primary component of covert operations in social media. Within the context of the findings, recommendations were presented, accordingly.

Keywords: Artificial Intelligence, Social Media, Cambridge Analytica, Covert Operations, Strategic Intelligence Analysis.

Science Code	**:** 92432, 114111, 117105
Pages	**:** xiv + 139
Supervisor	**:** Doç. Dr. Güngör ŞAHİN, Ph.D

1. GİRİŞ

Örtülü operasyonlar, istihbarat teşekküllerinin kurumsal bir kimliğe büründüğü son yüzyılda sıklıkla başvurulan araçlar olmuşlardır. Doğasındaki gizlilik olgusu gereği, literatürde örtülü operasyonun kavramsal çerçevesi çok çeşitli ve tartışmalıdır. Rory Cormac ve Richard J. Aldrich, *"Grey is the New Black: Covert Action and Implausible Deniability"* adlı makalelerinde, bu çeşitlenmenin kavramsal netliğin yetersiz olduğunu vurguladığını ve bu netlik eksikliğinin, örtülü operasyonun paradoksal dünyasına dönüştüğünü savunmuşlardır.[1] Literatürde örtülü operasyonun tanım yönünden ittifak edilen yönleri, sponsor kimliğinin gizliliği ve eylemin görünürlüğüdür. Allan E. Goodman, örtülü operasyonları, *"istihbaratın, karşı tarafın hedef ve kapasitelerini öğrenmenin ötesine geçip bu kapasiteleri yönlendirmesi ve meydana gelen gelişmelerdeki rolünü ustaca saklayabilmesi"* olarak tanımlamıştır.[2] Goodman'ın tanımlamasındaki ustaca saklama kavramı, literatürde *"makul inkâr edilebilirlik"* olarak yer almaktadır. Makul inkâr edilebilirlik, örtülü operasyonların, sponsor kimliğinin gizli kalması yahut eylem ortaya çıktığında dahi hukuki yahut itibarı zedeleyici bir sonuç doğurmaması adına inkâr edilebilir olma yönünü ifade etmektedir. John Radsan, ABD'de 1947 Ulusal Güvenlik Yasası ile CIA'nin kuruluşundan itibaren Soğuk Savaş dönemini de kapsayan süre zarfını *"makul inkâr edilebilirlik çağı"* olarak nitelendirmiş ve makul inkâr edilebilirliği bir doktrin olarak ele almıştır.[3] Buna karşın Cormac ve Aldrich, örtülü operasyonların tanımlanmasında sıklıkla kullanılan makul inkâr edilebilirlik kavramının tanımlanmasını muğlak bulmuşlar ve örtülü operasyonların hem dâhili hem hârici gözlemcileri olduğundan,

---

[1] Rory Cormac, Richard J. Aldrich, "Grey is the New Black: Covert Action and Implausible Deniability", *International Affairs* C. 94, S. 3 (2018): 477. https://doi.org/10.1093/ia/iiy067.

[2] Allan E. Goodman, "Reforming U. S. Intelligence", *Foreign Policy*, C. 67 (1987): 130. doi:10.2307/1148934.

[3] John A. Radsan, "An Overt Turn on Covert Action", *St Louis University School of Law Journal*, C. 53, S. 2 (2009): 520.

doğal bir ifşaat mekanizması olduğunu ve bu yüzden gizlilik ve inkâr edilebilirliğe yapılan keskin atfın genel geçer olmadığını ileri sürerek eleştirmişlerdir.[4]

William J. Daugherty, örtülü operasyon bileşenlerini, propaganda, siyasi operasyon ve paramiliter operasyonları içeren geleneksel yöntemler ve ek olarak teknolojinin gelişmesinin katkısı ile bilgisayardaki verilere, yok etmek veya değiştirmek için gizlice erişme ve hatta donanımın kendisini imha etme yeteneği olarak tanımladığı enformasyon savaşı olarak belirtmiştir.[5] Soğuk Savaş yılları, özellikle siyasi operasyonlar ve propagandanın, dış politikanın başat araçlarından biri hâline geldiği bir dönemdir. Bu dönemde propaganda aracı olarak, radyo istasyonları ve gazeteler gibi iletişim araçları sıklıkla kullanılmıştır. ABD'nin, antikomünist yayınlar yapmak amacıyla kurduğu Özgür Avrupa Radyosu ve Özgürlük Radyosu, kitle iletişim araçları ile propagandanın örnekleridir.

Tüm bunların yanında, örtülü operasyonlar sivil söylemlerin yanı sıra resmî kanallarda da tanımlanmıştır. Örtülü operasyonun ABD'deki ilk resmi tanımı, Başkan Ronald Reagan döneminde çıkarılan *12333 No'lu Yürütme Emri*'nde *(Executive Order 12333), "özel faaliyetler"* adı altında şu şekilde belirtilmiştir:

> *"Özel faaliyetler, Birleşik Devletler Hükümeti'nin rolünün aleni olmadığı veya kamuoyu tarafından kabul edilmediği ve bu tür faaliyetleri destekleme işlevi gören, ancak Birleşik Devletler'i etkilemesi amaçlanmayan, yurt dışında ulusal dış politika hedeflerini desteklemek üzere yürütülen faaliyetler anlamına gelir. Siyasi süreçleri, kamuoyunu, politikaları veya medyayı belirtir ve diplomatik faaliyetleri veya istihbarat toplama ve üretimini veya ilgili destek işlevlerini içermez."*[6]

Daugherty, söz konusu tüzükte geçen 'özel faaliyetler' kavramınındaki muğlaklığa, özel faaliyetleri örtülü eylemin bir alt kümesi ve özel operasyonları da özel faaliyetlerin bir alt kümesi olarak tanımlayarak açıklık getirmeye çalışmıştır.[7]

---

[4] Cormac, Aldrich, a.g.e., 479.

[5] William J. Daugherty, "The Discipline of Covert Action", *Executive Secrets: Covert Action and The Precidency* (Kentucky: The University Press of Kentucky, 2004), 71-72.

[6] Executive Order (12333), United States Intelligence Activities, (4 Aralık 1981), 3 CFR 200 (1981, 46 FR 59955 [Değişiklik: Executive Order 12701, 14 Şubat 1990, 55 FR 5933]), https://www.archives.gov/federal-register/codification/executive-order/12333.html, [Erişim Tarihi: 15.11.2022].

[7] William J. Daugherty, "The Role of Covert Action in Intelligence and Foreign Policy", *Executive Secrets: Covert Action and The Precidency* (Kentucky: The University Press of Kentucky, 2004), 15.

Tanımdan anlaşılacağı üzere örtülü operasyon, konvansiyonel ve nükleer savaşlardan kaçınılan Soğuk Savaş yıllarında sıkça başvurulan ve bir dış politika enstrümanı hâlini alan bir istihbarat faaliyeti olmuştur. Sugnwon Lee, ABD'li karar vericilerin Soğuk Savaş yıllarında örtülü operasyonları bir dış politika aracı olarak kullanma motivasyonlarını araştırdığı *"Covert Action as a Foreign Policy Tool of The U.S.: Explaining the Role of Secrecy"* başlıklı yüksek lisans tezinde, karar vericilerin uluslararası ortamda olumsuz imajdan kaçınma motivasyonlarını *"dış kısıtlama hipotezi"*, ülke kamuoyu nezdinde itibarsızlaşmadan kaçınma motivasyonunu *"iç kısıtlama hipotezi"* olarak adlandırarak örtülü operasyonlardaki gizlilik motiflerini tanımlamıştır.[8] Yarattığı şiddet bakımından kısıtlama motivasyonları göz önünde bulundurulduğunda, örtülü operasyonların en sessiz seçeneklerinden biri dış kaynaklı seçim müdahalesi olmuştur. Dov H. Levin, dış kaynaklı seçim müdahalelerini *"uluslararası ilişkiler literatüründeki bir kör nokta"* olarak tanımlamış ve dış destekli rejim değişiklikleri içerisinde bilhassa yarattığı şiddet bakımından daha açık sonuçlar ortaya koyan askerî darbelerin yaygın olarak inceleme konusu olduğunu ancak dış kaynaklı seçim müdahaleleri konusunda literatürün eksik kaldığını ifade etmiştir.[9] Örtülü operasyonların Soğuk Savaş dönemindeki araç ve yöntemleri bugün ile karşılaştırıldığında, teknolojinin gelişmesi ve özellikle siber altyapıların kurulması ve gelişmesi, makul inkâr edilebilirlik ve sponsor kimliğinin gizliliği, daha geniş kitlelere daha düşük maliyetlerle ulaşılabilmesi gibi avantajlar bakımından bugün farklı bir zemin kazanmıştır. Özellikle web 2.0 dönemi ile internet iletişimin düalist bir yapıya bürünmesi ve sosyal medya platformlarının ortaya çıkması, internette yalnızca bilgiye erişilmesi döneminden, karşılıklı etkileşim kurulması ile her kullanıcı bireyin adeta birer yayın istasyonuna dönüşmesi dönemine bir geçiş sağlamıştır.

Özellikle 2010 sonrası dönemde, kitle hareketlerinin sosyal medya üzerinden organize olmaları durumu daha görünür hâle gelmiştir. Karim Sorour ve Bidit Lal Dey, Mısır ve Bangladeş'te *"sosyal medyanın yönlendirdiği"* siyasi hareketleri, gelişmekte olan ülkelerde sosyal medyanın siyasi hareketlere zemin oluşturması bakımından ele

---

[8] Sugnwon Lee, "Covert Action as a Foreign Policy Tool of The U.S.: Explaining the Role of Secrecy", (Yüksek Lisans Tezi, Graduate Faculty of The University of Georgia, 2010): Abstract.

[9] Dov H. Levin, "Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset". *Conflict Management and Peace Science,* (2016): 1. 0738894216661190–. doi:10.1177/0738894216661190.

almışlardır. Fakat bahse konu ülkelerde, makalenin yayınlandığı 2014 yılı itibariyle internete erişim oranının düşük olması, dolayısıyla dar gelirli kesimin ve işçi sınıfının sosyal medya üzerinden seslerini yükseltmelerinin olanaklar bakımından zor olduğu sonucuna varmışlardır.[10]

Kitlesel hareketlerin ve oy davranışlarının sosyal medya üzerinden manipüle edilebildiği sorunsalı literatürde birçok çalışmanın konusu olmuştur. Büyük veri analitiklerinin psikografik segmentasyon ve hedefleme aracı olarak kullanılmasıyla, kişileri ve kitleleri duygusal ve davranışsal olarak tetiklediği ve harekete geçirdiği konusu özellikle Cambridge Analytica vakasının ifşa edilmesiyle gündeme gelmiştir. Fakat burada bir sorun vardır; kişilerin ve kitlelerin çevirim içi ortamda gördükleri bir reklam, metin, ses, video yahut görsel ile harekete geçtikleri fikrinin bilimsel dayanağı nedir? Dahası, örnek vakanın ele alınarak gelecekte de sosyal medya üzerinden örtülü operasyonların yapılabileceğinin gözlem ve çıkarımlar dışında analizi hangi bilimsel verilere göre yapılmıştır? Ayrıca sosyal medyayı mikro hedefleme algoritmaları ile örtülü operasyonlara uygun bir zemin hâline getiren yapay zekânın, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün müdür? Bu çalışma, bu sorulara cevap aramaktadır. Sosyal medyanın, mikro hedefleme algoritmaları ile bir propaganda aracı olarak kullanılmaya ve kişileri/ toplumları manipüle etmeye müsait bir zemin oluşturabileceği fikri ve bunun etki düzeyi, psikoloji biliminin sunduğu bilimsel unsurların da dâhil edildiği bir perspektif ile incelenmeye muhtaçtır.

Bu çalışmada; algoritma, yapay zekâ, büyük veri, siber uzay ve siber istihbarat, sosyal medya ve psikografi kavramları çerçevesinde örtülü operasyonun yarattığı şiddet ve makul inkâr edilebilirlik unsurları kapsamında örtülü operasyon türlerinin nasıl konumlandığı, Cambridge Analytica'nın örtülü operasyonların siber uzaya taşınmasına nasıl bir örnek teşkil ettiği ve sosyal medyayı örtülü operasyonlara elverişli hale getiren birincil unsurun ne olduğu sorularına Rakip Hipotezlerin Analizi (ACH) ve Analitik Hiyerarşi Süreci (AHP) teknikleriyle gerçekleştirilecek olan stratejik istihbarat analiziyle cevap aranacaktır.

---

[10] Karim Sorour, Bidit Lal Dey, "Energising the political movements in developing countries: The role of social media", *Capital & Class,* (2014): 1- 8.

Ekseriyetle betimsel bir metod ile ele alınan sosyal medyada algı yönetimi ve kitle hareketleri konuları, Türkçe literatürde henüz yapılandırılmış teknik analitikler ile analiz edilmemiştir. Sosyal bilimlerin deneysel olmayan özellikleri gereği analiz sürecinde var olan bir dizi yönteme müracaat edilmesi; hem daha güvenilir ve tutarlı sonuçlara ulaşma noktasında hem de analiz sürecinde zihinde bir kör nokta olarak ifade edilebilecek, sezgi ve önyargılardan ötürü görmezden gelinen ayrıntıların dikkate alınması avantajını doğurur. Richards Heuer tarafından önerilmiş olan Rakip Hipotezlerin Analizi (Competing Hypoteses Analysis/ ACH) metodu, 20. yüzyılın bilim filozoflarından Karl Popper'ın bilim felsefesinin, istihbarat analizine uygulanması yöntemidir.[11] ACH yönteminde Heuer, analiz edilecek probleme ve elde edilen veri ve kanıtlara dayanarak birbirini tamamen dışlayan en az iki hipotez oluşturulmasını ve bu hipotezlerin kanıtlar ile yanlışlanmasını, sonuç olarak *"yanlışlanabilirlik"* ilkesinden hareketle, en az yanlışlanabilir olan hipotezi en olası hipotez olarak belirlemeyi önermiştir.[12] Fakat bu yöntemde de analist, mecvut hipotezleri hangi bilişsel yorumlamalar ile ele aldığının tam bir resmini çizemeyebilir. Ayrıca analiz sürecinde ortaya konulan kanıtlar yine öznel yargılar vasıtası ile puanlandığından dolayı, bilişsel yargılar ile yapılacak puanlamanın bir tutarlılık kontrolünün yapılması analizin güvenilirliği bakımından önemlidir. Bu sebeple ACH analizinden elde edilen sonucun tutarlılık testine tabi tutulması ve nicelleştirilmesi ihtiyacı doğmuştur. Analitik Hiyerarşi Süreci (Analytic Hyerarchy Prosess/ AHP), 1968 yılında. James H Myers ve Mark I. Alpert tarafından ortaya konulan ve 1977 yılında Thomas L. Saaty tarafından geliştirilen bir çok kriterli karar verme modelidir.[13] Model, çok kriterli karar verme probleminde nicel ve nitel verilerin ölçümü için sıklıkla kullanılan bir tekniktir.[14] Saaty AHP tekniğini kriterler arasındaki subjektif mesafeyi ölçme maksadıyla geliştirmiştir.[15] Bu sebeple bu çalışmada tartışılan konu,

---

[11] Richards Heuer, Randolph H. Pherson, "Hypothesis Generation and Testing", *Structured Analytic Techniques for Intelligence Analysis*, 2. bs (California: CQ Press, 2015): 247.

[12] *a.g.e.*, 264.

[13] İrem Figen Gülenç, Gülşah Aydın Bilgin, "Yatırım Kararları İçin Bir Model Önerisi: AHP Yöntemi", *Öneri Dergisi,* C.9, S.34 (2010): 98.

[14] Omkarprasad S. Vaidya, Sushil Kumar, "Analytic Hierarchy Process: An Overview of Applications", *European Journal of Operational Research* C. 169, S. 1 (2006): 2 doi:10.1016/j.ejor.2004.04.028 .

[15] Seher Arslankaya, Kübra Göraltay, "Analitik Hiyerarşi Prosesi Yöntemi", *Çok Kriterli Karar Verme Yöntemlerinde Güncel Yaklaşımlar* (Ankara: İksad Yayınevi, 2019), 16.

Rakip Hipotezlerin Analizi (ACH) ile analiz edilecek ve ardından ACH sürecinde ortaya konulan subjektif yargılar Analitik Hiyerarşi Süreci (Analytic Hyerarchy Prosess/ AHP) ile nicelleştirilecektir. Teknik, kriter ve seçeneklerin önem derecelerinin hesaplanması ve yargıları tutarlılık testine tabi tutması bakımından önemlidir. Böylece ACH metodundan elde edilen analiz bulguları AHP metodu ile sınanacak ve subjektif yargıları nicelleştirerek en optimal sonucu ortaya koyacaktır.

Literatürde sosyal medya üzerinden örtülü operasyonların, stratejik istihbarat analizi ile analiz edilmesi konusunda bir eksiklik fark edilmiştir. YÖK Ulusal Tez Merkezi'nde, sosyal medyayı örtülü operasyon sistematiği ile inceleyen ve bu konunun stratejik istihbarat analizini yapan bir çalışmaya rastlanmamıştır. YÖK Ulusal Tez Merkezi'nde, Sosyal Medya ve İstihbarat konulu 13 adet tez mevcuttur. Bu tezlerin kahir ekseriyeti, güvenlik ve terörle mücadele amaçlı önleyici istihbarat perspektifinde incelenmiştir. Mevcut tezler arasında Rekabet İstihbaratı ve Gazetecilikte enformasyon akışı bakımından sosyal medya ve istihbarat olguları araştırılmıştır. Büyük veri analitiklerinin ve Açık Kaynak İstihbaratının sosyal medya üzerinde kullanımı ve istihbarat çarkı içerisinde konumlandırılması da yayınlanmış tezlerin odaklandığı konular arasındadır. Ayrıca YÖK Ulusal Tez Merkezi'nde Cambridge Analytica konulu 6 adet tez mevcuttur. Bu çalışmaların içerisinde, vaka perspektifinde Facebook'un marka itibarı, yeni ve farklı bir iktidar türü olarak data politik ve sahte haberlerin marka imajlarına olan etkisi incelenmiş ve geri kalan çalışmalar kişisel verilerin korunmasına ve bunun hukuki altyapılarına odaklanmıştır. YÖK Ulusal Tez Merkezi'nde, Cambridge Analytica ve istihbarat analizi konulu bir çalışmaya rastlanılmamıştır. Bahse konu veri tabanında, Analitik Hiyerarşi Süreci ve İstihbarat konulu 3 adet tez mevcuttur. Bu tezlerden biri dış ticaret ve hedef pazar yönelim analizi, biri bankaların ticari kredi değerlendirme kriterleri bir diğeri ise "Büyük veya Doğal Arnavutluk İdealinin Stratejik İstihbarat Analizi" başlıklı tezdir. Söz konusu çalışma, jeopolitik perspektifinde incelenmiştir. Rakip Hipotezler Analizi yöntemi, söz konusu veri tabanında yine "Büyük veya Doğal Arnavutluk İdealinin Stratejik İstihbarat Analizi" başlıklı tezin analiz yöntemlerindendir.

Yukarıda verilmiş olan bilgilerden anlaşılacağı üzere Türk akademisinde bu tez, sosyal medya ve örtülü operasyonu, Rakip Hipotezler Analizi ve Analitik Hiyerarşi Süreci ile stratejik istihbarat analizine tabi tutması bakımından ve Cambridge Analytica

vakasının çok yönlü olarak incelendiği ve stratejik istihbarat analizine konu edildiği bir çalışma olması bakımından öncüdür.

Bu çalışmada, mevcut durumun analizinden hareketle geleceğe yönelik bir öngörü sunmak maksadıyla stratejik istihbarat analizi, Cambridge Analytica vakası örnek olay olarak incelenerek yapılmıştır. Çalışmada analiz edilecek olan problem, Cambridge Analytica vakası kapsamında yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsur olup olamayacağının belirlenmesidir. Söz konusu analiz sorusu, yapay zekâ, büyük veri analitikleri ve psikografi enstrümanlarının sağladığı avantajların hem güncel teknolojik gelişmeler hem de Cambridge Analytica'nın faaliyet yöntemleri bakımından kanıtların ortaya konulması ile incelenecektir.

Çalışmanın ilk bölümünde, algoritma ve yapay zekâ kavramları incelendikten sonra büyük veri kavramı ve büyük veri analitiği yönntemleri tanımlanmıştır. Ardından siber uzayın yapısı ve siber istihbarat konusu ele alınmıştır. Devamında ise hedef kitle hareketleri ve mikro hedefleme, psikografik bilgi ile demografik bilgi arasındaki farklar ve psikografiye müracaat edilen alanlar yönünden psikografi kavramı açıklanmıştır. Son olarak, sosyal medyada büyük verinin kullanımı, siber saldırıların kullanımı ve sosyal medyanın kitle hareketlerine zemin oluşturması yönünden sosyal medya analitiği incelenmiştir. İkinci bölümde, örtülü operasyonlar tanımlanmış, örtülü operasyonları bir dış politika seçeneği hâline getiren ve makul inkâr edilebilirlik olgusuna motivasyon sağlayan caydırıcı unsurlar ele alınmış akabinde türleri bakımından örtülü operasyonlar ve propaganda kavramı incelenmiştir. Ardından bir siyasi örtülü operasyon türü olan rejim değişikliği şemsiye terimi altında dış kaynaklı seçim müdahaleleri ve askerî darbeler, örnek vakalar ile incelenmiştir. Üçüncü bölümde, Cambridge Analytica vakası, şirketin yapısı, dâhil olduğunun iddia edildiği demokratik seçimler ve çalışmalarında kullandıkları propaganda ve manipülasyon teknikleri büyük veri, sosyal medya ve psikografi özelinde incelenmiştir. Akabinde 2016 ABD Başkanlık Seçimlerine Rusya müdahalesi konusunda yargılama süreci incelenmiştir. Dördüncü bölümde ise, Cambridge Analytica vakasının incelemeye dâhil olan konuları perspektifinde, sosyal medyanın örtülü operasyonlara elverişli bir zemin hâline gelmesinde avantaj sağlayan enstrümanlar, Rakip Hipotezler Analizi (ACH) ve Analitik Hiyerarşi Süreci (AHP) ile analiz edilmiştir.

Elde edilen bulgular sonucunda, devletlerin, halklarını propaganda ve manipülasyon ile sosyal medya üzerinden etki altına almayı hedefleyen odaklara karşı korumalarına

yönelik bir dizi öneri sunulmuştur. Doğası gereği istihbarat çalışmalarına dair tüm bilgi ve vakalara açık kaynaklardan ulaşmanın zorluğu dolayısıyla, çalışmada açık kaynaklardan ulaşılan bilgilerin bu çalışma için yeterli olduğu varsayılmıştır.

Çalışmada; kavramları ve ilişkilerini açıklayan tanımlayıcı araştırma yöntemi, araştırmaya konu olan Cambridge Analytica vakasının incelenmesiyle suretiyle bir olayı derinlemesine inceleyen örnek olay incelemesi, geçmişte meydana gelen vakaları ve bunların günümüzdeki etkilerini inceleyen tarihsel araştırma yöntemi ve araştırılan konu ile ilgili kitaplar, gazeteler, makaleler, biyografi ve otobiyografileri ve video kayıtlarını inceleyen içerik analizi araştırma yöntemlerinden yararlanılmıştır. Ayrıca, probleme dair kavramların ve vakaların holistik perspektif ile ele alındığı nitel araştırma ile vakaların sayısal yöntemlerle sınandığı nicel analizin bir arada kullanıldığı karma analiz yöntemi benimsenmiştir. Araştırmada Türkçe ve İngilizce kaynaklardan yararlanılmış ve gazete, kitap, dergi, yayınlanmış videolar, tezler, kongre bildirileri, raporlar gibi açık kaynakların yanı sıra eğitim alınan kurumun ders notlarından da yararlanılmıştır. Araştırma konusu ile ilgili farklı analiz teknikleri ve yaklaşımlar, alana ilgi duyan diğer araştırmacılara bırakılmıştır.

2. KAVRAMSAL ÇERÇEVE

Çalışmanın bu bölümünde, algoritma ve yapay zekâ, büyük veri analizi ve analitikleri, siber uzayın yapısı ve siber istihbarat, psikografi ve sosyal medya analitiği kavramları irdelenecektir. Bu bölüm, çalışmanın genel yaklaşımı konusunda sinaptik bağlantıları ifade etmesi ve izleyen bölümlerde ortaya konulan bilgiler ile basamaklandırılıp analiz konusuna dair yaklaşımları temellendirmesi bakımından önemlidir.

2.1. Algoritma ve Yapay Zekâ

Algoritma kavramı basitçe, bir girdi ile çıktı arasındaki işlemler silsilesini ifade eder. Oxford Dictionary'de algoritma, *"bir sorunu çözmek için talimatların bir listesi"* olarak tanımlanmıştır.[16] The Britannica Dictionary'de de benzer bir ifade ile *"bir matematik problemini çözmek veya bir bilgisayar işlemini tamamlamak için izlenen bir dizi adım"* olarak tanımlanmıştır.[17] Algoritma kavramının, sıfır rakamını tanıtması ile bugün bilgisayarda bir ve sıfır rakamlarından oluşan binary sistemi bir yönden borçlu olduğumuz El- Hârizmi'nin isminden türetildiği sanılmaktadır (Algorismi, Algorismo, Algorismus).[18] Söz konusu kavram, ilk etapta günümüzün modern yazılım mimarilerini akla getiriyor olsa da, algoritma tarihi oldukça eskidir ve bilgisayarın icadının çok öncesinde önemli buluşların dayanaklarındandır. Örnek olarak, Gerasalı Nicomachus (M.S. 60-120), bir tamsayıya kadar olan asal sayıların bulunmasını sağlayan Eratosten kalburunu tanıtmıştır ve bu yöntem günümüzde de kod yazımında kullanılmaktadır.[19] Bilinen en eski sayısal hesaplama örneğine, Fırat nehri üzerindeki Şuruppak'ta bulunan M.Ö. 2500 yıllarına ait bir Sümer kil tabletinde rastlanmıştır.[20]

---

[16] Oxford Dictionary, *"Algorithm",* https://dictionary.cambridge.org/dictionary/english/algorithm. [Erişim Tarihi: 17.02.2023].

[17] The Britannica Dictionary, "Algorithm Definition & Meaning", https://www.britannica.com/dictionary/algorithm, [Erişim Tarihi: 17.02.2023].

[18] Giorgio Ausiello, "Algorithms, An Historical Perspective", *The Power of Algorithms*, ed. Rossella Petreschi (Berlin: Springer, 2013), 12. doi:10.1007/978-3-642-39652-6_1.

[19] Marek Kowalkiewicz, "How did we get here? The story of algorithms", *Towards Data Science*, https://towardsdatascience.com/how-did-we-get-here-the-story-of-algorithms-9ee186ba2a07#_ftn2. [Erişim Tarihi: 17.02.2023].

[20] Ausiello, *a.g.e.*, 4.

Günümüz programlanabilir bilgisayarlarının icadı ise, İkinci Dünya Savaşı yıllarına dayanmaktadır. Kriptolojinin öneminin arttığı İkinci Dünya Savaşı sırasında, İngiliz Mühendis Tommy Flowers tarafından Colossus adında, Nazi Almanyası'nın kriptoloji aygıtı olarak kullandığı Enigma kodlarını kıracak bir makine icat edilmiştir. Colossus, saniyede 5.000 karakter tarayarak haftalar süren işlem süresini saatlere indirgemiştir ve dünyanın ilk programlanabilen dijital elektronik bilgisayarı olarak kabul edilmektedir.[2122] ABD Ordusu'nun, top mermilerin muhtemel yörüngelerini daha isabetli hesaplaması amacıyla imal edilen ve ilk deneme çalışmalarına 1945 yılında başlanan decimal (onluk) tabanlı ENIAC'ın (Electronic Numerical Integrator And Computer /Elektronik Sayısal Entegreli Hesaplayıcı) tasarım ve inşası esnasında, 20 adet 10 ondalık basamak sayısından daha fazla depolama ihtiyacı fark edilmiştir ve binary (ikilik) tabanlı EDVAC tasarlanmıştır. EDVAC (Electronic Discrete Variable Automatic Computer/ Elektronik Ayrık Değişkenli Otomatik Bilgisayar), ilk depolanabilir program bilgisayarı olarak kabul edilmektedir.[23]

Eski Babil, Mısır, Antik Yunanistan dönemlerinden bugüne çok sayıda sayısal hesaplama formülasyonunu ifade eden algoritmalar, bilgisayarın icadından itibaren yapay zekâ ve veri analitiği gibi alanların var olmasını ve bir gelişim devinimi içinde olmasını sağlamış, biyometrik tanıma, otonom modelleme, tıbbi görüntüleme gibi çok sayıda örneği bulunan gelişmeleri insanlığa kazandırmıştır.[24]

Yapay zekâ/ YZ (Artificial Intelligence/ AI), insanlar ve hayvanların sahip olduğu doğal zekânın bilgisayar tabanlı algoritmalar vasıtası ile matematik, istatistik, veri bilimi gibi farklı alanlardan beslenerek taklit edilebilmesini ifade etmektedir. Kavramsal olarak ilk kez 1955 yılında Dartmouth Konferansı'nda John McCarthy

[21] Keith D. Foote, "A Brief History of Big Data", https://www.dataversity.net/brief-history-big-data/. [Erişim Tarihi: 14.07.2022].

[22] Burak ÖZ, "Bilgisayarın Tarihçesi", slayt 11, https://cdn3.beun.edu.tr/insaat/f6342b2189e35b8d6f273e9455060f69/bilgisayar-kullanimi.pdf, [Erişim Tarihi: 26.09.2022].

[23] EDVAC, Encyclopedia of Computer Science, ACM Digital Library, https://dl.acm.org/doi/abs/10.5555/1074100.1074362, [Erişim Tarihi: 26.09.2022].

[24] İTÜ Yapay Zekâ ve Veri Mühendisliği, "Bilgisayarla Görü", https://yapayzeka.itu.edu.tr/arastirma/bilgisayarla-goru. [Erişim Tarihi: 18.02.2023].

tarafından ifade edildiği bilinmektedir.[25] Eric Horvitz'in tanımlamasına göre yapay zekâ *"düşünce ve akıllı davranışın altında yatan mekanizmaların bilimsel olarak anlaşılmasını ve bu ilkelerin insanlara ve topluma değer sağlayabilen makinelerde somutlaştırılmasını amaçlayan bir dizi bilgisayar bilimi disiplini"*dir."[26] Temelde yapay sinir ağları (YSA) teknolojilerinin alanı olan *"insan zekâsının taklidi"*, insan beyin yapısındaki nöronlar arası sinapsların makinelere modellenmesi çalışmalarıyla geliştirilmiştir.[27] Stuart J. Russell ve Peter Norvig, yapay zekâ ile ilgili tanımlamaları 4 farklı kategoride organize etmişlerdir.

Tablo 2.1: Kategorize Edilmiş Yapay Zekâ Tanımları.

İnsan gibi düşünen sistemler (Systems that think like humans)	Rasyonel düşünen sistemler (Systems that think rationally)
İnsan gibi davranan sistemler (Sytems that act like humans)	Rasyonel hareket eden sistemler (Systems that act rationally)

Yazar tarafından Türkçeleştirilmiştir. [28]

Russell ve Norvig'in çerçeveledikleri tanımlamadan anlaşılacağı üzere YZ, insan gibi düşünmek ve davranmak, rasyonel düşünmek ve davranmak etrafında tanımlanmıştır. YZ teknolojileri, var olduğu günden bugüne önemli bir ilerleme katetmiştir. Yapay sinir ağları, derin öğrenme, doğal dil işleme gibi diğer YZ alanlarının örüntülü olarak geliştirilmesiyle günümüzde bireysel olarak insan hayatını kolaylaştıran sistemler dışında devletler bazında suç önlemeye yönelik sistemler de geliştirilmiştir. Örnek olarak, Apple Inc.'nin Siri uygulaması ve Google Assistant gibi chatbot'lar, bireysel

[25] Gül Ekinci, Fatma Gül Bilginer- Özsaatçi, "Yapay Zekâ ve Pazarlama Alanındaki Yayınların Bibliyometrik Analizi", *Sosyoekonomi*, C. 31, S. 56 (2023): 371.

[26] Eric Horvitz, "Reflections on the Status and Future of Artificial Intelligence", *Before The Committee on Commerce Subcommittee on Space, Science, And Competitiveness United States Senate: Hearing on the Dawn of Artificial Intelligence* (2016): 2, http://erichorvitz.com/Senate_Testimony_Eric_Horvitz.pdf. [Erişim Tarihi: 12.10.2022].

[27] Fatma Tüminçin, Alper Aytekin, Ahmet Ayaz, "İnsan Beyni Modellemesi ve Yapay Sinir Ağları", *SADAB 5th International Social Research and Behavioral Sciences Symposium*, (Tiflis: 11- 12 Ekim 2019): 164.

[28] Stuart J. Russell, Peter Norvig, "What Is AI?", *Artificial Intelligence: A Modern Approach* (1995: Prentice-Hall, New Jersey), 5.

olarak ulaşılabilen ve hizmet alınan uygulamalara birer örnektir. Öte yandan Çin Halk Cumhuriyeti'nde Sosyal Kredi Sistemi ile vatandaşların kanunlara ve kurallara uyumları dâhil sosyal hayatlarındaki pek çok hareketlerinin bir puanlama sistemine tabi tutulması ve puanlarına göre uçak ve trenlere binmekten men edilmek dâhil birçok yaptırıma çarptırılmalarını öngören sistem[29] ile ülkenin çoğu alanında yer alan yüz tanıma ve ses tanımayı içeren kameralar ile kurduğu gözetim sistemi de veri bilimi ve YZ tabanlı algoritmaların devlet düzeyinde kullanımına örnektir.

YZ konseptlerinin devlet düzeyinde kullanımı yalnızca iç güvenlik uygulamaları ile sınırlı değildir. Devletlerin dış politikalarını gerçekleştirmeye yönelik uygulamalarında da pek çok alanda yapay zekâya başvurulmaktadır. Savunma sanayi, askerî teknolojiler gibi sistemlerin yanı sıra, devletlerin açıkça üstlenemeyecekleri operasyonlarında da YZ kullanılabilmektedir. Bunun en güncel örneklerinden biri, İsrail menşeli Team Jorge adlı şirketin otomatik dezenformasyon ile seçim müdahalelerinde bulunmuş olması vakasıdır. Team Jorge adlı şirketin, sosyal medyada Advanced Impact Media Solutions (AIMS) yazılımı ile oluşturulan otuz binden fazla bot hesap ile dezenformasyon yayıldığı ve otuz üç cumhurbaşkanlığı seçimini manipüle ettiği ortaya çıkmıştır. [30] Vakanın çarpıcı yönü ise dezenformasyon yayan bu bot hesapların vatandaşlar tarafından çoğu zaman gerçek kişilerden ayırt edilemeyecek kadar profesyonel olarak oluşturulmasıdır.

Örneklerden anlaşılacağı üzere, günümüzde programlama dilleri ile yazılan modern algoritmaların insanlığa sunduğu hizmet tartışmasızdır fakat bunun yanında insan tercihlerini keşfetmeden yönlendirmeye kadar birçok uygulamayı da var etmiştir. Veri analitiği ve psikografinin yapay zekâ tabanlı algoritmalar vasıtası ile geliştirilmesi, web siteleri ve sosyal medya uygulamalarında kullanıcı bilgilerinin çekilerek belirli disiplinlere göre formüle edilmesi, gerek bireysel gerekse toplumsal anlamda veri mahremiyetinin önemini arttıran sonuçlar doğurmasının yanı sıra devletlerin dış

[29] Amanda Lee, "What is China's social credit system and why is it controversial?", *South China Morning Post*, 09.08.2020, https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial. [Erişim tarihi: 21.02.2023].

[30] Stephanie Kirchgaessner ve diğ., "Revealed: The Hacking and Disinformation Team Meddling in Elections", *The Guardian*, 15.02.2023, https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan. [Erişim Tarihi: 21.02.2023].

politika hedeflerini gerçekleştirmek maksadıyla başvurdukları fakat doğrudan üstlenemeyecekleri eylem konseptlerinde de yeni fırsatlar meydana getirmiştir.

2.2. Büyük Veri: Analiz ve Analitik

Yalnızca istihbarat analizi için değil, bir bulgunun elde edilmesi sürecini ifade eden her türlü analiz için, veri ve enformasyon ne kadar fazlaysa, sürece o kadar fazla katkı sağlar. Fakat bir noktada eldeki verilerin hacmi, hızı ve çeşitliliği öyle bir boyuta ulaşır ki, bu verileri ayıklamak, düzenlemek hatta depolamak imkânsız hâle gelmeye başlar ve analiz sürecini akamete uğratır. Bu sorun; "Büyük Veri (Big Data)" olarak adlandırılmıştır.

Büyük veri (Big Data), klasik veri tabanlarının kaldıramayacağı kadar hacme sahip veri yığınını ifade etmektedir.[31] Kavramsal olarak Büyük Veri, bilgisayar dünyasında ilk kez 2005 yılında O'Reilly Media çalışanı Roger Magoulas tarafından, klasik verilerin hacmi göz önünde bulundurularak, bu verilerin klasik tekniklerle işlenememesi dolayısıyla çok büyük miktarda veriyi tanımlamak için kullanılmıştır.[32] Günümüzde sosyal medya paylaşımları, GSM operatörlerinden elde edilen arama kayıtları, video, fotoğraf, blog ve log dosyaları gibi çeşitli kaynaklardan damıtılan verilerin anlamlı ve işlenebilir hâle dönüştürülmüş biçimi, büyük veridir.[33] Büyük verinin nihai para birimi olarak algılanması farkındalığı giderek artmaktadır ve gelişmiş modeller ve algoritmalar, görünüşte zorlu güvenlik sorunlarına veri odaklı ve daha doğru çözümler sunma olasılığını arttırmıştır.[34] 1960'lı yıllarda ortaya çıkan "bilgi devrimi" ve "dijital çağ" gibi kavramlara objektif bir zemin sağlamakla birlikte büyük veri, 2000'li yıllardan itibaren hemen hemen tüm araştırma disiplinlerinde etkisi artan bir olgu hâlini almıştır.[35] Büyük veri, bilimsel araştırma örneklemini

---

[31] Şevki Işıklı, "Büyük Veri, Epistemoloji ve Etik Tartışmalar", *AJIT-e: Online Academic Journal of Information Technology* C. 5, S. 17 (2014): 93. DOI: 10.5824/1309-1581.2014.4.006.x.

[32] http://strata.oreilly.com/2010/01/roger-magoulas-on-big-data 'dan aktaran Rajesh Math, "Big Data Analytics: Recent and Emerging Application in Services Industry" (2018): 2011. DOI:10.1007/978-981-10-6620-7_21. [Erişim Tarihi: 21.06.2022].

[33] Can Eyüpoğlu ve diğ., "Büyük Veride Kişi Mahremiyetinin Korunması", *Bilişim Teknolojileri Dergisi*, C.10, S.2 (2017): 177, https://doi.org/10.17671/gazibtd.309301.

[34] Lewis Herrington, "Cyberespionage and Cyberwar", *Secret Intelligence: A Reader*, ed. Christopher Andrew, Richard J. Aldrich, Wesley K. Wark, 2. bs, (Oxon: Routledge, 2020), 567.

[35] Işıklı, *a.g.e.*, 90.

genişletmiştir. Küçük bir gruba uygulanan ölçüm ve gözlemlerin bütün popülasyona genellenmesiyle (tümevarım) varılan bilimsel sonuçlar, büyük veri ve veri analitiği yeterince efektif kullanılmaya başladığında yerini daha fazla veri ve daha fazla ölçüm ile daha geniş bir örneklem uzayından elde edilmiş bulgulara bırakabilecektir.

Büyük veri, kavramsal olarak ilk kez Michael Cox ve David Ellsworth tarafından 1997 yılında yazılan "Application-Controlled Demand Paging for Out-of-Core Visualization" başlıklı makalede tanımlanmıştır. Cox ve Ellsworth, veri görselleştirmede veri kümelerinin, ana belleğin, yerel diskin ve hatta uzak diskin de kapasitesini zorladığını açıklamış ve "buna büyük veri sorunu diyoruz" ifadesiyle kavramı vurgulamıştır.[36] Francis X. Diebold, Ağustos 2000'de düzenlenen Dünya Ekonometrik Toplum Kongresi için hazırlanan bildirilerin bir tartışması olarak yazdığı makalede[37] büyük veriyi, "büyük ölçüde veri kaydı ve depolama teknolojisindeki son ve benzeri görülmemiş gelişmelerin sonucu olarak, mevcut ve potansiyel olarak ilgili verilerin miktarındaki (ve bazen kalitesindeki) patlama" olarak ifade etmiştir ve birçok bilim alanının yüz yüze gelmek zorunda olduğu bir 'fenomen' olarak tanımlamıştır.[38] Özünde büyük veri, insanın yanı sıra esas olarak teknolojik araçlar aracılığıyla üretilen ve paylaşılan kolektif istihbaratın eseridir.[39]

Andrew McAfee ve Erik Brynjolfsson, büyük veri ve analitik ilişkisi için şu ifadeleri kullanmışlardır: *"Büyük veri hareketi, kendisinden önceki analitik gibi, verilerden istihbarat toplamayı ve bunu iş avantajına dönüştürmeyi amaçlar. Fakat aralarında üç temel fark vardır: Hacim, hız ve çeşitlilik."*[40] Büyük veri, yaygın olarak hacim (volume), hız (velocity), çeşitlilik (variety) olmak üzere "3V" olarak adlandırılan

---

[36] Michael Cox, David Ellsworth, "Application-Controlled Demand Paging for Out-of-Core Visualization", *NASA* (California: NASA, 1997), 1.

[37] Francis X. Diebold, "'Big Data' Dynamic Factor Models for Macroeconomic Measurement and Forecasting", *Advances in Economics and Econometrics (Theory and Applications: Eighth World Congress* (2003): 121.

[38] *a.g.e.*, 115.

[39] Uthayasankar Sivarajah ve diğ., "Critical analysis of Big Data challenges and analytical methods", *Journal of Business Research* (2016): 1. http://dx.doi.org/10.1016/j.jbusres.2016.08.001.

[40] Andrew McAfee, Erik Brynjolfsson, "Big Data: The Management Revolution", *Harvard Business Review* (Ekim, 2012). https://hbr.org/2012/10/big-data-the-management-revolution. [Erişim Tarihi: 12.11.2022].

özelliklerle tanımlanmakta ve bazı kaynaklarda değer (value) ve gerçeklik (veracity) de bu özelliklere dâhil edilerek 5V olarak adlandırılmıştır.[41]

McAffee ve Brynjolfsson, bir veri setinin büyük veri olarak tanımlanabilmesi için, hacim, hız ve çeşitlilik özelliklerini barındırması gerektiğini ifade etmişlerdir. Yani, çok büyük miktarda, kısa zaman aralıkları ile ve çeşitli veri akışından bahsediliyor olmalıdır. Örnek vermek gerekirse; kamu kurumları vatandaşların birçok kişisel bilgilerini dijital ortama aktarmaktadır. Birçok devlet gibi Türkiye'de de e- devlet sistemiyle, sistem içine entegre edilen sağlık, nüfus ve vatandaşlık, tapu- kadastro, adli işlemler dâhil birçok kamu hizmeti dijital ortama aktarılmıştır ve aktarılmaya devam etmektedir. Böylece bireysel olarak dijital ortamda, her yeni güncellemeyle artan bir veri hacmi söz konusudur. Fakat buradaki bireysel verileri büyük veri olarak adlandırılamayacaktır. Çünkü ne hacim, ne çeşitlilik, ne de hız unsurlarını karşılamaz. Fakat bir toplumun tamamının sağlık verileri tüm bu unsurları karşılar; dolayısıyla büyük veridir. Kamu sektörünün, vatandaşların kişisel bilgilerini dijital ortama aktararak gelişen teknolojiye adapte olması, bürokrasideki hantallığı hafifletmesi bakımından olumludur fakat bu verilerin çoğu kişiseldir ve gerektiği gibi korunmadığı takdirde bir milli güvenlik sorunu hâlini alacaktır.

Günümüzde istihbarat dünyasıyla iş dünyasının sınırlarını en çok bulanıklaştıran kavramlardan biri olarak büyük veriden söz edilebilir. Çünkü çok sayıda firma da geleneksel reklamcılık konseptlerinin çok üstünde teknolojiler ve yöntemlerle, internet ortamı ve algoritmalar yardımıyla kişiselleştirilmiş reklamlara müracaat etmektedirler ve bu reklamların oluşum aşamasında adeta istihbari bilgi gibi, bireyler hakkında her türlü bilginin depolandığı veri tabanlarından yararlanılmaktadır. Büyük verinin bir sorun olarak tanımlanmasından bu yana, geliştirilen analitik yöntemleriyle bu sorun avantaja dönüşmeye başlamıştır.

Çok sayıda verinin elde edilebilmesi bir avantajken, klasik veri analizi yöntemlerinin artık bu akan bir şekilde artan veri yığınının analizinde eksik kalmaya başlaması ile yeni analiz yöntemleri ihtiyacı fark edilmiştir. Veri analizi ve veri analitiği sıklıkla birbirinin yerine kullanılmaktadır ve yaygın olarak aynı anlamı ifade ettiği gibi yanlış

---

[41] Ahmed Foad Mohammed, Vikas T. Humbe, Santosh S. Chowhan, "A review of Big Data Environment and its Related Technologies", *International Conference on Information Communication and Embedded System* (2016): 1- 5. DOI:10.1109/ICICES.2016.7518904.

bir kanı söz konusudur. Oysa veri analizi, veri analitiğinin bir parçasıdır.[42] Veri analizi, yararlı bilgilere ulaşma sürecinde verileri temizleme, dönüştürme, modelleme ve sorgulama süreçlerini içerir.[43] Veri analizi, veriyi sorgular ve anlaşılmalarını sağlar. Verilerin analiz sürecine kadar olan zaman dilimindeki durumunu ve çıktılarını ortaya koyar. Veri analitiği ise, analizde elde edilen bulgular ışığında belirli yöntemler kullanarak geleceğe dair bir çıkarım ve içgörü oluşturur.[44] Yani veri analizi farkındalık, veri analitiği strateji oluşturma sürecidir denilebilir. Veriler önyargısızdır, bu nedenle anlamlandırılırken sezgisel yanılgılardan arınmış bir veri analizi ve veri analitiği, yapbozun parçalarını doğru yere koymak için önemlidir.

NoSQL veritabanları, BigQuery, MapReduce, Hadoop, WibiData ve Skytree gibi gelişmiş Büyük Veri analiz teknolojileri ile sağlık, finansal üretkenlik gibi kritik sektörlerde, enerji gelecekleri ve doğal felaketi tahmin etmek gibi iş stratejilerini ve karar verme sürecini iyileştirmeye yönelik içgörüler daha iyi elde edilebilir.[45] Bu, verilerden anlam elde etmek için bir dizi analitik yöntem kullanıldığında mümkündür:[46]

- Tanımlayıcı Analitik (Descriptive Analytics): Bir işin mevcut durumunu, standart raporlar, geçici raporlar ve uyarılar üreterek gelişmelerin, kalıpların ve istisnaların belirginleşeceği şekilde tanımlamak için verileri ve bilgileri inceler,[47] Tanımlayıcı analitik; merkezi eğilim (ortalama, medyan ve mod), dağılım ölçüleri (standart sapma), çizelgeler, grafikler ve frekans dağılımı gibi istatistiksel tekniklerden oluşan keşif analizi kullanılarak büyük veri kümelerinin anlaşılmasına ve görselleştirilmesine yardımcı olmak için kullanılır.[48]

---

[42] Makers Turkiye, "Veri Analizi ve Veri Analitiği Aynı Şey midir?", https://makersturkiye.com/veri-analizi-ve-veri-analitigi-ayni-sey-midir/ [Erişim Tarihi: 20.07.2022].

[43] Chrissy Kidd, Rachel Hornay, "Data Analytics vs Data Analysis: What's The Difference?", BMC, 8 Ocak 2021, https://www.bmc.com/blogs/data-analytics-vs-data-analysis/ [Erişim Tarihi: 20.07.2022].

[44] Makers Turkiye, a.g.e., https://makersturkiye.com/veri-analizi-ve-veri-analitigi-ayni-sey-midir/ [Erişim Tarihi: 20.07.2022].

[45] Sivarajah ve diğ. *a.g.e.*, 2.

[46] Rhoda C. Joseph, Norman A. Johnson, "Big Data and Transformational Government", *IT Professional* C.15, S.6 (2013): 43. DOI:10.1109/mitp.2013.61.

[47] Joseph ve Johnson, *a.g.e.*, 43.

[48] Ayisat Wuraola Yusuf-Asaju, Zulkhairi Md Dahalin, Azman Ta'a, "Framework for Modelling Mobile Network Quality of Experience Through Big Data Analytics Approach" *Journal of Information and Communication Technology (JICT)* C.17, S.1 (2018): 96.

• Tahmine Dayalı Analitik (Predictive Analytics): Geçmiş verileri kullanarak istatistiksel modelleme, veri madenciliği teknikleri ve makine öğrenimi ile gelecekteki sonuçlar hakkında tahminlerde bulunur.[49] Tahmine Dayalı Analitik, yapay zekâ, istatistik, makine öğrenimi ve veri madenciliği tekniklerinden yararlanır ve verilerdeki kalıpların veya eğilimlerin gelecekte ortaya çıkma olasılığını tahmin etmeyi amaçlar.[50]
• Kuralcı Analitik (Prescriptive Analytics): Optimizasyon ve rastgele testlerle ilgilidir. Tanımlayıcı ve tahmine dayalı analitik süreçlerinin ardından alınması gereken aksiyonların belirlendiği süreçtir.[51] Veriye dayalı karar vermenin önemli bir parçasıdır.

Veri analitiği günümüzde çeşitli algoritmalar ve programlar ile, ilgili verilerin doğru bir şekilde seçilmesi, ayıklanması ve yapılandırılması anlamlı sonuçlar verilen bir araçtır. Veri tabanında bilgi keşfi; veri sınıflandırması, tahmine dayalı veri madenciliği tekniği, veri kümeleme tekniği, aykırı değer analizi tekniği ve veri karakterizasyon ve ayrımcılığı tekniğini içeren madenlenebilir bilgi türlerinin tespiti; veri temizleme teknikleri, veri bütünleştirme teknikleri, veri dönüştürme teknikleri ve veri azaltma tekniklerini içeren veri ön işleme tekniklerini içeren veri madenciliği türleri ve sürecinin birer parçasıdır.[52]

ABD merkezli düşünce kuruluşu CFR'a (Council on Foreign Relations) bağlı Bağımsız Görev Gücü'nün güncellenmiş Temmuz 2022 tarihli ve siber uzay konulu raporunda (No. 80), veri bir jeopolitik güç ve rekabet kaynağı olarak ifade edilmiş ve bu sebeple ekonomik ve ulusal güvenliğin merkezi olarak vurgulanmıştır.[53] Bu durumda ekonomik ve ulusal güvenliğin merkezi olarak görülen verinin güvenliği de bir milli güvenlik meselesi olarak değerlendirilebilir. O halde, veri güvenliği bileşenlerinden biri olan siber güvenliği, siber uzay ve siber istihbarat bağlamında incelemek yararlı olacaktır.

---

[49] IBM, "What is Predictive Analytics?", https://www.ibm.com/analytics/predictive-analytics#:~:text=Predictive%20analytics%20is%20a%20branch,to%20identify%20risks%20and%20opportunities, [Erişim Tarihi: 20.07.2022].

[50] Asaju ve diğ. *a.g.e.*, 96.

[51] Sivarajah ve diğ. *a.g.e.*, 4.

[52] Agarwal, *a.g.e.*, 204- 207.

[53] Adam Segal, Gordon M. Goldstein, "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet", *Independent Task Force Report: No.80*, CFR (Temmuz 2022): 3.

2.3. Siber Uzay ve Siber İstihbarat

Teknolojik ilerlemeler ile siber ortamda güvenlik anlayışı, harbin çehresiyle birlikte gerçekleştiği ortamları da değiştirmiştir. Kara, deniz ve hava muharebe alanlarına önce uzay yeni bir harekât alanı olarak dâhil olmuş ve gelinen noktada bilgi teknolojilerinin savaşların kaderine yön vermesindeki kritik rolünden dolayı "siber uzay" da harbin beşinci harekât alanı olarak nitelendirilmiştir.[54]

Siber uzay terimi ilk kez, bilim kurgu yazarı William Gibson tarafından 1982'de Omni dergisinde yayınlanan bir hikâyede ve ardından cyberpunk türündeki romanı *Neuromancer*'da (1984) kullanılmış[55] ve dijitalleşmenin hayatın her alanına nüfuz ettiği günümüzde bir olgu hâlini almıştır. Steve Katzman siber uzay için "ölçemezseniz iyileştiremezsiniz" demiştir.[56] Bu yüzden siber uzayı ölçmek için ilk aşamada iyi tanımak elzemdir.

David D. Clark, 2010 yılında siber uzay kavramını; fiziksel katman, mantıksal katman, bilgi katmanı ve insan katmanı olmak üzere dört katman çerçevesinde karakterize etmiştir.[57] Fiziksel katman, somut olması bakımından siber uzay katmanları arasında en kolay tanımlanan katmandır. Bilgisayarlar, sunucular, sensörler, dönüştürücüler, elektronik iletim kabloları, teller, fiber optik lifler, veri depolama cihazları gibi kısaca fiziksel özelliği olan aygıtlardan oluşur.[58] Mantıksal katman, siber uzayın merkezî sinir sistemi olarak bilinir. Alan adı sistemleri (DNS), İnternet protokolleri, tarayıcılar, web siteleri ve yazılımlar aracılığıyla veri paketlerini nihai varış noktalarına teslim etmekten sorumludur.[59] Enformasyonun var edilmesi, yakalanması, depolanması ve

---

[54] Hasan Çiftçi, " Harbin Beşinci Boyutu", *Her Yönüyle Siber Savaş*, 2.bs, (2017: TÜBİTAK Popüler Bilim Kitapları), 7.

[55] Jennifer Bussell, "Cyberspace", *Encyclopedia Britannica*, 12 Mart 2013. https://www.britannica.com/topic/cyberspace. [Erişim Tarihi: 22.11.2022].

[56] Steve Katzman, "Operational Assesments Fieldwork", *Operational Assessment of IT*, (Boca Raton: CRC Press, 2016), 135'den aktaran, Adrian Venables, "Modelling Cyberspace to Determine Cybersecurity Training Requirements", *Frontiers in Education*, C.6, S.768037 (2021): 5. DOI: 10.3389/feduc.2021.768037.

[57] David D. Clark, "Characterizing Cyberspace: Past, Present and Future", *ECIR Working Paper No:2010-3* (Massachusetts: MIT Political Science Department, 2010), 1- 3.

[58] *a.g.e.*, 2.

[59] Alison Lawlor Russel, "The Logic Layer", *Stratejik A2/AD in Cyberspace* (Cambridge: Cambridge University Press, 2017), 40. doi:10.1017/9781316817001.004.

işlenmesi siber deneyimin merkezindedir. Enformasyon katmanı, paylaşılan müzik, metinsel içerikler, videolar, işletmelerin depolanan kayıtları ve dünya çapında çevrimiçi tüm aktiviteleri ifade etmektedir.[60] İnsan katmanı ise Clark'ın yaklaşımıyla, kullanmayı seçtikleri yollarla siber uzayın karakterini oluşturur ve değiştirirler.[61] Bu noktada insanların demografik koşullarına göre değişen karakterleri, siber uzaydaki etkinliklerini de etkiler ve bu da siber uzayın çehresinde mozaik bir etki yaratır.

Adrian Venables, 2021 yılında, siber uzay katmanlarını daha da detaylandırmış ve farklı bir yaklaşımla ele alarak siber uzayı sekiz katman olarak çerçevelemiştir.[62] Adrian Venables'in sekiz katmanlı siber uzay modeli aşağıdaki gibidir:



Şekil 2.1. Sekiz Katmanlı Siber Uzay Modeli.

(Yazar tarafından Türkçeleştirilmiştir).[63]

[60] Clark, *a.g.e.*,3.

[61] *a.g.e.*, 4.

[62] Adrian Venables, "Modelling Cyberspace to Determine Cybersecurity Training Requirements", *Frontiers in Education* C.6, S.768037 (2021): 5. doi: 10.3389/feduc.2021.768037 .

[63] *a.g.e.*, 6- 11.

Venables bu katmanları şöyle açıklamıştır:[64]

- Coğrafi (Geographical) katman; siber uzayın üzerinde şekillendiği, altyapıların ve kullanıcıların üzerinde ikâmet ettiği gerçek dünya ortamını vurgular. Venables, coğrafi şartların desteklediği şartlar bakımından; hava veya uzay yoluyla yayılımın yalnızca radyofrekans yoluyla, denizde ise denizaltı kablolarıyla, gemiler arasında veya kıyı ile kablosuz olarak gerçekleştirilebileceğini ayrıca dağlık bölgelerin gömülü kablo sistemini desteklemeyebileceğini veya çöl ikliminin direğe monteli mikrodalga bağlantılarını desteklemeyebileceğini örnek olarak göstermiştir. Ayrıca Venables, bazı ülkelerin, izleme veya sansür olmadan sınırların ötesinde verilerin serbest geçişine izin vermeyebileceğinden siyasi yönlerin de bu katmanda değerlendirilmesini önermiştir. Örnek olarak Çin Halk Cumhuriyeti'nde 1 Kasım 20212'de yürürlüğe giren Kişisel Enformasyonu Koruma Yasası ile, kişisel enformasyonun işlenmesi hususunda bireysel izin almayı ve yurt dışı menşeli şirketlerin işledikleri kişisel enformasyonu Çin Anakarasından çıkarabilmeleri için, öncelikle ÇHC siber uzay yetkilileri tarafından yapılan güvenlik değerlendirmesinden geçmek, gereken sertifikayı almak ya da siber uzay yetkililerinin öngördüğü standart bir mukavele imzalamak gibi belirli sınırlama ve şartlar getirilmiş, kararı ihlâl eden şirketler için para cezası, işletme faaliyetlerinin durdurulması, şirket lisanslarının iptali gibi yaptırımlar öngörülmüştür.[65]
- Hizmet katmanı; Venables, bu katmanı güvenlik açıkları bakımından siber saldırganlar için en çekici katman olarak değerlendirmiş ve ülkelerin kritik altyapıları, bölgesel bağlantıları temin eden merkezî noktalar ve siber sistemin kullanımı için enerji sağlayan elektrik trafoları gibi fiziksel saldırılara da açık olan noktaların korunmasını bu katmana dâhil etmiştir. Hizmetler katmanı kısaca, siber uzayın sürdürülebilirliğini ifade etmektedir.
- Altyapı katmanı; siber uzayın fiziksel düzenlemesini içerir ve verileri toplayan, depolayan, işleyen, ileten, sunan ve aktaran donanım bileşenlerini içerir. Bileşenlerin çalınması veya fiziksel olarak yok edilmesi gibi kinetik saldırılara karşı hassas olması

---

[64] *a.g.e.,* 6- 11.

[65] The Office of the Privacy Commissioner for Personal Data (PCPD), "Personal Information Protection Law of the Mainland", Hong Kong, https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html. [Erişim Tarihi: 28.11.2022].

ve onarımının oldukça maliyetli olması nedeniyle bu katmanın güvenliği bileşenlerin korunmasını öncelemektedir.

- Fiziksel katman, kablolu bağlantılarda, fiber optik kablolardaki fotonların ve kablolamadaki elektronların geçişini içerir. Ayrıca kablosuz iletişim araçlarını (mobil telefon, wi-fi, bluetooth, mikrodalga, uluslararası uydu bağlantıları) da içeren geniş bir frekans aralığı içerir.
- Sözdizimsel katman, yazılım protokollerini içerir.
- Semantik katman, bundan önceki katmanların ifade ettiği makineler arası etkileşimin ardından insanı işleve dâhil eden, makine ile insan arasındaki çevirim içi ortamı ifade eden ilk katmandır. Bilgisayar uygulamalarını ve bunların arayüzlerini içerir. Tüm sistem içinde güvenlik tehdidine en açık katman olarak değerlendirilmiştir çünkü insan faktörü, bilişsel insani faktörleri siber uzayda bir zafiyet hâline getirir. Semantik katmanın içinde siber uzayda bireysellik başlığıyla benzersiz dijital varlıklarımız ve persona kavramıyla siber uzayda takındığımız roller ve yansıttığımız çeşitli kişilik türleri ve sıfatlar da ifade edilmiştir.
- Misyon, siber uzayın bir parçası değildir fakat diğer katmanları bağlamsallaştırmak açısından katmanlar arasında ifade edilir. Her yeni aksiyonun bir amaca yönelik alınmasına atıfla, siber uzayın bir amacı yerine getirmek için tasarlandığını ve inşa edildiğini ifade eder.

Siber uzay katmanlarının her biri ayrı güvenlik açıkları barındırır ve tabiatlarına uygun güvenlik tehditlerini çekerler. Siber tehditlerin ortaya çıkmasıyla da siber güvenlik konseptleri oluşturulmuştur ve ortaya çıkan yeni tehditlere yönelik yeni güvenlik önlemleri de geliştirilmeye devam etmektedir. Saldırının, siber uzayın hangi katmanında yahut katmanlarında hasar oluşturduğunu bilmek, hasarın giderilmesi açısından elzemdir. Aynı zamanda güvenlik açığı hangi katmanda ise o katmana yönelik siber güvenlik yöntemleri takip edilecektir. Örnek olarak, altyapı katmanına yönelik bir siber saldırıda yahut doğal afetler gibi olağanüstü durumların yol açtığı hasarlarda yazılım kodlarından oluşan bir siber güvenlik yöntemi tek başına yararlı olmayacaktır.

ABD Ticaret Bakanlığı'na bağlı Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), siber uzay kavramını *"internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler dâhil olmak üzere birbirine bağlı bilgi sistemleri*

altyapıları ağından oluşan bilgi ortamında küresel bir etki alanı" olarak tanımlamıştır.[66]

NATO liderleri, Temmuz 2016'da Varşova'daki NATO Zirvesi'nde siber savunmaya kaynak sağlamayı birincil öncelik haline getirmiştir.[67] Siber ortamın, mütearrıza en önemli katkıları, saldırılacak ülkeye ayak basmadan, ikmal, ulaştırma ve diğer lojistik faaliyetlerden tasarruf sağlaması, kimliğin gizlenme imkânı ve saldırının kendisini dahi gizleyebilmeye elverişli olmasıdır. Örnek vermek gerekirse, 2007 yılında Estonya'ya düzenlenen ve emarelerin Rusya'yı işaret ettiği siber saldırılar ile, Estonya halkının o dönemlerde oy kullanmak, vergilerini ödemek ve cep telefonlarıyla alışveriş yapmak, park yeri için ödeme yapmak gibi işlemler için rutin olarak kullandığı internetin çökmesi, ülkede hayatı neredeyse durma noktasına getirmiştir. Estonya Savunma Bakanı Jaak Aaviksoo bir röportajda, siber saldırının bir ulusal güvenlik sorunu olduğu farkındalığına ulaştıklarını ifade etmiştir.[68]

Günümüzde ülkelerin; bireyler, STK'lar ve devlet kurumları dâhil her türlü ekonomik, ticari, kültürel, sosyal ve bürokratik faaliyetlerinin ve etkileşimlerinin ekseriyeti siber uzay üzerinden yürütülmektedir.[69] Bu durumda, siber uzayda kullandıkları sistemler ile ilgili herhangi bir istikrarsızlık, vatandaşların, kurumların ve dolayısıyla devletlerin bilgi ve işlem güvenliklerini tehlikeye atacak bir millî güvenlik sorunu teşkil edecektir. Siber saldırılar, siber uzayın herhangi bir alanını ihlâl edebilen, yıkıcı sonuçlara neden olabilen eylemlerdir. Devletler, siber ortama bu denli adapte olunan bu çağda sistemlerinin istikrarlı ve güvenli bir şekilde çalışmaya devam etmesi sağlamak için çeşitli önlemler almak durumundadırlar. Nitekim, Mayıs 2011'de dönemin ABD Başkanı Barack Obama tarafından imzalanan *"Uluslararası Siber Uzay Stratejisi"* belgesinde, elektrik, su ve hava trafiği kontrolünü ifade eden ve finansal sistem için

---

[66] National Institute of Standards and Technology, "Glossary", *Information Security*, Eylül 2012, B-2.

[67] Neil Robinson, "Spending for success on cyber defence", *NATO Review*, 6 Nisan 2017, https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html [Erişim Tarihi: 12.07.2022].

[68] Mark Landler, John Markoff, "Digital Fears Emerge After Data Siege in Estonia", *The NewYork Times*, 29 Mayıs 2007, https://www.nytimes.com/2007/05/29/technology/29estonia.html. [Erişim Tarihi: 03.10.2022].

[69] Yuchong Li, Qinghui Liu, "A Comprehensive Review Study of Cyber Attacks and Cyber Security; Emerging Trends and Recent Developments", *Energy Reports* C. 7 (2021): 8176.

büyük önem taşıyan kritik altyapıların tümünün ağ bağlantılı bilgi sistemlerine bağlı olduğu hatırlatılmış ve kritik altyapıların siber uzaydaki güvenliğine önemle vurgu yapılmıştır.[70]

Eski CIA ve NSA yöneticisi Michael Hayden, siber âlemde saldırı amaçlı istihbarat çalışması ile savunma amaçlı güvenlik çalışmasının, sabotaj amaçlı bilgisayar korsanlığı gibi birlikte bulanıklaşma eğiliminde olduğunu ifade etmiştir.[71] Analistlerin müracaat ettikleri veri kaynakları, süpermarket indirim kartlarından, bulut hizmet sağlayıcılarından, sosyal medyadan ve e-posta, tarayıcı geçmişi ve anlık mesajlaşma gibi daha hassas kaynaklardan kolayca elde edilmektedir ve teknolojinin sağladığı bu elverişlilik, siber güvenlik ve siber istihbaratı giderek iç içe geçirmektedir.[72]

ABD Savunma Bakanlığı'na tavsiyelerde bulunmak için bir federal danışma komitesi olarak kurulan Savunma Bilim Kurulu'nun (DSB), Ocak 2013'te Savunma Bakanlığı'na siber direnci arttırmaya yönelik tavsiyelerde bulunduğu bir rapor yayınlamıştır. Raporda, *"Düşman siber yetenekleri, planları ve niyetlerini anlamak ve karşı stratejileri etkinleştirmek için istihbarat toplama ve analizine yeniden odaklanılmalı"* tavsiyesi yer almaktadır.[73] Buradaki tanımın, taktik ve operasyonel seviyede bir istihbarattan daha uzun vadeli bir amaca yönelik olduğu için, stratejik siber istihbarata yönelik bir tanımlama olduğunu söylemek doğru olacaktır. Siber istihbarat faaliyetleri, siber güvenliği sağlama yahut bir siber saldırı gerçekleştirme maksadının ötesinde, bir istihbarat faaliyetidir. Siber istihbarat, siber güvenlik uygulamalarının yanı sıra istihbaratın siber uzaydaki uygulamalarını da içerir ve hem istihbaratın diğer bileşenlerinden de yararlanır hem de istihbaratın diğer bileşenlerine katkı sunar.

Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü (SEI) İnovasyon Merkezi, Siber İstihbarat Ticaret Projesi (CITP) olarak bilinen çalışmasında siber istihbaratı *"karar verme sürecini geliştirmek için eylem etüdleri sunan siber*

---

[70] The White House, "İnternational Strategy for Cyberspace", Mayıs 2011, Washington, 3.

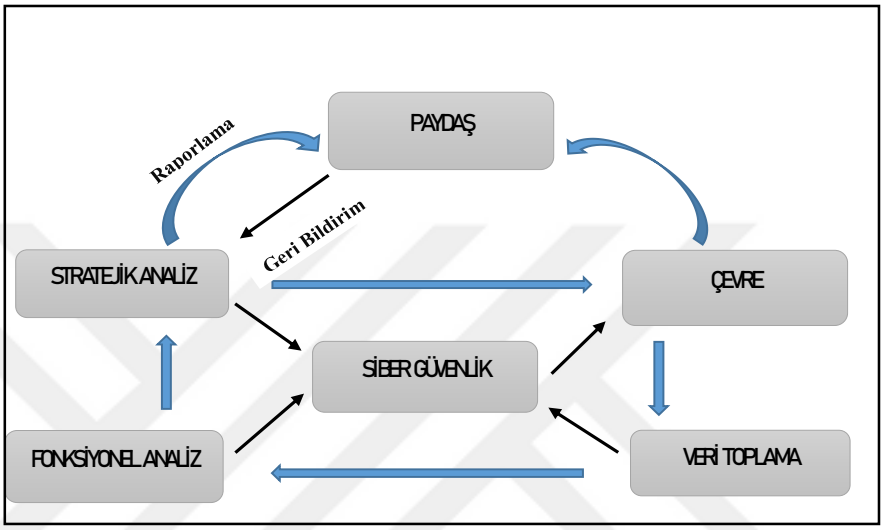
[71] Herrington, *a.g.e.*, 566.

[72] *a.g.e.*, 567.

[73] Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat", Washington DC, (01.01.2013): 46.

yetenekleri, niyetleri ve faaliyetleri belirlemek, izlemek ve tahmin etmek amacıyla bilgilerin elde edilmesi ve analizi" olarak tanımlamıştır.[74]

Townsend ve arkadaşları, CITP raporunda, ABD'nin geleneksel istihbarat döngüsünü siber istihbarat açısından eksik bulmuş ve siber istihbarat analizini özel teknik analiz ve stratejik analiz olmak üzere iki ayrı işleve ayırarak yeni bir istihbarat döngüsü modeli oluşturmuşlardır.[75]



Şekil 2.2: CITP Analitik Çerçevesi.

(Yazar tarafından Türkçeleştirilmiştir).[76]

CITP Analitik Çerçevesinin açıklaması özetle şöyledir;[77]

- *Çevre: Siber istihbaratın kapsamını belirleyip gerekli verileri belirlemek,*
- *Veri Toplama: Otomatikleştirilmiş ve emek yoğun araçlar aracılığıyla, analistlerin veri kaynaklarını keşfetmesi, bilgi toplaması ve analiz yapmak için bunları bir araya getirmesi,*

[74] Troy Townsend, Melissa Ludwick, Jay McAllister, Andrew O. Mellinger, Kate Ambrose Sereno, "SEI Innovation Center Report: Cyber Intelligence Tradecraft Project Summary of Key Findings", *Cyber Intelligence Tradecraft Project (CITP)* (2013): 2.

[75] Townsend ve diğ., *a.g.e.*, 2.

[76] *a.g.e.*, 3.

[77] *a.g.e.*, 3.

- *Fonksiyonel Analiz: Analistlerin, tipik olarak bir siber güvenlik misyonunu desteklemek için teknik ve özel analiz yapmak maksadıyla toplanan verileri kullanması,*
- *Stratejik Analiz: Analistlerin, işlevsel verilere stratejik bir mercek uygulayarak bu istihbaratı bir paydaşa bildirmesi veya çevreyi etkilemek için kullanması. (Fonksiyonel analiz, siber tehditlerin "ne" ve "nasıl" sorularına yanıt vermeye çalışıyorsa, stratejik analiz "kim" ve "neden" yanıtlarını vermeyi amaçlar).*
- *Paydaş Raporlama ve Geri Bildirim: İstihbaratın paydaşlara dağıtıldıktan sonra, geri bildirim sağlanması ve/veya istihbaratı çevreyi etkilemek maksadıyla kullanmaları.*

Ulusal çıkarlara hizmet etmek maksadıyla yapılan ve deşifre olmuş birçok siber istihbarat girişimi ve teşekkülü vardır, deşifre olmamış birçok faaliyetin de hâlihazırda devam ediyor olabileceğini unutmamak gerekir. Siber istihbarat faaliyetleri internetin henüz var olmadığı dönemlerden itibaren var olmuştur. Bir siber elektronik istihbarat faaliyeti olan ECHELON, bu konuya verilecek iyi örneklerden biridir. ECHELON, 1947 yılında İngiliz ve Amerikan sistemlerini, personelini ve istasyonları bir araya getiren ve gizli bir antlaşma olan "UKUSA Anlaşması" altında kurulmuştur. Tarafların önceleri inkâr ettiği fakat 2010 yılında Birleşik Krallık Hükümet İletişim Merkezi'nin (GCHQ) bazı belgelerini yayınlamasıyla[78] artık varlığı bir tartışma konusu olmaktan çıkan UKUSA Anlaşması'na kısa süre sonra Kanada, Avustralya ve Yeni Zelanda da dâhil olmuştur. Çalışma prensibi, uydu sinyalleri ile mikro dalga sinyallerinin yakalanması ve okyanus dibi uluslararası iletişim kablolarının dinlenmesi olmak üzere iki bileşenden oluşan sistem ile telefon trafiğini, telgrafları ve elektronik postaları (e-posta) izleme ve bunların verilerini tutma yeteneğine sahip olan sistem, haberleşme ağlarını yıllarca gözetim altında tutmuştur.[79] Makine öğrenmesi, derin öğrenme ve doğal dil işleme gibi bileşenleriyle yapay zekânın henüz var olmadığı dönemlerde bu gibi siber istihbarat faaliyetlerinin var olması, günümüzde siber istihbaratın geldiği durum bakımından çarpıcı bir fragman niteliğindedir.

---

[78] The National Archives, "Newly released GCHQ files: UKUSA Agreement" Haziran 2010, https://www.nationalarchives.gov.uk/ukusa/ [Erişim Tarihi: 03.10.2022].

[79] Gökhan Bayraktar, "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat", *Güvenlik Stratejileri Dergisi*, C.10, S.20 (2013): 134.

2.4. Psikografi

Psikografi, pazarlama ve reklam araştırmalarında demografik bilgilerinin yetersiz görülmesiyle, özellikle 2. Dünya Savaşı'ndan sonra hızlanan bir dizi çalışmanın sonucunda, pazar segmentasyon çalışmalarında demografiye alternatif bir yöntem olarak uygulanmaya başlanmıştır.[80] Erken çağlarında pazar araştırmalarında segmentasyon tekniği olarak ve müşterilerin psikolojik eğilimleri üzerinden ürün tercihlerini tahmin etmek için kullanılan bir yöntem olan psikografide, teknolojinin gelişmesi ve hızlıca ilerleyen dijitalleşme ile, büyük veri analitiği yöntemlerinden de yararlanılmaya başlanmıştır. Bilgisayar bilimi ve psikoloji bilimini bir potada eritmeye başlayan psikografi ve psikometri, büyük veri analitiği yöntemleriyle daha nokta atışı tespitlerin elde edilmesi evresine ulaşmıştır.

William D. Wells, psikografik araştırmayı operasyonel olarak, tüketicileri demografik boyutlardan farklı olarak psikolojik boyutlara yerleştirmeyi amaçlayan bir nicel araştırma olarak tanımlamıştır.[81] Yaş, cinsiyet, etnik köken, eğitim seviyesi, çalışma durumu, meslek, gelir, konuşulan dil, coğrafi konum, hobiler ve ilgi alanları gibi özellikleri ifade eden demografiden farklı olarak psikografi, tüketicilerin yahut hedef grubun psikolojik envanteri üzerinden ürün ve yan ürün tercihlerini belirlemeyi amaçlamıştır. Wells, genel segmentasyonların yeni ürün ve hizmetleri, tüketici popülasyonundaki farklı grupların ihtiyaçlarına göre uyarlama fırsatı sunduğunu ve psikografik yöntemlerin, tüketicileri tanımlama yönünden alternatif yöntemlere göre birçok ek avantajı olduğunu ifade etmiştir.[82] Psikografi, pazar araştırmalarının yanı sıra reklamcılık sektörünün de rehber araçlarından biridir. Nica ve arkadaşları, çevrimiçi ortamda müşteri hedeflemenin bir belirleyicisi olarak psikografik ve demografik yönlere dayalı müşteri segmentasyonu üzerine yaptıkları çalışmada, davranışsal hedefli afiş reklamcılığı, metin içi reklamcılık, sosyal ağ pazarlaması, çevrimiçi video reklamcılığı, konum tabanlı pazarlama, PPC pazarlaması, etkileyici

---

[80] William D. Wells, "Psychographics: A Critical Review", *Journal of Marketing Research*, C.12, S.2 (1975): 196. DOI:10.1177/002224377501200210.

[81] *a.g.e.*, 197.

[82] *a.g.e.*, 209.

pazarlama, çevrimiçi rezervasyon sistemleri, e-posta pazarlaması ve kurumsal internet sayfalarını pazarlama iletişiminin yeni bişimleri olarak tanımlamışlardır.[83]

Diaz ve arkadaşları, İspanyol politikacıların 2020'de atılan tweetlerinden oluşan bir veri seti (PoliCorpus-2020) üzerinden, yazar analizi ile siyasi ideolojiye dayalı psikografik özelliklerin belirlenmesini sınadıkları çalışmalarında, "geliştirilen otomatik sınıflandırıcıları rastgele kullanıcılarla değerlendirmek ve aynı dilsel özelliklerin siyasi ideolojilerini belirlemek için geçerli olup olmadığını değerlendirebilmek" yönünden umut verici bulmuşlardır.[84]

Kullanıcıların e-ticaret sitelerinden yaptığı alışverişler, incelediği ürünler, sosyal medya platformlarında beğendiği ya da yalnızca incelediği gönderiler, irtibat kurduğu diğer sosyal ağ kullanıcıları gibi internet vasıtasıyla yaptıkları tüm eylemler, *dijital ayak izleri* olarak kaydedilmektedir. Gelinen nokta psikografi ve hedeflemeyi oldukça tehlikeli bir hâle getirmiştir. İnsanların duygu dünyaları, kişilikleri, tercihleri gibi psikometrik bilgilerini içeren veriler, istihbarat kurumları için oldukça elverişli bilgilerdir. İnternete artan bağımlılık, dijital gözetimin tahmin edilemez ve önlenmesi zor boyutlara ulaşmasına neden olmuştur. Bu bakımdan psikografi, uygun analitik yöntemleriyle birleştiğinde kâbiliyeti elinde bulunduran odağın gücünü belirgin şekilde arttıracaktır.

Wells, pazarlamanın neredeyse tamamı iletişim olduğundan, pazarlamacıların en çok hedef kitlelerini tanıdıklarında etkili olacaklarını ifade etmiştir.[85] Psikografik çalışmaların erken çağlarında, yapılan araştırmalarda genel olarak tüketici anket verilerinden ve istatistik biliminden yararlanılmıştır.[86] Fakat günümüzde bu işlemleri,

---

[83] Elvira Nica, Lubica Gajanova, Eva Kicova, "Customer Segmentation Based on Psychographic and Demographic Aspects as a Determinant of Customer Targeting in The Online Environment", *Littera Scripta*, C. 12, S. 2 (2019): 109. https://doi.org/10.36708/Littera_Scripta2019/2/0.

[84] José Antonio García-Díaz, Ricardo Colomo-Palacios, Rafael Valencia-García, "Psychographic Traits İdentification Based on Political İdeology: An Author Analysis Study on Spanish Politicians' Tweets Posted in 2020", *Future Generation Computer Systems*, C.130 (2022): 59- 74. https://doi.org/10.1016/j.future.2021.12.011.

[85] Wells, *a.g.e.*, 197.

[86] Jack A. Lesser, Marie Adele Hughes, "The Generalizability of Psychographic Market Segments across Geographic Locations", *Journal of Marketing*, C.50, S.1 (1986): 20. DOI:10.1177/002224298605000102.

çevrimiçi kullanıcıların dijital ayak izleri vasıtasıyla, akan veriler ile yarışan gelişmiş algoritmalar yapmaktadır.

Gelişimini sürdüren çevrimiçi reklamcılık, hedef odaklı reklam yayınları için oldukça elverişli hâle gelmiştir. Geleneksel iletişim araçlarından biri olan televizyonlarda, reklamlar, ürünle ilgisi olsun yahut olmasın, reklamın yayınlandığı anda o kanalda olan kişiler için görünür olmaktaydı. Bugün televizyon kanallarında durum hâlâ aynı olmasına karşın, çevrimiçi ortamlarda tüketicilerin psikografik tekniklerle hedeflenmesi ve segmentasyonu sayesinde, ilgili reklamlar daha çok ilgili kişilere görünür olmaktadır. Çevrimiçi ortamlardaki sayısız statik ve akışkan verinin daha nokta atışı bir hedefleme paterni oluşturabilme avantajına dönüştürdüğü bu hedeflemeye "mikro hedefleme" denilmektedir. Birleşik Krallık Bilgi Komisyonu Ofisi (ICO), mikro hedeflemeyi şöyle tanımlamaktadır: *"Mikro hedefleme, belirli bir kitlenin veya bireyin eylemlerini etkilemek için ilgi alanlarını belirlemek için kişisel verileri analiz eden bir çevrimiçi hedefli reklamcılık biçimidir*."[87] Facebook (ve bünyesindeki Instagram), Twitter, YouTube gibi sosyal medya şirketleri, platformu ticari amaçla kullanan kullanıcılarına mikro hedefleme ile sponsorlu reklamlar yayınlama imkânı tanımaktadırlar. Örnek vermek gerekirse; Instagram'da işletme hesabı oluşturularak; reklamın yayınlanma hedefi (daha fazla profil ziyareti, daha fazla internet sitesi ziyareti, daha fazla mesaj) ve hedef kitle (konum genişliği, ilgi alanları, yaş ve cinsiyet) seçimleri düzenlendikten sonra, ödeme tutarı ve reklam yayınlanma süresi seçilerek reklam yayınlanabilmektedir. Algoritmik bir onay sürecinden geçtikten sonra reklam onaylanıp yayınlanmakta yahut reddedilmektedir. Instagram'ın reklam araçlarını tanıtırken kullandığı şu ifadeler çarpıcıdır:

> "*Gönderilerinizden birini öne çıkararak reklama dönüştürün. Kullanıcıları nereye yönlendireceğinize, reklamı kimlerin göreceğine ve ne kadar harcama yapacağınıza karar vermeniz yeterlidir*", "*İşletmenizin reklamını verin, hassas hedefleme ve eyleme dönüştürülebilir istatistiklerle yeni müşterilerinize erişin.*"[88]

[87] ICO, "What Is Microtargeting?", https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting/. [Erişim Tarihi: 10.11.2022].

[88] Instagram Business, *Instagram'da Reklam Verilmesi*, https://business.instagram.com/advertising?locale=tr_TR. [Erişim Tarihi: 10.11.2022].

Büyük veri analitiği algoritmalarının markalar için önemli bir marifeti olan bu uygulamalar, yalnızca markalara ait ürünleri değil, sosyal mesaj içeren mesajları da aynı hedefleme algoritmaları sayesinde adrese teslim etmektedir. Örneğin, Instagram'da hem kişisel hesapların hem de işletme hesaplarının ücretsiz olarak oluşturabildikleri *reels* içerikleri, belirli keşfedilmiş tekniklerin uygulamasıyla daha fazla görüntülenme, beğeni, kaydetme ve içerik etkileşimi alabilmektedir. Bir propagandist, dolaylı duygusal çekicilik gibi bir propaganda yöntemi ile söz konusu sosyal medya şirketlerinin yasal kısıtlamalarına takılmadan birçok kullanıcıya ulaşabilir.

Wells, psikografilerin; bazen demografik profillerden elde edilebilecek özelliklerin varlığını doğruladığını, bazen bir demografik profilin gösterdiği özelliklerin varlığını ortaya çıkardığını, bazen de yanlış olabilecek çıkarımları çürüttüğünü öne sürmüştür.[89] Jack A. Lesser, Marie Adele Hughes, 1986 yılında psikografik pazar bölümlerinin coğrafi konumlarda genellenebilirliğini sınadıkları çalışmalarında, 17 pazarda elde edilen prototip segmentasyon çözümlerinin benzerliğinin, bir coğrafi pazarda geliştirilen psikografik segmentlerin diğer coğrafi pazarlara genellenebilir olduğu sonucuna ulaşmışlardır.[90] Bu noktada duygu durum ve kişiliğin etkilediği psikografik segmentasyon, segmentasyonda demografik özellikleri aşan başka bir durum olarak ortaya çıkmıştır.

Psikografik bilgi ile demografik bilgi arasındaki en önemli fark, psikografilerin, davranışları yönlendirme (ürün satışı gibi) amacıyla duygu ve kişilik çözümlemelerine yönelmesidir. Davranış ve kişilik arasındaki ilişki, Çinlilerin ve Mısırlıların, Hipokrat'ın ve bazı Avrupalı filozofların ilk yazılarına kadar uzanan tarih dönemlerinden beri inceleme konusu olmuştur.[91] Pazarlama ve tüketici davranışı alanlarında kişilik konusundaki çalışmalar, Sigmund Freud'un, vurguladığı kişiliğin ve motivasyonun bilinçdışı doğası ve davranışın çoğunun kişilik sistemindeki streslerle ilgili olduğu teorisinden önemli ölçüde etkilenmiştir.[92] Wells, psikografiye

---

[89] Wells, *a.g.e.*,209.

[90] Lesser ve Hughes, *a.g.e.*, 25.

[91] Harold H. Kassarjian, "Personality and Consumer Behavior: A Review". *Journal of Marketing Research*, C.8, S.4 (1971): 409. DOI:10.2307/3150229.

[92] Kassarjian, *a.g.e.*, 409.

av malzemeleri satan bir yer üzerinden örnek verirken; avcılığın şiddet içerikli bir spor olmasından dolayı avcının şiddete meyyal olabileceğinden, avcılığın risk içermesinden dolayı avcının risk alabilen biri olabileceğinden ve avcıların kendi işini yapmayı tercih eden bir yapıda olabileceklerinden bahsetmektedir.[93]

Yukarıda Instagram reklamlarındaki örneklemede anlatıldığı üzere, tüketiciye demografik bilgilerle belirlenmiş bir hedefleme ile reklam seçeneği sunulmaktadır fakat veriyi dolayısıyla çağımızda gücü elinde bulunduran panoptik odaklar, her saniye akan yüksek miktarda veri ile psikografik segmentasyon oluşturarak nokta atışı, mikro hedeflemeler ile reklam ve propaganda amaçlarını gerçekleştirebilmektedirler.

2.5. Sosyal Medya Analitiği

We Are Social'ın Dijital 2022 Küresel Genel Bakış Raporuna (Digital 2022 Global Overview Report) göre, Ocak 2022'de dünya çapında 4,62 milyar sosyal medya hesabı vardır ve bu rakam dünya toplam nüfusunun yüzde 58,4'üne eşittir. Rapor, buradaki her bir sosyal medya hesabının benzersiz bireyleri temsil etmeyeceğini de vurgulamaktadır. Rapora göre, küresel internet kullanıcıları 2022'nin başında 4,95 milyara yükselmiştir ve internet penetrasyonu, raporun yayınlandığı tarih itibariyle dünya toplam nüfusunun yüzde 62,5'ini oluşturmaktadır.[94]

Hem bireysel hem de toplumsal hayatla bu denli iç içe geçen internet, ilk olarak farklı amaçlar için icat edilmiş olsa da geçirdiği gelişim aşamaları ile bugün bambaşka bir konumdadır. 1957'de SSCB'nin Sputnik lansmanının ardından, 1958 yılında ABD Savunma Bakanlığı bünyesinde, "stratejik ve teknolojik sürprizlerden kaçınmak amacıyla" kurulan DARPA (Defense Advanced Research Projects Agency)[95], 1969'da, "coğrafi olarak farklı yerlerde konumlanmış bilgisayarlar arasında dijital kaynakları paylaşmak" amacıyla ARPANET'i kurmuştur.[96] Bugünkü internetin ilk

---

[93] Wells, *a.g.e.*, 198.

[94] We Are Social, "Digital 2022: Another Year Of Bumper Growth", 26 Ocak 2022, https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/ [Erişim Tarihi: 24.10.2022].

[95] DARPA, "About DARPA", https://www.darpa.mil/about-us/about-darpa, [Erişim Tarihi: 23.10.2022].

[96] DARPA, "ARPANET", https://www.darpa.mil/about-us/timeline/arpanet [Erişim Tarihi: 23.10.2022].

temelleri böyle atılmıştır. CERN'de çalışan İngiliz bilim adamı Tim Berners-Lee'nin 1989 yılında World Wide Web'i (www) icat etmesiyle[97] internet kullanımı önce kurumlar sonra bireyler arasında yayılmaya başlamış ve gelinen son noktada neredeyse tüm işlerin ve iletişimin olağan bir zemini hâlini almıştır.

Web 1.0, işletmelerin bilgilerini yayınlamalarını ve bireylerin bu bilgileri yalnızca aramalarına ve okumalarına izin veren bir sistemdir.[98] Açık kaynakların (open source) internet ayağı böylece oluşmuştur. Web 2.0'da ise, işletmelerin yayınlarını bir broşür gibi okuyabilmek dışında kullanıcıların da yorum ve paylaşım yapabilmelerinin önü açılmıştır. Zeng ve arkadaşları, kullanıcı tarafından oluşturulan içerik veya tüketici tarafından oluşturulan medya gibi sosyal medyanın ana bileşenlerinin, web 2.0'ın tanımlayıcı özellikleri olarak görüldüğünü ifade etmişlerdir.[99] Böylece, web'in 4 nesli olarak tanıtılan web 1.0, web 2.0, web 3.0 ve web. 4.0 içerisinde bugünkü sosyal medya kullanımını yaratan bireylerin bir enformasyon ağına dâhil olmalarını sağlayan en önemli aşamanın, web 1.0'dan web 2.0'a geçiş aşaması olduğu düşünülmektedir. Araç açısından, web günlükleri, mikrobloglar, çevrimiçi forumlar, wiki'ler, podcast'ler, yaşam akışları, sosyal yer imleri, w eb toplulukları, sosyal ağlar ve avatar tabanlı sanal gerçeklik gibi web tabanlı birçok uygulama, sosyal medyanın işleyişini tanımlamaktadır.[100] Bu sitelerin birçoğu (örneğin Facebook, YouTube, Twitter, LinkedIn, Instagram), açılışından kısa süre sonra mobil uygulama formatlarıyla, internete erişilebilen her yerde ve her vakitte ulaşılabilir olmalarıyla, insanların hayatına daha fazla dâhil olmaya başlamışlardır.

İlk kullanıcı etkileşimi, Duke Üniversitesi'nden Tom Truscott ve Jim Ellis'in bir tartışma platformu olarak 1979'da tasarlayıp 1980'de kurdukları USENET ile olmuştur. Bugünkü sosyal medya konseptine daha yakın olarak Open Diary (OD),

---

[97]CERN Accelerating Science, "Where the Web was Born", https://home.cern/science/computing/birth-web/short-history-web, [23.10.2022].

[98] Sareh Aghaei, Mohammad Ali Nematbakhsh, Hadi Khosravi Farsani, "Evolutıon Of The World Wıde Web: From Web 1.0 To Web 4.0", *International Journal of Web & Semantic Technology (IJWesT),* C.3, S.1 (Ocak 2012): 1.

[99] Daniel Zeng, Hsinchun Chen, Robert Lusch, Shu-Hsing Li, "Social Media Analytics and Intelligence", *IEEE Intelligent Systems,* C. 25, S.6 (2010): 13. DOI:10.1109/MIS.2010.151.

[100] *a.g.e.*, 151.

Bruce Ableson ve Susan Ableson tarafından 1998'de kurulmuştur.[101] Bahsedilen platformlar konsept açısından bir temel sunsa da, sosyal medya teriminin formal tanımı, web 2.0 ve Kullanıcı Tarafından Oluşturulan İçerik (UGC) kavramlarına değinmeyi gerektirmektedir.[102] User Generated Content (UGC) ya da User-Created Content (UCC) olarak bilinen Kullanıcı Tarafından Oluşturulan İçerik'in, OECD 2007 raporuna göre 3 belirleyici unsuru vardır.[103] Bunlar;

- Yayın gerekliliği: Herkese açık (açık kaynaklı- open source) veya belirli bir gruba yönelik (örneğin üniversite öğrencileri) bir web sitesinde veya erişilebilir bir sosyal ağ sitesindeki bir sayfada yayınlanmasıdır. (Bu özellik, e-posta ve karşılıklı anlık iletiler ve benzerlerini hariç tutar).
- Yaratıcı çaba: Kullanıcıların değer kattığı, ilk kez oluşturulan yahut restore edilen, uyarlanan, belirli bir miktarda yaratıcı çaba içeren paylaşımlar olması gerekmektedir. (Yalnızca bir televizyon programının yahut bir gazete haberinin bir bölümünü kopyalamak ve doğrudan paylaşmak UCC olarak kabul edilmeyecektir).
- Profesyonel rutinlerin ve uygulamaların dışında oluşturulma: Kısaca finansal ya da ticari kâr amacı gütmeden yapılan paylaşımlardır. Motivasyon motifleri; "akranlarla iletişim, şöhret, kötü şöhret ya da prestij elde etmek yahut kendini ifade etmek" olarak tanımlanmıştır. (Ticari amaçlı/ sponsorlu reklam, tanıtım ve paylaşımları hariç tutar).

Kaplan ve Haenlein sosyal medyayı OECD'nin UCC standartlarından hareketle, "web 2.0'ın ideolojik ve teknolojik temelleri üzerine inşa edilen ve Kullanıcı Tarafından Oluşturulan İçeriğin (UGC) oluşturulmasına ve değiş tokuşuna izin veren bir grup internet tabanlı uygulama" olarak tanımlamışlardır.[104]

Bugün bildiğimiz anlamıyla sosyal medya sitelerinin başlıcaları; Facebook, Twitter, YouTube, LinkedIn gibi yoğun içerik üretilen ve paylaşılan sitelerdir.

---

[101] Andreas M. Kaplan, Michael Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media", *Business Horizons* C. 53, S. 1 (2010): 60.

[102] *a.g.e.,* 61.

[103] OECD, ""Defining and Measuring the Participative Web and User-Created Content*", Participative Web and User-created Content: Web 2.0, Wikis and Social Networking,* (2007): 18. ISBN 978-92-64-03746-5.

[104] Kaplan ve diğ., *a.g.e.,* 61.

Sosyal medya analitiği (SMA), tüm işletme genelinde sosyal ağların yıllar süren hızlı ve artan bir şekilde benimsenmesinden sonra yenilikçi bir araştırma alanı olarak ortaya çıkmıştır.[105] Bilgi ekosisteminin önemli bir parçası olan sosyal medyadan, kâr amacı gütmeyen kuruluşlar, ürün tasarımı ve inovasyonu, tüketici ve paydaş ilişkileri yönetimi ve pazarlama için hem zengin bir bilgi kaynağı hem de bir iş yürütme platformu olarak yararlanmaktadır.[106] Siyasetçiler ve hükümetler de toplumsal sosyal, ekonomik ve siyasi trendleri takip etmek, kamuoyu araştırmaları, propaganda ve tanıtım amacıyla sosyal medyadan yararlanmaktadırlar. Kullanıcıların sosyal medyada paylaştığı fikirleri, eğilimleri, konum bilgileri, ürün yorumları, fotoğraf ve videoları, ses kayıtları gibi kamuya açık olarak paylaştıkları veriler ile uygulanacak analitik yöntemleriyle ham verilerin temizlenmesi, anlamlandırılması ve analiz edilmesi yoluyla belirli bir gruba yönelik istihbarat da elde edilebilmektedir. İç güvenlik ve istihbarat kurumları için sosyal medya, radikal eğilimli ve terörist grup davranışlarını, onların işe alma ve halkla ilişkiler planlarını ve temel sosyal ve kültürel bağlamları da dahil olmak üzere incelemek için oldukça avantajlı bir platformdur.[107]

Zeng ve arkadaşları sosyal medya analitiğini, "genellikle bir hedef uygulamanın belirli gereksinimleri tarafından yönlendirilen sosyal medya verilerini toplamak, izlemek, analiz etmek, özetlemek ve görselleştirmek için bilişim araçlarını ve çerçevelerini geliştirmek ve değerlendirmek" olarak tanımlamışlardır.[108] Weiguo Fan ve Michael D. Gordon, sosyal medya analitiğini girdi- süreç- çıktı modelinden türettikleri 3 aşamalı bir süreç olarak incelemişlerdir: Sosyal medya kaynaklarını izleyerek veya dinleyerek, ilgili sosyal medya verilerini elde etmeyi, ilgili verileri arşivlemeyi ve ilgili bilgileri çıkarmayı içeren "yakalama (capture)", veriler üzerinde çeşitli gelişmiş veri analitik yöntemlerini kullanarak gürültülü ve düşük kaliteli verileri kaldırma ve modelleme için ilgili verileri seçmeyi içeren "anlama (understand)" ve karar vermek için elde edilen bulguları derlemeyi içeren "sunma (present).[109] Elde edilen sonuçlar tahmin

---

[105] Samuel Fosso Wamba ve diğ., "The Primer of Social Media Analytics", *Journal of Organizational and End User Computing*, C.28, S.2 (2016): 1. DOI: 10.4018/JOEUC.2016040101.

[106] Zeng ve diğ., *a.g.e.*, 14.

[107] *a.g.e.*, 14.

[108] *a.g.e.*, 14.

[109] Weiguo Fan, Michael D. Gordon, "The Power of Social Media Analytics", *Communications of the ACM*, C.57, S.6 (2014): 75. DOI:10.1145/2602574.

gücünden yoksun ve tutarsız ise, daha fazla veri elde etmek yahut analitik için yeni parametreler belirlemek için yakalama yahut anlama aşamasına tekrar dönülür.

Sosyal medya analitiği, hem veri kümelerinin analizi, yönetimi ve görselleştirilmesi bakımından büyük veri analitiğine hem de sosyal medyadaki tüketici faaliyetlerinin temel ilişkisel bileşenlerini anlamaya çalışması bakımından sosyal ağ analizine benzerlik göstermektedir.[110] Sosyal medya analitiğinin ilk aşaması olan veri toplama ya da Fan ve Gordon'un tabiriyle "yakalama" aşaması için öncelikle sosyal medya veri türlerini tanımlamak gerekir. Wamba ve arkadaşları, sosyal medya verilerini, demografik veriler, ürün verileri, psikografik veriler, davranış verileri, yönlendirme verileri, konum verileri ve niyet verileri olmak üzere 7 kategoride ele almışlardır.[111] Demografik veriler, yaş, ırk veya etnik köken, cinsiyet, eğitim, gelir ve coğrafya gibi kamuya açık olarak paylaşılan bilgileri; ürün verileri, sosyal medya kullanıcılarının tanıttığı, bahsettiği yahut tartıştığı marka ve ürünleri; psikografik veriler, tüketicilerin bir ürün veya marka ile ilgili kişiliğini, değerlerini, tutumunu, ilgi alanlarını ve yaşam tarzını ortaya koyan veriler; davranış verileri, tüketicilerin sosyal medyadaki satın alma kaydı gibi geçmişteki satın alma davranışlarını ifade eden veriler; yönlendirme verileri, kuruluşların veya şirketlerin bilgileri paylaşma maksadını belirlemelerine katkı sunan, tüketicileri "ağızdan ağıza reklam" oluşturmaya teşvik eden veriler; konum verileri kullanıcıların sosyal medyada yaptığı yer bildirimleri ve konum paylaşımlarını içeren verileri; niyet verileri ise, tüketicilerin bir ürün ile ilgili beklentilerini ve bunlarla ilgili gelecekteki yönelimlerini tahmin etme avantajı sağlayan verilerdir.[112]

Veri türlerinin tanımlanmasının dışında veri analizi türlerinin tanımlanması da önem arz etmektedir. Fan ve Gordon, sosyal medya analitiğinin birkaç aşamasını destekleyen bazı teknikleri, 3 aşamalı sosyal medya analitiğine göre şu şekilde sıralamışlardır: Anlama aşamasını desteklemesi bakımından duygu analizi (sentiment analiz) ve eğilim analizi; öncelikle anlama aşamasını desteklemesi fakat yakalama ve sunma aşamalarında da yararlanılabilmesi bakımından konu modelleme ve sosyal ağ

---

[110] Wamba ve diğ., *a.g.e.,* 2.

[111] *a.g.e.*, 3.

[112] *a.g.e.*, 3.

analizi; tüm aşamaları desteklemesi bakımından görsel analitik.[113] Fikir madenciliği veya duygu analizi (sentiment analiz), metin kaynaklarından kullanıcı duyarlılığını ve fikirlerini otomatik olarak analiz etmek için hesaplamalı dilbilim, doğal dil işleme ve diğer metin analizi yöntemlerinden yararlanır.[114]

Dünya nüfusunun neredeyse yarısının sosyal medya kullanıyor olması,[115] ki bu milyarlarca sosyal medya kullanıcısı anlamına gelir, sosyal medyanın yarattığı pazar açısından siber korsanlar için oldukça elverişli bir ortamdır. En temel zafiyetinin insan faktörü olduğu sosyal mühendislik saldırıları, sosyal medya üzerinden yapılan siber saldırıların oldukça yaygın bir yöntemidir. Sosyal mühendislik saldırıları, siber korsanın saldıracağı kişi ya da kurum bilgilerini sosyal becerilerini ve ikna kabiliyetini kullanarak ele geçirmesi ile gerçekleşmektedir.[116] Örnek olarak, Türkiye Cumhuriyeti İçişleri Bakanlığı'nın vatandaşlara zaman zaman SMS yoluyla gönderdiği "kendini polis ya da savcı olarak tanıtıp 'adınız terör örgütü soruşturmasına karıştı' diyerek para ve altın isteyenlere itibar etmeyin" tarzındaki mesajları, vatandaşların korku ve panik duygu durumlarından yararlanılarak yapılan sosyal mühendislik saldırılarına yönelik bir uyarıdır. İnsanın korku, panik gibi zafiyetleri gibi maddiyata düşkünlüğü ve para zafiyeti de saldırganların hedeflediği insan zafiyetlerindendir. Sosyal medya siteleri, algoritmalar yoluyla kullanıcılarını baktığı, beğendiği, paylaştığı, yorumladığı gönderilere yani dijital hareketlerine ve yaş, coğrafi konum, cinsiyet gibi demografik özelliklerine göre sınıflandırdığı veri tabanlarına sahiptir. İşletmeler reklam vermek istedikleri zaman, belirttikleri reklamın görüneceği bölgenin kaç km yarıçap civarında ya da hangi bölgede olacağı, hangi ilgi alanlarına mensup kullanıcılara hitap edeceği, yaş aralığı ve cinsiyet gibi tercih aralıklarını belirterek reklam verebilmektedirler. Siber korsanlar da bu işletmeleri taklit ettikleri, aslına çok benzer sosyal medya hesapları açarak benzer reklamları yayınlayabilmektedirler. Bu yöntemle, ücretin ödendiği fakat ürünün teslim alınamadığı ticari dolandırıcılıklar gerçekleşmektedir.

---

[113] Fan, Gordon, *a.g.e.*, 77.

[114] *a.g.e.*, 75.

[115] McAfee, "Staying Safer on Social Media", *The McAfee Safety Series*, 9, https://www.mcafee.com/content/dam/consumer/en-us/docs/guides/gd-staying-safer-social-media-guide.pdf. [Erişim Tarihi: 24.11.2022].

[116] Cybersecurity and Infrastructure Security Agency (CISA), "Avoiding Social Engineering and Phishing Attacks", *Security Tip* (ST04-014), 25 Ağustos 2020, https://www.cisa.gov/uscert/ncas/tips/ST04-014. [Erişim Tarihi: 25.11.2022].

ABD Federal Ticaret Komisyonu (FTC), 2021'de dolandırıcılık nedeniyle para kaybettiğini belirten kişilerin dörtte birinden fazlasının, sosyal medyada bir reklam, gönderi veya mesaj yoluyla dolandırıcıların ağına düştüklerini ve dolandırıcılığın gerçekleştiği sosyal medya sitesi olarak dolandırılanların onda dokuzunun Facebook veya Instagram'ı işaret ettiğini bildirmiştir.[117]

Akıllı telefonların yaygınlaşması ve sosyal medyanın uygulama (app) konseptinin; internete ulaşılabilen her vakitte ve her yerde erişilebilir olması, gerçek zamanlı paylaşımlara izin vermesi, kullanıcıların sevinçlerini, üzüntülerini, öfkelerini, fikirlerini, bilgilerini, başarılarını ve başarısızlıklarını, sevdikleri ve sevmedikleri şeyleri, ilgi alanlarını yoğun olarak paylaşmalarını yaygınlaştırmıştır. Bilginin kontrol edilmesinin ve doğrulanmasının zorlaştığı internet ortamı, sosyal medya platformlarında fitili ateşlenen ve yayılan kitlesel hareketlere de zemin oluşturmuştur. Örnek olarak, 17 Aralık 2010'da Tunus'ta Muhammed Buazizi adlı seyyar satıcı, ruhsatsız satış yaptığı gerekçesiyle karşı karşıya kaldığı bürokratik müdahaleyi protesto etmek amacıyla bir intihar eylemi gerçekleştirerek kendini ateşe vermiştir. Olayın geniş çapta yankı bulmasıyla işsizlik ve refah seviyesi düşüklüğü gerekçesiyle sokak eylemleri başlamış ve protestolar ülke geneline yayılmıştır. Video paylaşım sitelerinde ve Facebook gibi sosyal medya platformlarında protestolar ile ilgili yapılan yoğun paylaşımlar hem protestoların daha da yayılmasını hem dünyaya duyurulmasını kolaylaştırmış ve olayların ardından Bin Ali Hükümeti düşmüştür.[118] Kuzey Afrika'da başlayan isyanların adeta bir domino etkisiyle Ortadoğu'ya da sıçramasıyla literatürde "Arap Baharı" olarak adlandırılan Arap ayaklanmaları baş göstermiştir. Tunus örneği, global internet ağları sayesinde sosyal medyanın örgütlenmeye elverişli bir ortam oluşturması açısından iyi bir örnektir.

---

[117] Emma Fletcher, "Social Media a Gold Mine for Scammers in 2021", *Data Spotlight*, 25 Ocak 2022, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021#footnote1. [Erişim Tarihi: 24.11.2022].

[118] Paul R. Viotti, Mark V. Kauppi, "Uluslararası İlişkiler ve Dünya Siyaseti", *Uluslararası İlişkiler ve Dünya Siyaseti*, 5. bs, çev. Ayşe Özbay Erozan, (Ankara: Nobel Yayınevi, 2017), 2.

3. ÖRTÜLÜ OPERASYONLAR

İstihbarat, tabiatının getirdiği amaç ve metodolojiler bakımından; istihbarat toplama ve analizi, karşı istihbarat/ kontrespiyonaj ve örtülü operasyon olmak üzere üç disiplin veya misyondan oluşmaktadır.[119] İstihbarat toplama ve analiz süreçleri, karar vericinin ilgili istihbaratı talep etmesinden sonra, veri ve enformasyonun insan istihbaratı, teknik istihbarat ve açık kaynak istihbaratı gibi kaynaklardan toplanması ile başlayan, analiz edilen ve karar vericiye teslim edilen klâsik istihbarat döngüsü sürecini ifade eder.[120] Karşı istihbarat, düşman unsurların enformasyon elde etme amaçlı operasyonlarını elde etme amacıyla düşman unsur istihbarat görevlilerinin angaje edilmesi de dâhil olmak üzere çeşitli gizli operasyonların kullanılmasını; kontrespiyonaj (karşı casusluk) ise sırların düşman unsur tarafından ele geçirilmesinin engellenmesini kapsamaktadır.[121]

Örtülü operasyon ise istihbarat toplama ve analizi ile karşı istihbarat/ kontrespiyonajın dışında başlı başına bir istihbarat disiplinidir. Devletler, örtülü operasyonları dış politika hedeflerine ulaşmada diplomasinin yetersiz kalacağı ve askerî harekâtlardan da kaçınmayı yeğledikleri durumlarda bir dış politika aracı olarak kullanabilmektedirler. Örtülü operasyonlar, yalnızca hükümetler tarafından başka devletlere yönelik gerçekleştirilen eylemler değildir fakat bu çalışmada bir dış politika enstrümanı olarak, sınır aşan örtülü operasyon uygulamaları incelenecektir.

İstihbaratın ve dolayısıyla örtülü operasyonların tabiatındaki gizlilik olgusu nedeniyle, örtülü operasyonların üzerinde ittifak edilen tek bir tanımlaması yoktur. İstihbarat disiplinine bir dış gözlemci olarak çeşitli yaklaşımlar ve tanımlar getiren

---

[119] Daugherty, "The Role of Covert Action in Intelligence and Foreign Policy", 9.

[120] Christopher Andrew, Richard J. Aldrich, Wesley K. Wark, "Introduction", *Secret Intelligence: A Reader*, ed. Christopher Andrew, Richard J. Aldrich, Wesley K. Wark (Oxon: Routledge, 2020), 1.

[121] Daugherty, "The Role of Covert Action in Intelligence and Foreign Policy", 11.

akademisyenler ve araştırmacılar, istihbarat kurumlarında görev almış olan yazarlardan ya da iç gözlemcilerden daha özgürce ifadelerde bulunabilirler fakat onların eriştikleri belge ve bilgilere erişimlerinin olmaması da bir dezavantaj yaratmıştır.

Bu bölüm; çalışmanın hipotezindeki ana kavramlardan biri olan örtülü operasyonların incelenmesi, tartışılması, yarattığı şiddet ve makul inkâr edilebilirlik düzeyleri bakımından örtülü operasyon türlerinin incelenmesi ve örtülü operasyonların devletler için neden bir seçenek olduğunun tartışılması bakımından önemlidir.

3.1. Örtülü Operasyonun Tanımlanması

Örtülü operasyonlar, devletlerin dış politika hedeflerini gerçekleştirme aracı olarak yüzlerce yıldır var olan bir müdahale opsiyonudur.[122] Bu opsiyon, 2. Dünya Savaşı'nın ardından istihbarat örgütlerinin kurumsallaşmasından ve profesyonelleşmesinden bu yana, olayları makul bir şekilde inkâr ederek etkileme faaliyeti olarak Amerikan literatüründe "örtülü eylemler (covert actions)"[123], Sovyet literatüründe ise "aktif önlemler (aktivnyye meropriyatiya/ активные мероприятия)"[124] olarak adlandırılmaya başlanmıştır. İstihbarat, politikayı bilgilendirme aracı olduğu kadar politikanın yürütülmesi için de yardımcı bir unsurdur.[125] Bu bağlamda düşünüldüğünde, politikayı yürütme unsuru olarak örtülü operasyonları, diğer istihbarat disiplinlerinden ayıran en önemli özelliği bir etki yaratmayı amaçlamasıdır. Michael Warner, örtülü operasyonları *"güven ve sadakat kalıplarını değiştirmek için çatışmanın marjlarında kullanılan savaş ve diplomasinin gizli tamamlayıcısı"* olarak tanımlamıştır.[126] Elizabeth Anderson ise örtülü operasyonun "*bir hükümetin çıkarlarını ve dış politika hedeflerini, açıkça izlenemeyecek şekilde yahut olmaması gereken bir şeyi başarmak amacıyla gizli araçlar kullanarak ilerletmenin ayrılmaz bir*

---

[122] Cormac, Aldrich, *a.g.e.*, 277.

[123] *a.g.e.*, 277.

[124] Abram Shulsky, "What Is Covert Action?", *Silent Warfare: Understanding the World of Intelligence*, 2. bs (New York: Brassey's US, 1993), 76.

[125] Len Scott, Peter Jackson, "The Study of Intelligence in Theory and Practice", *Intelligence and National Security*, C.19, S.2 (2004): 142. DOI: 10.1080/0268452042000302930.

[126] Michael Warner, "A Matter of Trust: Covert Action Reconsidered", *Studies in Intelligence*, C. 63, S. 4 (2019): 33- 35.

unsuru" olduğunu ifade etmiştir.[127] Her iki ifadedeki dış politika vurgusu dikkate değerdir çünkü devletlerin dış politikalarıyla ilgili gerek konjonktürel gerekse stratejik hedeflerini savaşlardan kaçındıkları her durumda diplomasi işlevsel bir seçenek olmayabilir.

RF eski Genel Kurmay Başkanı general Valery Gerasimov'un 2013 yılında yayımladığı "Bilimin Değeri Öngörüdedir (The Value of Science is in the Foresight)" başlıklı makalesinde, savaşın kurallarının değiştiğini, siyasi ve stratejik hedeflere ulaşmada askerî olmayan enstrümanların rolünün arttığını hatta çoğu durumda silahların etki kabiliyetini aştığını ifade etmiştir.[128] Garasimov burada daha çok asimetrik savaşları kastetmiştir ancak bu tanım örtülü operasyonlarla da uyumludur. Garasimov ayrıca, stratejik ve operasyonel seviyede büyük kuvvet oluşumlarının cepheden angaje edilmesinin artık geçmişte kalma eğiliminde olduğunu, hasım odağa karşı uzun mesafeli ve temassız eylemlerin hedeflere ulaşmanın ana yolu hâline geldiğini ifade etmiştir.[129]

3.2. Makul İnkâr Edilebilirliği Destekleyen Caydırıcı Unsurlar

Devletler, stratejik hedeflerine ulaşmak için iç ve dış politikalar belirler ve yürütürler. Jonathan Wilkenfeld dış politikayı, *"Egemen devletlerin kendi sınırlarının dışında bir koşulu değiştirmek veya yaratmak amacıyla başlattıkları resmî eylemler"* olarak tanımlamıştır.[130] Devletlerin irredantist, hegemonik yahut emperyalist politikaları ve sınırları ötesinde güttükleri emelleri zaman zaman başka devletlerin politikalarıyla örtüşür yahut çelişir. Bu örtüşmeler ittifakları, çelişmeler ise hasımlıkları meydana getirebilmektedir. Devletlerin kendi politikalarını gerçekleştirmek için diplomasi ve silah kullanımı gibi araçları vardır fakat diplomasi her zaman fayda

---

[127] Elizabeth Anderson, "The Security Dilemma and Covert Action: The Truman Years*", International Journal of Intelligence and CounterIntelligence*, C.11, S.4 (1998): 404. DOI:10.1080/08850609808435385.

[128] Valery Gerasimov, "The Value of Science is in the Foresight", *Military Review*, (2016): 24.

[129] *a.g.e.*, 24.

[130] Jonathan Wilkenfeld ve diğ., *Foreign Policy Behaviour: The Interstate Behaviour Analysis Model*, (Beverly Hills: Sage Publications, 1980): 22'den aktaran M. Fatih Tayfur, "Main Approaches to the Study of Foreign Policy: A Review", *METU Studies in Development*, C. 21, S. 1 (1994): 115.

sağlamayabilmekte ve silah kullanımı, yaratacağı ekonomik, sosyal ve hukuki maliyetler dolayısıyla caydırıcı olabilmektedirler.

Örtülü operasyonların neden caydırıcılık ile motive edilen bir tercih unsuru olduğunu, sponsor kimliğini gizlemeye yönelik atfedilen *"makul inkâr edilebilirlik"* kavramını tanımlayarak başlamak yararlı olacaktır. Mark Lowenthal makul inkâr edilebilirlik kavramını, eylemin kökeninin neredeyse tamamen gizli kalmasına bağlı olarak yorumlamıştır.[131] Michael Warner ise makul inkâr edilebilirliği, eylemin etkili olabilmesi için, en azından görevin başarıldığı noktaya kadar, askerî planlamacıların ve komutanların savaş zamanı operasyonel gizliliğine benzer bir gizlilik içinde yürütülmesi gereği perspektifinde yorumlamıştır.[132]

Örtülü operasyonların tanımı gereği örtük/ gizli icrasının ve sponsor kimliğine yönelik inkâr edilebilirlik maksadı gütmenin caydırıcılık bakımından önemli sebepleri vardır. Mustafa Kibaroğlu, caydırıcılığı *"rakibin zarar verebilecek bir davranışı sergilemesinden vazgeçmesini sağlayacak tutum ve davranışı açık ve kararlı bir biçimde ortaya koymak"* olarak tanımlamıştır.[133] Devletlerin örtülü operasyonlara başvurmalarının bir sebebi, eylemler aleni olarak gerçekleştirildiği takdirde gerek iç hukuk gerekse uluslararası hukuk kuralları bakımından sorumlu hâle gelme ihtimalinin yarattığı caydırıcılıktır. Diğer bir caydırıcı unsur ise, uluslararası ilişkiler terminolojisinde *"mütekabiliyet esası"* olarak bilinen karşılıklılık ilkesinden doğacak eylemleri yüklenme ihtimalidir.

Makul inkâr edilebilirlik, hukuki perspektifte çoğunlukla kanıt eksikliğine dikkat çeken bir terimdir.[134] Masumiyet karinesi (suç ispat edilene kadar masum sayılma ilkesi) bakımından değerlendirildiğinde, söz konusu kavramın "gizlilik" nosyonundan büyük ölçüde güç aldığı görülmektedir. Bu noktada, örtülü operasyonlara atfedilen politik, askerî ve ekonomik eylemlerin açıkça gerçekleştirildiği birçok noktada,

---

[131] Mark M. Lowenthal, "Covert Action", *Intelligence : From Secrets to Policy*, 8. bs (Thousand Oaks: CQ Press, 2020): 386. ISBN 9781544358376 (epub).

[132] Warner, "A Matter of Trust: Covert Action Reconsidered", 36.

[133] Mustafa Kibaroğlu, "11 Eylül Ardından Strateji, Tehdit ve Caydırıcılık", *Foreign Policy*, (2002): 1. http://www.mustafakibaroglu.com/sitebuildercontent/sitebuilderfiles/Kibaroglu-11EylulArdndanStratejiTehditCaydiricilik-22dec01.pdf.

[134] The Law Dictionary, "Plausible Deniability Definition, Examples and Laws", *Criminal Law*, https://thelawdictionary.org/article/plausible-deniability/. [Erişim Tarihi: 10.12.2022].

devletler uluslararası bir hukuki yaptırım ile karşı karşıya kalabileceklerdir. Ayrıca, söz konusu eylemleri gerçekleştirmesi durumunda hükümetler kendi ülkelerinin iç hukuki yaptırımları ile de karşı karşıya kalabilecekler ve halklarının nazarında itibar kaybına uğrayabileceklerdir. Söz konusu uygulamalar, bir ülkede siyasal seçimlere etki etmeyi ifade eden dış kaynaklı seçim müdahalelerini ve askerî darbeleri, ekonomik örtülü operasyonlar ile muhatap devleti zayıflatmayı yahut ekonomik kapasitesine zarar vermeyi ve paramiliter örtülü operasyonlar ise hedef ülkenin muhalif silahlı gruplarının askerî teçhizat ile donatılması ve eğitilmesini içeren operasyonları ifade etmektedir. Bu eylemlerin şiddet oranı ve meşru neden olmaksızın ortaya çıkması yahut meşru neden olsa dahi hukuk dışı uygulamalar ile gerçekleştirilmesi, devletler açısından "haksız fiil" kapsamına girebilecek ve uluslararası hukuki sorumluluğu yönüyle devleti hukuki yaptırımlar ile karşı karşıya getirebilecektir. Bu bölümde, örtülü operasyonların aleni gerçekleştirilmesi durumunda ihlal edebileceği birçok mevzuat ve ilke içerisinden, çalışmanın odaklandığı "dış kaynaklı seçim müdahaleleri" konusunu ilgilendiren hususlar incelenecektir.

2001 yılının Kasım ayında Birleşmiş Milletler Uluslararası Hukuk Komisyonu tarafından kabul edilen *"Devletin Haksız Fiilden Kaynaklanan Sorumluluğuna İlişkin Taslak Metin"*, devletleri uluslararası hukukun bir süjesi olarak kabul etmiş ve bir davranışın uluslararası hukuka aykırı bir fiil olarak nitelendirilebilmesi için, öncelikle devlete atfedilebilir olmasını şart koşmuştur.[135] Taslak Metin 26'nın 5. Maddesinde, *"saldırganlık, soykırım, kölelik, ırk ayrımcılığı, insanlığa karşı suçlar ve işkence ve kendi kaderini tayin hakkı yasakları"* emredici normlar olarak vurgulanmıştır.[136] 26 Haziran 1945 tarihinde imzalanan ve 24 Ekim 1945'te yürürlüğe giren Birleşmiş Milletler Antlaşması Madde: 1.2 ve Madde: 55'te de, "halkların kendi kaderini tayin hakkı"na atıfta bulunulmuştur.[137] Kendi kaderini tayin hakkı (öz belirtim, self

---

[135] International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts", Kasım 2001, Ek No. 10 (A/56/10), bölüm. 2, md. 5, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. [Erişim Tarihi: 28.12.2022].

[136] *a.g.e.*, bölüm. 26, md. 5, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. [Erişim Tarihi: 28.12.2022].

[137] Birleşmiş Milletler Antlaşması, 26 Haziran 1945, San Francisco, https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf. [Erişim Tarihi: 28.12.2022].

determinasyon/ self- determination), en temel anlamıyla *"kendini tanımlayan ulusların, kendi devletleri üzerinde kontrol sahibi olması gerektiği"* anlamına gelmektedir.[138] Bir ülkenin demokratik seçimlerine çeşitli şekillerde müdahale etmek, (oy sayımlarına hile karıştırmak, seçim esnasında seçim kanunlarına aykırı uygulamaları desteklemek gibi) o ülke halkının iradesi dışında bir sonuç doğuracaktır. Dolayısıyla bir ülkedeki demokratik seçimlere müdahale etmek (dış kaynaklı seçim müdahalesi), ulusların kendi kaderini tayin hakkına aykırılık teşkil etmektedir. Uluslararası hukukun bir diğer temel ilkesi ise *"devlet egemenliği ilkesi"*dir.[139] Devlet egemenliği, en temel anlamıyla, bir devletin coğrafi sınırları içerisindeki alan (siyasi coğrafya) ve o alanda yaşayan nüfus üzerinde münhasır yetkisidir.[140] Özetle, devletin üzerinde egemenlik sahibi olduğu tüm faaliyetleri kontrol edebilmesini ifade etmektedir.[141] Bu bağlamda, bir devletin sınırları içerisinde askerî darbenin yahut isyan ve ayaklanmaların desteklenmesi, *"devlet egemenliği"* ilkesine aykırıdır. Kapsamı bakımından bu tür örtülü operasyonlar, uluslararası hukukun ve Birleşmiş Milletler Şartı'nın, bir başka devletin "*iç işlerine karışmama"* ilkesine de aykırıdır."[142]

Askerî teorisyen Carl von Clausewitz, savaşları başka araçların da eklenmesiyle siyasi ilişkilerin basit bir devamı olarak yorumlamış ve askerî olayları sonraki barışa kadar devam eden siyasi hatlar olarak nitelendirmiştir.[143] Fakat ABD'nin, 2. Dünya Savaşı sonlarında, Ağustos 1945'te, Hiroşima ve Nagazaki'ye atom bombalarıyla gerçekleştirdiği saldırılar, kitle imha silahlarının yıkım gücünün, savaşlara yüklenen anlamın gözden geçirilmesi gerekliliğini doğurmuştur. 1952'de hidrojen bombasının ilk kez test edilmesi, 1961'de Sovyetler Birliği'nin gerçekleştirdiği ve Dünya üzerinde insan eliyle gerçekleştirilen en büyük patlama sayılan 60 megatonluk nükleer denemenin yarı gücünde gerçekleştirilen bir deneme olduğu halde 2. Dünya

---

[138] Neil MacFarlane, Natalie Sabanadze, "Sovereignty and Self-Determination: Where Are We?" *International Journal* C.68, S.4 (2013): 611. http://www.jstor.org/stable/24709362.

[139] Chris McGrath, "Principles of Sovereignty Under International Law", (10 Aralık 2018): 1, http://envlaw.com.au/wp-content/uploads/handout_sovereignty.pdf. [Erişim Tarihi: 22.12.2022]. (makale sayfa aralıkları: 1-3).

[140] MacFarlane, Sabanadze, *a.g.e.*, 611.

[141] Chris McGrath, *a.g.e.*, 1.

[142] Daugherty, "The Role of Covert Action in Intelligence and Foreign Policy", 18.

[143] Carl Von Clausewitz, "War Is an Instrument of Policy", *On War*, çev. Michael Howard, Peter Paret (New York: Oxford University Press, 2007), 252.

Savaşı'nda kullanılan patlayıcı güç toplamının 20 katı güce sahip olduğunun anlaşılması[144], nükleer silahların ortaya çıkardığı yok edicilik boyutunu ortaya koymuştur. Joseph S. Nye ve David A. Welch, nükleer silahlar için "*bu silahlar fazla güçlü, dolayısıyla anlamlı bir siyasi hedefe varmak için fazla orantısızdır"*[145] ifadeleriyle, Clausewitz'in "politikanın bir aracı" olarak tanımladığı savaşların, nükleer silahların var olması ile artık başka bir boyuta varabileceğini vurgulamışlardır.

Elbette örtülü operasyonların miladı Hiroşima ve Nagazaki'ye gerçekleştirilen atom bombası saldırıları değildir. 2. Dünya Savaşı boyunca ve daha öncesinde de örtülü operasyonlar başvurulan araçlar olmuşlardır. Fakat nükleer caydırıcılık artık bir savaşa girme kararının eskisine göre daha ciddiyetle düşünülerek alınması gerektiğini ortaya çıkarmıştır. Nye ve Welch'in bahsettiği orantısızlığın sebebi, nükleer silahların yok etme kabiliyetidir. Nitekim Nye ve Welch, nükleer savaşın birkaç saat içinde bitebildiği koşullarda artık tedricen seferberlik ve savaşa hazırlık imkânının olmadığını ifade etmişler ve ABD ile Sovyetler Birliği'nin nükleer bir savaşın yaratacağı yıkımı göze alamadıkları için, zaman zaman nüfuzlarını genişletmeyi sürdürseler yahut vekâlet savaşlarına başvursalar da doğrudan bir konvansiyonel savaştan da kaçındıklarını vurgulamışlardır.[146] Mustafa Kibaroğlu, Hiroşima ve Nagazaki'ye atılan ilk atom bombasının ardından 1960'lı yıllarda özellikle ABD ve Sovyetler Birliği tarafından daha da geliştirilen nükleer silahların gerek sayısı ve etkinliğinin gerekse korunaklı ortamlarda muhafaza ediliyor olmasının, bir tarafın toprakları ciddi bir nükleer saldırıya maruz kalsa dahi, nükleer silah sistemleri saldırının etkilerinden önemli ölçüde etkilenmeyeceğinden, nükleer bir çatışma durumunda kazanan bir tarafın olma ihtimalini ortadan kaldırdığını ifade etmiştir.[147] Olası bir nükleer savaşta kazananın olmayacağı kabulüne *"dehşet dengesi"* denilmektedir.[148] Ancak nükleer çatışmalardan kaçınılıyor olma durumu bazı durumlarda nükleer güç kullanma tehditlerinin yükselmesine engel olmamıştır. Örnek

---

[144] Joseph S. Nye, David A. Welch, "Nükleer Silahların Rolü: Fizik ve Politika", Küresel Çatışmayı ve İşbirliğini Anlamak, çev. Renan Akman (Beyoğlu: Türkiye İş Bankası ve Kültür Yayınları, 2017), 248.

[145] *a.g.e.*, 248.

[146] *a.g.e.*, 250.

[147] Mustafa Kibaroğlu, "Amerikan Ulusal Füze Savunma Sistemi", *Avrasya Dosyası - Amerika Özel Sayısı*, C.6, S.3 (2000): 97.

[148] *a.g.e.*, 98.

olarak, “Soğuk Savaş Sonrası Gelişen Ulusal Güvenlik Sorunları" konulu Rus- ABD konferansında bir Rus teorisyenin olası enformasyon savaşına karşın gösterilecek mütekabiliyete dair şu ifadeleri, konunun anlaşılması bakımından dikkat çekicidir:

> *“Askeri bir bakış açısından, Rusya'ya veya silahlı kuvvetlerine karşı enformasyon savaşı araçlarının kullanılması, bir kayıp olsun ya da olmasın, kategorik olarak bir çatışmanın askeri olmayan bir aşaması olarak kabul edilmeyecektir. Bir düşman tarafından stratejik enformasyon savaşı araçlarının kullanılmasının, ekonomik veya devlet komuta- kontrol sistemleri veya silahlı kuvvetlerin savaş potansiyeli üzerindeki olası felaket sonuçlarını göz önünde bulundurarak; Rusya, nükleer silahları önce enformasyon savaşının araç ve güçlerine karşı, sonra da saldırgan devletin kendisine karşı kullanma hakkını saklı tutar.”*[149]

1995 yılında yapılan bu konuşma, nükleer saldırıya yönelik tehdit ifadelerinden yalnızca biridir. Devletler her ne kadar nükleer caydırıcılık nedeniyle diplomasi yollarını zorluyor olsalar da diplomasi her zaman bir sonuç vermemektedir. Diplomasinin yarar sağlamadığı fakat savaştan da kaçınılan bir ortamda, dış politika hedeflerini gerçekleştirmek için örtülü operasyonlar oldukça kullanışlı araçlar olacaktır. Sponsor kimliğini gizlemeye yönelik hassas yönü, bu gizlilik başarıyla korunduğunda, mütekabiliyet riski doğurmadan politika hedeflerini gerçekleştirme yolunda örtülü operasyonları özel bir konuma getirmektedir.

3.3. Örtülü Operasyon Türleri

Örtülü operasyonlar, yabancı tutumlarının ve koşullarının gizli olarak etkilenmesine yönelik gizlice teknik yardım sağlamak, suikast veya bir darbeyi desteklemek yahut kışkırtmak gibi çeşitli yöntemler yelpazesini kapsar.[150] Abram Shulsky, örtülü operasyonları, yabancı bir hükümetin yahut yabancı bir toplumun unsurlarının algılarını siyasi, ekonomik yahut askerî yönden etkilemek perspektifinden değerlendirmiştir.[151] William J. Daugherty ise daha çok CIA ve ABD eylem tarzı

---

[149] V. I. Tsymbal, "Kontseptsiya `Informatsionnoy voyny'" (Concept of Information Warfare), speech given at the Russian-US conference on "Evolving Post-Cold War National Security Issues," Moscow 12-14 September 1995, p. 7.’den aktaran, Timothy L. Thomas, “Deterring Information Warfare: A New Strategic Challenge”, *The US Army War College Quarterly: Parameters*, C, .S.26 (1996): 1.

[150] Abram Shulsky, Gary J. Schmitt, “Types and Examples of Covert Action”, *Silent Warfare: Understanding the World of Intelligence*, 2. bs (New York: Brassey’s US, 1993), 77.

[151] Shulsky, Smith, “Types and Examples of Covert Action”, 79.

perspektifinden yazdığı *"The Role of Covert Action"* başlıklı yazısında, bu etki yelpazesini, bir hükümet yahut hükümetin üst düzey lider kadrosu, bir ulusun tamamı yahut bir bölümü, bir terör örgütü veya uyuşturucu karteli gibi uluslar üstü (supranational) gruplara kadar genişletmiştir.[152]

Mark Lowenthal, örtülü operasyonları şiddetin boyutu ve makul inkâr edilebilirlik düzeyi bakımından değerlendirdiği "örtülü eylem merdiveni" ile açıklamıştır.[153]



Şekil 3.1: Mark Lowenthal Örtülü Eylem Merdiveni.

(Yazar tarafından Türkçeleştirilmiştir). [154]

Lowenthal'ın örtülü eylem merdivenine göre, şiddetin boyutu ile makul inkâr edilebilirlik ters orantılıdır. Merdivenin en üst basamağındaki paramiliter operasyonlar şiddet bakımından en üst düzeydeyken, makul inkâr edilebilirlik bakımından en zayıf konumdadır.

Örtülü eylem merdiveninden de anlaşılacağı üzere, Lowenthal sabotaj ve propagandayı da bir örtülü operasyon türü olarak ele almıştır. Ancak sabotaj ve propaganda, hem paramiliter, hem ekonomik hem siyasi örtülü operasyonlarda

[152] William J. Daugherty, "The Role of Covert Action in Intelligence and Foreign Policy", *Handbook of Intelligence Studies*, ed. Loch K. Johnson, (Oxon: Loch K Johnson, 2007), 280.

[153] Lowenthal, *a.g.e.*, 381.

[154] *a.g.e.*, 381.

kullanılabilecek, doğurduğu sonuç açısından ekonomik, siyasi yahut askerî neticeler yaratabilecek bir araçtır. Bu sebeple bu çalışmada propaganda, örtülü operasyon türü olarak değil, örtülü operasyon aracı olarak ele alınmıştır.

William J. Daugherty, örtülü operasyonu *"diplomasi, ticari teşvik ya da yaptırımlar ve dış yardım gibi açık önlemler (overt measures) ile askerî güç kullanımı arasında bir orta yol"* olarak tanımlamıştır.[155] Daugherty, örtülü operasyonlarda maksadı "bir davranış değişikliği yaratmak" olarak vurgulamış ve bu sebeple etkilediği kitlenin en azından bir kısmı için mutlaka "görünür" olması gerektiğini, aksi hâlde tamamen gizlenen eylemin bir etki yaratmasının imkânsız olduğunu değerlendirmiştir.[156]

Makul inkâr edilebilirlik (dolayısıyla gizlilik) ve etki bağlamında açıklanan örtülü operasyon türleri, bu çalışmada paramiliter, ekonomik ve siyasi örtülü operasyonlar başlıkları altında incelenecektir.

3.3.1. Paramiliter Örtülü Operasyonlar

Paramiliter örtülü operasyonlar, teknik olarak operatör devletin kendi askerinin alenen muharip birimlerinde kullanılmaksızın, silahlı grupların düşmanlarına yönelik güçlü bir askerî kapasite ve saldırı kabiliyeti elde edebilmesi maksadıyla eğitilmesini ve askerî teçhizatlar ile donatılmasını içeren örtülü eylem türleridir.[157] Lowenthal'in örtülü eylem merdivenine göre paramiliter örtülü operasyonlar, yarattığı şiddet bakımından en üst seviyede ve dolayısıyla makul inkâr edilebilirlik bakımından en zayıf örtülü operasyon türüdür. William J. Daugherty de, paramiliter örtülü operasyonların üç geleneksel kategori içerisinde en az yararlanılan programlar olduğunu belirtmiş ve kapsamlarının sınırlılığı dolayısıyla kamuoyunun nadiren dikkatini çektiğini ifade etmiştir.[158] Paramiliter örtülü operasyonları açık bir savaştan ayıran en önemli unsur, devletin silahlı kuvvetleri tarafından bir savaş ilanıyla yapılmaksızın, çoğu zaman devletin gizli servisi tarafından organize edilmesi ve en önemlisi ülkenin silahlı kuvvetler personelinin doğrudan yahut açıkça çatışmalara

---

[155] Daugherty, "The Role of Covert Action in Intelligence and Foreign Policy", *a.g.e.,* 280.

[156] *a.g.e.,* 280.

[157] Lowenthal, *a.g.e.,* 381.

[158] Daugherty, "The Discipline of Covert Action", 84.

dâhil edilmemesidir. Paramiliter örtülü operasyonlar genellikle bir gerilla örgütünü askerî teçhizatla donatma ve eğitme gibi yöntemleri içermektedir. Örnek olarak CIA, Sovyetler Birliği'nin Doğu Avrupa ve diğer bölgelerdeki yayılmacılığına bir set çekebilmek maksadıyla söz konusu bölgelerde "düşman içine bırakılan (stay- behind)" gerilla kuvvetlerini Sovyet ordularına yönelik sabotaj operasyonları düzenlemeleri maksadıyla silahlandırmıştır.[159]

3.3.2. Ekonomik Örtülü Operasyonlar

Ekonomik örtülü operasyonlar, bir hasım devletin yahut devlet dışı aktörün ekonomik kaynaklarını baltalamak ve dost ve müttefik devleti yahut devlet dışı aktörü ekonomik kaynakları yönünden güçlendirmek amacıyla sübvansiyonları içeren örtülü operasyon türüdür. Bu ekonomik müdahaleler sahte para basmadan ekonomi ve ticarete yön verme, rakiplerin piyasaya girişini engellemeye çalışmaya kadar çeşitli yöntemler ile gerçekleştirilir.[160] Loch K. Johnson, CIA'nın ekonomik örtülü operasyonlarını, hedef ülkelerde enflasyonist baskıları tetiklemek için sahte döviz bastığı, sahte gıda kuponları ve banka poliçeleri ürettiği, hasım tarafın ekonomisinin can damarı sayılabilecek tarım ürünlerinin fiyatlarını düşürdüğü faaliyetleri ile örneklendirmiştir.[161]

ABD'de 1948 yılında yayınlanan NSC 10/2 no'lu kararnamede, örtülü operasyonların;

> *"Propaganda, ekonomik savaş, sabotaj da dâhil olmak üzere önleyici doğrudan eylem, sabotaj önleme, yıkım ve tahliye önlemleri; yeraltı direniş hareketlerine, gerillalara ve mülteci kurtuluş gruplarına yardım ve özgür dünyanın tehdit altındaki ülkelerinde yerli anti-komünist unsurların desteklenmesi dâhil olmak üzere düşman devletlere karşı yıkım"*[162]

faaliyetlerini içereceğine dair bir madde yer almaktadır. Lowenthal, yiyecek ve emtianın mevcudiyeti, fiyat istikrarı, temel ihtiyaçların karşılanmasındaki kolaylık ya da zorluk durumunun ister demokratik ister totaliter olsun, her siyasi liderin endişesi

---

[159] Chris Whipple, *The Spy Masters: How the CIA Directors Shape History and the Future* (New York: Scribner, 2020): 13'den aktaran, Loch. K. Johnson, "The Forms of Covert Action", *The Third Option: Covert Action and American Foreign Policy* (New York: Oxford University Press, 2022): 35.

[160] Kaan Kutlu Ataç, "İstihbarat, Casusluk, Karşı Casusluk, Örtülü Operasyonlar ve Güvenlik", *Güvenlik Yazıları Serisi*, S. 45 (2019): 8. DOI: 10.13140/RG.2.2.22313.95849.

[161] Johnson, "The Forms of Covert Action", 33.

[162] Office of the Historian, "Document 292: National Security Council Directive on Office of Special Projects (NSC 10/2, Md.5)". *U.S. Department of State* (Washington, 18.05.1948). https://history.state.gov/historicaldocuments/frus1945-50Intel/d292. [Erişim Tarihi: 13.12.2022].

olduğunu vurgulamıştır.[163] Ekonomik koşullar, bir ülkenin siyasi istikrarını ve halkın hükümete olan desteğini de etkileyecektir. Propaganda ile bir kıtlık endişesi yaratmak da ülke halkının ekonomi ile ilgili endişelerini tetikleyebilecektir. Aynı zamanda sabotaj faaliyetleriyle hayati mahsulleri yok etmek, ülkenin parasal sistemine olan inancı sarsmak, veya sahte para basarak ülkede enflasyonun yükselmesini tetiklemek gibi daha doğrudan teknikler de ekonomik örtülü operasyon yöntemlerindendir ve ABD, bu tür girişimleri hasım hükümetlere karşı kullanma eğiliminde olmuştur.[164]

3.3.3. Siyasi Örtülü Operasyonlar

Siyasi örtülü operasyonlar en temel tanımı ile hasım bir hükümeti askerî darbe yahut iç savaş ile devirmek, siyasi seçimlerini manipüle etmek gibi yöntemleri ifade etmektedir.[165] Propaganda, siyasi örtülü operasyonların en temel aracıdır. Ayrıca bir hükümeti baskı altında tutmak amacıyla çeşitli istihbarat toplama faaliyetleri neticesinde elde edilen hayati veri ve enformasyonlar üzerinden şantaj yapmayı, rüşvet ile kontrol altında tutmayı yahut kendi politikalarıyla örtüşecek politikalar güdecek olan siyasi liderleri yönetime getirme çalışmalarını içerebilir. ABD perspektifinde siyasi örtülü operasyon, diğer ülkelerdeki batı yanlısı bürokrat ve politikacılara finansal yardım, seçim kampanyası destekleri gibi faaliyetleri içerebilmektedir.[166]

Dış kaynaklı seçim müdahaleleri ve askerî darbeler, siyasi örtülü operasyon türleridir. Siyasi örtülü operasyonlar, bir ülkenin millî menfaatleri doğrultusunda takip edeceği dış politika hedeflerini akamete uğratmanın en görünmez yollarından biridir. Lowenthal'ın örtülü eylem merdiveninde de siyasi örtülü opersayonlar ikinci sırada yer almaktadır. Burada en alt basamaktaki propagandanın bir örtülü operasyon türü değil, örtülü operasyon aracı olduğu dikkate alındığında siyasi örtülü operasyonlar, şiddet seviyesi bakımından en alt basamakta ve makul inkâr edilebilirlik düzeyi en üst seviyede olarak değerlendirilebilecektir. Lowenthal, askerî darbeleri paramiliter örtülü operasyonların bir alt basamağında konumlandırmıştır ancak paramiliter örtülü

---

[163] Lowenthal, *a.g.e*., 380.

[164] *a.g.e*., 380.

[165] Lindsey A. O'Rourke, "The False Promise of Covert Regime Change", *Convert Regime Change : America's Secret Cold War* (Ithaca: Cornell University Press, 2018), 1.

[166] Loch K. Johnson, "Introduction", *Handbook of Intelligence Studies*, ed. Loch K. Johnson (Oxon: Routledge, 2007): 11. e-kitap ISBN 0-203-08932-4. (bölüm sayfa aralıkları: 1-14).

operasyonlar, dış kaynaklı seçim müdahalelerine nispetle daha doğrudan bir girişim olsalar da, gizlilik süreçleri iyi yönetildiğinde makul inkâr edilebilirlik bakımından paramiliter örtülü operasyonlar kadar yahut ona yakın bir seviyede dezavantajlı olmayabilirler. Bununla birlikte askerî darbeler ile gerçekleştirilen rejim değişiklikleri halkın üzerinde yarattığı baskı ve korkunun gevşemesi durumunda çok uzun ömürlü olmayabilmektedirler. Ayrıca askerî darbeler meşruiyet bakımından bir dış kaynaklı seçim müdahalesinden daha görünür aksaklıklara sahiptir.

3.4. Örtülü Operasyonlarda Propagandanın Yeri ve Propaganda Türleri

Örtülü operasyonları gerçekleştirmek maksadıyla aynı anda bir ya da birden fazla yöntem kullanılabilmektedir. Bu noktada, tanımındaki gizlilik ve makul inkâr edilebilirliği destekleyecek araçlar ile gerçekleştirilen örtülü operasyonlar hem hedefin söz konusu çalışmaları fark etmesini yahut sezgisel olarak fark etse dahi karşı koymasını güçleştirecek hem de iyi bir planlama ile gerçekleştirildiği takdirde operasyonun başarı olasılığını arttıracaktır. Elbette örtülü operasyonların çok çeşitli yöntemleri vardır fakat bu bölümde çalışmanın temel odağı bakımından propaganda konusu incelenecektir.

Algı yönetiminin bir bileşeni olan propaganda, belirli doktrinlerin, bakış açılarının veya mesajların seçilen bir kitleye sistematik olarak yayılmasıdır.[167] Propaganda, hedeflenen belirli bir kişinin, grubun yahut toplumun, görüş ve tutumlarını kasten etkilemeyi ve manipüle etmeyi amaçlayan yazılı ve sözlü oluşum olarak tanımlanabilir.[168] Devletler, uluslararası örgütler, sivil toplum kuruluşları, siyasi partiler ve terör örgütleri, propagandayı stratejik hedeflerine giden yolda mevzî kazanma aracı olarak kullanmaktadırlar. Lowenthal, propagandayı *"belirli bir siyasi sonuç gözeterek oluşturulmuş eski bir bilgi yayma tekniği"* olarak tanımlamıştır.[169] Propaganda, bir ideolojiyi yayma yahut karalama bakımından akademisyenler, siyasetçiler, sanatçılar, gazeteciler, edebiyatçılar, şairler ve kanaat önderleri

---

[167] Daugherty, "The Discipline of Covert Action", 72.

[168] Richard H. Shultz, Roy Godson, "Overt Propaganda and Cover Political Techniques: Distinctions and Definitions", *Dezinformatsia: Active Measures in Soviet Strategy*, (Virginia: Pergamon Brassey's International Defense Publishers, 1984), 34.

[169] Loventhal, a.g.e., 380.

tarafından, bilinçli yahut bilinçsiz olarak kullanılan bir yöntemdir. Gazeteler, broşürler, kitaplar, radyolar, TV kanalları ve sosyal medya platformları propagandanın en sık kullanılan zeminleridir. Köşe yazıları, seminer ve söyleşiler, filmler, diziler, tiyatrolar, müzik, resimler, şiirler, videolar ise propagandanın en sık kullanılan araçlarıdır.

Daniel Lerner, *"Psychological Warfare Against Nazi Germany"* adlı kitabında; politikanın diplomasi, propaganda, yaptırımlar ve savaş olmak üzere dört ana araçtan yararlandığını ifade eder ve politika gerçekleştirme sürecini mekanizma- araç ve teknik olarak şöyle bir şemada tasniflendirir;[170]

Mekanizma	*Araç*	*Teknik*
Diplomasi	*Sözleşmeler*	*Müzakereler*
Propaganda	*Semboller*	*İkna*
Yaptırımlar	*Tedarik*	*Yoksun bırakma*
Savaş	*Şiddet*	*Zorlama*

Daugherty, propagandanın örtülü operasyonun en az görünür, en az tehditkâr ve en incelikli olan metodolojisi olduğunu ancak etkili olması için en fazla süreyi gerektirdiğini ifade etmiştir.[171]

Propaganda, farklı düzlemleri, kaynakları, teknikleri, seviyeleri ve amaçları barındıran oldukça kapsamlı bir alandır. Bu çalışmada, konusuna, kaynağına ve yöntemine göre propaganda türleri incelenecektir.

---

[170] Daniel Lerner, "Policy and Propaganda In World War II", *Psychological Warfare Against Nazi Germany: The Sykewar Campaign, D-Day to VE- Day*, (Cambridge: MIT Press, 1971), 2. ISBN: 9780262620192.

[171] Daugherty, "The Discipline of Covert Action", 71.

• Konusuna göre propaganda türleri;

- Siyasi Propaganda: Propaganda kavramı yaygın olarak siyasi propaganda yönünden tanımlanmaktadır. Tarihin en eski çağlarından bu yana başvurulan propagandanın, İkinci Dünya Savaşı ve Soğuk Savaş yıllarında gerçekleşmiş çok sayıda örneği mevcuttur. Örnek vermek gerekirse, Nazi Almanyası döneminde Halkı Aydınlatma ve Propaganda Bakanı olarak görev yapmış olan Joseph Goebbels, propaganda söz konusu olduğunda literatürde adı sıklıkla zikredilen propagandistlerdendir.[172]
- Ekonomik Propaganda: Ticari amaçla yapılan reklamlar ve ürün tanıtımları bu propaganda türünün örnekleridir.
- Dini Propaganda: Propagandanın en kadim türlerinden biri dini propagandalardır. Bazı dinlerdeki "tebliğ" inancının paravan olarak kullanılarak siyasi güç elde etmek maksadıyla yapılan misyonerlik faaliyetleri, dini propagandaların çeşitli örneklerini oluştururlar. Bu örneklerden biri; Papa Gregory XII'nin (1572-85), Katolik doktrinlerini Hıristiyan olmayan topraklarda yaymak için üç kardinalden oluşan bir propaganda komisyonu kurması ve 1627'de Papa Urban VIII'in, misyonerler yetiştirmek için Pontificio Collegio Urbano de Propaganda Fide'yi kurmasıdır.[173]
- Askeri Propaganda: Bir ülkenin ordusunun gücünü yansıtmak, halkının orduya bağlılığını ve sempatisini tesis etmek yahut yaptığı sınır ötesi operasyonlarda sınır ötesindeki toplumun sempatisini kazanmak için yaptığı propagandadır. Fırat Kalkanı Operasyonu sırasında Türk askerinin küçük bir çocuğa çikolata verirken çektiği videonun paylaşılması konuya bir örnek teşkil etmektedir.[174]

• Kaynağına göre propaganda türleri;

Hedef kitlenin kaynağından ne ölçüde haberdar olacağına ve yayılan propagandanın doğruluk derecesine göre; kara propaganda, gri propaganda ve beyaz propaganda olmak üzere üç gruba ayrılır.

---

[172] Leonard W. Doob, "Goebbels' Principles of Propaganda", *The Public Opinion Quarterly*, C.14, S.3 (1950): 419.

[173] Vatican, "The Congregation For The Evangelization Of Peoples", Https://Www.Vatican.Va/Roman_Curia/Congregations/Cevang/Documents/Rc_Con_Cevang_20100524_Profile_En.Html, [Erişim Tarihi: 07.11.2022].

[174] Hürriyet Gazetesi, "Türk Askerinden Yürekleri Isıtan Paylaşım", 09.01.2017, https://www.hurriyet.com.tr/video/turk-askerinden-yurekleri-isitan-paylasim-40330519 [Erişim Tarihi: 08.11.2022].

• Beyaz Propaganda: Kaynağı ve mesajı aleni olan propaganda türüdür. Beyaz propaganda, yabancı izleyicilere, menşe hükümetin meseleler hakkındaki görüşlerini sunmak, politika kararlarını açıklamak, yerel medyada bulunmayan haberleri sunmak için kullanılır.[175] Radio Moscow ve Radio Free Europe gibi yayınların faaliyetlerini beyaz propaganda araçlarının örnekleridir.[176] Lerner, Nazi Almanyasına karşı yapılan "sykewar"ın büyük oparasyonunu beyaz propagandanın çıktısına dayandırmıştır.[177]

• Gri Propaganda: Kaynağı tecrübesiz halktan gizlenen fakat bilinçli gözlemcilerden gizlenmeyen, yaydığı mesaj doğru, yanlış yahut her ikisinin bir kombinasyonu olabilen propaganda türüdür. 1930'larda radyo alıcılarının yaygın olarak kullanılabilmesiyle başlayan gizli radyo yayıncılığı bir gri propaganda türüdür.[178]

• Kara Propaganda/ Dezenformasyon: Kaynağı belirsiz ve tamamen sahte haberlerden oluşan propaganda türüdür ve tarihi muhtemelen medeniyet kadar eskidir.[179] Dezenformasyonun başarılı sonuç vermesi için etkilenmek istenilen kişi yahut topluluğun inanmaya hazır durumda olması önemlidir.

• Yöntemine göre propaganda türleri;

Propagandanın nasıl uygulanacağı, nasıl bir sonuç getireceğini belirler. Bu yönüyle etkili olduğu kadar risk de içermektedir. William Biddle, propaganda yöntemlerini temel olarak dört kavram etrafında çerçevelemiştir: ikna, doğrudan duygusal çekicilik, doğrudan telkin ve dolaylı duygusal çekicilik.[180]

• İkna: İdeo- motor bir davranış anlayışına dayanır.[181] Bir kişinin yahut grubun zihnini ele geçirdiğinde amacına ulaşmış demektir.

---

[175] Daugherty, "The Discipline of Covert Action", a.g.e., 76.

[176] Abram Shulsky, "Elements of Strategic Denial and Deception", *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson, James J. Wirtz (Oxon: Routledge, 2017), 32.

[177] Daniel Lerner, "Sykewar Themes", *Psychological Warfare Against Nazi Germany: The Sykewar Campaign, D-Day to VE- Day*, (Cambridge: MIT Press, 1971), 185. ISBN: 9780262620192.

[178] Roy Godson, "Handmaiden of Policy: Principles of Covert Action", *Dirty Tricks or Trump Cards : U.S. Covert Action and Counterintelligence*, (New Brunswick: Transaction Publishers, 2011): 151- 152.

[179] *a.g.e.*, 155-156.

[180] WM. W. Biddle, "A Psychological Definition of Propaganda", *The Journal of Abnormal and Social Psychology, C.26,* S.3 (1931): 283. https://doi.org/10.1037/h0074944).

[181] *a.g.e.*, 283.

- Doğrudan Duygusal Çekicilik: Fikirleri, duygusal güdüleme ile belirginleştirir ve ortaya çıkarır. Kişinin yahut topluluğun öfke, korku, güven gibi birçok duygusuna hitap eder ve muhatabı duygularına hitap ederek kontrol etmeyi amaçlar.
- Doğrudan Telkin: Hipnoid ve hipnotik telkin çalışmalarından ilham almıştır.[182] Reklamcılık sektöründe sıklıkla kullanılan sloganlar ve komutlardan yararlanır. Özellikle radikal köktendinci ve siyasi örgütlerin eleman angaje ederken dini, etnik ve ideolojik motifleri kullanarak tetiklediği korku, öfke gibi duygularla tarihin eski çağlarından bu yana başarıya ulaşmış bir yöntemdir.
- Dolaylı Duygusal Çekicilik: Daha manipülatif, ufak imgelemeler ve teşbihlerden yararlanarak oluşan duygusal güdülemeden yararlanır.

3.5. Dış Kaynaklı Seçim Müdahaleleri ve Askerî Darbeler

Özellikle, 2. Dünya Savaşı'nın getirdiği yıkım ve yorgunluk ile konvansiyonel savaşlardan ve nükleer silahlanma yarışının getirdiği nükleer savaş ihtimalinden kaçınmanın bir yansıması olarak istihbari faaliyetlere ve örtülü operasyonlara müracaatın arttığı Soğuk Savaş yıllarında ve sonrasında dış kaynaklı seçim müdahalesi ve askerî darbe desteklerine örnek teşkil edecek birçok faaliyet gerçekleşmiştir. Örnek vermek gerekirse; ABD ve SSCB dönemi dâhil Rusya, 1946- 2000 yılları arasında bilinen yüz on yedi rekabetçi siyasal seçime müdahil olmuşlardır.[183] Bu da yaklaşık olarak her dokuz rekabetçi seçimden birine müdahil oldukları anlamına gelmektedir. Dov H. Levin, büyük bir gücün başka bir ülkenin seçimine belirli bir aday veya parti lehine müdahale etme girişimlerinin, seçim sonuçlarını şekillendirebileceğini değerlendirmiştir.[184] Levin'in bir başka değerlendirmesi ise, dış kaynaklı seçim müdahalelerinin çoğu durumda, müdahale ülkesinin çıkarlarının, seçim ülkesindeki bir adayın yahut siyasi partinin tehlikeye düşürdüğünü algılaması ve seçim ülkesinde

---

[182] *a.g.e.*, 283.

[183] Dov H. Levin, ''When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results'', *International Studies Quarterly*, C.60, S.2 (2016): 189, https://doi.org/10.1093/isq/sqv016.

[184] *a.g.e.*, 189.

müdahale ülkesiyle işbirliği yapmaya istekli bir yerel aktörün var olması olmak üzere iki koşulun eş zamanlı olarak var olduğu durumlarda gerçekleşmesidir.[185]

Siyasi örtülü operasyonlar, özellikle Soğuk Savaş yıllarında askeri darbeler ve toplumsal siyasi olayların kışkırtılması yoluyla gerçekleştirilmekteydi. ABD'nin 37. Başkanı Richard M. Nixon'ın konuya dair şu ifadeleri dikkate değerdir:

> *"Bazen açık ekonomik veya askeri yardım, hedeflerimize ulaşmak için yeterlidir. Diğerlerinde bunu yalnızca doğrudan bir askeri müdahale yapabilir. Ancak ikisi arasında, Amerika Birleşik Devletleri'nin gizli eylemler üstlenebilmesi gereken geniş bir alan var. Bu kâbiliyet olmadan, ABD'nin önemli çıkarlarını koruyamayız."*[186]

Dov H. Levin, askerî darbelerin güçlü devletler için dahi giderek artan maliyeti ve bunun yanı sıra dış kaynaklı seçim müdahalesinin çoğunlukla şiddet içermeyen bir müdahale türü olmasından ötürü, dış kaynaklı seçim müdahalelerinin her zamankinden daha önemli bir araç hâline geldiğini ifade etmiştir.[187]

Askerî darbe desteği örneklerinden biri, CIA'nın 2013 yılında belge gizliliğini kısmen kaldırması ile dahlini resmen kabul ettiği TPAJAX Operasyonu'dur. Söz konusu operasyon, ABD ve İngiltere'nin yürüttüğü ve İran'da Muhammed Musaddık'ın liderliğindeki Ulusal Cephe Partisi Hükümeti'nin devrilmesiyle başarıya ulaşmıştır.[188] 2017 yılında bazı gizli bölümleri açılarak tekrar yayınlanan raporda, TPAJAX'ın ilk aşamalarında analitik süreçlerden ziyade operasyonel süreçlere odaklanmasından ötürü operasyonu tehlikeye düşüren ve eylemleri daha çok psikolojik savaş ve propaganda ile halk desteğini konsolide etmeye yönlendiren bir dizi zorluğa değinilmiş ve teknolojinin kaydettiği ilerleme dolayısıyla bugünün analistlerinin ulaştığı bilgilerin 44 yıl önceki meslektaşlarının hayal dahi edemeyecek boyutlarda olduğunu ve dolayısıyla bugünün şartlarında bir örtülü eylem programında analizi göz

---

[185] Dov. H. Levin, "Throwing Their Hat into the Ring: When Electoral Interwentions Occur", *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions* (New York: Oxford University Press, 2020), 76.

[186] William J. Daugherty, ''The Role of Covert Action in Intelligence and Foreign Policy'', 9.

[187] Levin, "Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset", 2.

[188] Scott A. Koch, "Zendebad, Shah!: The Central Intelligence Agency and the Fall of Iranian Prime Minister Mohammad Mossadeq, August 1953", *National Security Archieve*, (Washington DC: CIA History Staff, 1998/ 2017), https://nsarchive.gwu.edu/dc.html?doc=4375470-Document-2-Zendebad-Shah, [Erişim Tarihi: 13.09.2020].

ardı etmenin sonuçlarının 1953 yılından çok daha ciddi hale geleceği vurgulanmıştır.[189] ABD'nin gizliliğini kaldırdığı bir diğer belge ise kod adı "PBSUCCESS Operasyonu" olan 1954 Guatemala askerî darbesine ait belgelerdir. 1953 yılında dönemin ABD Başkanı Eisenhower tarafından onaylanan operasyonun; paramiliter operasyonun yanı sıra psikolojik savaş, siyasi operasyon ve yıkım için 2.7 milyon dolarlık bir bütçe tanımlandığı, belgeler arasında 58 kişinin isminin yer aldığı bir "suikast listesinin" yer aldığı ve "siyasi cinayet klavuzu" niteliğinde 19 sayfalık bir suikast rehberi de içerdiğine dair bilgiler yer almaktadır.[190] ABD'nin yürüttüğü bir diğer örtülü operasyon seçeneği de dış kaynaklı seçim müdahalesi olmuştur. Filipinler'de 1950'de Komünizm yanlısı Hukbalahap İsyanı'nı psikolojik savaş teknikleriyle bastıran CIA ajanı Edward Lansdale, 1953'teki genel seçimde yürüttüğü örtülü operasyon ile Ramon Magsaysay'ın seçimi kazanmasını sağlamıştır.[191][192] Soğuk Savaş sonrası dönemde de birçok dış kaynaklı seçim müdahalesi gerçekleşmiştir. Bunlardan biri, 21 Kasım 2004 Ukrayna Genel Seçimlerine Rusya müdahalesidir. 2004 seçiminde Rusya Devlet Başkanı Vladimir Putin'in, Viktor Yanukoviç'i açıkça desteklemiş ve gerek seçime yakın dönemde Yanukoviç'i ziyaretleri ve övgü dolu konuşmalarıyla gerekse seçim sonuçları açıklanmadan evvel Yanukoviç'i tebrik etmesiyle bu desteği alenileştirmiştir.[193]

Örneklerden anlaşılacağı üzere, dış kaynaklı seçim müdahaleleri, askerî darbelere nispetle gerek operasyonel özellikleri gerekse yaygın şiddet içermemesi bakımından gizliliğe ve dolayısıyla makul inkâr edilebilirliğe daha elverişli bir örtülü operasyon türüdür. Günümüz teknolojik gelişmelerinden ve veri toplamadan bilgi yaymaya kadar

---

[189] National Security Archieve, "CIA and TPAJAX: The Tension Between Analysis and Operations", (2017): 120. https://nsarchive.files.wordpress.com/2018/03/cia-and-operation-tpajax.pdf. [Erişim Tarihi: 24.12.2022].

[190] Kate Doyle ve Peter Kornbluh, "CIA and Assassinations: The Guatemala 1954 Documents", *National Security Archive Electronic Briefing: Book No. 4,* https://nsarchive2.gwu.edu/NSAEBB/NSAEBB4/. [Erişim Tarihi: 31.12.2022].

[191] Bart Barnes, '' Edward Lansdale, Prototype For 'Ugly American,' Dies'', The Washington Post, https://www.washingtonpost.com/archive/local/1987/02/24/edward-lansdale-prototype-for-ugly-american-dies/d2ff2042-05c8-4f1d-b12d-972bf8338b14/.

[192] Nick Cullather, *Illusions of Influence: The Political Economy of United States-Philippines Relations 1942- 1960*. (Stanford: Stanford University Press, 1994): 108-109.

[193] Stephen Shulman ve Stephen Bloom, ''The Legitimacy of Foreign İntervention in Elections: The Ukrainian Response'', *Review of International Studies*, C.38, S.2 (2012): 453, doi:10.1017/S0260210512000022.

birçok seçeneğin artık siber ortamda mümkün olmasından ötürü, başarılı bir planlama ve yürütme mekanizması koşuluyla siyasi ve ekonomik örtülü operasyonlar eskisinden daha mahir yürütülebilecektir. Siber ortamın örtülü operasyonlara ne derece elverişli olduğu konusu, çalışmanın analiz bölümünde geniş çapta incelenecektir.

Tarihi geçmişi oldukça eski zamanlara dayanmakla birlikte Vestfalya Barışı ile oluşan uluslararası sistem ve uluslararası hukukun inşası, devletlerin dış politika hedeflerine ulaşma maksadıyla konvansiyonel yöntemlere başvurmaları bakımından caydırıcı unsurlar doğurmuştur. Bilhassa 2. Dünya Savaşı'nın yarattığı yıkım ve devletlerin kitle imha silahları geliştirme konusundaki yarışları güvenlik ikilemi doğurmuş ve konvansiyonel savaşlara girmeksizin dış politika hedeflerini gerçekleştirme konusunda devletlerin alternatif yöntemlere yönelimini arttırmıştır. Sponsor kimliğinin gizlenmesi bakımından eylemin kendisinin gizlenebildiği fakat sonuçlarının gözlemlenebildiği, makul bir şekilde inkâr edilebilmesi bakımından devletleri hukuki yaptırımlardan koruyacak dış politika araçlarından biri örtülü operasyondur. Örtülü operasyon türlerinden olan rejim değişikliği, dış kaynaklı seçim müdahalesi ve askerî darbelerin her ikisini de içeren bir şemsiye terim olmasına karşın yarattığı şiddet ve bununla bağlantılı olarak makul inkâr edilebilirlik bakımından birbirinden oldukça farklı sonuçlara sebebiyet verebilmektedirler. Lowenthal Örtülü Eylem Merdiveni'ne göre dış kaynaklı seçim müdahaleleri yarattığı şiddet bakımından düşük seviyede ve makul inkâr edilebilirlik bakımından yüksek seviyede olması bakımından, diğer örtülü operasyon türlerine nazaran daha elverişli bir seçenektir. Siber uzay, yapısı itibariyle cari dönemde makul inkâr edilebilirlik olgusunu destekleyen en önemli unsurlardan biridir. Bu bölümde bazı örnekleri incelenen örtülü operasyonların planlama, lojistik, maliyet ve gizlilik bakımından doğurduğu sonuçlar göz önünde bulundurulduğunda, siber uzayda özellikle sosyal medya zemininde gerek daha mikro ölçekte verilerin elde edilebilmesi, gerek daha kantitatif analitik yöntemler ile analiz edilebilmesi, gerek başka bir ülkeye ayak basmadan uzaktan kumanda edilebilmesi ve gerekse siber uzayın geleneksel yöntemlere nazaran desteklediği gizlilik avantajı bakımından, yapay zekâ tabanlı algoritma çağında örtülü operasyon araç ve yöntemlerinin yeni bir zemin kazandığı görülmektedir. İzleyen bölümde Cambridge Analytica vakası incelenecek ve dış kaynaklı seçim müdahalesinin yapay zekâ tabanlı algoritma çağında geldiği boyut ortaya konulacaktır.

4. CAMBRİDGE ANALYTİCA VAKASI

Cambridge Analytica, veri analitiği ile davranış bilimlerini birleştirerek seçmen eğilimlerini ve hassasiyetlerini çözümleme ve yönlendirme faaliyeti yürüten bir stra. 2013 yılında kurulmuş olan Londra merkezli şirket, SCL Group'un iştirakı olarak kurulmuş ve dünyanın birçok bölgesinde seçim kampanyaları yürütmüştür.

Şirket yöneticisi Mark Turnbull'un, basına sızan ifadelerine göre SCL ve Cambridge Analytica; Meksika, Malezya ve Brezilya, Avustralya ve Çin'de projeler yürütmüşlerdir.[194] Adı geçen ülkeler dışında birçok bölge ve ülkede projeler ve seçim kampanyaları, izleyen bölümlerde incelenecektir.

Şirketin veri analizinde davranış bilimlerinden yararlanarak nasıl isabetli propaganda hedefleri belirlediği ise şirketin CEO'su Alexander Nix'in 2016'da New York'ta gerçekleşen Concordia Zirvesi'nde "*Büyük Veri ve Psikografinin Gücü"* konulu sunumunda oldukça detaylı bir şekilde anlatılmıştır.[195] Nix sunumda özetle Cambridge Analytica'nın, dünya liderlerine ve iş dünyasına büyük verinin gücü ve psikografi üzerinden veri analizi ile nasıl bir propaganda ve reklam hizmeti verdiğinden söz etmiştir. Kitle hedefleme ve veri modelleme yaklaşımını psikolojik profil ile birleştirerek anlatan Nix, bunun geleneksel propaganda ve reklam modellerinden daha etkili olduğunu ifade etmiş; 2016'da Donald Trump ve 2015'te ABD senatörü Ted Cruz'a seçim kampanyaları için Cambridge Analytica'nın hizmet verdiğini belirtmiştir.[196]

Nix, psikografik bilginin ehemmiyetini *"günümüzde kitle iletişimi çoğunlukla demografi ve jeografi üzerinden kurgulanıyor oysa bu, buz dağının görünen kısmıdır. Hedef kitle hakkında analiz yaparken nokta atışı tespitler yapabilmek için psikografik*

---

[194] Channel 4 News, "Cambridge Analytica Uncovered: Secret Filming Reveals Election Tricks" [Video], *YouTube*, 19 Mart 2018, https://www.youtube.com/watch?v=mpbeOCKZFfQ.

[195] Concordia, (27 Eylül 2016), Cambridge Analytica - The Power of Big Data and Psychographics [Video], YouTube, https://www.youtube.com/watch?v=n8Dd5aVXLCc. [Erişim Tarihi: 20.10.2020].

[196] a.g.e., https://www.youtube.com/watch?v=n8Dd5aVXLCc. [Erişim Tarihi: 20.10.2020]

bilgileri gereklidir" sözleriyle değerlendirmiştir.[197] Nix, Cambridge Analytica şirketinin, psikografi üzerine çalıştığını ve seçmenlere uygun seçim propagandası üretmek için Beş Faktörlü Kişilik Modeline (The OCEAN) başvurduklarını ifade etmiştir. Dünya kamuoyu, Cambridge Analytica şirketinden, 2016 ABD Başkanlık Seçimlerinden sonraki süreçte şirketin eski çalışanı Christopher Wylie'nin şirket faaliyetlerini faş etmesiyle haberdar olmuştur.

Çalışmanın bu bölümünde, Cambridge Analytica vakası incelenecek ve dış kaynaklı seçim müdahalesinde siber uzayın sağladığı avantaj ile büyük veri, sosyal medya ve psikografinin algoritmalara entegre edilerek nasıl sistematik bir örtülü operasyon aracı hâline geldiği problemi incelenecektir.

4.1. SCL ve Cambridge Analytica

SCL (Strategic Communications Laboratories), 1993 yılında kurulmuş, yirmi beş yılı aşkın bir süre boyunca küresel çapta savunma sözleşmeleri tedarik etmiş ve dünyanın dört bir yanındaki ülkelerde siyasi seçim kampanyaları yönetmiştir.[198] Kuruluşundan itibaren yaklaşık 50 ülkede 200'ü aşkın seçim kampanyası ile siyasi, insani ve savunma projeleri gerçekleştirmiştir.[199] Cambridge Analytica ise SCL Group'un bir iştiraki olarak, başlangıçta yalnızca ABD'deki operasyonları yönetmek maksadıyla kurulmuştur.[200]

Cambridge Analytica ihbarcısı (whistleblower) Christopher Wylie, SCL şirketinin İngiliz hükümeti tarafından *"gizli"* düzeydeki bilgilere erişme iznine sahip olduğunu ve yönetim kurulunda Margaret Thatcher döneminin kabine bakanları ve emekli komutanların yanı sıra profesörler ve yabancı politikacıların da olduğunu ifade etmiştir.[201] Bu bağlamda SCL şirketi ve onun iştiraki olan Cambridge Analytica,

---

[197] a.g.e., https://www.youtube.com/watch?v=n8Dd5aVXLCc. [Erişim Tarihi: 20.10.2020]

[198] Britanny Kaiser, *Targeted: The Cambridge Analytica Whistleblower s Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again,* (Harper: HarperCollins Publishers, 2019), 11.

[199] *a.g.e.,* 15.

[200] *a.g.e.,* 28.

[201] Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America*, (New York: Random House, 2019), 43. e-book ISBN: 9781984854643.

vekâlet savaşlarının ve istihbarat faaliyetlerinde özel şirketlerinin kullanımının iyi bir örneğidir. İhbarcı Christopher Wylie, Cambridge Analytica vakasını ve kendisinin şirkete dâhil oluş süreçlerini anlattığı otobiyografik kitabında, işe giriş sürecinde bir gizlilik sözleşmesi imzaladığını ve şirketin CEO'su Alexander Nix'in kendisine firmanın çalışmalarının çoğunun, askeri ve istihbarat teşkilatları için, *"hükümetlerin resmi olarak üstlenemeyecekleri"* projeler üzerinde çalıştığını söylediğini ifade etmiştir.[202] Bu ifadeler, örtülü operasyonun literatürde üzerinde en çok ittifak edilen *"gizlilik"* ve *"makul inkâr edilebilirlik"* kavramları ile sıkı sıkıya örtüşmektedir.

Cambridge Analytica, 2018 yılında ana şirketi SCL tarafından kapatılmıştır fakat şirketin eski çalışanları AUSPEX adında yeni bir şirket kurmuşlardır.[203] AUSPEX, çalışmalarını, davranış araştırmaları, veri bilimi, hedefli iletişim ve kapasite geliştirme olarak tasniflendirmiş ve seçim kampanya yasalarına, AB veri güvenliği yasalarına ve etik değerlere sadık kalarak çalışacaklarını, çalışmalarını öncelikli olarak Afrika ve Ortadoğu'da gerçekleştireceklerini ifade etmişlerdir.[204] Ancak, söz konusu eski çalışanlar arasında, basına yansıyan ifadeleri nedeniyle Exeter Üniversitesi Strateji ve Güvenlik Enstitüsü'ndeki (SSI) onursal üyeliği iptal edilen Mark Turnbull[205] da yer almış ve kendisinin LinkedIn profilindeki beyanına göre Haziran 2018 ile Eylül 2021 arasında AUSPEX Genel Müdürü olarak çalışmıştır.[206]

SCL öncelikle, Pakistan'da köktenci militan angajmanıyla mücadele, Güney Sudan'da muharip silahsızlanma ve terhis, Latin Amerika'da uyuşturucuyla mücadele ve insan kaçakçılığıyla mücadele operasyonları gibi dünya çapında etki operasyonları ve psikolojik operasyonlar yürütmek için ordulara hizmet vermiştir.[207] SCL önceleri Ukrayna Devlet Başkanına bir rapor hazırlamış ve bu raporu Birleşik Krallık Savunma

---

[202] a.g.e., 44.

[203] BBC News, "Cambridge Analytica Staff Set Up New Firm", 12 Temmuz 2018, https://www.bbc.com/news/technology-44807093. [Erişim Tarihi: 20.12.2022].

[204] AUSPEX, https://www.auspex.ai/. [Erişim Tarihi: 20.12.2022].

[205] BBC News, "Uni Drops Cambridge Analytica Executive as Fellow", 22 Mart 2018, https://www.bbc.com/news/uk-england-devon-43506270. [Erişim Tarihi: 20.12.2022].

[206] LinkedIn, https://www.linkedin.com/in/marknturnbull/?originalSubdomain=uk. [Erişim Tarihi: 20.12.2022].

[207] Wylie, a.g.e., 43.

Bakanlığı (MOD) ile de paylaşmıştır.[208] Ayrıca SCL, NATO ile 2015 yılında Letonya'daki NATO Mükemmeliyet Merkezi'nde, Rus propagandasına karşı koymayı amaçlayan eğitim kursu yürütmüştür. Tüm bu çalışmalar ile birlikte SCL ve onun iştiraki olan Cambridge Analytica, çalışmaları ile Rus istihbaratının dikkatini çekmiş ve Rusya'nın dış politikalarıyla bir şekilde örtüştüğü düşünülen bir dizi saha çalışması ve seçim kampanyasına yönelmiştir.[209]

SCL, özellikle Aleksandr Kogan'ın *"This is Your Digital Life"* adlı anket uygulaması ile, 2010'lu yıllarda birçok ülkede veri ihlallerine sebep olmuş ve çok sayıda kişisel veri toplamıştır. Avustralya Enformasyon Komiserliği Ofisi (OAIC), Cambridge Analytica'nın üst kuruluşu olan SCL'in, söz konusu uygulama aracılığıyla Avustralya'da yaklaşık 311.127 Avustralyalının kişisel verisinin toplandığı iddiasıyla Facebook'a dava açmıştır.[210] Ülkede uygulamayı yalnızca 53 kişinin indirmesine karşın, 311 bin 117 kişinin verilerinin şirket tarafından ele geçirildiği tespit edilmiştir.[211] Şirketin, Avustralya'da Siber Güvenlikten sorumlu Bakan Dan Tehan ile yaptığı görüşmelerin yanı sıra, Channel 4 News'ta yayınlanan gizli görüşmede, Mark Turnbull, Meksika, Malezya ve Brezilya'da seçim kampanyaları yürüttüklerini ve sıradaki rotasyonlarının Avustralya ve Çin Halk Cumhuriyeti olduğunu ifade etmiş ancak Çin Halk Cumhuriyeti'nde seçim çalışmaları için değil, muhaliflerin kişisel verileri üzerinde çalışmak maksadıyla bulunduklarını eklemiştir.[212]

Channel 4 News kanalının yayınladığı videoda ayrıca, kanalın kendi iddiasına göre SCL ve bünyesindeki Cambridge Analytica, Nijerya, Kenya, Çek Cumhuriyeti, Hindistan ve Arjantin'de de seçim çalışmaları yürütmüşlerdir.[213] Kenya'da Uhuru

---

[208] Liam O'hare, "SCL and the Phantom Contract", *Bella Caledonia*, 22 Mart 2018, https://bellacaledonia.org.uk/2018/03/22/scl-and-the-phantom-contract/. [Erişim Tarihi: 20.12.2022].

[209] Wylie, a.g.e.,170.

[210] Office Of the Australian Information Comissisioner, "Commissioner Launches Federal Court Action Against Facebook", 9 Mart 2020, https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook. [Erişim Tarihi: 20.12.2022].

[211] Christopher Knaus, "Facebook Appeal Over Cambridge Analytica Data Rejected by Australian Court as Divorced From Reality", *The Guardian*, 7 Şubat 2022, https://www.theguardian.com/technology/2022/feb/07/facebook-appeal-over-cambridge-analytica-data-rejected-by-australian-court-as-divorced-from-reality. [Erişim Tarihi: 09.12.2022].

[212] Channel 4 News, *a.g.e.*, https://www.youtube.com/watch?v=mpbeOCKZFfQ.

[213] *a.g.e.*, https://www.youtube.com/watch?v=mpbeOCKZFfQ.

Kenyatta için çalışan Cambridge Analytica, seçmenlerin sağlık, terör tehdidi ve altyapılar ile ilgili endişelerini sosyal medya platformları, Google ve akıllı telefonlar üzerinden tetiklemek maksadıyla sahte haberler (dezenformasyon) yaymış ve söz konusu propaganda içerikleri halkın %90'ına ulaşmıştır.[214] Cambridge Analytica ayrıca, kendi web sitesinde İtalya'da 1980'lerden itibaren mevzi kaybeden bir siyasi parti için de çalıştıkları bilgisine yer vermiştir.[215] Cambridge Analytica'nın bir diğer projesi ise Nijerya'da seçmenlerin sivil kurumlara yönelik güvenini sarsmaya yönelik yürüttüğü *"Aşılama"* etiket adlı projedir. *"Aşılama"* bir teşbih olarak şirketin, şeçim sonuçlarını etkilemeye yönelik dezenformasyon yayma ve seçmeni etkilemeye yöntemlerine atıfta bulunmaktadır. Bu proje ile Nijerya seçmeninin yaklaşan seçimlerde hile olacağına inanması sağlanmış, Wylie'nin ifadesine göre Nix, Nijerya seçmeninin bunu düşünmesini sağladıklarını ifade etmiştir.[216] Cambridge Analytica, Nijerya'da Müslüman aday Muhammadu Buhari'ye karşı seçimleri tekrar kazanmak isteyen Hıristiyan aday Goodluck Jonathan'ı destekleyen ve Buhari'nin seçilmesi durumunda petrol ve maden arama haklarını iptal ederek gelirlerinin önemli bir kaynağını ortadan kaldıracağından endişelenen Nijeryalı milyarder bir grup ile anlaşmıştır.[217] Cambridge Analytica, Goodluck Jonathan adına olumlu propaganda yapmak yerine Muhammedu Buhari hakkında dezenformasyon çalışmalarına odaklanmıştır.[218] Wylie'nin ifadesine göre, muhalif kesimin e-posta hesapları, veri tabanları ve tıbbi kayıtları gibi hassas bilgileri, Cambridge Analytica tarafından ele geçirilmiş ve hatta Buhari'nin muhtemelen kanser olduğunu keşfedilmiştir.[219]

SCL ayrıca Trinidad ve Tobago'da da faaliyetler yürütmüştür. Trinidad Ulusal Güvenlik Bakanlığı SCL'den, suç işleme olasılığı yüksek olan vatandaşların belirlenmesi için bir çalışma yapmasını istemiş ve ülkenin nüfus sayım verilerini SCL'in kullanımına açmıştır.[220] Wylie, Trinidad hükümetinin tek bir hamlede tüm

---

[214] *a.g.e.*, https://www.youtube.com/watch?v=mpbeOCKZFfQ.

[215] CA Political, "Italy", *Cambridge Analytica*, 29 Mayıs 2014, https://ca-political.com/casestudyitaly/.

[216] Wylie, *a.g.e.*, 154.

[217] *a.g.e.*, 168.

[218] *a.g.e.*, 167.

[219] *a.g.e.*, 169.

[220] *a.g.e.*, 58.

vatandaşlarının mahremiyetini ihlal ettiğini ve Telekom altyapıları üzerinden seçtiği IP adresleri vasıtasıyla SCL'in, istediği anda bir Trinidad vatandaşlarının o anda internette neler yaptığını izleyebildiğini bildirmiştir.[221]

SCL ve bünyesindeki Cambridge Analytica, yukarıda söz edilen ülkeler dâhil beş kıtada 100'ü aşkın ülkede seçim kampanyası yürütmüştür.[222] Ancak şirketin eski çalışanı Christopher Wylie'nin ifşaatı ile, söz konusu şirketlerin faaliyetleri daha çok Birleşik Krallık'ın Avrupa Birliği'nden Ayrılma Referandumu (BREXIT) ve 2016 ABD Başkanlık Seçimleri odağında gündeme gelmiştir. şirketin, Birleşik Krallık'ın Avrupa Birliği'nden ayrılma referandumu olan Brexit seçimlerine de müdahalede bulunduğu konusu, şirketin eski çalışanlarından ihbarcı Christopher Wylie[223] ve ihbarcı Brittany Kaiser[224] tarafından açıklanmıştır. Brexit seçiminde AB'den ayrılma taraftarları, Leave.EU ve Vote Leave adlarında iki ana seçim kampanyası ile seçime hazırlanmışlardır. Bu kampanyalardan Leave.EU, Cambridge Analytica ile çalışmış[225] ve İngiltere halkını göçmen karşıtı görüşlerin alevlenmesi ve zaman zaman şiddete dönüşmesi[226] yoluyla *"ayrılma"* fikri etrafında konsolide etmiştir. Vote Leave ise, Michael Gove ve Boris Johnson gibi politikacılara danışmanlık yapmış stratejist Dominic Cummings ve Birleşik Krallık'taki birçok sağcı lobi grubunun kurucusu Matthew Elliott tarafından ortaklaşa kurulmuştur.[227] Vote Leave, Zack Massingham ve Jeff Silvester tarafından 2013 yılında kurulan Kanada merkezli AggregateIQ (AIQ) adlı siyasi danışmanlık ve teknoloji şirketi ile işbirliği yapmıştır.[228] AIQ yasal olarak müstakil bir şirket gibi görünüyor olsa da, SCL şirketi ile çalışmalarının haklarını SCL'e devrettiği bir fikri mülkiyet anlaşması imzalamış olması[229], Brittany Kaiser'in ifadesiyle AIQ çalışanlarının iş amaçları için SCL ve Cambridge Analytica e-

---

[221] *a.g.e.*, 59.

[222]BBC News, "Cambridge Analytica: The Data Firm's Global Influence", 22 Mart 2018, https://www.bbc.com/news/world-43476762. [Erişim Tarihi: 09.12.2022].

[223] Wylie, *a.g.e.*, 5.

[224] Kaiser, *a.g.e.*, 108- 126.

[225] Wylie, *a.g.e.*, 177.

[226] *a.g.e.*, 190.

[227] *a.g.e.*, 186.

[228] *a.g.e.*, 182.

[229] AggregateiQ Data Services, "Intellectual Property Rights", (28 Mart 2014): 6.

postalarını dahi kullanmaları ve SCL ekibi içinde AIQ'nun *"SCL Kanada"* olarak anılması, söz konusu şirketin SCL'in bir paravan şirketi olduğu hususunda güçlü emareler taşımaktadır.[230]

Cambridge Analytica'nın dâhil olduğu bir diğer seçim kampanyası ise 2016 ABD Başkanlık Seçimleridir. ABD'nin liberal kurumsal kültürü, ülkenin veri gizliliği politikalarına da yansımıştır. ABD'de de Cambridge Analytica skandalından sonra değiştirilen veri gizliliği politikaları öncesinde, bir kullanıcı aksini beyan etmediği sürece kişisel verilerinin ticari ve akademik amaçlarla kullanılması serbestti. Elbette ele geçirilen verilerin ticari amaçlarla kullanılıp kullanılmayacağına dair ciddi bir kontrol de bulunmamaktaydı. ABD'nin aksine AB, kullanıcıların rıza ve onay verdiği açıkça belirtilmeksizin kişisel verilerinin kullanımını yasaklayan daha katı veri gizliliği politikalarına sahiplerdi.[231] Bu duruma vakıf olan ve ABD'nin liberal ve özgürlükçü yaklaşımını bir güvenlik açığı olarak değerlendiren kurucuların, Cambridge Analytica'yı bu sebeple ABD'de kurarak, şirketin ABD veri politikalarına tabi olmasını istemiş olmaları ve bu şekilde daha serbest bir çalışma olanağına sahip olunacağını değerlendirmiş olmaları muhtemeldir.

Wylie, Cambridge Analytica'nın, kuruluşundan sonra Afrika'da birçok pilot proje gerçekleştirmiş ve yeteneklerini geliştirip test ettikten sonra ABD'de uygulamaya geçirdiğini ve kampanya reklamları ile ABD'de şiddeti körüklediğini belirtmiştir.[232] Cambridge Analytica, ABD'de hem Ted Cruz'a senato seçimlerinde hem de Donald Trump'a başkanlık seçimlerinde hizmet vermiştir. Şirketin ABD'deki faaliyetleri, yargılama raporlarının incelendiği bölümde detaylandırılacaktır.

4.2. Cambridge Analytica ve Siyasi Kampanya Yöntemleri

Siyasal seçim kampanyalarında dijital dış kaynak kullanımı Cambridge Analytica öncesi sürece dayanmaktadır. Örnek olarak Barack Obama'nın, 2012 ABD başkanlık seçimlerine hazırlandığı süreçte, kampanya ekibinin Analitik Sorumlusu olan Dan

---

[230] Kaiser, *a.g.e.*, 146.

[231] Christina Pop, "EU vs US: What Are the Differences Between Their Data Privacy Laws?", *Endpoint Protector*, 27 Eylül 2022, https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws/. [Erişim Tarihi: 18.12.2022].

[232] Wylie, *a.g.e.*, 16.

Wagner, veri analitiklerinden etkin bir şekilde yararlanmak için bir veri bilimi şirketi olarak Civis Analytics'i kurmuştur.[233] Dan Wagner'in ekibi, parti seçmen listesindeki veriler ile TV derecelendirme şirketlerinden sağlanan demografik verileri birleştirerek makine öğrenmesi yöntemleriyle dönemin ABD Başkanı Barack Obama'ya oy verme olasılığı daha fazla ya da daha düşük olan seçmenleri yüksek tahmin oranlarıyla belirlemeyi başarmıştır.[234] Obama ayrıca kampanya sürecinde BlueLabs adlı veri analitiği şirketinden de yararlanmıştır. Civis Analytics, BlueLabs ve benzeri diğer şirketler Obama 2012 kampanyasına tahmine dayalı analitik ve modelleme yetenekleri ile destek vermişlerdir."[235] Obama'nın kampanya ekibinin nispeten daha profesyonel olarak dijital kaynaklardan ve veri analizinden yararlanmasından önce, 2004 yılında Vermont Valisi Howard Dean'in ABD başkanlık seçimi kampanyası; dönemin ilkel şartları altında kampanya adına bağış toplamak, seçmenlere ulaşmak ve seçmen grupları toplamak amacıyla internete kampanyaya yönelik RealPlayer, QuickTime ve Windows Media Player formatlarında videolar yüklemek ve Google arama motoru optimizasyonu ile kampanya web sitesinin Google sayfalarında görünürlüğünü arttırmak (SEO) gibi birçok dijital gelişime öncülük etmiştir.[236] Dean kampanyasının dijital gönüllüleri ve çalışanlarının bir kısmı daha sonraki süreçte Barack Obama'nın 2004 İllinois Senatosu seçim kampanyasında ve 2012 ABD Başkanlık kampanyasında görev almışlardır. [237]

Cambridge Analytica ise, çalışmaları süresince daha fazla veriye erişmek kadar onları psikoloji biliminden yararlanarak en iyi şekilde ayıklamak ve anlamlandırmakla da ilgilenmiştir. Şirket, kişilerin Facebook beğenileri (hayran sayfaları) ve arkadaş

---

[233]EAP, "From a Presidential Campaign to a Data Analytics Start-Up – Civis Analytics" ,*Digital Innovation and Transformation of Harvard University*, 1 Şubat 2018, https://d3.harvard.edu/platform-digit/submission/from-a-presidential-campaign-to-a-data-analytics-start-up-civis-analytics/. [Erişim Tarihi: 20.12.2022].

[234] *a.g.e.,* https://d3.harvard.edu/platform-digit/submission/from-a-presidential-campaign-to-a-data-analytics-start-up-civis-analytics/. [Erişim Tarihi: 20.12.2022].

[235] Kaiser, *a.g.e.,* 145.

[236] Steve Friess, "The father of All Web Campaigns", *Politico*, 30 Eylül 2012, https://www.politico.com/story/2012/09/how-deans-wh-bid-gave-birth-to-web-campaigning-081834. [Erişim Tarihi: 20.12.2022].

[237] *a.g.e.*, https://www.politico.com/story/2012/09/how-deans-wh-bid-gave-birth-to-web-campaigning-081834. [Erişim Tarihi: 20.12.2022].

listelerini kullanarak elde ettiği verilere, fiziksel olarak erişim sağladığı kamu verileri ve bilgisayar korsanlığı ile ele geçirdiği verileri de dâhil ederek makine öğrenmesi yöntemlerini titizlikle kullanmıştır. Tüm bu çalışmaların ufkunda, kişilerin psikolojik profillerinin oluşturulması ve kişilik tiplerinin anlaşılmasının ötesinde, tutumlarının da değiştirilmesi fikri yer almıştır.[238]

Cambridge Analytica'nın siyasi kampanya yöntemlerinden büyük veri, sosyal medya ve psikografilerin kullanımı daha ön planda görünüyor ve tartışılıyor olsa da, rüşvet, şantaj, casusluk faaliyetleri ve bal tuzakları gibi istihbari operasyon yöntemlerinin de kullanıldığı, bir muhabirin şirket CEO'su Alexander Nix'in konuşmalarını gizli kamera ile kayıt altına alması ve yayınlaması ile ortaya çıkmıştır. Söz konusu muhabirin, kendisini, Sri Lankalı seçkin bir ailenin mensubu olarak oluşturduğu maske lejantı ile tanıtması ve Sri Lanka seçimleri ile ilgili Cambridge Analytica ile yaptığı toplantıyı gizli kamera ile kayıt altına alıp yayınlamasıyla ortaya çıkan vakada, şirketin CEO'su Nix, eski İngiliz ve İsrail casusları ile çalıştıklarını, muhaliflere yönelik bal tuzakları ile ele geçirilen kanıtlar üzerinden skandallar yarattıklarını, yolsuzluk skandallarını da şantaj aracı olarak kullandıklarını ve tüm bunları *"izi Cambridge Analytica'ya sürülemeyecek şekilde"* paravan şirketler ve gizli ağlar ile yaptıklarını ifade etmiştir.[239] Ancak bu bölümde, şirketin büyük veri, sosyal medya ve psikografi kullanımları incelenecektir.

4.2.1. Büyük Verinin Kullanımı

Siyasal seçim kampanyalarında sosyal medya ve büyük veriyi ilk kez ABD 2008 seçimlerine hazırlanan, dönemin İllinois Senatirü Barack Huseyin Obama kullanmıştır. Daha sonra Cambridge Analytica vakası ile adını duyuracak ve ihbarcı olarak Cambridge Analytica sürecini yayımladığı bir kitapla anlatacak olan Brittany Kaiser, Barack Obama'nın 2008 başkanlık seçimi kampanya ekibinde de çalışmıştır.[240]

---

[238] Wylie, *a.g.e.*, 88.

[239] Emma Graham-Harrison , Carole Cadwalladr, Hilary Osborne, "Cambridge Analytica Boasts of Dirty Tricks to Swing Elections", *The Guardian*, 19 Mart 2018, https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections. [Erişim Tarihi: 01.11.2020].

[240] Kaiser, *a.g.e.*, 15, 145- 147.

2018 yılında Cambridge Analytica Baş Veri Sorumlusu Alex Tayler, "IT Weekend: Ukraine" Konferansında, *"iletişim ve pazarlama endüstrisinde yoğun bir uzmanlığa sahip veri bilimi danışmanlığı"* olarak tanımladığı Cambridge Analytica'nın büyük veri ve psikografiyi nasıl kullandığına dair *"Büyük Veri ve Psikografinin Gücü"* konulu bir sunum gerçekleştirmiştir. Tayler, sunumunda 3 anahtar teknoloji tanımlamıştır: İlki, büyük verinin yaygınlığı, ortaya çıkışı ve veri toplayıcılar (Experian ve Acxiom gibi veri sağlayıcı şirketleri örnek olarak vermiştir), ikincisi Amazon AWS gibi yaygın, düşük maliyetli ve yüksek performanslı bilgi işlemin ortaya çıkışı ve üçüncüsü ise açık kaynaklı makine öğrenimi kütüphanelerinin oluşmasıdır.[241] Tayler; Experian, Acxiom, IRI ve konum verileri toplayan NinthDecimal gibi veri derleyen üçüncü taraf uygulamalarının sağladığı veriler ile, gazete ve dergi yayıncılarından, süpermarket sadakat kartlarından, ABD nüfusuna kayıtlı herkesi yaşam tarzları hakkında büyük miktarda ayrıntıyla kapsayan ticari dosyalardan, sosyal medyadan, açık (open source) kaynaklardan ve diğer kaynaklardan temin edilen verileri lisanslayarak ABD'deki 240 milyon yetişkin tüketicinin tamamına ilişkin dört veya beş bin kadar veri noktası içeren muazzam bir veri tabanı oluşturmayı başardıklarını ifade etmiştir.[242]

Cambridge Analytica'nın projelerinde yer almış olması bakımından Christopher Wylie'nin de bu konudaki ifadeleri dikkate değerdir. Wylie, SCL'de işe başladığı ilk birkaç ay boyunca, Cambridge merkezli Psikolog Brent Clickard ve onun arkadaşı Tadas Jucikas ile birçok ülkede küçük ölçekli pilot projelerde çalıştığını, Jucikas'ın otomatikleştirilmiş veri toplama araçları oluşturup farklı veri kaynaklarını her bir birey için tek bir kimlikte birleştirmek için algoritmik tahminler kullanarak ve ardından arzu edilen davranışları tahmin etmek için derin öğrenme sinir ağları vasıtası ile çok çeşitli verileri çekmeyi önerdiğini ifade etmiştir.[243] SCL, ilk veri yığınını Amazon'un Mturk (Mechanical Turk) adlı pazaryeri (marketplace) uygulaması vasıtası ile elde etmiştir.[244] Aleksandr Kogan, MTurk adlı uygulama üzerinde bir anket düzenlemiş ve

---

[241] SoftServe, "Dr Alex Tayler: The Power of Big Data and Psychographics", 8 Şubat 2018, https://www.youtube.com/watch?v=mHSsGKU35GY. [Erişim Tarihi: 13.12.2022].

[242] *a.g.e.,* https://www.youtube.com/watch?v=mHSsGKU35GY. [Erişim Tarihi: 13.12.2022].

[243] Wylie *a.g.e.,* 55- 56.

[244] *a.g.e.*, 119.

1-2 dolar karşılığında bu anketi dolduran on binlerce kullanıcının ad, cinsiyet, yaş, konum, durum güncellemeleri, beğeniler, arkadaş listesi gibi bilgilerini elde etmiştir.[245] Şirket, anket dolduran kullanıcıların Facebook bilgileri ile Graph API uygulamasına giriş yapmaları ve özel bir kod girmeleri karşılığında ödeme alabildikleri bir sistem oluşturmuş[246], buradan ulaştığı kullanıcıların beğenileri ile diğer seçmen ve tüketici verilerini birleştirip profil oluşturma algoritmalarını *"eğiterek"* isabetli tahminler elde etmeyi başarmıştır.[247]

Cambridge Analytica, Facebook verilerinin yanı sıra saha çalışmaları ile de veri elde etmiştir. Algoritmaları eğitirken yapılan tahminlerin bu süreçte bir teste tabi tutulması gerekmiştir. Bu gereksinim ise, 2014 yılı başlarında Cambridge Analytica'nın ABD'ye hiçbiri Amerikalı olmayan sosyologları ve antropologları göndererek odak grup görüşmeleri yapmaları ile mümkün olmuştur.[248] Şirket bu şekilde, bir dış gözlemci olarak Amerikanların kanıksadıkları için fark etmedikleri nüansları fark ederek sorularına aldıkları cevaplar neticesinde, anketlerde kullanacakları doğru soruları oluşturma imkânı bulmuştur. Buradan anlaşıldığı üzere, SCL ve Cambridge Analytica veri toplama ve anlamlandırma çalışmalarını yalnızca sosyal medya üzerinden yapmamış, maske lejantı ile saha çalışmaları gerçekleştiren araştırmacıların insan istihbaratı teknikleri ile elde ettikleri verilerden de yararlanmıştır.

4.2.2. Sosyal Medyanın Kullanımı

Facebook, 2010- 2015 yılları arasında üçüncü taraf uygulamalarının Facebook kullanıcıları ve onların arkadaş listesindeki kişilerin verilerini toplamalarına izin vermiştir. 2015 yılında arkadaş bilgilerinin elde edilmesine artık olanak tanınmayacağını duyurmuş olsa da, Cambridge Analytica hâlihazırda söz konusu arkadaş listelerindeki kişisel verileri toplamıştır.[249] 2010 yılında F8 Geliştirici Konferansı'nda konuşma yapan Facebook CEO'su Mark Zuckerberg ve Facebook

---

[245] *a.g.e.*, 118- 120.

[246] Kaiser, *a.g.e.*, 140.

[247] Wylie, *a.g.e.*, 120.

[248] *a.g.e.*, 98.

[249] Nicole Nguyen, "Here's How Facebook Got Into This Mess: A Timeline", *BuzzFeed.News*, 22 Mart 2018, https://www.buzzfeednews.com/article/nicolenguyen/cambridge-analytica-facebook-timeline. [Erişim Tarihi: 12.12.2022].

Ürün Direktörü Bret Tylor, Açık Grafik (Open Graph) isimli hizmeti duyurarak üçüncü taraf uygulamalarına kullanıcıların profil bilgilerine dair erişim izni verildiğini açıklamışlardır.[250] Graph API uygulaması ile web siteleri, kullanıcıların zevkleri, ilgi alanları ve ilişkilerine dair verileri elde etme fırsatı yakalamışlardır. Kullanıcılar Facebook'ta oturum açtıklarında, Graph API kullanan web siteleri, söz konusu web sitesinde oturum açılmasa yahut herhangi bir bilgi verilmese dahi, kullanıcıların bilhassa ilgi alanlarına göre hazırlanmış bilgileri, ürünleri ve hizmetleri görüntüleyebilmişlerdir. Wylie'nin ifadesine göre Aleksandr Kogan, Facebook üzerinden söz konusu uygulama ile özel mesajların dahi çekilebileceğini iddia etmiştir.[251] 2012 yılında Facebook, kullanıcılarının kişisel bilgilerinin kullanımına izin verdiklerini daha az fark ettirecek şekilde izin talep sayfasının tasarımını değiştirerek, *"oyunlar için izin"* sayfasındaki seçenekleri *"izin ver" ve "izin verme"* yerine *"oyun oyna"* şeklinde değiştirmiştir.[252] Yükselen tepkiler üzerine Facebook, Graph API (v1) kullanımını kaldırmıştır. Ne var ki 2015 yılında Graph API (v1) kaldırılmadan evvel, Cambridge Üniversitesi'nden David Stillwell 2007'de Facebook kullanıcılarına, uygulamaya katılmalarına yönelik myPersonality adlı kişilik profili sunan bir uygulama geliştirmişti.[253] Wylie, Facebook nezdinde sosyal medya platformlarının kişisel verileri nasıl izlediğini ve kaydettiğini şu ifadelerle çarpıcı bir biçimde vurgulamıştır:

"Her kaydırma izlenir, her hareket izlenir, her beğeni izlenir. Hepsi oradadır; nüanslar, ilgi alanları, hoşlanılmayan şeyler; hepsi ölçülebilir. Bu, Facebook'tan gelen verilerin giderek daha fazla ekolojik geçerliliğe sahip olduğu anlamına gelir."[254]

Wu Youyou, Michal Kosinski ve David Stillwell, 2015 yılında yayınladıkları bir makalede, dijital ayak izlerine dayalı bilgisayar modelleri ile, insanların kişilikleri

---

[250] Samuel Axon, "Facebook's Open Graph Personalizes the Web", *Mashable.com*, 21 Nisan 2010, https://mashable.com/archive/facebook-open-graph#WQ_Po8XekkqE. [Erişim Tarihi: 12.12.2022].

[251] Wylie, *a.g.e.*, 118.

[252] Nguyen, *a.g.e.*, https://www.buzzfeednews.com/article/nicolenguyen/cambridge-analytica-facebook-timeline. [Erişim Tarihi: 12.12.2022].

[253] Wylie, *a.g.e.*, 113.

[254] Wylie, *a.g.e.*, 115.

hakkındaki yargıları hakkında arkadaşları, aileleri, iş arkadaşları, eşleri gibi yakınları tarafından verilen yargılardan daha doğru ve geçerli tahminler yapılabileceğini ortaya koymuşlardır.[255] Youyou, Kosinski ve Stillwell'in çalışmalarının çarpıcı bulgusu ise bilgisayar tabanlı yargıların, katılımcıların kendi değerlendirmeleriyle ortalama insan yargılarından daha güçlü bir şekilde ilişkili olduğudur.[256]

4.2.3. Psikografinin Kullanımı

Sandra Matz, Ruth Appel ve Michal Kosinski 2019 yılında yayınladıkları çalışmada psikolojik hedeflemeyi, insanların dijital ayak izlerinden elde edilen psikolojik profiller vasıtasıyla duygularını, davranışlarını veya tutumlarını etkileme pratiği olarak tanımlamışlardır.[257] Psikolojik hedefleme Cambridge Analytica vakası ile kamuoyu tarafından geniş çapta bilinir hale gelmiş olsa da, psikolojik hedeflemeyi dijital ortamda ilk kez kullanan şirket Cambridge Analytica değildir. 2012 yılında Facebook, "*kullanıcı kişilik özelliklerinin sosyal ağ sistemi iletişimlerinden ve özelliklerinden belirlenmesi"* konulu psikolojik hedefleme patent başvurusunu yapmış ve sonrasında patenti Facebook, Instagram ve Whatsapp'ın çatı şirketi olan Meta Platform INC.'ye devretmiştir.[258]

Cambridge Analytica ise psikografik tekniklerden, Aleksandr Kogan'ın oluşturduğu *"This is Your Digital Life"* adlı uygulamanın topladığı psikolojik veriler vasıtası ile yararlanmıştır. Christopher Wylie, Aleksandr Kogan'ın SCL'e Trinidad ve Tobago projesi ile dâhil olduğunu ve SCL'den, projenin planlamasına yardımcı olmak karşılığında veri istediğini ifade etmiştir.[259] Kogan ve Wylie; Psikoloji, Antropoloji ve Sosyoloji gibi sosyal bilim alanlarının ölçülmesindeki zorluklarından kaynaklanan sayısal veri eksikliğini, sosyal medyanın sağladığı daha geniş örneklem uzayı

---

[255] Wu Youyou, Michal Kosinski, David Stillwell, "*Computer-based Personality Judgments are More Accurate Than Those Made by Humans", Proceedings of the National Academy of Sciences, C.112, S.4 (2015):1. 1036–1040.* doi:10.1073/pnas.1418680112.

[256] *a.g.e.*,4.

[257] Sandra Matz, Ruth Appel, Michal Kosinski, "Privacy in the Age of Psychological Targeting", *Current Opinion in Psychology*, (2019): 1. S2352250X19301332–. doi:10.1016/j.copsyc.2019.08.010.

[258] Google Patents, "Determining User Personality Characteristics From Social Networking System Communications and Characteristics", US13/608,943, 10.09.2012, https://patents.google.com/patent/US8825764B2/en. [Erişim Tarihi: 19.12.2022].

[259] Wylie, *a.g.e.*, 111.

fırsatından yararlanarak, çok fazla kişinin büyük miktarda kişisel verisi yardımıyla algoritmik olarak çözmeyi ve bu şekilde *"hesaplamalı psikoloji"* ve "hesaplamalı sosyoloji" alanlarında çığır açacak bir buluş yapmayı hedeflemişlerdir.[260] O dönemde Cambridge Üniversitesi Psikometri Laboratuvarı'nda psikolojik modellemeler üzerinde çalışan Kogan'ın, psikolojik özelliklerin sayısal modellemesi konusundaki uzmanlığı[261], Cambridge Analytica şirketinin bu modellemeleri geliştirmesi için oldukça elverişli bir durum meydana getirmiştir. Şirket, bazı kamu kurumlarından sağladığı demografik veriler ile sosyal medya ve diğer internet açık kaynaklarından edindiği kişisel verileri ve sahadaki anket ve araştırmalardan edindiği verileri bir psikografik modelleme üzerinde birleştirmiş ve *"algoritmaları eğiterek"* bunları kişisel hedefleme maksadıyla kullanmıştır.

Öte yandan Cambridge Analytica CEO'su Alexander Nix, 2016 yılında katıldığı Concordia Zirvesi'nde *"Büyük Veri ve Psikografinin Gücü"* konulu bir sunum gerçekleştirmiştir. Nix sunumda özetle Cambridge Analytica'nın, dünya liderlerine ve iş dünyasına büyük verinin gücü ve psikografi üzerinden veri analizi ile nasıl bir propaganda ve reklam hizmeti verdiğinden söz etmiştir.[262] Kitle hedefleme ve veri modelleme yaklaşımını psikolojik profil ile birleştirerek anlatan Nix, bunun geleneksel propoganda ve reklam modellerinden daha etkili olduğunu anlatmıştır. Zirve'deki sunumu sırasında, Cambridge Analytica'nın 2015'te ABD senatörü Ted Cruz'a ve 2016 ABD başkanlık seçimlerinde Donald Trump'a başkanlık seçimi kampanyası için hizmet verdiğini ifade etmiştir.[263] Nix, psikografik bilginin ehemmiyetini *"günümüzde kitle iletişimi çoğunlukla demografi ve jeografi üzerinden kurgulanıyor oysa bu, buz dağının görünen kısmıdır. Hedef kitle hakkında analiz yaparken nokta atışı tespitler yapabilmek için psikografik bilgileri gereklidir"* sözleriyle ifade etmiştir. Nix, Cambridge Analytica'nın, psikografi üzerine çalıştığını ve seçmenlere uygun seçim

[260] Wylie, *a.g.e.*, 111- 113.

[261] Wylie, *a.g.e.*, 109.

[262] Concordia, *a.g.e.*, https://www.youtube.com/watch?v=n8Dd5aVXLCc. [Erişim Tarihi: 20.10.2020].

[263] *a.g.e.*, https://www.youtube.com/watch?v=n8Dd5aVXLCc. [Erişim Tarihi: 20.10.2020].

propagandası üretmek için Beş Faktörlü Kişilik Modeli'ne (The OCEAN) başvurduklarını ifade etmiştir. Beş Faktörlü Kişilik Modeli ise kısaca şöyledir;[264]

- Açıklık: Sanata teveccühe, hisse, maceraya, atipik fikirlere, tahayyül etmeye, ve deneyimlemeye elverişlilik.
- Sorumluluk: Öz disiplin göstermeye meyyal olma, başarı için azmetme, sorumluluk şuuruyla hareket etme ve planlı hareket etme.
- Dışadönüklük: Enerjiklik, olumlu duygular ve diğerlerinin ortaklığını ve teşvikini aramaya meyilli olma.
- Uyumluluk: Şüpheci ve agresif olmaktan çok merhametli ve yardımsever olmaya meyyal olma.
- Duygusal dengesizlik (Nevrotizm): Öfke, bunalım, kaygı, alınganlık gibi agresif duygulara kolayca çekilme meyli.

Sunumda Nix, Cambridge Analytica'nın bu verilerden yola çıkarak aynı argümanı, bir gruba nevrotizmi tetikleyecek biçimde servis ederken diğer bir gruba ise uyumluluk ve sorumluluk gibi kişilik özelliklerini tetikleyecek şekilde sunduğunu ifade etmiştir. İhbarcı Christopher Wylie ise söz konusu seçmen manipülasyon tekniklerini, nevrotik ve komplocu yatkınlıkları olan insanları tanımlayıp hedeflemek suretiyle bu özellikleri harekete geçirecek propaganda içerikleri yayarak gerçekleştirdiklerini ve Cambridge Analytica'nın Facebook'tan alınan veriler ile çoğu durumda, kullanıcıların davranışlarını kendi eşlerinden daha iyi tahmin edebildiğini ve firmanın bu bilgiyi Cumhuriyetçi Parti içindeki insanları fiilen radikalleştirmek için kullandığını ifade etmiştir.[265]

4.3. 2016 ABD Başkanlık Seçimlerine Müdahalelerin Yargılama Süreci

Cambridge Analytica'ın yanı sıra Rusya menşeli Internet Research Agency (IRA) kuruluşu da, 2016 ABD başkanlık seçimlerine müdahale iddiasıyla yargılamaların taraflarından olmuştur. Bu konu başlığı altında 2016 ABD başkanlık seçimlerine müdahaleye ilişkin öne çıkan yargılama ve raporlar incelenecektir.

---

[264] Tayfun Doğan, ''Beş Faktör Kişilik Özellikleri Ve Öznel İyi Oluş'', *Doğuş Üniversitesi Dergisi*, C.14, S.1 (2013): 56-57.

[265] Wylie, *a.g.e.*, 204.

ABD'de, Başsavcı Yardımcısı Rod J. Rosenstein'in, eski Federal Soruşturma Bürosu (Federal Bureau of Investigation/ FBI) direktörü Robert S. Mueller'i, Rus hükümetinin 2016 ABD başkanlık seçimlerine müdahalesi iddialarını incelemek üzere danışman olarak atamıştır. Mueller, 2001 ve 2013 yılları arasında Obama hükümeti de dâhil olmak üzere hem Demokrat hem de Cumhuriyetçi başkanlara hizmet vermiştir.[266] Mueller Raporu 2 ciltten oluşmaktadır. Birinci cilt, Rusya'nın 2016 ABD başkanlık seçimlerine müdahalesi ve Trump Kampanyası ile etkileşimleri hakkında Özel Danışman tarafından yürütülen soruşturmanın olgusal sonuçlarını ele almıştır. İkinci cilt ise, FBI'nın, 2016 ABD başkanlık seçimlerine Rusya müdahalesine yönelik soruşturmasına ve ilgili konulara yönelik Başkan'ın eylemleri ile Özel Danışman'ın soruşturmasına yönelik eylemlerini ele almıştır.[267]

- Mueller Raporu'nda çalışmaya göre öne çıkan maddeler şunlardır:

- Rus hükümeti, 2016 ABD başkanlık seçimlerine; birincisi, Donald Trump'ı desteklemek ve Hillary Clinton'ı itibarsızlaştırmak, ikincisi ise Rus istihbarat servisi tarafından Clinton kampanyasında çalışan kuruluşlara, çalışanlara ve gönüllülere karşı bilgisayar korsanlığı olmak üzere iki operasyon ile kapsamlı ve sistematik bir şekilde müdahale etmiştir.[268]
- Internet Research Agency (IRA)/ Glavset, ABD'de siyasi ve sosyal konulardaki anlaşmazlıkları derinleştirmek ve kışkırtmak maksadıyla tasarlanan bir sosyal medya kampanyası yürütmüştür.
- IRA, merkezi St. Petersburg kentinde bulunan, Rusya'nın siyasi ve ticari çıkarlarına hizmet etmek maksadıyla *"troller"* vasıtasıyla sosyal medyada etki operasyonları yürüten ve Rus oligark Yevgeniy Prigozhin ile bağlantıları olan bir şirkettir.[269]
- IRA, Concord Management and Consulting LLC ve Concord Catering dâhil olmak üzere Yevgeniy Prigozhin'in kontrolü altında olan Rus kuruluşlar tarafından finanse

---

[266] Rebecca R. Ruiz, "Robert Mueller, Former F.B.I. Director, Is Named Special Counsel for Russia Investigation", *The New York Times*, 17 Mayıs 2017, https://www.nytimes.com/2017/05/17/us/politics/robert-mueller-special-counsel-russia-investigation.html. [Erişim Tarihi: 11.12.2022].

[267] Special Counsel Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", *U.S. Department of Justice*, (2019): 1.

[268] *a.g.e.*, 1.

[269] *a.g.e.*, 4.

ediliyordu ve Rus güvenlik servisleri tarafından sosyal medyada *"hayali kişilikler"* (troller) vasıtasıyla, ABD vatandaşlarını ve *"uluslararası ilişkilerin gidişatını"* etkilemek maksadıyla yürüttüğü aktif önlemlere (активные мероприятия), 2014 gibi erken bir tarihte başlamıştır.[270]

- 2014 yılında istihbarat toplama faaliyetleri yürütmek maksadıyla ABD'ye giden ve IRA ile olan bağlantılarını gizleyen, ABD vatandaşı kılığına bürünen IRA çalışanları, açtıkları sosyal medya hesapları üzerinden yaptıkları paylaımlarla oldukça geniş kitlelere ulaşmışlardır.
- Kasım 2017'de bir Facebook temsilcisi, Facebook'un Ocak 2015 ile Ağustos 2017 arasında toplu olarak 80.000 gönderi yapan 470 IRA kontrollü Facebook hesabı tespit etmiştir, Ayrıca Facebook'un, IRA'nın Facebook hesapları aracılığıyla 126 milyon kişiye ulaştığı tahmin edilmektedir, 6 Ocak 2018'de Twitter'ın, IRA kontrolündeki 3.814 Twitter hesabı tespit edilmiş ve Twitter, IRA kontrolündeki bir hesapla temas halinde olabileceği değerlendirilen yaklaşık 1,4 milyon kişiyi bildirmiştir.[271]
- IRA'nın ABD operasyonları, *"Project Lakhta"* olarak bilinen daha geniş bir iç içe geçmiş operasyonlar dizisinin bir parçasıdır.[272]

Federal Ticaret Komisyonu (FTC) Raporunda öne çıkan maddeler şunlardır:

- Cambridge Analytica şirketi nezdinde Alexander Nix ve Aleksandr Kogan'a müteselsilen, *"GSRApp adlı uygulama vasıtası ile, siyasi ve ticari hedefli reklam amaçlarıyla Facebook kullanıcılarından kişisel bilgileri toplamaya yönelik aldatıcı eylem ve uygulamalarından*" müteselsilen sorumludur.[273]
- Davalıların, Facebook'un Graph uygulama programlama arabirimi ("Graph API") vasıtasıyla, uygulamayla doğrudan etkileşim kuran yaklaşık 250.000–270.000 Facebook kullanıcısından ve ayrıca 50–65 milyon Facebook kullanıcısından Facebook kullanıcı profili verilerini toplamıştır.[274]

---

[270] *a.g.e.*, 14.

[271] *a.g.e.*, 15.

[272] *a.g.e.*, 16.

[273] United States Of America Before The Federal Trade Commission, "In the Matter of Cambridge Analytica LLC", 182 3107, 1.

[274] *a.g.e.*, 1.

- Alexander Nix, hem SCL Elections direktörü hem Cambridge Analytica CEO'su olan bir Birleşik Krallık vatandaşıdır ve Aleksandr Kogan, Eylül 2018'e kadar Cambridge Üniversitesi Psikoloji Bölümü'nde kıdemli araştırma görevlisi ve öğretim görevlisi olarak görev yapan ve burada Cambridge Prosociality and Well-Being Lab'ı ("CPW Lab") kuran ve yöneten bir ABD vatandaşıdır.[275]
- Facebook kullanıcılarının profil bilgileri; deneyimlere açıklık, vicdanlılık, dışadönüklük, uyumluluk ve nevrotiklik yönünden ölçüm yapan "OCEAN" ölçeğine göre, kullanıcının kişilik özelliklerini başarılı bir şekilde tahmin etmek için kullanılabilir.[276]
- Cambridge Analytica'nın çalışmaları sırasında, herkese açık olan Facebook profillerindeki beğenilen sayfalar ve yapılan diğer beğeniler aracılığıyla, bireylerin kişiliğini tahmin edebilen algoritmalar geliştirilmiştir. *"Örnek olarak, How to Lose a Guy in 10 Days, George W. Bush ve rap ve hip-hop ile ilgili Facebook sayfalarını beğenmek, muhafazakâr ve gelenekçi bir kişiliğe bağlanabilir."*
- Facebook; bünyesindeki Graph API (v1) uygulaması ile, kullanıcıların Facebook bilgileriyle oturum açma işlemi sonrasında geliştiricilerin uygulamasını veya web sitesini doğrudan yükleyen veya *"bunlarla başka bir şekilde etkileşimde bulunan"* uygulama kullanıcılarının yanı sıra, onların Facebook arkadaş listesindeki kişilerin de Facebook profil verilerinin toplanmasına olanak tanımıştır. Facebook daha sonra arkadaş verilerine erişim iznini kaldırdığı Graph API (v2)'yi duyurmuş olsa da, Kogan Graph API (v1) döneminde elde etmek istediği verileri zaten elde etmişti.

Kolombiya Bölgesi Büyük Jüri heyeti, (The Grand Jury for the District of Columbia) 13 Rus kişi ve kuruluşunu 2016 ABD Başkanlık Seçimleri'ne müdahale ile suçlamıştır. Raporta Internet Research Agency'den "Organizasyon" olarak söz edilmektedir. Bu çalışmada söz konusu şirketten "IRA" olarak söz edilecektir.

- Raporda öne çıkan maddeler şunlardır;

[275] *a.g.e.*, 2.

[276] *a.g.e.*, 2.

- Internet Research Agency LLC, seçimlere ve siyasi süreçlere yönelik müdahale operasyonları düzenleyen bir Rus kuruluşudur.[277]
- Sanıklar 2014'ten bu yana, kasıtlı olarak komplo kurmuşlardır.[278]
- Internet Research Agency, Yevgeniy Vıktorovich Prigozhin'den ve Concord Management And Consultıng LLC ile Concord Catering şirketlerinden faaliyetleri için fon almıştır.[279]
- IRA, Rus kimliklerini "VPN" vasıtasıyla gizlemek üzere ABD sınırları içerisinde bulunan bilgisayar sunucularından yer satın almıştır.[280]
- IRA çalışanları, ABD vatandaşlarının sosyal güvenlik numaralarını ve doğum tarihlerini vatandaşların bilgi ve rızası olmaksızın ele geçirmişler ve kullanmış ve bu şekilde bir dijital ödeme hizmeti sağlayıcısı olan PayPal'da hesap açarak sahte sürücü belgeleri de dâhil olmak üzere sahte kimlik belirleme araçları oluşturarak ve kurbanların kimliklerini kullanarak IRA kontrolündeki sosyal medya hesaplarında yayınlanmışlardır. Ayrıca, sosyal medya sitelerinde hesap açmak ve reklam satın almak gibi işlemlerde bu kimlik bilgilerini kullanmışlardır.[281]
- IRA çalışanları ayrıca, sahte ABD kişilikleri yaratmak ve ele geçirdikleri gerçek ABD kimliklerini kullanmak suretiyle ABD'li aktivistler gibi davranarak sosyal medya sayfaları ve grupları yönetmişlerdir.[282]
- Sanıklar ve işbirlikçileri, dolandırıcılık ve aldatma yoluyla yüzlerce sosyal medya hesabı oluşturmuş ve hayali (fake) ABD kişilikleri ile ABD'de *"kamuoyu liderleri/ kanaat önderleri"* haline getirmek için kullanmışlardır[283]
- IRA çalışanları bu eylemleri ABD gece ve gündüz vardiyası ve ABD tatil listelerine göre hareket ederek gerçekleştirmiştir.

---

[277] In The United States District Court for The District of Columbia, "Internet Research Agency Indictment", (Washington, DC: U.S. Department of Justice, 2018): 2. https://www.justice.gov/file/1035477/download. [Erişim Tarihi: 10. 11. 2022].

[278] *a.g.e.*, 3.

[279] *a.g.e.*, 3.

[280] *a.g.e.*, 3.

[281] *a.g.e.*, 16.

[282] *a.g.e.*, 3.

[283] *a.g.e.*, 33.

- IRA çalışanlarına, *"radikal grupları, sosyal ve ekonomik durumdan memnun olmayan kullanıcıları ve muhalif toplumsal hareketleri destekleyerek siyasi yoğunluk yaratma"* ve ABD'nin ekonomik sorunları ve dış politika meseleleri gibi konularda paylaşımlar yapmaları talimatı verilmiştir.[284]
- Sanıklar ve işbirlikçileri, @TEN_GOP (Tennessee GOP) Twitter hesabı gibi çok sayıda taklit sosyal medya hesabı oluşturmuşlardır.[285]
- Sanıklar ve işbirlikçileri, sosyal medyada yürüttükleri operasyonların etkisini ölçmek için sosyal medya üzerinden yayınladıkları içeriklerin performansını takip etmişlerdir.[286]

Web 2.0 dönemi ile var olan sosyal medya, gerek kullanıcılara erişim gerekse büyük veri analitikleri ve psikografi yöntemlerinin algoritmalara entegre edilmesiyle aynı zamanda bir istihbarat toplama ve aksiyon alanı hâline gelmiştir. Cambridge Analytica vakasının yöntemleri ve özellikle dış kaynaklı seçim müdahalesi nezdinde dâhil olduğu faaliyetleri, sosyal medyanın örtülü operasyonlara yeni ve elverişli bir zemin olduğunu ortaya koymuştur.

[284] *a.g.e.*, 34.

[285] *a.g.e.*, 37.

[286] *a.g.e.*, 15.

5. SOSYAL MEDYADA ÖRTÜLÜ OPERASYONUN ANALİZİ

Örtülü operasyonların bir dış politika aracı olarak tercih nedeni olmasını sağlayan en önemli unsurlardan biri makul inkâr edilebilirlik olgusudur. Siber uzay, gerek fiziki yapısı gerekse anonimliğe sağladığı katkı nedeniyle makul inkâr edilebilirlik konusunda avantaj sağlamaktadır. Web 2.0 dönemi ile sosyal medyanın var olması, siber iletişimde hem daha fazla insana ulaşma imkânı sağlamış hem de dezenformasyonun yayılması ve bunun anonim kimlikle yapılabilmesi yönünden avantaj sağlamıştır. Fakat sosyal medyayı örtülü operasyonlara elverişli hâle getiren siber uzay faktörünün yanı sıra, avantajı arttıran teknolojik gelişmeler ve bu gelişmelerle bir takım metodolojilerin modernizasyonu da söz konusudur. Makine öğrenmesi, doğal dil işleme, yapay sinir ağları gibi yapay zekâ teknikleri ile oluşturulan yeni tekniklerin yanı sıra sosyal medya verilerinin büyük veri analitiklerine sağladığı katkı ve psikografi alanındaki mikro hedefleme formüllerinin algoritmalara entegre edilmesi de sosyal medyayı örtülü operasyon açısından avantajlı bir zemin olarak öne çıkarmaktadırlar. Bu bilgiler ışığında bu bölümde sosyal medyayı örtülü operasyon için elverişli hâle getiren en avantajlı unsurun yapay zekâ, büyük veri analitikleri ve psikografi seçeneklerinden hangisi olduğu problemi, Rakip Hipotezlerin Analizi ve Analitik Hiyerarşi Süreci ile analiz edilecektir.

5.1. İstihbarat Analizi ve Bilişsel Tuzaklar

İstihbarat analizinde sezgi ve öngörüler, hızlı kararlar almanın elzem olduğu acil koşullarda ve proaktif kararlar almak gerektiğinde bazen günü kurtarabiliyor olsa da, tek başına zihin ve öngörülerden yararlanmak yanıltıcı sonuçlar doğurabilmektedir. Analiz sürecinde *"şeytanın avukatlığı",* empat bir yaklaşım, sağduyu ve objektiflik, sağlıklı bir analiz süreci ve daha isabetli bir yorum için son derece önemlidir. Sherman Kent, istihbarat raporlarını sürekli olarak göz ardı eden müşterinin, bu eğiliminin sezgilerinden kaynaklı olduğunu, dolayısıyla akıl ve bilimsel yönteme sırt

çevirdiğini değerlendirmiştir.[287] William F. Brei, istihbarat analizinin doktriner bir çerçevede incelenmesi gerektiğini savunmuş ve *"ilkelere dayanmayan sezgi, gereksiz hatalara ve desteklenemez sonuçlara yol açar"* sözüyle, başarılı sonuçlara götürecek sezginin titiz bir eğitim ve temel ilkelere bağlılığın doğal bir sonucu olduğunu ifade etmiştir.[288] Bununla birlikte istihbarat analizi gibi yüksek kıymete haiz konularda insan zihni karmaşık yapısı itibariyle, tek başına yaslanıldığı durumlarda büyük tehlikeleri gözden kaçırma yahut zamansız alarm durumlarına sebebiyet verebilecektir. Emarelerin tüm yönleri ile güçlü bir bilgi ve sağlama süzgecinden geçirilmesi ve bir metodoloji takip edilmesi isabetli bir analizin temel ihtiyaçlarındandır. Başvurulan metodoloji, analisti bilişsel tuzak ve önyargılardan uzak tutacak güçlü bir algoritmaya sahip olmalıdır. Analistlerin, verileri daha isabetli bir analitik süreçten geçirmeleri için bir dizi analiz yöntemi mevcuttur. Richards Heuer'in derlediği "Yapılandırılmış Teknik Analizler" çalışması, bu bağlamda çok çeşitli bir metodoloji seçeneği sunmaktadır.

Çalışmanın bu bölümünde, önceki bölümlerde yer alan bilgiler ışığında sosyal medyada örtülü operasyonun stratejik istihbarat analizi gerçekleştirilecektir. Söz konusu problem, öncelikle Rakip Hipotezlerin Analizi (ACH) ile eldeki veri ve bilgiler ışığında analiz edilecek ve ardından Analitik Hiyerarşi Süreci (AHP) ile, yazarın ACH analizi sürecinde verdiği kararların bilişsel ağırlık noktaları tespit edilecek ve analizin tutarlılığı test edilecektir. AHP metodu ayrıca, subjektif yargıların nesnelleşmesi adına faydalı bir adımdır. Böylece elde edilen analiz daha küçük bir resimde toparlanmış bir görüntüye kavuşacaktır.

5.2. Stratejik İstihbarat

İstihbarat, doğasındaki gizlilik olgusu nedeniyle üzerinde ittifak edilen tek bir tanımlamaya sahip değildir ve bilimsel literatürdeki tanımlamaları oldukça zengindir. Bu tanım çeşitliliğinde, devletlerin istihbarat teşekküllerinin farklı ekol ve tarzlarının, istihbarat felsefelerinin ve mimarilerinin ve stratejik kültürden gelen uygulamalarının

---

[287] Sherman Kent, "Producers and Consumers of lntelligence", *Strategic Intelligence for American World Policy* (Hamden: Archon Books, 1965), 206.

[288] William F. Brei, *a.g.e.,* 48.

da payının olması muhtemeldir. Ekseriyetle meslekî geçmişi olan istihbaratçıların epizodik yaklaşımları, tanımlamalara kendi gözlemlerini katmıştır ve gizliliğin sebep olduğu paradoks, bunları değerlendirmeyi oldukça zorlaştırmaktadır. Her ne kadar Türkçe literatürde "ölü operasyonlar"[289] olarak tanımlanan, ifşa olmuş yahut başarısızlığa uğramış istihbarat öyküleri mevcut olsa da, hâlâ sır perdesi aralanmamış çok sayıda faaliyet ve bilginin de olduğu göz ardı edilmemelidir. Michael Warner, gizliliğin neden olduğu bu paradoksun, orijinal belgelere erişimi olmayan dış araştırmacılar ile meslekî geçmişi ve kısmen de olsa orijinal belgelere erişim imkânı olan iç araştırmacıların tanımlamalarındaki farklılıktan kaynaklandığını vurgulamış ve bu nedenle istihbaratın tanımı gereği bilime direndiğini ifade etmiştir.[290]

Abram Shulsky, istihbaratı temelde, karşı tarafın gizlemeye çalıştığı bilgilere ulaşma çabası olarak yorumlamıştır.[291] Warner ise, *"devletlerin, kendilerine zarar verebilecek diğer ulusları yahut hasımları yumuşatmak, etkilemek veya yalnızca anlamak amacıyla gizlice yürüttükleri faaliyetler"* olarak tanımlamıştır.[292] Tomislav Dokman, nicel ve nitel içerik analizi yöntemiyle istihbarat teriminin 35 bilimsel, uzman ve kurumsal tanımını analiz ettiği makalesinde, nicel analizden elde ettiği verilere göre tanımlamalarda en çok kullanılan kelimenin "enformasyon" olduğunu, bunu sırasıyla "son kullanıcı/karar verici", "harekete geçirilebilir karakter", "yabancı ülkeler" ve "bilgi" terimlerinin takip ettiğini bulmuştur.[293] Bu ifadeye göre istihbarat temel olarak, düşman veya müttefik ülkeye ait gizli enformasyon ve bilgilerin toplanması, işlenmesi, analiz edilmesi ve müşteriye (istihbaratın sunulacağı hükümet, devlet başkanı, siyasetçi vb) sunulması sürecidir denilebilir.

Tarih profesörü ve eski CIA analisti Sherman Kent, *"istihbarat bilgidir"* demiştir ve bu bilgiyi, üst düzey ulusal politikayı temel alan ve diğer devletler ile ilgili sahip

---

[289] Milli Savunma Üniversitesi İstihbarat Araştırmaları bölümü ders notları.

[290] Michael Warner, "Sources and Methods for the Study of Intelligence", *Handbook of Intelligence Studies,* ed. Loch. K. Johnson (Oxon: Routledge, 2007), 17.

[291] Abram Shulsky, "Toward a Theory of Intelligence", *Silent Warfare: Understanding the World of Intelligence*, 2. bs (New York: Brassey's US, 1993), 172.

[292] Warner *a.g.e.,* 17.

[293] Tomislav Dokman, "Defining The Term 'Intelligence' - Insight into Existing Intelligence Knowledge", *Informatologia,* C.52, S.3-4 (2019): 194- 195. DOI: 10.32914/i.52.3-4.7.

olunması gereken bilgi olarak tanımlamıştır.[294] İstihbarata yönelik bilgi, Loch K. Johnson'un ifadesiyle *"ortalama bir gazete okuyucusunun ilgisini çekebilecek şeylerin ötesinde"* olan bilgileri ifade eder.[295] İstihbâri bilgi, herkesin ulaşabildiği açık kaynaklardan edinilen bilgi ile gizlilik ihtiva eden veri ve enformasyonun harmanlanmasıyla elde edilir. Gizlilik burada anahtar kavramdır çünkü bir devletin gizlemeye gayret gösterdiği bilgiler, açığa vurulduğunda o devletin stratejisini, güçlü yönlerini ve aşil topuğunu ortaya çıkarabilirken, gizli bilgiyi ele geçiren tarafa da bir güç transfer edebilir, analiz ve strateji geliştirme aşamalarında analistin ve dış politika faaliyeti aşamasında karar vericinin elini güçlendirebilir. Bu noktada ihtiyaç duyulan gizli bilgilerin espiyonaj faaliyetleriyle ele geçirilmesi yahut bir ihtiyatsızlık nedeniyle ifşa olması bazı durumlarda mümkün olsa da, birçok durumda çok iyi saklanan bu bilgilere erişim imkânı olmaz. Bu noktada istihbarat analistlerine, eldeki veriler ışığında, güçlü bir bilgiye ve analitik bir çalışmaya dayalı sezgiler vasıtasıyla, yapbozun eksik parçalarını tamamlama sorumluluğu yüklenir. Johnson'un ifadesiyle istihbarat başarısızlıkları, yapbozun eksik kalan parçalarının bir sonucudur.[296] Stratejik istihbarat, istihbaratın çeşitli kaynaklardan çeşitli tekniklerle toplanmasından sonra analiz edilip geleceğe yönelik öngörü sunma çalışmasıdır. Stratejik istihbarat süreci önemlidir fakat aynı oranda zordur çünkü aynı anda hem eldeki istihbaratın doğru olması, hem analistlerin konu ile ilgili oldukça bilgili olması hem de eldeki veriler ışığında geleceğe yönelik doğru tahminler yapmayı gerektirir ki bunlardan birinin eksikliği tüm süreci akamete uğratabilir.

Devletlerin, dış politikalarını şekillendirme ve hamlelerini belirleme sürecinde, kendilerini tanıdıkları kadar yabancı devletleri de tanımaları avantajlarını ve gücünü arttırır. Thrasymakhos, Sokrates ile gerçekleştirdiği bir diyalogda *"doğruluk, güçlünün işine gelendir"* demiştir.[297] Burada kast edilen güçlü, iktidar erkidir.

---

[294] Sherman Kent, "Intelligence is Knowledge", *Strategic Intelligence for American World Policy* (Hamden: Archon Books, 1965), 3.

[295] Johnson, "Introduction", 2.

[296] *a.g.e.*, 3.

[297] Platon, "Birinci Kitap", *Devlet*, çev. Sabahattin Eyüboğlu ve M. Ali Cimcoz (Beyoğlu: Türkiye İş Bankası Kültür Yayınları, 1999), 338c- 339a.

Hans Morgenthau, *"bir siyasi parti lideri, parti üyelerinin eylemlerini kendi iradesine göre şekillendirebildiği sürece siyasi güce sahiptir"* demiştir.[298] Bu durum uluslararası alan perspektifinde değerlendirildiğinde, devletler arasında yaptırım kâbiliyeti de, gücü kimin elinde bulundurduğuna göre şekillenecektir.

Eski CIA analisti Ray Steiner Cline, Algılanan güç için şöyle bir formül geliştirmiştir:[299]

Algılanan Güç = (K + E + A) * (S + U)

K= Kritik kütle: Nüfus + bölge

E= Ekonomik kapasite

A= Askerî kapasite

S= Stratejik hedef

U= Ulusal stratejiyi takip etme arzusu

Formülden anlaşıldığı üzere, güç çarpanının bir tarafını nüfus, bölge, ekonomik kapasite ve askerî kapasite oluştururken, diğer tarafını stratejik hedef ve ulusal stratejiyi takip etme arzusu oluşturmaktadır. Denklemin sol tarafındaki faktörlerin bilgisine ulaşmak kısmen daha mümkünken, sağ tarafındaki stratejik hedef ve ulusal stratejiyi takip etme arzusu faktörlerinin bilgisine erişmek zordur ve toplanan parçalı bilgiler analize muhtaçtır. Abram Shulsky, diplomatlara yahut komutanlara fayda verecek en iyi türden bilginin dahi analize muhtaç olduğunu ifade etmiş ve toplanan bilgiler genellikle parçalı ve belirsiz olduğu için analiz üretmenin zor olduğunu, yabancı bir hükümetin yahut siyasi örgütün gelecekteki niyet, yetenek ve eylemlerini tahmin etmenin oldukça zorlu bir süreç olmasının yanında istihbarat sürecinin de

[298] Hans Morgenthau, "International Politics As a Struggle for Power", *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1948), 14.

[299] Ray Steiner Cline, "Elements of Power: The Formula", *World Power Trends and U.S. Foreign Policy for the 1980s* (New York: Routledge, 2019), 39- 40.

hayati bir parçası olduğunu vurgulamıştır.[300] 17. yüzyılda Francis Bacon, *"bilgi güçtür"* demiştir.[301] Aynı zamanda, insanlık tarihinin en eski strateji eserlerinden biri olarak kabul edilen Savaş Sanatı kitabında Sun Tzu da, "akıllı bir hükümdar ve iyi bir generalin saldırı ve fetih yapmasını, sıradan insanların erişiminin çok ötesindeki şeylere ulaşmasını sağlayan, önbilgidir" ifadesiyle, rakip hakkında edinilecek bilginin, bilgiyi edinen tarafa sağlayacağı güç bakımından ehemmiyetini vurgulamıştır.[302] İstihbarat kurumlarına ve analistlere bu noktada kritik seviyede önemli bir sorumluluk düşmektedir: bilgiye erişmek ve erişilen bilgiler uyarınca doğru bir analiz yapmak. Elbette burada kastedilen bilgi, doğru bilgidir. Zira, bir askı (tuzak/ dangle) ajanın yanıltıcı bilgi ulaştırması gibi birçok yöntemi olan hasım istihbarat servislerinin bir kontrespiyonaj faaliyetine maruz kalmış olmak, yapılacak istihbarat analizini temelinden sarsar ve zayıf temel üzerine sağlam bina inşa edilemeyeceği gibi yanlış bilgi üzerinden de doğru bir istihbarat analizi elde edilemez.

İstihbarat hataları bazı durumlarda devleti telafisi zor hatta imkânsız durumlara sürükleyebilmektedir. Stratejik istihbarat hakkında yazılmış kitap ve makalelerin çoğu, bu tür hataların sebep olduğu millî travmalardan izler taşımaktadır. Philip Davies, Ülkelerin istihbarat başarısızlıklarını açığa çıkaran kilit kötü deneyimlerinin, istihbaratın ne olması gerektiğine dair ulusal algıları yönlendirdiğini ifade etmiştir.[303] Örnek olarak, Amerikan tandanslı birçok stratejik istihbarat yazısında Pearl Harbor Baskını ve 9/11 saldırılarından çıkarılması gereken dersler ve bu vakalardan sonra ABD'nin istihbarata yaklaşımındaki dönüşümden bahsedilmiştir. İstihbarat örgütlerinin, olumsuz deneyimlerinden ders çıkarmaları ve revizyona gitmeleri önemlidir fakat devleti stratejik bir sürprizden korumak için, istihbarattan, özellikle stratejik istihbarattan söz ediliyorsa, bilginin erkenden temin edilmesi ve gerekli hamlelerin de önceden yapılması gerekir. Devletler ve milletler de, istihbarat

---

[300] Abram Shulsky, "What is Intelligence?", *Silent Warfare: Understanding the World of Intelligence*, 2. bs (New York: Brassey's US, 1993), 8.

[301] Heiner Müller-Merbach, "Francis Bacon's Praise: Knowledge, The Source of Power", *Knowledge Management Research & Practice,* C.3, S.1 (2005): 45. DOI:10.1057/palgrave.kmrp.8500048.

[302] Sun Tzu, *Savaş Sanatı*, çev. Tuğçe Ayteş (İstanbul: İlgi Kültür Sanat Yayıncılık, 2017), 99.

[303] Philip Davies, "Ideas of intelligence: Divergent national concepts and institutions", *Secret Intelligence: A Reader*, ed. Christopher Andrew, Richard J. Aldrich, Wesley K. Wark (Oxon: Routledge, 2020), 17.

servislerinden, bir saldırıyı yahut hasmâne bir girişimi gerçekleşmeden önce öğrenmesini beklerler. ABD literatüründe bunun tespiti için üretilen disiplin, *"göstergeler ve uyarılar (I & W)"* olarak adlandırılır.[304] Öte yandan, analistler bir stratejik sürprizi öngördüğünde ve hasım, sürprizin açığa çıktığını öğrendiğinde planı iptal edebilir. Buna "uyarı paradoksu" denir.[305] Uyarı paradoksu fenomeni, saldırgan bir girişimin öngörülerek ortadan kaldırılmasının başarısına değil, yanlış tahmin algısıyla karar vericinin nazarında istihbarat kurumunun ya da toplumun nazarında hükümetin yahut istihbarat örgütünün başarısızlığı algısına neden olur. Uyarı paradoksunun tehlikeli yönü, daha sonraki uyarıların göz ardı edilmesi ihtimalidir.

5.3. Sosyal Medyada Örtülü Operasyon

Üssel bir hızla artan dijitalleşme, sosyal medyayı birçok yönden örtülü operasyonlara elverişli hâle getirmiştir. Bunlardan biri, sosyal medya verilerinin diğer teknoloji temelli veriler ile birleştiğinde geleneksel istihbarat toplama tekniklerine nispetle toplum hakkında daha fazla enformasyon üretme kapasitesidir. Sosyal medyada herkese açık olarak paylaşılan veriler önemli bir veri kaynağıdır. Kullanıcıların ad, soyad, yaş, eğitim durumu, medeni durum, iş deneyimleri, ikamet edilen yer gibi bilgileri demografik veriler sağlarken, yaptıkları paylaşımların metin ve duygu analizleri önemli psikografik veriler sağlamaktadır. Kullanıcılar paylaşımlarını anonimleştirilmiş kimliklerle yapsalar dahi, kendi duygu durumlarını yansıttıklarından dolayı kolaylıkla bir mikro hedeflemenin odağı hâline gelebilmektedirler.

Web sitelerin, bazıları seçimlik olan bazıları söz konusu hizmetin alınması için zorunlu kılınan çerez politikaları ve mobil uygulamaların erişim izinleri, kullanıcıların akıllı telefonlarındaki hareket sensörleri, mikrofon, kamera ve telefonun dâhili hafızasında tutulan fotoğraf, video gibi çok çeşitli türlerden verilerinin yalnızca sosyal medya uygulamaları değil birçok mobil uygulama ve web sitesi tarafından da çekildiği anlamına gelmektedir. 2018 yılında bir grup araştırmacı, uygulamaların konum verilerini çekmek için erişim iznine tabi olurken, hareket, ışık ve yakınlık

---

[304] Loch. K. Johnson, *a.g.e.,* 3.

[305] William F. Brei, "Getting Intelligence Right: The Power of Logical Procedure", *Learning With Professionals,* (Washington DC: Joint Military Intelligence College, 2005), 54.

sensörlerinde herhangi bir erişim iznine tabi olmadıklarını ve inceledikleri 9 arama motorunun (Chrome, Edge, Safari, Firefox, Brave, Focus, Dolphin, Opera Mini, and UC Browser) bu sensörleri kullanıcı iznine tabi olmadan kullandıklarını saptamışlardır.[306] Söz konusu tarayıcılardan Firefox, bu erişim izinlerini kaldırmıştır. Araştırmacılar ayrıca, yaklaşık 1200 web sitenin "izleme, analitik toplama veya kitle tanımaya" yardımcı olmak için sensör verilerini kullandığını saptamıştır.

Elde edilen verilerden anlaşılan odur ki, sosyal medya ve sosyal medyanın ötesinde birçok web site de son derece kritik kullanıcı verilerine erişebilmektelerdir. Özellikle elde edilen verilerin psikografi ile tanımlanmasının, hedefleme olanaklarını arttırabildiği Cambridge Analytica vakasından da anlaşılmıştır. Bu doğrultuda, internet çağının, standart istihbarat toplama yöntemlerinin çok ötesinde bir veri ve enformasyon toplama pratiğine elverdiği anlaşılmaktadır.

Bir diğer husus, sosyal medyanın algı yönetimi ve propaganda seçimi için ulaşabildiği kişi sayısı bakımından ana akım medyadan daha avantajlı bir zemin olmasıdır.

5.4. Rakip Hipotezlerin Analizi (Analysis Of Competing Hypotheses – ACH)

Rakip Hipotezlerin Analizi (Analysis of Competing Hypoteses- ACH), Richards Heuer tarafından, istihbarat analizinde kullanılmak üzere geliştirilmiş bir tekniktir. Teknik, 20. yüzyılın bilim filozoflarından Karl Popper'ın *"yanlışlanabilirlik"* tezinden hareketle, hipotezler arasında en az yanlışlanabilir olan hipotezi en geçerli hipotez olarak kabul etme yaklaşımı ile formülize edilmiştir.[307] Adından da anlaşılacağı üzere ACH, birbirini tamamen reddeden hipotezlerin, kanıtlar vasıtasıyla sınanması sürecidir. Analiz sürecinde, özellikle istihbarat analizi stresli bir süreci içerebileceğinden, analist karar verme aşamasında birçok bilişsel önyargının kurbanı olabilir. Deneyimli bir analistin dahi geçmiş tecrübelerinin benzer veya yeni durumlarda zihnini kör etmesi muhtemeldir. Ayrıca bir alarm durumunun

[306] Lily Hay Newman, "Mobile Websites Can Tap Into Your Phone's Sensors Without Asking", *Wired,* 26 Eylül 2018, https://www.wired.com/story/mobile-websites-can-tap-into-your-phones-sensors-without-asking/. [Erişim Tarihi: 24.12.2022].

[307] Richards J. Heuer, Randolph H. Pherson, "Analysis of Competing Hypotheses", *Structured Analytic Techniques for Intelligence Analysis* (London: CQ Press, 2015), 201.

değerlendirilmesi mecburiyeti, stres altında ve kısa sürede karar verme zorunluluğunun bir tezahürü olarak analisti yine hızlı karar almaya çalışırken önemli ayrıntıları gözden kaçırmaya sürükleyebilir. Yahut eldeki belirli emarelerin zihinde kati bir kanaat oluşturması, başka kanıtları gözden kaçırmaya sebep olabilir. Bu ve benzeri durumlar, analiz sürecini akamete uğratır.

Heuer, analitik düşüncenin geliştirilebilir olduğunu iddia etmekte fakat bunun ancak üzerinde aktif olarak çalışılarak mümkün olabileceğini, bisiklet yahut araba sürmek gibi kas hafızasına benzer bir süreçle açıklamaktadır.[308] ACH, analistlerin eldeki problem ile ilgili tüm verileri, varsayımları ve boşlukları kullanarak mümkün olduğunca çok sayıda makul hipotezi belirlemesini ve ardından çürütmesini ister.[309]

5.4.1. Rakip Hipotezlerin Analizi (ACH) Metodolojisi

ACH, uygulamada aşağıda sunulan bir dizi metodolojiyi takip etmektedir; [310]

- Hipotezlerin tanımlanması: Hipotezler birbirini dışlamalı, tüm makul olasılıkları içeren bir hipotez listesi hazırlanmalıdır.

- Kanıtların ortaya konulması: Bu aşamada analist, tanımlanan hipotezleri destekleyen ve reddeden tüm argümanları ortaya koyarak bir kanıt listesi oluşturmalıdır.

- Matris oluşturulması: Bu aşamada, üstte satır olarak hipotezlerin, sol tarafta sütun olarak kanıtların yer aldığı bir matris oluşturulmalıdır. Bilgiler, hipotezlerle uyumluluk, tutarlılık, uygulanabilirlik ve alaka düzeyi bakımından titizlikle incelenmelidir. Bilgiler tutarlı ise matristeki uygun kutuya bir "C" (consistent) işareti konulur. Tutarsız ise bir "I" (inconsistent) işareti konulur. Bu hipoteze uygulanamaz ise "NA" (Not Applicable) işareti konulur. Kanıtlar hipotezler için çok tutarlı ise "CC", çok tutarsız ise "II" işareti konulur.

---

[308] Richards Heuer, "Our Mental Machinery", *Psychology of Intelligence Analysis* (CIA: Center for the Study of Intelligence, 1999), 2. ISBN 1 929667-00-0.

[309] Heuer ve Pherson, *a.g.e.,* 202.

[310] *a.g.e.,* 208.

- Bu aşamada, değerlendirmelerin yorumlanmasında farklılık gösteren noktalar gözden geçirilmeli, düzenleme gerektiren noktalar varsa tekrar değerlendirilmeli.

- Bu aşamada, hipotezler yeniden gözden geçirilmeli. Ayrı ayrı yazılan hipotezler birleştirilebilir yahut yeni bir hipotez matrise eklenebilir. Hipotezlerde revizyon yapılması durumunda, yeni hipotezler kanıtlar ile birlikte yeniden değerlendirilmelidir.

- ACH metodolojisi, doğası gereği, yanlışlanabilirlik üzerinden yorumlandığı için, bu noktada tutarsızlık puanları (I, II) toplanır ve en az yanlışlanan hipotez, geçici olarak en olası hipotez olarak değerlendirilir.

- Elde edilen sonucun hassasiyeti değerlendirilerek var olması muhtemel yanıltıcı bilgilerin varlığı sorgulanır ve elde edilen bilgiler tekrar gözden geçirilir. Bu noktada en olası görünen hipotezi destekleyen, dolayısıyla diğer hipotezleri en az olası kılan bilgiler ve kanıtlar titizlikle tekrar değerlendirilmelidir.

- Sonuç raporu: Bu aşamada yine yalnızca en olası hipotez değil, tüm hipotezlerin göreceli olasılıkları tekrar değerlendirilir. İlgili bilgilerden en tanısal olanlar, olası hipotezi zorlayıcı olarak nasıl destekledikleri noktasında değerlendirilmelidir.

- Gelecekteki gözlem için göstergeler ve kilometre taşlarının belirlenmesi: Bu aşamada iki liste oluşturulur. İlki, gelecekteki vakalara yahut analitik yargının geçerliliğini kanıtlamaya yarayacak ek araştırmalar vasıtasıyla geliştirilebileceklere odaklanan; ikincisi ise yargının doğru olma olasılığının düşük olduğunu yahut değiştiğini gösteren göstergelerin bir listesidir. Göstergeler doğrulanmalı ve sürekli olarak izlenmelidir. İleriye dönük bir stratejik sürprizle karşılaşılmaması açısından, bu madde önem arz etmektedir.

5.4.2. Rakip Hipotezlerin Analizi (ACH) Uygulaması

Çalışmanın bu aşamasında, Cambridge Analytica, IRA ve Team Jorge adlı kuruluşların gerçekleştirdiği yahut paydaş olduğu siyasi seçim müdahalelerindeki benzer yöntemleri göz önünde bulundurularak, yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil kaynağı olup olamayacağı sorunsalı analiz edilecektir. Söz konusu şirketlerin büyük miktarda veri elde etme, verileri analiz etme, veri odaklı hedefli propaganda üretme yöntemleri, söz konusu şirketlerin faaliyetleri

ile güncel teknolojik gelişmeler ve bilimsel çalışmalar bakımından bilgilerin ortaya konulmasıyla analiz edilecektir. Söz konusu şirketlerin kampanya yöntemlerinin oy davranışlarına etki edip etmediği konusunda görüş ayrılıkları söz konusu olduğundan[311], sosyal medyanın örtülü operasyonlara elverişli bir zemin olmadığı hipotezi de sınanacaktır.

- Analiz Sorusu ve Hipotezlerin Oluşturulması

ACH metodunun ilk aşaması olarak, analiz edilecek analiz sorusu ve hipotezler belirlenecektir. Bu çalışmanın analiz sorusu şudur: "Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir mi?"

Belirlenen analiz sorusu için şu hipotezler belirlenmiştir:

Hipotez 1: Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir.

Hipotez 2: Yapay zekânın, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir.

Hipotez 3: Sosyal medya örtülü operasyona elverişli bir zemin değildir.

Hipotezler ve analiz sorusundan oluşturulan matris aşağıdaki gibidir;

Tablo 5.1: ACH Analiz Sorusu ve Hipotezler.

Analiz sorusu: "Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir mi?"			
Hipotezler	Hipotez 1: Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsur olabilir.	Hipotez 2: Yapay zekânın, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir.	Hipotez 3: Sosyal medya örtülü operasyona elverişli bir zemin değildir.

Yazar tarafından oluşturulmuştur.

[311] Jamie Doward, Alice Gibbs, "Did Cambridge Analytica Influence the Brexit Vote and the US Election?", *The Guardian*, 04.03.2017, https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump. [Erişim Tarihi: 05. 02. 2023].

İkinci aşamada analiz sorusu ile ilgili kanıtlar sunulacaktır.

Örtülü operasyonların operasyonel başarıya ulaşabilmeleri için planlama aşaması ile elde edilen neticenin yüksek oranda tutarlı olması gerekir. Bu doğrultuda iyi bir planlama yapılabilmesi için istihbarat toplama aşaması oldukça önemlidir. Ardından gerçekleştirilen operasyonun bir etki yaratması elzemdir. Son olarak gerek operasyonun adımları gerekse operasyon için seçilen yöntem ve zemin, örtülü operasyonların başat maksatlarından biri olan makul inkâr edilebilirlik olgusunu desteklemelidir. Bu doğrultuda "Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir mi?" sorusuna yanıt olarak üretilen hipotezler, aşağıdaki kanıtlar doğrultusunda sınanacaklardır:

Kanıt 1: Erişim imkânı; İstihbarat toplama aşamasında sağladığı erişim kabiliyetini ifade etmektedir.

Kanıt 2: Etki imkânı; Etki operasyonlarının başarıya ulaşması ile ilgili varlık ve durumları ifade etmektedir.

Kanıt 3: Makul inkâr edilebilirlik; Operasyonun, operatör aktöre izi sürülemeyecek biçimde gerçekleştirilebilmesini ifade etmektedir.

Kanıtlara sunulan bilgiler şu şekildedir;

Kanıt 1: Erişim imkânı

Bilgi 1: Tahmine Dayalı Analitik ile örtülü operasyonları gerçekleştirmek için ihtiyaç duyulan verilerin algoritmalar vasıtasıyla yapılandırılıp geleceğe yönelik isabetli operasyon perspektifi sunması mümkündür.

Bilgi 2: Sosyal medya şirketlerinin kullanıcı verilerine erişimi kısıtlama yahut engelleme çabalarını aşarak büyük miktarda veri kazımak mümkündür.

Bilgi 3: Sosyal medya kullanıcılarının ürettiği büyük miktarda verinin isabetli olarak ve çok kısa sürede analiz edilmesi, makine öğrenmesi yöntemleri ile mümkündür.

Bilgi 4: Diğer istihbarat faaliyetleri olmaksızın sosyal medya verileri bir örtülü operasyon için yeterli değildir.

Kanıt 2: Etki imkânı

Bilgi 5: Cari dönemde yapay zekâ alanındaki gelişmeler ile sosyal medya kullanıcısı olarak oluşturulan sosyal robotlar, söylemin yayılması bakımından algı yönetimi ve dezenformasyona elverişliliği arttırmıştır.

Bilgi 6: Sosyal medyada mikro hedefleme teknikleriyle algı yönetimi, psikoloji alanındaki bilimsel çalışmalarla uyumludur.

Bilgi 7: Sosyal robotlar ile oluşturulan dezenformasyonun yayılması, gerçek kullanıcılar tarafından paylaşılmadığı sürece mümkün değildir.

Bilgi 8: Sosyal medyada yayılan dezenformasyonun yapay zekâ programları ile tespiti mümkündür.

Bilgi 9: Cari dönemde yapay zekâ uygulamaları, kullandığı dil tibariyle ürettiği içeriğin gerçek bir kullanıcınınkinden ayırt edilmesini oldukça güçleştirecek seviyede gelişmiştir.

Kanıt 3: Makul İnkâr Edilebilirlik

Bilgi 10: Yapay zekâ sistemleri, etkilenenler tarafından tespit edilemeyecek şekilde tasarlanabilir.

Bilgi 11: Cambridge Analytica vakası, sosyal medyada örtülü operasyonların bir şekilde açığa çıkabileceğini ispat etmiştir.

- Hipotezler ve Kanıtların Analizi

Kanıt 1: Erişim imkânı

Tablo 5.2: Bilgi 1 ACH Matrisi.

ERİŞİM İMKÂNI	**Hipotez 1**	**Hipotez 2**	**Hipotez 3**
Bilgi 1: Tahmine Dayalı Analitik ile örtülü operasyonları gerçekleştirmek için ihtiyaç duyulan verilerin algoritmalar vasıtasıyla yapılandırılıp geleceğe yönelik isabetli operasyon perspektifi sunması mümkündür.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

Örtülü operasyonların planlanmasında ilk olarak istihbarat toplama sonrasında elde edilen enformasyonu kıymetlendirme aşamalarının isabetli olması, operasyonel hedefe ulaşmak bakımından elzemdir. Bu doğrultuda, teknolojik gelişmeler, geleneksel bilgi toplama ve kıymetlendirme yordamlarına nispeten daha isabetli sonuçlar vermektedir. Sosyal medyanın hacim, hız ve çeşitlilik (3V) unsurlarını bir arada sağladığı büyük miktarda veri akışı elde edilen veri ve enformasyonun boyutunu geleneksel veri toplama imkânlarına nispeten dramatik ölçüde arttırmıştır. Elde edilen verilerin temizlenmesi, anlamlandırılması ve bu sonuçlardan bir içgörü elde edilmesi, Tahmine Dayalı Analitik (Predictive Analytics) ile mümkündür. Bu yöntem, geçmiş verilerin istatistiksel modellemesini, veri madenciliği teknikleri ve makine öğreniminin bir alt dalı olan derin öğrenme ile geleceğe yönelik bir öngörü elde etmeyi sağlar.[312] Sosyal medyada propaganda için oluşturulacak içerik, haber ve söylem akışlarının propagandayı akamete uğratacak olan geri tepmeye (blowback) sebebiyet vermeden operasyonel başarıya ulaşması bakımından bu yöntem elverişlidir.

Bu bilgiler ışığında, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezi ile örtüşmektedir. Bu doğrultuda "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır.

Tablo 5.3: Bilgi 2 ACH Matrisi.

ERİŞİM İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 2: Sosyal medya şirketlerinin kullanıcı verilerine erişimi kısıtlama yahut engelleme çabalarını aşarak büyük miktarda veri kazımak yapay zekâ ile mümkündür.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

Twitter'ın kullanıcı verilerine erişim için sunduğu API hizmetini kullanmadan açık kaynak kodlu TWINT (Twitter Intelligence Tool) ile Twitter'da hesap açma ve onaylama aşamasını atlayarak büyük miktarda veri çekmek mümkündür. GitHub'da

[312] Asaju ve diğ. *a.g.e.*, 96.

tanıtılmış olan söz konusu araç ile belirlenen konular, hashtagler, telefon numaraları, e- posta adreslerini içeren hassas veriler, beğenilen tweetler, takip edilen hesaplar gibi çok sayıda verinin Twitter doğrulaması olmadan kazınmasına olanak sağlanmıştır.[313] Söz konusu veriler, eğitilen algoritmalar ile hem toplumsal eğilimi takip etmeyi hem de mikro hedefleme algoritmalarının eğitilmesini mümkün kılabilir. Bu noktada öncelikli olarak elde edilecek veri çeşitliliği avantajı arttıracaktır. Sonrasında söz konusu verilerin psikografik segmentasyonu ile makine öğrenmesi ve doğal dil işleme gibi yapay zekâ programları vasıtasıyla eğitilen algoritmalar operatörlerin daha isabetli eylemlere yönelmelerini mümkün kılacaktır. Söz konusu örnek, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini desteklemektedir. Bu doğrultuda, "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır.

Tablo 5.4: Bilgi 3 ACH Matrisi.

ERİŞİM İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 3: Sosyal medya kullanıcılarının ürettiği büyük miktarda verinin isabetli olarak ve çok kısa sürede analiz edilmesi, makine öğrenmesi yöntemleri ile mümkündür.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

Sosyal medyada üretilen büyük miktarda akan verinin bir insan operatör tarafından çekilip analiz edilmesi oldukça zaman alması bakımından . Fakat makine öğrenmesi algoritmaları ile veri analizi çok daha kısa sürede verileri yapılandırılmış hale getirebilmektedir. Ayrıca sosyal medya her saniye ürettiği gerek görsel veriler gerek metinsel veriler gerekse konum verileri gibi farklı türdeki veri tiplerinin akışı yönünden dinamik bir ortamdır. Makine öğrenmesi ile dinamik ortamın hızına adapte olabilecek mimariler geliştirilmesi de mümkündür. Bu bilgiler, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini

[313] Twint Project, GitHub, https://github.com/twintproject/twint/blob/master/README.md. [Erişim Tarihi: 20.03.2023].

desteklemektedir. Bu doğrultuda, "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır.

Kanıt 2: Etki imkânı

Tablo 5.5: Bilgi 4 ACH Matrisi.

ETKİ İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 4: Diğer istihbarat faaliyetleri olmaksızın sosyal medya verileri bir örtülü operasyon için yeterli değildir.	**I**	**C**	**C**

Yazar tarafından oluşturulmuştur.

Cambridge Analytica, 2016 ABD Başkanlık seçimleri için ABD'ye sosyologlar ve antropologlardan oluşan saha çalışanları göndererek odak grup görüşmeleri yaptırmıştır. Bu şekilde sosyal medyada elde edilip anlamlandırılan verilerin test edilmesi gerekmiştir. Ayrıca Söz konusu şirket, Trinidad ve Tobago'da telekomünikasyon altyapılarına erişerek vatandaşlar ile ilgili bilgi toplamışlardır. Yine ABD dâhil birçok ülkede, seçmek kayıtları, banka verileri, gelir durumu, medeni durum gibi demografik verileri de ele geçirerek kurdukları sistemi bu veriler ile güçlendirmek durumunda kalmışlardır. Bu bilgiler, hipotez 2 ve hipotez 3'ü doğrulamakta ve hipotez 1'i yanlışlamaktadır.

Tablo 5.6: Bilgi 5 ACH Matrisi.

ETKİ İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 5: Cari dönemde yapay zekâ alanındaki gelişmeler ile sosyal medya kullanıcısı olarak oluşturulan sosyal robotlar, söylemin yayılması bakımından algı yönetimi ve dezenformasyona elverişliliği arttırmıştır.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

İsrail menşeli Team Jorge adlı şirketin, sosyal medyada Advanced Impact Media Solutions (AIMS) yazılımı ile oluşturulan otuz binden fazla bot hesap ile dezenformasyon yayıldığı ve otuz üç cumhurbaşkanlığı seçimini manipüle ettiği ortaya çıkmıştır.[314] Söz konusu şirketin oluşturduğu sosyal robotların ürettiği propagandist içerikler, çok sayıda gerçek kullanıcı tarafından paylaşılarak yayılmıştır. Bu bilgiler, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini desteklemektedir. Bu doğrultuda, "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır.

Tablo 5.7: Bilgi 6 ACH Matrisi.

ETKİ İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 6: Sosyal medyada mikro hedefleme algoritmaları ile algı yönetimi, psikoloji alanındaki bilimsel çalışmalarla uyumludur.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

Algı, insanlarda duyusal uyarımın organize deneyime çevrildiği süreci ifade eder.[315] Gestalt kuramına göre, kişilerin uyaranları işleme biçimi, dış uyaranları içsel süreçlerle konsolide eden karmaşık bir süreçtir.[316] Yani, insanın dış dünyaya yönelik algısı, içsel etkilerden büyük ölçüde etkilenmektedir. Bu nedenle algı yönetiminde genel olarak öncelikle insanların ve toplumların duygusal kontrolleri hedeflenmektedir. Bu durumda, önceden koşullanmış ya da koşullandırılmış birey ve toplumların, verileri nasıl anlamlandıracakları ve bu verilere karşılık ne tepki vereceklerini belirleme gücü, onları koşullandıran odakların ya da durumların eline geçmiş demektir.

---

[314] Kirchgaessner, *a.g.e.*, https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan. [Erişim Tarihi: 21.02.2023].

[315] William Epstein, Louis Jolyon West, William N. Dember, "Perception", *Encyclopedia Britannica*, 14 Ekim. 2022, https://www.britannica.com/topic/perception. [Erişim Tarihi: 16 Ekim 2022].

[316] Irvin Rock, Stephen Palmer, "The Legacy of Gestalt Psychology", *Scientific American*, C. 263, S. 6, (1990): 89- 90.

Jennifer S. Lerner, Ye Li, Piercarlo Valdesolo ve Karim S. Kassam; 2015 yılında "Duygu ve Karar Verme" konusunda geniş bir literatür incelemesine dayanan bir araştırma gerçekleştirmişlerdir. Lerner ve arkadaşları çalışmalarında, duyguların, karar vermede güçlü, yaygın, öngörülebilir itici güçler olduğunu, tesadüfi duyguların genel olarak bilinçsiz ve istenmeyen etkiler ürettiğini, duyguların karar vermedeki etkisinin düşünce içeriği, düşünce derinliği ve örtük hedeflerin içeriğindeki değişiklikler vasıtasıyla meydana geldiğini ve duyguların ekonomik ve siyasi tercihler üzerinde nedensel etkileri olduğunu bulmuşlardır.[317] Algı yönetimi doğrudan muhakeme kabiliyetini hedef almaktadır. Sosyal medya, bir haber yahut gönderi ile duygusal olarak uyarılmış ve muhakeme yetisi zayıflamış kişilerin, benzer duygu ve düşüncelerdeki insanlara rastlayıp örgütlenmeleri için oldukça uygun bir platformdur. Manipüle edilmiş veri ve enformasyon ile bozulan muhakeme, insanın yahut toplumun, doğrusunu bilme durumunda vereceği tepkiden büyük ölçüde uzaklaşacaktır.

Sosyal medya, bir haberin kaynağının, özellikle haberin hızlıca yayıldığı durumlarda, bulanıklaşabildiği bir ortamdır. Bir kişi yahut odak, sosyal medyada pompaladığı bir haberi, yayıldıktan sonra kendi hesabından silebilir ve bu şekilde, üzerinde ciddi bir araştırma yapılmadıkça hem haber yayılmış olur hem de kaynağı bulmak oldukça güçleşir. Bu durumu sosyal medyadaki sahte (fake) yahut anonim kimliklenme kabiliyeti de destekleyebilmektedir. Paylaşım yapan kişi yahut kişilerin isim, fotoğraf gibi kişisel bilgilerini kullanmaksızın yönettikleri yahut başkasının kimliğine bürünerek açtıkları sosyal medya hesaplarından yaptıkları paylaşımlar, bir haberin ciddi ölçekte yayılabildiği durumlarda çoğunlukla sorgulamadan uzak kalırlar. Özellikle kişiyi öfke gibi rasyonel karar almaya engel bir ruh hâline büründürebilecek türdeki haber ve paylaşımlar, haberin kaynağının sorgulanması fikrini devre dışı bırakabilmektedir.[318] Ayrıca bilgisayar modellerinin, sosyal medya verilerine

---

[317] Jennifer S. Lerner, Ye Li, Piercarlo Valdesolo ve Karim S. Kassam, "Emotion and Decision Making", *Annual Review of Psychology,* C. 66 (2015): 799- 823. https://doi.org/10.1146/annurev-psych-010213-115043.

[318] Wylie, *a.g.e.,* 86.

dayanarak kullanıcılar hakkında ailesi ve arkadaşlarından daha isabetli tahminler yapabildiği ortaya konulmuştur.[319]

Bu bilgiler, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini desteklemektedir. Bu doğrultuda "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır.

Tablo 5.8: Bilgi 7 ACH Matrisi.

ETKİ İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 7: Sosyal robotlar ile oluşturulan dezenformasyonun yayılması, gerçek kullanıcılar tarafından paylaşılmadığı sürece mümkün değildir.	**I**	**C**	**C**

Yazar tarafından oluşturulmuştur.

Her ne kadar yapay zekâ ile sosyal medya üzerinde dezenformasyon üretmek mümkün olsa da, üretilen içeriklerin gerçek kullanıcılar tarafından itibar görmesi gerekmektedir. Yine bu içeriklerin gerçek kullanıcılar tarafından yayılması gerekmektedir. Bu durumda sosyal robotların, işlevsellik kazanabilmeleri için gerçek kullanıcıların etkin rolü tamamen dışlanamaz. Bu bilgiler, "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezini desteklemektedir. Bu doğrultuda "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezi yanlışlanmıştır.

Tablo 5.9: Bilgi 8 ACH Matrisi.

ETKİ İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 8: Sosyal medyada yayılan dezenformasyonun yapay zekâ programları ile tespiti mümkündür.	**I**	**C**	**C**

Yazar tarafından oluşturulmuştur.

[319] Youyou, Kosinski ve Stillwell, *a.g.e.*, 4.

Yapay zekâ, dezenformasyon üretebileceği gibi dezenformasyonun tespiti için de elverişli bir unsurdur. Örnek olarak Süleyman Gökhan Taşkın, Ecir Uğur Küçüksille ve, Kamil Topal, 2021 yılında denetimli ve denetimsiz makine öğrenmesi algoritmaları kullanılarak Twitter'da Türkçe sahte haber tespiti yapılabildiğini ortaya koymuşlardır. Bu bilgiler, "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezini desteklemektedir. Bu doğrultuda "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezi yanlışlanmıştır.

Tablo 5.10: Bilgi 9 ACH Matrisi.

ETKİ İMKÂNI	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 9: Cari dönemde yapay zekâ uygulamaları, kullandığı dil tibariyle ürettiği içeriğin gerçek bir kullanıcınınkinden ayırt edilmesini oldukça güçleştirecek seviyede gelişmiştir.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

Örnek olarak Team Jorge adlı şirketin oluşturduğu dezenformasyon yayan bu bot hesapların vatandaşlar tarafından çoğu zaman gerçek kişilerden ayırt edilemeyecek kadar profesyonel olarak oluşturulduğu ortaya çıkmıştır. Bir başka örnek ise OpenAI tarafından tasarlanan Chat GPT uygulamasıdır. Chat GPT, algoritma dizaynından bilgi gerektiren sorulara, matematik problemi çözümlerinden kitap özetlemeye kadar birçok görevi başarı ile yerine getirebilmektedir. Ayrıca kullandığı dil yapısı itibariyle gerçek bir kullanıcı izlenimi vermektedir. Söz konusu örnekler, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini desteklemektedir. Bu doğrultuda, "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır.

Tablo 5.11: Bilgi 10 ACH Matrisi.

MAKUL İNKÂR EDİLEBİLİRLİK	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 10: Yapay zekâ sistemleri, etkilenenler tarafından tespit edilemeyecek şekilde tasarlanabilir.	**C**	**I**	**I**

Yazar tarafından oluşturulmuştur.

Derin öğrenme mimarilerindeki gelişmelerin yanı sıra yapay zekâ ile siber korsanlık da çağımızın önemli gelişmelerinden biridir. Örtülü operasyonların en önemli koşulu olarak görülen makul inkâr edilebilirlik bakımından bu avantaj önemlidir. Sosyal medyanın siber uzayın yapısından aldığı anonimlik avantajı, yapay zekâ uygulamaları ile boyut atlamıştır. Bu bilgiler, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini desteklemektedir. Bu doğrultuda "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi yanlışlanmıştır

Tablo 5.12: Bilgi 11 ACH Matrisi.

MAKUL İNKÂR EDİLEBİLİRLİK	Hipotez 1	Hipotez 2	Hipotez 3
Bilgi 11: Cambridge Analytica vakası, sosyal medyada örtülü operasyonların bir şekilde açığa çıkabileceğini ispat etmiştir.	**I**	**I**	**C**

Yazar tarafından oluşturulmuştur.

Siber uzayın yapısı ve sosyal medyanın anonim kimliklenmeye müsait bir zemin oluşu örtülü operasyonlara elverişli bir ortam sunuyor olsa da, söz konusu operasyonların cari dönemde insan operatörler tarafından gerçekleştirildiği unutulmamalıdır. Operatörleri itirafa itebilecek çeşitli motivasyonlar yahut karşı istihbarat çalışmalarının doğuracağı sonuçlar, söz konusu operasyonların açığa çıkmalarına olanak tanıyabilmektedir. Örnek olarak Cambridge Analytica vakası, şirketin eski çalışanı Christopher Wylie'nin, Cambridge Analytica ve onun üst kuruluşu SCL şirketinin faaliyetlerini ifşa etmesi ile açığa çıkmış ve ardından şirketin bir diğer eski çalışanı Britanny Kaiser de söz konusu şirketler grubunun çok sayıda ülkede gerçekleştirdiği seçim müdahalelerini itiraf etmiştir. Bu durum, Rory Cormac ve Richard Aldrich'in, örtülü operasyonların hem dâhili hem hârici gözlemcileri olduğundan ötürü doğal bir ifşaat mekanizması olduğu ve bu yüzden gizlilik ve inkâr

edilebilirliğe yapılan keskin atfın genel geçer olmadığı yönündeki tezlerini doğrular niteliktedir.[320]

Bu bilgiler, "yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezini yanlışlamaktadır. Bu doğrultuda "yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir" hipotezi ile yanlışlanmıştır.

5.4.3. ACH Genel Değerlendirmesi

Yukarıda verilen bilgiler doğrultusunda ACH genel değerlendirme matrisi aşağıdaki gibidir;

Tablo 5.13: ACH Genel Değerlendirme Matrisi.

Yapay zekâ yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir mi?			
HİPOTEZLER ⟹	**Hipotez 1**	**Hipotez 2**	**Hipotez 3**
KANITLAR ⇓	⇓	⇓	⇓
ERİŞİM İMKÂNI			
Bilgi 1: Tahmine Dayalı Analitik ile örtülü operasyonları gerçekleştirmek için ihtiyaç duyulan verilerin algoritmalar vasıtasıyla yapılandırılıp geleceğe yönelik isabetli operasyon perspektifi sunması mümkündür.	**C**	**I**	**I**
Bilgi 2: Sosyal medya şirketlerinin kullanıcı verilerine erişimi kısıtlama yahut engelleme çabalarını aşarak büyük miktarda veri kazımak mümkündür.	**C**	**I**	**I**
Bilgi 3: Sosyal medya kullanıcılarının ürettiği büyük miktarda verinin isabetli olarak ve	**C**	**I**	**I**

[320] *a.g.e.*, 479.

çok kısa sürede analiz edilmesi, makine öğrenmesi yöntemleri ile mümkündür.			
Bilgi 4: Diğer istihbarat faaliyetleri olmaksızın sosyal medya verileri bir örtülü operasyon için yeterli değildir.	**I**	**C**	**I**
ETKİ İMKÂNI			
Bilgi 5: Cari dönemde yapay zekâ alanındaki gelişmeler ile sosyal medya kullanıcısı olarak oluşturulan sosyal robotlar, söylemin yayılması bakımından algı yönetimi ve dezenformasyona elverişliliği arttırmıştır.	**C**	**I**	**I**
Bilgi 6: Sosyal medyada mikro hedefleme algoritmaları ile algı yönetimi, psikoloji alanındaki bilimsel çalışmalarla uyumludur.	**C**	**I**	**I**
Bilgi 7: Sosyal robotlar ile oluşturulan dezenformasyonun yayılması, gerçek kullanıcılar tarafından paylaşılmadığı sürece mümkün değildir.	**I**	**C**	**I**
Bilgi 8: Sosyal medyada yayılan dezenformasyonun yapay zekâ programları ile tespiti mümkündür.	**I**	**C**	**C**
Bilgi 9: Cari dönemde yapay zekâ uygulamaları, kullandığı dil tibariyle ürettiği içeriğin gerçek bir kullanıcınınkinden ayırt edilmesini oldukça güçleştirecek seviyede gelişmiştir.	**C**	**I**	**I**

MAKUL İNKÂR EDİLEBİLİRLİK			
Bilgi 10: Yapay zekâ sistemleri, etkilenenler tarafından tespit edilemeyecek şekilde tasarlanabilir.	**C**	**I**	**I**
Bilgi 11: Cambridge Analytica vakası, sosyal medyada örtülü operasyonların bir şekilde açığa çıkabileceğini ispat etmiştir.	**I**	**I**	**C**
Yanlışlanabilirlik Puanı:	**4**	**8**	**9**

Yazar tarafından oluşturulmuştur.

Tabloya göre en az yanlışlanan seçenekler şu şekildedir:

Hipotez 1: 4 kanıt tarafından yanlışlanmıştır (I), 7 kanıt tarafından doğrulanmıştır (C).

Hipotez 2: 8 kanıt tarafından yanlışlanmıştır (I), 3 kanıt tarafından doğrulanmıştır (C).

Hipotez 3: 9 kanıt tarafından yanlışlanmıştır (I), 2 kanıt tarafından doğrulanmıştır (C).

Hipotezler arasından en az yanlışlanan hipotez "Yapay zekâ, yakın gelecekte sosyal medyayı örtülü operasyonun birincil unsuru olabilir" hipotezi olmuştur. Bu durumda en doğru hipotez olarak kabul edilecektir.

5.5. Analitik Hiyerarşi Süreci (Analytical Hierarchy Process- AHP)

Analitik Hiyerarşi Süreci 1968 yılında. James H Myers ve Mark I. Alpert tarafından ortaya konulan ve 1977 yılında Thomas L. Saaty tarafından geliştirilen bir karar verme modelidir.[321] Model, çok kriterli karar verme probleminde nicel ve nitel verilerin

[321] Gülenç, Bilgin, *a.g.e.,* 98.

ölçümü için sıklıkla kullanılan bir tekniktir.[322] Saaty AHP tekniğini kriterler arasındaki subjektif mesafeyi ölçme maksadıyla geliştirmiştir.[323]

AHP metodolojisi aşağıdaki algoritmayı takip eder:[324]

- Problemin tanımlanması
- Seçenekler ve kriterlerin oluşturulması
- Hiyerarşik yapının dizaynı
- İkili karşılaştırma matrislerinin oluşturulması
- Kriterlerin önem derecelerinin belirlenmesi
- İkili karşılaştırma matrislerinin normalize edilmesi
- Öz vektörlerin bulunması
- Özdeğerlerin bulunması
- En büyük özdeğerin bulunması
- Tutarlılıkların test edilmesi
- Karar matrisinin oluşturulması
- Nihai öncelik vektörleri ile en iyi alternatifin seçilmesi

5.5.1. Analitik Hiyerarşi Süreci (AHP) Metodolojisi

- ACH Analizinde elde edilen bulgulara göre ikili karşılaştırma matrisinin hazırlanması:

Bu aşamada, AHP analizi için belirlenen kriterlerin sayısal değerleri ifade edilecektir.[325]

Tablo 5.14: AHP Kriterlerin Önem Dereceleri ve Nicel Değerleri.

Önem Derecesi	Tanım	Açıklama	Nicel Değer
1	Eşit derecede önemlidir	Her iki kriter eşit öneme sahiptir	Kriter 1=1, Kriter 2=1

[322] Vaidya, Kumar, *a.g.e.,* 2.

[323] Seher Arslankaya, Kübra Göraltay, "Analitik Hiyerarşi Prosesi Yöntemi", *Çok Kriterli Karar Verme Yöntemlerinde Güncel Yaklaşımlar* (Ankara: İksad Yayınevi, 2019), 16.

[324] *a.g.e.,* 16.

[325] *a.g.e., 219.*

3	Orta derecede önemlidir	Kanıtlara göre bir kriter diğerinden biraz daha önemlidir	Kriter 1=3, Kriter 2= 1/3= 0,33
5	Kuvvetli derecede önemlidir	Kanıtlara göre bir kriter diğerinden kuvvetle daha önemlidir	Kriter 1=5, Kriter 2= 1/5= 0,20
7	Çok kuvvetli derecede önemlidir	Kanıtlara göre bir kriter diğerinden çok kuvvetli derecede daha önemlidir	Kriter 1=7, Kriter 2= 1/7= 0,14
9	Kesinlikle önemlidir	Kanıtlara göre bir kriter diğerinden kesinlikle daha önemlidir	Kriter 1=9, Kriter 2= 1/9= 0,11
2, 4, 6, 8	Ara değerler	Faktörler arasındaki derecelendirmede yukarıdaki derecelendirmelerin ara değerlerini ifade eder.	Kriter 1=2 için, Kriter 2= 0,50 Kriter 1=4 için, Kriter 2= 0,25 Kriter 1=6 için, Kriter 2= 0,16 Kriter 1=8 için, Kriter 2= 0,125

Yazar tarafından oluşturulmuştur.

• İkili Karşılaştırma Matrisi ve Normalizasyonu

Bu aşamada, ikili karşılaştırma matrislerinde sütunlardaki değerlerin toplamları hesaplanır ve sütunlardaki her bir değerin bulunan toplama bölünmesi ile matris normalize edilir. *n* sayıda kriteri bulunan bir matris $[x_{ij}]_{nxn}$ ile ve normalize edilmiş matris ise $[y_{ij}]_{nxn}$ ile gösterilmek üzere ikili karşılaştırma matrisinin normalizasyon işlemi şu formül ile gerçekleştirilir:

$$y_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}}$$

• Öz vektörün hesaplanması

Bu aşamada, normalize edilmiş matristeki her satırın aritmetik ortalaması alınarak Öz vektör bulunur. Bu işlem, kriterlerin problem açısından önemini tespit etmek

maksadıyla kriterlere; seçeneklerin kriterler açısından önemini tespit etmek maksadıyla da seçeneklere uygulanır. Öz vektör:

$$S = [s_{ij}]_{nx1} \text{ olmak üzere;}$$

$$s_1 = \frac{\sum_{i=1}^{n} y_{1j}}{n}$$

• Tutarlılık Testlerinin Yapılması

Bu aşamada, ikili karşılaştırma matrislerinin kendi aralarındaki tutarlılıkları test edilmelidir. Bunun için öz değer hesaplanır. Öz değer, karşılaştırma matrisinin öz vektör ile çarpımından elde edilen bir değerdir. Bu işlem yapılırken, karar matrisi satırlarındaki her bir değerin, öz vektör sütunundaki değer ile çarpımı bulunur ve satır bazında toplanır. Test sonucunun tutarsız çıkması durumunda ikili karşılaştırma matrisleri tekrar oluşturulmalıdır.

n sayıda kriterin ikili karşılaştırma matrislerinin tutarlılık testleri aşağıdaki formül ile gerçekleştirilir:

$$[t_{ij}]_{nx1} = [x_{ij}]_{nxn} * [s_1]_{nx1}$$

Tutarlılık testi sonucunda bulunan vektörün elemanları sırasıyla ağırlık vektörü elemanlarına bölünür. Buradan elde edilen değerlerin ortalaması alınarak λ_{max} en büyük öz değeri hesaplanır.

$$\frac{t_i}{s_i},\ \lambda_{max} = \frac{\sum_{i=1}^{n} \frac{t_i}{s_i}}{n}$$

Daha sonra, bu hesaplama ile tutarlılık endeksi (*CE*) hesaplanır. Son aşamada ise tutarlılık oranının hesaplanması yapılır. Tutarlılık oranı ise tutarlılık endeksinin (*CE*), rassal endekse (*RE*) oranlanması ile bulunur.

$$\text{Tutarlılık Endeksi: } CE = \frac{\lambda_{max} - n}{n-1}$$

$n < 10$ olmak üzere Rassal Endeks tablosu şu şekildedir;

Tablo 5.15: *n* Sayıda Kritere Göre Rassal Endeks Değerleri.

n	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RE	0,00	0,52	0,89	1,11	1,25	1,35	1,40	1,45	1,49

Yazar tarafından oluşturulmuştur.

$$\text{Tutarlılık oranı: } CR = \frac{CE}{RE}$$

Tutarsızlık oranının kabul edilebilir bir ölçüde olması için 0,1'den küçük olmalıdır ($CR = CE/RE < 0{,}1$). Tutarsızlık oranı bu seviyenin üzerinde ise karşılaştırma matrisi tekrar değerlendirilmelidir.

- Karar Matrisinin Oluşturulması

Bu aşamada, daha önce oluşturulmuş olan öncelik vektörleri birleştirilerek karar matrisi oluşturulur. A_i, alternatiflerin i. Kriter için karşılaştırılması ile elde edilen bir öncelik vektörü olmak üzere, *n* sayıda kriter ve *m* sayıda alternatife sahip olan probleme dair bir örnek matris ile *W* kriterlerin ağırlıkları aşağıdaki gibidir;

$$D = [A_1 \quad A_2 \quad \cdots \quad A_n]_{mxn}$$

$$D = \begin{bmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & \ddots & \vdots \\ d_{m1} & \cdots & d_{mn} \end{bmatrix}_{mxn}$$

$$W = [w_1 \quad w_2 \quad \cdots \quad w_n]_{1xn}$$

- Nihai öncelik vektörlerinin hesaplanması

Bu aşama, AHP yönteminin sonuncu aşamasıdır. Bu aşama ile en iyi alternatif seçilir. *D* karar matrisi ile *W* kriter ağırlıkları çarpıldıktan sonra $A = [\alpha_i]_{mx1}$ alternatiflerin nihai öncelik vektörü olmak üzere, alternatiflerin önem ağırlıkları, *A* = *D* x *W* formülü ile hesaplanır.

5.5.2. Sosyal Medyada Örtülü Operasyonun Analitik Hiyerarşi Süreci (AHP) ile Analizi

- Problemin Tanımlanması

Devletler özellikle Soğuk Savaş döneminde örtülü operasyonları dış politika hedeflerine ulaşma aracı olarak sıklıkla kullanmışlardır. Devletleri örtülü operasyon müracaatına iten caydırıcı motiflerin en önemli yolu, örtülü operasyonların doğasındaki gizlilik olgusu ve makul bir şekilde inkâr edilebilme yeteneği olmuştur. Bilhassa paramiliter, ekonomik ve siyasi örtülü operasyonlar, izi sponsora atfedilemeyecek şekilde gerçekleştirilmeyi amaçlar. Fakat Lowenthal'ın Örtülü Eylem Merdiveni'nden de anlaşılacağı gibi, örtülü operasyon türleri arasında yarattığı şiddet ile makul inkâr edilebilirlik arasındaki ters orantı göz önünde bulundurulduğunda, siyasi örtülü operasyonlar paramiliter ve ekonomik örtülü operasyonlardan daha özel bir alanda konumlanmaktadır.

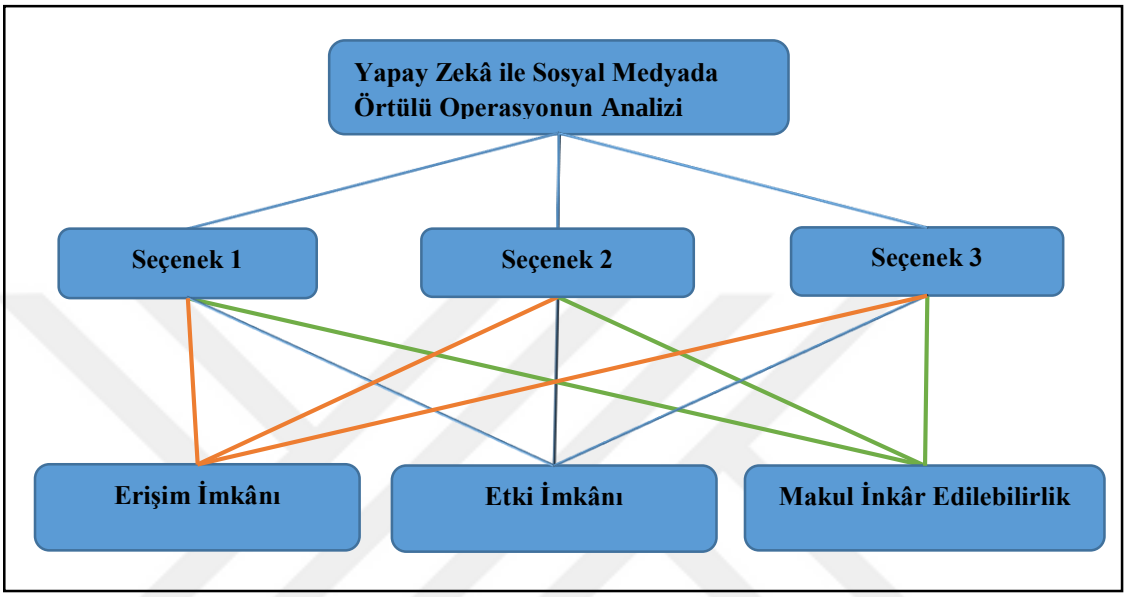
Devletler, dış politika hedeflerini gerçekleştirme maksadıyla yürütecekleri örtülü operasyonlar için öncelikle başarı olasılığını arttıracak elverişli alanı/ zemini tespit etmelidirler. Bu bağlamda, siber uzay, örtülü operasyonların gerçekleştirilmesinde yarattığı şiddetin düşük olması ve makul inkâr edilebilirlik derecesinin yüksek olması bakımından geleneksel yöntemlere nazaran daha avantajlı bir konumdadır. Sosyal medya, her bir bireyin gerek haber alma gerekse bir yayın istasyonu gibi haber yayması hususunda örtülü operasyonlar için eşsiz bir zemin hâlini almıştır.

Bu aşamadan itibaren ACH analizindeki analiz sorusu, problem olarak adlandırılacaktır. AHP uygulamasında, "Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir mi?" problemi, söz konusu hipotezler (bu aşamadan sonra seçenek olarak adlandırılacaktır) ve hipotezlere (seçeneklere) etki eden kriterlerin ağırlıklandırılması bakımından AHP tekniği ile analiz edilecektir.

Seçenek 1: Yapay Zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir.
Seçenek 2: Yapay Zekânın, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir.
Seçenek 3: Sosyal medya örtülü operasyona uygun bir zemin değildir.

Kriterler: Erişim İmkanı, Etki İmkanı, Makul İnkâr Edilebilirlik.

• Hiyerarşik Yapının Oluşturulması:



Şekil 5.1: AHP Problemi Hiyerarşik Yapı

Yazar tarafından oluşturulmuştur.

Sosyal medyada örtülü operasyonun istihbarat analizi önceki bölümde Rakip Hipotezler Analizi (ACH) ile analiz edilmiştir. Bu bölümde, Sosyal medyada örtülü operasyonun analizi AHP tekniği ile tekrar analiz edilecek ve ACH analizi ile elde edilen sonuç bu şekilde sınanacaktır. AHP tekniğinin faydalarından biri, analiz sürecinde yararlanılan kanıtların hangisinin sonuç üzerinde daha fazla etkiye sahip olduğunu da ortaya koymasıdır. AHP analizi ayrıca, sayısal verilerin olmadığı subjektif yargıların nicelleştirilmesi bakımından önem arz etmektedir. Bu şekilde yukarıda ifade edilen analiz sorusu, matematiksel olarak formule edilecek ve elde edilen sonuçlara en fazla etki eden kriter bazında çalışmanın sonuç ve değerlendirmeleri ortaya konulacaktır.

Unutulmamalıdır ki, analiz edilen analiz sorusu, mevcut durumdaki veriler ışığında değerlendirilmiştir. Bu bakımdan, bu aşamada eldeki veriler ışığında yapay zekânın

yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olma yahut olamama durumu, erişim imkânı, etki imkânı ve makul inkâr edilebilirlik yönünden sunduğu kabiliyetler kapsamında incelenecektir.

Analiz sorusu: Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir mi?

Seçenek 1: Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir.

Seçenek 2: Yapay zekânın, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir.

Seçenek 3: Sosyal medya örtülü operasyona uygun bir zemin değildir.

ACH yönteminde başvurulan kanıtlar, AHP metodunda kriter olarak belirlenmiştir. Bu aşamada seçenekler, aşağıdaki kriterler bazında kıyaslanacaktır;

Kriter 1: Erişim imkânı

Kriter 2: Etki imkânı

Kriter 3: Makul inkâr edilebilirlik

Herhangi bir proje, politika yahut operasyonun her birinden evvel, yürütücünün ilgili kurum ve organları, fizibilite çalışmaları, çeşitli hazırlıklar ve durum değerlendirmeleri yaparlar. Tabiatı ile bu hazırlıklar örtülü operasyonlar için de geçerlidir. İnternet öncesi dönemlerde örtülü operasyonların algı yönetimi ve propaganda gibi süreçleri hem daha kitlesel özellikte hem de hazırlık aşamaları bakımından daha uzun süreli ve çetrefilli aşamalara sahip olmuştur. Örnek olarak, bir kanaatin bir topluma yahut kitleye *"aşılanması"* için, söz konusu kitle yahut toplum tarafından itibar gören yazarlar, gazeteciler, sanatçılar, akademisyenler ve politik isimler gibi aday etki elemanlarının tespit edilmesi ve angaje edilmesi mühim bir süreçtir. Fakat toplum özellikle fikir olarak kendisine yakın yayınlar yapan yayınları takip etme eğilimindedir. Bu yayınlar benzer düşüncedeki insanları etrafında konsolide etmede bir derece başarılıdırlar fakat, yanlılık eğiliminden ötürü başka hedeflere ulaşmaları sosyal medya ile kıyaslandığında nispeten daha zordur.

Sosyal medyada hem verilere hem kitlelere hatta bireylere erişim olanağı, sosyal medya öncesi dönemle kıyaslandığında ciddi ölçüde artmıştır. Cambridge Analytica

bölümünde incelendiği üzere, sosyal medyada etki operasyonları yaratmada makine öğrenmesi yöntemleri, büyük veri ve psikografi teknikleri, operatöre daha isabetli bir operasyon başarısı vadetmekle birlikte siber uzayın anonim kimliklenmeye tanıdığı olanak, örtülü operasyonlarda kimi araştırmacının "doktrin" addettiği makul inkâr edilebilirlik açısından da uygun bir zemin olmuştur. Ayrıca, Cambridge Analytica bölümünde geniş bir biçimde incelendiği üzere, sosyal medya üzerinden örtülü operasyonun kolaylıkla tercih edilebilir olmasının bir nedeni caydırıcı yasal mekanizmalardan yoksunluktur. 2016 ABD Başkanlık Seçimleri ve BREXIT Referandumu yargılamaları göz önünde bulundurulduğunda, devletlerden ziyade sosyal medya şirketleri ciddiye alınabilecek hukuki ve ekonomik yaptırıma tabi olmaktadırlar.

Bu doğrultuda, yapay zekâ alanındaki gelişmelerden en çok hangi kriterin sosyal medyayı örtülü operasyon için daha elverişli bir zemin hâline getirdiği sorusu, eldeki verilerin sistematik olarak organize edilmesi yoluyla ortaya konulmalıdır. Bu, devletlerin bir dış politika aracı olarak örtülü operasyonlara yönelmeleri yönünden olduğu kadar, bir stratejik sürprize maruz kalmamak maksadıyla karşı istihbarat faaliyetleri geliştirmeleri yönünden de birincil yönelim tercihi belirleme avantajı sağlayabilecektir.

Mikro hedeflemenin bireylerin duygularını anlama ve davranışlarını değiştirme kabiliyetine yönelik ACH analizinde ele alınmış olan bilimsel çalışmalar, psikografi çalışmalarının algoritmalara entegre olarak kullanılmasının, sosyal medyayı örtülü operasyonlarda kitleleri ve hatta bireyleri etkileme yönünden avantajlı hâle getirdiğini ortaya koymuştur. Sosyal medyanın hacim, hız, çeşitlilik unsurlarının tümü yönünden sağladığı büyük verinin ele geçirilmesi tek başına operasyonel başarı vadetmeyecektir. Makine öğrenmesi ve doğal dil işleme alanlarındaki gelişmeler, yapay zekâ tanımlamalarındaki "insan gibi davranma" öncülünü giderek daha fazla başarma eğilimindedir; bu durum da etki kabiliyetini arttırır dolayısıyla operasyonel başarı olasılığını arttırmıştır.

İsrail menşeli Team Jorge adlı şirketin otomatik dezenformasyon ile seçim müdahalelerinde bulunmuş olması vakası, yapay zekâ ile oluşturulan sosyal robotların birer birey gibi hareket ederek dezenformasyon oluşturma ve yaymada başarılı olabildiğini ortaya koymuştur. Yapay zekâ programlamaları, insanın yapabildiği

faaliyetleri yapabilme bakımından hem iş gücünden tasarruf sağlamakta hem de doğru modellemeler ile daha isabetli sonuçlar verebilmektedir.

Yukarıdaki bilgiler ışığında kriterlerin ikili olarak karşılaştırılarak, "hangisi daha önemlidir?" sorusuna verilen cevaplar şu şekildedir:

- Etki imkânı, erişim imkânından kuvvetli derecede daha önemlidir.
- Etki imkânı makul inkâr edilebilirlikten çok kuvvetli derecede daha önemlidir.
- Erişim imkânı makul inkâr edilebilirlikten biraz daha önemlidir.

Bu doğrultuda, ikili karşılaştırma matrisi aşağıdaki gibidir;

Tablo 5.16: Kriterlere İlişkin İkili Karşılaştırma Matrisi.

Kriter Karşılaştırmaları	Erişim imkânı	Etki imkânı	Makul İnkâr Edilebilirlik
Erişim imkânı	1	0,2	3
Etki imkânı	5	1	7
Makul İnkâr Edilebilirlik	0,33333333	0,14285714	1
Toplam	**6,33333333**	**1,34285714**	**11**

Yazar tarafından oluşturulmuştur.

İkili karşılaştırma matrisindeki her bir değerin, değerin bulunduğu sütunun toplamına bölünmesi ile matris normalize edilir. Bu işlemin ardından yeni tablodaki her bir satırın ortalaması alınarak her bir kriterin öz vektörü bulunur;

Tablo 5.17: Kriterlere İlişkin Normalizasyon Matrisi.

Normalizasyon Matrisi	Erişim imkânı	Etki imkânı	Makul İnkâr Edilebilirlik
Erişim imkânı	0,15789474	0,14893617	0,27272727
Etki imkânı	0,78947368	0,74468085	0,63636364

Makul İnkâr Edilebilirlik	0,05263158	0,10638298	0,09090909

Yazar tarafından oluşturulmuştur.

Bu aşamada, her bir satırın aritmetik ortalaması alınarak öz vektörü bulunacaktır. öz vektör, bu aşamada kriterlerin karşılaştırması yapıldığından, problem üzerinde öncelikli öneme haiz kriteri belirleyecektir.

Öz vektör tablosu aşağıdaki gibidir;

Tablo 5.18: Kriterlere İlişkin Öz Vektör Tablosu.

Normalize Edilmiş Kriterler	Öz Vektör Tablosu
Erişim imkânı	0,19318606
Etki imkânı	0,723506057
Makul İnkâr Edilebilirlik	0,083307883

Yazar tarafından oluşturulmuştur.

Tablodan anlaşıldığı üzere, en yüksek değeri veren etki imkânı kriteri, problem üzerindeki en etkili kriter olarak bulunmuştur.

Bu durumda kriterlerin önem sıraları şöyledir: Etki imkânı > Erişim imkânı > Makul İnkâr Edilebilirlik.

Ancak bu aşamada kesin karar vermeden evvel, öncelik vektörlerinin tutarlı olup olmadığını belirlemek için tutarlılık endeksi ile tutarlılık oranının hesaplanması gerekmektedir. Bu şekilde analist, kriterlerin önceliklerini puanlarken verdiği yanıtların tutarlılığını gözden geçirecektir. Böylece istihbarat analizinde ortaya çıkan bilişsel tuzaklardan çalışmadaki analiz esnasında ne derece etkilenildiği de anlaşılacaktır.

Tutarlılık endeksi için öncelikle öz değer bulunur. Öz değer, karar matrisi satırlarındaki her bir değerin, öz vektör sütunundaki değerler ile sırası ile çarpılıp satır bazında toplanması ile elde edilir.

Tablo 5.19: Kriterlere İlişkin Özdeğer Tablosu.

Kriter Karşılaştırmaları	Erişim İmkânı	Etki İmkânı	Makul İnkâr Edilebilirlik	Öz Vektör Tablosu	Öz Değer Tablosu
Erişim İmkânı	1	0,2	3	0,19318606	0,587811
Etki İmkânı	5	1	7	0,723506057	2,272592
Makul İnkâr Edilebilirlik	0,33333333	0,14285714	1	0,083307883	0,251061
Örnek olarak, erişim imkânının öz değer hesabı için uygulama şöyledir: (1*0,19318606+ 0,2*0,723506057+ 3*0,083307883) = 0,587811.					

Yazar tarafından oluşturulmuştur.

Sonrasında en büyük öz değer bulunur. En büyük öz değer, öz değerlerin öz vektörlere oranlarının kriter sayısına bölümü ile hesaplanır. En büyük öz değer aşağıdaki şekildedir;

Tablo 5.20: Kriterlere İlişkin En Büyük Özdeğer Hesaplanması.

Öz Değer Tablosu		Öz Vektör Tablosu		En Büyük Öz Değer Tablosu (λ_{max})
0,587811	÷	0,19318606	=	3,06581867
2,272592		0,723506057		
0,251061		0,083307883		

Yazar tarafından oluşturulmuştur.

λ_{max}: 3,06581867.

Elde edilen öz değer ile tutarlılık endeksi hesaplanır. Tutarlılık endeksi (*CE*), en büyük öz değeri ile kriter sayısının farkının kriter sayısından bir küçük rakama oranlanması ile bulunur. Rassal Endeks Tablosu'nda (Tablo 5.15) 3 kriterli AHP hesaplaması için 0,52 değeri rassal endeks (*RE*) olarak alınır.

$$CE = \frac{3{,}06581867 - 3}{3 - 1} = 0{,}032909.$$

Elde edilen tutarlılık endeksinin rassal endekse oranlanması ile de tutarlılık oranı (*CR*) bulunur.

$$CR = \frac{CE}{RE} = \frac{0{,}032909}{0{,}52} = 0{,}063287.$$

Tutarlılık oranı: 0,063287 olarak bulunmuştur. AHP tekniğinde 0,1'den küçük olan tutarlılık oranı kabul edilebilir seviyedir. ($CR = CE/RE < 0{,}1$).Bu durumda, kriter seçimine verilen yanıtlar tutarlıdır.

Bu aşamadan itibaren aynı işlemler kriterler ile seçeneklerin kıyaslanması maksadıyla gerçekleştirilecektir. Seçenekler, ACH analizinde kanıtların açıklamalarına göre sıralanmıştır. Seçenekler, aşağıdaki gibi kısaltmalarla ifade edilecektir:

Seçenek 1: Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir. (S1)

Seçenek 2: Yapay zekânın, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olması mümkün değildir. (S2)

Seçenek 3: Sosyal medya, örtülü operasyona elverişli bir zemin değildir. (S3)

- Erişim imkânı için seçeneklerin karşılaştırılması:

Tablo 5.21: Erişim İmkânı İçin Seçeneklerin Karşılaştırılması.

Erişim İmkânı	S1	S2	S3
S1	1	5	7
S2	0,2	1	3
S3	0,142857143	0,333333333	1
Toplam	**1,342857143**	**6,333333333**	**11**

Yazar tarafından oluşturulmuştur.

Normalize edilmiş seçenekler matrisi, öz vektör, öz değer ve en büyük öz değer tablosu aşağıdaki gibidir:

Tablo 5.22: Erişim İmkânı İçin Normalize Edilmiş Seçenekler Matrisi, Öz Vektör, Öz Değer Ve En Büyük Öz Değer.

Erişim İmkânı	S1	S2	S3	Öz Vektör	Öz Değer	En Büyük Öz Değer
S1	0,744680851	0,789473684	0,636363636	0,72350606	2,27259154	3,06581867
S2	0,14893617	0,157894737	0,272727273	0,19318606	0,58781092	
S3	0,106382979	0,052631579	0,090909091	0,08330788	0,25106124	

Yazar tarafından oluşturulmuştur.

λ_{max}: 3,06581867.

Elde edilen öz değer ile tutarlılık endeksi hesaplanır. Tutarlılık endeksi (*CE*), en büyük öz değeri ile seçenek sayısının farkının seçenek sayısından bir küçük rakama oranlanması ile bulunur. Rassal Endeks Tablosu'nda (Tablo 5.15) 3 seçenekli AHP hesaplaması için 0,52 değeri rassal endeks (*RE*) olarak alınır.

$$CE = \frac{3,06581867-3}{3-1} = 0,032909.$$

Elde edilen tutarlılık endeksinin rassal endekse oranlanması ile de tutarlılık oranı (*CR*) bulunur.

$$CR = \frac{CE}{RE} = \frac{0,032909}{0,52} = 0,063287.$$

Tutarlılık oranı: 0,063287 olarak bulunmuştur. AHP tekniğinde 0,1'den küçük olan tutarlılık oranı kabul edilebilir seviyedir. $(CR = CE/RE < 0,1)$.Bu durumda, erişim imkânına göre seçeneklere verilen yanıtlar tutarlıdır.

- Etki imkânı için seçeneklerin karşılaştırılması:

Tablo 5.23: Etki İmkânı İçin Seçeneklerin Karşılaştırılması

Etki İmkânı	S1	S2	S3
S1	1	7	9
S2	0,142857143	1	3
S3	0,111111111	0,333333333	1
Toplam	1,253968254	8,333333333	13

Yazar tarafından oluşturulmuştur.

Normalize edilmiş seçenekler matrisi, öz vektör, öz değer ve en büyük öz değer tablosu aşağıdaki gibidir:

Tablo 5.24: Etki İmkânı İçin Normalize Edilmiş Seçenekler Matrisi, Öz Vektör, Öz Değer Ve En Büyük Öz Değer

Etki İmkânı	S1	S2	S3	Öz vektör	Öz değer	En Büyük Öz Değer
S1	0,797468354	0,84	0,692307692	0,77659202	2,47746835	3,08214127
S2	0,113924051	0,12	0,230769231	0,15489776	0,47137015	
S3	0,088607595	0,04	0,076923077	0,06851022	0,20643081	

Yazar tarafından oluşturulmuştur.

λ_{max}: 3,08214127.

Elde edilen öz değer ile tutarlılık endeksi hesaplanır. Tutarlılık endeksi (*CE*), en büyük öz değeri ile seçenek sayısının farkının seçenek sayısından bir küçük rakama oranlanması ile bulunur. Rassal Endeks Tablosu'nda (Tablo 5.15) 3 seçenekli AHP hesaplaması için 0,52 değeri rassal endeks (*RE*) olarak alınır.

$$CE = \frac{3{,}08214127 - 3}{3 - 1} = 0{,}041071.$$

Elde edilen tutarlılık endeksinin rassal endekse oranlanması ile de tutarlılık oranı (*CR*) bulunur.

$$CR = \frac{CE}{RE} = \frac{0{,}041071}{0{,}52} = 0{,}078982.$$

Tutarlılık oranı: 0,078982 olarak bulunmuştur. AHP tekniğinde 0,1'den küçük olan tutarlılık oranı kabul edilebilir seviyedir. ($CR = CE/RE < 0{,}1$).Bu durumda, erişim imkânına göre seçeneklere verilen yanıtlar tutarlıdır

- Makul İnkâr Edilebilirlik için seçeneklerin karşılaştırılması:

Tablo 5.25: Makul İnkâr Edilebilirlik İçin Seçeneklerin Karşılaştırılması

Makul İnkâr Edilebilirlik	S1	S2	S3
S1	1	5	7
S2	0,2	1	3
S3	0,142857143	0,333333333	1
Toplam	1,342857143	6,333333333	11

Yazar tarafından oluşturulmuştur.

Normalize edilmiş seçenekler matrisi, öz vektör, öz değer ve en büyük öz değer tablosu aşağıdaki gibidir:

Tablo 5.26: Makul İnkâr Edilebilirlik İçin Normalize Edilmiş Seçenekler Matrisi, Öz Vektör, Öz Değer Ve En Büyük Öz Değer.

Makul İnkâr Edilebilir-lik	S1	S2	S3	Öz Vektör	Öz Değer	En Büyük Öz Değer
S1	0,744680851	0,789473684	0,636363636	0,72350606	2,27259154	3,06581867
S2	0,14893617	0,157894737	0,272727273	0,19318606	0,58781092	
S3	0,106382979	0,052631579	0,090909091	0,08330788	0,25106124	

Yazar tarafından oluşturulmuştur.

λ_{max}: 3,06581867.

Elde edilen öz değer ile tutarlılık endeksi hesaplanır. Tutarlılık endeksi (*CE*), en büyük öz değeri ile seçenek sayısının farkının seçenek sayısından bir küçük rakama oranlanması ile bulunur. Rassal Endeks Tablosu'nda (Tablo 5.15) 3 seçenekli AHP hesaplaması için 0,52 değeri rassal endeks (*RE*) olarak alınır.

$$CE = \frac{3{,}06581867 - 3}{3-1} = 0{,}032909.$$

Elde edilen tutarlılık endeksinin rassal endekse oranlanması ile de tutarlılık oranı (*CR*) bulunur.

$$CR = \frac{CE}{RE} = \frac{0{,}032909}{0{,}52} = 0{,}063287.$$

Tutarlılık oranı: 0,063287 olarak bulunmuştur. AHP tekniğinde 0,1'den küçük olan tutarlılık oranı kabul edilebilir seviyedir. ($CR = CE/RE < 0{,}1$).Bu durumda, erişim imkânına göre seçeneklere verilen yanıtlar tutarlıdır.

- Karar matrisinin oluşturulması:

Bu aşamada, her bir seçeneğin kriter bazında elde ettiği öz vektör tek tek kriterlerin özvektörleri ile çarpılarak karar matrisi oluşturulur.

Tablo 5.27: AHP Karar Matrisi.

Karar Matrisi	Erişim İmkânı	Etki İmkânı	Makul İnkâr Edilebilirlik
S1	0,723506057	0,776592016	0,723506057
S2	0,19318606	0,15489776	0,19318606
S3	0,083307883	0,068510224	0,083307883
Kriter Öz Vektörleri	0,19318606	0,723506057	0,083307883

Yazar tarafından oluşturulmuştur.

- Seçeneklerin Önem Dereceleri

Son aşama olan karar matrisinde seçeneklerin kriter bazında elde ettiği değerler toplanır ve seçeneklerin önem dereceleri elde edilir.

Tablo 5.28: Seçeneklerin Önem Dereceleri.

	Erişim İmkânı	Etki İmkânı	Makul İnkâr Edilebilirlik	SONUÇ
S1	0,139771285	0,561869027	0,060273758	0,76191407
S2	0,037320854	0,112069468	0,016093922	0,165484243
S3	0,016093922	0,049567562	0,006940203	0,072601687

Yazar tarafından oluşturulmuştur.

(Tutarlılık oranı (CR): 0,0680 olarak bulunmuştur. 0,1'den küçük olduğu için sonuç tutarlıdır.

5.5.3. AHP Karar Grafiği

Yukarıdaki bilgiler ışığında AHP analiz sonucu, bu aşamada karar grafiği ile gösterilecektir. Karar grafiği aşağıdaki gibidir;



Şekil 5.2: AHP Karar Grafiği.

Yazar tarafından oluşturulmuştur.

5.6. Analiz Sonucu

Çalışmada, yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun kılan birincil unsur olup olamayacağı analiz edilmiştir. Öncelikle Rakip Hipotezler Analizi (ACH) ile, analiz sorusuna yönelik birbirini dışlayan iki hipotez üretilmiştir. Yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsur olabileceği ve olamayacağı hipotezleri, belirlenen kriter ve kanıtlara göre sınanmıştır. Kriterler, siber uzayın yapısı, klasik istihbarat toplama yöntemlerine nispetle sağladığı avantaj bakımından büyük veri ve erişilebilen kişi sayısı bağlamında "erişim imkânı"; mikro hedefleme ile algı yönetimi ve manipülasyona elverişliliği ve diğer istihbari faaliyetler olmaksızın etki yaratma kabiliyeti bağlamında "etki imkânı" ve gizlilik koşulları bağlamında "makul inkâr edilebilirlik" kriterleri altında incelenmiştir. Gerçekleştirilen değerlendirmeler neticesinde "Yapay zekâ, yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabilir" hipotezi, 2 kanıt tarafından yanlışlanmış ve en az yanlışlanan hipotez olmuştur. Karl Popper'ın "yanlışlanabilirlik ilkesi"nden türetilen Rakip Hipotezler Analizi (ACH), analistin kanıtları organize ederek çalışmasına ve böylece bilişsel tuzaklardan korunabileceği varsayılmış olsa da ekstra bir doğrulama yordamına muhtaçtır. Bu metodun bir tutarlılık kontrol mekanizması olmadığından ötürü analist, elde ettiği bilgiler ışığında hipotezlere verdiği yanıtları

tamamen birbirinden bağımsız olarak yorumlar ve tamamen subjektif olarak yaptığı değerlendirme yine de bilişsel kör noktalardan etkilenebilir. Bu doğrultuda bir kontrol mekanizması ile analizi derinleştirmek daha elverişli olacaktır.

Analitik Hiyerarşi Süreci (AHP), kriterler ve seçeneklere verilen subjektif yanıtların tutarlılıklarının hesaplanabilmesi ve elde edilen optimal sonuca hangi kriterin daha fazla etki ettiğinin ortaya konulabilmesi yönüyle, nitel karar verme metotlarını geliştirme ve sınama bakımından özel bir metottur. Ayrıca AHP, nitel kararların ağırlıklandırılarak nicelleştirilmesini de sağlamaktadır. Bu çalışmada, ACH analizindeki hipotezler birer seçenek olarak varsayılmış ve söz konusu hipotezlerin değerlendirilmesinde başvurulan kanıtlar da kriter olarak ele alınmıştır. Bu kriterler arasından etki imkânının, yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru olabileceği seçeneğini en fazla etkileyen kriter olduğu görülmüştür. AHP metodundan elde edilen sonuç hem kendi içinde bir tutarlılık testinden geçmiş hem de etki imkânının baskın etkinliği yönünden ACH analizi ile de tutarlı olduğu görülmüştür.

Analiz neticesinde yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsur olabileceği anlaşılmıştır.

6. SONUÇ VE ÖNERİLER

Art arda iki dünya savaşı yaşamış ve gerek ekonomik, gerek askerî gerekse sosyolojik bir yorgunluğa maruz kalmış olan devletler, konvansiyonel savaşlardan kaçınarak dış politika hedeflerini gerçekleştirmenin bir yolu olarak örtülü operasyonlara çok kez başvurmuşlardır. Özellikle ABD ve SSCB'nin, ideolojileri yoluyla yayılımcı politikalar sürdürdükleri Soğuk Savaş yıllarında gerçekleşen örtülü operasyon faaliyetleri gerek ekonomik, gerek paramiliter, gerekse siyasi araçlar vasıtasıyla yürütülmüştür. SSCB'nin Sputnik Uydusunu fırlatması ile teyakkuza geçen ABD, ilerleyen süreçlerde stratejik sürprizlerden korunmak maksadıyla DARPA'yı kurmuş ve günümüze kadar uzanan birçok teknolojik gelişmenin öncüsü olmuştur. Bu teknolojik gelişmeler ve buluşlar içerisinde en önemlisi olarak interneti göstermek, muhtemelen mübalağa sayılmayacaktır. Günümüzde gerek devletlerin gerekse bireylerin hayatlarını kesintisizce sürdürmelerinin ön koşullarından biri hâline gelen ve ciddi bir refah sağlayan internet, avantajlarıyla birlikte birçok avantajı da beraberinde getirmiştir. Özellikle web 2.0 olarak adlandırılan, internet kullanıcılarının karşılıklı etkileşimlerine zemin oluşturan ve sosyal medyayı da var eden[326] süreç ise, bu çalışmanın odaklandığı konu bakımından bir dönüm noktasıdır.

Kullanıcıların fikirlerini, fotoğraflarını, duygu ve durumlarını yansıtan paylaşımları sosyal medyayı hem bir serbest kürsü konumuna getirmiş hem de arka planda kullanıcıların en mahrem veri ve enformasyonlarını istismara açık hâle getirmiştir. İnternetin kullanıldığı her alanda oluşan ve hacim, hız ve çeşitlilik unsurlarıyla tanımlanan ve başlangıçta bir analiz sorunu ortaya çıkan[327] büyük veri, gelişmiş analitik yöntemler sayesinde veri gücünü elinde bulunduran taraflar için büyük bir avantaj hâlini almıştır. ABD merkezli düşünce kuruluşu Dış İlişkiler Konseyi'ne (CFR/ Council on Foreign Relations) bağlı Bağımsız Görev Gücü, Temmuz 2022 tarihli Siber Uzay raporunda (No. 80) *"bir jeopolitik güç ve rekabet kaynağı"* olarak ifade edilen veri, bir emtia ve millî güvenlik merkezi olarak değerlendirilmiştir. [328]

---

[326] Zeng ve diğ., *a.g.e.,*13.

[327] Mohammed ve diğ., *a.g.e.,* 1-5.

[328] Segal, Goldstein, *a.g.e.,* 3.

Propaganda yaymak için erişilebilen kişi sayısı ve makine öğrenimi tekniklerindeki gelişmelerin sağladığı etki imkânı bakımından gerek bir tehlike arz ettiği gerekse bir avantaj sağladığı yönünden olsun, temel olarak elverişlilik tartışmalarını başlatan sosyal medya, bu yönüyle örtülü operasyonlar için de en sessiz seçeneklerden biri hâline gelmiştir. Siber uzayın özellikleri bakımından makul inkâr edilebilirlik avantajı sağlayan sosyal medya, Cambridge Analytica ve onun üst kuruluşu olan SCL tarafından da psikolojik savaş yöntemlerinin kullanıldığı elverişli bir zemin teşkil etmiştir. Siyasi kampanyaların geleneksel demografik veriler ışığında yürütülmesine bir alternatif olarak veriler ile psikografi yöntemlerini birleştiren Cambridge Analytica, beş kıtada yüzden fazla siyasal seçim kampanyası yürütmüş ve son olarak 2016 yılında ABD başkanlık seçimleri ile BREXIT referandumu süreçlerine olan müdahalesi sonrasında şirketin eski çalışanı Christopher Wylie tarafından ifşa edilmiş ve sosyal medyanın istihbari yönden arz ettiği tehlike konusundaki tartışmaların da yükselmesine zemin oluşturmuştur. Facebook'un "dark post" özelliği ile kişiye özel reklam hedeflemelerine elverişli bir zemin oluşturması, kişileri yönelimlerine göre tasniflendirip duygusal olarak tetiklemeye de zemin oluşturmaktadır. Facebook Cambridge Analytica skandalı dışında 2018 yılında *"öfke algoritması"* olarak adlandırılan bir skandala daha sebebiyet vermiştir. Şirket, Anlamlı Sosyal Etkileşimler (MSI) olarak adlandırdığı yeni bir puanlama sistemi ile haber akışında "kullanıcılarda paylaşımlara yorum yapma isteği uyandıracak" algoritmalar kullanmaya başlamış ve bu algoritmaların insanlarda özellikle öfke duygusunu tetiklediği ve şirket çalışanlarının durumun farkında olduğu anlaşılmıştır.[329] İhbarcı Christopher Wylie'nin Cambridge Analytica'nın sosyal medya vasıtası ile öfke tetiklemeye yönelik algoritmik faaliyetler yürüttüğü ifadesi[330]de dikkate alındığında, sosyal medyanın birçok yönüyle propaganda ve dezenformasyon yoluyla bireyleri toplumsal hareketlere sürükleyebilecek kabiliyette olduğu anlaşılmaktadır.

---

[329] The Journal, "The Facebook Files, Part 4: The Outrage Algorithm", *WSJ Podcasts*, 09.18.2021, https://www.wsj.com/podcasts/the-journal/the-facebook-files-part-4-the-outrage-algorithm/e619fbb7-43b0-485b-877f-18a98ffa773f. [Erişim Tarihi: 01.01.2023].

[330] Wylie, *a.g.e.*, 86.

Cambridge Analytica, Facebook verilerinin yanı sıra devletlerin önemli kurumlarından çektiği verileri de kullanmış ve veri analitiği dışında bal tuzakları, rüşvet ve şantaj gibi birçok başka yönteme de müracaat etmiştir.[331] Cambridge Analytica ve SCL, Siber İstihbarat yöntemleri, Sosyal Medya İstihbaratı (SOCMINT), büyük veri analitiği ve İnsan İstihbaratı (HUMINT) unsurlarından faydalanmıştır. Söz konusu ekstra yöntemlerin kullanımı, sosyal medyanın örtülü operasyonlar için hangi ölçülerde ve ne derece elverişli olduğu sorusuna cevap arama ihtiyacı doğurmuştur. Bu çalışmada, sosyal medyayı mevcut koşullar içerisinde örtülü operasyonlara uygun bir zemin hâline getiren unsurlar; yapay zekâ, siber güvenlik, veri bilimi, psikoloji, uluslararası hukuk, örtülü operasyonlar ve örnek vaka olarak Cambridge Analytica perspektifinde incelenmiş ve sosyal medya şirketlerinin sunduğu hizmetler ile uygulama yöntemleri etraflıca analiz edilmiştir. Analiz, yapay zekânın yakın gelecekte sosyal medyada örtülü operasyonun birincil unsuru hâline gelebileceğini ortaya koymuştur. Analiz sürecinde kişilere ve kullanıcıların kişisel verilerine erişiminin yanı sıra, yapay zekâ sayesinde üretilen propagandanın etki imkânının da arttığı ortaya çıkmış ve yasal caydırıcı unsurların eksikliği anlaşılmıştır.

Ancak, yapay zekânın siber güvenlik aygıtı olarak da kullanılabileceği anlaşılmıştır. Bu kabiliyetin geliştirilmesine yönelik çalışmalar, sosyal medyanın yapay zekâ ile örtülü operasyona elverişli bir konuma gelmesi durumunu tamamen ortadan kaldırmasa da kısmen güçleştirebilecektir. Yine sosyal medyada yayılan dezenformasyonu tespit edebilen yapay zekâ yöntemlerinin de geliştirilebileceği anlaşılmıştır. Analizde müşahede edilen önem sırası dolayısıyla bu konuda öncelikli olarak sosyal medya kullanıcılarının bilinçlenmesinin oldukça önemli olduğu ortaya çıkmıştır. Siber saldırı yöntemlerinden biri olan sosyal mühendislik saldırılarında en büyük güvenlik açığı insan zafiyetidir. Kullanıcıların ziyaret ettikleri web sitelerindeki çerez politikalarını okumadan kabul etmeleri, keza kullandıkları sosyal medya şirketlerinin sunduğu gizlilik sözleşmelerini okumadan onaylamaları, ücretsiz olarak kullandıkları birçok hizmette aslında ücretin kişisel verileri olduğu bilincinden yoksun olmaları yahut tüm bunları önemsememeleri, söz konusu konunun ilk güvenlik

[331] Harrison, *a.g.e.,* https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections. [Erişim Tarihi: 01.11.2020].

açığıdır. Bu doğrultuda, bir siber güvenlik bileşeni olan son kullanıcı eğitiminin, kullanıcıların yalnızca siber saldırıların hedefi olmaktan korunması amacının ötesine geçip sosyal medyada algı yönetimine maruz kalmaması yönünde genişletilmesi gerekmektedir. Bu konuda devletler kadar sivil toplum kuruluşları ve konunun bilincinde olan aktivistler ile vatandaşlara da görev düşmektedir. Öncelikle bir sosyal medya kullanıcısının kendisinde şaşkınlık, öfke gibi ani duygusal tetiklenmelere sebep olan gönderileri gördüğünde söz konusu gönderiyi neden gördüğünü sorgulayacak farkındalığa erişmiş olması gerekir. Devletlerin de vatandaşlarının kişisel verilerini korumaları için geliştirebilecekleri yöntemler vardır. Bir örnek olarak Çin Halk Cumhuriyeti'nde 1 Kasım 20212'de yürürlüğe giren *"Kişisel Enformasyonu Koruma Yasası"* ile, kişisel enformasyonun işlenmesi hususunda bireysel izin almayı ve yurt dışı menşeli şirketlerin işledikleri kişisel enformasyonu Çin Anakarası'ndan çıkarabilmeleri için, öncelikle ÇHC siber uzay yetkilileri tarafından yapılan güvenlik değerlendirmesinden geçmek, gereken sertifikayı almak ya da siber uzay yetkililerinin öngördüğü standart bir mukavele imzalamak gibi belirli sınırlama ve şartlar getirilmiş, kararı ihlâl eden şirketler için para cezası, işletme faaliyetlerinin durdurulması, şirket lisanslarının iptali gibi yaptırımlar öngörülmüştür.[332] Söz konusu yasa kısıtlayıcılığı nedeniyle demokrasi yönünden tartışmaya açık olsa da, vatandaşların kişisel verilerinin istismarını engellemek adına devletler benzer önlemler alabileceklerdir. Bir diğer öneri ise, devletlerin sosyal robotları tespit edebilecek yapay zekâ programlarının gelişimine öncelik vermeleridir. Böyle bir girişim, devletlerin kendi vatandaşlarını dezenformasyona karşı daha etkin bir şekilde korumaları açısından faydalı olabilecektir.

Uluslararası örgütlerin de siber çağda dezenformasyon konusunda ciddiyet teşkil eden bir farkındalık ile aksiyonlar almaları yararlı olacaktır. Bu konuda 27 Kasım 2018'de yirmi bir ülkeden bakanlar, gazeteciler, parlamenterler, uzmanlar ve teknoloji girişimlerinin yer aldığı açılış oturumu ile faaliyetlerine başlayan ve misyonunu *"çevirim içi dezenformasyon, nefret söylemi ve seçim müdahaleleriyle mücadeleye*

---

[332] The Office of the Privacy Commissioner for Personal Data (PCPD), "Personal Information Protection Law of the Mainland", Hong Kong, https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html. [Erişim Tarihi: 28.11.2022].

yönelik ortak etkili stratejiler ve uluslararası ittifaklar oluşturmak ve söz konusu konular ile ilgili soruşturmalarına öncülük etmek" olarak ilan eden[333] Dezenformasyon ve Sahte Haberler Büyük Komitesi (International Grand Committee on Disinformation/ IGC) yaptırım mekanizmasına sahip olmaması yönüyle etkinliği tartışmalı olabilse de, ilan ettiği misyon bakımından yararlı olabilecektir. Ayrıca Temmuz 2016'da Varşova'da gerçekleşen NATO Zirvesi'nde, NATO liderlerinin siber savunmaya kaynak temin etmenin birincil öncelik olarak kabul etmeleri[334] iyi bir girişim olmakla birlikte caydırıcılık yönünden henüz yeterli değildir.

Stratejik boyutta devletlerin, vatandaşlarını dezenformasyondan sakınabilmeleri adına gerek yapay zekâ alanına ciddiyetle eğilmeleri ve bu konuda AR- GE çalışmalarına ağırlık vermeleri, gerekse ÇHC modelinde olduğu gibi vatandaşları için tercih edilebilir gelişmişlikte yerli sosyal medya platformlarını geliştirmeleri hem vatandaşlarının verilerinin hasım kanalların eline geçmesi hem de siber korsanlık ve etki operasyonlarına karşı daha fazla kontrol sahibi olabilmeleri adına yararlı olabilecektir.

Sonuç olarak, sosyal robotlar ve diğer yapay zekâ analitikleri ile sosyal medyada yürütülecek örtülü operasyonlar, Ray Steiner Cline'ın Algılanan Güç formülünde sonucu önemli derecede etkileyebilecek bir çarpan olan *"ulusal stratejiyi takip etme arzusu"* bakımından toplumları yönlendirebilme kabiliyetindedir. Her ne kadar yapay zekâ alanındaki gelişmeler, sosyal medyanın sunduğu serbest kürsü ortamı ve veri havuzu ile siber uzayın ontolojik olarak gizliliğe sunduğu katkı örtülü operasyon kabiliyetlerine katkı sağlıyor olsalar da; devletlerin toplumlarına sundukları güven, huzur, refah ve olabildiğince şeffaf bir yönetim tarzı, toplumlarını hasım odakların girişimlerinden koruyabilmelerinin en etkili yollarındandır. Bu anlamda eski CIA operasyon görevlisi William Daugherty'nin *"Her ne kadar propagandanın kısmî veya tamamen yanlıştan oluştuğu sık sık bir varsayım olsa da, aslında en iyi propaganda,*

---

[333] International Grand Committee on Disinformation, " Who We Are", https://www.igcd.org/who-we-are/. [Erişim Tarihi: 31.12.2022].

[334] Robinson, *a.g.e.,* https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html [Erişim Tarihi: 12.07.2022].

iyi sunulan ve iyi tartışılan gerçektir" [335] ifadesi, *"manipüle olmaya hazır"* hâle gelmiş bir toplumun, yabancı servislerin yönlendirmelerine ne kadar açık olabilecekleri fikrine önemli bir vurgudur.

[335] Daugherty, "The Discipline of Covert Action", 73.

KAYNAKÇA

http://strata.oreilly.com/2010/01/roger-magoulas-on-big-data

AggregiateiQ Data Services. "Intellectual Property Rights". (28 Mart 2014): 4- 18.

Aghaei, Sareh, Mohammad Ali Nematbakhsh, Hadi Khosravi Farsani, "Evolution of The World Wide Web: From Web 1.0 to Web 4.0", *International Journal of Web & Semantic Technology (IJWesT)*. C.3. S.1 (Ocak 2012).

Anderson, E. Elizabeth. "The Security Dilemma and Covert Action: The Truman Years*". International Journal of Intelligence and CounterIntelligence*. C.11. S.4 (1998): 403– 427. doi:10.1080/08850609808435385.

Andrew, Christopher, Richard J. Aldrich, Wesley K. Wark, "Introduction", Secret Intelligence: A Reader. ed. Christopher Andrew, Richard J. Aldrich, Wesley K. Wark. Oxon: Routledge, 2020, 1-3.

Arslankaya, Seher, Kübra Göraltay. "Analitik Hiyerarşi Prosesi Yöntemi". *Çok Kriterli Karar Verme Yöntemlerinde Güncel Yaklaşımlar.* Ankara: İksad Yayınevi, 2019.

Ashworth, Louis, Todd Gillespie. "Who is Dr Aleksandr Kogan, the Cambridge Academic Accused of Misusing Facebook Data?". *Varsity*. 17 Mart 2018. https://www.varsity.co.uk/news/15192. [Erişim Tarihi: 10.12.2022].

Ataç, Kaan Kutlu. "İstihbarat, Casusluk, Karşı Casusluk, Örtülü Operasyonlar ve Güvenlik". *Güvenlik Yazıları Serisi*. S. 45 (2019): 1- 10. DOI: 10.13140/RG.2.2.22313.95849.

Ausiello, Giorgio. "Algorithms, An Historical Perspective". *The Power of Algorithms*. ed. Rossella Petreschi. Berlin: Springer, 2013. doi:10.1007/978-3-642-39652-6_1.

AUSPEX. https://www.auspex.ai/. [Erişim Tarihi: 20.12.2022].

AWS. "Siber Güvenlik Nedir?". https://aws.amazon.com/tr/what-is/cybersecurity/. [Erişim Tarihi: 24.11.2022].

Axon, Samuel. "Facebook's Open Graph Personalizes the Web". *Mashable.com*. 21 Nisan 2010. https://mashable.com/archive/facebook-open-graph#WQ_Po8XekkqE. [Erişim Tarihi: 12.12.2022].

Barnes Bart. The Washington Post. '' Edward Lansdale, Prototype For 'Ugly American,' Dies'', https://www.washingtonpost.com/archive/local/1987/02/24/edward-lansdale-prototype-for-ugly-american-dies/d2ff2042-05c8-4f1d-b12d-972bf8338b14/.

Bayraktar, Gökhan. "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat". *Güvenlik Stratejileri Dergisi*. C.10. S.20 (2013): 119- 147.

BBC News. "Cambridge Analytica Staff Set Up New Firm", 12 Temmuz 2018, https://www.bbc.com/news/technology-44807093. [Erişim Tarihi: 20.12.2022].

_____."Cambridge Analytica: The Data Firm's Global Influence". 22 Mart 2018. https://www.bbc.com/news/world-43476762. [Erişim Tarihi: 09.12.2022].

_____."Uni Drops Cambridge Analytica Executive as Fellow", 22 Mart 2018, https://www.bbc.com/news/uk-england-devon-43506270. [Erişim Tarihi: 20.12.2022].

Biddle, WM. W., "A Psychological Definition of Propaganda", *The Journal of Abnormal and Social Psychology. C.26.* S.3 (1931): 283- 295. https://doi.org/10.1037/h0074944.

Birleşmiş Milletler Antlaşması. 26 Haziran 1945. San Francisco. https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf. [Erişim Tarihi: 28.12.2022].

Brei, William F. "Getting Intelligence Right: The Power of Logical Procedure". *Learning With Professionals*. Washington DC: Joint Military Intelligence College, 2005, 47- 76.

CA Political. "Italy". *Cambridge Analytica*. 29 Mayıs 2014. https://ca-political.com/casestudyitaly/.

Cadwalladr, Carole, Emma Graham-Harrison. "Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University". *The Guardian*. 17 Mart 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university. [Erişim Tarihi: 10.12.2022].

CERN Accelerating Science. "Where the Web was born". https://home.cern/science/computing/birth-web/short-history-web, [23.10.2022].

Channel 4 News. "Cambridge Analytica Uncovered: Secret Filming Reveals Election Tricks" [Video], *YouTube*, 19 Mart 2018, https://www.youtube.com/watch?v=mpbeOCKZFfQ.

Clausewitz, Carl Von. "War Is an Instrument of Policy". On War. çev. Michael Howard and Peter Paret. .New York: Oxford University Press, 2007.

Cline, Ray Steiner. "Elements of Power: The Formula". *World Power Trends and U.S. Foreign Policy for the 1980s*. New York, Routledge, 2019, 30- 41.

Concordia. (27 Eylül 2016). Cambridge Analytica - The Power of Big Data and Psychographics [Video]. YouTube.

https://www.youtube.com/watch?v=n8Dd5aVXLCc. [Erişim Tarihi: 20.10.2020].

Cormac, Rory, Richard J. Aldrich. "Grey is the New Black: Covert Action and Implausible Deniability". *International Affairs*. C.94. S.3. 2018: 477- 494. https://doi.org/10.1093/ia/iiy067.

Cox, Michael, David Ellsworth. "Application-Controlled Demand Paging for Out-of-Core Visualization". NASA. California: NASA, 1997.

CrowdStrike. *2022 Global Threat Report*. (2022)

Cullather, Nick. Illusions of Influence: The Political Economy of United States-Philippines Relations 1942- 1960. Stanford University Press, 1994.

Cybersecurity and Infrastructure Security Agency (CISA). "Avoiding Social Engineering and Phishing Attacks", Security Tip (ST04-014), 25 Ağustos 2020. https://www.cisa.gov/uscert/ncas/tips/ST04-014. [Erişim Tarihi: 25.11.2022].

D1gi. "Itemized Posts and Historical Engagement - 6 Now-Closed FB Pages". *Tableau Public*. 5 Ekim 2017. https://public.tableau.com/app/profile/d1gi/viz/FB4/TotalReachbyPage. [Erişim Tarihi: 10.12.2022].

DARPA. "About DARPA". https://www.darpa.mil/about-us/about-darpa, [Erişim Tarihi: 23.10.2022].

_____."ARPANET". https://www.darpa.mil/about-us/timeline/arpanet [Erişim Tarihi: 23.10.2022].

Daugherty, William J. "The Discipline of Covert Action". *Executive Secrets: Covert Action and The Precidency*. Kentucky: The University Press of Kentucky, 2004).

_____."The Role of Covert Action in Intelligence and Foreign Policy". *Executive Secrets:Covert Action and The Precidency*. Kentucky: The University Press of Kentucky, 2004.

Davies, Philip. "Ideas of intelligence: Divergent national concepts and institutions". Secret Intelligence: A Reader, ed. Christopher Andrew, Richard J. Aldrich, Wesley K. Wark. Oxon: Routledge, 2020, 13- 20.

Defense Science Board. "Resilient Military Systems and the Advanced Cyber Threat". Washington DC, (01.01.2013).

Diebold, Francis X. "'Big Data' Dynamic Factor Models for Macroeconomic Measurement and Forecasting". *Advances in Economics and Econometrics*. Theory and Applications: Eighth World Congress, 2003.

Doğan, Tayfun. ‘’Beş Faktör Kişilik Özellikleri Ve Öznel İyi Oluş’’. *Doğuş Üniversitesi Dergisi*. C. 14. S. 1 (2013).

Dokman, Tomislav. “Defining the Term "Intelligence" - Insight into Existing Intelligence Knowledge. *Informatologia*. C. 52. S. 3- 4. (2019): 194–205. doi:10.32914/i.52.3-4.7

Doob, Leonard W. “Goebbels' Principles of Propaganda”. *The Public Opinion Quarterly*. C. 14. S. 3 (1950): 419–442.

Doward, Jamie, Alice Gibbs, “Did Cambridge Analytica Influence the Brexit Vote and the US Election?”, *The Guardian*. 04.03.2017. https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump. [Erişim Tarihi: 05. 02. 2023].

Doyle, Kate, Peter Kornbluh. “CIA and Assassinations: The Guatemala 1954 Documents”. *National Security Archive Electronic Briefing: Book No. 4.* https://nsarchive2.gwu.edu/NSAEBB/NSAEBB4/. [Erişim Tarihi: 31.12.2022].

EAP. “From a Presidential Campaign to a Data Analytics Start-Up – Civis Analytics”. *Digital Innovation and Transformation of Harvard University*. 1 Şubat 2018. https://d3.harvard.edu/platform-digit/submission/from-a-presidential-campaign-to-a-data-analytics-start-up-civis-analytics/. [Erişim Tarihi: 20.12.2022].

EDVAC. Encyclopedia of Computer Science. ACM Digital Library. https://dl.acm.org/doi/abs/10.5555/1074100.1074362. [Erişim Tarihi: 26.09.2022].

Ekinci, Gül, Fatma Gül Bilginer- Özsaatçi. “Yapay Zekâ ve Pazarlama Alanındaki Yayınların Bibliyometrik Analizi”. *Sosyoekonomi*. C. 31. S. 56 (2023): 369- 388.

Epstein, William, Louis Jolyon West, William N. Dember. "Perception". *Encyclopedia Britannica*, 14 Ekim. 2022. https://www.britannica.com/topic/perception. [Erişim Tarihi: 16 Ekim 2022].

Eyüpoğlu, Can ve diğ. “Büyük Veride Kişi Mahremiyetinin Korunması”. *Bilişim Teknolojileri Dergisi*. C.10. S.2. (2017): 177- 184. https://doi.org/10.17671/gazibtd.309301.

Fan, Weiguo, Michael D. Gordon. “The Power of Social Media Analytics”. *Communications of the ACM*. C.57. S.6 (2014): 74- 81. doi:10.1145/2602574.

Feifer, Gregory. “Czech Power Games: How Russia is Rebuilding Influence in The Former Soviet Bloc”. *Radio Free Europe*. 25 Eylül 2010.

https://www.rferl.org/a/Czech_Mate_How_Russia_Is_Rebuilding_Influence_In_The_Former_Soviet_Bloc/2168090.html. [Erişim Tarihi: 10.12.2022].

Fletcher, Emma. "Social Media a Gold Mine for Scammers in 2021". Data Spotlight. 25 Ocak 2022. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021#footnote1. [Erişim Tarihi: 24.11.2022].

Foote, Keith D. "A Brief History of Big Data". https://www.dataversity.net/brief-history-big-data/. [Erişim Tarihi: 14.07.2022].

Friess, Steve. "The father of All Web Campaigns". *Politico*. 30 Eylül 2012. https://www.politico.com/story/2012/09/how-deans-wh-bid-gave-birth-to-web-campaigning-081834. [Erişim Tarihi: 20.12.2022].

García-Díaz, José Antonio, Ricardo Colomo-Palacios, Rafael Valencia-García. "Psychographic Traits İdentification Based on Political İdeology: An Author Analysis Study on Spanish Politicians' Tweets Posted in 2020". *Future Generation Computer Systems*. C.130 (2022): 59- 74. https://doi.org/10.1016/j.future.2021.12.011.

Gerasimov, Valery. "The Value of Science is in the Foresight". *Military Review*. (2016): 23- 29.

Godson, Roy. "Handmaiden of Policy: Principles of Covert Action". *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*. New Brunswick: Transaction Publishers, 2011.

Goodman, Allan E. "Reforming U. S. Intelligence". *Foreign Policy. C. 67 (1987): 121- 136.* DOI:10.2307/1148934.

Google Patents. "Determining User Personality Characteristics From Social Networking System Communications and Characteristics". US13/608,943. 10.09.2012. https://patents.google.com/patent/US8825764B2/en. [Erişim Tarihi: 19.12.2022].

Graham-Harrison, Emma. Cadwalladr, Carole. Osborne, Hilary. "Cambridge Analytica Boasts of Dirty Tricks to Swing Elections". The Guardian, 19 Mart 2018. https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections. [Erişim Tarihi: 01.11.2020].

Gülenç, İrem Figen, Gülşah Aydın Bilgin. "Yatırım Kararları İçin Bir Model Önerisi: AHP Yöntemi". Öneri Dergisi. C. 9. S. 34 (2010): 97- 107.

Herrington, Lewis. "Cyberespionage and Cyberwar", *Secret Intelligence: A Reader*. ed. Christopher Andrew, Richard J. Aldrich, Wesley K. Wark. 2. bs. Oxon: Routledge, 2020, 566- 582.

Heuer, Richards, Randolph H. Pherson. “Hypothesis Generation and Testing”. *Structured Analytic Techniques for Intelligence Analysis*. 2. bs. California: CQ Press, 2015.

Heuer, Richards. “Our Mental Machinery”. *Psychology of Intelligence Analysis*. (1999: Center for the Study of Intelligence). ISBN 1 929667-00-0.

Horvitz, Eric. “Reflections on the Status and Future of Artificial Intelligence”. *Before The Committee on Commerce Subcommittee on Space, Science, and Competitiveness United States Senate: Hearing on the Dawn of Artificial Intelligence*.(2016). http://erichorvitz.com/Senate_Testimony_Eric_Horvitz.pdf. [Erişim Tarihi: 12.10.2022].

Hürriyet Gazetesi. “Türk Askerinden Yürekleri Isıtan Paylaşım”. 09.01.2017. https://www.hurriyet.com.tr/video/turk-askerinden-yurekleri-isitan-paylasim-40330519 [Erişim Tarihi: 08.11.2022].

Iasiello, Emilio. “Cyber Attack: A Dull Tool to Shape Foreign Policy”. *5th International Conference on Cyber Conflict*. ed. K. Podins, J. Stinissen, M. Maybaum. Tallinn: NATO CCD COE Publications, 2013.

IBM. “What is cybersecurity?”. https://www.ibm.com/topics/cybersecurity. [Erişim Tarihi: 22.11.2022].

_____.“What is predictive analytics?”. https://www.ibm.com/analytics/predictive-analytics#:~:text=Predictive%20analytics%20is%20a%20branch,to%20identify%20risks%20and%20opportunities. [Erişim Tarihi: 20.07.2022].

ICO. *What Is Microtargeting?*, https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting/. [Erişim Tarihi: 10.11.2022].

Instagram Business. “Instagram’da Reklam Verilmesi”. https://business.instagram.com/advertising?locale=tr_TR. [Erişim Tarihi: 10.11.2022].

International Court of Justice. “Case Concerning Miliıtary and Paramilitary Activiiıes in and Against Nicaragua”. *Reports of Judgments: Advisory Opinions and Orders*. (27 Haziran 1986).

International Law Commission. “Draft Articles on Responsibility of States for Internationally Wrongful Acts”, Kasım 2001, Ek No. 10 (A/56/10), b. 2. md.5, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [Erişim Tarihi: 28.12.2022].

Işıklı, Şevki. “Büyük Veri, Epistemoloji ve Etik Tartışmalar”. *AJIT-e: Online Academic Journal of Information Technology*. C.5. S.17 (2014): 89- 122. DOI: 10.5824/1309-1581.2014.4.006.x.

İTÜ Yapay Zekâ ve Veri Mühendisliği. "Bilgisayarla Görü". https://yapayzeka.itu.edu.tr/arastirma/bilgisayarla-goru. [Erişim Tarihi: 18.02.2023].

Jobson, Barney. "Facebook to Release 3,000 Russian-Bought Election Ads". *Financial Times*. 22 Eylül 2017. https://www.ft.com/content/de59ab54-9f03-11e7-8cd4-932067fbf946. [Erişim Tarihi: 04.06.2022].

Johnson, Loch. K. "The Forms of Covert Action". *The Third Option: Covert Action and American Foreign Policy*. New York: Oxford University Press, 2022,19- 39.

Johnson, Loch. K., "Introduction". *Handbook of Intelligence Studies*. ed. Loch. K. Johnson. Oxon: Routledge, 2007, 1- 14.

Joseph, Rhoda C. Norman A. Johnson, "Big Data and Transformational Government", *IT Professional*, C.15, S.6, (2013):43- 48. DOI:10.1109/mitp.2013.61.

Kaplan, Andreas M. Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media". *Business Horizons*. C. 53. S. 1 (2010): 59- 68.

Kassarjian, Harold H. "Personality and Consumer Behavior: A Review". *Journal of Marketing Research*. C.8. S.4 (1971):409- 418. DOI:10.2307/3150229.

Kent, Sherman. "Intelligence is Knowledge". *Strategic Intelligence for American World Policy*. Hamden: Archon Books, 1965, 3- 10.

Kent, Sherman. "Producers and Consumers of lntelligence". *Strategic Intelligence for American World Policy*. Hamden: Archon Books, 1965, 180- 209.

Khillar, Sagar. "Difference Between Dark Post and Boost Post". *DifferenceBetween.Net*.http://www.differencebetween.net/technology/differen_ce-between-dark-post-and-boost-post/. [Erişim Tarihi: 24.12.2022].

Kibaroğlu, Mustafa. "11 Eylül Ardından Strateji, Tehdit ve Caydırıcılık". *Foreign Policy*. (2002). http://www.mustafakibaroglu.com/sitebuildercontent/sitebuilderfiles/Kibaroglu-11EylulArdndanStratejiTehditCaydiricilik-22dec01.pdf.

_____."Amerikan Ulusal Füze Savunma Sistemi". *Avrasya Dosyası - Amerika Özel Sayısı*. C.6. S.3 (2000): 90- 105.

Kidd, Chrissy, Rachel Hornay. "Data Analytics vs Data Analysis: What's The Difference?". *BMC*. 8 Ocak 2021. https://www.bmc.com/blogs/data-analytics-vs-data-analysis/ [Erişim Tarihi: 20.07.2022].

Kirchgaessner, Stephanie, Manisha Ganguly, David Pegg, Carole Cadwalladr, Jason Burke. "Revealed: the hacking and disinformation team meddling in elections". *The Guardian*. 15.02.2023. https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-_____ team-jorge-claim-meddling-elections-tal-hanan. [Erişim Tarihi: 21.02.2023].

Knaus, Christopher. “Facebook Appeal Over Cambridge Analytica Data Rejected by Australian Court as Divorced From Reality”. *The Guardian*. 7 Şubat 2022. https://www.theguardian.com/technology/2022/feb/07/facebook-appeal-over-cambridge-analytica-data-rejected-by-australian-court-as-divorced-from-reality. [Erişim Tarihi: 09.12.2022].

Koch, Scott A. “Zendebad, Shah!: The Central Intelligence Agency and the Fall of Iranian Prime Minister Mohammad Mossadeq, August 1953”. *National Security Archieve*. CIA History Staff: Washington DC, 1998/ 2017. https://nsarchive.gwu.edu/dc.html?doc=4375470-Document-2-Zendebad-Shah. [Erişim Tarihi: 13.09.2020].

Kowalkiewicz, Marek. “How did we get here? The story of algorithms”. *Towards Data Science*. https://towardsdatascience.com/how-did-we-get-here-the-story-of-algorithms-9ee186ba2a07#_ftn2. [Erişim Tarihi: 17.02.2023].

Landler, Mark, John Markoff. “Digital Fears Emerge After Data Siege in Estonia”. *The NewYork Times.* 29 Mayıs 2007. https://www.nytimes.com/2007/05/29/technology/29estonia.html. [Erişim Tarihi: 03.10.2022].

Lee, Amanda. “What is China’s Social Credit System and Why Is It Controversial?”. *South China Morning Post*. 09.08.2020. https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial. [Erişim tarihi: 21.02.2023].

Lee, Sugnwon. “Covert Action as a Foreign Policy Tool of The U.S.: Explaining the Role of Secrecy”. Yüksek Lisans Tezi, Graduate Faculty of The University of Georgia, 2010.

Lerner, Daniel. “Policy and Propaganda In World War II”. *Psychological Warfare Against Nazi Germany: The Sykewar Campaign, D-Day to VE- Day*. Cambridge: MIT Press, 1971, 1- 17. ISBN: 9780262620192.

_____. “Sykewar Themes”. *Psychological Warfare Against Nazi Germany: The Sykewar Campaign, D-Day to VE- Day*. Cambridge: MIT Press, 1971, 164-193. ISBN: 9780262620192.

Lesser, Jack A. Marie Adele Hughes. “The Generalizability of Psychographic Market Segments across Geographic Locations”. *Journal of Marketing.* C. 50. S. 1 (1986): 18- 27. DOI:10.1177/002224298605000102.

Levin, Dov H. ‘’When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results’’. *International Studies Quarterly*. C. 60. S. 2 (2016): 189-202. https://doi.org/10.1093/isq/sqv016.

_____. “Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset”. *Conflict Management and Peace Science.* (2016): 1- 19. doi:10.1177/0738894216661190.

_____. "Throwing Their Hat into the Ring When Electoral Interwentions Occur", *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions*. New York: Oxford University Press, 2020, 76- 143.

Li, Yuchong, Qinghui Liu, "A Comprehensive Review Study of Cyber Attacks and Cyber Security; Emerging Trends and Recent Developments", *Energy Reports*, C.7 (2021): 8176–8186.

LinkedIn. https://www.linkedin.com/in/marknturnbull/?originalSubdomain=uk. [Erişim Tarihi: 20.12.2022].

Lowenthal, Mark M. "Covert Action". *Intelligence : From Secrets to Policy*. 8. bs. Thousand Oaks: CQ Press, 2020, 370-410. ISBN 9781544358376 (epub).

Lukoil. "Lukoil Signs Cooperation Agreement Wıth Federal Security Service of Russian Federation". 23 Mayıs 2017. https://www.lukoil.com/PressCenter/Pressreleases/Pressrelease?rid=118730. [Erişim Tarihi: 10.12.2022].

MacFarlane, Neil, Natalie Sabanadze. "Sovereignty and Self-Determination: Where Are We?". *International Journal.* C. 68. S. 4 (2013): 609– 627. http://www.jstor.org/stable/24709362.

Makers Turkiye. "Veri Analizi ve Veri Analitiği Aynı Şey midir?". https://makersturkiye.com/veri-analizi-ve-veri-analitigi-ayni-sey-midir/. [Erişim Tarihi: 20.07.2022]

Math, Rajesh. "Big Data Analytics: Recent and Emerging Application in Services Industry". *In Advances in Intelligent Systems and Computing Big Data Analytics*. C. 654. Singapore: Springer, 2018, 211- 219. DOI:10.1007/978-981-10-6620-7_21. [Erişim Tarihi: 21.06.2022].

Matz, Sandra, Ruth Appel, Michal Kosinski. "Privacy in the Age of Psychological Targeting". *Current Opinion in Psychology*. (2019). doi:10.1016/j.copsyc.2019.08.010.

McAfee, Andrew, Erik Brynjolfsson. "Big Data: The Management Revolution". *Harvard Business Review*. (Ekim, 2012). https://hbr.org/2012/10/big-data-the-management-revolution. [Erişim Tarihi: 12.11.2022].

McAfee. "Staying Safer on Social Media". *The McAfee Safety Series.* https://www.mcafee.com/content/dam/consumer/en-us/docs/guides/gd-staying-safer-social-media-guide.pdf. [Erişim Tarihi: 24.11.2022].

McGrath, Chris. "Principles of Sovereignty Under International Law". (10 Aralık 2018). http://envlaw.com.au/wp-content/uploads/handout_sovereignty.pdf. [Erişim Tarihi: 22.12.2022].

Meta Inc. "Audience Network Nasıl Çalışır?". https://www.facebook.com/business/help/987564874649426?id=21141211_____0064838. [Erişim Tarihi: 24. 12.2022].

Milli Savunma Üniversitesi İstihbarat Çalışmaları Bölümü Ders Notları.

Mohammed, Ahmed Foad, Vikas T. Humbe, Santosh S. Chowhan. "A Review of Big Data Environment and Its Related Technologies". International Conference On Information Communication and Embedded System. (2016): 1- 5. DOI: 10.1109/ICICES.2016.7518904.

Morgenthau, Hans. "International Politics as a Struggle for Power". *Politics Among Nations: The Struggle for Power and Peace.* New York: Alfred A. Knopf, 1948, 13- 69.

Müller-Merbach, Heiner. "Francis Bacon's Praise: Knowledge, The Source of Power". *Knowledge Management Research & Practice.* C. 3. S. 1 (2005): 45- 46. doi:10.1057/palgrave.kmrp.8500048.

National Institute of Standards and Technology. "Glossary", Information Security, Eylül 2012, B- 2.

Newman, Lily Hay. "Mobile Websites Can Tap Into Your Phone's Sensors Without Asking". *Wired.* 26 Eylül 2018. https://www.wired.com/story/mobile-websites-can-tap-into-your-phones-sensors-without-asking/. [Erişim Tarihi: 24.12.2022].

Nguyen, Nicole. "Here's How Facebook Got Into This Mess: A Timeline". *BuzzFeed.News*. 22 Mart 2018. https://www.buzzfeednews.com/article/nicolenguyen/cambridge-analytica-facebook-timeline. [Erişim Tarihi: 12.12.2022].

Nica, Elvira, Lubica Gajanova, Eva Kicova. "Customer Segmentation Based on Psychographic and Demographic Aspects as a Determinant of Customer Targeting in The Online Environment". *Littera Scripta,* C. 12, S. 2 (2019): 108- 126. https://doi.org/10.36708/Littera_Scripta2019/2/0.

Nye, Joseph S., David A. Welch. "Nükleer Silahların Rolü: Fizik ve Politika". *Küresel Çatışmayı ve İşbirliğini Anlamak*. çev. Renan Akman. Beyoğlu: Türkiye İş Bankası ve Kültür Yayınları, 2017.

O'hare, Liam. "SCL and the Phantom Contract". *Bella Caledonia.* 22 Mart 2018. https://bellacaledonia.org.uk/2018/03/22/scl-and-the-phantom-contract/.[Erişim Tarihi: 20.12.2022].

O'Rourke, Lindsey A. "The False Promise of Covert Regime Change". *Convert Regime Change : America's Secret Cold War*. Ithaca: Cornell University Press, 2018, 1- 21.

OECD. “Defining and Measuring the Participative Web and User-Created Content”. *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking*. (2007): 17- 26. ISBN 978-92-64-03746-5.

Office Of the Australian Information Comissisioner. “Commissioner Launches Federal Court Action Against Facebook”. 9 Mart 2020. https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook. [Erişim Tarihi: 20.12.2022].

Office Of the Historian. “Document 292: National Security Council Directive on OfficeOf Special Projects (NSC 10/2, Md.5)”. U.S. Department of State (Washington, 18. 05. 1948). https://history.state.gov/historicaldocuments/frus1945-50Intel/d292. [Erişim Tarihi: 13.12.2022].

Oxford Dictionary. *“Algorithm”.* https://dictionary.cambridge.org/dictionary/english/algorithm. [Erişim Tarihi: 17.02.2023].

Öz, Burak. “Bilgisayarın Tarihçesi”. slayt 11. https://cdn3.beun.edu.tr/insaat/f6342b2189e35b8d6f273e9455060f69/bilgisayar-kullanimi.pdf. [Erişim Tarihi: 26.09.2022].

Partisan CIA and TPAJAX: The Tension Between Analysis and Operations. (2017). https://nsarchive.files.wordpress.com/2018/03/cia-and-operation-tpajax.pdf. [Erişim Tarihi: 24.12.2022].

Platon. “Birinci Kitap”. *Devlet*. Çev. Sabahattin Eyüboğlu ve M. Ali Cimcoz. Beyoğlu: Türkiye İş Bankası Kültür Yayınları, 1999.

Pop, Hristina. “EU vs US: What Are the Differences Between Their Data Privacy Laws?”. *Endpoint Protector*. 27 Eylül 2022. https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws/. [Erişim Tarihi: 18.12.2022].

Radsan, John A. “An Overt Turn on Covert Action”. *St Louis University School of Law Journal*. C. 53. S. 2 (2009): 486- 552.

Retruster Website. “2019 Phishing Statistics and Fraud Statistics”. https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html. (Erişim Tarihi: 10.04.2019)’den aktaran Sanchari Das ve diğ. “All About Phishing: Exploring User Research through a Systematic Literature Review”. 2019. http://arxiv.org/abs/1908.05897. [Erişim Tarihi: 10.11.2022].

Robinson, Neil. “Spending for Success on Cyber Defence”. *NATO Review*. 6 Nisan 2017. https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html [Erişim Tarihi: 12.07.2022].

Rock, Irvin, Stephen Palmer. “The Legacy of Gestalt Psychology”. *Scientific American*. C. 263. S. 6. (1990): 84- 91.

Ruiz, Rebecca R. “Robert Mueller, Former F.B.I. Director, Is Named Special Counsel for Russia Investigation”. *The New York Times*. 17 Mayıs 2017. https://www.nytimes.com/2017/05/17/us/politics/robert-mueller-special-counsel-russia-investigation.html. [Erişim Tarihi: 11.12.2022].

Russel, Alison Lawlor. " The Logic Layer". *Stratejik A2/ AD in Cyberspace.* Cambridge: Cambridge University Press, 2017, 40- 52. doi:10.1017/9781316817001.004.

Russell, Stuart J., Peter Norvig. “What Is AI?”. *Artificial Intelligence: A Modern Approach.*1995: Prentice-Hall, New Jersey, 4- 7.

Scott, Len, Peter Jackson. “The Study of Intelligence in Theory and Practice”. *Intelligence and National Security*. C. 19. S. 2 (2004): 139- 169. DOI: 10.1080/0268452042000302930.

Segal, Adam, Gordon M. Goldstein. “Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet”. *Independent Task Force Report: No.80, CFR*. (Temmuz 2022).

Shulman, Stephen ve Stephen Bloom, ‘’The Legitimacy of Foreign İntervention in Elections: The Ukrainian Response’’, *Review of International Studies.* C. 38. S. 2 (2012): 445–471. DOI:10.1017/S0260210512000022.

Shulsky, Abram. “Elements of Strategic Denial and Deception”. *Strategic Denial and Deception: The Twenty-First Century Challenge*. ed. Roy Godson, James J. Wirtz. Oxon: Routledge, 2017, 23- 50.

_____. “Toward a Theory of Intelligence”. Silent Warfare: Understanding the World of Intelligence. 2. bs. New York: Brassey’s US, 1993, 169- 176.

_____. “What Is Covert Action?”. *Silent Warfare: Understanding the World of Intelligence.* 2. bs. New York: Brassey’s US, 1993, 75- 97.

_____. “What Is Intelligence?”. Silent Warfare: Understanding the World of Intelligence. 2. bs. New York: Brassey’s US, 1993, 1- 9.

Shulsky, Abram. Gary J. Schmitt. “Types and Examples of Covert Action”. *Silent Warfare: Understanding the World of Intelligence.* 2. bs. New York: Brassey’s US, 1993, 77- 90.

Shultz, Richard H., Roy Godson. “Overt Propaganda and Cover Political Techniques: Distinctions and Definitions”. *Dezinformatsia: Active Measures in Soviet Strategy*. Virginia: Pergamon Brassey’s International Defense Publishers, 1984.

Sivarajah, Uthayasankar, Muhammad Mustafa Kamal, Zahir Irani, Vishanth Weerakkody. "Critical analysis of Big Data Challenges and Analytical Methods". *Journal of Business Research*. (2016): 1- 24. http://dx.doi.org/10.1016/j.jbusres.2016.08.001.

SoftServe. "Dr Alex Tayler: The Power of Big Data and Psychographics". 8 Şubat 2018. https://www.youtube.com/watch?v=mHSsGKU35GY. [Erişim Tarihi: 13.12.2022].

Sorour, Karim, Bidit Lal Dey. "Energising the Political Movements in Developing Countries: The Role of Social Media". *Capital & Class*. (2014): 1- 8.

Special Counsel Robert S. Mueller, III. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election". *U.S. Department of Justice*. (2019).

Şafak, Erdi. "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar". Selçuk Üniversitesi Hukuk Fakültesi Dergisi. (11.02.2020): 127- 160. 155. 10.15337/suhfd.640029.

Techopedia. "What Does Zero Day Mean". https://www.techopedia.com/definition/29736/zero-day. [Erişim Tarihi: 10.11.2022].

The Britannica Dictionary. "Algorithm Definition & Meaning". https://www.britannica.com/dictionary/algorithm. [Erişim Tarihi: 17.02.2023].

The Law Dictionary. "Plausible Deniability Definition, Examples and Laws". *Criminal Law*. https://thelawdictionary.org/article/plausible-deniability/. [Erişim Tarihi: 10.12.2022].

The Moscow Times. "Ukraine Accuses Russia's LUKoil of Financing Terror in War Torn East". 16 Ocak 2015. https://www.themoscowtimes.com/2015/01/16/sp-delays-decision-on-whether-to-downgrade-russia-to-junk-a42956. [Erişim Tarihi: 10.12.2022].

The National Archives. "Newly released GCHQ files: UKUSA Agreement" Haziran 2010, https://www.nationalarchives.gov.uk/ukusa/ [Erişim Tarihi: 03.10.2022].

The Office of the Privacy Commissioner for Personal Data (PCPD). "Personal Information Protection Law of the Mainland". Hong Kong. https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html. [Erişim Tarihi: 28.11.2022].

The United States District Court for The District of Columbia. "Internet Research Agency Indictment". Washington, DC: U.S. Department of Justice, 2018, 1-37. https://www.justice.gov/file/1035477/download. [Erişim Tarihi: 10. 11. 2022].

The White House. “İnternational Strategy for Cyberspace”. Mayıs 2011. Washington.

The White House. Executive Order 12333: United States Intelligence Activities”. 40 Fed. Reg. 59,941 (04.12. 1981). değişiklik: Executive Order 13284. 68 Fed. Reg. 4,077 (23.01. 2003), ve Executive Order 13355. değişiklik: Executive Order 13470. 73 Fed. Reg. 45,328 (2008). https://irp.fas.org/offdocs/eo/eo-12333-2008.pdf. [Erişim Tarihi: 15.11.2022].

Timberg, Craig. “Russian Propaganda May Have Been Shared Hundreds of Millions of Times. New Research Says”. *The Washington Post*. 5 Ekim 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/10/05/russian-propaganda-may-have-been-shared-hundreds-of-millions-of-times-new-research-says/. [Erişim Tarihi: 10.12.2022].

Townsend, Troy, Melissa Ludwick, Jay McAllister, Andrew O. Mellinger, Kate Ambrose Sereno. “SEI Innovation Center Report: Cyber Intelligence Tradecraft Project Summary of Key Findings”. *Cyber Intelligence Tradecraft Project (CITP)*. (2013).

Tsymbal, V. I. "Kontseptsiya `Informatsionnoy Voyny'" (Concept of Information Warfare). speech given at the Russian-US conference on "Evolving Post-Cold War National Security Issues," Moscow 12-14 September 1995, p. 7’den aktaran, Thomas Timothy L. “Deterring Information Warfare: A New Strategic Challenge”. *The US Army War College Quarterly: Parameters*. C. 4. S. 26 (1996).

Tüminçin, Fatma, Alper Aytekin, Ahmet Ayaz. “İnsan Beyni Modellemesi ve Yapay Sinir Ağları”. *SADAB 5th International Social Research and Behavioral Sciences Symposium*. Tiflis: 11- 12 Ekim 2019, 163- 171.

Tzu, Sun. *Savaş Sanatı*. çev. Tuğçe Ayteş. İstanbul: İlgi Kültür Sanat Yayıncılık, 2017.

United States Of America Before The Federal Trade Commission. “Cambridge Analytica, LLC, a Corporation”. 182 3107. 9383.

Vaidya, Omkarprasad S., Sushil Kumar. “Analytic Hierarchy Process: An Overview of Applications”. *European Journal of Operational Research*. C. 169. S. 1 (2006): 1- 29. doi:10.1016/j.ejor.2004.04.028 .

Venables, Adrian. “Modelling Cyberspace to Determine Cybersecurity Training Requirements”. *Frontiers in Education*. C. 6. S. 768037 (2021): 1- 16. doi: 10.3389/feduc.2021.768037.

Viotti, Paul R., Mark V. Kauppi. “Uluslararası İlişkiler ve Dünya Siyaseti”. *Uluslararası İlişkiler ve Dünya Siyaseti*. 5. bs. çev. Ayşe Özbay Erozan. Ankara: Nobel Yayınevi, 2017.

Wamba, Samuel Fosso, Shahriar Akter, Hyunjin Kang, Mithu Bhattacharya, Mohammed Upal. “The Primer of Social Media Analytics”. *Journal of*

Organizational and End User Computing. C. 28. S. 2 (2016): 1- 12. DOI: 10.4018/JOEUC.2016040101.

Warner, Michael. "A Matter of Trust: Covert Action Reconsidered". *Studies in Intelligence*. C. 63. S. 4 (2019): 33- 41.

_____."Sources and Methods for the Study of Intelligence". *Handbook of Intelligence Studies*. ed. Loch. K. Johnson. Oxon: Routledge, 2007, 17- 27.

We Are Social. "Digital 2022: Another Year Of Bumper Growth". 26 Ocak 2022. https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/ [Erişim Tarihi: 24.10.2022].

Wells, William D. "Psychographics: A Critical Review". *Journal of Marketing Research*. C. 12. S. 2 (1975): 196- 213. DOI:10.1177/002224377501200210.

Whipple, Chris. The Spy Masters: How the CIA Directors Shape History and the Future. New York: Scribner, 2020.

Wilkenfeld, Jonathan, Gerald W. Hopple, Paul J. Rossa, Stephen J. Andriole. *Foreign Policy Behaviour: The Interstate Behaviour Analysis Model*. Beverly Hills: Sage Publications, 1980, 22 (Aktaran: Tayfur, M. Fatih. "Main Approaches to the Study of Foreign Policy: A Review". *METU Studies in Development*. C. 21. S. 1 (1994): 113- 141.

Wuraola, Ayisat, Yusuf-Asaju, Zulkhairi Md Dahalin, Azman Ta'a. "Framework for Modelling Mobile Network Quality of Experience Through Big Data Analytics Approach". *Journal of Information and Communication Technology (JICT)*. C. 17. S. 1. (2018): 79- 113.

Wylie, Christopher. *Mindf*ck: Cambridge Analytica and the Plot to Break America*. New York: Random House, 2019. e-book ISBN: 9781984854643.

Youyou, Wu, Michal Kosinski, David Stillwell. "*Computer-based Personality Judgments are More Accurate Than Those Made by Humans". Proceedings of the National Academy of Sciences.* C. 112. S. 4 (2015): 1036–1040. doi:10.1073/pnas.1418680112.

Zeng, Daniel, Hsinchun Chen, Robert Lusch, Shu-Hsing Li. "Social Media Analytics and Intelligence". *IEEE Intelligent Systems*. C. 25. S.6 (2010): 13- 16. DOI:10.1109/MIS.2010.151.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: KARA, Tuğçe Sena
Uyruğu	: TC.

Eğitim

Derece	**Üniversite ve Bölüm**	**Mezuniyet tarihi**
Lisans	Okan Üniversitesi	
	Uluslararası İlişkiler (İngilizce)	Temmuz 2016

Yabancı Dil:

İngilizce