



<https://dergipark.org.tr/pub/saga>

Sosyal Medya İstihbaratının Makine Öğrenmesi Çerçevesinde İncelenmesi: Terörizm Çalışmaları

Examining Social Media Intelligence within The Framework of Machine Learning: Studies of Terrorism

Sevil Başarır YURTSEVER^{1*}

¹Millî Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü, İstihbarat Çalışmaları Programı, 06654 Çankaya/ANKARA

Makale Bilgisi

Araştırma makalesi
Başvuru: 25.01.2024
Düzeltilme: 01.03.2024
Kabul: 21.03.2024

Keywords

Social Media Intelligence
Machine Learning
Defence Sciences
National Security
Terrorism

Anahtar Kelimeler

Sosyal Medya İstihbaratı
Makine Öğrenmesi
Savunma Bilimleri
Millî Güvenlik
Terörizm

Özet

Sosyal medya günümüz dünyasında birçok kişi tarafından kullanılan ve her gün devasa veri üreten bir platformdur. Bu platformdan elde edilen verileri işleyerek daha anlamlı sonuçlar çıkarmak ise oldukça önemli bir hale gelmektedir. Gelişen teknolojilerle beraber terör örgütleri de bu değişimi takip ederek taktiklerini geliştirmektedir. Artık terör örgütleri sosyal medyadan örgüt propagandası yapmak, örgüt ideolojisini yayarak eleman temin etmek, örgüt eylemlerine mali destek sağlamak gibi çeşitli nedenlerle sosyal medyayı kullanmaktadır. Bu sosyal medya platformlarından elde edilen sosyal medya istihbaratı ise kolluk kuvvetleri için oldukça önem teşkil etmektedir. Ancak geleneksel yöntemler artan verilerin analizi için yeterli olmamaktadır. Bu makalede terörizm konularında sosyal medya istihbaratı çalışmalarının makine öğrenmesi metotları kullanarak daha hızlı, daha ucuz ve daha efektif olarak yapılabileceğini ortaya koymak hedeflenmektedir. Bunu yaparken de hem makine öğrenmesi metotları hem bu metotlarla yapılan çalışmalar hem de sosyal medyadan ne tür analizler yapılabileceği karşılaştırmalı olarak sunulmuştur. Makale sonucunda ise Türkçe literatürde terörizm konularında yapılan sosyal medya istihbaratı çalışmalarında makine öğrenmesi tekniklerinin kullanılmadığı, çalışmalarda yapılan işlemlerin ya manuel ya da yazılım programları aracılığıyla yapıldığına ancak artan veri yoğunluğunun makine öğrenmesi ve yazılım dili kullanmanın daha kapsamlı ve daha anlamlı sonuçlar için çok önemli olduğu sonucuna ulaşılmıştır.

Abstract

Social media is a platform used by many people in today's world and produces huge data every day. It becomes very important to obtain more meaningful results by processing the data obtained from this platform. With developing technologies, terrorist organizations also follow this change and improve their tactics. Nowadays, terrorist organizations use social media for various reasons such as making propaganda for the organization through social media, recruiting personnel by spreading the organization's ideology, and providing financial support for the organization's actions. Social media intelligence obtained from these social media platforms is very important for law enforcement forces. However, traditional methods are not sufficient for the analysis of increasing data. This article aims to demonstrate that social media intelligence studies on terrorism issues can be carried out faster, cheaper and more effectively by using machine learning methods. While doing this, both machine learning methods, studies carried out with these methods, and what kind of analyzes can be done from social media are presented comparatively. As a result of the article, it was concluded that machine learning techniques were not used in social media intelligence studies on terrorism issues in the Turkish literature, the operations carried out in the studies were carried out either manually or through software programs, but the increasing data density, machine learning and using software language were very important for more comprehensive and more meaningful results.

* Sevil Başarır YURTSEVER, basarirsevil@gmail.com

1. GİRİŐ

Günümüz dünyasında geliŐen ve deęiŐen teknoloji ile insanların hayatlarını önemli ölçüde etkileyen deęiŐiklerde beraberinde gelmiŐtir. Eskiden insanlar bir araŐtırma yapmak, bir haber okumak, iŐ aramak, sosyalleŐmek, spor yapmak gibi birŐok Őey için çeŐitli aramalar yapıp ilgili olduęu konu hakkında bilgi ediniyordu. Ancak artık istedikleri Őeylerin çoęuna çeŐitli sosyal medya araŐları ile ulaŐabiliyorlar. İnsanlar haber okumak, gündemi takip etmek, yorumlarda bulunmak gibi sebeplerle Twitter, iŐ bulmak ve güncel sektör geliŐmelerini takip etmek için LinkedIn, çeŐitli hobilerle ilgili takip etmek ya da paylaŐımda bulunmak için Instagram gibi farklı platformlar kullanarak yaŐamlarının çok büyük bir bölümünü buralarda geçirmeye baŐladılar. Artık bir kiŐi hakkında istihbarat toplamak için bu açık kaynaklar arasında verisi en çok olan sosyal medya ve buradan elde edilen bilgilerin deęerlendirilerek oluŐturulan sosyal medya istihbaratı oldukça popüler bir konu haline geldi. Ancak bu kadar verinin oluŐturduęu büyük veri yığınları arasında analiz yapmak ise eskisine oranla oldukça zorlaŐmaktadır. Bu analizlerin gerŐekleŐtirilmesi için yapay zekanın aktif kullanımı gerekmektedir. Yapay zekanın alt alanı olan makine öęrenmesi metotlarının kullanılarak yapılan analizler neticesinde ise analizlerden daha anlamlı sonuçlar çıkarmak mümkün olmaktadır.

Açık kaynak istihbaratı; herkesin erişebildięi, talep edebildięi, satın alabildięi ya da gözlemleyebildięi yasal yollardan elde edilebilen ve kamuya açık verilerden elde edilebilen istihbarat olarak ifade edilmektedir (Antonius & Rich, 2013, s. 45). Dolayısıyla medya içerikleri, kamuya açık rapor, belge, bilimsel araŐtırma makalesi, internetten elde edilen bilgiler, sosyal medya verileri bu kapsamda deęerlendirilebilmektedir (Lowenthal, 2004, s. 1). Sosyal medya, kamuda gerŐekleŐtirilen hizmetlerin daha iyi yapılmasını isteyen hükümet yetkilileri, interneti kötüye kullanıp manipölasyonlarla yanlış yönlendirmeler yapan suçluları tespit etmeye çalışan kolluk kuvvetleri ve güvenlik, terörizm konularında bilgi toplayan istihbarat servisleri için çok büyük veri kaynaęı olmaktadır (Omand & Miller, 2017, s. 359). Sosyal medya istihbaratı ise sosyal medyada üretilen, ortaya çıkan verilerin toplanması, analizi ve kullanımı (Bartlett & Reynolds, 2015, s. 27) ya da baŐka bir ifadeyle sosyal medyadan elde edilen istihbarata (Omand & Miller, 2012a, s. 802) denilmektedir.

Sosyal medya istihbaratı elde etme konusunda en efektif metotlardan biri ise makine öęrenmesidir. Makine öęrenmesi algoritmaları kullanılarak daha büyük hacimli veride daha hızlı çalışmalar yapılabilir. En temel düzeyde Makine Öęrenimi, bilgisayarların kendi baŐlarına düşünmesini ve öęrenmesini saęlayan bir yapay zeka kategorisidir. Bu tamamen bilgisayarların eylemlerini daha fazla doęruluk elde edecek Őekilde iyileŐtirmek amacıyla eylemlerini deęiŐtirmelerini saęlamakla ilgilidir; burada doęruluk, seçilen eylemlerin kaç kez doęru eylemlerle sonuçlandıęıyla ölçülmektedir (Alzubi, Nayyar, & Kumar, 2018, s. 1). Makine öęrenimi, makinelere verileri nasıl daha verimli Őekilde kullanacaklarını öęretmek için kullanılmaktadır. Mevcut veri kümelerinin bolluęu nedeniyle makine öęrenimine olan talep gün geçtikçe artmaktadır. BirŐok endüstriler ilgili verilerden anlamlı sonuçlar

çıkarmak için makine öğrenimini tekniklerini kullanmaktadır (Mahesh, Machine Learning Algorithms- A Review, 2018, s. 381).

Makine öğrenmesi metotlarının terörizm konulu çalışmalarda çok az kullanıldığı görülmektedir. Ancak sosyal medya istihbaratı elde etme amacıyla makine öğrenmesi metotları kullanarak terörizm çalışmaları çok faydalı sonuçlar üretebilmektedir. Terörizm; siyasal amaçlara ulaşmak için kullanılan şiddet veya şiddet kullanma şekli olarak tanımlanmaktadır (Hoffman, 2006, s. 2-3). Daha geniş bir ifadeyle terörizm; korku üreten siyasal şiddet, taktik ya da planlı bir etkinliğin özel biçimini ifade eden bir doktrini, aynı zamanda ahlaki ve yasal sınırları olmayan, organize edilmiş, gösteri amaçlı, daha çok sivilleri hedef alan, propaganda ve psikolojik etkiler için gerçekleştirilen şiddet eylemleri şeklinde kavramsal bir ifade ile de anlatılmaktadır (Schmid, 2011, s. 86).

Bu çalışmanın amacı istihbarat analizlerinin yapay zeka ile yapılmasının olumlu etkilerini ortaya koymaktır. Fakat yapay zeka kavramı içine birçok konuyu dâhil etmesi nedeniyle özellikle makine öğrenmesi metotları ile istihbarat kavramının da kendi içerisinde birçok alt disiplini olması sebebiyle bu konu da açık kaynak istihbaratı özelinde daha güncel ve yeni bir konu olan sosyal medya istihbaratı olarak sınırlandırılmıştır. Bu çerçevede neticesinde hipotezimiz, sosyal medya istihbaratından terörizmle mücadele noktasında faydalı bilgiler sağlayabileceği, sosyal medya istihbaratının makine öğrenmesi metotları ile yapıldığında daha efektif, daha hızlı ve daha fonksiyonel sonuçlar vereceğidir.

Bu kapsamda çalışmada öncelikle kavramsal ve teorik çerçeve tartışılacak olup kavramsal çerçeve de terör ve istihbarat ile ilgili kavramlar, teorik çerçeve de ise yapay zeka, makine öğrenmesi ve makine öğrenmesi çevresinde öğrenme metotları açıklanacaktır.

Bir sonraki bölümde hem sosyal medya istihbaratı kapsamında hem de makine öğrenmesi kapsamında çalışma alanları, yapılabilecek uygulamalar ve bu çalışmalar esnasında öğrenme metotlarına göre kullanılacak makine öğrenmesi metotları ifade edilecektir. Ayrıca bu makine öğrenmesi metotlarının terörle mücadele konusunda ne tür çalışmalarda kullanabileceği de açıklanacaktır.

Sosyal medya istihbaratı uygulama alanlarının ve makine öğrenmesi kullanarak yapılabilecek sosyal medya istihbaratı uygulamalarının anlatıldığı diğer bir bölümde literatürde yapılmış çalışmalarının içeriklerinin analiz edilerek çalışmaların amaçlarına, kullanılan yöntemlere, sonuçlarına yer verilerek açıklamalar yapılmıştır. Özellikle yapılan çalışmalarda terörizmi konu olan ve terör, sosyal medya ve suç veri tabanlarının kullanıldığı çalışmalar seçilmiştir.

Son bölümde yapılan incelemeler neticesinde sosyal medya istihbaratı ve makine öğrenmesi beraber ele alındığında terörizm konularında nasıl çalışmalar yapılabileceği, hangi metotların kullanılmasının daha uygun olabileceği, daha efektif çözümler için nasıl teknolojilerden faydalanılabileceği konusunda çıkarımlar ortaya konulacaktır.

Sonu bölümünde ise tüm alıřmanın özet bir deęerlendirilmesi yapılarak alıřmanın ıktılarına, yola ıktığımız hipotezin tüm alıřmalar sonucunda deęerlendirilmesine, yazılan makalenin literatüre katkılarına ve gelecek alıřmalar için önerilere deęinilecektir.

2. YÖNTEM

Bu makalede sosyal medya istihbaratı makine öęrenmesi çerevesinde incelemek olup özellikle terörizm alıřmalarına nasıl katkı vereceęi tartışılacaktır. Öncelikle kuramsal ve teorik çereve ortaya konacaktır. Sonrasında sosyal medya istihbaratı kapsamında ve makine öęrenmesi kapsamında yapılabilecek alıřmalar ve makine öęrenmesi metotları incelenecektir. Akabinde hem sosyal medya istihbaratı hem de makine öęrenmesi üzerine yapılmıř alıřmalar içerik analizi yöntemi ile incelenecek olup bu alıřmalarla neler yapılabildięine, terörizm konularında hangi alıřmaların yer aldığına, en popüler makine öęrenmesi türlerine ve popüler algoritmalarına yer verilecektir. Bu alıřma kapsamında hem yabancı literatürdeki hem de Türke literatürdeki alıřmalara yer almaktadır. Analiz boyunca da nitel arařtırma yöntemlerinden faydalanılacaktır.

Makalede ele alınan arařtırma deseni makine öęrenmesi kullanarak terörizm konularında daha aktif, daha büyük hacimli ve daha hızlı sosyal medya istihbaratı üretilebileceęi çerevesinde kurgulanmıřtır. Bu noktada incelenen arařtırma sorusu ise makine öęrenmesinin terörizm konularında nasıl sosyal medya istihbaratı üretilebileceęidir. Yapılan alıřmanın sonucunda ise sosyal medya istihbaratının hangi alanlarda ve konularda kullanılabileceęini, bu alıřmaların terörizm alıřmalarıyla nasıl baędařtırılacağı ve makine öęrenmesinin bu alıřmalara vereceęi yeni bakıř açısı ve faydaları tümevarım yöntemi ile birleřtirilerek açıklanacaktır.

3. KAVRAMSAL VE TEORİK ÇEREVE

Bu bölümde makalenin kavramsal ve teorik çerevesi ele alınarak açıklanacaktır. Kavramsal çerevede terör ve istihbarat ile ilgili terimlerden bahsedilecek olup teorik çerevede ise makaledeki incelemelerle ilgili üzerinde durulan yapay zeka ve makine öęrenmesi konularına açıklık getirilecektir.

3.1 Kavramsal Çereve

Makalenin kavramsal çerevesi açıklanırken öncelikle terör, terörizm, terörle mücadele kavramları sonrasında ise istihbarat, açık kaynak istihbaratı ve açık kaynak istihbaratı alıřmaları ve sosyal medyanın yaygınlařması ile hayatımıza girmiř ve önem kazanmıř olan sosyal medya istihbaratından bahsedilecektir.

3.1.1 Terör, Terörizm ve Terörle Mücadele

Terör kelimesi Latince “korkudan titreme” veya “titremeye sebep olma” olarak ifade edilmektedir (Wilkinson, 1974, s. 9). Terör ifadesi Fransız Devrimi’nden sonra kullanılmaya bařlanmıř olup Mart 1973 ile Temmuz 1974 arasındaki döneme “Terör Dönemi” veya “Terör Rejimi” olarak adlandırılmıřtır

(Laqueur, 1977, s. 7). Literatürdeki birçok alıřmada ise terör kelimesi řiddet, siyasal řiddet ya da anarři kelimeleriyle eř anlama gelecek řekilde kullanılmıřtır (Yayla, 1990, s. 335). Bařka bir tanıma göre ise; hedefe yönelik korku yaratmak üzere birtakım bireyler ya da gruplar tarafından gerekleřtirilen řiddet ierikli eylemler olarak tanımlanmıřtır (Saral, 2016, s. 25).

Terörizm bir siyaset yapma ve bu siyasetin ise en radikal biçimi olarak düşünölmektedir. Aynı zamanda terörizm, daha az gü sahiplerinin daha gü sahibi olan yapıya karřı gerekleřtirdiđi gayri-muntazam bir savař biçimi olarak da tanımlanmaktadır (Ergil, 1992, s. 139). Birok kaynađın taranması ile yapılan bařka bir alıřmada ise terörizm, korku yaratmak iin gerekleřtirilen siyasal řiddet, taktik veya etkinin özel biçimini ifade eden doktrini, diđer yandan ise yasadıřı, ahlaki olmayan, planlanmış, gösteri amaçlı, çođunlukla sivilleri hedef alan, propaganda ve psikolojik etkiler iin gerekleřtirilen, dođrudan řiddet eylemleri olarak tanımlanmaktadır (Schmid, 2011, s. 86-113). Uluslararası bir olgu olan terörizm kavramı 11 Eylül 2001 ABD'ye yapılan terör saldırılarından dünya apında daha ok tartıřılmıř ve toplumun gündemini daha sık meřgul etmeye bařlamıřtır (řimřek, 2016, s. 320).

Terörle Mücadele yalnızca silah ile gerekleřtirilen dar perspektifli bir bakıř aısıyla deđil terörü önemli ve sosyal bir sorun olarak görerek mevcut bu soruna yönelik daha akılcı, pratik ve etkili özüm önerileri geliřtirmeye alıřan geniř perspektifli bir mücadele olarak algılanmalıdır (Akbulut & Beren, 2012, s. 259). Bu sebeplerden dolayı terörle mücadele yöntemlerinin hem uygulanmasında hem de terörle mücadelenin bařarıya ulařmasında hükümet ve kurumların ortak bakıř aısı geliřtirerek el ele bir mücadele iinde bulunması önem tařımaktadır (Saran & Bitirim, 2010, s. 95).

3.1.2 İstihbarat

İstihbarat, istihbar kökünden üretilmiř, yeni elde edilen bilgi veya haber alma (Ata, 2019, s. 1) olarak tanımlanmaktadır. İstihbarat 1949 yılında Kent tarafından (Kent, 1949, s. 1,51,136) bilgi, organizasyon ve faaliyet olarak tanımlanmaktadır. Bařka bir tanıma göre istihbarat, devletlerin kendilerine yönelik tehditlerinden önceden haberdar olması, bu tehditlerin ortadan kaldırılması ve muhtemel sürprizlerden korunulması maksadıyla, gerekli verilerin uygun kaynaklardan en uygun yöntemle toplanması, analiz edilmesi, ihtiya sahibi kurumlara ve karar alıcılara ulařtırılması, ulařtırılan kurumlardan alınan geri besleme ile kendisine yön veren, döngüsel bir süreci ifade eden gizli bir faaliyet (Bural, 2021, s. 51) řeklinde tanımlanmıřtır.

İstihbarat toplama disiplini, insan istihbaratı (HUMINT), açık kaynak istihbaratı (OSINT), sinyal istihbaratı (SIGINT), ölçüm ve imza istihbaratı (MASINT) ve cođrafı konum istihbaratı (GEOINT) (Stottlemyre, 2015, s. 584) olmak üzere beř ana yöntemle açıklanmaktadır. Bu makalede istihbarat toplama disiplinleri özelinde Açık Kaynak İstihbaratı kapsamında incelemeler yapılacaktır.

3.1.3 Açık Kaynak İstihbaratı

Açık kaynak bilgisi herkesin yasal sınırlar çerevesinde talep ederek, satın alarak veya gözlemleyerek elde edebileceđi kamuya açık olan bilgileri ifade ederken, açık kaynak istihbaratı ise bu bilgilerin

istihbarat ihtiyaları kapsamında toplanması, analiz edilmesi, iřlenmesi ve kullanılması ile zamanında uygun bir hedef kitleye dađıtılan kamuya aık bilgileri ifade etmektedir (Benes, 2013, s. 23). Aık kaynak istihbaratı retilen organlardan bazıları olarak medya yayınları, gazeteler, dergiler, kitaplar, halka aık olarak yayınlanan raporlar, sempozyum ve konferans bildirileri, haritalar, aık veri tabanları, internet siteleri, bloglar, forumlar, canlı yayınlar ve sosyal medya (Clark, 2007, s. 27-28), (Hribar, Iztok, & Teodora, 2014, s. 531), (Gruters & Gruters, 2018, s. 98-99) olarak ifade edilmektedir. Bu platformlardan ham veri toplanırken iřlenmiř ve dođrudan istihbarat olarak kullanılabilir bilgilere de ulařmak mmkn olabilmektedir (Stottlemyre, 2015, s. 584-585). Bu makale kapsamında Aık Kaynak İstihbaratı elde etmek amacıyla zellikle sosyal medya zerine alıřmalar yapılarak elde edilen sosyal medya istihbaratı konusu zerinde durulacaktır.

3.1.4 Sosyal Medya İstihbaratı

Sosyal medya insanların, grupların veya toplulukların birbirleri, yařamları veya iřleri hakkında resimler, videolar, yazılar, sesler veya bunların karıřımını kullanarak bilgiler paylařtıkları veya tartıřtıkları eřitli internet siteleri, uygulama ya da platformlardır (McIntyre, 2014, s. 7). Bu platformlarda insanlar fikirlerini, kendi ieriklerini ve dřncelerini evrimii olarak paylařabilmektedir (Scott, 2010, s. 38). Sosyal medya, kullanıcıların paylařılan ierikleri katkı sunması sebebiyle katılım; paylařılan ieriklerin genellikle diđer kullanıcılar tarafından grntlenebilmesi sebebiyle aıklık; kullanıcıların birbiri ile interaktif iliřki kurabilmeleri sebebiyle iletiřim; iletiřim ađlarından eřitli gruplařmalar ortaya ıkabilmesi sebebiyle topluluk; kullanıcıların birbiri ile bađ kurabilmesi sebebiyle bađlantılılık (Bural, 2021, s. 81-82) olarak beř ana zellikten oluřmaktadır.

Sosyal medya istihbaratı, temelde sosyal medyadan elde edilen verilerin toplanması, iřlenmesi, analiz edilmesi ile retilen istihbarata denilmektedir. Bařka bir tanıma gre ise ulusal gvenliđi etkileyecek davranıřlarda bulunan insanların durumlarının analiz edilmesi, anlamlandırılması maksadıyla sosyal medya verilerine veri madenciliđi teknikleri uygulanarak elde edilen istihbarata (řuřnea & Iftene, 2018, s. 231-239) sosyal medya istihbaratı denilmektedir. Sosyal medyadan elde edilecek veriler beř ayrı kategoride toplanabilmektedir (Hassan & Hijazi, 2018, s. 206-207). Bu kategorilerden birincisi paylařımlardır. İkinici sosyal medya zerinden yapılan paylařımlara verilen cevaplardır. cnc kategori kullanıcıların grsel, video, ses gibi farklı alanda paylařım yapabildikleri oklu ortamlardır. Drdnc alan ise bu paylařımlara ait st veri olarak adlandırılan paylařımların yapıldıđı zaman, konum, cihaz bilgileri veya paylařımın yapıldıđı profil bilgileridir. Son alan ise kullanıcıların birbirleriyle iletiřimleri esnasında ortaya ıkan etkileřim verileridir. Bu verileri de kullanıcıların takip ettikleri arkadaşlardan veya sosyal ađından elde edilebilmektedir.

3.2 Teorik ereve

Makalenin teorik erevesi kapsamında ncelikli olarak yapay zekadan bahsedilecektir. Daha sonrasında alt alanı olan makine đrenmesi konusuna geiř yapılacak ve makine đrenmesi trlerine yer

verilecek ve bu kapsamda denetimli/gözetimli öğrenme, denetimsiz/gözetimsiz öğrenme, yarı denetimli/gözetimli öğrenme ve pekiřtirmeli/takviyeli öğrenme metotlarından bahsedilecektir.

3.2.1 Yapay Zeka

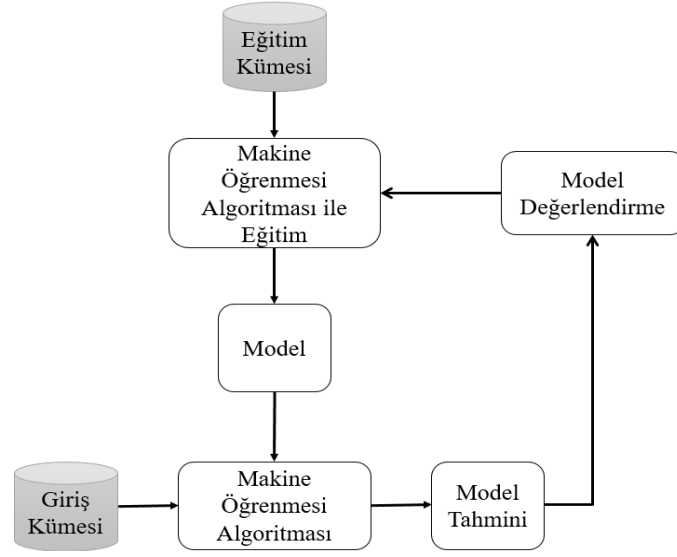
İnsanlar varoluřları geređi merak eden, arařtıran ve sürekli öğrenen varlıklardır. Bununla beraber insan zihninin nasıl çalıştığı, öğrenmenin nasıl gerçekleştiđi, insan dıřı varlıkların zekâsının olup olmadığı veya insan dıřı varlıklarda da öğrenmenin mümkün olup olmayacağı gibi sorular her zaman merak edilmiřtir. İnsan dıřı varlıklarında akıllı davranıřları sergileyebilmesini insan beynini model olarak çeřitli algoritmalar ile öğretilmesini hedefleyen sistem yapay zeka olarak tanımlanmaktadır (Nabiyev, 2012, s. 25). Bir grup bilim insanı yapay zeka ile her řeyi yapmanın mümkün olduđunu savunurken (Yılmaz, 2017, s. 4-7) diđer taraftan bazı bilim insanları sevgi, saygı, hořgörü, ahlaki seçimler gibi karmařık konuların yapay zeka sistemleri tarafından yapılamayacağını savunmaktadır. Ama önemli olan insanlar ile makinelerin uyumlu (Oruç, 2022, s. 4228) bir şekilde çalışarak problemlere hızlı, faydalı çözümler geliřtirilmesine katkı sađlanmalıdır. Diđer tanımlardan da yola çıkarak yapay zeka, insanların zekasını, sinir sistemini ve nörolojik yapısının modellenerek yazılıma aktarılması iřlemi olarak tanımlanmaktadır. Daha da açık bir ifadeyle insan gibi davranan, insan gibi düşünen, akılcı düşünen ve davranan bilgisayar sistemleri olarak tanımlanmakta (Balaban & Kartal, 2015, s. 16) olup makine öğrenmesi ise bu anlamda yapay zekanın son evresi (Atalay & Çelik, 2017, s. 159) olarak görölmektedir.

3.2.2 Makine Öğrenmesi

Veri hacimlerin gün geçtikçe artması sebebiyle veri analizlerinin ve veriden anlamlı sonuçlar çıkarmak için kullanılan yöntemlerin manuel gerçekleştirilebilmesi git gide zorlaşmaktadır. Bu nedenle de makine öğrenimine talep gün geçtikçe artmaktadır. Problemler karşısında yazılımlar ile büyük hacimli verilerin daha hızlı ve efektif olarak çözüm bulunabilmektedir. Arthur Samuel'e göre makine öğrenimi makineler veriye nasıl daha verimli şekilde kullanacağını öğretmek için kullanılmaktadır (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 381). Bařka bir deyiřle makine öğrenimi sistemlere öğrenme ve geliřtirme yeteneđi sađlamaktadır (Sarker, 2021, s. 1). Makine öğrenmesinde modeli eđitmek için çeřitli algoritmalar kullanılmaktadır. Ancak hangi algoritmaların kullanılabileceđi problemin amacına göre deđiřmektedir. Arařtırma problemine uygun çözümler kullanıldıđında modelin başarısı da dođru orantılı olarak artmaktadır. Makine öğrenmesinde öğrenme stratejileri problemin konusuna göre dört farklı şekilde (Sarker, 2021, s. 3) uygulanabilmektedir: Denetimli/Gözetimli Öğrenme, Denetimsiz/Gözetimsiz Öğrenme, Yarı Denetimli/Yarı Gözetimli Öğrenme, Takviyeli/Pekiřtirmeli Öğrenme.

Temel olarak makine öğrenme süreci ise verinin belirlenmesi verinin belli kısmının bu bazı kaynaklara göre %80 bazı kaynaklara göre %70 olarak kabul edilir eđitim için kullanılması, daha sonrasında da makine öğrenmesi algoritmalarını kullanarak modelin oluřturulması ve verinin kalan %20 veya %30'luk

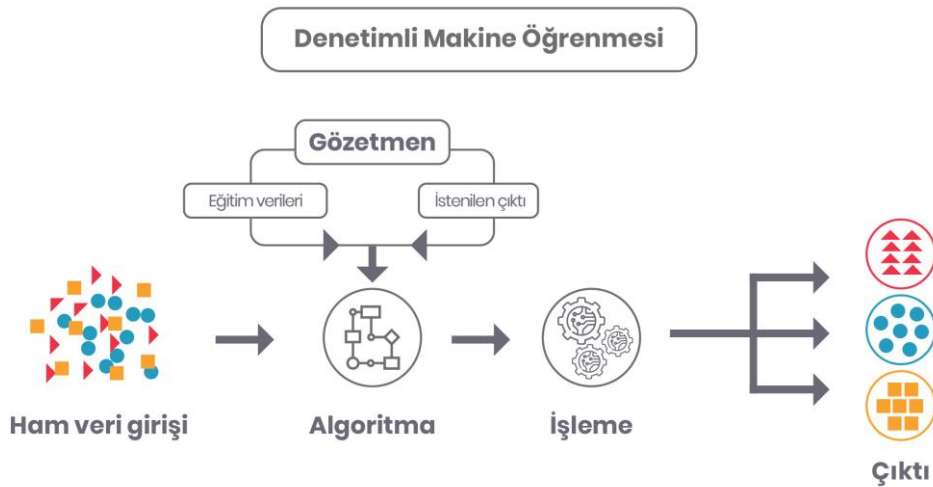
kısmıyla modelin test edilmesi sürecine dayanmakta olup grafiksel olarak Şekil 1 de gösterildiği şekilde gerçekleşmektedir.



Şekil 1: Makine Öğrenmesi ile Model Geliştirme Süreçleri
(Gültepe, 2019, s. 13)

3.2.3 Denetimli/Gözetimli Öğrenme

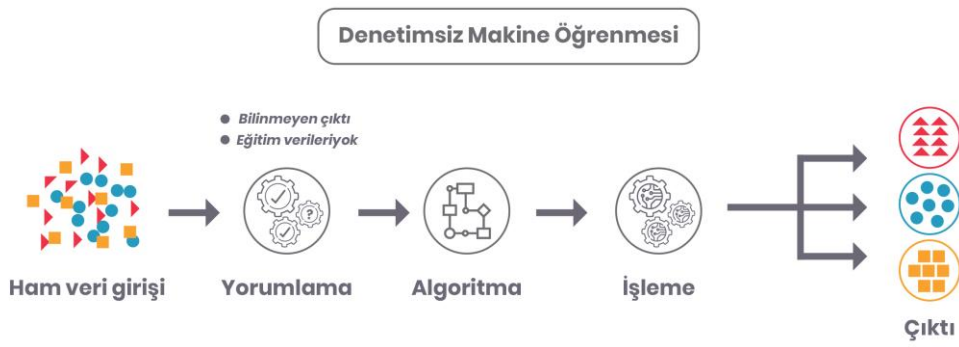
Denetimli (Gözetimli) öğrenmede sisteme örnek girdiler verilmekte ve çıktıyla eşlenmektedir. Bu tür öğrenmede her örnek bir giriş nesnesi ve istenen bir çıkış değerinden oluşan çiftler şeklinde oluşmaktadır (Somvanshi, Chavan, Tambade, & Shinde, 2016, s. 2). Bir dizi eğitim örneğinden oluşan etiketli eğitim verilerden bir fonksiyon çıkarmayı hedeflemektedir. Denetimli makine öğrenimi algoritmaları dışardan yardıma ihtiyaç duymaktadır (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 381). Bu öğrenme metodu belli bir dizi eğitim çifti verisi ile belli hedefler üzerinde gerçekleştirilmektedir. Ayrıca denetimli öğrenmenin genel iş diyagramı Şekil 2 de görülmektedir.



Şekil 2: Denetimli/Gözetimli Öğrenme İş Akış Diyagramı
(Makine Öğrenmesi (Machine Learning) Nedir?, 2021)

3.2.4 Denetimsiz/Gözetimsiz Öğrenme

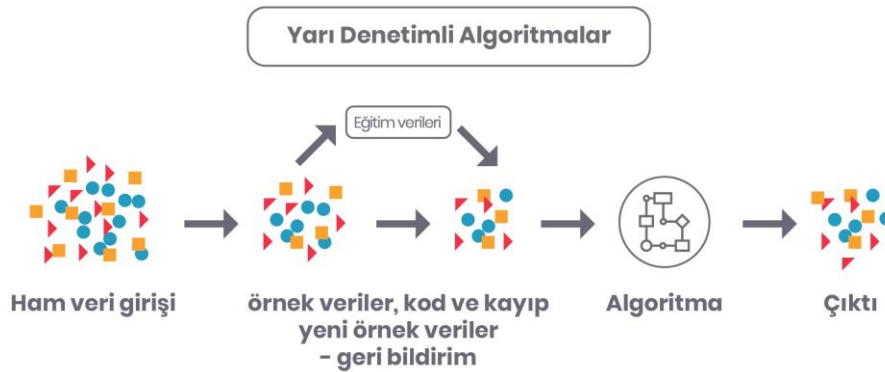
Denetimsiz (Gözetimsiz) öğrenmede sisteme örnek çıktıları sağlanmakla birlikte herhangi bir çıktı verisi yer almamaktadır. Burada beklenen etiketli çıktı kümesi olmadan algoritmanın doğru ayrımı yaparak sınıflandırmayı yapabilmesi olarak ifade edilmektedir (Somvanshi, Chavan, Tambade, & Shinde, 2016, s. 2). Denetimsiz öğrenmede algoritmalar aracılığıyla veri kümesine ait birkaç özellik öğrenilir ve yeni veriler geldiğinde verinin sınıfını bulmak için daha önceden öğrendiği özelliklerden yararlanmaktadır (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 383). Bu yöntem üretken özelliklerin çıkarılması, anlamlı eğilimlerin ve yapıların belirlenmesi için yaygın olarak kullanılmaktadır (Sarker, 2021, s. 4). Denetimsiz öğrenmeye ait genel iş diyagramı Şekil 3 de gösterilmektedir.



Şekil 3: Denetimsiz/Gözetimsiz Öğrenme İş Akış Diyagramı
(Makine Öğrenmesi (Machine Learning) Nedir?, 2021)

3.2.5 Yarı Denetimli/Gözetimli Öğrenme

Yarı denetimli (Yarı Gözetimli) öğrenme ise denetimli ve denetimsiz makine öğrenimi yöntemlerinin birleşimidir (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 384). Yarı denetimli öğrenmenin asıl amacı sadece etiketli veriler kullanarak üretilenden daha iyi sonuç sağlayabilmektir (Sarker, 2021, s. 4). Hem denetimli hem de denetimsiz öğrenmenin birleşimi olduğu için her iki öğrenmenin çözmeyi hedeflediği problemlerde de kullanılmaktadır.



Şekil 4: Yarı Denetimli/Gözetimli Öğrenme İş Akış Diyagramı
(Makine Öğrenmesi (Machine Learning) Nedir?, 2021)

deęerini arttırmaktadır. Sosyal medya istihbaratı kavramı açıklanırken istihbarat kavramından itibaren ele alınması tüm resmi görmek için faydalı olacaęı deęerlendirilmekle beraber alıřma alanları ve literatüre yapılan katkılar üzerinde durularak detaylı incelemelere yer verilecektir.

Yapay zeka, gelişimi hızla artan bir konu olup önemi gün geçtikçe daha fazla artmaktadır. Yapay zekanın bir alt dalı olan makine öğrenmesi ise temelde makinelere insan davranışlarının çeşitli algoritmalar ile öğretilerek sonucunda doğru kararlar vermesini ve tahminler yapmasını hedeflemektedir. Problemin asıl amacına göre makine öğrenmesinin türüne ve algoritmasına karar verilmelidir. Algoritmaların çeşitli analizler ve optimizasyonlarla geliştirilerek kurulan makine öğrenmesi modelinin hedeflenen probleme en yüksek doğrulukla tahmin edebilmesi amaçlanmaktadır. Bu bölümde makine öğrenmesi algoritmaları ve bu algoritmaların nasıl çalışmalarda daha iyi sonuçlar verebileceęi tartışılırken aynı zamanda literatürdeki yapılmış çalışmalara da yer verilecektir.

4.1 Sosyal Medya İstihbaratı Çalışma Alanları

Sosyal medya istihbaratı üretmek için sosyal medyadaki veriler üzerinde çeşitli analizler yapılmaktadır. Bu verilerin analizi sonucunda ise karar alıcılar için çok önemli bilgilere ulaşılabilmektedir. Ancak sosyal medyadaki verilerin hacminin oldukça büyük olması sebebiyle çeşitli yaklaşımlar benimsenmektedir. Bu yaklaşımlardan en önemlilerinden biri yapay zekanın alt dalı olan ve temelde bazı kalıpları tanımanın öğretilmesine dayanan makine öğrenmesi metodudur (Akay, 2018, s. 41-53). Makine öğrenmesi metotları kullanarak büyük hacimli verilerin analiz edilmesi noktasında çeşitli yaklaşımlar mevcuttur. Bu yaklaşımların seçimi verinin tipine, hacmine, konusuna ve amacına göre belirlenerek karşılaştırılmalıdır.

Makine öğrenmesi temelli çalışan Doğal Dil İşleme (NLP) bilgisayarlara belgeleri sınıflandırmayı öğretmeyi amaçlamaktadır (Bartlett & Reynolds, 2015, s. 34). Buradaki belgelerden kasıt Twitter uygulamasında paylaşılan bir tweet, Facebook uygulamasında paylaşılan bir gönderi olabilmektedir. Temelde metnin analizine dayanmaktadır. Sınıflandırma ise pozitif, negatif veya nötr olarak yapılmaktadır. Doğal dil işleme kapsamında yapılabilecek bir diğer uygulama ise duygu analizidir. Duygu analizi insanların paylaştıkları metinlerdeki duygu ve düşüncelerini analiz ederek gönderinin olumlu veya olumsuz olarak sınıflandırılmasını sağlayan metottur (Kırıcı & Gülbak, 2020, s. 361). Anlam analizi ise güncel veya yaygın konularda eğilimlerin daha iyi anlaşılmasını sağlamak için kullanılan kelimelerden veya cümlelerden anlam çıkarma metodudur (Evans, 2013, s. 8). Terörizmle mücadele kapsamında sosyal medya verilerinin doğal dil işleme algoritmalarıyla incelenmesi ile mevcut ortamdaki hâkim duyguya, herhangi bir tehdit potansiyeli oluşup oluşmadığına ve durumsal farkındalığa ulaşılabilmektedir.

Olay Tespit Yöntemi, bir olayın gerçekleşebileceğine dair emarelerin, kelimelerin veya kelime gruplarının normalden fazla artmasının gözlemleyerek olayların tespit ve tasnif etmeye çalışmaktadır (Bartlett & Reynolds, 2015, s. 41). Sosyal medya istihbaratı kamu düzenini bozma eğilimdeki olayları engellemek için de kullanılmaktadır (Ivan, Iov, Lutai, & Grad, 2015, s. 506). Terörle mücadele

kapsamında sosyal medya istihbaratı sayesinde řiddet içeren davranıřların tespiti, öngörülmesi, eğiliminin tespit edilmesi ve önlenmesi mümkün olmaktadır (Bural, 2021, s. 120). Bu çerçevede de en çok kullanılan yöntem anahtar kelimeler ile arama yapılarak olası tehditler ve olaylar ile ilgili yapılan filtreleme (Pelzer, 2018, s. 175-177) yöntemidir.

Teknolojik ağ veya internet etnografisi olarak ifade edilen netnografi, etnografi gibi gözlemlerle insan davranıřlarını ve bu davranıřların altında yatan çeřitli nedenleri bağlamsal düzeyde analiz edilme yöntemi olarak ifade edilmektedir (Kozinets, 1997, s. 473). Topluluklarında incelenmesine imkân sađlayan bu yöntemin suç ve terör eylemleri hakkında bilgiler tespit edilmesi ve toplanmasında etkili bir yöntem olduđu deđerlendirilmektedir (Bural, 2021, s. 121). Bu sebeplerden dolayı terörist grupların incelenmesi olası terör faaliyetleri veya yasadıřı eylemlerin tespit edilmesi ve bunların ilgili kurumlarla paylařılması noktasında önemli bir faktör olabileceđi deđerlendirilmektedir.

Büyük hacimli verilerden sıklıkla tekrar eden kelimelerin metin içeriđinden çıkarılarak daha küçük hacimli veriye dönüřtürülmesi iřleminde kullanılan metot İçerik Analizi yöntemi olarak adlandırılmaktadır (Stemler, 2001, s. 1). Diđer bir deyiřle metindeki mesajların özetlenmesine dayanan niceliksel bir metottur (Lai & To, 2015, s. 140). Bu yöntem ile gündemi meřgul eden konular, metnin genel eğilimi, yoğunlukta olan düşünce kalıpları tespit edilebilmektedir. Terörle mücadele kapsamında taranan metinlerden çıkarılan içerik analizlerinden sıklıkla geçen kelimelerden metne hâkim temel düşünceler, genel eğilim tespit edilerek gündemle beraber deđerlendirilerek olası eylem durumu ya da alınabilecek tedbirlerle ilgili çeřitli çıkarımlar yapılarak farkındalık arttırılabilmektedir.

Bir diđer metot olan Sosyal Ağ Analizi yöntemi ile bir ağ içerisindeki belli bir konu hakkındaki içeriklerdeki artışı takip etmek, ağ içerisindeki bilginin yayılmasını takip etmek ve gözlemlemek, ağ oluřturan kullanıcıların davranıřlarını anlamak amaçlanmaktadır. Yani kısacası, ağ içerisindeki iliřkinin dođasını, yoğunluđunu ve sıklıđını tanımlamak için kullanılan matematik ve sosyolojik yöntemlerin bir arada kullanıldıđı bir yöntemdir (Omand, Miller, & Bartlett, 2014, s. 30-31). Sosyal Ağ Analizi yöntemi ile belirli bir hedef özelinde ilgili hedefin açıklarının tespit edilmesi, analiz edilmesi, konular arasındaki bađlantı ve iliřkilerin deđerlendirilmesini sađlayan hedef istihbaratı yöntemi olarak da kullanılmaktadır (Mahood, 2014, s. 8-14). Terörle mücadele kapsamında ise sosyal ağ analizi yöntemi ile terör sempatanlarının arasındaki iliřkiyi oluřturan ağın tespiti, kullanıcılar arasındaki iliřkilerin gücü veya ağa yön veren kanaat önderlerinin tespiti yapılabilmektedir.

4.2 Makine Öğrenmesi Çalışma Alanları ve Kullanılan Algoritmalar

Denetimli metot ile regresyon ve sınıflandırma problemlerine çözümler üretilmektedir (Sarker, 2021, s. 4). Örneđin atılan bir tweetin olumlu mu olumsuz mu olduđunu ifade eden duygu analizi metodunu içeren sınıflandırma problemlerinde veya artan ev fiyatlarının gelecek ay ne kadar olacađı tahminine dayanan regresyon problemlerinde kullanılabilmektedir. Denetimli Öğrenme kapsamında hem sınıflandırma hem de regresyon problemlerinde yaygın olarak Decision Tree, Navie Bayes, Support Vector Machine (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 382), A Neural Network

(Atalay & Çelik, 2017, s. 161-162), Random Forest, K-Nearst Neighborhood, Extreme Gradient Boosting (Sayli & Basarir, 2022, s. 300) kullanılmaktadır. Terörle mücadele kapsamında paylaşılan haberlerin sahte mi gerçek mi ya da sosyal medya istihbaratı çerçevesinde terör olayları sonrası Twitter’da duygu analizi gibi çalışmalarda kullanılabilir.

En yaygın denetimsiz öğrenme görevleri arasında kümeleme, yoğunluk tahmini, özellik öğrenme, boyutluluk azaltma, birliktelik kurallarını bulma, anormallik tespiti yer almaktadır (Sarker, 2021, s. 4). Örneğin bankalarda müşteri profili çıkarılması, bir filmi izleyen izleyicinin birliktelik kuralına göre bir diğer filmi izlemesi için önerilerde bulunulması denetimsiz öğrenme problemlerine örnek oluşturmaktadır. Denetimsiz Öğrenme kapsamında K-Means Clustering ve Principal Component Analysis en yaygın olarak kullanılan algoritmaları oluşturmaktadır (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 383). Terörle mücadele kapsamında terör eylemlerinin gerçekleşme biçimine, olayın niteliklerine göre sınıflandırarak kümeleme çalışmaları yapılabilir.

Denetimli ve denetimsiz öğrenme metotlarının birleşiminden oluşan yarı-denetimli öğrenme metodu çoğunlukla metin sınıflandırma, sahtekarlık tespiti, veri etiketleme gibi problemlerde kullanılmaktadır (Sarker, 2021, s. 4). Transductive Support Vector Machine, Generative Models ve Self-Training (Mahesh, Machine Learning Algorithms-A Review, 2018, s. 384) en yaygın yarı denetimli öğrenme algoritmalarını oluşturmaktadır. Terörle mücadele kapsamında hem denetimli hem de denetimsiz öğrenmede aranan problemlerin verilerin bir kısmının sınıfı belliyse yarı denetimli öğrenme metotları da kullanılabilir.

Takviyeli öğrenme ise ödül ceza sistemine dayalı uygulama alanı olmakla birlikte çoğunlukla oyun teorisi, kontrol teorisi, yöneylem araştırması, bilgi teorisi, sürü zekası, statik ve genetik algoritmalar gibi birçok teoride incelenmekte ve kullanılmaktadır. Markov Decision Processes, multi armed bandits gibi yöntemler çoğunlukla takviyeli öğrenme problemlerinde kullanılmaktadır. Terörle mücadele kapsamındaki örneklerde kullanılmak için denetimli ya da denetimsiz öğrenmeye göre daha az kullanışlı olabilir. Bu nedenle diğer öğrenme metotları tercih edilmelidir.

5. SOSYAL MEDYA İSTİHBARATININ UYGULAMA ALANLARI VE MAKİNE ÖĞRENMESİNİN SOSYAL MEDYA İSTİHBARATINDA KULLANIMI

Bu başlık altında açık kaynak istihbaratı ve sosyal medya istihbaratında ele alınmış çalışmalardan, bunların makine öğrenmesi metotlarıyla ilişkisinden, makine öğrenmesi metotlarının kullanılarak yapıldığı çalışmalardan bahsedilecektir. İncelenen çalışmalar terör ve terörizmle konularında; sosyal medya, terör ve suç veri tabanları kullanılarak yapılan çalışmalar ile sınırlandırılmıştır. Çalışmanın amaçları, kullanılan yöntemlere ve sonuçlara yer verilerek detaylandırılacaktır. İncelenen çalışmalar arasında sosyal ağ analizi, içerik analizi, duygu analizi, siber istihbarat analizi ve suç analizi çalışmaları yer almaktadır.

Aksoy ve Nisan tarafından yapılan ‘‘Türkiye’deki Terör Olayları Çerçevesinde Ankara Patlamaları Üzerine Bir İçerik Analizi Çalışması’’ adlı çalışmada 10 Ekim 2015 Ankara Gar saldırısı, 17 Şubat 2016 Ankara Genelkurmay saldırısı ve 13 Mart 2016 Ankara Güvenpark saldırısıyla ilgili yapılan haberler birer haftalık süreçlerle analiz edilerek halkın terörü içselleştirmesine neden olup olmadığı sorusuna temel oluşturmak amacıyla çalışma gerçekleştirilmiştir.17 gazetenin terör saldırılarını ele alışı incelenmiştir. İçerik analizi ile metinlerin altında yatan anlamları açığa çıkarmak ve yorumlamak için belli kategoriler oluşturularak sistematik sonuçlara ulaşmayı amaçlamıştır. Haberler içerisinde kullanılan söylemin toplum içerisinde korku yarattığı sonucuna varılmıştır. Tüm bulgular sonucunda da Türk ulusal basınında terör saldırılarına yönelik öznel ve duygusal bir tutum sergiledikleri sonucuna varılmıştır (Aksoy & Nisan, 2017, s. 134-158). Genel olarak incelemek gerekirse açık kaynak istihbaratı kapsamında haberler üzerinde terör olayları içerik analizi yöntemi ile incelenmiştir. Ancak tüm işlemler manuel yapılarak makine öğrenmesi algoritmaları kullanılmamıştır. Bu nedenle de kapsam dar tutulmuştur.

Abanoz tarafından yapılan ‘‘Bir Terör Saldırısı Sırasında Sosyal Medya Reaksiyonun Duygu Analizi’’ adlı çalışmanın amacı; travma oluşturan şiddeti araç olarak kullanan bir terör saldırısı anında, sosyal medya kullanıcıları tarafından oluşturulan içeriğin anlamsal boyutunun incelenmesidir. 2015 yılında İstanbul Adalet Sarayı’nda yaşanan ve savcı Mehmet Selim Kiraz’ın öldürülmesiyle sonuçlanan terör saldırısı sırasında Twitter üzerindeki kullanıcı paylaşımları, duygu analiz yöntemiyle değerlendirilmiştir. Tweetler Twitter Stream API üzerinden çekilmiştir. Toplamda 125,234 adet metin verisi incelenmiştir. Kelime gruplarının analizi neticesinde çeşitli etiketler çıkarılmıştır. Bunlar hem pozitif, negatif ve nötr olarak hem de kelimelerin sıklıkları özelinde incelemeler yapılmıştır (Abanoz, 2018, s. 214-232). Genel değerlendirme yapmak gerekirse sosyal medya istihbaratı üzerine bir çalışma yapmış ve Twitter verileri API kullanarak çekilmiştir. Ancak sonrasında gerçekleştirilen tüm analizler Doğal Dil İşleme metotları kullanılarak daha derinlemesine, efektif bir çalışma yapılır dense de ve istatistiksel grafik ve tablolara yer verilse de makine öğrenmesi algoritmaları kullanılmamış ve duygu analizleri manuel olarak gerçekleştirilmiştir.

Bural tarafından yapılan ‘‘Terörizmle Mücadelede Sosyal Medya İstihbaratı: FETÖ/PDY Terör Örgütü Sosyal Ağ Analizi Örneği’’ adlı çalışmada sosyal medyadan elde edilecek istihbaratın terörizmle mücadelede ne şekilde kullanılabileceğini arařtırmayı amaçlamaktadır. Daha da özelinde Twitter’da bulunan FETÖ/PDY terör örgütü sempatanları ağının sosyal medya istihbaratıyla analiz edilmesiyle örgütün iletişim ağının tespit edilebileceği hedeflenmektedir. Çalışma kapsamında FETÖ/PDY terör örgütü sempatanları ve iltisaklı buldukları kişiler ile son attıkları tweetler incelenmiştir. Yapılan sosyal ağ analizi ve içerik analizi çalışmalarının sonucunda FETÖ/PDY terör örgütü sempatanlarının sosyal medyada oluşturdukları sosyal ağlarda örgütün iletişim, propaganda ve haberleşme ağlarının, ayrıca bu ağlar içerisinde önemli roller üstlenen bireylerin tespit edilebildiği sonucuna erişilmiştir (Bural, Terörizmle Mücadelede Sosyal Medya İstihbaratı: Fetö/Pdy Terör Örgütü Sosyal Ağ Analizi Örneği, 2022, s. 60-83). Çalışma genel olarak değerlendirildiğinde çalışma sonucunda elde edilen

bulgular terörle mücadele kapsamında oldukça önemlidir. Ancak veri toplanmasının manuel yapılması, veri analizlerinin programlar üzerinden yapılmaması hem yavaş hem de kısıtlı bir analiz yapılmasına sebep olmuştur. Hem sosyal ağ analizinde hem de içerik analizinde makine öğrenmesi metotları kullanılmamıştır.

Ünver tarafından yapılan “Türkiye’deki Rus Dijital Medya ve Bilgi Ekosistemi” adlı çalışmada Türkiye’deki Rusya yanlısı bilgi faaliyetlerinin etkisini ve önemini arařtırmayı amaçlamıştır. Bu kapsamda beş ana olay ele alınmıştır. Bunlardan birincisi SU24 düşürme olayı, ikincisi Temmuz 2016 Darbe Girişimi, üçüncüsü Ankara Rus Büyükelçisi Suikastı, dördüncüsü Seçime Karışma İhtimali ve sonuncusu ise S400 Tedarik Süreci vakasıdır. Bu vakalar kapsamında medyada ve sosyal medya üzerinde yayılan yanlış bilgilerin ve yapılan dezenformasyon çalışmalarının nasıl geliştiğine dair söylem ve içerik analizleri yapılmaktadır (Ünver, 2019, s. 1-47). Ancak analizlerde makine öğrenmesi metotları kullanılmamış olup çeşitli yazılımlarla analiz gerçekleştirilmiş ve sonuçlara bu şekilde ulaşılmıştır.

Ateş, Bostancı ve Güzel tarafından yapılan “Veri Madenciliği Teknikleri ile Açık Kaynak İstihbaratı: Sosyal Medya İle Bbc, Cnn, Al Jazeera Ve Reuters Haber Ajanslarına Ait Gündemin Mukayesesi” adlı çalışmada sosyal medyadan elde edilen veriler ile haber ajanslarının paylaşımlarının mukayese edilerek, ne kadar benzerlik gösterdiğinin belirlenmesi amaçlanmıştır ve bu amaçla da doğal dil işleme yöntemleri kullanarak açık kaynak istihbaratı üretmek hedeflenmiştir. Bu kapsamda çeşitli haber siteleri incelenmiş, metin benzerliğini ortaya koymak için ise TF-IDF doküman benzerliğinde terim frekansı baz alınmıştır. Elde edilen sonuçlarda en fazla benzerliğin %51 ile BBC News (World)’de olduğu, diğer sonuçların oldukça düşük olduğu gözlemlenmiştir. Bu durum da istihbarı açıdan önemi tartışmalı olsa da açık kaynak istihbaratı yapılarak, nadir bilgilere erişebileceğini göstermektedir (Ateş, Bostancı, & Güzel, 2021, s. 329-338). Genel olarak incelendiğinde analiz makine öğrenmesi metotları kullanarak python üzerinde yapılmış ancak bir tanesine yer verilmiştir. Ancak yapılan çalışma ufak bir örnekleme test etse de suç ve suçla önlemede fikir verdiği değerlendirilmektedir.

Meral ve Diri tarafından yapılan “Twitter Üzerinde Duygu Analizi” adlı çalışmada Twitter’den toplanan verilerle algı analizi yapılmıştır. Analiz gerçekleştirilirken doğal dil işleme ve Naïve Bayes, Random Forest ve Support Vector Machine gibi makine öğrenmesi yöntemleri kullanılarak, akıllı bir sistem oluşturulmuş ve elde edilen sonuçlar karşılaştırmalı olarak verilmiştir. Doğal dil işleme kapsamında verileri öncelikle olumlu, olumsuz ve nötr olarak sınıflandırmıştır. Doğal dil işleme kapsamında n-gram ve kelime tabanlı yöntemler; sınıflandırma kapsamında ise Naive Bayes, Random Forest ve Support Vector Machine yöntemlerini kullanmıştır. Toplamda ise %90’a yakın başarı tespit edilmiştir (Meral & Diri, 2014, s. 690-693). Algı analizi kapsamında hem makine öğrenme metotlarını hem python kullanılarak yapılmış bir çalışma olmuştur. Hem de sosyal medya verileri ortaya koymakla beraber sosyal medya istihbaratı kapsamında yapılacak algı analizleri kapsamına örnek teşkil etmektedir.

Özgür ve Erdem tarafından yapılan “Saldırı Tespit Sistemlerinde Kullanılan Kolay Erişilen Makine Öğrenme Algoritmalarının Karşılaştırılması” adlı çalışmada Saldırı Tespit Sistemleri kapsamında bir

sınıflandırma projesi yapılmıřtır. KDD99 veri setini kullanarak eđittiđi veriden gelen test verilerinin normal mi yoksa saldırımı olduđunu tahmin ettirmiřtir. Verinin sınıfını makine öğrenmesi metotlarından Decision Tree, Artificial Neural Network, Boosting-AdaBoost ve Support Vector Machines algoritmalarını Weka kullanarak deneyerek bulmuřtur. Yapılan çalıřmanın her algoritma için toplam başarısının %90 üzerinde olduđu tespit edilmiřtir (Özgür & Erdem, 2012, s. 41-48). Siber saldırılar üzerine bir makine projesi yapılmıř ancak python kullanılmadan Weka üzerinde çalıřmalar yapılmıřtır. Veri setinin uygunluđu sebebiyle detaylı bir ön iřleme adımları yapılmadan %90 üzerinde başarı sađlansa da verinin başarısını arttırmaya yönelik bařka çalıřmalarda uygulanarak veri başarısının daha yüksek olması hedeflenebilirdi.

řaylı ve Bařarır tarafından “Suç Veri Setini Analiz Etmek İçin Makine Öğreniminde Örnekleme Teknikleri ve Uygulaması” adlı çalıřmada elde edilen suç veri seti üzerinde üç hedef üzerinde sınıflandırma projesi gerçekteřtirilmiřtir. K-Nearest Neighborhood, Random Forest ve Extreme Gradient Boosting algoritmaları kullanılarak pythonda gerçekteřtirilmiř bir çalıřmadır. Hedefler özelinde Principal Component Analysis metodu kullanarak kümele çalıřmasına da yer verilmiřtir. Çalıřma sonunda algoritmaların başarı oranları K-Nearest Neighborhood ve Random Forest algoritmaları için benzer ve genelde %95’in üzerinde çıkarken Extreme Gradient Boosting algoritması her hedef için deđiřmekle beraber ortalama %85 olarak belirlenmiřtir (Saylı & Bařarır, 2022, s. 296-310). Çalıřma kapsamında makine öğrenmesi metotları ve python kullanarak veri seti üzerinde sınıflandırma çalıřması yapılmıřtır. Ayrıca sınıflandırma başarısının yükselmesi için farklı veri temizleme, veri üretme, veri normalizasyonu ve birbirinden farklı örnekleme teknikleri de kullanılarak yapılmıřtır.

Dereli, Adıgüzel ve Karagöz tarafından yapılan “Eriřime Açık Terörizm Veri Kümeleri Kullanarak Makine Öğrenmesi ve Büyük Veri Mimarileri ile Terörle Mücadeleye Yönelik Tahminleme Yaklařımları” adlı çalıřmada makine öğrenmesi veya büyük veri teknolojileri kullanılarak terörizm alanında yapılan on tane makale belirlemiř ve bunları analiz etmiřtir (Dereli, Adıgüzel, & Karagöz, 2022, s. 119-151). Bu makaleler arasında Türkçe kaynak olmayıp tamamı yabancı literatür kaynaklıdır. Bu yapılan çalıřmalar arasında Wang, Cui ve He tarafından yapılan teröristlerin riskini deđerlendirmek için yaptıđı sınıflandırma çalıřması (Wang, Cui, & He, 2022, s. 1965-1972) üzerine yaptıđı sınıflandırma çalıřması, Huamani, Alva ve Gonzales tarafından yapılan dünya çapında terörist saldırıları tespit etmek (Huamani, Alva, & Gonzalez, 2020) için yaptıđı sınıflandırma çalıřması ve Atsa’am, Douglas, Wario ve Okpo tarafından yapılan terörizm kategorisi (Atsa’am, Douglas, Wario, & Okpo, 2020, s. 369-384) bulan kümeleme çalıřması en dikkat çekici olanlarıdır. Atsa’am vd. tarafından yapılan kümeleme çalıřmasında 168 terör olayı verisi üzerinde Aglomeratif Hiyerarşik Kümeleme uygulanmıř ve 4 küme elde edilmiř ve meydana gelen zayıta ve oluřan sonuca göre yapılan bu kümelemelerin, bütçeleme ve kaynakların dađıtımı açısından küresel terörle mücadele stratejisine katkı sađladıđı vurgulanmıřtır. Huamani vd. (2020) çalıřmasında, terör verileri üzerine Decision Tree ve Random Forest algoritmaları ile bölge ve saldırı türüne göre tahminleme sonuçları incelenmiř ve Random Forest

algoritmasının yaklaşık %90'lık başarı ile daha iyi sonuç verdiđi tespit edilmiştir. Wang, Cui ve He tarafından sunulan çalışmada teröristlerin risk tahmin için “Top-K Algoritması” ve CNN yapay sinir ađı modeli birleştirilmiştir. Çıkan sonuçlar tahmin başarısında %90-%95 arasında deđişmekte olup gerçekleştirilen çalışmalarda en yüksek başarı oranını vermiştir.

Joseph, Maher ve Neumann tarafından yapılan “#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks” adlı çalışmada sosyal medya istihbaratı kullanılarak sosyal medya haberlerinin yayılımı üzerine bir analiz gerçekleştirilmiştir (Joseph, Maher, & Neumann, 2014, s. 1-28). Çatışma bölgelerindeki bilgilerin resmi hesaplar üzerinden deđil yayıcı olarak ifade edilen hesaplar üzerinden dađıldığı tespit edilmiştir. Bu çalışmada makine öğrenmesi metotlarının kullanılmadığı görülmüştür.

Intelligence Advanced Research Projects Activity (IARPA) tarafından yapılan “TrojAI” projesinde makine öğrenmesi metotları kullanılarak siber istihbarat analizi yapılmıştır. Açık kaynak istihbaratının makine öğrenmesi teknikleri kullanılarak yapılacak projelerinden biridir. Siber saldırılara sebep olan Truva atlarının erken tespit edilmesi için makine öğrenmesi türlerinden pekiştirmeli/takviyeli öğrenme metodunun uygulanarak geliştirildiđi bir projedir (TrojAI, 2019).

Bu alanda yapılan çalışmaları genel olarak deđerlendirecek olursak; Türkçe ve yabancı literatürün her ikisinde de makine öğrenmesi aktif olarak çalışılmakta ve başarılı sonuçlar elde edilmektedir. Ancak açık kaynak istihbaratı veya sosyal medya istihbaratı konularında makine öğrenmesi teknikleri kullanan Türkçe literatürde çalışma görülmemiş yabancı literatürde ise oldukça az olduđu tespit edilmiştir. Türkçe literatürdeki sosyal medya istihbaratı çalışmaları yapay zeka teknolojileri kullanılmadan daha manuel süreçlerle yönetilmiştir. Ancak suç ve terör veri tabanları kullanılarak ve yapay zeka teknolojilerinden faydalanılan çalışmaların olduđu gözlemlenmiştir. Terörizm konularında sosyal medya istihbaratı üretmeyi hedefleyen yapay zeka teknolojileri kullanmış Türkçe literatürde çalışma gözlemlenmemiş olup yabancı literatürde ise örneklerinin az olduđu tespit edilmiştir.

6. MAKİNE ÖĞRENMESİ KULLANARAK TERÖRİZM KONULARINDA SOSYAL MEDYA İSTİHBARATI ÜRETİLEBİLİR Mİ?

Sosyal medya istihbaratı özellikle sosyal medyanın gün geçtikçe popüler olmasından da kaynaklı olarak oldukça önemli bir konudur. Her kesimden, gruptan, görüşten, inanıştan insan çeşitli amaçlarla sosyal medya kullanmaktadır. Terör örgütlerinin ise propaganda yapmak, ideolojilerini yaymak, eleman temin etmek, dezenformasyon yapmak gibi birçok sebeple sosyal medya kullandığı bilinmektedir. Bu nedenle de sosyal medya kullanarak elde edilecek istihbarat oldukça önem teşkil etmektedir. Ancak verinin zaman geçtikçe büyümesi dakikada sosyal medyada milyonlarca verinin üretilmesi elde edilen bu büyük verinin analizini yapmayı zorlaştırmıştır. Eskiden manuel olarak yapılan istihbarat analizleri büyük verinin varlığıyla yapay zeka teknolojileri kullanılarak yapılan analizlerle yer deđiştirmiştir. Bu analizlerde kullanılan makine öğrenmesi metotları ise amaca yönelik çalışma yapmada oldukça yararlı

olduđu gözlemlenmektedir. Öncelikli olarak ana problemin türüne göre makine öğrenmesinin çeşidi belirlenerek daha sonrasında ise bu problemi çözmek için çeşitli algoritmalar kullanarak en uygun model tespit edilir. Son olarak ise modelin başarısını yükseltmek amacıyla çeşitli optimizasyon çalışmaları gerçekleştirilerek en doğru analizlerin ortaya çıkması hedeflenmektedir.

Yapılan çalışmalar incelendiğinde açık kaynak istihbaratı kullanarak çalışmalar yapıldığı ve bunların çoğunda sosyal medya platformlarından özellikle de Twitter'dan yararlandığı tespit edilmiştir. Ancak yapılan çalışmalarda özellikle Türkçe literatürde makine öğrenmesi metotlarının kullanılmadığı, bu nedenle veri ön işleme adımlarının çoğunlukla manuel yapıldığı, veri kümelerinin oldukça sınırlı kaldığı, verileri analiz etme sürelerinin verinin azlığına rağmen uzun sürdüğü gözlemlenmiştir. Makine öğrenmesi metotlarının ancak sosyal medya istihbaratı çalışmalarında değil suç ve terör veri tabanlarını analiz etmede kullanıldığını ve başarılı sonuçlar elde edildiği gözlemlenmiştir.

İncelenen makine öğrenmesi projelerinde çoğunlukla sınıflandırma problemleri üzerinde çalışıldığı Random Forest, Decision Tree ve K-Nearest Neighborhood algoritmaları kullanarak en yüksek başarı oranlarına ulaşıldığı tespit edilmiştir. Bu başarıyı arttırmak için hem veri analiz kısmında hem metin analiz kısmındaki ön işleme adımlarında ve modelde test verilerindeki sınıf farkının azaltılması noktasında tahminleme başarısını arttırmak için çeşitli teknikler kullanılmıştır. Bu yöntemler sonucunda bazı verilerde %90 bazılarında ise %95'in üzerinde başarı oranlarına ulaşıldığı tespit edilmiştir.

Makine öğrenmesi çalışmalarında oldukça faydalı çalışmalar olmakla beraber sosyal medya istihbaratı kapsamında terörizm konularında çalışma özellikle Türkçe literatürde yer almadığı sonucuna ulaşılmıştır. Yabancı literatürde ise sosyal medya kullanılarak sosyal medya istihbaratı kapsamında değil açık kaynak terör veri tabanları kullanarak çalışmalar yapıldığı görülmüştür.

Tüm bu sonuçlardan hareketle yabancı literatürde açık kaynak istihbaratı projelerinde makine öğrenmesi tekniklerinin kullanıldığı ancak terörizm konusunda yapılan özellikle sosyal medya istihbaratı çalışmalarının bazılarında manuel ve kısıtlı analizler görüldüğü makine öğrenmesi tekniklerinin kullanıldığı çalışmaların ise çok sınırlı olduğu tespit edilmiştir.

Türkçe literatürde ise terörizm konularında makine öğrenmesi teknikleri kullanarak sosyal medya istihbaratı çalışmaları yapılmadığı tespit edilmiştir. Ancak makine öğrenmesinin özellikle büyük veriler üzerindeki başarısı düşünüldüğünde verinin hacminin oldukça büyük olduğu sosyal medya kullanılarak yapılacak sosyal medya istihbaratı çalışmalarında hem daha geniş bir örnekleme hem de farklı tekniklerle daha hızlı, daha efektif sonuçlar vereceği değerlendirilmektedir. Bu kapsamda öncelikli olarak çoğunlukla kullanılan sınıflandırma problemleri üzerine başarıları yüksek olan algoritmalar üzerinden sosyal medya platformlarından elde edilecek veriler ile terörizm kapsamında anlamlı bir analiz yapılırsa faydalı sonuçların çıkarılacağı ve bu sonuçların terörizmle mücadele kapsamında kullanılabilmesi değerlendirilmektedir.

7. SONUÇLAR

Terörizm ortaya çıktığı ilk zamanlardan itibaren gün geçtikçe farklılaşarak varlığını sürdürmek için çeşitli yollar aramış ve bulmuştur. Günümüzde yaşanan devrim niteliğinde olan teknolojik gelişmeleri terör örgütleri de yakından takip etme ve bu değişime ayak uydurmak için örgüt yapılarını geliştirmişlerdir. Sosyal medyanın çok aktif olarak kullanıldığı günümüzde terör örgütleri de çok yakından bu platformları takip etmiş, kendi menfaatleri doğrultusunda kullanmış ve kullanmaya da devam etmektedir.

Sosyal medya her geçen gün artan kullanıcısı ve bu kullanıcıların paylaşmış oldukları veriler ile artarak çoğalan bir yapıya sahiptir. Kullanıcılar tarafından bu platform çok farklı amaçlara hizmet etmek üzere değerlendirilmektedir. Teknolojiyi yakından takip eden terör örgütleri ise kendi lehlerine bu platformları kullanmanın yollarını aramış ve uygulamıştır. Terör örgütleri tarafından günümüzde sosyal medya örgüt propagandası yapmak, örgüte eleman temin etmek, örgüt elemanlarına eğitim vermek, örgüt ideolojisini yaymak, örgüte mali destek sağlamak gibi birçok amaçla kullanılmaktadır. Bu noktada ise kolluk kuvvetlerinin bu eylemleri fark etme, önceden tespit etme ve engelleme gibi noktalarda sorumlulukları daha da çok artmıştır.

Makine öğrenmesi gelişen çeşitli yapay zeka teknolojileriyle beraber hızı durdurulamaz bir şekilde gelişmeye, popülerliği artmaya ve sağladığı faydalarla birçok çalışma için umut verici sonuçlar elde etmeye devam etmektedir. Sağlıktan ekonomiye, bankacılıktan telekomünikasyona, ulaşımdan savunma sanayiye kadar birçok alanda yaygın bir şekilde kullanılmaktadır. Sosyal medyanın popülerleşmesiyle beraber sosyal medya istihbaratı üretme konusunda da çeşitli duygu analizleri, içerik analizleri gibi alanlarda da aktif bir şekilde kullanılmaktadır.

Bu makalede sosyal medya istihbaratından terörle mücadele noktasında faydalı bilgiler sağlanacağı ve makine öğrenmesi metotları ile bu çalışmaların gerçekleşmesi durumunda ise hem daha büyük bir veride hem daha hızlı bir şekilde hem de daha efektif sonuçlara ulaşılabileceği tartışılmıştır.

Öncelikli olarak sosyal medya istihbaratı konusu ele alınmış, tümdengelim metodu kullanılarak istihbarat kavramından sosyal medya istihbaratına kadar kısaca tanımlanmıştır. Daha sonrasında sosyal medya çalışma alanlarına ve bu alanlarda yapılmış uygulamalara yer verilmiştir. Yapılan çalışmalar neticesinde sosyal medya istihbaratı kullanılarak terörizm kapsamında faydalı bilgilere ulaşıldığı ve bu alanda yapılacak kapsamlı çalışmalarla terör örgütlerinin örgüt yapısı, eylem planları, haberleşme ağı gibi bilgilere ulaşılabileceği görülmüştür.

Daha sonrasında makine öğrenmesi çerçevesi tümdengelim metodu ile yapay zekadan derinlemesine inerek incelenmiş, bu alandaki çalışma alanlarına ve yapılmış örnek çalışmalara yer verilmiştir. Random Forest, Decision Tree ve K-Nearest Neighborhood gibi algoritmalarının başarı oranlarının yüksek olduğu ve veri ön işleme de ya da sınıflandırılacak verilerde uygulanacak geliştirmelerle başarı oranının daha çok yükselebileceği gözlemlenmiştir.

Tüm çalışmalar deęerlendirildięinde gn getike byyen sosyal medya verilerinden manuel ya da program aracılıęıyla yapılan tekniklerde ok dar bir alanda alıřmanın mmkn olabildięi, sosyal medya istihbaratı alıřmalarının makine ęrenmesi teknikleri ile yapılırsa daha byk veri setlerinde alıřılabileceęi, iřlemlerin kullanılan yazılım dilleri sayesinde bir yazılım programına gre daha hızlı bir Őekilde sonulanacaęı, ıkan sonuların ise daha verimli anlamlar ifade edeceęi sonucuna varılmıř ancak zellikle Trke literatrde terrizm konularında makine ęrenmesi tekniklerinin ve yazılım dilinin kullanıldıęı alıřmalar olmadıęı tespit edilmiřtir.

Sosyal medya istihbaratının her geen gn artan sosyal medya kullanımı uzunca bir sre daha poplerlięini koruyacaęı dřnlmektedir. Bununla birlikte bu platformlardaki byk verinin varlıęı hem de ok hızlı bir Őekilde artan verinin analizi byk veri ve yapay zeka teknolojileri kullanılmazsa bir sorun olarak varlıęını srdrmeye devam edecektir. Hem istihbarat hem de kolluk kuvvetleri iin buradaki verilerin analizi ve anlamlandırılması olası gvenlik problemlerinin tespiti, nlenmesi veya takibi aısından da olduka nemlidir. Makine ęrenmesi ve derin ęrenmesi teknikleri kullanarak gerekleřtirilecek analizlerde bařarılı sonular elde edileceęi grlmektedir. Tm bu sebeplerden dolayı yapılacak sonraki alıřmalarda iř birimlerinden de destek alarak terrizm konularında sosyal medya istihbaratı noktasında makine ęrenmesi teknikleri ile daha akılcı zmler elde edilebileceęi deęerlendirilmektedir. Eęer sosyal medya istihbaratı kapsamında grntler zerine analiz yapılacaksa derin ęrenme alıřmalarının da olduka faydalı sonular verebileceęi deęerlendirilmektedir.

KAYNAKLAR

- Abanoz, E. (2018). Bir Terr Saldırısı Sırasnda Sosyal Medya Reaksiyonun Duygu Analizi. *Terr ve Uyuřturucu Madde Őiddeti*, s. 214-232.
- Akay, E. . (2018). Ekonometride yeni bir ufuk: Byk veri ve makine ęrenmesi. *Sosyal Bilimler Arařtırma Dergisi*, s. 41-53.
- Akbulut, F., & Beren, F. (2012). Terrle Mcadelede Btncl Yaklařımın Sosyal Politika Uygulamaları Baęlamından Algılanması: Suru İlesi rneęi. *Akademik İncelemeler Dergisi (Journal of Academic Inquiries)*, s. 257-283.
- Aksoy, G. P., & Nisan, F. (2017). Trkiye'deki terr olayları erevesinde Ankara patlamaları zerine bir ierik analizi alıřması. *TRT Akademi*, s. 134-158.
- Alzubi, J., Nayyar, A., & Kumar, A. (2018). Machine Learning from Theory to Algorithms: An Overview. *Second National Conference on Computational Intelligence*, s. 1-16.
- Antonius, N., & Rich, L. (2013). Discovering Collection and Analysis Techniques for Social Media to Improve Public Safety . *The International Technology Management Review*, s. 42-53.
- Ata, K. K. (2019). İstihbarat, Casusluk, Karřı Casusluk, rtl Operasyonlar ve Gvenlik. *Gvenlik Portalı Gvenlik Yazıları Serisi*, s. 1-12.
- Atalay, M., & elik, E. (2017). Byk Veri analizinde Yapay Zeka ve Makine ęrenmesi uygulamaları. *Mehmet Akif Ersoy niversitesi Sostal Bilimler Enstits Dergisi*, s. 155-172.

- Ateř, E. C., Bostancı, E., & Güzel, M. S. (2021). Veri Madencilięi Teknikleri İle Açık Kaynak İstihbaratı: Sosyal Medya İle Bbc, Cnn, Al Jazeera Ve Reuters Haber Ajanslarına Ait Gündemin Mukayesesi. *Uluslararası Hitit Güvenlik Çalıřmaları Kongresi*, s. 329-338.
- Atsa'am, Douglas, D., Wario, R., & Okpo, F. E. (2020). A new terrorism categorization based on casualties and consequences using hierarchical clustering. *Journal of applied security research*, s. 369-384.
- Balaban, M. E., & Kartal, E. (2015). *Veri Madencilięi ve Makine Öğrenmesi*. İstanbul: Çaęlayan Kitapevi.
- Bartlett, J., & Reynolds, L. (2015). The State of the Art 2015: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism. *Demos*.
- Benes, L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security*, s. 22-37.
- Bural, E. B. (2021). *Açık Kaynak istihbaratında Yeni Bir Boyut Sosyal Medya İstihbaratı*. Ankara: Yeditepe Akademi Yayıncılık.
- Bural, E. B. (2022). Terörizmle Mücadelede Sosyal Medya İstihbaratı: Fetö/Pdy Terör Örgütü Sosyal Ağ Analizi Örneęi. *İstihbarat Çalıřmaları ve Arařtırmaları Dergisi*, s. 60-83.
- Clark, J. R. (2007). *Intelligence and national security: A reference handbook*. Wetsport: Bloomsbury Publishing USA.
- Dereli, C., Adıgüzel, F., & Karagöz, P. (2022). Eriřime Açık Terörizm Veri Kümeleri Kullanarak Makine Öğrenmesi ve Büyük Veri Mimarileri ile Terörle Mücadeleye Yönelik Tahminleme Yaklaşımları. *Savunma Bilimleri Dergisi*, s. 119-151.
- Ergil, D. (1992). Uluslararası terörizm. *Ankara Üniversitesi SBF Dergisi*, s. 139-143.
- Evans, R. (2013). *Social media intelligence: Current approaches & emerging opportunities*. IHS White Paper.
- Gruters, P. C., & Gruters, K. T. (2018). Publicly available information: Modernizing defense open source intelligence. *Special Operations Journal*, s. 97-102.
- Gültepe, Y. (2019). Makine Öğrenmesi Algoritmaları ile Hava Kirlilięi Tahmini Üzerine Karşılařtırılmalı Bir Deęerlendirme. *European Journal of Science and Technology*, s. 8-15.
- Hassan, N. A., & Hijazi, R. (2018). *Open source intelligence methods and tools*. New York: NY: Apress.
- Hoffman, B. (2006). *Inside Terrorism*. New York: Columbia University Press.
- Hribar, G., Iztok, P., & Teodora, I. (2014). OSINT: a "grey zone"? *International Journal of Intelligence and CounterIntelligence*, s. 529-549.
- Huamaní, E. L., Alva, M. A., & Gonzalez, A. R. (2020). Machine learning techniques to visualize and predict terrorist attacks worldwide using the global terrorism database. *International Journal of Advanced Computer Science and Applications*.
- İște Türkiye'de bu yıl kullanıcı sayısını en fazla artıran sosyal medya platformu*. (2023). In Business: <https://www.inbusiness.com.tr/sektorler/is-dunyasi/2023/08/16/iste-turkiyede-bu-yil-kullanici-sayisini-en-fazla-artiran-sosyal-medya-platformu> adresinden alındı
- Ivan, A. L., Iov, C. A., Lutai, R. C., & Grad, M. N. (2015). Social media intelligence: opportunities and limitations. *CES Working Papers*, s. 505-510.

- Joseph, A. C., Maher, S., & Neumann, P. R. (2014). #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks. *International Center for the Study at Radicalisation*, s. 1-28.
- Kent, S. (1949). *Strategic Intelligence for American World Policy*. Oxford: Oxford University Press.
- Kırıcı, P., & Gülbak, E. (2020). Instagram Verileri ile Duygu Analizi. *Avrupa Bilim ve Teknoloji Dergisi*, s. 360-364.
- Kozinets, R. V. (1997). "I want to believe": a netnography of the X-Philes' subculture of consumption. *Advances in consumer research*, s. 470-475.
- Lai, L. S., & To, W. M. (2015). Content analysis of social media: A grounded theory approach. *Journal of electronic commerce research*, s. 138-152.
- Laqueur, W. (1977). *Terrorism*. Boston: Little Brown and Company.
- Lowenthal, M. M. (2004). Open Source Intelligence: New Myths, New Realities. *National Defence University Press*, s. 1-6.
- Mahesh, B. (2018). Machine Learning Algorithms-A Review. *International Journal of Science and Research*, s. 380-386.
- Mahood, L. E. (2014). SOCMINT: Following And Liking Social Media Intelligence.
- Makine Öğrenmesi (Machine Learning) Nedir?* (2021). turhost.com: <https://www.turhost.com/blog/makine-ogrenmesi-machine-learning-nedir/> adresinden alındı
- McIntyre, K. E. (2014). The evolution of social media from 1969 to 2013: A change in competition and a trend toward complementary, niche sites. *The Journal of Social Media in Society*, s. 5-25.
- Meral, M., & Diri, B. (2014). Twitter Üzerinde Duygu Analizi. *2014 IEEE 22nd Signal Processing and Communications Applications Conference (SIU 2014)*, s. 690-693.
- Nabiyev, V. (2012). *Yapay Zekâ*. Ankara: Seçkin Yayıncılık.
- Omand, D., Miller, C., & Bartlett, J. (2014). *Towards the Discipline of Social Media intelligence*. Hobbs, C., Moran, M. ve Salisbury, D. (Ed.). *Open source Intelligence in the twenty-first century: new approaches and opportunities*. London: Palgrave Macmillan.
- Omand, D.-J. B., & Miller, C. (2012a). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, s. 801-823.
- Omand, D.-J. B., & Miller, C. (2017). Introducing Social Media Intelligence. *The Palgrave Handbook of Security, Risk and Intelligence*, s. 355-371.
- Oruç, M. A. (2022). İstihbarat ve Yapay Zekâ İlişkisi. *Social Sciences Studies Journal (SSSJJournal)*, s. 4224-4234.
- Özgür, A., & Erdem, H. (2012). Saldırı Tespit Sistemlerinde Kullanılan Kolay Erişilen Makine Öğrenme Algoritmalarının Karşılaştırılması. *Bilişim Teknolojileri Dergisi*, s. 41-48.
- Pelzer, R. (2018). Policing of terrorism using data from social media. *European Journal for Security Research*, s. 163-179.
- Saral, C. (2016). *Terörün Gizli Efendileri (Dünyayı Armageddona Zorlayanlar)*. Ankara: Kripto Yayınları.

- Saran, M., & Bitirim, S. (2010). Terörle mücadelede sosyal pazarlama ve iletişim stratejileri. *Uluslararası Güvenlik ve Terörizm Dergisi*, s. 87-109.
- Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research. *SN Computer Science*, s. 1-21.
- Sayli, A., & Basarir, S. (2022). Sampling Techniques and Application in Machine Learning in order to Analyse Crime Dataset. *European Journal of Science and Technology*, s. 296-310.
- Schmid, A. P. (2011). Prevention of Terrorism: Towards A Multi-Pronged Approach. *The Routledge Handbook of Terrorism Research*, s. 86-113.
- Schmid, A. P. (2011). *The Routledge handbook of terrorism research*. Wales: Taylor & Francis.
- Scott, D. M. (2010). *The new rules of marketing and PR: How to use social media, blogs, news releases, online video, and viral marketing to reach buyers directly*. New Jersey: John Wiley & Sons.
- Somvanshi, M., Chavan, P., Tambade, S., & Shinde, S. V. (2016). A Review of Machine Learning Techniques using Decision Tree and Support Vector Machine. *2016 international conference on computing communication control and automation (ICCUBEA)*. IEEE, s. 1-7.
- Son 50 Yılda Meydana Gelen Sansasyonel Terör Olayları*. (2020). Terör Olayları Takvimi: <https://terortakvimi.wordpress.com/2001/09/11/200111-eylul-saldirilari/> adresinden alındı
- Stemler, S. (2001). An overview of content analysis. Practical Assessment. *Research & Evaluation*, s. 1-6.
- Stottlemyre, S. A. (2015). HUMINT, OSINT, or something new? Defining crowdsourced intelligence. *International Journal of Intelligence and CounterIntelligence*, s. 578-589.
- Şimşek, M. (2016). Terörizm: Kavramsal Bir Çalışma. *Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi*, s. 319-335.
- Şuşnea, E., & Iftene, A. (2018). The significance of online monitoring activities for the social media intelligence (SOCMINT). *In Conference on mathematical foundations of informatics*, s. 230-240.
- TrojAI*. (2019). Intelligence Advanced Research Projects Activity (IARPA): <https://www.iarpa.gov/research-programs/trojai> adresinden alındı
- Ünver, H. A. (2019). Türkiye'deki Rus Dijital Medya Ve Bilgi Ekosistemi. *Siber Politikalar ve Dijital Demokrasi*, s. 1-47.
- Wang, Y., Cui, X., & He, P. (2022). Winning the War On Terror: Using "Top-K" Algorithm And CNN To Assess The Risk Of Terrorists. *International Journal of Information Technology and Web Engineering (IJITWE)*, s. 1-15.
- We Are Social 2023 Global ve Türkiye Raporu*. (2023). #WEAREOMGTEAM: <https://omgiletisim.com/we-are-social-dijital-2023-global-ve-turkiye-raporu-yayinlandi/> adresinden alındı
- Wilkinson, P. (1974). Political terrorism. *London: Macmillan*.
- Yayla, A. (1990). Terör ve terörizm kavramlarına genel bakış. *Ankara Üniversitesi SBF Dergisi*, s. 335-385.
- Yılmaz, A. (2017). *Yapay Zekâ*. İstanbul: Kodlab Yayınları.