



T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

TERÖRİZMLE MÜCADELEDE SOSYAL MEDYA İSTİHBARATININ
ÖNEMİ: PKK TERÖR ÖRGÜTÜNÜN TWİTTER'DAKİ GÖRÜNÜRLÜĞÜ
ÜZERİNE SOSYAL AĞ ANALİZİ

YÜKSEK LİSANS TEZİ
ULUSLARARASI GÜVENLİK VE TERÖRİZM ANA BİLİM DALI

HAZIRLAYAN
Erol Başaran BURAL

TEZ DANIŞMANI
Doç.Dr. Serhat Ahmet ERKMEN

ANKARA-2021
“Her Hakkı Saklıdır”

Erol Başaran BURAL tarafından hazırlanan “Terörizmle Mücadelede Sosyal Medya İstihbaratının Önemi: PKK Terör Örgütünün Twitter’deki Görünürlüğü Üzerine Sosyal Ağ Analizi” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü Uluslararası Güvenlik ve Terörizm Ana Bilim Dalı Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Serhat Ahmet ERKMEN

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü

Uluslararası Güvenlik ve Terörizm Ana Bilim Dalı

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Nihat Ali ÖZCAN

TOBB ETÜ

Siyaset Bilimi ve Uluslararası İlişkiler Ana Bilim Dalı

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye: J.Yb.Dr. Bürke Uğur BAŞARANEL

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 27/04/2021

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Doç.Dr.Tekin AVANER

Enstitü Müdürü

ETİK BEYAN

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü Tez Yazım Kurallarına 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 çalışmamın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Erol Başaran BURAL

27/04/2021

T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

TERÖRİZMLE MÜCADELEDE SOSYAL MEDYA İSTİHBARATININ ÖNEMİ: PKK TERÖR
ÖRGÜTÜNÜN TWİTTER'DAKİ GÖRÜNÜRLÜĞÜ ÜZERİNE SOSYAL AĞ ANALİZİ

(Yüksek Lisans Tezi)

Erol Başaran BURAL

Nisan 2021

ÖZET

Bu tezin amacı, sosyal medyadan elde edilecek istihbaratın terörizmle mücadelede nasıl kullanılabileceğini araştırmaktır. Tezde cevabı aranan temel araştırma problemi; “Sosyal medya üzerinden verilerin toplanması, toplanan verilerin sosyal ağ analizi yöntemi ile analizi şeklinde yürütülecek sosyal medya istihbaratı çalışmaları, PKK terör örgütüyle mücadelede hangi katkıları sağlayabilir?” şeklinde ortaya konulmuştur.

Tez üç bölümden oluşmaktadır. Birinci bölümde; terörizm ve terörizmle mücadele yöntemleri ele alınmıştır. Terörizmle mücadele yöntemleri olarak istihbarat ve istihbaratın terörizmle mücadeledeki yeri ve önemi konusundaki kavramsal, kuramsal tartışmalara bu bölümde yer verilmektedir.

Tezin ikinci bölümünde sosyal medya kavramı genel olarak incelenmiş, terör örgütlerinin sosyal medya kullanımlarına ilişkin bilgilere yer verilmiştir. Sosyal medyadan elde edilecek bilgilerin istihbarata dönüştürülmesi ve sosyal medya istihbaratı konusu bu bölümde yer almaktadır. Sosyal medya istihbaratının terörizmle mücadelede nasıl kullanılabileceğine yönelik örnek olaylar bu bölümde analiz edilmektedir.

Tezin üçüncü bölümünde, sosyal medyada oluşan sosyal ağlar ve buna bağlı olarak sosyal ağ teorisi tartışılmaktadır. Araştırmanın yöntem ve uygulamasına bu bölümde yer verilmiştir. Sosyal ağların incelenmesi neticesinde terör örgütleri hakkında istihbarat elde edilebileceğinden yola çıkılarak bu ağların analiz edilmesinin gerekliliği bu bölümde ele alınmaktadır. Çalışmanın uygulama bölümünde, PKK terör örgütü sempatizanlarına ait Twitter verileri sosyal ağlar çerçevesinde analiz edilmektedir.

Sonuç kısmında ise elde edilen sonuçların terörizmle mücadelede nasıl hayata geçirilebileceğine ilişkin çıkarımlarda bulunulmuştur. Elde edilen bulgular bu bölümde değerlendirilmiş, tezin varsayımlarına ilişkin sorulara cevaplar aranmıştır. Bu bölümde ayrıca konuyla ilgili olarak gelecekte araştırılması önerilen konulara da yer verilmiştir.

Bilim Kodu : 114111

Anahtar Kelimeler : Terörizm, Terörizmle Mücadele, İstihbarat, Sosyal Medya, Sosyal Ağ Analizi, Sosyal Medya İstihbaratı.

Sayfa Adedi : 171

Tez Danışmanı : Doç.Dr.Serhat Ahmet ERKMEN

T.R.
MINISTRY OF INTERIOR
GENDARMERIE AND COAST GUARD ACADEMY
SECURITY SCIENCES INSTITUTE

THE IMPORTANCE OF SOCIAL MEDIA INTELLIGENCE IN COMBATING TERRORISM: SOCIAL
NETWORK ANALYSIS ON THE VISIBILITY OF THE PKK TERRORIST ORGANIZATION IN
TWITTER

(M.Sc. Thesis)

Erol Başaran BURAL

Nisan 2021

ABSTRACT

The aim of this thesis is to explore how the intelligence gained by analysing social media can be used in the combatting terrorism. The main research problem is; “how data gathering through social media and social media intelligence by processing social network analysis of these obtained data can contribute to counter terrorism efforts against PKK terrorist organization?” The focus of the study will be on collecting data in social media and analyzing the collected data with the method of social network analysis in the terms of Social Media Intelligence (SOCMINT).

The thesis consists of three parts. In the first part; terrorism and combatting terrorism methods are discussed. This part of the thesis includes the conceptual and theoretical debates about the importance of intelligence in combatting terrorism.

In the second part of the study, the concept of social media is examined in general terms, and information on the use of social media by terrorist organizations is given. The issue of converting information obtained from social media into intelligence and social media intelligence is included in this part of the thesis. Case studies on how social media intelligence can be used in combatting terrorism are analyzed in this part.

In the third part of the thesis, social networks occurring in social media and social network theory are discussed. The methodology and the application of the research are studied in this part. The necessity of analyzing social networks based on the fact that intelligence about terrorist organizations can be obtained is discussed in this section. In the application part of the study, twitter data of PKK terrorist organization sympathizers are analyzed within the framework of social networks.

In the conclusion part, how the obtained results can be implemented in the fight against terrorism is discussed. The findings of the social network analysis application on PKK terrorist organization sympathizers have been evaluated in this section, and answers have been sought regarding the assumptions of the thesis. This section also includes topics that are suggested to be researched in the future.

Science Code : 114111

Keywords : Terrorism, Combatting Terrorism, Intelligence, Social Media, Social Network Analysis, Social Media Intelligence.

Page Number : 171

Supervisor : Assoc.Prof. Serhat Ahmet ERKMEN, Ph.D.

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren, kıymetli tecrübelerinden faydalandığım; yüksek lisans programına başlamam için beni teşvik eden Doç.Dr. Nihat Ali ÖZCAN'a, tez danışmanım Doç.Dr. Serhat Ahmet ERKMEN'e ve tüm Jandarma ve Sahil Güvenlik Akademisi çalışanlarına teşekkür ederim. Bu süreçte, manevi desteklerini esirgemeyen çok değerli aileme de teşekkürü bir borç bilirim.



İÇİNDEKİLER

ÖZET.....	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ.....	ix
ŞEKİLLERİN LİSTESİ.....	x
SİMGELER VE KISALTMALAR	xii
GİRİŞ.....	1

BİRİNCİ BÖLÜM

TERÖRİZMLE MÜCADELEDE İSTİHBARATIN YERİ VE ÖNEMİ

1.1. Kavramsal Çerçeve ve Terörizm ve Terörizmle Mücadele.....	13
1.1.1. Terörizm Kavramı	13
1.1.2. Terörizmle Mücadele Kavramı.....	15
1.2. Terörizmle Mücadele Yöntem ve Araçları	20
1.3. Terörizmle Mücadele Aracı Olarak İstihbarat	23
1.4. Terörizmle Mücadele Çerçevesinde İstihbarat Teorileri	28
1.5. Terörizmle Mücadele Aracı Olarak İstihbaratın Amacı ve Önemi.....	31
1.5.1. Terörizmle mücadelede istihbaratın amacı.....	31
1.5.2. Terörizmle mücadelede istihbaratın önemi	33

İKİNCİ BÖLÜM

SOSYAL MEDYA İSTİHBARATI

2.1. Sosyal Medya.....	43
2.2. Terör Örgütlerinin Sosyal Medya Kullanımı.....	49
2.2.1. Terör Örgütlerinin İnternet Kullanımı	49
2.2.2. Terör Örgütlerinin Sosyal Medya Kullanımı	50
2.2.3. Terör Örgütlerinin Sosyal Medya Kullanımına Örnekler	53
2.3. Sosyal Medya İstihbaratı	59
2.3.1. Sosyal Medya İstihbaratının Yeri	59
2.3.2. Sosyal Medya İstihbaratı	60
2.3.3. Sosyal Medya İstihbarat Süreci	65
2.3.3.1. Yönlendirme ve planlama	66
2.3.3.2. Sosyal medyadan verilerin toplanması	67
2.3.3.3. Sosyal medya verilerinin analizi.....	70
2.3.3.4. Sosyal medya istihbaratının teyit edilmesi	77

2.3.3.5. Sosyal medya istihbaratının dağıtımı	79
2.3.4. Sosyal Medya İstihbaratının Avantajları ve Dezavantajları	79
2.3.5. Sosyal Medya İstihbaratının Terörizmle Mücadelede Kullanımına İlişkin Örnekler	81

ÜÇÜNCÜ BÖLÜM

PKK TERÖR ÖRGÜTÜNÜN TWITTER'DAKİ GÖRÜNÜRLÜĞÜ ÜZERİNE SOSYAL AĞ ANALİZİ

3.1. Ağ Kavramı.....	85
3.2. Sosyal Ağ Analizinde Ölçütler	91
3.3. Sosyal Ağ Analizi	93
3.4. Terörizmle Mücadelede Sosyal Medya İstihbaratı Analiz Yöntemi Olarak Sosyal Ağ Analizi.....	97
3.5. PKK Terör Örgütü Sempatizanlarının Sosyal Ağ Analizi.....	100
3.5.1. Araştırmanın Yöntemi	100
3.5.2. Yöntem Uygulaması Birinci Aşama: PKK Terör Örgütü Sempatizanlarına Ait Twitter Hesaplarının Tespit Edilmesi	104
3.5.3. Yöntem Uygulaması İkinci Aşama: Çekirdek Twitter Hesapların Takip Ettiği Hesapların Tespiti, Ayıklanması ve Verilerin Toplanması.....	107
3.5.4. Yöntem Uygulaması Üçüncü Aşama: Toplanan Verilerin NodeXL Pro Uygulaması ile Analiz Edilmesi	108
3.5.5. PKK Terör Örgütü Sempatizanları Sosyal Ağ Analizi Uygulamasının Sosyal Medya İstihbaratı Kapsamında Değerlendirilmesi	122
SONUÇ VE DEĞERLENDİRME.....	127
KAYNAKÇA.....	137
EKLER	154
ÖZGEÇMİŞ.....	155

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 2.1. SOMİS Doğrulama ve Güvenilirlik Matrisi.....	78
Çizelge 3.1. Örnek Ağ Matrisi.....	90
Çizelge 3.2. Gruplar Arasındaki Bağlantılar Tablosu.....	116
Çizelge 3.3. Ağda En Çok Kullanılan Kelimeler.....	119



ŞEKİLLERİN LİSTESİ

Şekil		Sayfa
Şekil 1.1.	Terörizmle Mücadelenin Unsurları.....	17
Şekil 1.2.	İstihbarat Süreci.....	27
Şekil 1.3.	Terörizmle Mücadelede İstihbarat Süreci.....	38
Şekil 2.1.	Sosyal Medyanın Tarihçesi.....	46
Şekil 2.2.	Sosyal Medya Kullanıcı Miktarları.....	48
Şekil 2.3.	Suriye Elektronik Ordusu Tarafından Yayınlanan Tweet.....	55
Şekil 2.4.	El Şebab Tarafından Yayınlanan Tweetler.....	56
Şekil 2.5.	“The Lions of Rojava” Facebook Sayfası Görüntüsü.....	58
Şekil 2.6.	Askeri Personel Tarafından Paylaşılan Özçekim Fotoğrafı.....	64
Şekil 2.7.	Konum Özelliği Açık Olarak Yapılan Instagram Paylaşımı.....	64
Şekil 2.8.	Instagram Paylaşımının Coğrafi Konumunu Gösteren Harita.....	65
Şekil 2.9.	SOMİS Süreci.....	66
Şekil 2.10.	Örnek Kelime Bulutu.....	75
Şekil 2.11.	Bali Saldırısını Gerçekleştiren Teröristlere Ait Ağ.....	83
Şekil 3.1.	Königsberg Köprüleri.....	85
Şekil 3.2.	İstanbul Raylı Sistemler Ağ Haritası.....	87
Şekil 3.3.	Ağ Yolu.....	88
Şekil 3.4.	Ağda Kenar ve Göbekler.....	88
Şekil 3.5.	Yedinci Sınıf Öğrencileri İlişki Sosyogramı.....	89
Şekil 3.6.	Yönlü Ağ Örneği.....	90
Şekil 3.7.	Yönsüz Ağ Örneği.....	90
Şekil 3.8.	Tartılı Ağlar.....	91

Şekil 3.9.	Yıldız Şeklindeki Ağlarda Merkezilik.....	92
Şekil 3.10.	Döngü Şeklindeki Ağlarda Merkezilik.....	92
Şekil 3.11.	NodeXL Pro Arayüzü	101
Şekil 3.12.	Gephi 0.8 Alpha Programı Arayüzü.....	103
Şekil 3.13.	TweetBeaver Uygulamasına Ait Arayüzü.....	103
Şekil 3.14.	NodeXL ile Twitter Kullanıcı Ağına Ait Verilerin Toplanması....	108
Şekil 3.15.	NodeXL Pro Tarafından Hesaplanan Ölçütler Tablosu.....	108
Şekil 3.16.	İç Derece Merkezliği Derecesi En Yüksek Kullanıcı.....	111
Şekil 3.17.	Dış Derece Merkezliği Derecesi En Yüksek Kullanıcı.....	112
Şekil 3.18.	Arasındalık Merkezliği Derecesi En Yüksek Kullanıcı.....	113
Şekil 3.19.	NodeXL Pro Programı ile Hesaplanan Grup Bilgileri Tablosu.....	114
Şekil 3.20.	PKK Terör Örgütü Sempatizanlarının Twitter Ağına Ait Gruplar.	114
Şekil 3.21.	1 Numaralı Grup Kanaat Önderinin Diğer Gruplara Erişimi.....	115
Şekil 3.22.	PKK Terör Örgütü Sempatizanları Twitter Ağının Gephi ile Görselleştirilmesi.....	117
Şekil 3.23.	NodeXL Pro ile Kelime Sayılarının Hesaplanması.....	117
Şekil 3.24.	PKK Terör Örgütü Sempatizanlarının Gündemi Kelime Bulutu...	120

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
ABD	Amerika Birleşik Devletleri
AKİS	Açık Kaynak İstihbaratı
API	<i>Application Programming Interface</i> , Uygulama Programlama Arayüzleri
BAK	Bundeskriminalamt, Federal Almanya Kriminal Polis Teşkilatı
CESID	<i>Centro Superior de Información de la Defensa</i> , Askeri İstihbarat Örgütü
DEAŞ	<i>ed Devlet’ul İslamiy el-İrak veş-Şam</i> , Irak ve Şam İslam Devleti
ETA	<i>Euskadi Ta Askatasuna</i> , Bask Anavatanı ve Özgürlük
FAC	Federal Almanya Cumhuriyeti
IRA	<i>Irish Republican Army</i> , İrlanda Cumhuriyet Ordusu
KDP	Kürdistan Demokratik Partisi
KKTC	Kuzey Kıbrıs Türk Cumhuriyeti
LTTE	<i>Liberation Tigers of Tamil Eelam</i> , Tamil Kaplanları
NLP	<i>Natural Language Processing</i> , Doğal dil işleme yöntemleri
NodeXL	<i>Network Overview Discovery and Exploration add-in for Excel</i> , Ağların Keşfi ve Araştırması için Excel Eklentisi
PKK	<i>Partiya Karkerên Kurdistanê</i> , Kürdistan İşçi Partisi
PYD	<i>Partiya Yekîtiya Demokrat</i> , Demokratik Birlik Partisi
RAF	<i>Red Army Faction</i> , Kızıl Ordu Fraksiyonu
SAA	Sosyal Ağ Analizi
SOMİS	Sosyal Medya İstihbaratı

GİRİŞ

Modern terörizm, devletlerin egemenliğini yüzyıllardır tehdit etmekte, insanların hayatlarına son vermektedir. Bir salgın hastalık gibi tüm dünyaya yayılan, etkin olduğu ülkelerde büyük boyutlarda ekonomik zararlara neden olan terörizm, devletleri ve toplumları yıpratmaktadır.

Teknolojinin ilerlemesine paralel olarak, değişen şartlara ayak uyduran terörizm, zaman içerisinde sürekli yeni taktik ve teknikler üretmiş, teknoloji sayesinde elde ettiği yeni imkân ve kabiliyetlerle etki alanını genişletmiştir. Teknolojide yaşanan gelişmeleri kendi lehlerinde kullanan terör örgütleri; daha geniş bir coğrafyada diğer terör örgütleriyle iş birliği imkânı yakalamış, terör eylemlerini çeşitlendirmiştir.

Toplumların iletişim imkânlarını geliştirmek üzere telgrafın, ardından telefonun icadıyla başlayan iletişim teknolojisindeki gelişmeler, radyo ve televizyon yayınlarıyla bir üst seviyeye taşınmıştır. İnternetin yaygın kullanımıyla birlikte ise bireyler ve toplumlar arası iletişim çok hızlı ve aynı zamanda oldukça da ucuz bir hale gelmiştir. Terör örgütleri de bu imkândan faydalanarak hem kendi aralarındaki iletişim kabiliyetini artırmış hem de kitle iletişim araçlarını kullanarak yürüttükleri propaganda faaliyetlerini genişletmişlerdir. Terör örgütlerinin teknolojik imkânlardan kaynaklanan kapasite artışı, hem terör örgütlerinin kullandığı eylem tekniklerini değiştirerek terörizmin etkilerini daha da artırmış hem de terör örgütlerinin iletişim ve propaganda yeteneklerini geliştirmiştir.

Terörizm, bir yandan silahlı eylemlerle gündemde kalırken diğer yandan gelişen teknoloji alt yapısını kullanarak yürüttüğü bilgiye dayalı faaliyetlerle; korku, stres, kargaşa ortamı yaratarak sosyal düzende değişiklik meydana getirmeye çalışmıştır. Burada belirtilen silahlı eylemler geleneksel silahlı saldırı çeşitlerini içerirken, bilgiye dayalı faaliyetler ise daha çok internet ortamındaki (siber alandaki) eylemleri içermektedir (Minchev, 2015: 1). Daha önceki dönemlerinde kırsalda ve şehirlerde faaliyet gösteren örgütler günümüzde kendilerine üçüncü bir barınma alanı açmış ve siber alandaki yerini almıştır.

Weimann (2004) terör örgütlerinin siber alandaki faaliyetlerini ortaya koyduğu, “Modern Terörizm İnterneti Nasıl Kullanıyor?” isimli çalışmasında, terör örgütlerinin interneti, kolay erişilebilir olması; büyük bir kitleye hitap etmesi; bilgiyi hızlı aktarabilmesi; kullanımıyla ilgili yasal düzenlemelerin oldukça az olması ya da olmaması; kullanıcıya gizlenme imkânı sağlaması; maliyetinin diğer kitle iletişim araçlarına göre daha

az olması; yazı, grafik, ses, video gibi görsel ve işitsel ürünleri bir arada barındırabilmesi nedeniyle tercih ettiklerini ifade etmektedir. Terör örgütleri tarafından hazırlanan internet siteleri, mevcut ve potansiyel sempatizanları, uluslararası kamuoyunu ve karşı tarafta gördükleri kamuoylarını doğrudan hedef alabilmektedir. Terör örgütleri interneti psikolojik harekât faaliyetleri yürütmek, propaganda yapmak, istihbarat toplamak, finans sağlamak, eleman temin etmek, bilgi paylaşmak, plan yapmak ve koordinasyon amacıyla kullanmaktadır (ss.1-12).

1990'lı yıllardan sonra giderek yaygınlaşan internet kullanımı, internet sitelerinin sayısının da artmasıyla daha fazla insan tarafından kullanılır hale gelmiştir. 2000'li yılların başından itibaren sosyal medyanın yoğun olarak kullanılmasıyla birlikte internet, gelişmiş toplumların vazgeçilmezi haline gelmiştir. Günümüzde neredeyse bireylerin hayatlarının merkezine yerleşen ve toplumları birbirine bağlayan internet, hızını oldukça artırmış, fonksiyon alanlarını genişletmiştir. İnternetin toplum hayatını etkileyen en büyük özelliği birbirlerini dahi görmemiş insanların birbirleriyle etkileşime girmesini sağlayan sosyal medyanın ortaya çıkması olmuştur.

Sosyal medya; fikirlerin, bakış açılarının ve bir takım içeriklerin paylaşılabilceği çevrimiçi araçlar olarak tanımlanmaktadır (Nair, 2011: 45). Günümüzde insanların günlük hayatlarında sıklıkla kullandıkları sosyal medya araçları ile bireyler, duygu ve düşüncelerini oldukça hızlı bir şekilde büyük bir hedef kitleyle paylaşabilmektedir. Bireylerin sosyal medya araçlarıyla yaptıkları paylaşımlar metinlerden oluşabildiği gibi resim, video gibi görsellerden de oluşabilmektedir.

Tıpkı internette olduğu gibi internet alt yapısından doğan sosyal medya araçları da sadece iyi niyetli bireyler, kurumlar, örgütlenmeler tarafından değil aynı zamanda organize suç örgütleri ya da terör örgütleri gibi toplum için zararlı örgütlenmeler tarafından da kullanılmaktadır.

Bununla birlikte terörizmle mücadele eden devletler de teknolojinin tüm imkânlarını kullanılmaktadırlar. Terörizmle mücadele yöntem ve araçlarında da teknolojinin gelişimine paralel olarak değişimler yaşanmış, mücadele gün geçtikçe daha teknoloji yoğun bir hal almış, terör örgütlerinin takibi kolaylaşmış, silah-teçhizat-araç ve gereçler daha etkili bir seviyeye ulaşmış, terör eylemlerinin önlenmesine yönelik daha etkin tedbirler alınmaya başlamıştır.

Bu araştırmanın çıkış noktası da hem terör örgütlerinin hem de terörizmle mücadele eden kurumların teknolojiyi kullanımından hareketle; terör örgütlerinin sosyal medyadaki varlığı, bu varlığa ilişkin verilerin toplanması, toplanan verilerin sosyal ağ analiz yöntemiyle analizi neticesinde istihbarata dönüştürülmesi, örgütlerin ağ yapılarının ortaya çıkarılması, terörizmle mücadele çerçevesinde sosyal medyada tespit edilen terör ağlarının hedef alınması ve sonuçta terör örgütü faaliyetlerinin sınırlandırılması şeklinde hazırlanan bir araştırma desenine dayanmaktadır.

Günümüzde terörizm fiziksel alandan (coğrafi bölgelerden) sanal alana (siber uzay), terörizm tehditleri ise insansız hava araçları kullanımından, Twitter, Youtube ve Facebook gibi sosyal medya araçlarının kullanımına kadar geniş bir alana yayılmıştır. Örneğin, Afrika’da faaliyet gösteren terör örgütlerinden El Şebab, internet üzerinde çevrimiçi (online) olarak en çok varlık gösteren terör örgütüdür. Twitter’ı etkin biçimde kullanan El Şebab, Twitter’dan terör eylemlerini düzenli olarak yayımlamakta, resmi söylemlere cevap verecek şekilde gerçek zamanlı paylaşımlar yapmaktadır (Falode, 2018: 153-160). Kuruluşu daha eskilere dayanmakla birlikte 2014 yılından itibaren terör eylemlerini artıran DEAŞ (*ed Devlet’ul İslamiy el-Irak veş-Şam*) terör örgütünün sosyal medyayı kullanma yeteneği ve kapasitesi de konuya ilgi duyanların hafızasındaki yerini korumaktadır.

Bu kapsamda; terör örgütlerinin sosyal medya kullanımıyla ilgili olarak yapılan “Yeni Medya Ortamında Terörizmle Mücadele (Combating Terrorism in the New Media Environment)” isimli çalışmada, yeni teknolojilerin kullanımının, terör örgütlerinin; propaganda, eleman temini, eğitim ve komuta kontrol kapasitelerini artırdığı sonucuna varılmaktadır (Amble, 2012: 342).

Sosyal medyanın terör örgütlerince neden tercih edildiğini inceleyen “Gelişmekte Olan Ülkelerde Çevrimiçi Sosyal Ağlar ve Terörizm 2.0 (Online Social Networks and Terrorism 2.0 in Developing Countries)” isimli çalışmada, tüm sosyal medya araçları “Çevrimiçi Sosyal Ağlar (Online Social Networks)” şeklinde tanımlanmıştır. Araştırmada çevrimiçi sosyal ağların kolay ulaşılabilir olması; devletler tarafından yeterince kontrol edilememesi; dünya genelinde büyük bir hedef kitleye hitap edebilmesi; sahte hesaplar üzerinden kimliği saklama imkânı sunması; bilginin süratle paylaşımına imkân vermesi; maliyetinin oldukça düşük olması; metin, grafik, ses, video gibi çoklu medya olanaklarını bir arada barındırması nedeniyle terör örgütlerince tercih edildiği belirtilmektedir. Ayrıca çevrimiçi sosyal ağların terör örgütleri tarafından bilgi alışverişi; eleman temini ve eğitim;

eylem planlama, finans temini, siber saldırı düzenleme ve propaganda yapma maksadıyla kullanıldığı ifade edilmektedir (Ishengoma, 2014: 4-5).

Terör örgütleri değişen teknolojiye paralel olarak kendilerini sürekli geliştirip, internet ve sosyal medyada giderek artan şekilde varlıklarını sürdürürlerken, terörizmle mücadele eden devletler de bu gelişmelere ayak uydurarak terörizmle mücadele politikalarına yön vermektedirler. Terörizmle mücadele yöntemleri devletlerin yönetim şekline göre farklılık gösterebilmekte, devletler tarafından hangi yöntem ve araçların kullanılması gerektiği ise halen tartışılmaya devam etmektedir.

Terörizmle mücadeleye ilişkin tartışmalardan birisi, devletlerin; terör örgütlerini cezalandıracak ve böylece gelecekte meydana gelebilecek terör olaylarını caydırarak önleyecek, sert politikaları mı ya da terörizmin kök nedenlerine odaklanarak, terörizmin bir araç olarak kullanılmasını teşvik eden hususların azaltılmasına yönelik yumuşak politikaları mı geliştirmesi gerektiği yönündedir. Örneğin bazı araştırmacılar (O'Brien, 1985; Carr, 1996; Bremer, 1992) teröristlere misilleme yaparak ya da en azından teröristlerle pazarlık yapmayarak devletlerin itibar kazanmaları gerektiğini iddia etmektedir. Bu görüş, devletlerin terörizme karşı saldırgan bir tutum izlediklerinde sert bir görünüme kavuştuklarını ve gelecekteki terör olaylarını önlediklerini; sert tedbirler kullanmayan ve teröristlerin taleplerine boyun eğenlerin ise yumuşak davranan ve şiddeti teşvik eden bir tavır çizdiklerini ifade etmektedir (Miller, 2007: 331-332).

Bu düşünceler çerçevesinde, devletlerin terörizmle mücadele yöntemleri hiçbir şey yapmama (ortaya çıkan terörizmi yok sayma), uzlaştırma, yasal reformlar yapma, kısıtlamalar getirme ve şiddet kullanma başlıkları altında beş kategoriye ayrılabilir (Miller, 2007: 335).

Tıpkı terörizmle mücadele yöntemlerinde olduğu gibi terörizmle mücadele araçları da alanyazında farklı biçimlerde tasnif edilmektedir. Örneğin Wilkinson (2006), terörizmle mücadele araçlarını; siyasal ve sosyo-ekonomik reformları içeren siyaset, diplomasi ve barış (diyalog) süreçleri, ceza adalet sistemi ve kolluk kuvvetlerinin kullanımı, askeri birliklerin terörizmle mücadelede kullanımı şeklinde tasnif etmiştir (ss.61-103). Pillar (2004), terörizmle mücadelede kullanılan araçları; diplomasi, ceza adalet sistemi, terörizmin finansmanının önlenmesi, askeri kuvvet kullanımı, istihbarat ve örtülü operasyon araçları şeklinde kategorize etmiştir (ss.73-130). Demir (2017) ise terörizmle mücadele araçlarını; ceza adalet sistemi, siyasal ve sosyo-ekonomik tedbirler, diplomasi, askeri kuvvet kullanımı ve istihbarat başlıkları altında toplamıştır (ss.131-146).

Terörizmle mücadele araçlarından istihbarat; terör örgütü yapılanmasının deşifre edilmesi, terör örgütü mensuplarının konuşlanmasının ve faaliyetlerinin ortaya çıkarılması, terör örgütünün eleman ve finans kaynaklarının kesilmesi, terör örgütü propagandasının önlenmesi için mutlak suretle gereklidir. Terör örgütlerine yönelik bu tür faaliyetlerin engellenebilmesi, terör örgütleriyle mücadele edilebilmesi için etkin bir istihbarat gereklidir.

Pollard'a (2009) göre de terörizmle mücadelede; tehdidin anlaşılması ve ortaya konulması, terör örgütlerinin kapasiteleri ve niyetleri hakkında erken ikazlar verilmesi, terör örgütü elemanlarının bulunması ve etkisiz hale getirilmesi istihbarat faaliyetlerine doğrudan bağlıdır (s.117). Terörizmle mücadelede, terörizmle mücadele araçlarından hangisi tercih edilirse edilsin, bu araçların etkin kullanımı için mutlak suretle istihbarata ihtiyaç duyulmaktadır. İstihbarat; terörizmle mücadelenin öncesinde, mücadele süresince ve mücadele sonrasında yürütülen, diğer mücadele araçlarını doğrudan ya da dolaylı olarak destekleyen en önemli araçtır.

Günümüzde terörizmle mücadele kapsamında yürütülen istihbarat gayretleri internet ve sosyal medyayı toplama kaynağı olarak kullanılmaktadır. Bireylerin taşınabilir cihazlarla internete ve sosyal medyaya kolaylıkla erişebilmeleri, sosyal medya üzerinden günlük olayları takip etmeleri, iletişimlerini sosyal medya üzerinden gerçekleştirmeleri, sosyal medyada oldukça büyük miktarlarda veri birikmesine neden olmaktadır.

Sosyal medyada oluşan büyük veri¹, göz önüne alındığında, sosyal medya araçlarının geleneksel açık kaynak araçlarından farklı bir yere sahip olduğu anlaşılmaktadır. Sosyal medyada paylaşılan verilerin büyüklüğü üzerinden hareket edilecek olursa, sosyal medya araçlarından istihbarat üretme gayretlerinin de ne kadar yerinde olduğu sonucuna ulaşabilmektedir. Bu kapsamda sosyal medya istihbaratını en yalın haliyle; sosyal medya platformlarından elde edilen istihbarat olarak tanımlamak mümkündür (Hassan ve Hijazi, 2018: 205).

¹ Büyük veri kavramı internet üzerinde üretilen büyük hacimdeki veriyi tanımlamak için kullanılmaktadır. Büyük veri; dinamik, hızla gelişen verilerden oluşan, bilgi iletişim teknolojilerinde yaşanan gelişmeler neticesinde ortaya çıkan, geleneksel veri tabanı yönetim sistemlerinin işlem kapasitesini aşan, yüksek hız ve çeşitlilikteki verileri ifade etmek için kullanılmaktadır. Büyük veri, akıllı sensörler, gökyüzü araştırmaları, cep telefonu verileri, Facebook beğenileri, Twitter'da paylaşılan tweetler gibi çeşitli yollarla bireyler tarafından üretilmekte ve üretilen bu veriler çoğu zaman istemeden ve farkında olmadan gerçekleşmektedir. Ayrıntılı bilgi için bkz.: Kılınç, O. ve Arıcı, A. (2020). Sosyal ağlarda büyük veri: Teknoloji markaları üzerine bir araştırma. *Connectist: İstanbul University Journal of Communication Sciences*, 58, 201-240. <https://doi.org/10.26650/CONNECTIST2020-0082>.

Terör örgütlerinin de; propaganda yapmak, örgüte eleman temin etmek, daha etkin bir iletişim sistemi kurmak maksadıyla sosyal medyayı kullandıkları görülmektedir (Özkaya, 2017: 49-52). Terör örgütleri ayrıca, sosyal medyayı kullanarak bireyleri kendi amaçları doğrultusunda radikalleştirmeye uğraşmakta, terör eylemlerini bu platformları kullanarak planlamaktadırlar (Thompson, 2019: 28-31).

Terör örgütlerince sosyal medyanın kullanımı, terör örgütlerinin sosyal medya paylaşımlarından verilerin toplanması, verilerin analizi sonucu sosyal medya istihbaratının üretilmesi, sosyal medyadaki terör örgütü yapılanmasının ortaya çıkarılması şeklindeki bir süreçten yola çıkılarak kurgulanan bu araştırmanın konusu; sosyal medya istihbaratının terörizmle mücadelede ne şekilde kullanılabileceğinin incelenmesidir.

Terörizm, terörizmin tarihi, terör örgütleri, terörizmin çeşitleri gibi alanlarda çok sayıda araştırma mevcuttur. Özellikle 11 Eylül 2001 terör saldırılarının ardından alanyazında üretilen araştırma sayılarında bir artış meydana gelmiştir. Bu çerçevede uzun yıllardır terörizmle mücadele eden ülkemizde de terörizm ve terörizmle mücadele alanında akademik araştırmaların sayısının arttığını söylemek mümkündür.

Ancak, terörizmle mücadele konusunda belirgin bir alanyazın yetersizliğinin söz konusu olduğu da görülmektedir. Terörizmle mücadele araçlarından istihbaratın ne şekilde kullanılabileceğini ortaya koyan araştırma sayısı diğerlerine oranla daha da azdır. Türkçe alanyazında; sosyal medya istihbaratı, sosyal medya istihbaratının terörizmle mücadelede kullanımına ilişkin teze rastlanılmamıştır. Ayrıca, PKK terör örgütünün sosyal medyadaki görünürlüğü üzerinden veri toplanmasına, toplanan verilerin sosyal ağ analizi yöntemi ile istihbarata dönüştürülmesine yönelik bir araştırma ya da akademik çalışma da bulunmamaktadır.

Bu açıdan değerlendirildiğinde, çalışma Türkçe alanyazında terörizmle mücadelede sosyal medya istihbaratının kullanılmasına yönelik ilk araştırmalardan birisi olacaktır. Çalışmanın; terör örgütlerinin sosyal medya üzerindeki varlığına ilişkin verilerin toplanması, sosyal medyadaki terör örgütü varlığının sosyal ağ analizi yöntemi ile analiz edilmesi, sosyal medyadan elde edilen istihbaratın terörizmle mücadeleye sunabileceği katkıları incelemesi açısından alanyazına önemli katkılar sağlayabileceği düşünülmektedir.

Bu tezin amacı, sosyal medyadan elde edilecek istihbaratın terörizmle mücadelede nasıl kullanılabileceğini araştırmaktır. Tezde cevabı aranan temel araştırma problemi; “Sosyal medya üzerinden verilerin toplanması, toplanan verilerin sosyal ağ analizi yöntemi

ile analizi şeklinde yürütülecek sosyal medya istihbaratı çalışmaları, PKK terör örgütüyle mücadelede hangi katkıları sağlayabilir?” şeklinde ortaya konulmuştur.

Bu problemi çözebilmek üzere temel problem sorusu, alt problem cümlelerine ayrılmıştır. Araştırmanın alt problemleri şu şekilde sıralanmıştır:

- Terörizmle mücadele istihbaratı kapsamında sosyal medya uygulamaları, terör örgütleri hakkında veri elde etmek maksadıyla kullanılabilecek uygun bir araç mıdır?
- Hangi özelliklerinden dolayı sosyal medya istihbarat üretmek için uygun bir araçtır?
- İstihbaratın analiz safhasında sosyal ağ analizi ne şekilde kullanılabilir?
- Sosyal ağ analizi terör örgütleri yapılanmalarının belirlenmesinde nasıl kullanılabilir?
- Terörizmle mücadelede sosyal medya istihbaratı hangi amaçlarla ve nasıl kullanılabilir?

Araştırma, terörizm ve terörizmle mücadele gibi oldukça geniş bir alanyazın içerisinde yer alan konulardan terörizmle mücadele araçlarını, bu araçlardan ise istihbarat aracını kapsamaktadır. Yine istihbarat konusu içerisinde sosyal medya istihbaratı seçilerek çalışmanın konusu daraltılmıştır.

Araştırmanın temel konusu sosyal medya istihbaratının terörizmle mücadelede ne şekilde kullanılabileceğinin incelenmesi olduğundan, konunun ayrıntılı şekilde çalışılabilmesi maksadıyla, çok sayıda terör örgütü içerisinde Türkiye’de halen aktif olduğundan PKK terör örgütü seçilmiştir. Sosyal medya uygulamalarının sayıca fazla olması, farklı amaçlar için farklı sosyal medya uygulamalarının kullanılması nedeniyle bu çalışma Twitter uygulaması ile sınırlandırılmıştır.

Twitter üzerinde çok sayıda PKK terör örgütü sempatizanı hesap bulunduğu değerlendirilmektedir. Bütün PKK sempatizanı hesapları çalışma örneklemini içerisine almak mümkün olmayacağından araştırma 50 adet Twitter hesabı ile sınırlandırılmıştır.

Çalışmanın bir diğer sınırlılığı ise paylaşımların lisanı ile ilgilidir. PKK terör örgütü sempatizanları Türkçe haricinde İngilizce, Fransızca, İspanyolca, Kürtçe gibi çok sayıda dil ve lehçede Twitter paylaşımı yapmaktadır. Bu nedenle çalışma sadece Türkçe - İngilizce paylaşım yapan Twitter hesaplarıyla ve bu dillerde yapılan Twitter paylaşımlarıyla sınırlandırılmıştır.

Tezin temel varsayımı ise; PKK terör örgütü sempatzanlarının Twitter uygulaması üzerindeki varlığının sosyal medya istihbaratı kapsamında sosyal ağ analizi yöntemiyle incelenmesi neticesinde, terör örgütünün propaganda ve haberleşme ağının ortaya çıkarılabileceği şeklindedir.

Araştırmanın diğler varsayımı ise; Twitter'dan üretilecek sosyal medya istihbaratı sayesinde PKK terör örgütü faaliyetleri hakkında güvenlik güçlerinin farkındalığının en üst seviyeye çıkarılabileceğidir.

Araştırmanın son varsayımı ise PKK terör örgütü Twitter hesaplarının teşkil ettiğı sosyal ağların takibi sayesinde örgütün geleceğre yönelik muhtemel faaliyetlerinin tahmin edilebileceğidir.

Sosyal medyanın ürettiğı bilgi miktarı devasa boyutlara eriştiğinden, bu alandan veri elde edilmesi, elde edilen verilerin analiz edilmesi ve görselleştirilmesi gibi hususlarda bilgisayar sistemlerinden faydalanmak gerekmektedir. Henüz Türkçede kabul edilen ortak bir ismi bulunmamakla beraber sosyal olguları modellemek ve analiz etmek maksadıyla “Hesaplamalı Sosyal Bilimler”² (Computational Social Science) şeklinde isimlendirebileceğimiz yöntemler kullanılmaktadır.

Günümüzde insanlar ağlar içerisinde yaşamaktadırlar. İnsanlar her gün elektronik postalarını kontrol etmekte, mobil telefonlarıyla farklı konumlardan görüşmeler yapmakta, kredi kartlarıyla alışveriş yapmakta, çevrimiçi sosyal ağlar üzerinden arkadaşlarıyla görüşmektedir. Tüm bu işlemler hem bireysel hem de grup davranışları ortaya koyabilen takip edilebilir izler bırakmaktadır. Yine bu işlemler oldukça büyük boyutlarda veri oluşumuna neden olmaktadır. Bunun sonucunda ise benzeri görülmemiş bir büyüklük, derinlik ve ölçekteki bu veriyi toplama ve analiz etme kapasitesinden yararlanan hesaplamalı sosyal bilimler ortaya çıkmaktadır (Lazer vd, 2009: 721-722).

Hesaplamalı sosyal bilimler, sosyal medya tarafından üretilen büyük veri üzerinde çalışmanın bir alt kategorisidir. Hesaplamalı sosyal bilimler denildiğinde; terabayt veya petabayt ile ölçülen karmaşık veri kümelerini kullanan; bu verilerden modeller ve anlamlar üretmek için hesaplama veya algoritmik çözümleri kullanan; kamuoyu görüşlerinin incelenmesinden halk sağlığına, siyasi olayların incelenmesinden toplumsal hareketlere

² Henüz Türkçe alanyazında yaygın kullanılan bir isim verilmemiştir. Bu nedenle “Computational Social Science” için Programlamalı Sosyal Bilimler, Bilişimsel Sosyal Bilimler, Bilgisaymsal Sosyal Bilimler gibi ifadelerle rastlanılması mümkündür.

kadar çeşitli alanlarda sosyal olaylara uygulanabilen yöntemler anlaşılmaktadır (Shah vd., 2015: 7).

Bu araştırmada, hesaplamalı sosyal bilimlerin kapsama alanı içerisinde bir analiz yöntemi olarak değerlendirilen ve sayısal (digital) veya sanal (virtual) ortamlarda oluşturulan ağların analizi için kullanılan “Sosyal Ağ Analizi (Social Network Analysis)” yöntemi kullanılacaktır. Çalışmada sosyal ağ analizi, sosyal medya istihbaratının işlem basamaklarından birisi olan analiz basamağı olarak kabul edilmiştir.

Araştırmanın konusu, varsayımı ve temel problem cümlesi dikkate alınarak, çalışmanın yöntemi üç temel aşama üzerine inşa edilmiştir. Bunlardan birincisi Twitter sosyal medya uygulamasında faaliyet gösteren PKK terör örgütü sempatizanı hesapların tespiti, ikincisi tespit edilen hesaplarla ilgili verilerin toplanması, üçüncüsü ise toplanan verilerin sosyal ağ analizi yöntemiyle analiz edilmesidir.

Sosyal ağlardan Twitter uygulamasını temel alan bu araştırmada, Twitter’den PKK terör örgütü sempatizanlarına ait verilerin toplanması, sosyal ağ analizi ölçütlerinin hesaplanması ve analizi maksadıyla NodeXL Pro isimli uygulama kullanılmıştır. PKK sempatizanı hesaplara ait üst verilerin (metadata)³ elde edilmesi için çevrimiçi bir uygulama olan “Tweet Beaver” kullanılmıştır. Toplanan verilerin ayıklanması geleneksel yöntemlerle ve manuel olarak gerçekleştirilmiştir. Elde edilen verilerin görselleştirilmesi maksadıyla ise NodeXL Pro ve Gephi uygulamaları kullanılmıştır.

Yöntemin birinci aşaması; Twitter sosyal medya uygulamasında paylaşım yapan PKK terör örgütü sempatizanlarına ait hesapların tespiti aşamasıdır. Bu aşamada PKK terör örgütü sempatizanlarına ait Twitter hesaplarının tespiti için “Kartopu Örnekleme” yöntemi kullanılmıştır. Kartopu örnekleme tekniği, evreni oluşturan birimlere erişmenin zor olduğu veya evren hakkındaki bilgilerin eksik olduğu durumlarda kullanılmaktadır. Bu teknikte, veri elde edilebilecek kişilere odaklanılmakta ve araştırma evrenine bu kişileri takip ederek ulaşılmaktadır (Baltacı, 2018: 253).

Araştırmanın evrenini oluşturan “PKK terör örgütü sempatizanı Twitter hesaplarının” tamamını tez kapsamında inceleyebilmek mümkün görünmemektedir. Bu

³ Metadata; bir kaynağın öğelerini tanımlayan veridir. Bu nedenle bibliyografik veri olabildiği gibi içerik, kullanım koşulları, kapsam ve teknik ya da erişim özelliklerine ilişkin diğer tanımlamayı da içerebilmektedir. Metadata; veri hakkında bilgidir ve bu nedenle bir eserin yazarı, oluşturulduğu tarih, ilişkili çalışmalara bağlantılar vb. temel bilgileri sağlamaktadır. Bu açıdan yaklaşıldığında bir kütüphanedeki kart katalog veya bir veri tabanındaki bibliyografik verileri de metadata olarak isimlendirmek olanaklıdır. Ayrıntılı bilgi için bkz: Küçük, M.E. ve Al, U. (2001). *Metadata Kavramı*. Bilgi Dünyası, 2(2), ss.169-187. doi:10.15612/BD.2001.470.

maksatla “araştırmanın örneklemini oluşturmak maksadıyla” incelenecek Twitter hesap sayısı 50 ile sınırlandırılmıştır. İncelenecek 50 adet Twitter hesabını tespit edebilmek maksadıyla ilk etapta #SayinÖcalan, #PKK43yasında, #PKKisNotTerrorist, #BijiSerokApo, #PkkHalktırHalkBurada, #DelistPKK, #GlobalFreedom4OcalanDay, #YpsParastinaGele ismiyle açılan güncel etiketler (hashtag) altında paylaşım yapan hesaplar incelenmiştir. Bu hesaplar içerisinde en çok paylaşım yapanlar öncelikli olarak örnekleme dâhil edilmiştir.

Örnekleme dâhil edilen hesapların PKK terör örgütü sempatzanı olup olmadığını anlamak için bazı kriterler belirlenmiş, bu kriterlere uygun görülen Twitter hesapları araştırma kapsamına dâhil edilmiştir. Belirlenen kriterlerden birincisi Twitter hesabı profil ve kapak fotoğraflarının PKK simge ve sembollerini içermesidir. İkinci kriter ise hesap içeriklerinde PKK terör örgütünü ya da terör örgütü liderini destekleyen paylaşımların bulunmasıdır. Yöntemin belki de en zor ve en zaman alıcı bölümü PKK sempatzanı Twitter hesaplarının ayıklanması ve tespitidir denilebilir.

Etik açıdan değerlendirildiğinde ise her ne kadar PKK terör örgütü sempatzanı hesaplar üzerinde bir araştırma yürütülse de elde edilen Twitter kullanıcı hesap isimlerine çalışmada yer verilmeyecektir. Bu isimler veri olarak depolanmış olsa da çalışma sayfalarında yer almayacaktır.

Yöntemin ikinci aşaması; tespit edilen Twitter hesaplarından verilerin toplanması aşamasıdır. PKK sempatzanı hesapların tespit edilmesinin ardından yöntemin ikinci aşamasında, tespit edilen Twitter hesaplarının paylaşımları toplanmıştır. Twitter üzerinden yapılan paylaşımların toplanması maksadıyla NodeXL Pro uygulaması kullanılmıştır.

Yöntemin üçüncü aşaması; toplanan verilerin analiz edilmesi aşamasıdır. Bu aşamada, PKK terör örgütü sempatzanı Twitter hesaplarına ait veriler NodeXL Pro uygulaması ile analiz edilmiş; elde edilen verilerin görselleştirilmesi hem NodeXL Pro hem de Gephi 0.8 Alpha yazılımı ile gerçekleştirilmiştir.

Tez üç bölümden oluşmaktadır. Birinci bölümde; terörizm ve terörizmle mücadele yöntemleri ele alınmıştır. Terörizmle mücadele yöntemi olarak istihbarat ve istihbaratın terörizmle mücadeledeki yeri ve önemi konusundaki kavramsal, kuramsal tartışmalara bu bölümde yer verilmektedir.

Tezin ikinci bölümünde sosyal medya kavramı incelenmiş, terör örgütlerinin sosyal medya kullanımlarına ilişkin bilgilere yer verilmiştir. Sosyal medyadan elde edilecek

bilgilerin istihbarata dönüştürülmesi ve sosyal medya istihbaratı konusu bu bölümde araştırılmıştır. Sosyal medya istihbaratının terörizmle mücadelede nasıl kullanılabileceğine yönelik örnek olaylar da bu bölümde analiz edilmektedir.

Tezin üçüncü bölümünde, sosyal medyada oluşan sosyal ağlar ve buna bağlı olarak sosyal ağ teorisi tartışılmaktadır. Araştırmanın yöntem ve uygulamasına bu bölümde yer verilmiştir. Sosyal ağların incelenmesi neticesinde örgütler hakkında istihbarat elde edilebileceğinden yola çıkılarak ağların analiz edilmesinin gerekliliği bu bölümde ele alınmaktadır. Çalışmanın uygulama bölümünde, PKK terör örgütü sempatizanlarına ait Twitter verileri sosyal ağlar kapsamında analiz edilmektedir. Elde edilen bulgular bu bölümde değerlendirilmiş, tezin varsayımlarına ilişkin sorulara cevaplar aranmıştır.

Sonuç kısmında ulaşılan sonuçlara kısaca değinilmiş, elde edilen bulguların terörizmle mücadelede nasıl hayata geçirilebileceğine ilişkin çıkarımlarda bulunulmuştur. Bu bölümde ayrıca konuyla ilgili olarak gelecekte araştırılması önerilen konulara yer verilmiştir.



BİRİNCİ BÖLÜM

TERÖRİZMLE MÜCADELEDE İSTİHBARATIN YERİ VE ÖNEMİ

1.1. Kavramsal Çerçeve ve Terörizm ve Terörizmle Mücadele

1.1.1. *Terörizm Kavramı*

Tezin birinci bölümünde amaç; terörizmle mücadelede istihbaratın yeri ve önemi konusunu incelemektir. Bu bölümde öncelikle; terörizm, terörizmle mücadele ve terörizmle mücadele araçları konuları incelenecek, ağırlıklı olarak ise terörizmle mücadelede istihbaratın yeri ve önemi konusu tartışılacaktır.

Terörizmin ne olduğu, ne anlama geldiği üzerine yapılan çok sayıda akademik çalışma mevcuttur. Bunlardan birisine göre terörizm; “Şiddet kullanma ya da şiddet tehdidi içeren normal dışı yollarla siyasal davranışları etkilemek üzere tasarlanmış sembolik bir fiil” şeklinde tanımlanmaktadır (Thornton, 1964: 73).

Terörizmin; dikkat çekmek ve korku yaratmak için şiddetin veya şiddet tehdidinin kullanılması olarak tanımlanabileceğini belirten bir diğer çalışmaya göre terörist taktikler kullanan örgütlerin genellikle küçük ve zayıf oldukları, bu nedenle de uyguladıkları şiddetin kasıtlı olarak şok edici olduğu, bu durumun insanların terör örgütlerinin gücünü abartmasına neden olduğu vurgulanmaktadır (Jenkins, 1977: 1).

Bir başka tanıma göre terörizm; “Siyasal istekleri kabul ettirmek üzere, kişileri, grupları, toplumu ve hükümeti yıldırmak için sistematik olarak öldürme, tahrip etme ya da öldürme tehdidini kullanma” (Wilkinson, 1979: 49) şeklinde tanımlanmıştır. Bu tanımda terörizmin sistematik eylemler bütünü olduğuna dikkat çekilmektedir.

Terörizm; siyasal amaçlara erişmek maksadıyla kullanılan şiddet veya şiddet kullanma tehdidi şeklinde de tanımlanmaktadır (Hoffman, 2006: 2-3). Terörizmin siyasal amaçlara erişmek maksadıyla bir araç olarak kullanıldığını vurgulayan bu tanım, şiddetin kullanılmasının yanı sıra şiddet kullanma tehdidine de kavram içerisine yer vermektedir.

250’den fazla terörizm tanımından yola çıkarak gerçekleştirilen bir çalışma sonucunda terörizm; “Bir yandan korku üreten siyasal şiddetin, bir taktiğin veya hesaplanmış bir etkinin özel biçimini ifade eden bir doktrini, diğer yandan ise yasal ve ahlaki sınırları olmayan, hesaplanmış, gösteri amaçlı, ağırlıklı olarak sivilleri ve savaşımayan kişileri hedef alan, izleyiciler ile savaşan taraflar üzerindeki propaganda ve psikolojik etkileri için gerçekleştirilen, doğrudan şiddet eylemleri” biçiminde

kavramsallaştırılmıştır (Schmid, 2011: 86). Çok sayıda terörizm tanımının ortak noktalarını ön plana çıkartarak yapılan bu tanımlamada, terörizmin hesaplanmış siyasal şiddet yönü ile kamuoyunu etkilemeyi hedefleyen özelliğine vurgu yapılmaktadır.

Terörizmin tanımına ilişkin çalışmalardan, genel kabul gören ortak bir tanım bulunmadığı açıkça görülmektedir. Terörizm kavramına ilişkin genel kabul gören bir tanımlama yapmak yerine terörizme ilişkin kavramsal çalışmalarda ön plana çıkarılan ortak özelliklerin incelenmesinin daha yerinde olacağı değerlendirilmektedir.

Terörizme ilişkin tanımlamaların incelenmesi sonucunda; Thomas Patrick Thornton (1964: 73); Richard Shultz (1978: 8); Paul Wilkinson (2000: 19); Audrey Kurth Cronin (2003: 32-33); Louise Richardson (2006: 4); Bruce Hoffman (2006: 2-3) ve Alex Peter Schmid'in (2011: 86) terörizmin; siyasal davranışları etkilemek, siyasal amaçlara ulaşmak üzere kullanılan bir yöntem olduğunu, siyasal bir karakterinin bulunduğunu vurguladıkları görülmektedir. Tanımların hemen hemen en belirgin ortak özelliği olması nedeniyle, terörizmi diğer adi şiddet eylemlerinden ayıran en önemli özelliğin, terörizmin siyasal bir karakterinin bulunduğu sonucuna varılmaktadır.

Terörizm tanımlarında ön plana çıkan ikinci önemli özellik ise şiddet ve şiddet kullanma tehdididir. Bu çerçevede, Eugene Victor Walter (1964: 248); Richard Shultz (1978: 8); Paul Wilkinson (1979: 49); Walter Laqueur (1996: 24) ve Bruce Hoffman (2006: 2-3) tarafından yapılan tanımlamalarda, terörizmin siyasal bir değişim yaratmak amacıyla şiddet veya şiddet kullanma tehdidinin kullanılması olduğu ifade edilmektedir.

Terörizm tanımları içerisinde öne çıkan bir diğer özellik ise korku olgusudur. Eugene Victor Walter (1964: 248); Brian Michael Jenkins (1977: 1); Paul Wilkinson (2000: 19) ve Alex Peter Schmid'in (2011: 86) ortaya koydukları terörizm tanımlarında, terörizmin insanları korkutmak, genele yaygın bir korku ortamı yaratmak, korku üretmek özelliklerini ön plana çıkardıkları görülmektedir.

Terörizm tanımlarında vurgulanan bir diğer özelliğin ise semboliklik olduğu görülmektedir. Çalışmalarında bu konuya yer veren Thornton (1964: 73); Paul Wilkinson (2000: 19) ve Alex Peter Schmid (2011: 86), terör örgütlerinin terör eylemlerinin yarattığı fiziksel tahribatın büyüklüğünden daha çok eylemlerin psikolojik etkilerini önemsediklerini, bu nedenle terör eylemlerinin sembolik olduğunu ifade etmektedirler.

Terörizm tanımları içerisinde yer alan diğer bir özellik ise terörizmin sistematik olarak şiddet üretmesine ilişkindir. Paul Wilkinson (1979: 49) ve Manfred Funke

(Funke'den aktaran Schmid, 2011: 113) terörizmi planlı ve sistematik olarak sürdürülen şiddet hareketleri biçiminde tanımlamaktadırlar.

Tanımlar içerisinde ön plana çıkan hususlardan bir diğeri de terörizmin yarattığı sürpriz etkisi ile ilgilidir. Roger Trinquier (2006: 15) ve Daniel R. Morris (2009: 2) terörizmin ortaya koyduğu sürpriz etkisiyle hasımlara avantaj sağlayan bir araç olarak görüldüğünü; sürprizin terörizmin ayrılmaz bir parçası olduğunu; terör eylemlerinin bilinmeyen yer ve zamanda bilinmeyen yöntemlerle gerçekleştirilmesiyle terörizmin sürpriz etkisi ürettiğini ifade etmektedirler.

Sonuç olarak terörizmin temel özelliklerinin; siyasal bir karakterinin bulunması, şiddet kullanımı veya şiddet kullanma tehdidini içermesi, toplumun geneline yayılmış bir korku ortamı yaratması, sistematik olması, sembolik hedeflere yönelmesi, öngörülemez olması ve sürpriz etkisi yaratması olduğu değerlendirilmektedir.

Terörizmle ilgili alanyazının incelenmesi neticesinde bu çalışmada kullanılacak terörizm tanımı; “belirlenmiş siyasal hedeflere ulaşmak ve/veya bir takım siyasal kazanımlar elde etmek, yarattığı sürpriz etkisi sonucunda toplumda derin bir korku ortamı yaratmak, bir konuya dikkat çekmek maksadıyla planlanmış şiddet eylemlerinin, rastgele ve sembolik hedeflere yönelik olarak sistematik biçimde uygulanması ve/veya şiddet kullanımının bir tehdit unsuru olarak kullanılması” olarak belirlenmiştir.

1.1.2. Terörizmle Mücadele Kavramı

Terörizmin kavramsallaştırılmasının ardından, terörizmle mücadeleye ilişkin tanımlama ve sınıflandırma çalışmaları incelenecektir. Terörizmi ortaya çıkaran nedenlerin vakadan vakaya değişiklik göstermesi, terörizmle başa çıkabilmek üzere hemen hemen her devletin farklı mücadele yöntemlerini tercih etmesi sebebiyle, tıpkı terörizmde olduğu gibi terörizmle mücadelede de kavramsal çerçevenin farklı bakış açılarına göre şekillendiği görülmektedir.

Farklı bakış açıları kavramların da farklı şekillerde ifade edilmesinde kendisini göstermekte, terörizmle mücadele kavramlarıyla ilgili olarak da bu çeşitlilik karşımıza çıkmaktadır. Alanyazında, terörizmle mücadeleyi ifade etmek maksadıyla terörizmle savaş⁴ (Freedman, 2002; Pedahzur vd., 2002; Byman, 2006; Buzan, 2006; Gregory, 2003;

⁴ “Terörizmle Savaş” ya da “Terörizme Karşı Savaş” kavramı İngilizce dilinde genellikle “War on Terrorism”, “War on Terror”, “The War on Terrorism” ya da “The War Against Terrorism” şeklinde kullanılmaktadır.

Gregory, 2007; Henne, 2019), terörizmle mücadele⁵ (Murphy, 1990; Romanov, 1990; Wilkinson, 1996; Wilcox, 1997; Amble, 2012; Lasley ve Guffey, 2017), karşı terörizm⁶ (Hoffman, 2009; Cronin, 2010; Cronin, 2012; Sandler, 2011; Hellmich, 2012), anti terörizm⁷ (Badey, 1998; Joyner, 1988; Marotta, 1999; Hanlon, 2007; Dietrich, 2013), terörizme karşı koyma⁸ (Byman, 2005; Gendron, 2010; Sinclair, 2014; Saiya, 2020), terörizme müdahale⁹ (Cardona, 1992; Porta, 1992; Bonner, 1992; Chalk, 1995; Aguirre, 2009; Strom ve Eyerman, 2007) terörizme karşı mücadele¹⁰ (Bremer, 1989; Enders vd., 1990; Guillaume, 1992; Macfarlane, 1992; Wilkinson, 1993) ifadeleriyle karşılaşılmaktadır.

Bu kavramlardan terörizmle savaş (war on terrorism), dönemin Amerika Birleşik Devletleri (ABD) Başkanı George W. Bush tarafından 11 Eylül 2001 terör saldırıları sonrasında; bu saldırılara karşılık olarak başlatılan politikaya verilen isim olarak karşımıza çıkmaktadır (Reese ve Lewis, 2009: 781). Terörizmle savaş ne açık bir düşmanı ne de savaşılabilecek alanı tanımlamamaktadır. Terörizmle savaşın çerçevesi oldukça esnek olduğundan, “iyiye karşı kötü” algısı yaratılarak önleyici askeri harekât için ahlaki bir meşrutiyyet sağlanmaktadır (Lewis ve Reese, 2009: 86). ABD yönetimleri tarafından çeşitli strateji belgelerinde çok defa belirtildiği üzere terörizmle savaş; Amerikalıları korumayı, terör saldırılarını önlemeyi, belirli terör gruplarını bertaraf etmeyi ve demokrasiyi teşvik ederek terörü besleyen koşulları azaltmayı kapsamaktadır (Goepner, 2016: 108). 11 Eylül saldırılarının ardından ABD tarafından başlatılan terörizmle savaş konsepti oldukça geniş kapsamlı, çoğunlukla askeri kuvvet kullanımını içeren ancak terörizmi ortaya çıkaran nedenleri de azaltmayı hedeflediğini iddia eden bir yöntemi ifade etmektedir.

ABD Genelkurmay Başkanlığının JP 3-07.2 “Anti Terörizm” isimli yayınına göre terörizmle mücadele (combatting terrorism); terörizmin silahlı gücü olan teröristler ve terörizmi yönlendiren ideolojiyle mücadeleyi kapsayan, hem savunma hem de taarruz bileşenlerini içeren bir yaklaşımdır (US Army Joint Chiefs of Staff, 2014: vii). Savunma

⁵ İngilizce dilinde “Combatting Terrorism” şeklinde ifade edilen kavramın en yakın Türkçe karşılığı “Terörizmle Mücadele” karşılık geldiği değerlendirilmektedir.

⁶ Terörizmle mücadele kapsamında İngilizce dilinde sıklıkla kullanılan “Counter-Terrorism” ifadesinin “Counterterrorism” şeklinde de kullanıldığı görülmektedir. Bu kavramın Türkçe’ye en uygun karşılığının “Karşı Terörizm” olabileceği değerlendirilmektedir.

⁷ “Anti Terörizm” kavramı İngilizce dilinde “Anti-Terrorism” olarak kullanılmaktadır.

⁸ “Terörizme Karşı Koyma” şeklinde kullanılan kavram İngilizce dilinde “Confronting Terrorism” olarak kullanılmaktadır.

⁹ İngilizce dilinde “Response to Terrorism” olarak kullanılan kavramın Türkçe karşılığının “Terörizme Müdahale” kavramını karşıladığı düşünülmektedir.

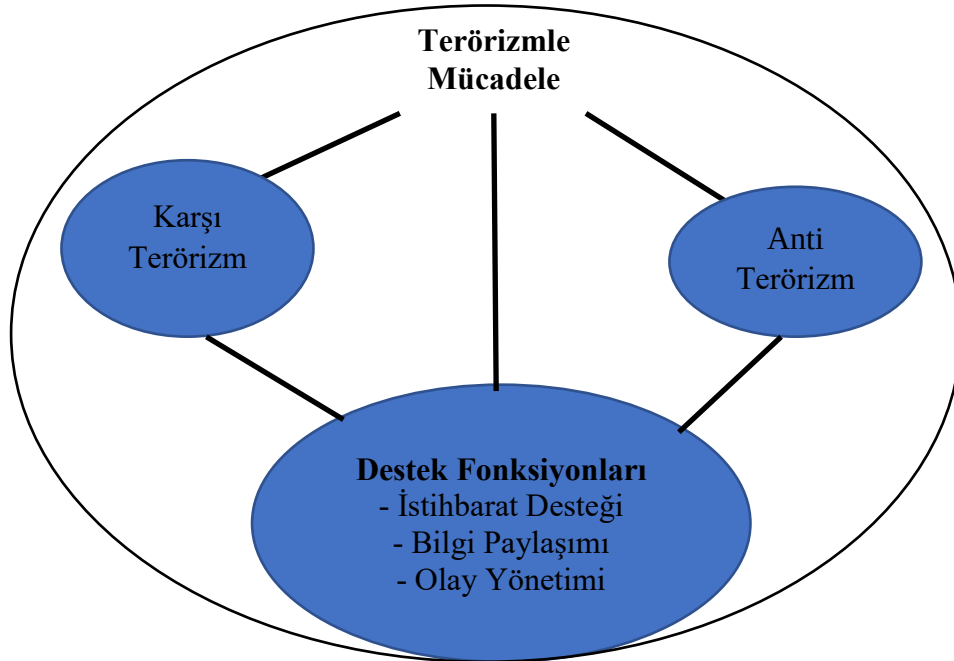
¹⁰ Terörizmle mücadele çerçevesinde kullanılan bir diğer kavram ise “Fight Against Terrorism” olup bu kavram “Terörizme Karşı Mücadele” şeklinde Türkçede karşılık bulabilir.

bileşenini oluşturan anti terörizm (anti terrorism); terör eylemlerinin yerel askeri ve sivil güçler tarafından hızlı bir şekilde kontrol altına alınmasını da içerecek şekilde, bireylerin ve bireylere ait mülkün terör eylemlerine karşı savunmasızlığını azaltmak üzere gerçekleştirilen faaliyetler şeklinde ifade edilmektedir (US Army Joint Chiefs of Staff, 2014: vii).

Karşı terörizm (counterterrorism) ise, hükümetleri veya toplumları hedeflerine ulaşmak maksadıyla zorlamak ve korku salmak için şiddet kullanan terör örgütlerini ve terör ağlarını etkisiz hale getirmek amacıyla yapılan faaliyetler / operasyonlar şeklinde tanımlanmaktadır (US Army Joint Chiefs of Staff, 2014: vii). Şekil 1.1.'de görüldüğü üzere terörizmle mücadele çatı kavram olup, aktif tedbirler içeren karşı terörizm ve pasif tedbirler içeren anti terörizm kavramları ile diğer destek fonksiyonlarını kapsamaktadır.

Karşı terörizm siyasal şiddete karşı alınan savunma ve saldırı tedbirleri biçiminde de tanımlanmaktadır (Newsome, 2006: 75). Karşı terörizm; siyasal, hukuki, diplomatik ve güvenlik alanındaki önlemlerin bir kombinasyonu ile terörizmi önlemeyi ve mücadele etmeyi amaçlayan çok yönlü bir politika şeklinde kavramsallaştırmıştır (Omelicheva, 2007: 371). Bu tanımlamalardan karşı terörizmin; hukuktan güvenliğe, diplomasiden siyasete kadar geniş bir alanda alınan çok boyutlu tedbirleri içeren terörizmle mücadele yöntemi olduğu anlaşılmaktadır.

Şekil 1.1. Terörizmle Mücadelenin Unsurları¹¹



¹¹ Kaynak: US Army Joint Chiefs of Staff, 2014, JP 3-07.2 Antiterrorism, s. I-2.

Terörizmle mücadele alanında karşılaşılan bir diğer kavram ise “terörizme karşı koyma (confronting terrorism)” kavramıdır. Suudi Arabistan’da yürütülen terörizmle mücadeleyi inceleyen bir çalışmada, güvenlik operasyonları ve istihbarat faaliyetleri, terör şüphelilerinin yakalanması ve gözaltına alınmasına yönelik operasyonlar, teröristlerin yargılanması, radikalleşme ile mücadele tedbirleri, terörizmin finansmanı ile mücadele konularının (Gendron, 2010: 492- 495) terörizme karşı koyma çerçevesinde ele alındığı belirtilmektedir. Bu kapsamda terörizme karşı koyma kavramının terörizmle mücadele anlamında ve terörizmle mücadelenin tüm unsurlarını kapsayacak şekilde kullanıldığını söylemek mümkündür.

Bir diğer kavram ise terörizme müdahale (response to terrorism) şeklinde karşımıza çıkmaktadır. İtalya’da terörizmle mücadele uygulamalarının değerlendirildiği bir çalışmada; terörizmle mücadele çerçevesinde gerçekleştirilen yasal düzenlemeler, olağanüstü hal uygulaması, özel hapisane sistemlerinin kurulması, kolluk kuvvetleriyle ilgili düzenlemeler, istihbarat servislerinin faaliyetleri, siyasal alanda yapılan değişiklikler (Porta, 1992: 156-167) terörizme müdahale kapsamında ele alınmıştır. Benzer şekilde Birleşik Krallık’ın terörizmle mücadelesini inceleyen başka bir araştırmada da; yasal düzenlemeler, terörizmin finansmanı kapsamında alınan tedbirler, polise verilen yetkiler, ekonomik tedbirler, siyasi tedbirler, askeri ve polisiye tedbirler, medyanın rolü dâhil olmak üzere psikolojik tedbirler, uluslararası iş birliği, terörizmle mücadele eden birimlerin yapısında yapılan düzenlemeler (Bonner, 1992: 179-200) terörizme müdahale başlığı altında değerlendirilmektedir. Terörizme müdahale kavramının oldukça geniş bir kapsamda terörizmle mücadele anlamında kullanıldığı anlaşılmaktadır.

Terörizmle mücadele alanında sıklıkla kullanılan bir diğer kavram ise “terörizme karşı mücadele (fight against terrorism)” kavramıdır. “Devam Eden Terörizme Karşı Mücadele” isimli çalışmada, terörizme karşı mücadele başlığı altında ABD’nin karşı terörizm politikalarının incelendiği, hukukun üstünlüğü ilkesinin ele alındığı, devletlerin terörizme verdikleri desteğin ifşa edilmesine öncelik verildiği, terörizme destek veren ülkelere karşı uluslararası iş birliğinin genişletilmesi, teröristlerin teknoloji kullanımıyla mücadele edilmesi (Bremer, 1989: 81-87) başlıklarına yer verildiği görülmektedir. “Pakistan’ın Terörizme Karşı Mücadelesi” başlıklı diğer bir çalışmada ise Pakistan Ordusunun terör örgütlerine yönelik askeri operasyonlarından, Pakistan Taliban’ı ile görüşmeler için henüz hazır olunamadığından, aşırıcılık ve radikalleşme ile mücadeleden,

terörizmin kök nedenlerinden, eğitim ve müfredat düzenlemelerinden (Masood, 2012: 16-23) bahsedilmektedir.

Terörizme karşı koyma, terörizme müdahale ve terörizme karşı mücadele kavramlarının terörizmle mücadeleden farklı şekilde ifade edilmelerine rağmen içerik olarak terörizmle mücadele yöntemlerini kapsadığı anlaşılmaktadır. Bu noktadan yola çıkarak bu üç kavramın esasen terörizmle mücadele kavramını karşıladığı, söz konusu kavramların terörizmle mücadele yerine kullanıldığı sonucuna varılmaktadır.

Yabancı dildeki alanyazında durum böyle iken Türkçe alanyazında da terörizmle mücadele (Demir, 2015; Kanat vd. 2016; Güneş, 2019), terörle mücadele (Baharçiçek, 2000; Arıboğan, 2007; Başbuğ, 2011; Yılmaz, 2011), teröristle mücadele (Saraçoğlu, 2016; Sancak, 2019; Altındağ, 2020) şeklinde farklı kavramlar kullanıldığı görülmektedir. Ayrıca tıpkı terör ve terörizm kavramlarında olduğu gibi terörizmle mücadele ve terörle mücadele kavramlarının da birbirleri yerine kullanıldığına rastlanılmaktadır. Ancak teröristle mücadele kavramı terörle mücadele ve terörizmle mücadele kavramlarından ayrı tutulmaktadır.

Teröristle mücadele, teröristlerin aranması, bulunması ve etkisiz hale getirilmesini içermektedir (Başbuğ, 2011: 108). Terörle mücadele ile teröristle mücadele arasındaki farklılığı vurgulayan bir çalışmaya göre terörle mücadele, terörün beslendiği toplumsal dengesizlikleri ve kültürel ya da etnik farklılıkların çatışma ihtimalini ortadan kaldırmayı hedefleyen faaliyetler bütünü iken teröristle mücadele ise eylem safhasına geçen terör örgütlerinin kentlerde ve kırsalda düzenledikleri eylemlere karşı koyma, teröristleri etkisiz hale getirme ve kamu düzenini sağlama çabası olduğu ifade edilmektedir (Saran, 02 Mayıs 2016). Başka bir ifadeyle terör örgütleri ve teröristlerle mücadelenin askeri ağırlıklı bir anlam taşıdığı buna karşılık terörizmle mücadelenin diğer boyutları da içine alan daha geniş kapsamlı bir süreç olduğu belirtmektedir (Altındağ, 2020: 39).

Türkçe alanyazında yer alan hususlardan, terör örgütlerinin eylemlerini önlemeye yönelik olarak, örgütlerin silahlı yapılanmalarına karşı yürütülen faaliyetlerin “teröristle mücadele” şeklinde kavramsallaştırıldığı; siyasal, kültürel, ekonomik, psikolojik alanlarda yürütülen mücadelenin ise “terörle mücadele” ya da “terörizmle mücadele” biçiminde ifade edildiği anlaşılmaktadır.

Tanımlar üzerinden yapılan inceleme sonucunda terörizmle mücadelenin, bir yandan mevcut yasal düzenlemeler çerçevesinde terör örgütlerinin silahlı yapılanmalarının eylem

kabiliyetini azaltmak amacıyla güç kullanarak mücadele ederken; eş zamanlı olarak terörizmi ortaya çıkaran kök sebepleri ortadan kaldırmak maksadıyla diğer alanlarda alınan tedbirleri ve yürütülen faaliyetleri kapsayan çok boyutlu bir strateji olduğu değerlendirilmektedir.

Terörizmle mücadeleyle ilgili alanyazının incelenmesi neticesinde bu çalışmada kullanılacak terörizmle mücadele tanımı; “bir yandan mevcut yasal düzenlemeler çerçevesinde terör örgütünün silahlı yapılanmalarının eylem kabiliyetini azaltmak amacıyla silahlı güç kullanarak mücadele ederken; eş zamanlı olarak terörizmi ortaya çıkaran kök sebepleri ortadan kaldırmak maksadıyla diğer alanlarda alınan tedbirleri ve yürütülen faaliyetleri kapsayan çok boyutlu yöntemler bütünüdür” şeklinde kabul edilmiştir.

1.2. Terörizmle Mücadele Yöntem ve Araçları

Gerek terör örgütlerinin faaliyette bulundukları ülkelerin yapısal ve yönetsel farklılıkları gerekse örgütlerin amaç, talep, eylemselliklerindeki çeşitlilik ve buna bağlı olarak tehdit algılamasına yüklenen önemin derecesi farklı mücadele yöntemlerini gündeme getirmektedir (Çitlioğlu, 2011: 75).

Terörizmle mücadele yöntemleri en basit şekilde, yumuşak ve sert tedbirler olarak ikiye ayrılmaktadır. Yumuşak tedbirler terörizme yol açan kök nedenlerle mücadeleyi, sert tedbirler ise müzakereyi reddeden etkin bir cezalandırma yöntemini kapsamaktadır (Crelinsten ve Schmid, 1992: 309).

Başka bir açıdan bakarak terörizmle mücadele yöntemleri; baskıcı ve uzlaşmacı şeklinde sınıflandırılmaktadır. Baskıcı yöntemler ceza adalet sistemi ve savaş modelini kapsamaktadır. Ceza adalet sistemi terörizmi bir suç olarak görerek hukuk kuralları çerçevesinde mücadeleyi, savaş modeli ise terörizmi özel bir savaş biçimi ya da düşük yoğunluklu çatışma şeklinde görerek savaş kuralları çerçevesinde mücadeleyi kapsamaktadır (Crelinsten ve Schmid, 1992: 311). Uzlaşmacı yöntemler ise; terör örgütleriyle doğrudan görüşme ya da belirli taleplerine cevap verme dâhil olmak üzere uzlaşıcı araçları, teröristlerin ön plana çıkarmaya çalıştığı görelî yoksunlukları gidermeye yönelik araçları kapsamaktadır (Crelinsten ve Schmid, 1992: 310).

Terör örgütü faaliyetlerinin sona ermesi; örgüt liderinin yakalanması ya da öldürülmesi; örgütün yasal siyasal faaliyetlere başlaması; örgütün amaçlarına erişmesi; örgütün halk desteğini kaybetmesi; terör örgütünün askeri güç kullanarak yenilmesi ve başka bir şiddet hareketine evrilmesi gibi altı farklı nedene dayandırılmaktadır. Belirtilen

nedenlerden yola çıkarak, etkili bir terörizmle mücadelede kullanılabilecek yöntemler; örgüte verilen halk desteğini sonlandırmak, örgütün silahlı faaliyetlerini sonlandırmak, terör örgütünün yasal siyasi zemine çekilmesini sağlamak şeklinde sınıflandırılabilir (Cronin, 2009: 8).

Terörizmle mücadele yöntemleri tasnif edilirken; baskıcı (repression) ve uzlaşmacı (conciliatory) yöntemler şeklinde iki farklı yöntemden bahsetmek de mümkündür. Bu tasnife göre baskıcı yöntemler askeri kuvvet kullanımı ve ceza sistemleri dâhil olmak üzere zorlayıcı yöntemleri, uzlaşmacı yöntemler ise terör örgütleriyle görüşmeler dâhil olmak üzere daha yumuşak önlemleri içermektedir (Sederberg, 1995: 299-309).

Terörizmle mücadele yöntemlerini sınıflandırmada başka bir yaklaşım ise tepkisel (reactive) ve proaktif (proactive) şeklinde iki yöntem belirlemektir. Tepkisel yöntem olay odaklı olup, gelecekteki ziyade geçmişle ilgilenen, mücadelenin muhtemel yan etkilerini görmezden gelen bir yaklaşımdır. Proaktif yöntem ise uzun dönemli bir bakış açısından terörizmle mücadeleye yaklaşarak, sonuca odaklı kalıcı çözümler sunmaya çalışmaktadır (Crelinsten ve Schmid, 1992: 310). Terörizmle mücadelenin proaktif yöntemleri içerisinde; örgütlere sızma, ön alıcı hava harekâtı, ikmal kaynaklarını sınırlama ve istihbarat toplama gibi araçlar bulunmaktadır (Enders ve Sandler, 2000: 323).

Terörizmle mücadele yöntemleri savunmacı (caydırıcı) veya proaktif (önleme) yöntemler şeklinde de ele alınabilmektedir. Savunmacı yöntemler, terör saldırılarının başarı olasılığını azaltmayı amaçlayan, terör eylemlerini önlemeye çalışan teknolojiye dayalı engellerin oluşturulmasını, daha sert hukuk tedbirlerinin tesis edilmesini içermektedir. Proaktif yöntemler ise, teröristleri etkisiz hale getirmek maksadıyla düzenlenen ön alıcı operasyonları, terör örgütlerine sızma faaliyetlerini, terör eylemlerinin ardından düzenlenen operasyonları kapsamaktadır (Faria, 2006: 47).

Terörizmle mücadele yöntemleri savunma ve proaktif yöntemler şeklinde iki ana başlık altında incelendiğinde; savunma yöntemleri içerisinde teröristler için muhtemel hedeflerin güçlendirilmesi ve böylece eylem düzenlenmesinin daha zor bir hale getirilmesi; teröristleri eylemden caydırmak amacıyla terör eylemlerine yönelik cezaların artırılması; uçakların füzeyle karşı koruma sistemleri ile donatılması kapsamındaki tedbirler sayılmaktadır (Sandler, 2011: 226). Proaktif tedbirler ise sert tedbirler olup; terör örgütlerini veya terör örgütü sempatanlarını doğrudan sınırlamaya çalışan tedbirlerdir. Bunlar içerisinde terör örgütü kaynaklarını yok etme; güvenli bölgelerini ve terör sempatanlarını hedef alma; devlet propagandasını yürütme; askeri operasyonlar

düzenleme; göreceli yoksunluğa neden olan hususları zayıflatmak için terörizmin kök nedenleri ile mücadele etme gibi tedbirler yer almaktadır (Sandler, 2011: 226).

Başka bir terörizmle mücadele sınıflandırması da terör örgütlerinin faaliyetleri kapsamında ortaya konulmaktadır. Buna göre mücadele; terör örgütlerinin baskıcı ve siyasal kabiliyetlerini önlemeye ilişkin yöntemlerden meydana gelmektedir. Bu yöntemlerden terör örgütünün baskıcı kabiliyetlerini önlemek için, örgütün şiddet veya şiddet tehdidini kullanımına yönelik askeri seçenekler dâhil olmak üzere yasal çerçevedeki baskıcı yöntemler kullanılmaktadır. Terör örgütünün siyasal kabiliyetlerine yönelik terörizmle mücadele yöntemi ise daha çok mücadelenin propaganda boyutu ile örgütlerin siyasal taleplerine yönelik reformları kapsamaktadır (Crelinsten ve Schmid, 1992: 310).

Bu bilgiler ışığında; terör örgütünün yapısına, terörizmle mücadele eden devletin demokratik yapısına, terörizmin ortaya çıkış nedenlerine, terör örgütünün eylem yöntemlerine uygun olarak farklı terörizmle mücadele yöntemleri kullanabildiğini söylemek mümkündür. Terörizmle mücadelede kullanılan araçlar ise; diplomasi, ceza adalet sistemi, terörizmin finansmanının önlenmesi, istihbarat, istihbaratın örtülü operasyonlar maksadıyla kullanılması, askeri kuvvet kullanımı araçları şeklinde kategorize edilebilmektedir (Pillar, 2001: 73-130). Terörizmle mücadelede araçlar; siyaset ve diplomasi, barış süreci, ceza adalet sistemi, kolluk kuvvetleri / askeri kuvvet kullanımı, havacılık güvenliği, medya faaliyetleri ve uluslararası iş birliği şeklinde de sıralanabilmektedir (Wilkinson, 2011: 64- 181).

Terörizmle mücadelede kullanılabilecek araçlar; ceza adalet sistemi içerisindeki yasal kovuşturmalar, terör örgütleri ve sempatizanlarının finansal faaliyetlerinin önlenmesi, kolluk kuvvetleri operasyonları, askeri birlik kullanımı, diplomasi ve istihbarat faaliyetleri biçiminde de sınıflandırılmaktadır (Carter, 2017: 15). Başka bir açıdan terörizmle mücadele araçları; ceza adalet sistemi, siyasal ve sosyo-ekonomik tedbirler, diplomasi, askeri kuvvet kullanımı ve istihbarat başlıkları altında toplanmaktadır (Demir, 2017: 131-146). Terörizmle mücadelede siyasal araçlar; terör örgütleriyle görüşme süreçlerini, sosyal ve kültürel alanlarda yapılabilecek düzenlemeleri, alınması gereken ekonomik önlemleri, terörizmin finansal ve psikolojik boyutlarıyla mücadeleyi içerisinde barındırmaktadır (Demir, 2017: 132-137).

Terörizmle mücadelede diplomasi aracı ise, yabancı muhataplara terörizmle mücadele politikalarını ifade etmek, onları ikna etmek ve onlarla mutabakata veya anlaşmalara ulaşmak amacını taşımaktadır. Diplomasi, terör örgütlerinin veya destek veren

devletlerin faaliyetlerini engellemeyi amaçlamaktadır (Pillar, 2001: 73-74). Diploması aracı; terörizmle mücadele eden kolluk kuvvetlerinin diğer ülkelerin kolluk kuvvetleriyle koordineli çalışması, terörizmle mücadeleyle ilgili uluslararası sözleşmelerin hazırlanması ve uygulanması, diğer ülkelerle istihbarat paylaşımı açısından önemli görülmektedir (Demir, 2018: 194).

Terör örgütlerinin silahlı güçlerine yönelik olarak askeri kuvvet, altı farklı şekilde kullanılabilir. Bu çerçevede askeri kuvvet; terör eylemlerini önleyici operasyonlar düzenlemek, terör örgütlerini eylem düzenlemekten caydırıcı faaliyetlerde bulunmak, terör eylemlerinin ardından cezalandırıcı operasyonlar düzenlemek, terör örgütünün lider kadrosuna yönelik operasyonlar yapmak, kriz döneminde kamu düzeninin tesisi maksadıyla sivil otoriteye yardım etmek, terör örgütü faaliyetlerini azaltmak veya tamamen ortadan kaldırılmak maksadıyla kullanılmaktadır (Duyvesteyn, 2008: 333-334).

Terörizmle mücadelede ceza adalet sistemi; bir terör örgütü mensubunun yakalanarak adalet önüne çıkarılması, cezalandırılması, cezasının infaz edilmesi şeklindeki kolluk ve adalet mekanizması iş birliği içerisinde yürütülen faaliyetler bütünüdür (Wilkinson, 2006: 61-88).

Terörizmle mücadele kapsamında istihbarat teşkilatları, terörizmden kaynaklanan tehdidin anlaşılması; terör örgütlerinin kapasiteleri ve niyetleri hakkında bilgi toplanması; teröristlerin bulunması ve etkisiz hale getirilmesinde öneme sahiptir. Bu kapsamda istihbarat teşkilatları terörizmle mücadele eden güçlere terör örgütlerinin yeteneklerini hedef alabilme ve böylece belirlenen hedeflere erişme imkânı sağlayabilecek fırsatlar yaratmaktadır (Pollard, 2009: 117).

Bu tezin ana çerçevesini terörizmle mücadelede istihbaratın kullanılması teşkil etmektedir. Bu kapsamda terörizmle mücadele araçlarının bir kısmına değinilmiş, terörizmle mücadele çerçevesinde istihbarat teorileri, terörizmle mücadele aracı olarak istihbaratın yeri ve önemi konusu müteakip başlık altında detaylı olarak incelenmiştir.

1.3. Terörizmle Mücadele Aracı Olarak İstihbarat

Hemen her devletin temel fonksiyonlarından birisi olan istihbarat; devletler, kurumlar, akademisyenler tarafından farklı bakış açılarıyla tanımlanmıştır. Bu nedenle; terörizm ve terörizmle mücadele gibi ortak ve üzerinde anlaşılmış bir istihbarat tanımının da bulunmadığını söylemek mümkündür.

Anlam itibarıyla istihbarat üç farklı anlamı ifade etmektedir. Bunlardan birincisi bilgidir. Bilgi anlamına gelen istihbarat, bir hükümetin ulusal güvenliğini desteklemek, fiili veya potansiyel düşmanlardan gelen tehditlerle başa çıkmak maksadıyla yürütülecek politikasını formüle etmesi ve uygulamasına ilişkin bilgileri ifade etmektedir. İstihbarat anlamına gelen ikinci fonksiyon faaliyettir. Bir faaliyet olarak istihbarat, bilgilerin toplanmasını ve analiz edilmesini içerir. Ayrıca, düşmanların bilgiye erişimini engelleyerek veya bilginin önemi konusunda onları aldatarak istihbarat faaliyetlerine karşı koymak için yapılan faaliyetler de bu kapsamda değerlendirilmektedir. İstihbaratın üçüncü anlamı ise örgüt anlamıdır. Bu anlamıyla istihbarat, istihbarat faaliyetlerini yürüten örgütü ifade etmektedir (Shulsky ve Schmitt, 2002: 1-2).

İstihbarat; “bilgi”, “süreç” ve “faaliyet” gibi birkaç farklı anlama gelmektedir. İstihbaratın; gizli kaynak ve yöntemlere bağlı, devletin faaliyetleri için devlet görevlileri tarafından yürütülen, genellikle diğer devletlere yöneltilen, bilginin üretilmesi ve dağıtımıyla ilişkili olan, yabancı kurum ve kuruluşları etkilemeye çalışan özellikleri mevcuttur. Bu kapsamda istihbarat; yabancı kurum ve kuruluşları anlamak ve etkilemek için yürütülen gizli devlet faaliyetleri şeklinde tanımlanmaktadır (Warner, 2002: 15-21).

Her ne kadar istihbarat kavramı hakkında anlaşılabilir bir gizem bulunsa da, esasen istihbarat basit ve açık bir olgudur. İstihbarat bir faaliyet olarak belirli bir tür bilginin peşinden gitmek, o bilgiyi izlemek takip etmek; bir olgu olarak ise faaliyet sonucunda ortaya çıkan bilgi anlamlarına gelmektedir (Kent, 1965: xxi).

Başka bir bakış açısına göre istihbarat; her türlü aracın kullanılması sonucu elde edilen veri, malumat ya da bilginin, politikaların gerçekleşmesi ve politikalara zarar verilmesinin önlenmesi maksadıyla, önemine ve doğruluğuna göre sınıflandırılması, karşılaştırılması, analiz edilerek değerlendirilmesi sonucunda ulaşılan bilgi şeklinde tanımlanmaktadır (Özdağ, 2018: 31). Bu tanımlamadan istihbarat kavramının; bir verinin elde edilmesi, sınıflandırılması, karşılaştırılması ve analizini içeren bir süreci ifade ettiği görülmektedir.

Bilgi (information) ile istihbarat kavramları arasındaki farka dikkat çeken bir çalışmada, çok sayıda insan için istihbaratın, bilgiden küçük bir farkının bulunduğu ifade edilmektedir. Buna göre istihbarat bilgidir, ancak her bilgi de istihbarat değildir. Bilgi ve istihbarat arasındaki farkı ayırt etmek önemlidir. Nasıl edinildiğine bakılmaksızın bilgi; bilinen şeydir. Bununla birlikte istihbarat, politika yapıcıların belirtilen ihtiyaçlarını

karşılaman ve bu ihtiyaçları karşılamak için toplanan, işlenen ve daraltılan bilgidir (Lowenthal, 2009: 2).

İstihbaratın ne olduđu değil, ne olmadığından yola çıkarak yapılan tanımlamada, istihbaratın sadece bilgi ve veri olmadığı belirtilmektedir. Bu çerçevede istihbarat; idareyi bilgilendirmek veya askeri çatışma durumunda askeri harekâtı desteklemek için kullanılan işlenmiş, değerlendirilmiş ve damıtılmış bilgi veya veriler biçiminde ifade edilmiştir (Dupont, 2003: 16).

İstihbaratı tanımlamaktan daha çok istihbaratın hangi maksatlarla kullanıldığı üzerinden kavram ortaya konulmaya çalışıldığında, istihbarat; stratejik bir sürprizden kaçınma; uzun vadeli bir perspektif ve öngörü sağlama; politika oluşturma sürecine yardımcı olma; devletin bilgi, ihtiyaç ve yöntemlerini gizleme amaçlarıyla yürütülen faaliyetler bütünü olarak tanımlanmaktadır (Lowenthal, 2009: 3).

İstihbarat; devletlerin dış politika ve milli güvenlikleri için ihtiyaç duyduğu, yabancı ülkeler ve bu ülkelerin casusları hakkında bilgilerin toplanması ve işlenmesi, dış politikanın uygulanmasını kolaylaştıracak yardımcı faaliyetlerin yürütülmesini içeren devlet faaliyetleri şeklinde tanımlanmaktadır (Bimfort, 1958: 78).

İstihbarat; karar alıcıları desteklemek amacıyla rekabetçi bir ortamda bilginin toplanması, analiz edilmesi ve dağıtımını kapsayan faaliyetler bütünüdür (Sims, 2009: 154). Tanımında devlete yönelik tehditlerin önceden tespit edilebilmesi hususuna vurgu yapılan bir tanıma göre istihbarat; devletlerin varlığına yönelik olası tehditlerden önceden haberdar olunarak bu riskleri ortadan kaldırmak ya da muhtemel zararlarına yönelik tedbirler almak için kullanılan bir kalkan şeklinde ifade edilmektedir (Kent, 2003: 10).

İstihbaratın; stratejik ve taktik seviyede düşünülerek tanımlanmasının uygun olacağını belirten bir tanıma göre stratejik istihbarat, liderlerin ulusal ve uluslararası seviyede muhtemel risk ve kazanımları anlayabilmesi, karar alabilmesi ve harekete geçebilmesi için çevrede olup biten hakkında sahip olunan analiz edilmiş bilgi olarak kavramsallaştırılmıştır. Taktik istihbarat ise harekât alanındaki durumsal farkındalığı artırmak maksadıyla toplanan analiz edilmiş bilgi şeklinde ifade edilmektedir (Johnson, 2007: 1).

Buraya kadar incelenen tanımlamalarda istihbaratın; gizlilik, bilgi, bilgi üretme, haberdar olma, devletlerin güvenlik ve dış politikalarını sağlıklı yönetebilmeleri için gerekli bilginin toplanması ve işlenmesi, devletin kendine ait bilgiyi gizlemesi gibi

anlamlarda algılandığı görülmektedir. Tanımlayan kişiye/kuruma göre değişen, oldukça geniş bir yelpazede farklı şekillerde anlaşılan istihbarat, geniş bir çerçevede bilgiyi toplama, işleme, analiz ve dağıtma aşamalarını içeren bir süreci ifade etmektedir.

Kavramsal çerçevenin incelenmesi neticesinde, istihbaratın amacının; karar alıcıları desteklemek, kaynakları doğru kullanmak, devletlerin dış politika ve milli güvenlikleri için ihtiyaç duyduğu bilgileri toplanmak, devletin kritik bilgi ve yöntemlerini gizlemek, uzun dönem için bir öngörü sağlamak, devletin varlığına yönelik olası tehditlerden önceden haberdar olmak ve sürprizlerden kaçınmak olduğu anlaşılmaktadır.

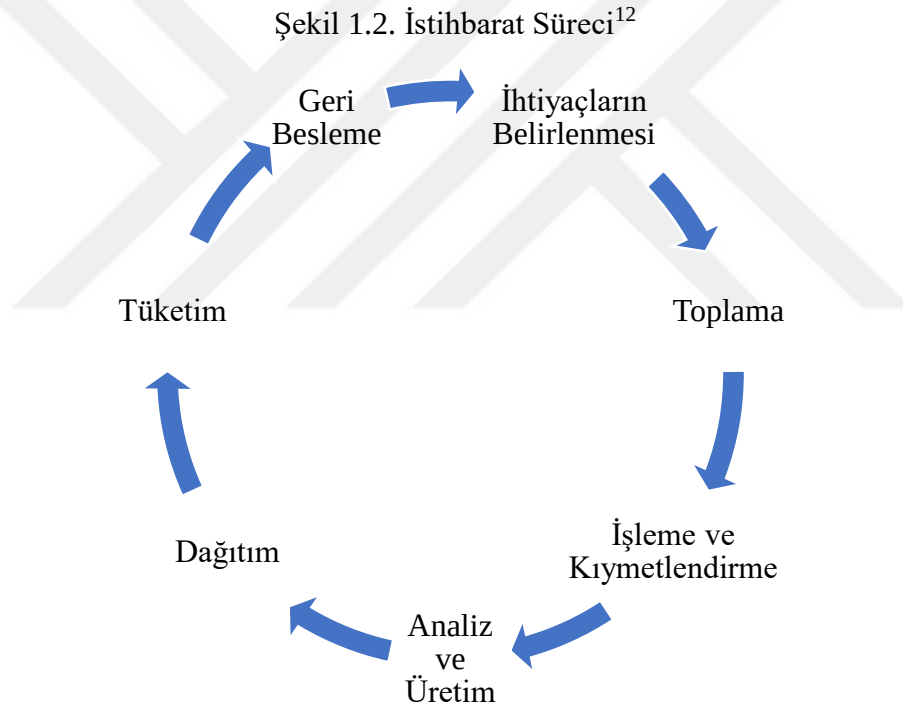
İstihbarat, büyük ölçüde ulusal güvenlikle ilgili konuları, yani savunma ve dış politikaya ilişkin hususları, 2001 terör saldırılarından bu yana ise giderek daha da önemli hale gelen iç güvenlik konularıyla ilgili görülmektedir (Lowenthal, 2009: 29). Trinquier, (2006: 15), Schmid (2011: 113), Morris (2009: 2) ve Wardlaw (1989: 131-134) tarafından belirtildiği üzere sürpriz etkisinin terör örgütlerine avantaj sağlayan, terörizmin ayrılmaz parçası olduğu ifade edilmektedir. İstihbaratın ise güvenlik açısından sürprizlerden kaçınmak maksadıyla kullanılan en önemli araç olduğu (Lowenthal, 2009: 3) göz önünde bulundurulduğunda, bu tezin amacı bakımından istihbaratın; terörizm gibi devletlerin güvenliğine yönelik tehditlerden önceden haberdar olunması, bu tehditlerin ortadan kaldırılması, terörizmden kaynaklı sürprizlerden korunma sağlanması konularıyla doğrudan ilgili olduğu sonucuna varılmaktadır.

İstihbaratla ilgili alanyazının incelenmesi neticesinde bu çalışmada kullanılacak istihbarat tanımı; “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, ihtiyaç sahibi kurumlara ve karar alıcılara ulaştırılması, ulaştırılan kurumlardan alınan geri besleme ile kendisine yön veren, döngüsel bir süreci ifade eden gizli bir faaliyet” şeklinde ifade belirlenmiştir.

İstihbarat bir faaliyetler bütünü, bir işlem döngüsünü ifade etmektedir. İstihbarat çarkı olarak da bilinen bu döngü; planlama ve yöneltme, toplama, işleme, analiz ve üretim ile dağıtım basamaklarını içermektedir (Gill ve Phythian, 2018: 35-36). Tezin müteakip bölümü olan sosyal medya istihbaratı bölümünde yeniden gündeme geleceği üzere, istihbarat tanımı içerisinde bahsedilen bu döngüyü daha kolay anlatabilmek ve işleyişe yön tutacak bir sistematik oluşturmak için istihbarat çarkı şeklinde adlandırılan sürecin işlem safhalarına kısaca değinmek gerekmektedir.

İstihbarat süreci (Şekil 1.2.) ihtiyaçların belirlenmesi, toplama, işleme ve kıymetlendirme, analiz ve üretim, dağıtım, tüketim ve geri besleme olmak üzere yedi ana basamakta incelenebilmektedir. Bu kapsamda ihtiyaçların belirlenmesi; istihbaratın katkıda bulunmasının beklendiği konuların veya alanların yanı sıra bu konulardan hangisinin diğerlerine göre daha öncelikli olduğuna dair alınan kararı ifade etmektedir (Lowenthal, 2009: 106).

İstihbarat sürecinin belki de en önemli safhası olan toplama ise uygun vasıtalarla yönlendirilen bilginin uygun tekniklerle toplanmasını ifade etmektedir. Toplanan bilgilerin kullanılabilir hale gelmesi, analize uygun hale getirilmesi maksadıyla; işlendiği, ayıklandığı, bilginin istihbarata dönüştürüldüğü safha ise işleme ve kıymetlendirme safhasıdır (Lowenthal, 2009: 117).



Analiz ve üretim safhası ise işlenen, ayıklanan, kullanıma hazır hale getirilen bilginin değerlendirildiği, istihbarat niteliği taşıyıp taşımadığına karar verildiği, elde mevcut diğer bilgilerle karşılaştırmaların yapıldığı, istihbarata son şeklinin verildiği safhadır (Lowenthal, 2009: 119-120).

Dağıtım aşamasında istihbarat karar alıcılara ve gerekli diğer birimlere ulaştırılırken, tüketim safhasında istihbarat brifing, rapor, değerlendirme şeklinde sunularak tüketilmektedir. Son aşama olan geri besleme safhası ise başta karar alıcılar olmak üzere

¹² Kaynak: Lowenthal, M. M. (2009). Intelligence From Secrets To Policy. Fourth Edition. CQ Press. s.106

istihbaratı kullananlar tarafından neyin fayda sağladığı, neyin gereksiz olduğu ve başka neye ihtiyaç duyulduğuna ilişkin görüş ve önerileri kapsamaktadır (Lowenthal, 2009: 121-124).

1.4. Terörizmle Mücadele Çerçevesinde İstihbarat Teorileri

İstihbarat teorilerinde karşılaşılan ilk çarpıcı ifade Walter Laqueur tarafından ifade edilen “...iddialı bir istihbarat teorisi geliştirme çabalarının hepsi başarısızlıkla sonuçlandı” şeklindeki sözüdür. Micheal Warner, Laqueur’un bu ifadesinden yola çıkarak, henüz üzerinde anlaşılmış bir tanımı dahi bulunmayan istihbarata ait bir teorinin geliştirilmesinin de mümkün olamayacağını belirtmiştir (Warner, 2002: 15). Bu düşünceye karşın, bugüne dek geliştirilen istihbarat teorileri de mevcuttur.

Bunlardan birisi David Kahn tarafından geliştirilen “İstihbaratın Tarihsel Teorisidir”. Teoride; akademik bir disiplin olarak kabul edilen istihbarat için bir teoriye ihtiyaç duyulduğu, bu konuda ileri düzeyde geliştirilmiş bir teori bulunmadığı, yapılan çalışmaların hiçbirisinde denemeye açık konseptler öne sürülemediğini belirtmektedir (Kahn, 2008: 4). Tarihsel istihbarat teorisinde; istihbaratın geçmişi, bugünü ve geleceği incelenmekte, tarihsel süreç içerisinde istihbaratın öneminin nasıl yükseldiği açıklanmakta, teorinin geliştirildiği tarihe kadar çözümsüz kalmış sorun alanları ortaya konulmaktadır (Kahn, 2008: 4).

Tarihsel istihbarat teorisinde; “geçmiş” dönemde istihbarat açıklanırken, her dönemde hükümdarların istihbaratı kullandığını, geçmiş dönemde komutanların düşmanların nerede olduklarını görmeye gayret ettiklerini, çoğunlukla istihbarat toplamak için düzenli bir çaba harcanmadığı ifade edilmektedir (Kahn, 2008: 5).

Teori, istihbaratı fiziksel ve sözel olarak iki ana bölüme ayırmakta; ilerleyen birlikleri gözetlemek, ordugâh ateşini görmek, motor gürültüsü duymak ve yemek kokusunu almak gibi fiziksel olayları fiziksel istihbarat kapsamında değerlendirmektedir. Teori ayrıca, 4000 yıllık savaş tarihi boyunca, I. Dünya Savaşına dek bilginin neredeyse tamamının fiziksel istihbarat yoluyla temin edildiğini vurgulamaktadır. Düşmanın morali hakkında bir rapor, duyulan bir emir, telgraf kablolarından elde edilen istihbaratın ise sözel istihbaratla oluşturulduğu belirtilmektedir (Kahn, 2008: 6).

Teori, sözel istihbaratın fiziksel istihbarata göre daha değerli bilgiler toplayabileceğini, sözel istihbaratın “gücü artırdığını”, II. Dünya Savaşında sözel kaynakların komutanlar için daha yararlı bir hale geldiğini ifade etmektedir (Kahn, 2008:

7). Teoriye göre istihbaratın prensipleri; kaynakların en iyi şekilde kullanılmasına yardımcı olması, savaşta esas unsur değil yardımcı kuvvet olması ve taarruza oranla savunmada daha gerekli olmasıdır (Kahn, 2008: 8-9). Teori, istihbaratın bu üç prensibi ile istihbaratın etkisini ve bugünkü önemine nasıl ulaştığını anlatmaktadır.

Tarihsel istihbarat teorisinde; istihbaratın “geleceği” ortaya konulurken, istihbaratın karşılaştığı iki temel sorun dile getirilmiştir. Bu sorunlardan birincisi olacakların önceden nasıl bilinebileceği, ikincisi ise karar alıcıların beğenmedikleri bilgiyi kabul etmeleri için nasıl ikna edilebilecekleridir. Tarihsel teoride bu iki sorunun gelecekte de kendisini muhafaza edeceği, kaynakların etkin kullanılması açısından askeri teçhizat alımına duyulan ihtiyacın azaltılmasıyla tasarrufa neden olunacağı belirtilmektedir. Teori ayrıca, savunmanın bir parçası olduğundan istihbaratın saldırgan olmayan uluslar için daha gerekli bir hale geleceğini ifade etmektedir (Kahn, 2008: 10-13).

Tarihsel istihbarat teorisi bu çalışmanın konusu açısından değerlendirildiğinde; gözün gördüğü verilerin toplanmasıyla başlayıp, zaman içerisinde sözelin daha ağırlıklı hale geldiği istihbaratın, gelişen teknolojiye paralel olarak artık daha dijital bir hal alacağına işaret etmektedir. Tarihsel süreçte gelişen istihbaratın iletişim altyapısı ve teknolojilerinin de gelişimiyle birlikte, internet ve özelinde sosyal medyada yer alan büyük boyuttaki verileri kıymetlendirmeye yoğunlaştığı da değerlendirilmektedir.

Bir diğer önemli istihbarat teorisi ise James J. Wirtz tarafından geliştirilen “Sürpriz Teorisidir”. Teori, sürpriz kavramını açıklamayı, sürprizin meydana gelmesinin engellenip engellenemeyeceğini, devletlerin neden rakiplerini diplomatik veya askeri girişimlerle şaşırtmaya çalıştıklarını, neden başarılı olduklarını, sürprizin onu kullanan tarafın hedeflerine ulaşmasına ne kadar yardımcı olduğunu açıklamaya çalışmaktadır (Wirtz, 2008: 73).

Teoride; sürpriz bir kuvvet çarpanı olarak tanımlamakta, sürprizin savaşan kuvvetlerin etkinliğini artıran bir faktör olduğu belirtilmektedir. Teoriye göre başarılı bir sürpriz saldırı, daha güçlü olan tarafı psikolojik olarak sarsmakta ve direncini geçici de olsa azaltmakta, düşman kuvvetlerinin büyük bir kısmının düşük bir maliyetle imha edilmesini kolaylaştırmaktadır. Sürpriz; güçsüz ve zayıf olanın, sayısal olarak daha küçük olanın, kendi seçtiği zaman ve yerde güçlerini yoğunlaştırarak kesin bir zafer elde etme olasılığını büyük ölçüde artırabilmektedir (Wirtz, 2008: 74).

Teori çerçevesinde sürpriz, zayıf olan tarafa, normal şartlarda ulaşamayacakları hedeflere ulaşmalarına imkân vermektedir. Daha güçlü olan tarafın, genellikle sürpriz faktörünü kullanmadığı, bunun yerine güçlü tarafın saldıracağını önceden bildirerek caydırıcı olmaya çalıştığı, ancak güçlü tarafların da zaman zaman sürpriz yapmayı ve sürpriz etkisinden yararlanmayı amaçladıkları belirtilmektedir (Wirtz, 2008: 76-77).

Sürpriz teorisine göre sürpriz etkisinin önlenmesi için birçok zorluğun üstesinden gelinmesi gerekmektedir. Örneğin, düşmanın aldatma gayretlerinin üstesinden gelinmeli, zayıf olan rakiplerin sürprizle desteklenen çığınca eylemlerle hedeflerine ulaşmayı ne kadar istediği tahmin edilmelidir. Ancak rakibin asimetrik saldırılar düzenleme olasılığını tahmin etmek de oldukça zor görünmektedir (Wirtz, 2008: 79).

Ayrıca, sürpriz saldırıların genellikle geçici süreli etkiler ve sonuçlar üreteceği, ancak sürpriz faktörünün nadiren savaşları kazandırdığı belirtilmektedir. Bu konuya örnek olarak, Japonlar tarafından Pearl Harbor'a düzenlenen saldırı verilmekte, bu saldırının belki de bin yıl boyunca hatırlanacağı, ancak "başarılı" olarak görülen bu saldırının Japonya için siyasi bir felaket yarattığı da vurgulamaktadır. Teori, sürprizin belirli bir faaliyetin etkisini en üst düzeye çıkarabileceğini, ancak en başarılı sürpriz saldırının bile savaşı kazanmak için tek başına yeterli olmadığını, sürprizin genel bir stratejiye bağlı olarak yürütülmesi gerektiğini ileri sürmektedir (Wirtz, 2008: 80).

Sürpriz teorisi, El Kaide'nin ABD'de düzenlediği saldırıların, terör örgütlerine kendisinden daha güçlü bir ülkeye saldırmanın yolunu gösterdiğini vurgulamaktadır. Bu nedenle ABD istihbarat topluluğunun, devlet dışı aktörlerin hedeflerine ulaşabilmek için sürpriz etkisinden yararlanmaya çalışacaklarını göz önünde bulundurması gerektiği belirtilmektedir (Wirtz, 2008: 82).

Teoride, güçlü olan tarafın çatışmayı zayıf tarafın bakış açısından görmeye başlaması, zayıf aktörlerin de savaşın kurallarını akıllarında tutmaları durumunda sürpriz olasılığının azalacağını, ancak gelecekte de sürprizin önlenebileceğini beklemenin çok iyimser olacağı açıklanmaktadır (Wirtz, 2008: 83-84).

Sonuç olarak sürpriz teorisi, sürpriz faktörünü bir kuvvet çarpanı olarak tanımlamakta, sürprizin zayıf olanın güçlü üzerinde yarattığı psikolojik etkisini ortaya koymakta, sürprizin daha zayıf olan tarafa geçici de olsa üstünlük sağlayacağını vurgulamaktadır. Trinquier (2006: 15), Morris (2009: 2) ve Wardlaw (1989: 131-134) tarafından belirtildiği üzere, terör eylemlerinin ne zaman, nerede ve nasıl düzenleneceğine

yönelik belirsizliklerden kaynaklanan sürpriz etkisi terör örgütlerine üstünlük sağlamaktadır.

Terörizmin en önemli özelliklerinden birisinin sürpriz etkisi olduğu; istihbaratın ise güvenlik açısından sürprizlerden kaçınmak maksadıyla kullanılan en önemli araç olduğu (Lowenthal, 2009: 3) göz önünde bulundurulduğunda, bu tezin amacı bakımından istihbaratın; terörizm gibi devletlerin güvenliğine yönelik tehditlerden önceden haberdar olunması, bu tehditlerin ortadan kaldırılması, terörizmden kaynaklı sürprizlerden korunma sağlanması konularıyla doğrudan ilgili olduğu sonucuna varılmaktadır. Sürpriz teorisi çerçevesinde istihbaratın terörizmden kaynaklanan sürpriz etkisini en aza indirmek için gerekli en önemli terörizmle mücadele araçlarından birisi olduğu sonucuna ulaşılmaktadır.

1.5. Terörizmle Mücadele Aracı Olarak İstihbaratın Amacı ve Önemi

1.5.1. Terörizmle mücadelede istihbaratın amacı

Terörizmle mücadelede istihbaratın amacı; terör örgütü taktik ve tekniklerinin belirlenmesi, terör eylemleriyle ilgili bilgilerin bir araya getirilmesidir. Esasen, terörizmle mücadele istihbaratının temel prensibi tahmin etmek değil, öngörülemez bir dünyada istihbaratı kullanan yöneticilerin doğru kararlar almalarına yardımcı olmaktır. Bu yardım, karar alıcılara tehdidin çapı, terörizm tehdidinin nereye evrilebileceği, her ihtimal için ulusal çıkarlar doğrultusunda atılabilecek adımları içermektedir (Pillar, 2004: 119-121).

Terörizmle mücadelede istihbarattan en çok beklenen katkı, tehdidi ortadan kaldırmak için tedbirler almak ve terör eylemi planlarını zamanında tespit etmektir (Pillar, 2001: 110). Terörizmden kaynaklanan tehdidin önlenmesi gerekmekte, terör örgütlerinin niyetlerinden eylemlerine kadar geniş bir alanda erken ikazlar verilmesi önemli hale gelmektedir. Terörizmle mücadelede tehdit, terör eylemleri gerçekleşmeden önce tespit edilmeli, eylemlerin durdurulması için istihbarat gerekli hale gelmektedir (Treverton, 2008: 101).

Terörizmle mücadelede terör örgütlerinin nerede faaliyet gösterdiklerini, ne şekilde örgütlendiklerini, nasıl iletişim kurduklarını, finans kaynaklarını ve eylemlerini nasıl planladıklarını bilmek gerekmektedir. İyi bir istihbarat sadece terör örgütlerinin saklandıkları yerler ve planladıkları eylemler hakkında değil aynı zamanda örgütün içyüzü ile ilgili önemli bilgiler de sunmaktadır (Richardson, 2006: 252-255).

Terörizmle mücadelede istihbarat dört ana amaç için kullanılmaktadır. Bu amaçlar; terörizmin nedenlerini ve tehdit seviyesini belirlemek, güvenlik önlemlerini belirlemek için

stratejik deęerlendirmeler yapmak; terörizmle ilgili hususlarda mahkemeler için suça yönelik bilgi toplamak; terörizmi önlemek maksadıyla bilgi toplamaktır (Walker, 2009: 153).

Bir başka çalışmada ise terörizmle mücadelede istihbaratın kullanılma amaçları on beş ayrı başlık altında toplamıştır. Buna göre terörizmle mücadelede istihbarat; terörizm faaliyetlerine katılanları tespit etmek; terör örgütlerinin yöntemlerine ilişkin veri tabanı hazırlamak; daha yüksek risk altında olan kişileri belirleyerek can kaybını önlemeye yardımcı olmak; örtülü operasyonlar düzenlemek; terör örgütlerinin ikmal güzergâhları, güvenli evleri, eleman-silah ve finans temin kaynaklarını belirlemek için kullanılmaktadır (Robertson, 1987: 48). Ayrıca, terör saldırılarıyla ilgili önceden ikazlar vermek ve terör saldırılarını önlemek; karşı propagandaya yardımcı olmak; kara propaganda yaymak; terör örgütünün parçalanmasını sağlamak; polis, ordu ve teçhizat gibi kaynakların uygun konuşlandırılmasına yön vermek maksadıyla terörizmle mücadelede istihbarat toplanabileceęi belirtmektedir (Robertson, 1987: 49). Terörizmle mücadele kapsamında, terör örgütü üyeleri arasındaki iletişimi sekteye uğratmak; terörizmle mücadelede müttefikler edinmek ya da hasımları caydırmak; terör örgütlerini yalnızlaştırmak ve cesaretlerini kırmak; dięer kurum ve kuruluşlarla paylaşmak yoluyla terörizmle ilgili bilgi miktarını artırmak ve son olarak muharebe istihbaratı sağlamak için istihbaratın gerekli olduęu belirtilmektedir. Bu amaçları yerine getirmek üzere istihbarat, etkili bir terörizmle mücadele stratejisinin merkezinde yer almaktadır (Robertson, 1987: 48-49).

Terörizmle mücadelede istihbarat; terör örgütleriyle görüşmelerde kullanılmak üzere bilgi temin etme, terör örgütü mensuplarının yargı önüne çıkarılması maksadıyla delil toplama, terör eylemlerinin ne zaman gerçekleşeceęine ilişkin bilgi toplama amacıyla kullanılmaktadır (Crenshaw, 1999: 1-11).

Terörizmle mücadelede eyleme geçirilebilir istihbarat (actionable intelligence) çerçevesinde; terör örgütü hücreleri ve bu hücrelerin yeteneklerine ait verilerin, terör örgütü ve teröristler hakkında bilgilerin temin edilmesi gerekmektedir. Ayrıca, terör örgütüne ait silahlar, terör örgütü mensuplarının yeri, planlanan eylemlere ait zaman, mekân ve dięer ayrıntılara ait bilgilerin mutlaka toplanması gerekmektedir (Wagner, 2007: 53). Terörizmle mücadele kapsamında istihbarat, terör örgütlerinin yenilikçi eylem ve hareket tarzlarının tahmin edilmesine yönelik kullanılabilmektedir (Faria, 2006: 48-54).

Terörizmle mücadelede istihbaratın kullanılması amaçları arasında mücadelenin dięer araçlarını desteklemek de bulunmaktadır. Örneęin diplomasi çerçevesinde istihbarat,

terörizmle mücadele eden diğer devletlerin iş birliği için ikna edilmesine ve bu devletlerle bilgi paylaşılmasına katkı sağlamaktadır. Terörizmle mücadelede askeri kuvvet kullanımına karar verildiğinde istihbarat, terör hedeflerine düzenlenecek operasyonlar için bilgi temin etmektedir. Terörizmle mücadelede kolluk kuvvetleri için ise istihbarat; faillerin yakalanması, terör eylemlerine ön ayak olanların takip edilmesi kapsamında bilgi temin etmektedir (Pillar, 2004: 118-119).

1.5.2. Terörizmle mücadelede istihbaratın önemi

Spartalıların askeri mesajlarını şifrelemek için sarmal şifreleme cihazı (scytale)¹³ kullanmalarından, II'nci Dünya Savaşı'nda kullanılan daha gelişmiş şifreleme sistemlerine kadar istihbarat; hem savaşta hem de savaşın önlenmesinde önemli bir rol oynamıştır. İçinde bulunduğumuz bilgisayar teknolojileri ve terörizm çağında ise istihbarat, her zamankinden daha önemli bir hale gelmiştir (Koshland, 1995: 311).

Terörizme karşı önleyici tedbirler almak, ön alıcı operasyonlar düzenlemek, terör eylemleriyle başa çıkabilmek, terör örgütü mensuplarını yargı önüne çıkartabilmek maksadıyla istihbarat oldukça önemli bir yere sahiptir (Wardlaw, 1989: 131). Ayrıca, önleyici tedbirleri ve ön alıcı operasyonları planlamak, terörizmle mücadele operasyonları düzenlemek maksadıyla güncel ve doğru bir istihbarat hayati öneme sahiptir (Wardlaw, 1989: 145).

İstihbarat ve karşı istihbarat, terörizmle mücadelede savunmanın birinci safhasında, en önde yer almaktadır. İyi planlanmış, sistematik, çok kaynaklı istihbarat (all source intelligence) ve karşı istihbarat faaliyetleri terörizmle mücadele için oldukça önemlidir. Terörizmle mücadelede istihbarat ve karşı istihbaratın rolü; terörizm tehdidini ortaya koymak, erken ikaz sağlamak, kritik istihbaratı kullanılabilir bir formda kullanıcılara dağıtmaktır (US Army Joint Chiefs of Staff, 1998: V-1).

Gelecekte meydana gelebilecek olası terör olaylarını tahmin edebilmek maksadıyla istihbarat, terörizmle mücadelede en önemli rolü oynamaktadır. Bu nedenle istihbarat, terörizmle mücadelede ilk savunma hattını teşkil etmektedir. Terörizmle mücadelede istihbarat, kolluk kuvvetlerinin faaliyetlerine yön verebilmekte ve askeri operasyonların kapsamını belirleyebilmektedir (Flavius-Cristian ve Andreea, 2013: 2-5).

¹³ Sarmal şifreleme cihazı (scytale) hakkında ayrıntılı bilgi için bkz: <https://www.sibervatan.org/makale/scytale-sifreleme/19>.

Gelecekte de bir güvenlik tehdidi olmaya devam edecek olan terörizm ile mücadele kapsamında istihbarat; terörizmin taktik etkilerini ve stratejik önemini azaltmada oldukça önemli bir araçtır (Karmon, 2002: 119). 21'nci yüzyılda terörizmle mücadelede istihbarat görevi en zor görevlerden birisidir (Karmon, 2002: 139).

Terörizm gibi sürprizlere dayalı olgularla baş edebilmenin ilk koşulu, profesyonel ve kaliteli bir istihbarat örgütüne sahip olmaktır. Terörizmle mücadelede istihbarat fonksiyonu terörizmle mücadele gayretlerinin büyük kısmını karşılayacak kadar önemlidir (Özcan, 2016).

Terörizmle mücadelede birincil koşul terör örgütü mensuplarını bulmaktır. Terör örgütü mensuplarını bulmak için ise iyi bir istihbarata mutlak suretle ihtiyaç duyulmaktadır. Bu nedenle terörizmle mücadelede istihbaratın rolü çok önemli görülmektedir (Kruys, 2007: 83-99).

ABD Genelkurmay Başkanlığının “Anti Terörizm” adlı yayınına göre terörizmle mücadelede; zamanında, doğru ve amacına uygun temin edilen istihbarat oldukça önemlidir. Muhtemel terör hedefleri, terör örgütlerinin yetenekleri, terör örgütlerinin planları ve niyetleri, yeni eğilimleri, eylemin büyüklüğü ile muhtemel eylem tarzlarının belirlenmesi ve değerlendirilmesi açısından terörizmle mücadelede istihbarata gerek duyulmaktadır (US Army Joint Chiefs of Staff, 2014: III-1).

Terörizmle mücadelede istihbaratın görevi; terör eylemleri gerçekleşmeden önce eylem planlarını açığa çıkarmaktır (Pillar, 2004: 116). Bununla birlikte terörizmle mücadelede istihbarat, yalnızca terör eylemlerini önlemekte değil aynı zamanda terör örgütünün işleyiş tarzını anlamak ve karar alma mekanizmalarının nasıl etki altına alınacağını ortaya koymak için de önem taşımaktadır (Crenshaw, 1999: 1-11).

Terör örgütleri gibi hücreler şeklinde teşkilatlanmış gizli yer altı örgütleriyle mücadelede en önemli araç istihbarattır. Çok dikkatli teşkilatlanmış terör örgütlerinde dahi yer altından yer üstüne çıkma ihtiyacı mevcuttur. Barınma, ulaştırma, para, doküman, silah, patlayıcı, iletişim gibi ihtiyaçlar terör örgütü mensuplarının sahada iz bırakmalarına neden olmaktadır (Schmid, 2004: 233). Terör örgütlerinin bir takım ihtiyaçlarını karşılama zorunluluklarından yola çıkarak terör örgütü faaliyetleriyle ilgili istihbarat toplamak da mümkün olmaktadır.

Terörizmle mücadelede yapılan hataları inceleyen bir çalışmada, geleneksel istihbarata göre terörizmle mücadele istihbaratının oldukça zor olduğu, terörizmle

mücadele istihbaratının temel sorununun insan istihbaratı eksikliği olduğu da vurgulanmaktadır (Dahl, 2005: 33-36).

Terörizmle mücadele kapsamında yapılan başka bir çalışmada, mücadelede kullanılan yöntemlerin hangisinin daha önemli ve etkili olduğunu araştırmak için bir grup uzmana “Uluslararası terörizmle mücadelede alınan en etkin tedbir hangisidir?” şeklinde bir soru yöneltilmiştir. Soruya verilen cevaplar arasında birinci sıradaki cevap “istihbarat”, ikinci sıradaki cevap “iş birliği”, üçüncü cevap ise “terör örgütlerinin finans kaynaklarının kesilmesi” şeklinde olmuştur (Schmid, 2011: 29).

Terörizmle mücadelede istihbarat; terör örgütü faaliyetleri hakkında mümkün olduğu kadar çok bilgi toplamak ve böylece muhtemel terör eylemlerini, dolayısıyla da terör eylemlerinden kaynaklı can kayıplarını azaltmada çok önemli bir role sahiptir. Bununla birlikte, en iyi istihbarat teşkilatlarının dahi tüm terör olaylarını ve can kayıplarını önleyemeyebileceği, bütün çabalara rağmen bazı terör eylemlerinin gerçekleşebileceği görülmektedir (Pillar, 2004: 116).

Terörizmle mücadelede istihbarat, terörizmin sürpriz etkisini önlemek ya da azaltmak için de oldukça önemlidir. Sayılarının azlığı, gücünün zayıflığı nedeniyle terör örgütleri için sürpriz stratejisini kullanmak bir zorunluluktur. Terörizmin sürpriz etkisini ortadan kaldırmak için terör eylemlerine yönelik eylem ikazları yapılmalıdır. Ancak eylemlerden önce yapılan istihbarat ikazları çok fazla yapıldığında “yalancı çoban sendromuna”¹⁴ neden olabilmektedir (Crenshaw, 1987: 14).

Sürpriz, “başarılı” bir terör saldırısında en önemli unsurdur. Terör örgütleri güvenlik güçlerinin potansiyel olarak kendilerinden daha büyük olan gücünü etkisiz hale getirmek için saldırının zamanını, yerini ve koşullarını kendileri belirlemektedirler. Dolayısıyla, terör eylemleri gerçekleşmeden önce engelleme, terörizmle mücadelenin anahtar unsuru haline gelmektedir. Terörizmle mücadelede istihbarat; terör örgütlerinin faaliyetleri, barınakları, teçhizatları ve terör örgütüne destek verenler hakkında, zamanında, doğru bilgi sağlamaya çalışmaktadır (Kerstetter, 1979: 109).

Terörizmle mücadelede istihbarat; stratejik ve taktik istihbarat şeklinde iki ana başlık altında incelenebilmektedir. Terörizmle mücadelede stratejik istihbarat; terör örgütlerinin muhtemel hareket tarzları, hassasiyetleri, imkân ve kabiliyetleri, sınırlılıkları, niyetleri, düşünce biçimleriyle ilgilenmektedir. Terörizmle mücadelede stratejik istihbarat ulusal

¹⁴ Yazar bu tabiri “cry-wolf syndrome” şeklinde kullanmıştır.

güvenlik tedbirlerinin alınması, terörizmle mücadele politikalarının belirlenmesinde ve askeri operasyonların icrasında kullanılmaktadır (Kruys, 2007: 89). Terörizmle mücadelede taktik istihbarat ise; terör eyleminin hedefleri, eylemin zamanlaması ve terör eyleminin tekniğiyle ilgilenmektedir (Kruys, 2007: 92).

Terörizmle mücadele kapsamında taktik istihbarat; terör eylemleri öncesi ikazda bulunmak, operasyon düzenlemek ve ceza adalet sistemi için üretilmektedir. Terörizmle mücadelede taktik istihbaratın amacı; terör eylemi gerçekleşmeden önce bu eylemi kimin, ne zaman ve nerede yapabileceği gibi sorulara cevap bulabilmektir (Özcan, 2016).

Terörizmle mücadelede stratejik istihbarat, uzun vadeli planlama ve terör örgütünün operasyonel yetenekleri, siyasi değerlendirmeleri konularını öğrenmek için kullanılırken, taktik istihbarat daha kısa vadeli, yakın geleceği ilgilendiren hususları tespit için kullanılmaktadır. Sahada görev yapan güvenlik görevlilerinin yerel kaynaklardan topladıkları bilgileri zamanında iletmeleriyle gelecekte muhtemel bir terör eylemini tespit etmek, muhtemelen durdurmak mümkün olabilmektedir. Bu nedenle terörizmle mücadelede taktik istihbarat oldukça önemlidir (Hughbank ve Githens, 2010: 32-33).

Stratejik istihbaratla terör örgütlerini destekleyen devletler tespit edilebilmekte, terör örgütlerinin hangi yöntemlerle eylem düzenleyebileceği öngörülebilme, terörizme neden olan sosyal nedenler analiz edilebilmektedir. Taktik istihbarat ise düzenlenecek askeri operasyonların ve terörizmi destekleyen ülkelere yönelik bir harekâtın desteklenmesinde kullanılmaktadır. Taktik istihbarat genel olarak yüksek doğrulukta bilgiye ihtiyaç duyarken, dağıtım safhasında da stratejik istihbarata göre daha hızlı bir dağıtımı gerektirmektedir (Berkowitz, 2002: 293).

Başka bir çalışmada terörizmle mücadele istihbaratı; stratejik, taktik ve psikolojik olmak üzere üç kategoriye ayrılmaktadır. Bunlardan birincisi olan stratejik istihbarat; terör örgütlerinin örgütlenme biçimi, örgütlerin niyetleri ve amaçları, terör örgütlerinin liderleri, hareket tarzları, finans kaynakları, silah ve teçhizatları, yabancı istihbarat teşkilatları dâhil olmak üzere aldıkları dış destek konularıyla ilgilenmektedir (Winkler vd., 2005: 143).

Taktik istihbarat ise terör eylemlerinin engellenmesini sağlayan önleyici ve ikaz edici istihbarattır. Üçüncü istihbarat türü olan psikolojik istihbarat, terör örgütlerinin psikolojik harekât propagandasının ayrıntılarını ve teröristlerle ilgili verileri kapsayan ve devletin onlara karşı kendi psikolojik harekâtını düzenlemesini sağlayan istihbarattır (Winkler vd., 2005: 143).

Taktik istihbarat ile terörizmle mücadelede terör örgütü mensubu olanlarla olmayanların birbirinden ayrılması, terör örgütü hücrelerinin dağıtılması, müteakip istihbarat gayretlerinin yönlendirilmesi ve istihbarat açıklarının kapatılması mümkün olabilmektedir. Stratejik istihbaratla ise ilgili ülkede ve bölgede faaliyet gösteren terör örgütlerinin yeteneklerinin, niyetlerinin açığa çıkarılması, uluslararası terörizmin küresel eğilimleri hakkında karar alıcıların bilgilendirilmesi sağlanabilmektedir (Pillar, 2004: 118).

Terörizmle mücadelede istihbaratın farklı yöntem ve teknikleri bulunmaktadır. Bu çerçevede, sinyal istihbaratı¹⁵, coğrafi istihbarat¹⁶, teknik istihbarat¹⁷, insan istihbaratı¹⁸ ve AKİS¹⁹ gibi farklı disiplinler, terörizmle mücadeleye katkı sağlamaktadırlar (US Army Joint Chiefs of Staff, 2014: III-1). Terörizmle mücadele istihbaratının tüm kaynaklardan faydalanması gerekmekte; insan istihbaratı, teknik istihbarat ve AKİS'ten gelen tüm bilgilerin bir arada eritilerek analiz edilmesi gerekmektedir (Pillar, 2004: 119).

Terörizmle mücadele istihbaratında hedef yalnızca terör örgütü olduğu kabul edilmiş ve ispatlanmış örgütler değil aynı zamanda gelecekte terör eylemleri düzenleyebilecek olanlardır. Ayrıca terörizmle mücadele kapsamında yalnızca bir örgütün terör eylemi düzenlemek istediğini bilmek değil bununla birlikte nerede, nasıl, ne zaman ve kimin eylem düzenleyeceğini de öğrenmek gerekmektedir. Terörizmle mücadelede çeşitli istihbarat toplama yöntemleri içerisinde; insan istihbaratı, sinyal istihbaratı ve görüntü istihbaratından²⁰ faydalanılabilmektedir (Byman, 2013: 5-7).

Terörizmle mücadeledeki başarı, zamanında ve doğru bir istihbaratın varlığına bağlıdır. Terörizmle mücadelede zamanında bilgi sağlamaya yönelik bir yaklaşım, terör örgütlerine sızan insan istihbaratı ile teknik istihbarat yeteneklerini içermektedir. Taktik seviyede kolluk istihbaratını toplamak, terör örgütü faaliyetlerini izlemeye yardımcı olmaktadır. Terörizmle mücadelede istihbarat, karar vericilere gerekli önlemleri

¹⁵ “Hedef devletin muharebe elektronik sistemleri tarafından yayımlanan elektromanyetik enerjinin alınması, kaydedilmesi, değerlendirilmesi ve yorumlanması ile elde edilen istihbarattır” (Özdağ, 2018, s.122).

¹⁶ “Coğrafi istihbarat; savaşma ihtimali var olan bir ülkenin dağları, tepeleri, gölleri, denizleri, tarım durumu ve bütün coğrafi özelliklerinin detayları ile bilinmesi faaliyetidir” (Aköz, 2020, s.34).

¹⁷ “Bir dizi teknik yöntemin kullanılarak istihbarat toplanmasıdır” (Özdağ, 2018, s.121).

¹⁸ “İnsan istihbaratı, eğitilmiş toplayıcılar tarafından, insanlardan ve insanlarla ilişkili kaynaklardan toplanan istihbarat türüdür” (US Army Headquarters, 2006, s.1-4).

¹⁹ “Gazete, dergi, kitap, broşür, veri tabanı, radyo, TV, internet veya ikili görüşmeler ile elde edilenler dâhil olmak üzere kamunun kullanımına açık her türlü veri, haber ve bilgiden elde edilen istihbarattır” (Özdağ, 2018, s.296).

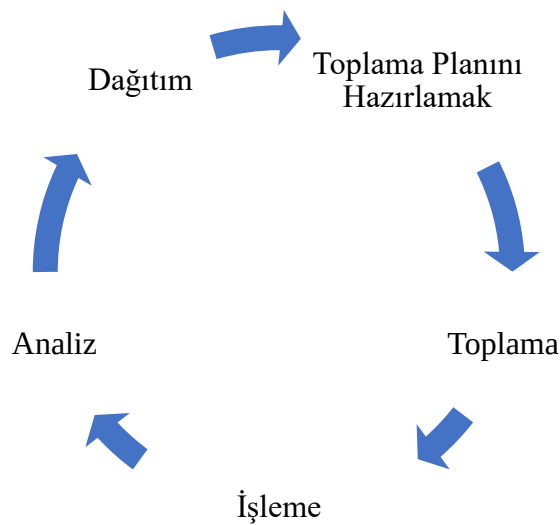
²⁰ “Görüntü istihbaratı; uçaklar ve uydulardan fotoğraf makineleri insanlı/insansız hava araçları, balon ve zeplinler ile çekilen fotoğraflardan elde edilen istihbarattır” (Karaağaç, 2018, s.57).

alabilmeleri maksadıyla; zamanında, açık, kesin, doğru tehdit uyarıları ve değerlendirmeler üretmeye yönlendirilmektedir (Sulc, 1987: 134).

Terörizmle mücadelede istihbaratın en iyi uygulanma şekli, terörizmin etkin olduğu bölgede yaşayan yerel halk içerisinde bir teşkilatın kurulmasıdır. Ancak bunu gerçekleştirebilmek için öncelikle o bölgede yaşayanların güvence altına alınması gerekmektedir. Terörizmle mücadele çerçevesinde bilgi getirecek yerel halk eğitilebileceği gibi eğitilen kişilerden; halkın arasına sızmak isteyen teröristler, terör propagandası yapanlar, terör örgütü için mali kaynak toplayanlar, terör örgütü liderleri hakkında bilgi elde edilebilmesi de mümkündür (Trinquier, 2006: 31-32). Terörizmle mücadelede terörizm faaliyetlerinin yaşandığı coğrafyadaki yerel halk en kıymetli bilgi kaynaklarından birisidir.

Şekil 1.3.'te görülen terörizmle mücadele istihbaratında kullanılan istihbarat süreci incelendiğinde, terörizmle mücadelede de geleneksel istihbarat gibi istihbarat çarkının beş temel basamağa ayrıldığı görülmektedir: istihbarat toplama planını hazırlamak, istihbaratı toplamak, işlemek, bilgiyi analiz etmek ve son olarak istihbaratı dağıtmak. Ancak özellikle toplama basamağı gibi bazı adımlarda yöntem farklılıkları, ilaveler ve çıkarmalar söz konusu olabilmektedir. Örneğin El Kaide neredeyse dünya geneline yayılmış bir terör örgütü olduğundan, örgütle ilgili toplama gayretlerini de bu yayılma doğrultusunda yeniden şekillendirmek gerekmektedir (Byman, 2013: 4-6).

Şekil 1.3. Terörizmle Mücadelede İstihbarat Süreci²¹



²¹ Terörizmle mücadele istihbarat süreci, Byman, D. (2013). The intelligence war on terrorism. Intelligence and National Security, 29(6): 837-863, doi: 10.1080/02684527.2013.851876. makalesinden esinlenerek oluşturulmuştur.

Tarihi süreç içerisinde devletlerin terörizmle mücadeleleri incelendiğinde de, istihbarattan azami derecede faydalandığı görülmektedir. Örneğin, Kuzey İrlanda’da 1969-1998 yılları arasında yaşanan dönemde istihbaratın, terörizmle mücadelede birincil öneme sahip olduğu değerlendirilmektedir. Bu dönemde terörizmle mücadelede yapılan her faaliyetin istihbarata dayanması gerektiği düşünülmüştür. Kuzey İrlanda’da yürütülen mücadelede istihbarat, bizzat sokaklarda görev yapan asker ve polisten elde edilen istihbarata dayandırılmaktadır (Smith ve Dingley, 2009: 551-557).

Kuzey İrlanda örneğinde, başlangıçta oldukça zayıf olan istihbarat birimlerinin sürekli şekilde geliştirildiği, imkân ve kabiliyetlerinin artırıldığı, helikopterlerin havadan gözetleme maksadıyla kullanıldığı, telefon hatlarının dinlendiği de belirtilmektedir. Ayrıca İrlanda Cumhuriyet Ordusunun (Irish Republican Army-IRA) silahlı şiddet eylemlerini bırakıp siyasal alanda faaliyet göstermesi için ikna edilmesinde ve örgütle görüşmelerde en önemli rolü, Birleşik Krallık istihbarat servislerinin oynadığı bilinmektedir (Smith ve Dingley, 2009: 561-565).

İspanya’da ise en yoğun terörizm dönemi, “Bask Anavatanı ve Özgürlük (Euskadi Ta Askatasuna-ETA)” terör örgütünün faaliyet gösterdiği dönem boyunca meydana gelmiştir. 1978-1980 yılları arasında ETA terörizminden kaynaklanan şiddet zirveye ulaşmış, İspanyol hükümeti, ETA ile mücadele maksadıyla iç güvenlik yapısında düzenlemeler yapmaya karar vermiştir. İspanya’nın terörizmle mücadele kapsamındaki bu düzenlemeleri daha çok Savunma Bakanlığı ve “Askeri İstihbarat Örgütü (Centro Superior de Información de la Defensa - CESID)” yapısında yapılan düzenlemelerle ilgili olarak görülmektedir (Celaya, 2009: 11).

CESID esasen, İspanya Savunma Bakanlığına organik olarak bağlı bir askeri istihbarat teşkilatı iken, fonksiyonel olarak hükümet bünyesinde görev yapmıştır. Bununla birlikte CESID, iç güvenlik açısından farklı polis birimleriyle birlikte karşı istihbarat ve terörizmle mücadele konularında çalışmıştır. CESID bu dönemde ETA ile mücadele kapsamında örgütün içerisinde istihbarat elemanları yerleştirme ve telefon dinlemesi gibi faaliyetler yürütmüştür (Celaya, 2009: 11-12).

İspanya’nın terörizmle mücadelesinde istihbarat açısından bir diğer dönüm noktası 2004 yılında Madrid’de düzenlenen terör eylemi olmuştur. 11 Mart 2004 tarihinde düzenlenen bu eylem “Polis İstihbarat (National Police)” ve “Sivil Muhafızlar (Guardia Civil)” teşkilatlarının ihtiyaçları karşılayamadığını açıkça ortaya koymuştur. Bu kapsamda stratejik analiz, bilgi sistemleri ve teknolojileri gibi alanlarda yeni birimler açılmış,

teçhizatlar yenilenmiştir. Polis istihbarat ve sivil muhafızlar teşkilatlarına 1.000 kişilik ilave kadro açılmış, istihbarat ve teknik konularda eğitimler verilmiştir (Reinares, 2009: 371-373).

Sri Lanka'nın terörizmle mücadele stratejisi; diğer devletlerle istihbaratın paylaşımı; Sri Lanka ordusunun etkin bir istihbarat üretmesi ve Sri Lanka'daki terörizm faaliyetlerine yönelik, sürekli istihbarat toplamak üzerine kurulmuştur. Sri Lanka terörizmle mücadelede, terör örgütü liderlerini ve sempatizanlarını ortaya çıkaran operasyonları yürütmek için etkin bir istihbarat toplama ve işleme faaliyeti yürütmüştür. Ayrıca, istihbarat servislerini en üst düzeyde koordine etmek için ulusal bir istihbarat bürosu kurulmuştur. Bununla birlikte Sri Lanka, halka açık yerlerde meydana gelen bombalı saldırılara karşı da istihbarat faaliyetlerini geliştirmiştir (Fabe, 2017: 643-646).

O dönemdeki adıyla Federal Almanya Cumhuriyeti (FAC) de ülkesinde yaklaşık 28 yıl boyunca, Kızıl Ordu Fraksiyonu (Red Army Faction – RAF) terörizmiyle mücadele etmiştir. FAC, RAF ile mücadelesinde; polis ve istihbaratı, özel paramiliter güçleri ve yasal reformları terörizmle mücadele araçları olarak kullanmıştır (Weil, 2017: 129).

RAF ile mücadele kapsamında atılan en önemli adımlardan birisi, 1972 yılında Federal Kriminal Polis Teşkilatına (Bundeskriminalamt - BKA) terörizmle mücadele yetkisi verilmesidir. 1970'lerin sonunda kart indeks sistemi vasıtasıyla 3 milyondan fazla belge ile istihbarat faaliyetlerini yürüten BKA, elindeki bilgileri bir bilgisayar sistemine aktarmış, yakalanan terör örgütü mensuplarını, teröristler ve eylemlerle ilgili bilgileri bu veri tabanına yüklenmiştir. Ayrıca 1977 yılında Ceza Kanunu'nda yapılan değişiklikle BKA'yı şüphelilerin evlerini arama, telefonlarını dinleme ve mektuplarını okuma izni verilmiştir (Weil, 2017: 139).

Bilgisayar veri tabanı RAF terör örgütüyle mücadelede oldukça faydalı olmuştur. 1978 yılında veri tabanının kullanılmaya başlanmasından sonraki altı hafta içinde, on beş terörist bilgisayar veri tabanı sayesinde yakalanmıştır. İstihbarat teşkilatı veri tabanı ve bilgisayar alt yapısı hudut kontrol noktalarına ve havaalanlarına da kurularak sınır geçişleri kontrol altına alınmaya çalışılmıştır (Weil, 2017: 144-145).

Sonuç olarak tezin bu bölümünde; terörizm, terörizmle mücadele ve terörizmle mücadelede istihbarat kavramları irdelenmiştir. Yapılan inceleme sonucunda terörizm kavramına yönelik çok farklı bakış açılarının bulunduğu, bu yaklaşımlardan kaynaklı olarak da farklı tanımlamalar yapıldığı görülmektedir. Tanımlama farklılıklarına rağmen

terörizmin; toplumda korku yaymayı, devlet yönetimlerine kendi istekleri doğrultusunda karar almaları maksadıyla bir takım mesajlar vermeyi hedefleyen, tamamen siyasal bir karakterde hareket eden şiddet eylemleri olduğu anlaşılmaktadır.

Terörizmle mücadele kavramı da tıpkı terörizm gibi farklı bakış açılarıyla şekillenmiştir. Esasen, terörizmle mücadelede farklı bakış açılarını ortaya koymak için bu kavrama verilen farklı isimlere göz atmak yeterlidir. Yabancı alanyazında bu kavram; terörizmle savaş, terörizmle mücadele, karşı terörizm, anti terörizm, terörizme karşı koyma, terörizme müdahale ve terörizme karşı mücadele şeklinde yedi farklı şekilde ifade edilmektedir. Türkçe alanyazında ise terörizmle mücadele ve teröristle mücadele şeklinde iki farklı kavramsallaştırmanın mevcut olduğu görülmektedir.

Terörizmle mücadele kapsamında kullanılan yöntemler de mücadeleye bakış açısına göre farklılıklar göstermektedir. Genel olarak terörizmle mücadele yöntemlerinin; sert ve yumuşak; baskıcı ve uzlaşmacı; tepkisel ve proaktif; proaktif, ön alıcı ve savunmacı yöntemler gibi farklı sınıflandırmalara tabi tutulduğu anlaşılmaktadır. Terörizmle mücadeleye yönelik olarak çok geniş bir yelpazede ve çok sayıda disiplin bulunduğundan, terörizmle mücadele yöntemlerinin sınıflandırılmasında çok sayıda farklı bakış açıları bulunmaktadır.

Terörizmle mücadele araçları da farklı bakış açılara göre tasnif edilmektedir. Terörizmle mücadele yöntemlerinin alt uygulamaları olarak terörizmle mücadele araçları; siyasal tedbirler, diplomasi, ceza adalet sistemi, terörizmin finansmanının önlenmesi, askeri kuvvet kullanımı, örtülü operasyonlar, medya faaliyetleri, uluslararası iş birliği, terör örgütleriyle görüşmeler ve istihbarat şeklinde tasnif edilmektedir.

Terörizmle mücadele aracı olarak istihbarat; terör örgütlerinin nerede konuşlandığını, ne şekilde örgütlendiklerini, nasıl iletişim kurduklarını, finans kaynaklarının neler olduğunu, eylemlerini nasıl planladıklarını tespit etmeye yöneliktir. Ayrıca istihbarat, mahkemelere sunmak üzere suça yönelik bilgi toplamak, terör örgütü taktik ve tekniklerini belirlemek, terör örgütü üyelerini tespit etmek, terör örgütlerinin ikmal faaliyetlerini önlemek, eleman-silah ve finans temin kaynaklarını belirlemek, terör örgütü propagandasını önlemek ve terör saldırılarını önlemek için kullanılması gereken en önemli terörizmle mücadele aracıdır.

Terörizmle mücadelede istihbarat, mücadelenin diğer araçlarını da destekleyen en önemli yardımcı olarak görülmektedir. Örneğin istihbarat, terörizmle mücadele eden diğer

devletlerin iş birliği için ikna edilmesine ve bu devletlerle bilgi paylaşılmasına katkı sağlayarak diplomasi aracını desteklemektedir. Askeri kuvvet kullanımı çerçevesinde istihbarat, terör örgütü hedeflerine düzenlenecek operasyonlar için bilgi temin ederek en büyük desteği vermektedir. Terörizmle mücadelede kolluk kuvvetleri için istihbarat; terör faillerinin yakalanması, terör eylemlerine ön ayak olanların takip edilmesi kapsamında yardımcı olmaktadır. Ayrıca istihbarat terör örgütleriyle görüşmelerde kullanılan bir araçtır. Siyasal ve sosyo-ekonomik araçların daha kolay işlemesi maksadıyla terörizmin kök nedenlerine yönelik bilgi toplanması, halkın terörizme neden destek verdiğinin araştırılması, terör örgütü propagandasının tespit edilmesi konularında istihbarat etkin bir şekilde kullanılabilir.

Terörizmle mücadelede istihbaratın farklı çeşitlerinin kullanıldığı da görülmektedir. Bu kapsamda terörizmle mücadelede; sinyal istihbaratı, coğrafi istihbarat, teknik istihbarat, sinyal istihbaratı, görüntü istihbaratı, insan istihbaratı, AKİS ve sosyal medya istihbaratı gibi istihbarat yöntemleri kullanılmaktadır.

Gözün gördüğü fiziksel verilerin toplanmasıyla başlayıp, sözelin daha ağırlıklı hale geldiği istihbaratın, gelişen teknolojiye paralel olarak artık daha dijital bir hal alacağı görülmektedir. Tarihsel süreçte gelişen istihbarat, iletişim altyapısı ve teknolojilerinin de gelişimiyle birlikte, internet ve özelinde sosyal medyada yer alan büyük boyuttaki verileri kıymetlendirmeye yönelmektedir. Bu çerçevede çalışmanın müteakip bölümünde sosyal medya istihbaratı ve sosyal medya istihbaratının terörizmle mücadelede kullanılması konusu araştırılacaktır.

İKİNCİ BÖLÜM

SOSYAL MEDYA İSTİHBARATI

Tezin ikinci bölümünde amaç; terörizmle mücadele aracı olarak sosyal medya istihbaratını incelemektir. Bu bölümde sosyal medya olgusu incelenecek, terör örgütlerinin sosyal medyayı kullanma amaç ve yöntemleri örnekleriyle ele alınacaktır. Sosyal medyadan elde edilecek verilerin istihbarata dönüştürülmesi ve sosyal medya istihbaratı konusu bu bölümde araştırılacak, sosyal medya istihbaratının terörizmle mücadelede nasıl kullanıldığı, örnekleriyle analiz edilecektir.

2.1. Sosyal Medya

Sosyal medya; insanların birbirleriyle etkileşimde bulundukları, kelimeler, resimler, videolar ve seslerden meydana gelen multimedya (çoklu ortam) karışımını kullanarak, birbirleri ve yaşamları hakkında bilgi paylaştıkları ve/veya tartıştıkları internet siteleri ya da platformlarıdır (McIntyre, 2014: 7).

Sosyal medya kavramı, günümüzde şemsiye bir terim olarak kullanılmaktadır. Esasen bu çatı kavram içerisinde birbirinden farklı işlevlere sahip bir dizi uygulama birlikte bulunmaktadır. Örneğin sosyal medya araçlarından Facebook insanların “arkadaş” ağlarıyla iletişim halinde olmalarına izin vermektedir. Çeşitli anlık mesajlaşma uygulamaları ise daha çok e-posta yerine kullanılan iletişim araçlarıdır. Genel olarak “sosyal medya” terimi, bu farklı uygulamaların farklı işlevlerini gizlemekte, “sosyal” ifadesi kavrama “iş dışı amaçları” ifade eden bir anlam katmaktadır (Treverton ve Miles, 2014: 7).

Sosyal medya²² kavramından ne kastedildiğini daha iyi anlayabilmek için bu kavramla bağlantılı “Web 2.0”²³ ve “Kullanıcı Tarafından Oluşturulan İçerik” (User Generated Content) kavramlarını da açıklamak gerekmektedir. Web 2.0 kavramı ilk olarak 2004 yılında, kullanıcıların interneti kullanım yöntemlerine ilişkin yeni bir boyutu

²² Sosyal medya kavramı yerine “Yeni Medya” kavramı da kullanılabilir. Bu çalışmanın konusu iki kavram arasındaki farkları incelemek olmadığından metin içerisinde bu ayrımın izahı yapılmamıştır. Yeni medya konusunda ayrıntılı bilgi için bkz: Livingstone, S. (1999). *New Media, New Audiences?* New Media & Society, 1(1), 59–66. doi:10.1177/1461444899001001010; Khondker, H. H. (2011). *Role of the New Media in the Arab Spring*. Globalizations, 8(5), 675–679. doi:10.1080/14747731.2011.621287; Friedman, L. ve Friedman, H.. (2008). *The New Media Technologies: Overview and Research Framework*. SSRN Electronic Journal. doi:10.2139/ssrn.1116771.

²³ Sosyal medya yerine “Web 2.0” kavramının da kullanıldığına rastlanılmaktadır. “Web 2.0” kavramı hakkında ayrıntılı bilgi için bkz: Constantinides, E., ve Fountain, S. J. (2008). *Web 2.0: Conceptual foundations and marketing issues*. Journal of direct, data and digital marketing practice, 9(3), ss.231-244; O'reilly, T. (2007). *What is Web 2.0: Design patterns and business models for the next generation of software*. Communications & Strategies, (1), ss.17-37.

tanımlamak için kullanılan bir terimdir. Bu yeni boyut, internetteki içeriklerin kullanıcılar tarafından sürekli olarak üretildiği bir platformu ifade etmektedir (Kaplan ve Haenlein, 2010: 60).

“Kullanıcı Tarafından Oluşturulan İçerik” terimi sosyal medya kullanıcılarınca oluşturulan medya içeriklerini tanımlamaktadır. Bu çerçevede sosyal medya; Web 2.0 dönemiyle ortaya çıkan, kullanıcılar tarafından içerik oluşturulmasına ve içerik alışverişine izin veren internet tabanlı uygulamalardır (Kaplan ve Haenlein, 2010: 61).

Sosyal medya, insanların fikirlerini, kendi hazırladıkları içerikleri ve düşüncelerini çevrimiçi (online) olarak paylaşımlarını sağlamaktadır. Sosyal medya; herkesin içerik oluşturabilmesi, yorum yapabilmesi ve başkalarının içeriklerine katkı sağlayabilmesi açısından “ana akım medyadan” farklılaşmaktadır. Sosyal medya; metinler, sesler, videolar, görseller ve topluluklar biçiminde karşımıza çıkabilmektedir (Scott, 2010: 38).

Sosyal medya, aşağıda sıralanan beş özelliği içeren çevrimiçi medya platformlarıdır.

- Katılım: Sosyal medya, tüm katılımcıların paylaşılan içeriğe katkı sunmasını ve içerikle ilgili yorum yapmasına imkân sağlamaktadır. Bu özelliği ile sosyal medya, medya ve medyayı kullanan izleyici arasındaki sınırları bulanıklaştırmaktadır.

- Açıklık: Sosyal medya araçlarında yayımlanan içerikler genellikle tüm kullanıcıların erişimine açıktır. Bu açıklık sosyal medyada yapılan paylaşımların diğer kullanıcılar tarafından da paylaşılabildiğini, kullanıcıların yapılan paylaşımlara katkı sunabilmesini sağlamaktadır.

- İletişim: Geleneksel medya tek taraflı olup sadece kullanıcıya ulaşmayı hedeflemektedir. Sosyal medya ise kullanıcı ile etkileşime girmeye ve iki taraflı iletişim kurmaya izin vermektedir.

- Topluluk: Sosyal medya araçları sosyal ağların hızlı bir biçimde teşkil edilmesine ve topluluk içinde etkin bir iletişim kurulabilmesine olanak sunmaktadır.

- Bağlantılılık: Sosyal medya araçları, aynı sosyal medya aracında kullanıcıları birbirine bağlar (Mayfield, 2008: 6).

Sosyal medya, kullanıcılara katılımcı bir ortam sağlayan çevrimiçi ve etkileşimli medya türüdür. Sosyal medya, bir kişiden çok sayıda kişiye iletişim modelini (one-to-many communicating), çok sayıda kişiden çok sayıda kişiye etkileşim modeline (many-to-many interacting model) dönüştürmüştür. Bu kapsamda sosyal medya; herkese açık bilgileri

içermesi, katılım, etkileşim, paylaşım ve bağlantılılık gibi özelliklere sahiptir (Jiao vd., 2013: 1095).

Sosyal medya; internet siteleri aracılığıyla toplum tarafından oluşturulan bilgi, deneyim ve bakış açılarının paylaşılmasını sağlayan bir internet alanıdır. Sosyal medya sayesinde, bireyleri birbirinden ayıran coğrafi duvarlar ortadan kalkmış ve yeni çevrimiçi topluluklar ortaya çıkmıştır. Bazı sosyal medya örnekleri arasında bloglar, forumlar, mesaj panoları, resim ve video paylaşım siteleri, kullanıcı tarafından oluşturulan siteler bulunmaktadır. Bu araçların her biri, kullanıcıların fikirlerini iletmelerine yardım etmekte ve benzer düşünen bireyleri birbirine bağlamaktadır (Weinberg, 2009: 1).

Sosyal medya; iletilen içeriğin, bu içeriği kullanan kişiler tarafından üretildiği internet siteleri veya internet tabanlı hizmetler şeklinde tanımlanmaktadır (Bright vd., 2014: 14). Sosyal medya, bir kişinin sosyalleşmesine veya diğer insanlarla içerik, haber, fotoğraf paylaşarak çevrimiçi sosyalleşmesine olanak sağlayan bir medya türüdür. Kullanıcı tarafından oluşturulan içeriklerin oluşturulmasına ve bu içeriklerin bireyler arasında değiş tokuşuna imkân veren, kullanıcılar arasında etkileşimi sağlayan tüm internet tabanlı uygulamalar, sosyal medya olarak sınıflandırılabilir. Bu uygulamalar, sosyal ağ siteleri (Facebook, Friendster, Google Plus), bloglar, internet forumları, konum işaretleme siteleri, çevrimiçi topluluk siteleri şeklinde olabilmektedir (Taprial ve Kanwar, 2012: 8).

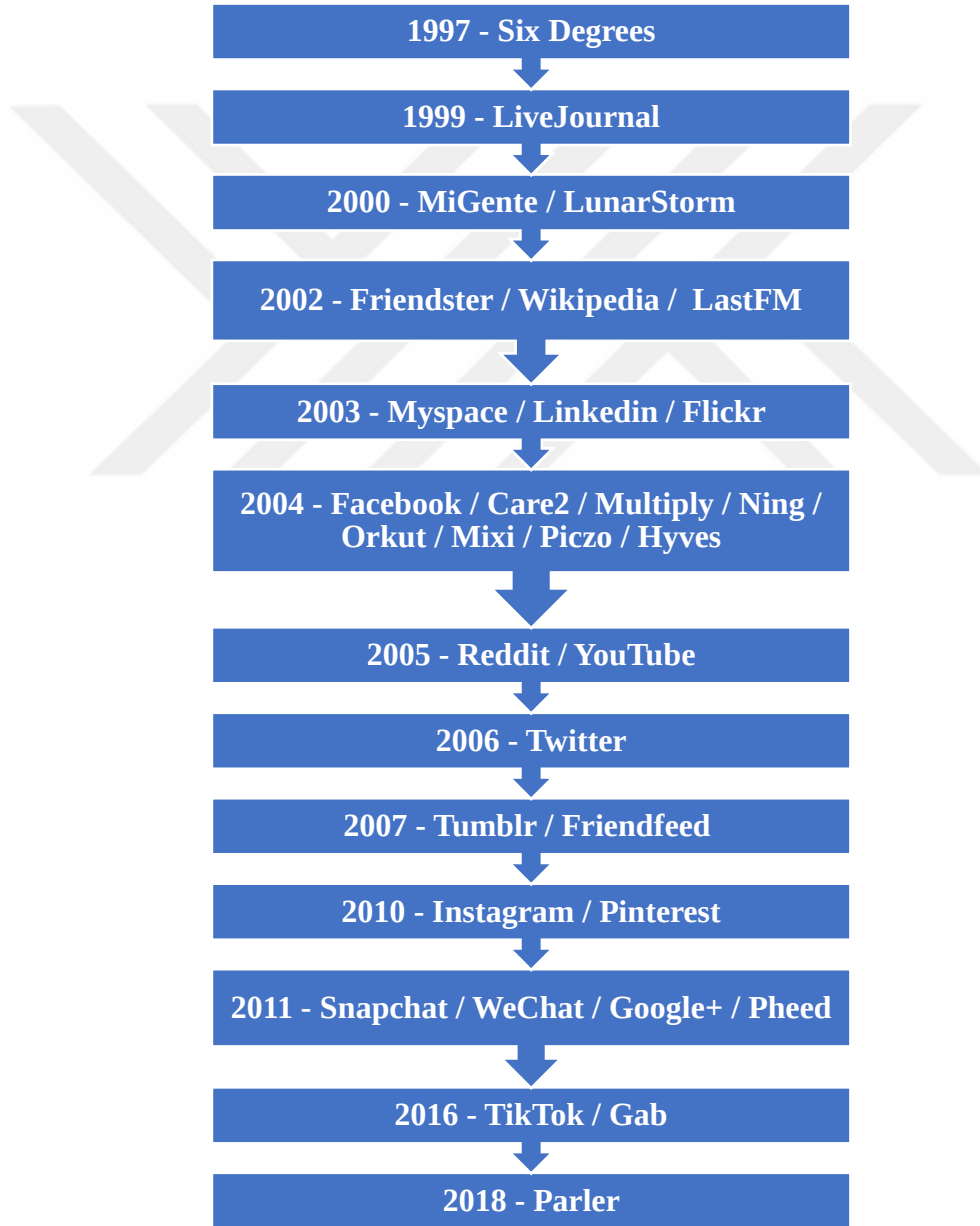
Sosyal medya ve sosyal ağ kavramları birbirine benzer görünen ancak birbirinden farklı kavramlardır. Sosyal medya çatı kavram olup; insanların sosyal bir şekilde çevrimiçi iletişim kurmak için kullandıkları çeşitli medya araçlarına atıfta bulunmaktadır. Sosyal medyada bloglar, wikiler, video ve fotoğraf paylaşımı yapan araçlar gibi çok fazla araç bulunmaktadır. Sosyal ağlar ise sosyal medyanın bir alt kümesi olup, insanların Facebook, Twitter, LinkedIn, MySpace gibi sitelerde birbirleriyle etkileşimde bulunduğunu ifade etmek için kullanılan bir terimdir. Sosyal ağlar; insanların kişisel bir profil oluşturmaları, kendisiyle benzer düşünen bir topluluğunun parçası olmaları ve bu toplulukla bilgi paylaşmak için etkileşimde bulunmaları ile ortaya çıkmaktadır (Scott, 2010: 38).

Sosyal ağ siteleri, kullanıcı tarafından hazırlanan içerikleri, kullanıcıların birbirlerine iletebilmesine imkân tanıyan mikro internet siteleridir. Hazırlanan içerikler, oluşturulan bir arkadaş ağı içerisinde, kişisel profiller, bloglar ve tartışma siteleri aracılığıyla grup üyelerine iletilmektedir. Sosyal ağ siteleri, çok hızlı bir şekilde oluşturulabilmektedir. Bu sitelerin kullanıcılarının gelişmiş okuma ve yazma becerilerine sahip olması

gerekmemektedir. Sosyal ağ sitelerine fotoğraf, müzik ve video eklemek ise oldukça kolaydır (Phillips ve Young, 2009: 26).

Şekil 2.1.'de görüldüğü üzere, ilk sosyal medyanın tarihçesi, 1997 yılında kurulan“SixDegrees.com” isimli internet sayfası ile başlamaktadır. 1997’de başlayan sosyal medya yolculuğu günümüzde de devam etmektedir. Weblog, blog, forum gibi çok sayıda sosyal medya çeşiti ve markası bulunmakla birlikte Şekil 2.1’de söz konusu sosyal medya uygulamalarından kamuoyu tarafından bilinenler sıralanmaya çalışılmıştır.

Şekil 2.1. Sosyal Medyanın Tarihçesi²⁴



²⁴ McFadden, C. (2020). A Chronological History of Social Media. Erişim tarihi: 11 Nisan 2021, <https://interestingengineering.com/a-chronological-history-of-social-media>. kaynağından alınan bilgiler doğrultusunda yazar tarafından oluşturulmuştur.

Sosyal ağ sitelerinin kendilerine has özellikleri mevcuttur. Bu özelliklerden birincisi kullanıcının “profil bilgilerinin” ve “arkadaş” listesinin görüntülenebilir olmasıdır. Profil bilgileri genellikle isim, yaş, mekân, ilgi alanları gibi kullanıcı hakkında bilgileri içermektedir. Sosyal ağ sitelerinde “arkadaş” tanımı; aynı ağ içerisinde birbirleriyle ilişki içerisindeki insanları ifade etmektedir. Bazı sosyal ağ siteleri arkadaş ifadesi yerine “kişiler (contacts)” ya da “tarafatlar (fans)” ifadelerini kullanmakta, bazıları ise “takipçi (followers)” tabirini kullanmaktadır (Boyd ve Ellison, 2007: 211-213).

Bir kişinin, bağlantı kurduğu diğer bireylerin tüm kullanıcılar tarafından görülmesi, sosyal ağ sitelerinin bir diğer önemli özelliğidir. “Arkadaşlar listesi” olarak adlandırılan bu liste, kullanıcının her bir arkadaşının profiline bağlantılar içermekte ve söz konusu arkadaş ağında gezinmeye imkân tanımaktadır. Bir diğer önemli özellik ise sosyal ağ sitelerinde yer alan kullanıcıların arkadaş oldukları kişilerin paylaşımlarına yorum yapmaya ve arkadaşlarla özel olarak mesajlaşmaya izin vermeleridir (Boyd ve Ellison, 2007: 213). Bu özellikler Facebook ve Twitter gibi bazı sosyal medya platformlarında kullanıcı tarafından kısıtlanabilmektedir.

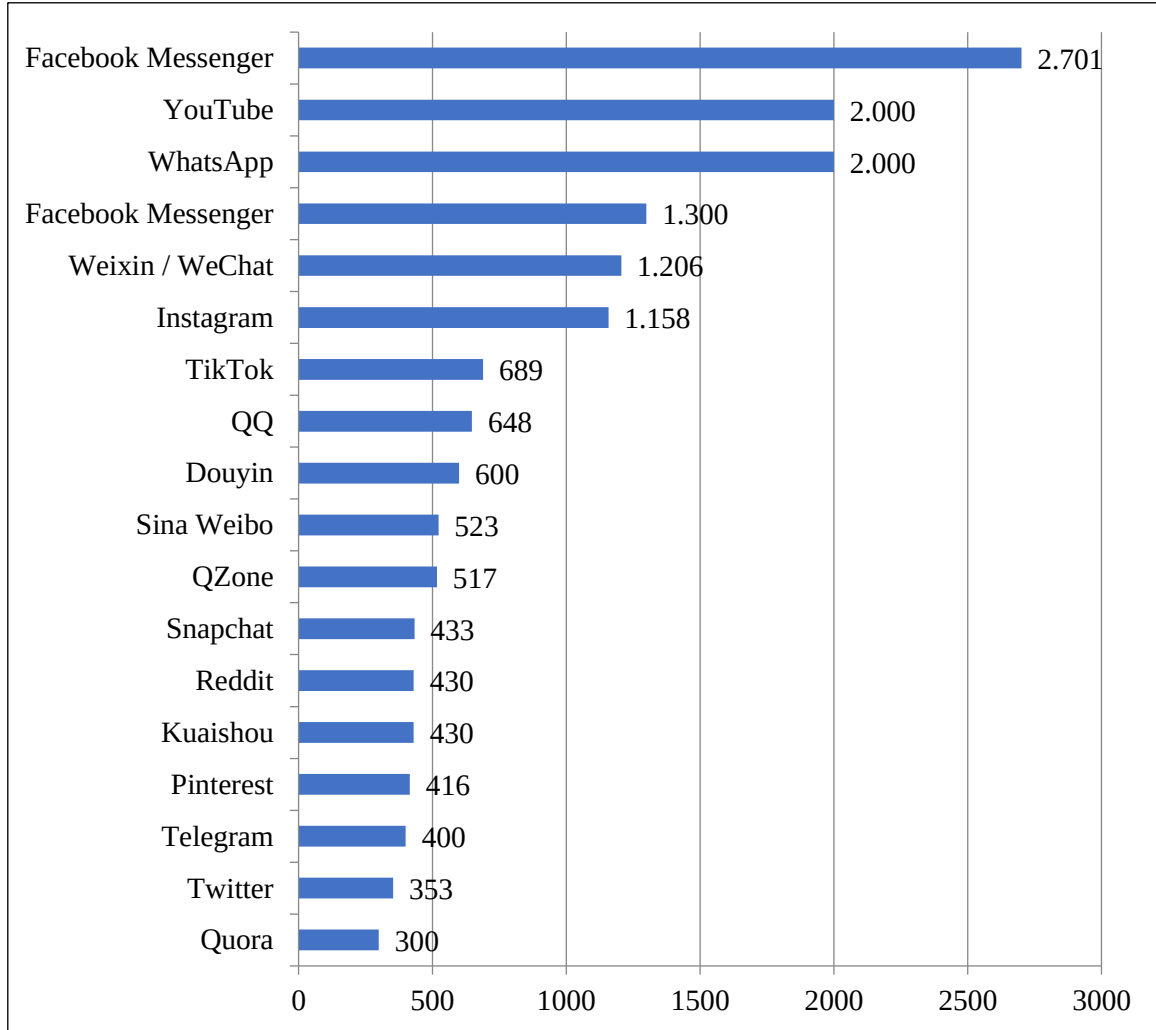
Araştırma kapsamında sosyal ağlar içerisinde seçilen ve bu tezin örneklemini de teşkil eden Twitter, 2006 yılında “Ne yapıyorsun?” sorusuna 140 veya daha az yazı karakteriyle cevap verebilmeyi sağlamak amacıyla oluşturulmuştur. İlk yıllarında Twitter, kullanıcılarının akşam yemeğinde ne yediklerini, nereye gittiklerini, kiminle tanıştıklarını paylaştıkları bir zaman geçirme aracı olarak görülmüştür. Ancak Twitter’ın çok sayıda insanı aynı platform üzerinde ve teknik olarak sorunsuz şekilde bir arada tutabilmesi, Twitter’ın kabul görmesine neden olmuştur. Zaman içerisinde Twitter, bireylerin duygu ve düşüncelerini paylaştığı, neyin önemli olduğunu vurgulamak istediği bir araç haline gelmiştir. Ardından, kanaat önderleri Twitter üzerinden düşüncelerini, kurumlar ise haberlerini paylaşmaya başlamıştır (Weinberg, 2009: 125-126).

Sosyal medya platformlarının önemine değinebilmek için, adı geçen sosyal medya araçlarından önemli görülenlerin kullanıcı sayılarına, Şekil 2.2.’de yer alan verilere göz atmakta fayda görülmektedir. 2020 yılının internet, sosyal medya ve mobil kullanıcı istatistiklerine göre²⁵; dünya üzerinde yaşayan 7,77 milyar insandan 3,81 milyarının sosyal medya kullandığı ve insanların ortalama olarak 2 saat 24 dakikalarını sosyal medya ile

²⁵ Sosyal medya kullanıcısı sayısının 2015 yılında 2 milyar 78 milyon, 2016’da 2 milyar 307 milyon, 2017’de 2 milyar 796 milyon, 2018’de 3 milyar 196 milyon, 2019 yılında 3 milyar 484 milyon olduğu belirtilmektedir.

geçirdikleri ifade edilmektedir. Dünya genelinde en çok kullanılan sosyal medya aracının 2.498.000.000 kullanıcı ile Facebook olduğu, ikinci sırada yaklaşık 2.000.000.000 kullanıcısıyla YouTube ve Whatsapp uygulamasının yer aldığı, üçüncü sırada ise 1.300.000.000 kullanıcılı Facebook Messenger'ın bulunduğu ifade edilmektedir. Aynı verilere göre Twitter'ın ise 339 milyon kullanıcısı bulunmaktadır (We Are Social, 2020).

Şekil 2.2. Sosyal Medya Kullanıcı Miktarları (x1.000) ²⁶



Sonuç olarak sosyal medyayı; bireylerin internet üzerinden çevrimiçi olarak bir araya geldikleri ve kendi ürettikleri içerikleri paylaştıkları platformlar şeklinde tanımlamak mümkündür. Sosyal medyanın bir alt grubunu oluşturan sosyal ağlar ise bireylerin bir profil oluşturarak katıldıkları, kendileri gibi düşünen bir toplulukla etkileşimde bulundukları Facebook, LinkedIn, Twitter gibi internet topluluklarını ifade etmektedir. Sosyal medya; kendine has özellikleri bulunan bir medya çeşidi olarak, internete erişimin

²⁶ Kaynak: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>

giderek daha da kolaylaştığı günümüzde, gün geçtikçe daha da fazla birey tarafından kullanılmaktadır.

Ancak sosyal medya sadece sıradan bireylerin sosyalleşmesi, kendi hazırladıkları içerikleri birbirleriyle paylaşmaları ve iletişim kurmaları maksadıyla kullanılmamaktadır. Paylaşılan içeriklerin çok kısa bir zaman dilimi içerisinde dünyanın diğer ucundaki kullanıcıya ulaşması, her ne kadar profil oluşturulması gerekse de gerçek olmayan profillerin oluşturulmasına imkân tanınması, diğer iletişim araçlarına oranla oldukça ucuz olması nedeniyle sosyal medya, suça bulaşmış bireyler ve suç örgütleri tarafından da kullanılmaktadır. Teknolojinin gelişimi ile birlikte değişen şartlara ayak uyduran terör örgütleri de, bu değişimden faydalanarak sosyal medyayı kullanmaya başlamıştır.

2.2. Terör Örgütlerinin Sosyal Medya Kullanımı

2.2.1. Terör Örgütlerinin İnternet Kullanımı

Terör örgütleri internet aracılığıyla hem bilgi paylaşımı yapmakta hem de bilgi temin etmektedir. Terör örgütleri interneti; propaganda yapmak, örgüt üyelerine ideoloji aşlamak, psikolojik harekât faaliyetleri yürütmek, örgüt üyelerini sosyalleştirmek ve motive etmek, örgüte mali kaynak sağlamak, terör eylemlerine ilişkin taktik, teknik ve talimatları iletmek, terör eylemlerini planlamak ve koordine etmek, örgüte eleman temin etmek maksadıyla kullanmaktadırlar (Cohen-Almagor, 2017: 1-7).

İnternet, terör örgütlerinin terör eylemleri için uzaktan keşif yapmasına, eylemleri koordine etmesine olanak sağlamaktadır. Terör örgütleri interneti, propagandalarını küresel alana yaymak; örgüte yeni elemanlar temin etmek; maddi kaynak toplamak maksadıyla kullanmaktadır. İnternet ayrıca, terör örgütlerinin mesajlarını, kendilerinden oldukça uzaktaki takipçilerine iletmelerine de izin vermektedir. Bu sayede, terör örgütlerinin mesajları daha geniş bir kitleye ulaşabilmekte ve kamuoyunu etkileyebilmektedir (Weimann, 2010: 46).

Terör örgütlerinin, örgüt dışında kalanlara karşı propaganda yapabilmeleri, kendi içlerinde ise iletişim kurabilmeleri açısından internet oldukça etkin bir iletişim aracıdır. Bu örgütler arasında interneti ilk kez kullananlardan birisi 1995 yılında “TamilNet.com” isimli internet sitesini kuran Tamil Kaplanları (LTTE) terör örgütüdür. İlk başlangıçta Sri Lanka devleti tarafından kontrol edilen medyaya alternatif olarak kamuoyunu bilgilendirmek amacıyla kurulan LTTE internet siteleri daha sonra, özellikle diasporadaki Tamillere yönelik propaganda aracına dönüşmüştür. İnterneti oldukça etkin kullanan El Kaide terör

örgütü ise interneti; eleman ve mali kaynak temini, Müslüman kamuoyunun fikirlerini şekillendirme, terör örgütü elemanlarının eğitimi, eylem planlaması maksadıyla kullanmaktadır (Hoffman, 2006: 202-214).

Terör örgütleri; kolay erişilebilmesi, üzerindeki devlet kontrolünün oldukça az olması veya hiç olmaması, dünya geneline yaygın ve büyük bir takipçi kitlesi bulunması, kullanıcının kimliğini gizleyebilmesi, bilginin çok hızlı bir şekilde akması, ucuz olması, çoklu ortam imkânı yaratması, geleneksel medyayı şekillendirebilmesi gibi nedenlerle interneti tercih etmektedirler (Weimann, 2004: 3). Terör örgütü mensupları kendileri için potansiyel terör hedeflerini internetten keşfedebilmektedirler. Teröristler bu araç sayesinde, evlerinden dahi çıkmadan bomba imal eden kişilere ve silah uzmanlarına erişebilmektedirler (Singer ve Brooking, 2018: 79).

2.2.2. Terör Örgütlerinin Sosyal Medya Kullanımı

İnternet sitelerinin büyük çoğunluğu istihbarat servisleri ile kolluk kuvvetleri tarafından hedef alındığından ve takip edildiğinden terör örgütleri de yeni arayışlar içerisine girmeye başladılar. Bu arayışların sonucunda terör örgütlerinin bir kısmı internet siteleri yerine sosyal medyaya yöneldiler (Weimann, 2014: 2).

Terör örgütleri ayrıca, çok daha büyük bir hedef kitleye hitap etmesi ve kullanılmasının daha kolay olması nedeniyle sosyal medyaya geçiş yaptılar. Terör örgütü sempatizanları da bu sayede terörizmle ilgili içeriklere daha kolay erişmeye başladılar (Weimann, 2014: 3-14). 2000 yılının sonlarından itibaren Twitter ve Facebook gibi ana akım sosyal medya platformları, çeşitli terör örgütleri için daha önemli hale gelmeye başlamıştır (Bartlett ve Reynolds, 2015: 12).

Sosyal medya kullanımına geçen terör örgütleri, kendilerini “haydutlar”, “sadistler” şeklinde resmeden geleneksel medyaya artık ihtiyaç duymamaktadırlar. Sosyal medya terör örgütlerine ucuz ve etkili propaganda yetenekleri sunarak, bilginin yayılmasını kolaylaştırmaktadır. Propagandanın ötesinde sosyal medya, yüz yüze ilişkileri tamamlayabilen ve terör örgütlerinin bulundukları bölgeler dışında kalan insanlarla da ilişkiler kurmasını sağlayan ağlar yaratmaktadır (Byman, 2018: 3).

Terör örgütleri; günümüzde daha ucuz, daha kolay, daha hızlı ve etkili bir iletişim yöntemi olduğu için sosyal medya platformlarını tercih etmekte, eleman temin etmek; eğitim vermek; takipçiler, sempatizanlar, örgüte mali destek sağlayanlar ile diğer terör örgütleriyle iletişim kurmak için kullanılmaktadırlar. Terör örgütleri, sosyal medya

platformlarını kullanarak ideolojik düşüncelerini, propagandalarını ve terör eylemlerini dünyaya yaymaktadırlar. Sosyal medya vasıtasıyla terör örgütleri çatışma bölgelerinden yönlendirici tavsiyeler alabilmekte, eğitim kitapçıkları veya videoları temin edebilmektedirler (Hossain, 2015: 136-140).

Terör örgütlerinin sosyal medyayı tercih etmelerinin üç temel nedeni bulunmaktadır. Bunlardan birincisi sosyal medya araçlarının terör örgütlerinin hedef kitleleri arasında oldukça popüler olmasıdır. İkincisi, sosyal medya kanallarının kullanıcı dostu²⁷, güvenilir ve ücretsiz olmasıdır. Üçüncüsü ise insanların internet sitelerini ziyaret etmelerini beklemek yerine terör örgütlerinin sosyal medya aracılığıyla hedef kitlelerine doğrudan ulaşmalarını ve tabir yerindeyse sanal olarak kapılarını çalmalarına imkân vermesidir (Weimann, 2014: 3).

Sosyal medyanın terör örgütlerince kullanımı, üç önemli açıdan güvenlik tehdidi oluşturmaktadır. Birincisi, sosyal medya terör örgütlerinin video, analiz ve yorumlarını yayımlayarak eylemlerinin etkisini artırmalarına izin vermektedir. Sosyal medya, terör örgütlerinin mesajlarını aracı kullanmadan, doğrudan iletmelerine imkân da sağlamaktadır. İkincisi, sosyal medya terör örgütlerine mali kaynak toplama, yeni elemanlar temin etme, propagandalarını yayma ve ideolojilerini daha geniş bir kitleye iletmenin yolunu açmaktadır. Son olarak, terör örgütleri, ideolojilerine karşı savunmasız olabilecek kişileri aramak ve bulmak için sosyal medyayı kullanmakta, böylece eleman temin çabalarını daha etkili hale getirebilmektedirler (Knox, 2014: 300-301).

Terör örgütleri teknoloji odaklı gelişimlerinin bir sonucu olarak sosyal medyayı kullanmaya başlamışlardır. Terör örgütlerine ait internet sitelerinin siber bir müdahaleye uğrama ihtimali mevcut iken sosyal medya sayfalarının böyle bir saldırıya maruz kalması olasılığının bulunmaması terör örgütlerini bu platformları kullanmaya yöneltmiştir. Ayrıca sosyal ağ siteleri terör örgütlerine, anonim içerik üretme, internette ücretsiz olarak barınma imkânı sağlamaktadır. Terör örgütlerinin sosyal medyayı kullanmalarının en önemli nedeni örgüte yeni elemanlar temin etmek üzere bireylerin radikalleşmelerini sağlamaktır (Waskiewicz, 2012: 2).

Kolay erişilebilir olması, devletler tarafından kontrolünün güç olması, küresel çapta bir hedef kitleye sahip olması, sahte hesaplar sayesinde anonim paylaşımlar yapılabilmesi, bilginin çok hızlı bir şekilde yayılmasına izin vermesi, yazı-grafik-ses-video gibi çok

²⁷ Herkes tarafından kolayca kullanılabilen, nasıl kullanılacağı konusunda açıklamaya gerek duyulmayan anlamında kullanılan ifadedir.

sayıda medya unsurunu içerisinde barındırması nedeniyle sosyal medya terör örgütleri için en kullanışlı araçlardan birisi haline gelmiştir. Terör örgütleri sosyal medyayı; eleman temini, eğitim, terör eylemi planlama, siber saldırılar düzenlemek, propaganda ve mali kaynak temini maksadıyla kullanmaktadır (Ishengoma, 2014: 4-5).

Suriye iç savaşı ve DEAŞ'ın yükselişi sırasında internet, terörizm için en çok tercih edilen mali kaynak yaratma alanı haline gelmiştir. İnternet terör örgütleri için “bağış” toplama alanını coğrafi olarak genişletmiştir. Bu bölgede çatışan taraflar; Instagram, Facebook ve YouTube sosyal medya araçlarını kullanarak kendilerine mali kaynak sağlamışlardır (Singer ve Brooking, 2018: 68).

Terör örgütleri; bilgi temin etme, sosyal mühendislik yapma, propaganda yayma, eleman temin etme, sempatizan bulma, psikolojik operasyonlar düzenleme, siber saldırı yapma amaçlarıyla sosyal medyayı kullanabilmektedirler (Bányász, 2018: 52). Terör örgütleri sosyal medyayı; potansiyel terör örgütü mensubu radikallere ulaşmak, grup forumları oluşturmak, terör örgütü sempatizanlarıyla iş birliği yapmak, eğitim ortamı yaratmak, örgütsel faaliyetleri koordine etmek ve terör örgütüne eleman temin etmek maksadıyla kullanmaktadır (Bertram, 2016,s.226).

Sosyal ağ sitelerinin özelliklerinden birisi, YouTube uygulamasında olduğu gibi, sözcükler yerine görüntülerle olayları iletme özelliğidir. Bu özellik, sosyal ağ sitelerini terör örgütleri için en iyi, en güvenli ve en hızlı iletişim aracı haline getirmiştir. Bu özellikleri sayesinde terör örgütleri topluma sirayet etme ve eleman temin etme çabalarını yoğunlaştırmaktadırlar (Al-Danani ve Amor, 2020: 62).

Terör örgütleri, kullanıcı dostu, güvenilir ve ücretsiz olması nedeniyle sosyal medyayı tercih etmektedirler. Terör örgütüne ait bir hesap kapatıldığında yenisinin açılmasının maliyeti hemen hemen yoktur. Örneğin terör örgütleri Facebook'u aşırılık yanlısı sitelere ve diğer “çevrimiçi radikal içeriğe açılan bir kapı” olarak kullanmaktadırlar. Twitter'ın neredeyse gerçek zamanlı işlevselliği teröristlerin iletişim ihtiyaçlarını karşılamalarına da imkân tanımaktadır. YouTube, propaganda videolarını yayınlamak ve yeni eleman temin etmek için bir forum olarak kullanılmaktadır. Terör örgütleri Instagram ve Flickr'ı terör örgütü liderlerini övmek veya rehinelerinin infazlarını göstermek için kullanmaktadırlar. Bu vakaların her birinde, sosyal medya terör örgütlerinin amaçlarına ulaşmaları için suistimal edilmektedir (Wu, 2015: 288-289).

Terör örgütleri en popüler üç sosyal medya sitesi olan Facebook, Twitter ve YouTube'u iletişim kurma, örgütlenme, eleman temin etme ve silahlı eğitim verme amacıyla kullanmaktadırlar. Dahası, terör örgütleri sosyal medyayı mali kaynak toplama amacıyla da tercih etmektedirler (Dean ve Bell, 2012: 10). El Kaide ve DEAŞ terör örgütleri, Twitter, Facebook, Instagram ve YouTube gibi sosyal medya araçlarını bu örgütlere mali kaynak temini ve bağış toplamak maksadıyla kullanmışlardır. Terör örgütleri; silah temin etmek, terör örgütü elemanlarına para ödemek, bulundukları bölgede altyapıyı güçlendirmek, sivil ve sosyal hizmetleri sürdürmek amacıyla insanların dikkatini çekmek ve finansmanı yönlendirmek için sosyal medyayı kullanmaktadırlar. Sosyal medya aracılığıyla toplanan mali kaynak miktarı, petrol satışlarından veya terör örgütü vergilendirmelerinden elde edilen gelirlere kıyasla çok daha az olsa da, El Kaide ve DEAŞ'ın mali kaynak toplayıcıları, sosyal medya tabanlı kampanyalar düzenleyerek milyonlarca dolar gelir elde etmişlerdir (The Camstoll Group, 2016: 2).

Sosyal medya, terör örgütlerine mali kaynak temini ve finansal destek sağlamak amacıyla sıklıkla kullanılmaktadır. Bu kapsamda sosyal medya; bir terör örgütünü desteklemek için finansman çağrı aracı; bir ödeme platformu; bağışçıları ve fon sağlayıcıları belirli bir ödeme platformuna yönlendirme vasıtası; bir terör örgütü için reklam hizmetleri ile gelir sağlama aracı (YouTube videolarından reklam geliri elde etmek vb.); terörizmin finansmanı stratejilerinin paylaşıldığı diğer sitelere yönlendirme aracı olarak işlev görmektedir (Keatinge ve Keen, 2018: 3).

2.2.3. Terör Örgütlerinin Sosyal Medya Kullanımına Örnekler

DEAŞ hem coğrafi hem de dijital olarak bir bölgeyi ele geçiren ilk terör örgütü olmuştur. DEAŞ'ın ele geçirdiği dijital alan DEAŞ propagandasının yapıldığı, DEAŞ terör örgütü mensupları ve sempatizanlarının bir araya gelebildikleri, küresel kamuoyunu izleyip manipüle edebildikleri ve örgütün coğrafi alanı kaybettikten sonra dahi üzerinde varlığını devam ettirebileceği bir alan olarak görülmektedir (Singer ve Brooking, 2018: 151).

DEAŞ oldukça geniş bir propaganda ağı oluşturmuştur. 2016 yılında her biri farklı hedef kitlelere sahip olan ve farklı bölgelerde bulunan, ancak hepsi internetten işletilen yaklaşık elli farklı DEAŞ medya merkezinin faaliyetleri tespit edilmiştir. Bu merkezler, sadece bir aylık bir süre içinde metinden videolara kadar binden fazla DEAŞ açıklaması yapmayı başarmıştır. DEAŞ bir düzineden fazla sosyal medya platformunda ve on binlerce DEAŞ bağlantılı hesap aracılığıyla küresel alana yayılmıştır (Singer ve Brooking, 2018:

151). DEAŞ sosyal medya paylaşımlarıyla, sempatizanlarının “bilgi cihadı” olarak nitelendirdiği, kalpleri ve zihinleri kazanmaya yönelik savaşta etkinliğini kanıtlamıştır. DEAŞ bunu “medya mermileri” olarak adlandırdığı sürekli bir bilgi yağmuruyla, “düşmanın moralini paramparça etmeyi” amaçlayan çevrimiçi içeriklerle yapmıştır (Singer ve Brooking, 2018: 152).

Somali’de faaliyet gösteren Ogaden Ulusal Kurtuluş Cephesi, Tayland’da etkin olan Patani ayrılıkçılar, Kafkasya’daki Çeçen gruplar, İsveç’teki Beyaz Milliyetçiler ve Birleşik Krallık’taki İslamcı aşırılıkçılar; konuşmalarını paylaşmak, videolarını yaymak, politik olaylara tepki vermek, genel olarak propaganda yapmak için Youtube platformunu kullanmaktadırlar. Mücahit Gençlik Hareketi, Mağrip El Kaide’si, Oromo Kurtuluş Cephesi, Nijer Deltası Kurtuluşu Hareketi ve Boko Haram terör örgütleri Twitter profillerini korumaya ve İngilizce içerik paylaşmaya gayret etmektedirler (Bartlett ve Reynolds, 2015: 13).

Facebook; Hizb ut Tahrir, Batı Afrika’da Birlik ve Cihat Hareketi (Mouvement Pour L’Unicité et le Jihad en Afrique de L’Ouest), Bulgar Milliyetçi gruplar, Boko Haram, Avusturyalı Neo-Naziler gibi çok çeşitli örgütler tarafından düzenli olarak kullanılmaktadır. El Kaide ve ona bağlı örgütlerin yanı sıra DEAŞ ve Çeçen aşırılık yanlısı örgütler, propaganda yapmak için Instagram ve Flickr’i kullanmaktadırlar. DEAŞ, Tumblr’i²⁸ Batılı kadınları Suriye ve Irak’ta “cihata çağırmak” için, Ask.FM’i²⁹ ideolojik tartışmalara ev sahipliği yapmak, JustPaste’i³⁰ diğer platformlardan alınan içerikleri barındırmak için kullanmaktadırlar (Bartlett ve Reynolds, 2015: 13).

Aşırılık yanlısı örgütler günümüzde, V Kontakte³¹, Kik³² ve Snapchat³³ gibi daha fazla anonim ve gizliliği artırılmış olan, Batılı ülkelerin kolluk kuvvetleri ile daha az iş birliği yaptığı düşünülen sosyal medya platformlarını kullanmaktadırlar. Örneğin DEAŞ sempatizanlarının Friendica³⁴, V Kontakte ve Quitter³⁵ platformlarını kullandıkları bilinmektedir (Bartlett ve Reynolds, 2015: 15).

²⁸ <https://www.tumblr.com/>

²⁹ <https://ask.fm/>

³⁰ <https://justpaste.it/>

³¹ <https://vk.com/>

³² <https://www.kik.com/>

³³ <https://www.snapchat.com/>

³⁴ <https://friendi.ca/>

³⁵ <https://quitter.se/>

Twitter, propagandayı yaymak ve örgüt içi iletişimi sağlamak maksadıyla terör örgütlerinin kendi tasarladıkları internet sitelerinden ve hatta Facebook'tan bile daha popüler hale gelmiştir. Terör örgütleri, haberlerin gerçek olup olmadığını doğrulamaya ve derinlemesine analize ihtiyaç duymayan son dönem habercilik eğilimi doğrultusunda Twitter'ın yarattığı avantajlardan faydalanmaktadırlar. Buna en çarpıcı örnek 23 Nisan 2013 tarihinde Suriye Elektronik Ordusunun³⁶ (Syrian Electronic Army) bir haber ajansının hesabını ele geçirerek “Beyaz Saray’da patlama, Barack Obama yaralandı” ifadelerine yer verdiği, Şekil 2.3.’de yer alan tweeti atmasına ilişkin olaydır. Bu olayın sonucunda ABD borsasının 136 milyar dolarlık kayba uğradığı da bilinmektedir (Weimann, 2014: 8).

Şekil 2.3. Suriye Elektronik Ordusu Tarafından Yayımlanan Tweet³⁷



Eleman temini maksadıyla DEAŞ öncelikle, internet ve sosyal medyayı kullanarak DEAŞ'ın faaliyetleri hakkında insanların dikkatini çekmeye çalışmıştır. Ardından çatışma alanlarına ulaşmak isteyenler için yönlendirici bilgiler, sosyal medya üzerinden irtibat kurarak verilmiştir. Bir sonraki aşamada potansiyel terör örgütü mensupları ile Twitter ve Facebook üzerinden sohbete başlayarak hem radikalleşmesini sağlamış hem de istihbarat birimlerinin terör örgütüne sızmalarını önlemek için mülakat yapmışlardır (Zgryziewicz, 2016,s.39).

Daha sonraki adım ise sohbeti özel olarak devam edebileceği şifreli platformlardan birine taşımaktır. Bundan sonra ise DEAŞ terör örgütü, örgüte kazandıracağı yeni kişilere

³⁶ 2011 yılında kurulan, Suriye’de Beşar Esad hükümetini destekleyen, internet üzerinden faaliyet gösteren hacker grubudur. Ayrıntılı bilgi için bkz: Warren, M. ve Leitch, S. (2016). The Syrian Electronic Army – a hacktivist group. *Journal of Information, Communication and Ethics in Society*, 14(2), ss.200–212. doi:10.1108/jices-12-2015-0042.

³⁷ Kaynak: Welch, 2013.

özel talimatlar vererek kendisinin örgüte katılmasını sağlamaktadır. Sosyal medyanın terör örgütleri tarafından kullanılmasına yönelik en çarpıcı örnek şüphesiz ki DEAŞ terör örgütü tarafından sosyal medya araçlarının yabancı terörist savaşçıları çatışma alanlarına çağırarak maksadıyla kullanılmasıdır (Zgryziewicz, 2016: 40).

Terör örgütleri tarafından sosyal medya araçlarından Twitter'ın kullanımına verilebilecek bir diğer örnek El Şebab terör örgütünün 2013 yılında Kenya'nın Nairobi şehrinde bulunan Westgate isimli alışveriş merkezine düzenlediği eyleme ilişkindir. Bu eylemde El Şebab Şekil 2.4.'te görülen Twitter mesajı ile eylemi üstlenmiştir. El Şebab, terör saldırısını haklı göstermeye çalışan ve tehditler üreten Twitter içeriklerini gün boyunca gerçek zamanlı olarak yaymaya devam etmiştir (Fassrainer, 2020: 86).

Şekil 2.4. El Şebab Tarafından Yayımlanan Tweetler³⁸



³⁸ Kaynak: Fassrainer, 2020, s.87.

Terör örgütleri sosyal medyayı durumsal farkındalıklarını artırmak ve bu sayede kendileri için daha doğru kararlar almak maksadıyla da kullanmaktadır. 26 Kasım 2008’de Hindistan’ın Mumbai şehrinde Leşker-i Tayyibe terör örgütü tarafından düzenlenen eylem süresince terör örgütü mensupları canlı yayın yapan medyayı ve Twitter’ı takip etmişlerdir. Terör örgütü mensupları özellikle Twitter’dan elde ettikleri bilgiler neticesinde daha etkin kararlar alarak dört gün süren terör saldırılarının etkisini artırmışlardır (Oh vd., 2011: 34-41). Bu örnekten yola çıkarak terör örgütlerinin sosyal medyayı bilgi toplamak ve analiz etmek, anlık olaylarla ilgili durumsal farkındalıklarını artırmak üzere kullandıkları sonucuna varılmaktadır.

Terörizmin finansmanı çerçevesinde sosyal medya El Kaide terör örgütü tarafından da sıklıkla kullanılmıştır. Örneğin; Suriye’de iç karışıklıkların başladığı ilk yıllarda Twitter vasıtasıyla yapılan bağış kampanyalarında; “bir mücahidin silah, hücum yeleği, askeri kıyafet ve askeri bot ile teçhiz edilmesi için 2.500 ABD Dolarına ihtiyaç duyulduğu” mesajları yayımlanmıştır. “Paranızla Cihat Yapın” isimli sosyal medya kampanyalarıyla insanları “cihat” için para bağışlamaya çağıran terör örgütleri, bireylerin nasıl para yatıracaklarına ilişkin bilgi almak isteyenlerin mesajla kendilerine ulaşmalarını istemişlerdir (Keatinge ve Keen, 2018: 10-11).

ABD İç Güvenlik Bakanlığının bir çalışmasına göre, terör örgütleri Facebook uygulamasını; patlayıcı hazırlamak; AK-47 piyade tüfeğinin bakımı ve taktik kullanımı gibi eyleme yönelik bilgiler paylaşmak; radikal internet sitelerine erişimi sağlamak; terör propagandası ve aşırılık yanlısı mesajları iletmek; terör eylemleri için seçilen hedeflere yönelik keşif yapmak maksadıyla kullanmaktadırlar (Department of Homeland Security, 2010).

Terör örgütleri tarafından sosyal medyanın kullanımı muhtemelen daha da yaygınlaşarak devam edecektir. Twister³⁹, BitChirp ve Bitmessage⁴⁰ gibi gizliliği artırılmış sosyal medya platformlarının geliştirilmesi, aşırılık yanlıları tarafından kullanılmaktadır. Örneğin, özel sunucularda çalışan ve bir merkezi olmayan Diaspora⁴¹ isimli sosyal medya platformunun din motifli örgütler tarafından kullanıldığı bilinmektedir (Bartlett ve Reynolds, 2015: 15-16).

³⁹ <http://twister.net.co/>

⁴⁰ <https://github.com/Bitmessage/PyBitmessage/releases/>

⁴¹ <https://github.com/diaspora/diaspora/releases>

Sosyal medyanın terör örgütlerince kullanımına verilebilecek en çarpıcı örneklerden bir diğeri de PKK/PYD terör örgütü tarafından Facebook'un eleman temini maksadıyla kullanılmasıdır. DEAŞ terör örgütünün Suriye'deki eylemlerinin artış göstermesinin ardından PKK/PYD terör örgütü tarafından Facebook'da açılan ve Şekil 2.5.'te görülen "The Lions of Rojava" sayfası 20.000'den fazla takipçiye sahip olmuştur. Söz konusu Facebook sayfasını takip eden çok sayıda batılı ülke vatandaşının Suriye'ye ulaşarak DEAŞ'la mücadele etmek adına PKK/PYD terör örgütüne katıldığı bilinmektedir (Taylor, 2014).

Şekil 2.5. "The Lions of Rojava" Facebook Sayfası Görüntüsü ⁴²



Sonuç olarak, terör örgütleri sosyal medyayı farklı amaçlar için kullanmaktadır. Sosyal medya araçları kolay erişilebilir olmaları, mobil olarak kullanım imkânı vermesi, çok sayıda bireye çok kısa bir zaman dilimi içerisinde ulaşabilmesi, maliyetinin düşük olması, isimsiz paylaşımlar yapmaya izin vermesi, devlet kontrolünün güç olması, yazı-ses-görsel içerikleri yayımlayabilmesi nedeniyle sosyal medyayı kullanmayı tercih etmektedirler.

Sosyal medyanın bu özelliklerinden fayda sağlayan terör örgütleri sosyal medya vasıtasıyla terör örgütünün fikirlerini yaymaya, propaganda yapmaya, bireyleri

⁴² Kaynak: Taylor, 2014.

radikalleştirerek terör örgütüne eleman temin etmeye çalışmaktadırlar. Terör örgütleri ayrıca sosyal medya sayesinde bilgi toplamakta, durumsal farkındalıklarını artırmakta, terör örgütü mensuplarına eğitim vermekte ve mali kaynak toplamaktadırlar.

Terör örgütlerinin sosyal medyayı kullanmalarına karşılık olarak devletler de sosyal medya kullanımından kaynaklanan tehditleri en aza indirmek için yeni terörizmle mücadele yöntemleri geliştirmektedirler. Sosyal medyanın dünya genelinde hızla yayılması ve terör örgütlerinin bu yenilikten faydalanması üzerine güvenlik güçleri de bu alanda terör örgütleriyle mücadele etmeye başlamışlardır. Terörizmle mücadele kapsamında güvenlik güçleri bir yandan terör örgütü sempatzanı sosyal medya hesaplarını takip altına alırken, diğer yandan sosyal medya platformlarından istihbarat elde etmektedirler.

2.3. Sosyal Medya İstihbaratı

2.3.1. Sosyal Medya İstihbaratının Yeri

Sosyal medya uygulamalarının, tıpkı internet siteleri gibi internet üzerinde faaliyet göstermeleri nedeniyle, açık kaynaklar kapsamında olup olmadıkları, buradan hareketle de sosyal medyadan elde edilen verilerle üretilen istihbaratın AKİS kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin tartışmalar devam etmektedir.

AKİS herkesin talep ederek, satın alarak veya gözlemleyerek, yasal yollardan elde edebileceği, kamuya açık verilerden sağlanan istihbarat olarak tanımlanmaktadır. Sosyal Medya İstihbaratının (SOMİS) kamuya açık bilgilerden üretildiği, dolayısıyla özünde AKİS'in bir parçası olduğu ifade edilmektedir (Antonius ve Rich, 2013: 45). Açık kaynak verisi kavramından, açık toplama yöntemleriyle elde edilebilecek her türlü bilgi kastedilmektedir. Buna göre her türlü medya, devlet raporu, belge, bilimsel araştırma raporu ve internetten elde edilen bilgiler bu kapsamda değerlendirilmektedir (Lowenthal, 2004: 273). Açık kaynaklar; gazeteler, dergiler, radyo ve televizyon yayınları gibi halka açık kaynaklar ile daha yaygın olarak sosyal medya ve internet biçiminde tanımlanmaktadır (Akhgar, 2017: 5).

Bu tartışmalar çerçevesinde AKİS'e ilişkin alanyazın incelendiğinde; birçok akademisyen uzman tarafından (Pastor-Galindo, vd., 2020: 10282); (Hobbs vd., 2014: 1); (US Army Headquarters., 2019: 4-8); (Andrei, 2015: 193); (Sampson, 2016: 2); (Trottier, 2015: 530); (Tylutki, 2018: 392); (Ju vd., 2020: 8); (Bean, 2011: 157); (Chauhan ve Panda, 2015: 16); (Agarwal vd., 2015: 21); (Akhgar, 2017: 5) yapılan çalışmalarda, internet

kaynaklarından ve sosyal medyadan elde edilen istihbaratın AKİS içerisinde değerlendirildiği görülmektedir.

(Lowenthal, 2004: 273); (Friedman, 2004: 286); (Gill ve Phythian, 2018: 129); (Shulsky ve Schmitt, 2002: 37); (Steele, 2007: 138) tarafından yapılan çalışmalar ise sadece internet kaynaklarını açık kaynaklar içerisine dâhil etmiş ancak sosyal medyayı bu kapsama almamıştır. Bu iki farklı akademik bakış açısı, sosyal medya verilerinin açık kaynaklar çerçevesinde kabul edilip edilmediğine, sosyal medya verilerinden elde edilen istihbaratın AKİS içerisinde kabul edilip edilmeyeceğine yönelik genel bir kanaat bulunmadığına işaret etmektedir.

2.3.2. Sosyal Medya İstihbaratı

Son zamanlarda sosyal medya kullanımındaki hızlı büyüme, SOMİS terimi ile ifade edilebilen bir istihbarat disiplini yaratmaya başlamıştır (Omand, 2013: 139). Sosyal medya; kamuya yönelik hizmetlerin yönetimini iyileştirmek isteyen hükümetler, interneti kötüye kullanan suçluları tespit etmeye çalışan kanun uygulayıcıları, güvenlik için bilgi toplayan istihbarat servisleri için büyük miktarlarda veri üretmektedir (Omand, 2017: 359).

SOMİS, sosyal medyada üretilen verilerin toplanması, analizi ve kullanımı anlamına gelmektedir (Bartlett ve Reynolds, 2015: 27). Daha yalın bir ifadeyle sosyal medyadan elde edilen istihbarata SOMİS denilmektedir (Omand vd., 2012a: 802).

SOMİS, bireylerin ulusal güvenliği etkileyecek davranışlarıyla karakterize edilen durumları tanımlamak ve anlamak maksadıyla sosyal medya verilerine, veri madenciliği tekniği uygulanarak elde edilen istihbarattır (Şuşnea ve Iftene, 2018: 231). Stratejik düzeyde SOMİS, hem krize yol açan örgütlerin düşmanca niyetleri hakkında hem de karar vericiler tarafından kullanılması gereken fırsatlarla ilgili erken ikazlar ve emareler sağlayabilmektedir (Şuşnea ve Iftene, 2018: 239).

Sosyal medya verilerinin toplanması ve kullanılması yoluyla elde edilebilen SOMİS AKİS'in bir alt dalı olduğu ve kamuya açık bilgilerden elde edildiği ifade edilmektedir. (Bartlett ve Reynolds, 2015: 25) SOMİS'te; bireylerin Facebook ve Twitter gibi sosyal medya platformlarına yükledikleri veriler istihbarat amacıyla toplanmaktadır. (Gill ve Phythian, 2018: 129). Bu veriler kolluk kuvvetleri ve devletin diğer güvenlik kurumları tarafından istihbarat gereksinimlerini karşılamak için toplanır, işlenir, analiz edilir ve raporlanır (Antonius ve Rich, 2013: 45). Ancak; yeni, oldukça analitik ve henüz net olarak

anlaşılmamış gibi görünen bir alan olduğundan diğer tüm yeni teknolojiler gibi, SOMİS yeteneğinin de geliştirilmesi bir miktar zaman alacaktır (Mahood, 2014: 3).

SOMİS'in amacı, karar verme mekanizmaları için bilinmeyenleri azaltabilmektir. İstihbarat kurumları, SOMİS'i kullanarak en uygun kararı alabilmeleri için politika yapıcıları ve istihbarat sürecinden yararlanan diğer paydaşları etkileyebilmektedirler. SOMİS aracılığıyla istihbarat kurumları; bireyler veya örgütler için geçerli olabilecek bazı davranış kalıplarını belirleyebilmekte, bu örgütleri daha ayrıntılı tanıyabilmektedir. SOMİS, kriz zamanlarında da gerçek zamanlı bir bilgi kaynağıdır ve kriz yönetiminde önemli bir işleve sahiptir (Ivan vd., 2015: 506).

Mahood (2014) SOMİS'in çok kaynaklı istihbarat çerçevesinde ele alınmasının uygun olacağını dile getirmektedir. İstihbarat çarkını tamamen kapsayan çok disiplinli bir yaklaşımın ürünü olan çok kaynaklı istihbarat; başta insan istihbaratı, sinyal istihbaratı, karşı istihbarat, görüntü istihbaratı, coğrafi istihbarat, füzyon⁴³ (birleştirme) ve analiz gibi alt disiplinleri ve yetenekleri kapsamaktadır (s.3). Ortak, birleştirilmiş, analiz edilmiş bir istihbarat resmi sağlayan çok kaynaklı istihbarat; taktik, operasyonel ve stratejik düzeyde kullanılmaktadır. Günümüzde tam bir istihbarat resmini oluşturabilmek, özellikle SOMİS olmadan mümkün değildir (Mahood, 2014: 4).

Sosyal medyanın sunduğu olanaklar, istihbarat analistine hem bilginin toplanmasında hem de doğrulanmasında yararlı olabilecek çok kaynaklı bir analize ulaşma imkânı sağlamaktadır. İstihbarat kurumlarının SOMİS aracılığıyla topladığı veriler ve bilgiler, diğer istihbarat yöntemlerinin planlanması için bir başlangıç noktası teşkil edebilmektedir (Ivan vd., 2015: 507).

Bazen tek bir sosyal medya ögesi, birden çok istihbarat disiplini için yararlı bilgiler içerebilmektedir. Örneğin, mobil bir cihazdan paylaşılan Facebook gönderisi; bazı metinler, etiketli bir fotoğraf ve coğrafi referanslı üst veriler içerebilmektedir. Verileri göndermek için kullanılan iletişim araçları bir sinyal istihbaratı yeteneği ile analiz edilebilirken, kullanıcının çevrimiçi faaliyetleri ve duyguları insan istihbaratı profiline eklenmek üzere kullanılabilir. Etiketli paylaşımlar ve metin paylaşımları muhtemelen karşı istihbarat, coğrafi konum ise görüntü istihbaratının bir parçası olarak kullanılabilir (Mahood, 2014: 4).

⁴³ Tüm istihbarat gayretlerinin birleştirilerek istihbarat üretimi anlamında kullanılmaktadır.

Çok kaynaklı istihbarat sisteminin avantajlarından birisi, SOMİS'i diğer istihbarat yeteneklerine odaklanmak veya diğer yeteneklere çapraz geçiş yapmak için kullanabilmesidir. Yukarıdaki Facebook örneğini kullanarak; paylaşımdan elde edilen coğrafi konum verileri, insansız hava araçlarının bölgeye yönlendirilmesi için kullanılabilir. Çapraz geçiş zamandan tasarruf sağlarken, verimliliği de artırmaktadır (Mahood, 2014: 4).

Sosyal medyadan elde edilebilecek verileri beş ayrı kategoride toplayabilmek mümkündür. Bunlardan birincisi paylaşımlardır. İnsanlar sosyal medyayı başkaları tarafından da görülebilecek metinler kaleme almak ve bu metinleri toplumla paylaşmak için kullanılmaktadırlar. Twitter kullanıldığında bu paylaşıma “tweet”, Facebook kullanıldığında ise “gönderi” denilmektedir. Paylaşımlar görsel, video veya metin şeklinde olabilirken bunların karışımı da olabilmektedirler. Sosyal medyadan verilerin elde edilebileceği ikinci alan cevaplardır. Cevaplar, başkalarının paylaşımlarına veya cevaplarına karşılık olarak paylaşılan metin, video veya görsel içerikli gönderilerdir (Hassan ve Hijazi, 2018: 206).

Verilerin elde edilebileceği üçüncü alan ise çoklu ortam alanıdır. Sosyal medya platformları kullanıcılarının paylaşımlarına görseller, videolar eklemelerine izin vermektedir. YouTube gibi bazı platformlar ise kullanıcıların video yüklemelerine ve hatta canlı yayın yapmalarına imkân yaratmaktadır. Dördüncü alan üst veri şeklinde isimlendirilen, sosyal medya kullanıcılarının profil bilgilerini, konum bilgilerini, hangi cihazı kullandıklarını, paylaşımın yapıldığı zaman bilgilerini içeren verilerdir. (Hassan ve Hijazi, 2018: 207).

Sosyal medyadan veri elde edilebilecek beşinci alan ise sosyal medyada birbirleriyle iletişime geçenlerin yaratmış olduğu sosyal etkileşim verileridir. Bu kapsamda sosyal medyadan; bireylerin sosyal medyada bulunan arkadaşları, ev arkadaşları, komşuları, aile bireylerini kapsayan sosyal ağlar hakkında bilgi elde etmek mümkün olmaktadır (Hassan ve Hijazi, 2018: 207).

Bu beş temel şekilde toplanan veriler tehdit değerlendirilmesine yardımcı olmak ile düşmanın ya da hedefin imkân ve kabiliyetlerini belirlemek ve maksadını ortaya koyabilmek maksadıyla incelenebilmektedir. Sosyal medyadan toplanan bilgiler, istihbarat resminin oluşumuna yardımcı olmak için diğer istihbarat raporlarıyla karşılaştırılabilmektedir (Mahood, 2014: 5).

Bu yöntemle elde edilen SOMİS genellikle istihbarat resmindeki boşlukları tamamlayan parçalı bilgiler sağlamaktadır. Bu boşluklar genellikle bir istihbarat toplama planının temelini oluşturmaktadır. Örneğin bir hedefe yönelik düzenlenen operasyon sonuçları görüntülere bakarak değerlendirilebilirken, hedef bir lider veya grup olduğunda görüntülere dayalı bir değerlendirmenin faydası olmayacaktır. Bu noktada sosyal medyada yer alan, liderin yerini kimin alabileceğine yönelik haberler SOMİS tarafından değerlendirilerek faydalı bir istihbarat üretilmektedir (Mahood, 2014: 5).

SOMİS, içerik açısından zengin uygulama ortamlarında sosyal medyadan eyleme geçirilebilir istihbarat elde etmeyi, karar alma mekanizmalarına yardımcı olmayı ve “kalabalıkların bilgeliğinden” yararlanabilecek çözüm önerileri sunmayı amaçlamaktadır (Zeng vd., 2010,s.15).

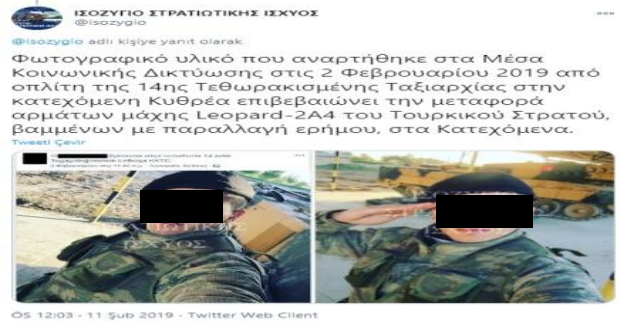
SOMİS, zaman baskısı altında zor kararlar vermek zorunda olanlara sunulan bilgileri güçlendirerek, kamu güvenliğine katkıda bulunabilmektedir. Sosyal medyanın analizi neticesinde, güvenlikle ilgili olarak “olaylar ne zaman meydana geldi”, “şimdi ne oluyor”, “bu olaylar nerede meydana geliyor” ve “olaylar kimleri kapsıyor” sorularına cevap verilebilmektedir. İkinci olarak SOMİS, terörizmden sokak suçlarına kadar gözlemledikleri şekliyle olayların olası nedensel açıklamasını ortaya koyabilmektedir. SOMİS’in üçüncü analiz seviyesi, “sırada ne var” ve “sıradaki olay nerede olacak” sorusuna cevap vermeye çalışan, geleceğe ilişkin tahmin değerlendirmelerini içermektedir (Omand, vd., 2014: 25-26). SOMİS “ne oldu”, “ne zaman oldu”, “kim gerçekleştirdi” sorularına cevap verecek şekilde güvenlik ve kolluk kuvvetlerini bilgilendirerek, durumsal farkındalıklarını artırmaktadır (Omand, vd., 2014: 27).

Son yıllarda, Orta Doğu’da ve Ukrayna’da meydana gelen çatışmalarda sosyal medyanın artan şekilde kullanılması, gelecekte neler olabileceğini düşünmemize neden olmaktadır. Bu düşünce sosyal medyanın istihbarat alanında yeni imkânlar yaratacağını göstermektedir. Örneğin, çatışma alanlarında telefon ile çekilen ve paylaşılan bir özçekim (selfie) fotoğrafından coğrafi konumu öğrenmek ya da fotoğrafın arka planında yer alan coğrafi bir ayrıntıdan, fotoğrafın çekildiği yeri bulmak mümkündür (Treverton ve Miles, 2014: 16).

Örneğin Şekil 2.6’da görülen özçekim fotoğrafı, Kuzey Kıbrıs Türk Cumhuriyetinin (KKTC) Lefkoşa şehrinde görevli bir asker tarafından çekilerek paylaşılmıştır. Fotoğrafı sosyal medyadan alan Rum basını, fotoğrafın arka planındaki tankların Leopard 2-A4

tankları olduğunu tespit etmiş, bu model 42 adet tankın KKTC’de bulunduğuna yönelik iddialarını basına taşımıştır (Süperhaber, 2019).

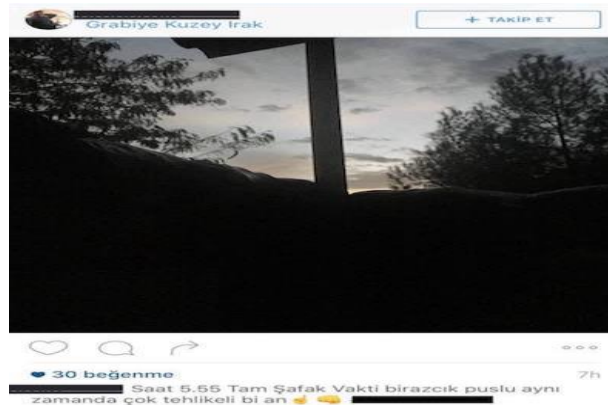
Şekil 2.6. Askeri Personel Tarafından Paylaşılan Özçekim Fotoğrafı⁴⁴



Benzer şekilde ABD ordusu askerleri, 2007 yılında AH-64 taarruz helikopterlerinin Irak’a gelişini kutlamak için cep telefonu ile özçekim fotoğrafı çekmiş ancak fotoğraf çekilirken telefonun coğrafi konum özelliğinin açık olduğunun farkına varmamışlardır. Facebook sosyal ağ platformuna yüklenen fotoğraf terör örgütleri tarafından ele geçirilmiş, fotoğrafın çekildiği mekânın coğrafi koordinatları tespit edilmiş ve bu noktaya havan saldırısı düzenlenmiştir. Saldırı sonucu ABD ordusu dört adet AH-64 taarruz helikopterini aynı noktada kaybetmiştir (Rodewig, 2012).

Bir diğer örnek de Instagram uygulamasından verilebilir. “Saat 5.55 tam şafak vakti. Birazcık puslu aynı zamanda çok tehlikeli bir an” yazısı ile birlikte, Şekil 2.7’de görülen, Instagram’da yapılan bir fotoğraf paylaşımında, paylaşımı yapan asker tarafından konum özelliğinin açık bırakıldığı görülmüştür. Fotoğrafın paylaşıldığı yerin “Grabiye Kuzey Irak” olduğu görülmekte, konum üzerine tıklanıldığında ise Şekil 2.8.’de görülen harita ve paylaşımın yapıldığı konum açılmaktadır (Ergürel, 2015).

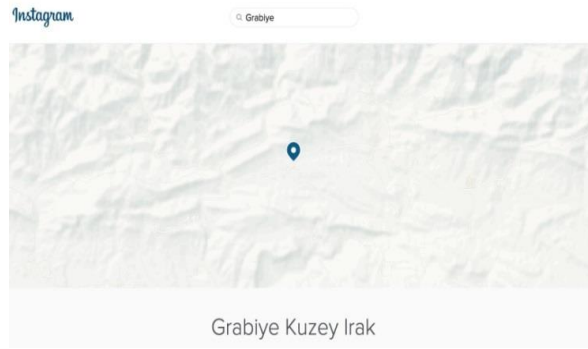
Şekil 2.7. Konum Özelliği Açık Olarak Yapılan Instagram Paylaşımı⁴⁵



⁴⁴ Kaynak: Süperhaber, 2019.

⁴⁵ Kaynak: Ergürel, 2015.

Şekil 2.8. Instagram Paylaşımının Coğrafi Konumunu Gösteren Harita ⁴⁶



SOMİS; güvenlik bağlamında taktik, operasyonel ve stratejik seviyelerde kullanılabilir. Taktik seviyede SOMİS, yetkililerin neredeyse gerçek zamanlı bir durumsal farkındalığa sahip olabilmeleri ve olayların nasıl gelişebileceğini ölçebilmeleri açısından en büyük faydayı sağlamaktadır (Omand, 2017: 361). SOMİS, gerçek zamanlı bir istihbarat toplama yöntemi olup gerek normal gerekse kriz durumlarında devam eden olaylarla ilgili gerçek zamanlı bilgi toplayabilmektedir (Ivan vd., 2015: 506).

Örneğin, önemli bir olay meydana geldiğinde Twitter paylaşım sayılarındaki olağanüstü artış, geleneksel istihbarat kapsamında üretilen raporlardan ve yetkililerin emir komuta zinciri çerçevesinde bilgilendirilmelerinden çok daha önce ve hızlı olacaktır. Asayiş olayları için ve terör saldırıları gibi olayların ardından sosyal medya paylaşımlarındaki artış, paylaşımların yapıldığı konumlarla ilişkilendirildiğinde, bu olayları yönetmekten sorumlu yetkililere bir durum haritası sağlamaktadır (Omand, 2017: 361).

Operasyonel seviyede, özellikle grupların ve ağların iletişim yapılarının ortaya çıkarılması dâhil olmak üzere sosyal medya iletişim modellerinin analizi, örgütlerin hedeflerinin tespit edilebilmesini sağlayabilmektedir. Bu maksatla, büyük hacimli sosyal medya iletişimini analiz etmenin zorluklarını ortadan kaldırmak için bilgisayar tabanlı uygulamalar daha fazla kullanılmaktadır. Stratejik seviyede ise sosyal medyadan elde edilen istihbarat, siyasi gelişmelerin veya yüksek düzeyli tehditlerin ilk işaretlerini sağlayabilmektedir (Omand, 2017: 362-363).

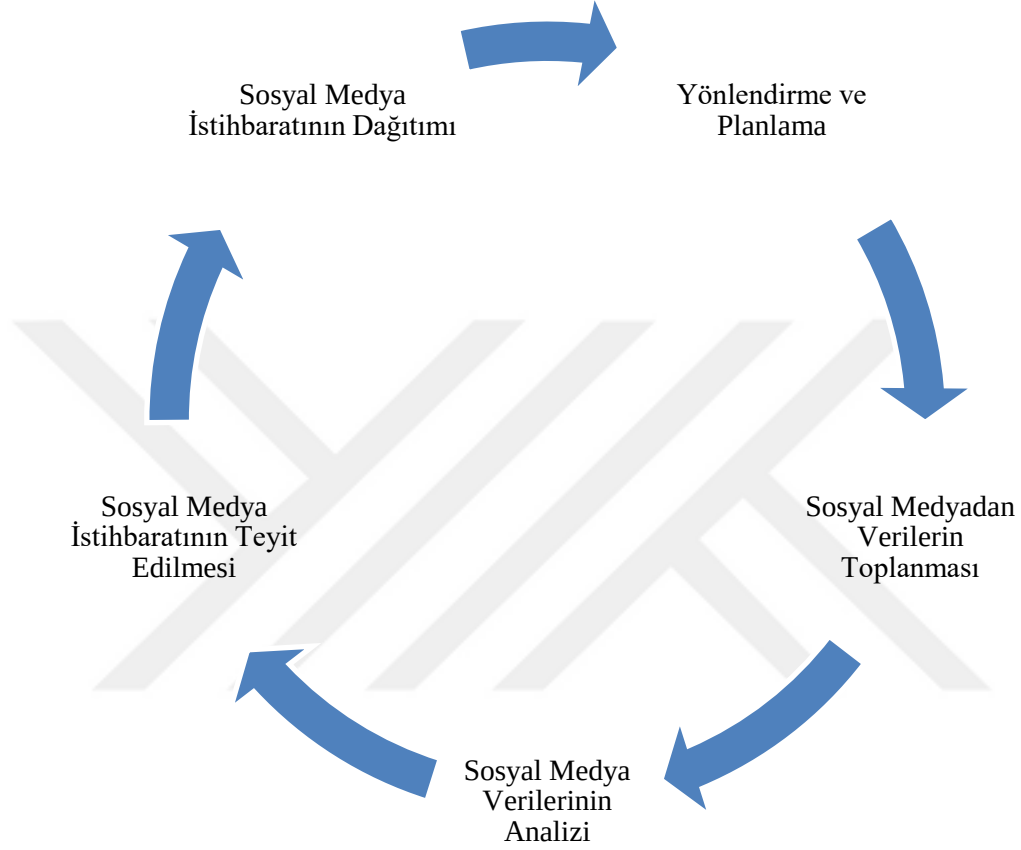
2.3.3. Sosyal Medya İstihbarat Süreci

Diğer istihbarat yöntemlerinde olduğu gibi, veriden istihbarat elde edilmesine kadar uzanan süreç, belirli aşamaları içermektedir. Genellikle yönlendirme, toplama, analiz ve

⁴⁶ Kaynak: Ergürel, 2015.

dağıtım basamaklarını içeren bu süreç, SOMİS için de geçerlidir. Bu kapsamda Şekil 2.9.'da görülen SOMİS süreci; yönlendirme ve planlama, verilerin toplanması, analiz, istihbaratın teyit edilmesi ve dağıtım şeklinde formüle edilmiştir.

Şekil 2.9. SOMİS Süreci⁴⁷



2.3.3.1. Yönlendirme ve planlama

SOMİS yönlendirme ve planlama aşaması, istihbarat sürecinin birinci safhasıdır. Planlama ve yönlendirme, ihtiyaç duyulan veri türlerinin tanımlanması, söz konusu verilerin toplanması için en uygun birimin ve en uygun istihbarat aracının görevlendirilmesini içermektedir (Johnson, 1986: 3). Bütün istihbarat çeşitleri için istihbarat sürecinin birinci basamağı yönlendirme ve planlamadır. Yönlendirme istihbarat açıklarının, bilgi eksikliklerinin tanımlandığı ve istihbarat ihtiyaçlarının belirlendiği safhadır.

Bu safha; istihbarat gereksinimlerinin belirlenmesi ve önceliklendirilmesi, bilgi ihtiyaçlarının belirlenmesi, istihbarat toplama gayretlerinin planlanması, toplama için

⁴⁷ İstihbarat kavramının incelendiği kaynaklarda yer alan hususlar sentezlenerek yazar tarafından oluşturulmuştur.

görevlerin verilmesi ve sürekli bir kontrolün sağlanması aşamalarından oluşmaktadır (UK Ministry of Defence, 2011: 3-6). Bilgi ihtiyaçları ise, istihbarat gereksinimlerini karşılamak için toplanması ve işlenmesi gereken bilgi öğeleridir (UK Ministry of Defence, 2011: 3-7). En basit anlatımıyla istihbarat ihtiyaçları, bir konu hakkında bilmek istediğimiz şeyleri ifade etmektedir.

Diğer istihbarat yöntemlerinde olduğu üzere SOMİS'in yönlendirme ve planlama aşamasında sosyal medyadan elde edilecek istihbarat ihtiyaçlarının neler olduğunun belirlenmesi gerekmektedir. İstihbarat ihtiyaçlarının belirlenmesinin ardından ise hangi ihtiyacın daha öncelikli olduğu tespit edilmeli ve öncelik sırası verilmelidir.

SOMİS planlaması yapılırken belirlenmesi gereken ilk husus hangi sosyal medya platformu kullanılarak ihtiyaç duyulan bilginin temin edileceği olmalıdır. Örneğin, elde edilecek bilginin bir video içeriğinde bulunabileceği düşünülüyor ise SOMİS YouTube platformuna yönlendirilmelidir. Meydana gelen bir olayın analizi bekleniyor ise analistlerin Twitter ya da Facebook platformlarına yönlendirilmesi daha uygun olacaktır.

2.3.3.2. Sosyal medyadan verilerin toplanması

Sosyal medyadan verilerin toplanması, SOMİS sürecinin ikinci safhasıdır. SOMİS çerçevesinde hangi verilere erişilmesi ve hangi verilerin analiz edilmesi gerektiğini bilmek en kritik aşamalardan birisidir. Bu zorluğu aşmanın en etkin yollarından birisi, geleneksel veri toplama yöntemlerinin büyük veri kümeleriyle nasıl başa çıktığını incelemektedir. İstatistikte araştırmacılar, araştırılan kitleyi temsil eden yönetilebilir miktarda veri örneği toplamaktadırlar. Bu örneklem üzerinden yapılan çıkarımların veya analizlerin güvenilirliği ve geçerliliği, örneklem kalitesine, özellikle de temsili olmasına bağlı olarak değişmektedir. Günümüzde genel sorun, sosyal bilimlerin sosyal medya veri setlerini doğru bir şekilde örneklemek için genel bir yaklaşım geliştirmemiş olmasıdır. Bu konuda çok az miktarda çalışma yapılmıştır (Omand vd., 2012b: 52-53).

Sosyal medyadan verilerin toplanmasına yönelik bir diğer yöntem ise veri madenciliğidir (data mining). Geleneksel madencilerin topraktan ve cevherden değerli metalleri çıkarmasına çok benzer şekilde, veri madencileri kolaylıkla görünmeyen ve her zaman kolayca elde edilemeyen bir veri kümesinden anlamlı bilgiler çıkarmaya çalışmaktadırlar. Veri madenciliğini sosyal medyaya uygulamak, insan davranışı ve insan etkileşimi hakkında ilginç bakış açıları sağlayabilmektedir. Veri madenciliği, insanların bir konu hakkındaki görüşlerini daha iyi anlamak, bir topluluğun içerisindeki insan gruplarını

belirlemek, grup içerisinde etkin olan insanları bulmak için kullanılabilir (Barbier ve Liu, 2011: 327-328).

Veri madenciliği, büyük hacim ve farklı tipteki veriden anlamlı bir takım desenler/örüntüler oluşturmayı, veri arasındaki ilişkileri keşfetmeyi ve veriden bilgi elde etmeyi amaçlayan bir alandır. Veri madenciliği, tıpkı bir maden keşfi yapar gibi veri yığınları arasından değerli ve anlamlı bilginin bulunmasını sağlamaktadır (Emre ve Erol, 2017: 163).

Veri madenciliği; “büyük veri tabanlarındaki bilgileri keşfetmek için karmaşık veri arama yeteneklerini kullanmak ve istatistiksel algoritmalarla veriyi işlemek” şeklinde tanımlanmaktadır. Veri madenciliğinin arkasındaki temel fikir; gizlenmiş bir veri kümesinde yeni bilgiler bulmaktır. Veri madenciliği, insanların büyük veri kümelerini daha iyi anlamalarına yardımcı olabilmektedir. Veri madenciliği, makine öğrenimi, bilgi erişimi, istatistikler, veri tabanları ve veri görselleştirme ile doğrudan ilgilidir (Barbier ve Liu, 2011: 329).

Veri madenciliğinde, incelenen sosyal medya türü ne olursa olsun, en anlamlı sonuçların üretilmesinin mümkün olmasını sağlamak için dikkate alınması gereken birkaç temel öge bulunmaktadır. Her sosyal medya türü ve veri madenciliğinin maksadı, farklı yaklaşımlar ve algoritmalar gerektirebilmektedir. Farklı veri kümeleri, farklı türde araçlar gerektirmektedir. Verilerin nasıl organize edilmesi gerektiği biliniyorsa, bir sınıflandırma aracını kullanmak da uygun olabilmektedir (Barbier ve Liu, 2011: 335).

Sosyal medyadan veri toplama; “veri kazıma (scraping)” şeklinde de isimlendirilebilmektedir. Facebook veya Twitter gibi sosyal medya platformlarından veri kazıma yöntemlerinden birisi “Uygulama Programlama Arayüzleri (Application Programming Interface - API)” kullanımıdır (Omand, 2017: 366).

Bu tezin de konusunu teşkil eden Twitter örneğinde API aracılığıyla Twitter verilerine programa dayalı erişim olanağı sunulmaktadır. API’lar bilgisayar programlarının birbirleriyle “konuşma” arayüzü olup API sayesinde birbirlerinden bilgi isteyebilmekte ve bilgiyi temin edebilmektedirler. Twitter API platformu kullanıcıların kamuya paylaşmayı tercih ettiği herkese açık verilerine erişim sağlamaktadır (Twitter, 2020).

Bununla birlikte, Facebook ve Twitter gibi siteler genellikle API kullanıcısının site ile olan ilişkisine bağlı olarak günlük API işlemlerinin sayısını sınırlamaktadırlar. Bazı sosyal medya araçları için, API’leri kullanmadan veri toplamak da mümkündür. Mevcut

sosyal medya verilerinin çok büyük boyutu göz önüne alındığında, tarayıcının topladığı veri miktarını sınırlamak gerekebilmektedir (Barbier ve Liu, 2011: 336).

Sosyal medyadan veri elde etmek amacıyla tasarlanmış çok sayıda internet sitesi ve bilgisayar uygulamasının mevcut olduğu görülmektedir. Örneğin TubeKit⁴⁸ isimli uygulama kullanılarak, YouTube platformunu tarayabilmek, videoların ayrıntıları ve kullanıcı profilleri gibi çeşitli verileri toplamak mümkün olabilmektedir. Socrates⁴⁹ isimli bir diğer uygulama ise sosyal medyanın incelenmesi için kullanılan hesaplamalı bir sistem ve platformdur. Socrates, araştırmacıların bir veya daha fazla sosyal medya kaynağından veri toplayabilecekleri, hipotezler oluşturabilecekleri, elde edilen veriyi analiz ederek istenilen bulgulara ulaşabilecekleri bir sistemdir.

Context Miner⁵⁰; bloglardan, YouTube, Flickr ve Twitter gibi sosyal medya araçlarından ve internet sitelerinden tarama yapabilmekte, bu araçlardan veri, üst veri toplayabilmekte, bu verileri analiz etmekte ve analiz edilen verileri görselleştirerek sunmaktadır.

Sosyal medyadan veri toplamak amacıyla kullanılan uygulamalardan bazıları özel olarak veri elde edilmek istenilen sosyal medya aracı için tasarlanmıştır. Örnek olarak internet tabanlı TweetBeaver⁵¹ uygulaması sosyal medya araçlarından Twitter üzerinden veri toplamaya izin vermektedir. TweetBeaver kullanılarak bir Twitter kullanıcısını takip edenlerin ve kullanıcının takip ettiği kişilerin listesini elde etmek mümkün olmaktadır. Ayrıca TweetBeaver ile bir kişinin Twitter kullanıcı bilgileri, son olarak paylaştığı 3.200 tweet elde edilebilmektedir.

Öte yandan, hem sosyal medyadan veri toplayabilen hem de bu verileri anlamlandırarak görselleştiren uygulamalar da mevcuttur. Bunlardan birisi Network Overview Discovery and Exploration add-in for Excel (NodeXL)⁵² isimli uygulamadır. Bir elektronik tablo uygulaması olan Microsoft Excel çerçevesini kullanan NodeXL, ağ veri kümelerini toplamak, depolamak, analiz etmek, görselleştirmek ve yayınlamak için gereken özellikleri bir arada barındırmaktadır. NodeXL kullanarak; Twitter, Facebook, YouTube, Flickr, Instagram, bloglar, wikiler gibi sosyal medya uygulamalarından veri toplamak mümkün olmaktadır (Himmelboim ve Smith, 2017: 1).

⁴⁸ Uygulamaya <http://www.tubekit.org/> internet adresinden erişilebilmektedir.

⁴⁹ Uygulamaya <https://socrates.peopleanalytics.org/> internet adresinden erişilebilmektedir.

⁵⁰ Uygulamaya <https://contextminer.org/about.php> internet adresinden erişilebilmektedir.

⁵¹ Uygulamaya <https://tweetbeaver.com/index.php> internet adresinden erişilebilmektedir.

⁵² Uygulamaya <https://www.smrfoundation.org/nodexl/features/internet> adresinden erişilebilmektedir.

2.3.3.3. Sosyal medya verilerinin analizi

Sosyal medyadan elde edilen verilerin analizi, SOMİS sürecinin üçüncü safhasıdır. Sosyal medya verileri büyük hacimli veriler olduğundan, verileri otomatik olarak anlamlandırmak için kapsamlı hesaplama yöntemleri geliştirilmiştir. En önemli yaklaşım, algoritmalara bazı kalıpları tanımanın öğretildiği ve yapay zekânın bir çeşidi olan “makine öğrenmesidir”⁵³. Makine öğrenmesinin, büyük veri tabanlarındaki kümeleri ve anormallikleri belirlemekten, metinden anlamsal bilgilerin çıkarılmasına kadar bir dizi önemli uygulaması mevcuttur (Omand vd., 2012b: 55).

Sosyal medya verilerinin analizi maksadıyla sıklıkla kullanılan analiz yöntemleri aşağıdaki gibidir.

2.3.3.3.1. Doğal dil işleme analiz yöntemleri

SOMİS, sosyal medya kullananların motivasyonları da dâhil olmak üzere, incelenen bir olayın ya da olgunun dinamiklerini anlamayı amaçlayan istihbarat analizine de katkı sağlayabilmektedir. Örnek olarak sosyal medya aracılığıyla oluşturulan büyük verinin analizini sağlayan “Doğal Dil İşleme”⁵⁴ (Natural Language Processing - NLP)” yöntemini vermek mümkündür. NLP ile bir konu hakkında paylaşılan tweetlerin “pozitif”, “nötr” ve “negatif” kategorilere ayrılarak, bu konu hakkında kamuoyunun duyarlılığını tespit etmek mümkündür. Bu yöntem, ticari alanda, örneğin pazarlama kampanyalarının etkisini ölçmek için sosyal medyada markalardan nasıl bahsedildiğini izlemek maksadıyla yaygın olarak kullanılmaktadır (Omand, vd., 2014: 29-30).

NLP sosyal medyada mevcut doğal dilin genellikle makine öğrenme yöntemlerini kullanan bir yapay zekâ dalıdır (Bartlett ve Reynolds, 2015: 25). Terörizmle mücadelede, bir terör eyleminin hemen sonrasında veya terör eylemi sırasında kullanılabilen en yararlı SOMİS yöntemi de NLP’dir. Büyük çaplı terör olayları sırasında yine büyük miktarda sosyal medya dolaşımı meydana gelmektedir. NLP, önemli bilgileri yayımlanır

⁵³ Makine öğrenmesi, matematiksel ve istatistiksel yöntemler kullanarak mevcut verilerden çıkarımlar yapan, bu çıkarımlarla bilinmeyene dair tahminlerde bulunan modelleme ve algoritmalarından oluşan yapay zekânın bir alt dalıdır. Makine öğrenmesinin temel amacı, doğru kestirimler yapmaktır. Ayrıntılı bilgi için bkz: Akay, E. Ç. (2018). *Ekonometride yeni bir ufuk: büyük veri ve makine öğrenmesi*. Sosyal Bilimler Araştırma Dergisi, 7(2), ss.41-53.

⁵⁴ Doğal Dil İşleme (Natural Language Processing - NLP) adı verilen bu bilim dalı, genel olarak, dillerin bilgisayar yardımıyla işlenmesi üzerinde çalışmaktadır. Bu çalışmaların sonunda, bir konuşma veya yazının anlaşılması, sorulara yanıt verilmesi ve diller arası çeviriler hedeflenmektedir. Ayrıntılı bilgi için bkz: Adalı, E. (2016). *Doğal Dil İşleme*. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 5 (2), Erişim tarihi: 12 Kasım 2020, <https://dergipark.org.tr/tr/pub/tbbmd/issue/22245/238797>.

yayımlanmaz hızlı ve oldukça doğru bir şekilde tespit edebilmekte, analistlerin bilgiyi temin etmesine ve işlemesine imkân tanımaktadır (Bartlett ve Reynolds, 2015: 27).

NLP, makine öğrenimine dayanmaktadır. En yaygın olarak bu alanda tanınan bir dizi farklı makine öğrenimi yöntemleri, bilgisayarlara belgeleri “sınıflandırmayı” öğretmeyi amaçlamaktadır. SOMİS kapsamında belge; bir tweet veya bir Facebook gönderisidir. Bu kapsamda bilgisayar, belgenin içerdiği metne dayalı olarak belirlenen bir kategoriye bir belge yerleştirmeye çalışmaktadır (Bartlett ve Reynolds, 2015: 34).

NLP’nin terörizmle mücadele çerçevesinde yarattığı operasyonel fırsat, algoritmik modelleri “sınıflandırıcılar” olarak kullanmasıdır. NLP kapsamında, sosyal medya verilerinin her bir parçasını, her bir tweet veya gönderiyi, önceden tanımlanmış kategorilerden birine sınıflandırmak için belirlenmiş algoritmalar uygulanmaktadır. Bu teknolojinin en eski ve en yaygın olarak uygulanan örneği, sınıflandırıcıların, bir sosyal medya verisinin genel olarak “olumlu mu” yoksa “olumsuz mu” olduğuna karar verildiği “duygu analizidir (sentiment analysis)” (Bartlett ve Reynolds, 2015: 35-36).

Duygu analizi, doğal dil işleme alanında, insanların yazdıkları metinlerdeki duygularını, düşüncelerini, değerlendirmelerini, tutumlarını analiz eden bir çalışma alanıdır. Duygu analizi, bir metnin pozitif, nötr veya negatif olup olmadığını belirleme üzerine yapılan çalışma sürecidir (Kırcı ve Gülbak, 2020: 361).

Duygu analizi, Twitter kullanıcılarının siyasi partilere yönelik duygularını ölçmekten gelirlerin geleceğini tahmin etmeye kadar birçok amaç için uygulanabilmektedir (Omand vd., 2012b: 55). Bu yöntem kullanılarak terörizmle mücadele kapsamında sosyal medyadan yapılan paylaşımların tasnif edilmesi, mevcut ortamın tehdit oluşturup oluşturmadığı, kamuoyunun tehdit algılama seviyesinin anlaşılabilmesi ve durumsal farkındalığın artırılması mümkün olmaktadır.

SOMİS tarafından kullanılabilen bir diğer analiz yöntemi ise anlam analizi yöntemidir. Dilbilimin bir parçası olan anlam analizi yoluyla sosyal medya verileri anlamlandırabilmektedir. Anlam analizi; kelimelerden, ifadelerden ve cümlelerden anlam çıkartabilen süreçtir (Mahood, 2014: 14). Anlam analizi, güncel ve yaygın olarak toplumda ele alınan temel konuların, eğilimlerin daha iyi anlaşılmasına yardımcı olmak için bir grupta hâkim olan duyguları araştırmak için kullanılabilir (Evans, 2013: 8).

Anlam analizi bir takım zorlukları da bünyesinde barındırmaktadır. Örneğin, bazı anahtar kelimelerin varlığının tespit edildiği ve izlendiği analizler yanlış yorumlamalara

yol açabilmektedir. Buna örnek olarak “bomba” anahtar kelimesi verilebilmektedir. Bomba kelimesi takip edilirken bir spor kulübünün performansı için “bomba” başlığı atılan bir paylaşım var olmayan bir tehdidin büyük bir tehdit gibi algılanmasına neden olabilmektedir (Mahood, 2014: 14).

Bununla birlikte Twitter gibi sosyal medya platformlarının paylaşım hacmi kısıtlamaları nedeniyle kullanıcıların kendi dillerini yaratmaları ve kısaltmalar kullanmaları da söz konusu olmaktadır. Bunun da ötesinde sosyal medyada çok sayıda dilin, üstelik Latin harfleri dışındaki karakterlerle yazılan farklı dillerin kullanıldığı da bilinmektedir (Mahood, 2014: 14).

NLP sistemlerindeki gelişmeler, sosyal medyadaki hızlı gelişime ayak uydurmuştur. Günümüzde otomatikleştirilmiş NLP işlemcileri, gerçeği düşüncelerden ayırabilmekte, birden çok anlama sahip kelimeleri doğru şekilde anlamlandırabilmektedir. NLP araçları ticari amaçlarla geliştirilmiş olsalar da, bu araçların SOMİS maksatlı kullanımı için büyük bir potansiyel bulunmaktadır. Gerçek ile düşünce arasındaki ayrım, istihbarat açısından kritik öneme sahiptir. Bir kaynağın gerçek olarak algıladığı ile bir kaynağın ne düşündüğü arasındaki farkı bilmek kritik bir istihbarat kabiliyetidir (Mahood, 2014: 14).

2.3.3.3.2. Olay tahmin analizi yöntemi

Sosyal medya; siyasi, kültürel ve ticari nitelikteki olayları içeren bir bilgi platformu olarak görülebilmektedir. Sosyal medyadaki bu bilgiler, meydana gelecek bazı olayların emareleri olabilmektedir. Olay tespit yöntemi, bir olayın meydana gelebileceğini gösteren kelime veya kelime öbeklerinin kullanımının anormal artışlarını gözlemleyerek olayları tespit ve tasnif etmeye çalışmaktadır (Bartlett ve Reynolds, 2015: 41).

Hızla gelişen kaotik olaylar genellikle ilk olarak Twitter’da gündem olmaktadır. İlk bildirimden kısa bir süre sonra da görgü tanıkları bilgi paylaşmaya başladıkça konuyla ilgili paylaşım miktarı aniden artmaktadır. Sosyal medya kullanıcıları, özellikle de Twitter kullanıcıları, bilgi paylaşımı yoluyla olayları önceden tespit etmede bir dizi rol oynayabilmektedir. Bu kişiler, olaylar hakkında ilk elden bilgi üretebilmektedirler (Bartlett ve Reynolds, 2015: 42).

Sosyal medyada üretilen veri miktarının giderek artması sosyal hayatı ölçülebilir ve kaydedilebilir hale getirmektedir. Sosyal medya verileri kullanılarak, seçim sonuçlarından ürün satışlarına kadar bir dizi sosyal olayı tahmin etmeye yönelik ilgi giderek artmaktadır (Bartlett ve Reynolds, 2015: 47).

Terörizmle mücadelenin temel amacı terör saldırılarını önlemektir. Dolayısıyla en önemli başarı kriteri bir terörist saldırıyı planlama aşamasında ortaya çıkarabilme yeteneğidir. Mevcut terörizmle mücadele uygulamalarında, Twitter gibi sosyal ağ sitelerinde çevrimiçi radikalleşmeyi ve terör eylemi öncesi davranışlara ilişkin işaretleri tespit etmeyi amaçlayan araç ve modellerin sayısı gittikçe artmaktadır (Pelzer, 2018: 167-170).

SOMİS, kamu düzeninin bozulmasına neden olabilecek olayları önlemek için kullanılmaktadır. SOMİS vasıtasıyla radikalleşme ve şiddet içeren davranış süreçlerinin izlenebilmesi, öngörülebilmesi ve gelecekteki eğilimlerinin tahmin edilebilmesi mümkün olabilmektedir (Ivan vd., 2015: 506).

Bu kapsamda en sık kullanılan yöntem anahtar kelimeye dayalı arama yaparak, belirli olaylar ve potansiyel tehditlerle ilgili verileri filtreleme yöntemidir. Yaklaşan tehditler konusunda farkındalık yaratmak için algoritma tabanlı araçlar kullanılmaktadır. Tahmine dayalı bilgi üretmek için sosyal medya verilerinin yorumlanması ve istihbarat analistinin riskleri değerlendirme konusundaki takdir yetkisi tahminin temel bileşenleri olmaya devam etmektedir. Bu nedenle makine öğrenmesiyle olayların tahminine yönelik üretilen bilginin analistleri destekleyebileceği ancak analist değerlendirmesi olmaksızın tam olarak bir tahmin üretilmeyeceği görülmektedir (Pelzer, 2018: 175-177).

Gelecekte ne olabileceğini doğru bir şekilde tahmin edebilmek ciddi derecede zor görülmektedir. Bununla birlikte sosyal medya, analitik araçları kullanarak ve gelişen olayları takip ederek, gelecekte meydana gelmesi muhtemel olayları belirlemek için bazı ipuçlarını sağlayabilmektedir. SOMİS, örüntü analizi (pattern analysis) ve anlam analizi (semantic analysis) yöntemlerini kullanarak geleceğe yönelik tahminde bulunabilmektedir (Mahood, 2014: 12).

Sosyal medyanın dezavantajlarından birisi olarak ele alınan, sosyal medyanın çok büyük hacimde veri içermesi hususu, tahmin yöntemi için bir avantaja dönüşebilmektedir. Olay meydana gelmeden önce sosyal medyadaki hareketliliğin takip edilmesi sayesinde bir takım davranış kalıpları tanımlanabilmektedir. Bu kalıpları belirleyen SOMİS analistlerinin bir model hazırlayarak, gelecekteki benzer olayları tahmin etmek için modellemeler yapmaları mümkün görülmektedir (Mahood, 2014: 12).

2.3.3.3.3. Netnografi analizi yöntemi

Netnografi⁵⁵, sosyoloji ve etnografiden türetilen, sosyal medya verileriyle ilgili verileri toplamak ve analiz etmek için imkân sunan yöntemdir. Bu disiplin aynı zamanda çevrimiçi etnografi olarak da bilinmekte, küçük çevrimiçi toplulukların incelenmesine izin vermektedir. Bu yöntemin, suç ve terör eylemleri hakkında bilgilerin bulunması ve toplanmasında etkili olduğu düşünülmektedir (Bartlett ve Reynolds, 2015: 26-28).

İnternet veya teknolojik ağ etnografisi şeklinde nitelendirilen netnografi, tıpkı etnografi gibi doğal ve katılımcı gözlemle insan davranışlarını ve bu davranışların altında yatan nedenleri bağlamsal düzlemde incelemeyi amaçlamaktadır. Bu yöntem internette var olan bilgiyi, araştırma yöntemlerinin aşamalarına dayanarak incelemekte ve oluşturulan tüm içeriği bağlamsal kodlarıyla birlikte yorumlamaktadır (Kozinets, 1997: 473).

Çevrimiçi araştırmalar için kullanışlı bir yöntem halini alan netnografi yönteminde araştırmacı birçok veriye aynı anda sahip olabilmektedir. Netnografi; etkileşim tarzlarını, kişisel anlatıları, ortak alışverişi, çevrimiçi kural, uygulama ve ritüelleri, söylemsel stilleri ya da yeni organizasyon biçimlerini ortaya çıkarma konusunda oldukça işlevseldir. Çevrimiçi toplulukların bireylerarası etkileşime imkân sunması bu toplulukları da netnografi yöntemi için elverişli bir araştırma alanına dönüştürmüştür (Çetin ve Ayhan, 2020: 56).

2.3.3.3.4. İçerik analizi yöntemi

İçerik analizi, büyük hacimli bir metni daha az hacimli içerik kategorisine sıkıştırmak için sistematik, tekrarlanabilir bir teknik olarak tanımlanmaktadır. İçerik analizi, araştırmacıların büyük hacimli verileri sistematik bir şekilde elemesini sağlamaktadır. İçerik analizi metin içerisindeki eğilimleri ve temel düşünce kalıplarını ortaya çıkarabilmektedir. İçerik analizi ayrıca, kamuoyunun düşüncelerindeki değişimleri izlemek için deneysel bir bakış açısı sağlamaktadır (Steve, 2000: 1).

İçerik analizi; metnin kendi bağlamıyla ilişkisi, metni üreten kişinin niyeti veya hedef kitlenin nasıl bir tepki verdiğiyle ilgili değil; bağlamlarından soyutlanan kelimelere veya büyük metinlere odaklanmaktadır. İçerik analizi daha çok saymaya ve kodlamaya izin veren bir yapıya sahiptir. Sistematik ve niceliksel bir yöntem olmaya odaklanarak,

⁵⁵ Netnografi, etnografi yönteminin bilgisayara dayalı sosyal dünyanın karmaşıklığına uyarlanmış halidir. Etnografide yüz yüze ve kültürel etkileşimler yoluyla veri toplanırken, netnografide çevrimiçi iletişim yoluyla veri toplanmaktadır. Netnografi, sanal topluluklarda giderek daha fazla sosyalleşen günümüz tüketicisini anlamak için çevrimiçi sosyal ağlardaki tüketici davranışını inceleyen bir araştırma yöntemi olarak kullanılmaktadır. Ayrıntılı bilgi için bkz: Özbölük, T. ve Dursun, Y. (2015). *Pazarlama araştırmalarında paradigmat dönüşüm ve etnografinin dijital evrimi: Netnografi*. Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, (46), ss.227-247.

toplumun inşasında söylemin rolüne ilişkin anlayışımızı genişletmede faydalı bir rol oynayabilen (Hardy vd., 2004: 20) içerik analizi, mesajların belirli özelliklerini belirleyerek çıkarımlar yapmaya yönelik bir yöntemdir. İçerik analizi, bilimsel bir yönetime dayanan, bir metindeki mesajların özetlenmesi ve nicel olarak analizi sürecidir (Lai ve To, 2015: 140).

İçerik analizi kullanılarak incelenen herhangi bir metin, bir içerik bulutunun oluşturulmasıyla görselleştirilebilmektedir. İçerik bulutları, bir internet sitesi aracılığıyla üretilebilme kolaylığı nedeniyle siyasi konuşmaları analiz etmenin popüler bir aracı haline gelmiştir. İçerik ya da kelime bulutları, yazı tipi boyutunun kelimenin kullanım sıklığıyla orantılı olduğu fikrine dayanmaktadır (Cidell, J. 2010: 516).

Kelime bulutları, kelimelerin görsel bir şekilde temsilinden daha fazlasını ifade etmektedir. Bir kelime bulutu; bir metin içerisindeki bir dizi kelimenin belirlenen özelliklerinin temsil edilmesi için söz konusu kelimelerin boyut veya renk olarak farklı biçimlerde görsel sunumlarını ifade etmektedir. Bir kelime bulutu tipik olarak, en sık kullanılan kelimeleri ele almakta ve bu kelimeleri, frekanslara bağlı olarak farklı boyut ve renklerde anahtar kelimeleri tanımlayan çekici bir görsel sunumda görüntülenmektedir (DePaolo ve Wilkinson, 2014: 38).

Kelime bulutları oluşturmak, bir metin içerisindeki kelimelerin frekansını ölçmek maksadıyla kullanılan çok sayıda internet uygulamasının mevcut olduğu görülmektedir. Bu çalışma kapsamında WordClouds isimli uygulama⁵⁶ üzerinden oluşturulan bir kelime bulutu örnek olarak Şekil 2.10.'da sunulmuştur. Şekil 2.10.'da yer alan kelime bulutu örneği bu tezin halen okuduğunuz ikinci bölümünden elde edilmiştir.

Şekil 2.10. Örnek Kelime Bulutu



⁵⁶ <https://www.wordclouds.com/> adresinden erişilebilmektedir.

Örnek kelime bulutunda görüldüğü üzere, okumakta olduğunuz tez bölümü içerisinde en sık kullanılan kelimeler, beklendiği üzere; “sosyal”, “medya”, “terör” ve “istihbarat” kelimeleri olmuştur. Bu çalışmada kelime bulutları terör örgütü gündemini tespit etmek üzere kullanılacaktır.

2.3.3.3.5. Sosyal ağ analizi yöntemi

SOMİS’in kullandığı yöntemlerden bir diğeri ve bu tezde de kullanılan analiz yöntemi ise “Sosyal Ağ Analizidir (SAA)”. SAA, insan grupları gibi oluşumlar içindeki ilişkilerin doğasını, bu ilişkinin yoğunluğunu ve sıklığını tanımlamak için kullanılan sosyolojik ve matematiksel yöntemleri birleştiren bir yaklaşımdır. Bu yöntem, insanların, onları çevreleyen sosyal ağlardan, psikolojik ve davranışsal açıdan etkilendikleri öngörüsüne dayanmaktadır. Bu çerçevede SAA, sosyal ağların yapısal özelliklerini belirleyerek, ağın ve üyelerinin genel davranışlarını, bu ağları etkileyen kişileri ağ içindeki konumlarına göre açıklamaya çalışmaktadır (Omand, vd., 2014: 30-31).

Sosyal medya istihbaratı üretmek için, sosyal medya siteleri dâhil olmak üzere farklı çevrimiçi platformlarda SAA yapılabilir. SAA vasıtasıyla, verilerin alındığı sosyal ağ platformunda açık ya da kapalı olarak oluşturulan ağların hem kendi içinde hem de diğer ağlarla olan ilişkileri anlaşılma çalışılmaktadır (Omand, vd., 2014: 31).

Kullanıcılar arasındaki bir ilişkinin ölçüldüğü ve anlaşılma çalışıldığı, sempatanlar ağı gibi ağ analizi biçimleri, çevrimiçi bir ağın geniş yapısını ve davranışını anlamak için oldukça faydalıdır. Ağ analizi, bir örgüt veya hareket içinde paylaşılan bilgi ve fikir türlerini daha iyi anlamak için son derece kıymetli görülmektedir (Bartlett ve Reynolds, 2015: 27-28).

Sosyal medyada uygulanan tipik bir SAA vasıtasıyla; belirli bir problem hakkında üretilen paylaşımlardaki ve içerikteki artışı izlemek; belirli bir bilginin yayılmasını takip etmek; bireyler arasındaki bilgi paylaşımını gözlemlemek; bireylerin oluşturduğu ağların benimsediği davranışları anlamak hedeflenmektedir (Omand, vd., 2014: 31).

SAA, sosyal medyadaki ilişkileri, bilgi akışını ve paylaşımların yayılma şeklini anlamak için SOMİS analiz yöntemi olarak kullanılabilir. Sosyal medyadan verilerin toplanmasını müteakip, belirli bir faaliyete çevrimiçi olarak kaç kişinin katıldığına analizinden bilgi akışlarının ve karmaşık sistemlerdeki etkinin değerlendirilmesine kadar çeşitli amaçlarla kullanılabilirler (Bartlett ve Reynolds, 2015: 52).

SOMİS, hedef istihbaratı (targeting intelligence) kapsamında da önemli bir rol oynayabilmektedir. Bir hedefin belirlenmesi, güvenlik açıklarının tespiti, analiz edilmesi işlevlerini yerine getiren hedef istihbaratı, kilit konumdaki kişiler ve hedefle ilgili güncel bilgilere sahip olmayı amaçlamaktadır. Bu açıdan bakıldığında SOMİS, özellikle SAA ile uyumluluğu açısından hedef istihbaratında kullanılmak üzere de en uygun araçlardan birisidir (Mahood, 2014: 8).

SAA, yüksek değerlikli hedefleri (high value targeting) tespit etmede önemli bir rol oynamaktadır. Bağlantı analizi veya ilişkilendirme analizi olarak da adlandırılan SAA, ele alınan konular arasındaki bağlantıları ve ilişkileri değerlendirmektedir. SAA, sadece bir ilişkinin var olduğu gerçeğiyle değil, ilişkinin içeriğiyle de ilgilenmektedir (Mahood, 2014: 8). SAA, yalnızca nicel değil, nitel verilerin de elde bulundurulmasını gerektirmektedir. Bu açıdan sosyal medya hem nicel hem de nitel verileri sağlamaya yardımcı olmaktadır. Ağ analizine konu olan kişi veya bu kişinin ailesi, arkadaşları ve hatta irtibatta olduğu kişiler sosyal medyayı kullandığı takdirde, SOMİS analitik analizi desteklemeye yardımcı olacak bilgiler sağlayabilmektedir (Mahood, 2014: 8).

SAA ile ilgili hususlar ayrıntılı olarak tezin bir sonraki bölümünde incelenecek, SAA'nin terörizmle mücadelede bir SOMİS analiz yöntemi olarak kullanımı PKK terör örgütü çerçevesinde ele alınacaktır.

2.3.3.4. Sosyal medya istihbaratının teyit edilmesi

Sosyal medyada yer alan veriler zaman zaman kasıtlı olarak yanlış yönlendiren verilerden oluşabilmekte, gerçeklerin tamamı değil sadece bir kısmı sosyal medyada paylaşılabilmekte, paylaşımlarda kasıtlı ya da kasıtsız olarak hatalar yapılabilmekte veya bilgiler bilerek çarpıtılabilmektedir (Omand vd., 2012b: 59). Bu kapsamda SOMİS'den kaynaklı olası hataların önüne geçebilmek maksadıyla, SOMİS ile elde edilen istihbaratın, diğer istihbarat yöntemlerinde olduğu gibi teyit edilmesi gerekmektedir.

SOMİS ile elde edilen istihbaratın, kullanıcıya ulaşmadan önce teyit edilmesini sağlamak için kapsamlı ve hızlı bir teyit süreci olmak zorundadır. İnsan istihbaratı gibi tek kaynaklı istihbarat türlerinden farklı olarak, SOMİS'in teyit edilmesi ve doğrulanması, verilere erişim ve analiz adımlarından daha önemlidir (Omand vd., 2012b: 60).

SOMİS'in teyidi açık kaynaklar dâhil olmak üzere tüm istihbarat kaynakları kullanılarak yapılabilmektedir. Bu kapsamda, bilginin elde edilmesinde ve analizinde yaşanabilecek muhtemel hatalar göz önünde bulundurularak ve güvenilirlik derecesi

ölçülerek, elde edilecek istihbarata ilişkin dağıtım öncesinde sınırlılıklar belirtilebilmektedir (Omand vd., 2012b: 61).

SOMİS kapsamında elde edilen bilginin ve bilginin elde edildiği kaynağın güvenilirlik derecesi, diğer istihbarat yöntemlerinde olduğu gibi, tamamen güvenilirden güvenilmeze kadar değişen bir yelpazede derecelendirilebilmektedir. Aynı şekilde haberin güvenilirliği de tamamen doğrudan başlayarak doğru olmayana kadar bir aralıkta, Çizelge 2.1.'de bulunan doğrulama ve güvenilirlik matrisi ile derecelendirilebilir.

Örnek teşkil etmesi amacıyla SOMİS haber kaynağının güvenilirlik derecesi; tamamen güvenilir, çoğunlukla güvenilir, güvenilir, çoğunlukla güvenilmez, güvenilmez biçiminde tasnif edilebilir. Haberin güvenilirliği; tamamen doğru (teyit edilmiş), muhtemelen doğru, doğru olması mümkün, doğruluğu şüpheli ve güvenilmez şeklinde sınıflandırılabilir. Bu örnek kapsamında devlet yetkilileri tarafından Twitter'da paylaşılan bir bilgi için kaynağı açısından tamamen güvenilir ve haberin içeriği açısından tamamen doğru şeklinde bir derecelendirme yapılması mümkündür. Bu sayede istihbaratı okuyan yetkililerin ve kurumların istihbaratın güvenilirliğini değerlendirmesi sağlanabilecektir.

Çizelge 2.1. SOMİS Doğrulama ve Güvenilirlik Matrisi⁵⁷

Haber Haber Kaynağı	Tamamen Doğru	Muhtemelen Doğru	Doğru olması Mümkün	Doğruluğu Şüpheli	Güvenilmez
Tamamen Güvenilir					
Çoğunlukla Güvenilir					
Güvenilir					
Çoğunlukla Güvenilmez					
Güvenilmez					

⁵⁷ SOMİS Doğrulama ve Güvenilirlik Matrisi, ABD Kara Kuvvetleri Komutanlığı FM 2-22.3 İnsan İstihbaratı Toplama Harekâtı isimli talimnamede yer alan, "Kaynak ve Bilgi Güvenilirlik Matrisi" içerisinde yer alan bilgilerden uyarlanarak SOMİS kapsamında kullanılmak üzere yazar tarafından oluşturulmuştur. Ayrıntılı bilgi için bkz: US Army Headquarters. (2006). *FM 2-22.3. Human intelligence collector operations*. EK-B.

SOMİS'i teyit etmek ve doğrulamak için bir dizi kurallar üretmek de faydalı olabilecektir. Bunlardan bir tanesi, SOMİS ile çevrimiçi olarak elde edilen istihbaratın mümkün olduğu takdirde çevrimdışı araçlarla doğrulanmasıdır. Örneğin, internette yaşanan çevrimiçi bir olayın gerçek hayatta insan davranışlarına nasıl yansıdığı karşılıklı olarak eşleştirilerek değerlendirilebilmektedir (Omand vd., 2012b: 61).

Ayrıca, SOMİS analistlerinin sosyal medyada yayılan bilgiler ve bu bilgileri yayanların güvenilirliğini değerlendirebilmeleri için belirgin bir tecrübeye de sahip olmaları gerektiği değerlendirilmektedir. Sosyal medya verilerinin yer aldığı internet ortamı ile gerçek hayat arasındaki farklılıkları algılayabilen, sosyal medyanın özelliklerini bilen, gerçek ve gerçeğe yakın ile gerçek olmayan arasındaki farkı değerlendirebilecek analistlerin yetiştirilmesi gerekmektedir.

2.3.3.5. Sosyal medya istihbaratının dağıtımı

Sosyal medya verilerinden elde edilen istihbaratın etkinliği, bu istihbaratın doğru kişilere, hızlı ve güvenli bir şekilde ulaştırılmasına, stratejik ve operasyonel karar vericiler için anlamlı bir formatta sunulmasına da bağlıdır. Bu dağıtım biçimi SOMİS'in amacına bağlı olarak; dipnotlu, ayrıntılı ve derinlemesine bir stratejik analiz raporundan, tek bir ekrana sığabilen görsellere kadar değişebilmektedir (Omand vd., 2012b: 58).

SOMİS'in dağıtımında yaşanabilecek bir takım sorunlar da söz konusudur. Bunlardan birincisi, elde edilen verilerin karmaşıklığı, ölçeği ve dinamizmi nedeniyle istihbarat sunumundaki zorluklardır. Karmaşık ve çoğu zaman birbirine ağ şeklinde bağlı bir istihbaratı, anlaşılabilir ve bilginin özünü koruyan bir şekilde görselleştirmek için veri görselleştirme tekniklerinin etkili bir şekilde uygulanması gerekmektedir. Ancak karmaşık bilgilerden oluşan bu tür görsellerin nasıl yorumlanacağına dair tecrübenin oluşması için veri analizi tekniklerini kullanma konusunda daha fazla deneyime ihtiyaç bulunmaktadır (Omand vd., 2012b: 59).

2.3.4. Sosyal Medya İstihbaratının Avantajları ve Dezavantajları

SOMİS'in avantajları üç başlık altında toplanabilmektedir. Bu avantajlardan birincisi gerçek zamanlıya yakın durumsal farkındalık sağlamasıdır. Sosyal medya içeriklerinin analizi, meydana gelen olayların geleneksel istihbarata göre daha hızlı tespit edilebilmesine imkân tanımaktadır (Omand vd., 2012a: 805-806).

SOMİS'in sağladığı ikinci avantaj, örgütlerin içyüzünü anlamaya olanak tanımasıdır. Bu avantaj sayesinde kolluk kuvvetleri veya istihbarat teşkilatlarının ilgisini çeken

örgütlerin faaliyetlerini ve davranışlarını daha iyi anlama becerisi kazanılabilmektedir. Üçüncü avantaj ise suça ilişkin delil toplanmasına imkân vermesidir. SOMİS kolluk kuvvetlerinin, suça karıştığından şüphelenilen kişilerin sosyal medya hesaplarını takip ederek, muhtemel suç ortaklarına ulaşabilmesi, suç ağlarının tanımlanması için kullanabilmektedir (Omand vd., 2012a: 806).

SOMİS'in bir takım dezavantajları da mevcuttur. Dijital sosyal alanlar, kendine özgü kuralları ve dilleri bulunan, psikolojik ve sosyal etkilere sahip olan, dolayısıyla yeni anlamlar ve değerler taşıyan sosyal faaliyet alanlarıdır. Sosyal medyanın yarattığı sosyal alanları anlamak için kullanılan araçlar ve teknikler de oldukça yenidir. Bu araçlarla verileri toplamak, toplanan verileri anlamlı sonuçlar üretecek şekilde yorumlamak, sosyal medyada sıklıkla kullanılan aldatıcı ve yanlış haberleri doğrulamak SOMİS açısından temel güçlüklerdir (Omand, vd., 2014: 26).

SOMİS'in sınırlılıklarından birisi de büyük veri ile çalışmanın yarattığı zorluktur. Örneğin sosyal medyadan elde edilen verilerin anlamsal düzeyde analiz edilmesi, bu verilerden duyguların tespit edilebilmesi, ironi, hiciv, alaycılık içeren içeriklerin tespit edilmesi bir takım zorluklar yaratmaktadır. Bir diğer zorluk ise yapılandırılmış, tablo haline getirilmiş statik geleneksel veriler yerine, sosyal medyada kısa zaman dilimleri içerisinde dinamik bir veri akışı olmasıdır (Schoder vd., 2013: 10-11). Bu nedenle sosyal medyadan elde edilen verilerin tasnifi ve analizi maksadıyla bilgisayar sistemlerinin ve yazılımların kullanılması gerekmektedir.

SOMİS'le ilgili bir diğer dezavantaj, SOMİS'in hem devlet kurumları hem de özel sektör tarafından kötü amaçlarla kullanılmasına yönelik çekincelerdir. Diğer tüm istihbarat yöntemleri gibi SOMİS'in de kötü amaçlarla kullanılmamasına yönelik yasal düzenlemelerin yapılması gerekmektedir (Omand, vd., 2014: 26).

SOMİS, birbiriyle bütünleşmiş çok disiplinli bir çalışma gerektirmektedir. Bu kapsamda SOMİS'in; bilişim, sosyal psikoloji, medya teorisi, siyaset bilimi ve sosyal bilimler gibi disiplinlerin yöntemlerinden faydalanması gerekmektedir. Bununla birlikte hem bilişim hem de diğer disiplinleri birlikte kullanan çok az araştırma programı mevcuttur (Zeng vd., 2010,s.15).

SOMİS'in kendini ispat yükümlülüğü karşılaşılan bir diğer dezavantaj olarak karşımıza çıkmaktadır. SOMİS'in karşı karşıya olduğu temel zorluk, yeni ortaya çıkan bir

istihbarat disiplini olarak SOMİS'in kendisini ve güvenilirliğini ispat etmesi gerektiğidir (Omand, vd., 2014: 33).

2.3.5. Sosyal Medya İstihbaratının Terörizmle Mücadelede Kullanımına İlişkin Örnekler

SOMİS'in terörizmle mücadelede kullanımına ilişkin yabancı alanyazında çok sayıda araştırma mevcuttur. Bu çalışmalardan en bilineni "DEAŞ Twitter Sayımı" isimli analizdir. Çalışma; DEAŞ terör örgütünün Suriye ve Irak'ta eylemlerini en üst seviyeye çıkardığı 2014 yılı sonlarında, Twitter üzerinden birbirleriyle ilişkili, kendi aralarında bir sosyal ağ kuran 20.000 Twitter hesabının izlenmesini temel almaktadır (Berger ve Morgan, 2015: 2).

DEAŞ Twitter Sayımı çalışmasının amacı; Twitter kullanan DEAŞ terör örgütü sempaticanlarının demografik görünümünü ortaya koymak, müteakip çalışmalar için geçerli bir veri setinin hazırlanmasına yönelik bir yöntem geliştirmek, Twitter şirketi tarafından DEAŞ terör örgütü sempaticanı hesapların askıya alınmasının etkilerini araştırmak şeklinde ifade edilmiştir (Berger ve Morgan, 2015: 2).

"DEAŞ Twitter Sayımı" isimli çalışmanın sonucunda; DEAŞ terör örgütü sempaticanlarının büyük çoğunluğunun Suriye ve Irak başta olmak üzere DEAŞ'ın faaliyet gösterdiği ülkelerde bulunduğu; her beş DEAŞ sempaticanından birisinin İngilizce dilini kullandığı; DEAŞ terör örgütü sempaticanı hesapların normalin üzerinde bir şekilde, ortalama 1.000'er takipçilerinin bulunduğu ifade edilmektedir. Twitter hesaplarının askıya alınmasının DEAŞ terör örgütünün sosyal medyadaki faaliyetlerini sınırlamada somut etkilere sahip olduğu; hesapların askıya alınmasının, sempaticanların DEAŞ ağına katılmasını engellediği ancak bu kişileri kapalı çevrimiçi ağlara ittiği, kapalı ağlara girmeyi başaran bireylerin radikalleşmelerinin hızlandığı sonucuna ulaşılmıştır (Berger ve Morgan, 2015: 3).

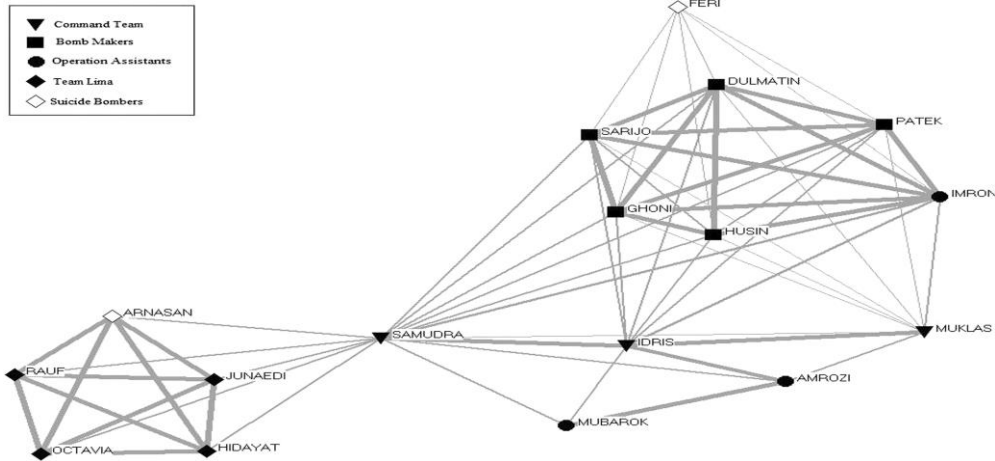
Bir diğer çalışma ise "Terörizmle İlgili Askıya Alınan Hesapların Sosyal Medyada Analizi" isimli araştırmadır. Bu çalışmada, Twitter'da terörizmle ilgili yayımlanan içerikleri belirleyebilmek maksadıyla anahtar kelimeler kullanılarak bir veri seti elde edilmiştir. Elde edilen veri seti vasıtasıyla tespit edilen Twitter paylaşımları anlam, mekân, zaman, üst veri ve sosyal ağ özellikleri açısından analiz edilmiştir (Kalpakis vd., 2018: 108). Araştırmada Twitter tarafından askıya alınmış ve askıya alınmamış hesaplar arasındaki farklara odaklanılarak Twitter'da yayımlanan terörizmle ilgili içerik analiz edilmiştir. Twitter'ı kötüye kullanan, askıya alınmış, terörizmle iltisaklı muhtemel

hesapların, askıya alınmamış diğer hesaplardan farklarını tespit eden çalışma, kötü amaçlı hesapların tespitine yönelik bulguları ortaya koymuştur (Kalpakis vd., 2018: 117).

“Propaganda, Radikalleşme ve Eleman Temini Maksadıyla Tweet Atma: İslam Devleti Destekçilerinin Çok Yönlü Twitter Ağları” isimli bir başka araştırmada; DEAŞ terör örgütü mensuplarının ve sempatanlarının Twitter’ı iletişim, propaganda, radikalleşme ve eleman temini maksadıyla nasıl kullandıkları incelenmiştir. Çalışmada @shamiwitness adlı kullanıcıdan toplanan tweetler, eğilim, sosyal ağ ve içerik analizi yöntemleriyle değerlendirilmiştir (Chatfield vd., 2015: 241-243). Eğilim analizi ile söz konusu hesabın Twitter kullanma eğilimleri analiz edilmiştir. @shamiwitness isimli kullanıcı etrafında oluşan ağ SAA ile analiz edilmiş, ağ içerisindeki düğüm noktaları ve bağlantılar, sıkı ve zayıf ilişkiler tweet alışverişine göre ortaya konulmuştur. Tweetlerin içerik analizi neticesinde ise adı geçen Twitter hesabının takipçilerinden terör örgütüne katılmalarını istediği, insanlara ve mülke karşı şiddet kullanımını talep ettiği, tweetlerin genelde aşırı siyasi görüşlere yer verdiği tespit edilmiştir (Chatfield vd., 2015: 243-247).

“#Yeşil Kuşlar: Suriye’de Yabancı Savaşçı Ağlarının Önem ve Etkisinin Ölçülmesi” isimli bir başka araştırmada; DEAŞ ve El Nusra terör örgütlerine bağlı olduğu değerlendirilen Facebook’tan 86, Twitter’dan 35 yabancı terörist savaşçının hesapları analiz edilmiş, Suriye’deki yabancı terörist savaşçıların bölgedeki çatışmalar hakkında bilgiyi nasıl temin ettikleri incelenmiştir (Carter vd., 2014: 8). Çalışma sonucunda; yabancı terörist savaşçıların bölgedeki çatışmalarla ilgili bilgiyi bağlı oldukları terör örgütlerinin “resmi” kanallarından ziyade örgüt içerisindeki kilit haberleşmecilerden aldıkları tespit edilmiştir (Carter vd., 2014: 29).

İslam Cemaati (Jemaah Islamiyah) isimli terör örgütü özelinde, SAA’nın terörizmle mücadele ve istihbarat alanında kullanılmasının araştırıldığı; “İslam Cemaati Sosyal Ağ Analizi: Terörizmle Mücadele ve İstihbarat Uygulamaları” isimli çalışmada, terör hücrelerinin yapısı ve iletişim modelleri ortaya konulmuş, SAA’nın gerçek zamanlı istihbarat analizinde kullanılması incelenmiştir. Çalışmada ayrıca 2002 yılında, Endonezya Bali’de İslam Cemaati tarafından düzenlenen terör eylemini gerçekleştiren teröristlerin oluşturduğu ağ, Şekil 2.11.’deki sosyogramla gösterilmiştir (Koschade, 2006: 559).

Şekil 2.11. Bali Saldırısını Gerçekleştiren Teröristlere Ait Ağ⁵⁸

Türkiye’de yapılan nadir araştırmalardan birisi olan “Türkçe Konuşan DEAŞ Destekçileri Üzerine Twitter Sosyal Ağ Analizi” isimli çalışma ise; Türkçe konuşan DEAŞ terör örgütü sempaticanlarının, sosyal medya araçlarından Twitter’deki gündemlerini tespit etmek amacını taşımaktadır (Yalçınkaya vd., 2016: 8). Çalışmada 21 Twitter hesabından hareketle 2.567 adet Türkçe konuşan DEAŞ terör örgütünü destekleyen hesaba erişilmiş, bu hesapların gündemlerinin ilk maddesinin PKK terör örgütü ve PKK ile ilgili hususlar olduğu tespit edilmiştir (Yalçınkaya vd., 2016: 31).

Sonuç olarak; bireylerin kendilerinin oluşturdukları içerikleri kamuoyu ile paylaştıkları sosyal medya coğrafi sınırları kaldırmış, internet üzerinde çevrimiçi sanal topluluklar ve ağlar yaratmıştır. İnsanların hayatlarının bir parçası haline gelen sosyal medya bireylerin ve toplulukların birbirleriyle etkileşimlerini sağlamaktadır. Sosyal medyanın diğer kitle iletişim araçlarına göre oldukça ucuz olması, çok sayıda insana aynı anda ulaşabilmesi, mobil cihazlarla kullanılabilmesi, iletişimi kolaylaştırması, kullanıcı kimliğinin gizlenebilmesi, oldukça süratli olması, kolaylıkla kullanılabilmesi, devlet kontrolünün güç olması özellikleri sadece sıradan bireylerin değil kötü amaçlı insanların ve örgütlerin de dikkatini çekmiş, sosyal medya terör örgütleri tarafından da kullanılmaya başlanmıştır.

Terör örgütleri sosyal medyayı, yeni örgüt elemanları temin etmek; elemanlarına eğitim vermek; takipçiler, sempaticanlar, örgüte mali destek sağlayanlar ve diğer terör örgütleriyle iletişim kurmak, propaganda yapmak, bireyleri radikalleştirmek için kullanmaktadırlar. Terör örgütleri ayrıca sosyal medyayı takip ederek bilgi toplamakta, durumsal farkındalıklarını artırmakta ve örgüte mali kaynak sağlamaktadırlar.

⁵⁸ Kaynak: Koschade, 2006, s.567.

Terör örgütlerinin sosyal medyayı kullanmaya başlamalarının ardından güvenlik güçleri ve istihbarat birimleri de sosyal medya uygulamaları üzerinden mücadele yöntemlerini geliştirmişlerdir. Terör örgütleri için sosyal medyanın yeni bir barınma alanı haline gelmeye başlamasının ardından istihbarat birimleri terör örgütlerini bu alanda da takip etmeye başlamış, aynı zamanda bu alandan istihbarat toplamaya başlamışlardır.

Sosyal medyadan elde edilen verilerin analiz edilmesi sonucunda ortaya çıkan SOMİS, terörizmle ilgili faaliyetlerin tespiti, önlenmesi ve bu alanda durumsal farkındalığın artırılması maksadıyla kullanılabilir. Diğer istihbarat kaynaklarından farklı olarak oldukça dinamik veri içeriklerine sahip olması, devasa boyutlarda veriyi barındırması, güncel gelişmelere süratle ayak uydurabilmesi gibi nedenlerle sosyal medya büyük ayrıcalıklara sahip görülmektedir. Bu ayrıcalıkları nedeniyle sosyal medyadan elde edilen istihbaratın da diğer istihbarat yöntemlerinden ayrı tutulması ve farklı bir disiplin olarak ele alınması gerekmektedir.

Büyük istihbarat resmindeki olası boşlukları doldurmak amacı taşıyan SOMİS, çok kaynaklı istihbarat yönteminin bir parçası olarak diğer istihbarat yöntemlerine katkı sağlayabilmektedir. Taktik, operatif ve stratejik seviyede istihbarata katkılar sunabilen SOMİS'in üretimi tüm istihbarat çeşitlerinde olduğu üzere bir istihbarat çarkının takibini gerektirmektedir. Yönlendirme ve planlama, toplama, analiz, teyit ve dağıtım safhalarını içeren bu süreç diğer istihbarat yöntemlerinden farklı olarak daha büyük verilerin işlenmesini gerektirebildiğinden bilgisayar destekli sistemlerin kullanılmasını zorunlu hale getirmiştir.

Terörizmle mücadele çerçevesinde SOMİS'in kullanımı, terör örgütleri hakkında durumsal farkındalığı artırmak, terör örgütlerinin kendi içerisinde ve diğer örgütlerle ilişki modellerini anlayabilmek, örgütlerin propaganda gündemlerini tespit etmek, terör eylemi öncesi davranışlara ilişkin emareleri tespit etmek, çevrimiçi radikalleşmeyi önlemek amaçlarını taşımaktadır. SOMİS ile ayrıca terör örgütlerine ait sosyal medya ağlarına üye olarak örgütleri içeriden gözetlemek, örgüt içi davranışları tespit edebilmek, örgütlerin bir eylem hazırlığında olduğunu önceden tespit etmek imkânı da bulunabilmektedir.

Tezin müteakip bölümünde, SOMİS analiz yöntemlerinden SAA yöntemi incelenecektir. Tezin yöntemini de açıklayacak şekilde PKK terör örgütü sempatizanlarının Twitter'daki varlığına ilişkin veriler toplanacak, toplanan veriler SAA ile analiz edilecek ve elde edilen bulgular değerlendirilecektir.

ÜÇÜNCÜ BÖLÜM

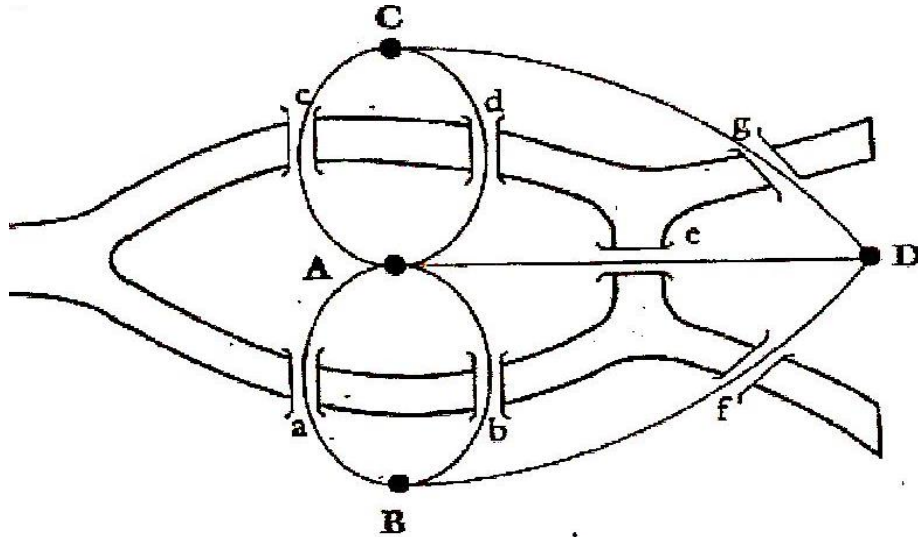
PKK TERÖR ÖRGÜTÜNÜN TWİTTER'DAKİ GÖRÜNÜRLÜĞÜ ÜZERİNE SOSYAL AĞ ANALİZİ

Tezin üçüncü bölümünde amaç; sosyal ağ analizi yönteminin SOMİS analiz basamağında nasıl kullanılabileceğini araştırmaktır. Tezin bu bölümünde ağ ve sosyal ağ analizi kavramları incelenecektir. Bu bölümde ayrıca, tezin yöntemi ortaya konulacak, PKK terör örgütü sempatizanlarının Twitter üzerinde oluşturduğu sosyal ağda sosyal ağ analizi yöntemi uygulanacaktır.

3.1. Ağ Kavramı

Ağ kavramının doğuşunun İsviçreli Matematikçi Leonhard Euler tarafından ortaya konulan “Königsberg Köprüleri” problemi ile başladığı kabul edilmektedir. Bu kabule göre St. Petersburg’a bağlı Königsberg’de halkın zekâ bilmeceleri ile eğlendikleri öne sürülmekte olup bu bilmecelerden bir tanesi Şekil 3.1.’de yer alan köprülerle ilgilidir. “Aynı köprüden iki kez geçmeksizin, yedi köprünün tümünden geçmek mümkün müdür?” sorusuna cevap arayan Euler, böyle bir güzergâhın mümkün olmayacağını matematiksel açıdan kanıtlayan bir makaleyi 1736 yılında yayımlamıştır (Gülpınar Demirci, 2020: 8).

Şekil 3.1. Königsberg Köprüleri⁵⁹



Euler’in makalesinin en önemli özelliği Königsberg’deki köprülerinin çizge ile gösterilmesidir. Makalede nehrin ayırdığı kara parçaları A, B, C ve D ile gösterilerek bu parçalar birer düğüm, köprüler ise birer bağlantı olarak ele alınarak bir ağ elde edilmiştir (Gülpınar Demirci, 2020: 8).

⁵⁹ Kaynak: Gülpınar Demirci, 2020, s.8.

Sosyal ağ teorilerinden bir diğeri, 1967 yılında Stanley Milgram tarafından gerçekleştirilen “Küçük Dünya Sorunu (The Small World Problem)” adlı deneyle ortaya konulmuştur. Milgram deneyinde; dünyadaki iki insanın birbirlerini tanıma olasılıkları nedir sorusundan yola çıkarak, birbirlerini doğrudan tanımayan X ve Z’nin, ikisinin de tanıdığı Y aracılığıyla bir tanıdık ağı oluşturabileceğini ortaya koymuştur (Milgram, 1967: 62).

Milgram, deneyinde ABD’de birbirlerinden mesafece uzak yaşayan 160 kişinin, başka bir şehirde yaşayan ve tanımadıkları bir başka kişiye mektup ulaştırması istenmiştir. Deneye katılan herkesten mektuba kendi adını yazması ve mektubun ulaştırılacağı kişiye en yakın olduğu bir arkadaşına mektubu ulaştırması, bu işlemin zincir şeklinde devam etmesi talimatı verilmiştir. Deneyin temel amacı; rastgele seçilen bireylerin hiç tanımadıkları bir kişiye ulaştıracakları mektubun kaç kişinin elinden geçerek ulaşacağını ölçmek olarak belirlenmiştir (Milgram, 1967: 64). Milgram “Küçük Dünya Deneyinin” sonucunda, birbirlerini tanımayan ve birbirlerinden mesafece oldukça uzakta olan insanların tanıdıkları vasıtasıyla iletişime geçebildiklerini, mektupların ortalama beş ya da altı kişi vasıtasıyla hedef adrese iletebildiği sonucuna varmıştır (Milgram, 1967: 67).

Sosyal ağ teorileri çerçevesinde yapılan bir diğer önemli çalışma Mark Granovetter’in 1973’te yaptığı “Zayıf Bağların Gücü (The Strength of Weak Ties)” isimli çalışmasıdır. Çalışmada toplumların, grupların, örgütlerin iç ilişkilerinin, kuvvetli bağlarla sürdürüldüğü ifade edilmektedir. Kuvvetli bağların, bu bağın olduğu zamanın miktarı, duygusal yoğunluk, aralarındaki güven ve birbirlerine karşı yükümlülükleriyle ilgili olduğu ifade edilmektedir. Zayıf bağların sayılarının çok olduğu, zayıf bağlarda duygusal yoğunluğun daha az, etkileşim sıklığının düşük olduğu ancak önemli haberlerin en yakın ve en yoğun ilişki içinde olunan güçlü bağlantılardan değil zayıf bağlardan geldiği iddia edilmektedir. Granovetter, az sayıda bireyle güçlü bir arkadaşlık bağı içerisinde olmak yerine çok sayıda kişiyle tanışarak daha zayıf bağlar kurmanın insanların iş hayatında başarılı olmasını sağladığını ifade etmektedir (Granovetter, 1973: 1371-1378).

Uzun yıllardır üzerinde akademik çalışmalar yapılan ağlar, birimler ve birimler arasındaki bağlantılardan meydana gelmektedir. Söz konusu birimlere düğüm (node veya vertex), düğümler arasındaki ilişkilere ise bağlantı (edges veya ties) denilmektedir. Ağların kolay anlaşılabilir hale getirilmesi, ağların içerisinde ve ağlar arasındaki ilişkileri göstermek için kullanılan ağ gösterimine ise çizge (graph) adı verilmektedir (Gürsaka ve Uça Güneş, 2016: 5).

Çizge teorisi, karmaşık problemlerin düğümler ve düğümler arasındaki bağlantılar kullanılarak bir çizge ile gösterilmesi yöntemidir. Çizge teorisinin bazı özellikleri modellenen problemin çözümüne yardımcı olmaktadır. Kısacası çizge teorisinin problem çözümünde kullanılabilmesi için öncelikle problemin çizge olarak modellenmesi, modelin çözülmesi ve ardından probleme uygulanması gerekmektedir (Seker, 2015: 17).

Çizgelere verilebilecek en uygun örneklerden birisi şehirlerarası karayolları haritasıdır. Bu kapsamda şehirler düğümleri, şehirleri birbirine bağlayan yollar bağlantıları, haritalar ise çizgeleri simgelemektedir (Gürsakaç ve Uça Güneş, 2016: 5). Metro duraklarının düğümleri, duraklar arasındaki rayların bağlantıları temsil ettiği İstanbul metro ağı çizgesi, Şekil 3.2.'de görülmektedir.

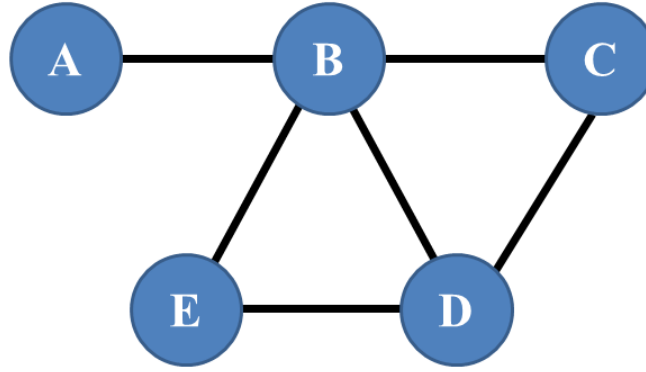
Şekil 3.2. İstanbul Raylı Sistemler Ağ Haritası⁶⁰



Bir ağ içerisinde komşu kenarlar takip edilerek bir düğümden diğerine ulaşana kadar takip edilen sürece yol ya da patika denilmektedir. Şekil 3.3.'de görülen ağda, A'yı D'ye bağlayan A noktasından B noktasına, B noktasından C noktasına, C noktasından D noktasına giden bir A-B-C-D yolu bulunmaktadır. Bu yol toplam 3 kenarı dolaştığı için yolun uzunluğu 3 birimdir. A noktasını D noktasına bağlayan en kısa yol ise 2 birim uzunluğundaki A-B-D yoludur (Tunalı, 2016: 13).

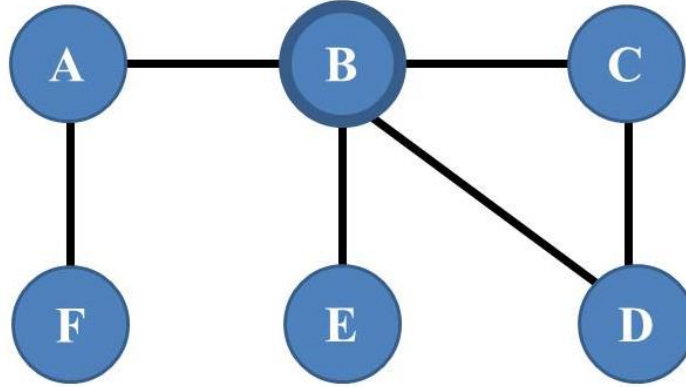
⁶⁰ Kaynak: <https://rayhaber.com/2020/01/istanbul-metro-haritasi-2020/>

Şekil 3.3. Ağ Yolu



Bir çizgede iki ayrı düğüm grubu mevcut ise ve bu düğüm gruplarını birbirine bağlayan, çizgeden çıkartılması halinde bu iki grubun iki ayrı bileşene ayrılmasına neden olacak kenarlar, köprü (bridge) olarak adlandırılmaktadır. Şekil 3.4.'te A-B kenarı bir köprüdür. Göbekler (hub) ise bir çizgedeki en önemli düğümlerdir. Bir çizgede en fazla bağlantıya sahip düğümler göbek olarak adlandırılır. Şekil 3'te 4 farklı bağlantıya sahip olan B düğümü bir göbektir (Tunalı, 2016: 15).

Şekil 3.4. Ağda Kenar ve Göbekler

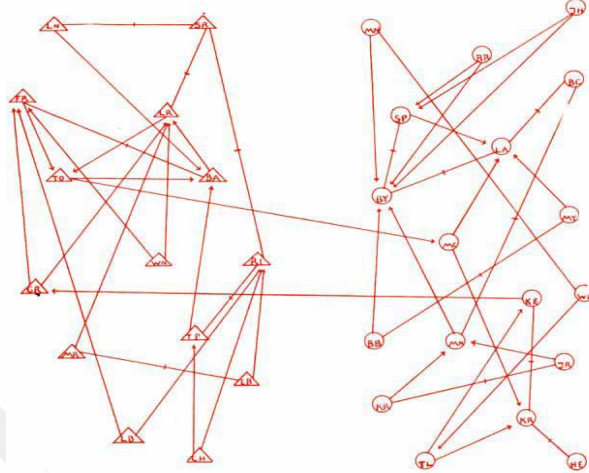


Sosyal ağ teorisi kapsamında kullanılan ifadelerden bir diğeri de “sosyogram” kavramıdır. Sosyogram, insanların iki boyutlu uzayda noktalar olarak temsil edildiği ve insan çiftleri arasındaki ilişkilerin, birbirlerine karşılık gelen noktaları bağlayan çizgilerle temsil edildiği bir gösterimdir (Wasserman ve Faust, 1994: 12).

Sosyogram kavramı ilk kez Jacob Moreno (1934) tarafından ilköğrencilerinin arkadaşlık yapılarını araştıran bir çalışma ile ortaya konulmuştur. Moreno çalışmasında okuldaki kız ve erkek öğrenciler arasındaki ilişkileri araştırmıştır. Moreno araştırmasında erkeklerin erkeklerle, kızların ise kızlarla arkadaşlık ilişkisi içerisinde olduğu sonucuna

varmış, elde ettiği bulguları ise bireyler arasındaki ilişkiyi Şekil 3.5.’teki sosyogramlara taşımıştır (ss.23-49).

Şekil 3.5. Yedinci Sınıf Öğrencileri İlişki Sosyogramı ⁶¹



Sosyal ağ analizinde (SAA), bireyler ve gruplar noktalarla temsil edilmekte ve sosyal ilişkiler sosyogramlarda gösterilen çizgilerle temsil edilmektedir. Çizge teorisi, ortaya konulan sosyogramların biçimsel özelliklerini analiz etmek için gerekli kanıtları sağlamaktadır (Scott, 2011: 22). Sosyogramlar, bir ağ içerisinde yer alan aktörlerin birbirleriyle olan ilişkilerini resmetmektedir. Sosyogram ile oluşturulan görseller sayısal analizlerin bir bütün halinde gösterimine yardımcı olmakta, karşılaştırma yapılmasına olanak tanımakta ve zaman tasarrufu sağlamaktadır. Sosyogramlarda düğümleri gösteren noktaların grafiğin neresinde yer aldığı, düğümleri birbirine bağlayan çizgilerin uzunluğu ya da kısalığı bir anlam ifade etmemektedir. Bununla birlikte bağlantı çizgilerinin kalın ya da ince olmaları aralarındaki ilişkinin güçlü ya da zayıf olduğunu gösterebilmektedir (Ağcasulu, 2018: 1920).

Sosyogramları çizebilmek amacıyla matrislerin oluşturulması da gerekmektedir. Çok miktarda aktörün yer aldığı ağlarda matrislerin hazırlanması, analizi daha kolay hale getirmektedir. Oluşturulan matrisler her zaman için ağdaki aktör sayısının karesi büyüklüğünde olmaktadır. Örneğin “n” sayıda aktörü olan bir ağda matris büyüklüğü, “n²” kadardır. Bir matriste bulunan başlıklar, o ağda yer alan aktörlerin isimlerinden oluşmaktadır. Matris içerisinde yer alan kutular, aktörler arasındaki ilişkinin varlığı, yokluğu veya sıklığına işaret etmektedir. Çizelge 3.1.’de görülen matris gösteriminde aktörler arasında bir ilişki varsa “1” ilişki yoksa “0” ile kodlanmaktadır (Ağcasulu, 2018: 1922). Tablo 1’de yer alan örnek ağ matrisinde Ali’nin; Burak, Doğan ve Erhan ile

⁶¹ Kaynak: Moreno, 1934, s.41.

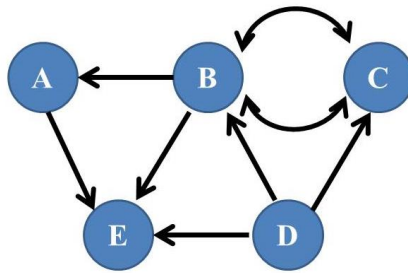
bağlantısı bulunurken, Burak'ın Erhan ve Doğan ile bağlantısının olmadığı gösterilmektedir. Aynı matriste aktör sayısı 5, ağın büyüklüğü ise $5^2=25$ 'tir.

Çizelge 3.1. Örnek Ağ Matrisi

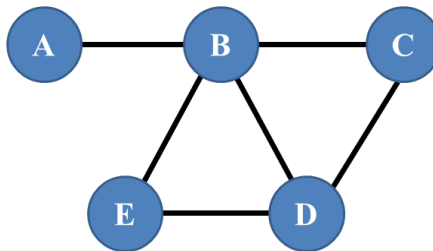
	Ali	Burak	Cezmi	Doğan	Erhan
Ali	0	1	0	1	1
Burak	1	0	1	0	0
Cezmi	0	1	0	1	1
Doğan	1	0	1	0	1
Erhan	1	0	1	1	0

Ağlar en temel şekilde yönlü ağlar (directed) ve yönsüz ağlar (undirected) olmak üzere ikiye ayrılmaktadır. Şekil 3.6.'da görülen yönlü ağlara örnek olarak Twitter uygulamasını göstermek mümkündür. Twitter'da B kişisi A'yı takip edebilirken, A'nın B'yi takip etmesi zorunlu değildir. Bu durumda ağ gösteriminde B'den A'ya doğru çizilen çizginin ucuna bir ok eklenmektedir. Şekil 3.7.'deki yönsüz ağlara örnek olarak ise Facebook uygulaması verilmektedir. Bu tür ağlarda karşılıklı bir ilişki bulunup, A kişisi B ile arkadaş ise B'nin A ile arkadaş olmaması ihtimali bulunmamaktadır (Tunalı, 2016: 7-8).

Şekil 3.6. Yönlü Ağ Örneği

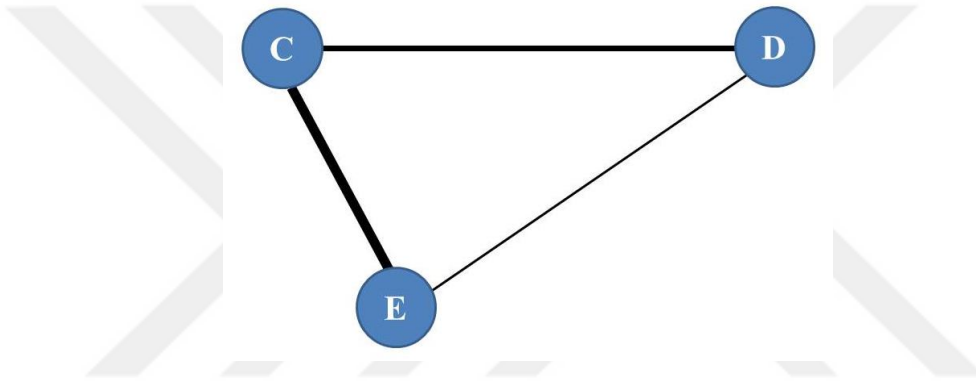


Şekil 3.7. Yönsüz Ağ Örneği



Ağlar, tartılı (weighted) ve tartısız (unweighted) ağlar şeklinde de tasnif edilebilmektedir. Örneğin cep telefonu ile iletişime geçen iki kişinin konuştuğu süre miktarı ağ için bir tartı olarak ele alınabilmekte, bu tür ağlar tartılı ağlar olarak adlandırılabilir. Bir kişinin bir diğer kişiye verdiği borç miktarı da ağ yapısı içerisinde bir tartı olarak ele alınabilmektedir. Şekil 3.8.'de görülen 3 düğümlü ve 3 bağlantılı bir ağda, bağlantıların güçlerinin birbirinden farklı olduğunu ortaya koymak amacıyla bağlantı çizgileri farklı kalınlıklarda gösterilmiştir. Buna göre C ile E arasındaki bağlantı çok kuvvetli, C ile D arasındaki bağlantı zayıf, D ile E arasındaki bağlantı ise en güçsüz bağlantı şeklinde gösterilmiştir (Gürsaka1 ve Uça Güneş, 2016: 24).

Şekil 3.8. Tartılı Ağlar



3.2. Sosyal Ağ Analizinde Ölçütler

Sosyal ağ analizi nicel ağ ölçütleri, analiz yapanların sosyal ağ içindeki bağlantı kalıplarını sistematik olarak incelemesine, ağları karşılaştırmasına, zaman içinde bir ağda meydana gelen değişikliklerin izlenmesine ve bir ağ içindeki bireylerin ve grupların göreceli konumlarının belirlenmesine imkân tanımaktadır. Örneğin, ağdaki düğüm sayısı ağdaki varlıkların sayısını, bağlantı ya da kenar sayısı ise düğümlerin aralarındaki bağlantıların sayısını göstermektedir. Merkezilik (centrality) ölçütleri, ağ içinde bir düğümün ne kadar “önemli” yani “merkezi” olduğunu ifade etmektedir (Hansen vd., 2020: 39). Bu çalışmada kullanılan ölçütler, okuma kolaylığı sağlaması amacıyla tablo şeklinde EK-A’da sunulmuştur.

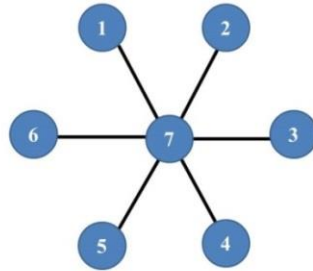
Bir ağın yoğunluğu ağda mevcut kenar sayısının, en fazla olası kenar sayısına oranıdır. Yoğunluk, bir ağın ortalama gücüdür. Bir ağın en yoğun olduğu durum, (yoğunluk değerinin 1 olması) her bir noktanın diğer noktalarla doğrudan bağlanmasını ifade etmektedir (Ağcasulu, 2018: 1923-1924). Bir ağın yoğunluğu, ağdaki bireyler arasındaki mevcut bağlantı sayısı ile; aynı ağdaki tüm bireylerin birbirine bağlı olduğu varsayılarak bulunan tüm bağlantıların sayısına oranını gösteren ölçüttür.

Ağ ölçütleri, ağları hem bütün olarak hem de düğümler bazında tanımlayan sayısal değerlerdir. Bu ölçütlerden merkezilik ağdaki en önemli düğümleri tespit etmeye yaramaktadır. Derece merkezliği (degree centrality) ise bir düğümün bağlı olduğu toplam kenar sayısını ifade ederek düğümün önemini belirlemeyi amaçlamaktadır. Yakınlık merkeziliği ölçütü (closeness centrality) bir düğümün ağdaki diğer düğümlere ne kadar yakın olduğunu göstermektedir (Tunalı, 2016: 42).

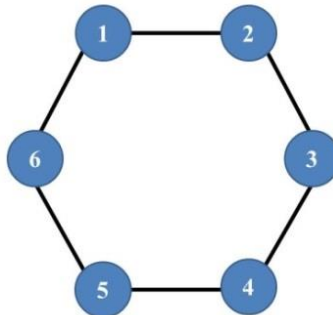
Merkezilik, bir ağda yer alan düğüm ve bağlantıların önem derecesini ortaya koymaya çalışan ölçüttür. Bir düğüm ya da bağlantı ne kadar çok sayıda birey ve grup arasında köprü görevi üstlenebiliyor, bilginin kaynağı haline gelebiliyorsa o kadar önemli hale gelmektedir. Merkeziliğin ölçülmesi ve merkezdeki düğümün belirlenmesi ağ içerisinde bilginin daha hızlı yayılmasını sağlayabilmektedir (Gürsakal ve Uça Güneş, 2016: 93).

Ağda yer alan bir elemana diğer elemanlar tarafından ne kadar kolay ulaşılabilirse, bir ağ elemanı ne kadar çok ağ elemanı arasında en kısa yollarla bağlanıyorsa o ağ elemanı merkezidir. Örneğin Şekil 3.9.'da yer alan yıldız şeklindeki ağda 7 numaralı düğüm merkezi iken, Şekil 3.10'da yer alan döngü şeklindeki ağda ise bütün düğümler eşit derecede merkezidir (Gürsakal ve Uça Güneş, 2016: 93).

Şekil 3.9. Yıldız Şeklindeki Ağlarda Merkezilik



Şekil 3.10. Döngü Şeklindeki Ağlarda Merkezilik



“İç derece merkeziliği”⁶² algoritması sosyal ağda en fazla etkileşimi alan bireyi (düğümü) öne çıkarmaktadır. “Dış derece merkeziliği”⁶³ ise diğer düğümlerle en çok ilişki kuran düğümü ön plana çıkarmaktadır. “Arasındalık merkeziliği”⁶⁴ ise ağ içerisindeki ilişkilerin merkezinde yer alan bireyi göstermektedir. Son olarak “özvektör merkeziliği”⁶⁵ özellikle sosyal medya analizlerinde en öne çıkan algoritma olup en çok etki sahibi olan, ağ içerisinde kurulan ilişkinin en önemli olduğu düğümü öne çıkarmaktadır. Özvektör merkeziliği bir sosyal ağdaki “kanaat önderlerini” tespit etmek için oldukça gereklidir (Kızılkaya ve Oğuzlar, 2017: 141).

Özvektör merkeziliği yönsüz ağlar için kullanılırken yönlü ağlar için aynı işlevi gören “sayfa değeri (page rank)”⁶⁶ algoritması kullanılmaktadır. Yakınlık merkeziliği (closeness centrality) ise her bir bireyin ağdaki konumunu diğer ağ ölçütlerinden farklı bir bakış açısıyla ölçerek, düğümler arasındaki ortalama mesafeyi ve bir düğüm ile diğer düğümler arasındaki ortalama mesafeyi ölçmektedir (Hansen vd., 2020: 41).

3.3. Sosyal Ağ Analizi

SAA, sosyal gruplar içerisindeki bireylerin birbirleriyle bağlantılarını ve davranışlarını incelemek için kullanılan bir metodolojidir (Clifton ve Webster, 2017: 442). Sosyal ağlardaki bağlantı ve düğümlerin arasındaki etkileşimlerin analizine SAA denilmektedir. Sosyal ağlardaki bireyler ve topluluklar hakkında çıkarımlar yapmaya yarayan SAA sayesinde; ağdaki en önemli, en etkili, en güçlü aktörlerin kimler olduğu; bireylerin ağ içerisindeki rollerinin ne olduğu; ağ içerisinde bilginin nasıl yayıldığı; bireylerin sosyal ortamdaki davranışlarının nasıl olduğu sorularını cevaplamak mümkündür (Tunalı, 2016: 2).

Günümüzde ağ denildiğinde aklımıza ilk olarak, düğümlerini insanların teşkil ettiği Twitter, Facebook, Instagram gibi sosyal ağ platformları gelmektedir. Sosyal ağların hayatımıza girmesiyle birlikte SAA kavramı daha fazla görünürlük kazanmıştır. SAA sosyal yaşamın, ilişkiler ve bu ilişkilerin oluşturduğu örüntülerle yaratıldığı hususunu başlangıç noktası olarak ele almaktadır (Gülpınar Demirci ve Çilingirtürk, 2020: 1).

⁶² “In degree centrality” algoritmasının Türkçe karşılığıdır.

⁶³ “Out degree centrality” algoritmasının Türkçe karşılığıdır.

⁶⁴ “Betweenness centrality” algoritmasının Türkçe karşılığıdır.

⁶⁵ “Eigenvector centrality” algoritmasının Türkçe karşılığıdır.

⁶⁶ “Page Rank” algoritmasının Türkçe karşılığıdır.

SAA, sosyal bilimlerde sosyal aktörler arasındaki etkileşimin incelenmesine dayanan yapısal yaklaşımdır. Sosyal ağ analistlerinin incelediği ilişkiler, genellikle insanları birbirine bağlayan ilişkiler olmaktadır. Ancak önemli sosyal ilişkiler, birey olmayan aktörleri de birbirine bağlayabilmektedirler. Ağ analistleri örgütler veya kuruluşlar hatta ulus devletler veya uluslararası ittifaklar arasındaki bağlantıları da inceleyebilmektedir (Freeman, 2004: 2).

SAA bir grubun veya daha büyük çaplı bir sosyal sistemin ilişki yapısı ve ağdaki aktörler arasındaki ilişki modelinden oluşmaktadır. Ağ kavramı, her bireyin diğer bireylerle bağları olduğu gerçeğini vurgulamaktadır. Sosyal ağ ifadesi, ağ içerisindeki aktörler kümesini ve aralarındaki bağları ifade etmektedir. SAA ile bir grubun yapısını ortaya koymak için aktörler arasındaki ilişkiler modellenmeye çalışılmakta, ardından bu modelin grubun işleyişi üzerindeki etkisi ve / veya bu yapının bireyler üzerindeki etkisi incelenmektedir (Wasserman ve Faust, 1994: 9).

SAA; örgütler, birimler, insanlar arasındaki ilişkilerin analiz edilerek haritalandırılmasını sağlamaktadır. SAA ağları değerlendirmek maksadıyla kullanılan sistematik bir araçtır. SAA, ağ içerisindeki çeşitli olayları ve olguları anlamayı sağlayan bir röntgen vazifesi görmektedir (Cross vd., 2001: 103).

Ağ analizi, sosyal davranışla ilgili olarak iki önemli varsayıma dayanmaktadır. Bu varsayımlardan birincisi, bir aktörün içerisinde birçok başka aktörün de bulunduğu sosyal bir sistem içerisinde yer aldığı ve aktörlerin birbirlerinin algılarını, inançlarını, eylemlerini ve karar alma süreçlerini etkileyebildikleridir. İkinci temel varsayım ise, toplumda çeşitli varlıklar arasındaki ilişki kalıplarından oluşan sosyal yapıların yer aldığıdır (Knoke ve Kuklinski, 1982: 9-10).

Ağ analizi sürecinde temel olarak iki ağ türü bulunmaktadır. “Tüm Ağlar (Whole Networks)” ve “Ego Ağları (Egocentric Networks)” birbiriyle ilişkili olsa da farklı konulara odaklanmaktadır. Tüm ağ çalışmaları, grup içindeki birimleri veya aktörleri birbirine bağlayan ilişki türleri hakkında veri toplayarak sosyal grupların yapısını ölçmeye çalışmaktadır. Ego ağları çalışmaları ise, bir veya birkaç aktöre odaklanarak, bu aktör ya da aktörlerin ilişkilerini ölçmeye çalışmaktadır. Tüm ağ çalışmaları bir anlamda ego ağları çalışmalarını da kapsamaktadır. Ego ağları üzerine yapılan çalışmalar daha sınırlı bir amaca sahiptir (Marsden, 2011: 370).

SAA'yı kullanarak yapılabilen üç ana araştırma alanı mevcuttur. Bunlardan birincisi ağın bütün yapısı, ikincisi ağ yapısı içindeki alt kümeler ve üçüncüsü ağ içerisindeki düğümlerdir. Başka bir deyişle, tek tek veya kümeler halinde bütünü oluşturan parçalar veya tüm ağın kendisi SAA'nın araştırma alanı içerisinde olabilmektedir (Fredericks ve Durland, 2005: 18).

SAA, sosyal ağları aktörler arasındaki ilişkiler açısından inceleyen, karmaşık sistemleri matematiksel olarak ifade eden, tanımlayıcı ve ampirik bir disiplindir (Benhiba vd., 2017: 148). SAA'nın kendine has özellikleri bulunmaktadır. Bu kapsamda SAA, sosyal aktörleri birbirine bağlayan bağlara dayanan bir analiz yöntemidir. SAA, sistematik ampirik verileri esas almaktadır. Yine SAA büyük ölçüde grafik tasvirlerle; matematiksel ve / veya hesaplamalı modellerin kullanımına dayanmaktadır (Freeman, 2004: 3).

SAA'nın asıl amacı; çıplak gözle görülmesi mümkün olmayan şeylerin görülebilmesini sağlamaktır (Kadushin, 2005: 142). SAA ile tanımlama, görselleştirme ve modelleme ile ağın yapısının anlaşılması amaçlanmaktadır. Sosyal ağ analizinin bir diğer önemli amacı, takip edilen ağı açıklamak için, aktörler arasındaki bağların modellenmesidir (van Duijn ve Vermunt, 2006: 2-3).

SAA'nın amacı; gizli, örtülü sosyal modelleri ortaya çıkarmaktır. Sosyal ağ analizinin gücü, bireysel sosyal aktörlerin niteliklerini analiz etmeye odaklanan geleneksel yöntemlerden çok daha fazladır. Sosyal ağ analizinde, bir ağdaki sosyal aktörler arasındaki ilişkiler ve bağlar, bireylerin kendi özelliklerinden daha önemli ve bilgilendirici olarak kabul edilmektedir (Tripathy vd., 2018: 48)

SAA, birbirleriyle etkileşimde bulunan birimler arasındaki ilişkilerin önemli olduğu varsayımına dayanmaktadır. Birimler arasındaki bağlantılarla tanımlanan ilişkiler, ağ teorilerinin temel bileşenidir (Wasserman ve Faust, 1994: 4). SAA'da, sosyal aktörlerin özellikleri aktörler arasındaki bağ kalıpları veya yapıları açısından incelenmektedir. SAA'da, aktörler arasındaki ilişki bağları birincil öncelikli, aktörlerin nitelikleri ise ikincil öncelikli olarak analiz edilmektedir (Wasserman ve Faust, 1994: 8). SAA'da her bir düğümün önemini belirlemek veya kullanıcılar arasındaki gizli ilişkileri ortaya çıkarmak için ağın yapısal bilgileri kullanılarak bir analiz yapılmaktadır (Behera vd., 2018: 3).

SAA; bir grubun oluşumu, grup içindeki uyum, grup içindeki sosyal roller gibi hususları açıklamaya yardımcı olabilmektedir. SAA aşağıdaki önemli sorulara cevap bulabilmektedir (Hansen vd., 2020: 48-49).

- Bir sosyal grup içinde ne tür sosyal roller oynanmaktadır?
- Bu grupta önemli rolleri yerine getiren yeterli sayıda birey mevcut mu?
- Grup içinde hangi bireyler önemli sosyal roller oynamaktadır?
- Ağ içerisindeki konumuna bağlı olarak kim iyi bir yönetici olabilir?
- Ağ içerisinde hangi alt gruplar mevcut?
- Alt gruplar arasında da bağlantılar mevcut mu?
- Grupları birbirine bağlayan köprü rolünü kim oynuyor?
- Fikirler ağ üzerinden nasıl yayılıyor?
- Fikirlerin yayılmasını tetikleyen etki ajanları kimlerdir?
- Belirgin bir olaydan sonra bu sosyal ağın genel yapısı nasıl değişmektedir?

SAA kullanılarak, ağ içerisindeki bireylerin nitelikleri incelenmeden bireyler aralarındaki ilişkilerin örüntüleri incelenebilmektedir. Bu tür analizler, bir bütün olarak ağın özelliklerine odaklanmaktadır. Bu çerçevede bağlantılar, ağdaki birimler arasında var olan herhangi bir ilişki olabilmektedir. Örneğin ağ bireyleri arasındaki bağlantılar; akrabalık, maddi işlemler, kaynak akışı gibi ilişkilerden oluşabilmektedir (Wasserman ve Faust, 1994: 8).

SAA, sosyal grupların birbiriyle olan ilişkisiyle ilgilenmektedir. SAA, bireysel davranışları, tutumları ve inançları analiz etmek yerine, birbirleriyle etkileşim halindeki aktörlerin teşkil ettiği grup davranışları, bu etkileşimlerin incelenip analiz edilebildiği bir yapıya odaklanılmaktadır (Tripathy vd., 2018: 48).

SAA teorisi, bireysel aktörlerin rasyonel seçimleri ile değil aktörler arasındaki sosyal bağlantılar ve ilişkilere odaklandığı için diğer sosyal bilimler disiplinlerinden ayrılmaktadır (Fredericks ve Durland, 2005: 15). SAA, aktörlerin bireysel özelliklerine değil, aktörler arasındaki ilişkilerin örüntülerine odaklanması açısından sosyal bilimlerde benzersizdir. Söz konusu aktörler; bireyler, gruplar, kuruluşlar veya birbirleriyle etkileşime giren diğer bireyler olabilmektedir. SAA, aktörler arasındaki hem makro hem de mikro bağlantıları; nicel, nitel ve grafiksel bir yaklaşımla inceleme yeteneği sağlamaktadır (Fredericks ve Durland, 2005: 17).

Alanyazında, sosyal ağ analizinin yalnızca sosyal bilimler alanında değil çok farklı disiplinlerde sıklıkla kullanıldığı görülmektedir. Bu çerçevede sosyal ağ analizi; sağlık hizmetlerinin halka daha etkin biçimde ulaştırılması (Introcaso, 2005); ikmal ve lojistik

sistemlerinin iyileştirilmesi (Carter vd., 2007); kanserin önlenmesi için çalışan kurumlar arasındaki iş birliğinin ortaya konulması (Luque vd., 2010); araç sigorta dolandırıcılığının tespit edilmesi (Šubelj vd., 2011); bilimsel iletişimin yapısal olarak ortaya konulabilmesi için atıf ağı analizinin kullanılması (Marion vd., 2005); farklı işlerde çalışan kişilerin hangi iletişim araçlarını tercih ettiğinin tespit edilmesi (Haythornthwaite vd., 1995); ekonomik kaynakların coğrafi dağılımının analiz edilmesi (Ter Wal ve Boschma, 2008); güvenilir çevrimiçi mezat satıcılarının tespiti (Wang ve Chiu, 2008); uyuşturucu kaçakçılığı ağının belirlenmesi (Bright vd., 2011); organize suç örgütlerinin açığa çıkarılması (Schwartz ve Rouselle, 2008) gibi oldukça farklı alanlarda, farklı disiplinler tarafından kullanılmıştır. Sosyal ağ analizinin etkin olarak kullanılabileceği bir diğer alan ise terörizmle mücadeledir.

3.4. Terörizmle Mücadelede Sosyal Medya İstihbaratı Analiz Yöntemi Olarak Sosyal Ağ Analizi

Ağ analizinin suç istihbaratına uyarlanmış hali olan ilişki / bağlantı analizi (link analysis) 1970’li yılların başından bu yana suç istihbaratında kullanılan temel tekniktir. Günümüzde sosyal ağ analizi de suç istihbaratında kullanılmış ve SAA istihbarat çalışmalarına dâhil edilmiştir (Strang, 2014: 2). İlişki analizi, suça karışan bireylerin birbirleriyle ve örgütle bağlantıları ile bireylerin suçla ilgili yerler, nesneler ve olaylarla bağlantılarını araştırmaktadır (Strang, 2014: 4).

Suç istihbaratının amacı, suç işleyen bireylerin oluşturduğu ağ yapısının ortadan kaldırılması ve işlevinin bozulmasını sağlamaktır. Bu ağların kritik unsurlarını keşfetmek ve ağları haritalamak amacıyla analitik ve bütüncül bir yaklaşım gerekmektedir. Bu maksatla SAA’ni kullanan istihbarat uzmanının temel soruları; “Ağ nasıl işliyor?” ve “Bu ağ nasıl sonlandırabiliriz?” şeklinde olmalıdır (Strang, 2014: 25).

Son yirmi yılda SAA alanındaki gelişmeler, bir ağ içerisinde hangi bireylerin en önemli role sahip olduğunun bulunabilmesine yarayan fırsatlar sağlamaktadır. SAA uygulamaları, terör örgütlerinin tedarik, saldırı hazırlığı gibi faaliyetlerine yönelik öngörüler sağlamaktadır. SAA ayrıca suç ağlarının kritik gereksinimlerini ve yeteneklerini belirlemeye yardımcı olmaktadır. Organize suç ve terör örgütlerinin faaliyetlerini kesintiye uğratabilmek için amaç, bu ağların işlevlerini ve yapılarını bozmaktır (Strang, 2014: 25).

Terör örgütü davranışlarının daha iyi anlaşılması, terörizmle mücadelenin daha etkili yürütülmesini sağlayabilmektedir. SAA ağların yapısını modellemek için kullanılmaktadır.

SAA çeşitli terörizmle mücadele stratejilerinin test edilebileceği ve öngörücü modellerin geliştirilebileceği terör ağlarını sentezlemek için kullanılabilir. SAA, ağ içerisinde kilit konumda olan bireylerin tanımlanmasını ve düğümleri ortadan kaldırarak ağ işleyişinin nasıl bozulabileceğinin ortaya konulmasını içermektedir. Genel fikir birliği, SAA'nın terörizm çalışmalarına artı değer kattığı ve terörizmle mücadele yeteneklerini artırma potansiyeline sahip olduğu yönündedir (Mullins, 2013: 67).

Hasmın hedeflerini anlayabilme istihbarata olan ihtiyacı daha fazla ön plana çıkartmaktadır. Bugün dünyada büyük bir kaos ortamı yaratan terör örgütleriyle mücadele için de benzer bir strateji gerekmektedir. Gizli faaliyet gösteren örgütlerin ağ yapılarının analizi ve anlaşılması, bu örgütlerin eleman temini gayretlerinin ortaya konulması, örgütlerin motivasyonlarının anlaşılması, terörist faaliyetlerin icrası ile eylemlerin kontrolünü sağlamak için hangi yöntemleri kullandıklarının anlaşılması anlamına gelmektedir (Hamill vd., 2008: 27). Terör örgütlerinin belirtilen özellikleri bir kez anlaşıldığında bu bilgi ışığında kilit rol oynayan kişilerin, kişiler arası ilişkilerin tanımlanması, belirlenen ağın ortadan kaldırılması için zayıf noktaların belirlenmesi mümkün olabilmektedir. Bu amaca ulaşabilmek için bazı fırsatlar sunan analiz yöntemi ise SAA'dır (Hamill vd., 2008: 27).

İç güvenlik tehditlerinin değişen doğası nedeniyle, iç güvenliğin sağlanması için yeni bir istihbarat türüne ihtiyaç duyulmaktadır. Bu yeni istihbarat türü, ağ bilimi ya da ağ sosyolojisi olarak da bilinen SAA yöntemidir. SAA'nın temelini, düğümlerin (ağ türüne bağlı olarak insanlar, olaylar vb. olabilir) ağları oluşturan karmaşık ancak anlaşılabilir ilişkilerle birbirine bağlanması meydana getirmektedir. Söz konusu ağlar, birçok doğal olayın, organizasyonun ve sosyal sürecin yapısal temelini oluşturmaktadır (Ressler, 2006: 1).

John Arquilla ve David Ronfeldt'in editörlüğünü yaptığı "Ağlar ve Ağ Savaşları: Terör, Suç ve Militanlığın Geleceği (Networks and Netwars: The Future of Terror, Crime and Militancy)" adlı kitap, savaşların artık tarafların karşı karşıya geleceği mücadeleler şeklinde olmayacağını ifade etmektedir. Buna göre artık ağ şeklinde örgütlenmiş teröristler, suçlular ve aşırılık yanlılarının yaratacağı düşük yoğunluklu bir savaş olan ağ savaşları yaşanacaktır. Bu ağlar genellikle leadersiz olup diğer örgütlenmelere göre daha hızlı saldırılar düzenleyebilmektedirler. Bu çerçevede ağ savaşları terimi gelecekteki ağ temelli çatışmalara dikkat çekmek amacıyla üretilmiştir (Arquilla ve Ronfeldt, 2001: 6-7).

Terör örgütleri belirli bir ideoloji etrafında şekillenen, ülkeleri ve kıtaları kapsayacak biçimde, bireylerin meydana getirdiği ağlardan oluşan yapılar olduğundan, SAA yöntemi ile incelenebilecek örgütlenmelerdir. Terör örgütleri, liderlik ve örgütsel yapı gibi özellikleri bakımından; hiyerarşik devlet organizasyonlarından farklılık göstermektedirler. SAA, terör örgütü ağının gelişimi, örgüte eleman temini ve radikal fikirlerin yayılması gibi konularda önemli bilgiler sağlayabilmektedir. Bir terör örgütünün ağ yapısı; yeni fikirlere erişme, örgüte yeni elemanlar sağlama ve uzun vadede faaliyetlerini sürdürebilme yeteneklerini etkilemektedir. SAA terörist ağları anlamak ve iç güvenlik bürokrasisini bilgilendirmek amacıyla kullanılabilir (Ressler, 2006: 2).

İstihbarat analistlerinin görevi, çok büyük miktardaki veriyi anlamlandırmak ve bir konu hakkında durumsal farkındalığı artırmaktır. Varlıklar ve bu varlıklar arasındaki ilişkiler söz konusu olduğunda istihbarat analistleri için en kullanışlı araç SAA'dır. SAA özellikle yüksek değerlikli hedefleri (high value targets) belirlemek konusunda aydınlatıcı olabilmektedir. SAA uygulamaları istihbarat analistlerine ve servislerine bir konuya odaklanma, bir konu hakkında analiz yapabilme, bir ağın temel özelliklerinden yararlanabilme imkânları sağlayarak; zamandan, paradan ve insan gücünden tasarruf sağlamaktadır (Waskiewicz ve LaMonica, 2008: 1). Bir terör ağı analiz edilirken, bilgi akışını kontrol altında bulunduran kişinin (düğümün) tespiti ve kritik olarak adlandırılan bu düğümün ağdan çıkartılması önem arz etmektedir. Örneğin bir terör ağı analizi, bomba yapımında kullanılan malzemelerin terör örgütlerince teminini önlemek amacını taşıyabilmektedir (Waskiewicz ve LaMonica, 2008: 2).

Terörizmle mücadele istihbaratı çerçevesinde sosyal ağ analizi kullanılırken, incelenen ağın ağırlık merkezinin tespiti hedeflenmektedir. Bunun temel nedeni bir ağın ağırlık merkezinin, ağdaki kritik yetenekler, güvenlik açıkları ve ağın ihtiyaçları gibi özelliklerini bir arada barındırmasıdır. Bir ağdaki ağırlık merkezini bulmak için, özvektör merkeziliği ölçütünün kullanılması gerekmektedir. Bir ağdaki yüksek özvektör merkeziliğine sahip bir düğüm, ağdaki ağırlık merkezinin özelliklerini sergilemektedir (Waskiewicz ve LaMonica, 2008: 5).

Uyuşturucu tacirlerinden terör örgütlerine kadar farklı nitelikteki suç örgütlerine yönelik istihbarat analizinde kullanılabilen ağ analizi yöntemleri; örgütün merkezinde yer alan kişileri, örgütten koparılması durumunda örgütü işlevsiz hale getirebileceklerin kimler olduğunu, bir örgüt içinde belirlenen bir kişinin hangi rolleri üstlendiği, uluslararası bir

terör ağı içerisinde hangi iletişim bağlantılarının takibe değer olduğu sorularına yanıt bulmaya çalışmaktadır (Sparrow, 1991: 251-252).

3.5. PKK Terör Örgütü Sempatizanlarının Sosyal Ağ Analizi

3.5.1. Araştırmanın Yöntemi

Tezin yöntemi, Yalçinkaya ve arkadaşları tarafından yapılan “Türkçe Konuşan DEAŞ Destekçileri Üzerine Twitter Sosyal Ağ Analizi” isimli çalışmanın yönteminden uyarlanmıştır (Yalçinkaya vd., 2016). Bu kapsamda tezin yöntemi üç temel aşama üzerine inşa edilmiştir. Bunlardan birincisi Twitter sosyal medya uygulamasını etkin olarak kullanan PKK terör örgütü sempatizanlarına ait hesapların tespiti, ikincisi çekirdek Twitter hesapların takip ettiği hesapların tespiti, ayıklanması ve verilerin toplanması, üçüncüsü ise toplanan verilerin NodeXL Pro programı ile analiz edilmesi ve sosyal medya istihbaratına dönüştürülmesidir.

Sosyal ağ uygulamalarından Twitter’ı temel alan bu araştırmada, Twitter’dan PKK terör örgütü sempatizanlarına ait verilerin toplanması, ölçütlerin hesaplanması ve analizi, PKK sempatizanlarının tweet içeriklerinin analiz edilmesi amacıyla NodeXL Pro isimli uygulama kullanılmıştır. Tespit edilen PKK sempatizanlarına ait hesapların üst verilerinin elde edilmesi için çevrimiçi bir uygulama olan “Tweet Beaver”⁶⁷ tercih edilmiştir. Toplanan verilerin ayıklanması manuel olarak gerçekleştirilmiştir. Elde edilen verilerin görselleştirilmesinde ise NodeXL Pro ve “Gephi 0.8 Alpha” (Bastian vd., 2009) isimli programlar kullanılmıştır.

Bu çalışmada, hem verileri toplayabilmesi hem de sayısal olarak ağ analizi yapabilmesi, üzerinde çalışılan ağı temel olarak görselleştirebilmesi nedeniyle NodeXL Pro uygulamasının kullanımı tercih edilmiştir.

Tezde Twitter üzerinden veri toplanarak, Twitter verilerinin analiz edilmesine yoğunlaşılmasının nedeni, Twitter’daki her bir tweetin az sayıda karakter ile sınırlandırılmış olması ve bilginin özünü taşımasıdır (Ekşim ve Civelek, 2019: 830). Twitter paylaşımlarının günümüzde 280 karakterle sınırlandırılmış olması nedeniyle Twitter paylaşımları ya da tweetler kısa ve öz bilgileri içermektedir.

Twitter; gerçek bilgi, fikir, düşünce ve diğer bilgileri içerebilen bir platformdur. Twitter içerisinde, ortak ilgi alanlarına sahip kullanıcılar ya da kendisini bir topluluğun

⁶⁷ <https://tweetbeaver.com/index.php>

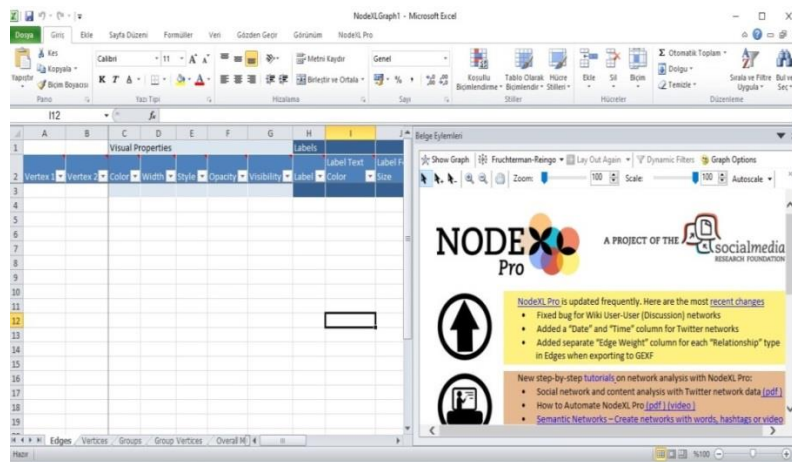
parçası hissedenler tarafından çok sayıda ve çeşitli topluluklar üretilmektedir. Twitter gibi sosyal ağ türleri, bilgi akışının karşılıklı olmadığı durumlarda bireyler arasındaki ilişkilerin izlenmesine izin vermektedir. En basit haliyle Twitter’da bir düğüm, başka bir düğümün takipçisidir. Takipçi sayısı, ağ içindeki bir düğümün popülerliğini tanımlamaktadır (Fornacciari vd., 2015: 53). Twitter, her kullanıcının bir dizi başka kullanıcıyı (takipçiler) izlemeyi seçebileceği ve benzer şekilde diğer kullanıcılar (takipçiler) tarafından takip edilebildiği yönlü bir ağ olarak yapılandırılmıştır (Fornacciari vd., 2015: 56).

Sosyal medya uygulamalarından Twitter’ın tercih edilmesinin bir diğer nedeni, terör örgütlerince bu uygulamanın sıklıkla kullanılıyor olmasıdır. Boko Haram’dan PKK’ya, El Kaide’den DEAŞ’a kadar çok sayıda terör örgütü bu platformlarda yer almakta ve bu uygulamaları değişik maksatlarla kullanılmaktadır. Twitter’ın tercih edilmesinin başka bir nedeni ise Twitter’ın politika olarak API kullanarak, kısıtlanmış miktarda dahi olsa, araştırmaya yönelik veri teminine izin vermesidir. Twitter’ın API platformu, Twitter kullanıcılarının kamuoyu ile paylaştığı açık verilere erişim izni vermektedir.

Tez kapsamında, yönteme ilişkin verileri elde etmek maksadıyla Twitter API platformuna başvuru yapılmış, API izni alınmış, Twitter’dan temin edilen API; NodeXL ve TweetBeaver uygulamalarında kullanılmıştır.

Sosyal medyadan veri toplayarak; bireyler, paylaşımlar, nesneler arasındaki görünmeyen bağları görselleştirmek için veri toplanan ağları görselleştiren, bilgisayar tabanlı uygulamalar, araçlar üretilmiştir. Bu araçlardan birisi akademisyen ve araştırmacılar tarafından ortaklaşa geliştirilen, kullanım kolaylığını ön planda tutan NodeXL Pro programıdır (Sert Etman vd., 2014: 3). Şekil 3.11.’de NodeXL Pro’ya ait bir arayüz örneği görülmektedir.

Şekil 3.11. NodeXL Arayüzü



Microsoft Excel tabanlı bir şablon olan NodeXL Pro uygulaması, Flickr; Wikipedia, YouTube ve Twitter sosyal ağlarından veri toplayabilmektedir.⁶⁸ NodeXL Pro uygulamasında sosyal ağ analizine ilişkin veriler, manuel olarak da girilebilmektedir. Sosyal ağlardan elde edilen verilerin teşkil ettiği ağlar, NodeXL Pro sayesinde çeşitli algoritmalarla görselleştirilebilmektedir. NodeXL Pro uygulaması; yoğunluk, derece, arasındalık gibi ağı tanımlayan gerekli istatistikleri otomatik olarak hesaplayabilmekte, ağı analiz edilebilmektedir. NodeXL Pro'nun filtreleme ve görüntüleme özellikleri, sosyal ağın önemli yapılarını vurgulamak için kullanılabilir (Sert Eteman vd., 2014: 3).

Bu çalışmada sosyal medyadan verilerin toplanması ve analizi amacıyla NodeXL Pro uygulamasının seçilmesinin birkaç nedeni bulunmaktadır. Bunlardan birincisi NodeXL Pro'nun kullanıcı dostu olması, bazı kısıtlamaları bulunsu da “NodeXL Temel (NodeXL Basic)” uygulamasının ücretsiz, “NodeXL Pro” uygulamasının ise diğer SAA uygulamalarına göre oldukça ucuz olmasıdır.

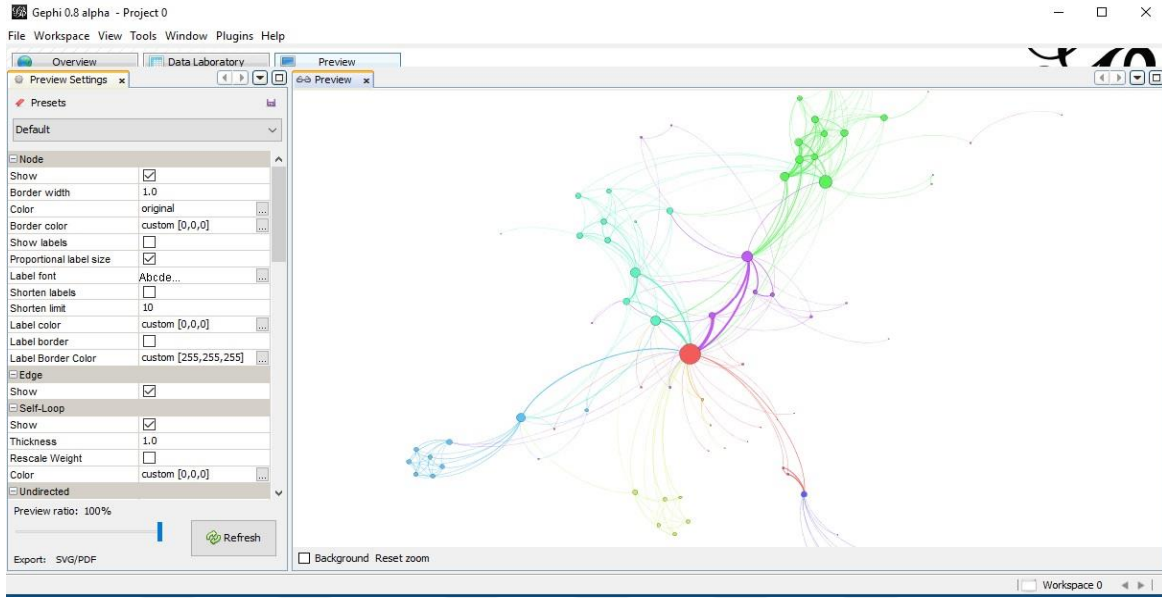
NodeXL Pro'nun tercih edilmesinin ikinci nedeni, NodeXL Pro ile sosyal medyadan hem verilerin toplanabilmesi hem de görselleştirilerek analiz edilebilmesidir. Üçüncüsü ise NodeXL Pro'nun diğer uygulamalara göre daha kolay kullanılabilmesidir. Microsoft Excel tabanında çalışan NodeXL Pro, programlama bilgisi olmayan kullanıcılar için kolay bir kullanım imkânı sunmaktadır. NodeXL Pro'nun en büyük kısıtlılığı, analiz sonuçlarını görselleştirme seçeneklerinin sınırlı olmasıdır.

Gephi, ağ analizi yapmayı sağlayan, analizi grafik olarak sunabilen bir bilgisayar yazılımıdır. Gephi yazılımı, büyük veri kümeleriyle görsel olarak çalışmaya olanak sağlamaktadır. Sosyal ağların araştırılması ve yorumlanmasını sağlayan Gephi, ağ görsellerini filtrelemeye, ağ içerisinde gezinmeye, ağları kümelemeye izin vermektedir (Bastian vd., 2009: 1). Bu çalışmada Gephi; hem ücretsiz kullanıma imkân vermesi hem de NodeXL Pro uygulamasına göre ağ görselleştirmesini daha ayrıntılı yapması nedeniyle tercih edilmiştir.

NodeXL Pro'nun veri görselleştirme sınırlılığını ortadan kaldırabilmek için, NodeXL Pro ile toplanan veriler Şekli 3.12.'de arayüz örneği görülen Gephi 0.8 Alpha programı kullanılarak görselleştirilmiştir.

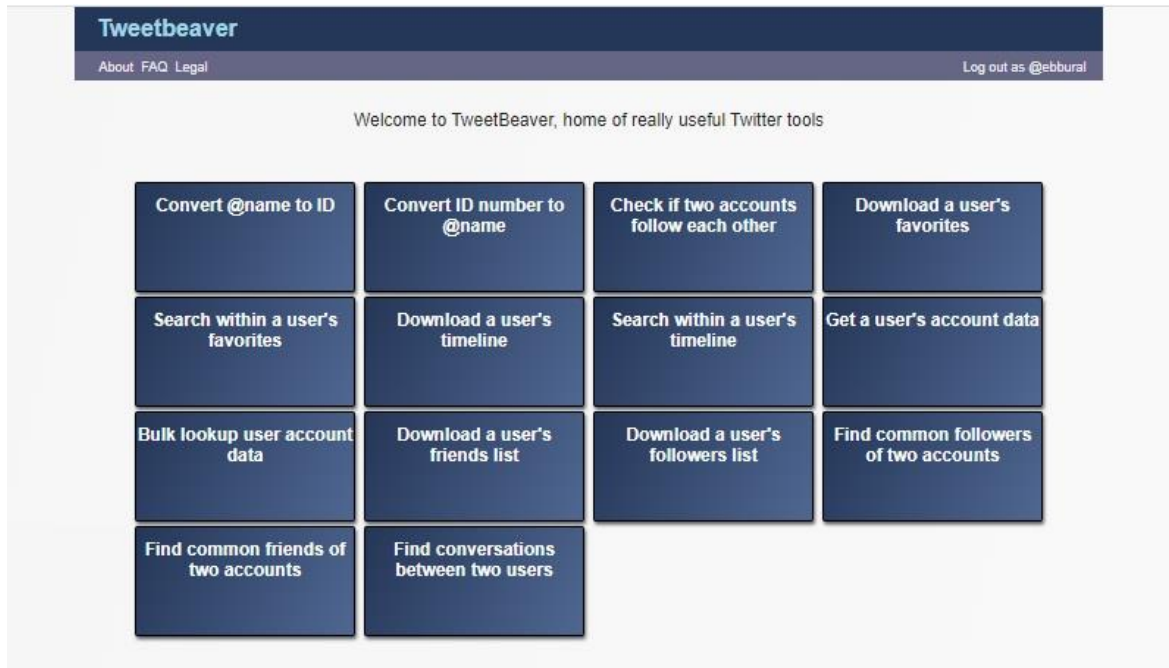
⁶⁸ NodeXL Pro uygulamasında Facebook'tan veri elde etmeye yönelik seçenekler bulunsu da, tezin hazırlandığı dönem itibarıyla Facebook uygulamasının kısıtlamaları nedeniyle Facebook'tan veri elde etmeye yönelik fonksiyonlar çalışmamaktadır.

Şekil 3.12. Gephi 0.8 Alpha Programı Arayüzü



Twitter hesaplarına ait üst verilerin toplanabilmesi için ise internet üzerinde çevrimiçi olarak kullanılabilen, Şekil 3.13’de arayüzü görülen TweetBeaver isimli uygulama kullanılmıştır. TweetBeaver, kullanımı oldukça kolay ve veriye hızlı erişebilen bir uygulama olması nedeniyle bu çalışmada tercih edilmiştir. TweetBeaver uygulaması Twitter API’den izin alarak çalışmakta, Twitter üzerinden belirli bir kullanıcının son 3.200 paylaşımını çekebilmekte, söz konusu son 3.200 tweet içerisinde anahtar bir kelimeyi arayabilmekte, bir kullanıcının en son beğendiği 200 tweeti bulabilmektedir.

Şekil 3.13. TweetBeaver Uygulamasına Ait Arayüzü



TweetBeaver ayrıca, belirlenen bir kullanıcının Twitter kullanıcı adı; Twitter kimlik numarası; Twitter adı; Twitter biyografi tanımlaması; hesabın kullanıma açılma tarihi; hesabın kullanıldığı yer; varsa Twitter hesabının bağlı olduğu internet sayfası; coğrafi koordinatları; kullanılan dil tercihi; bugüne kadar paylaşılan tweet miktarı; kullanıcıyı takip eden kişi sayısı; kullanıcı tarafından takip edilen kişi miktarı; hesabın koruma altında olup olmadığı ve son olarak hesaba ait profil resminin yer aldığı internet sayfası adresini elde edebilmektedir. Bu özelliklerine ilaveten TweetBeaver, bir kullanıcının takip ettiği kişilerin listesini; bir kullanıcıyı takip eden kişilerin listesini; iki Twitter kullanıcısını birden takip eden ortak hesapları; iki Twitter kullanıcısının birden takip ettiği ortak hesapları ve son olarak varsa iki kullanıcının tweetleri arasında etkileşime ilişkin veriler toplayabilmektedir. TweetBeaver'dan elde edilen veriler bilgisayar ekranında görüntülenebildiği gibi verilerin virgülle ayrılması anlamına gelen "csv" (Comma Separated Values - Virgülle Ayrılan Değerler) formatında kaydedilebilmektedir.

Tez kapsamında, PKK terör örgütü sempatizanlarının Twitter'dan alınan veriler içerisinden elde edilen paylaşım metinlerinin içerik analizlerini yapmak, metinlerden kelime bulutları oluşturabilmek için ise internet üzerinde çevrimiçi çalışabilen WordClouds⁶⁹ uygulaması kullanılmıştır. WordClouds uygulamasının tercih edilmesinin temel nedeni Türkçe kelimeler ve karakterlerle uyumlu çalışmasıdır.

3.5.2. Yöntem Uygulaması Birinci Aşama: PKK Terör Örgütü Sempatizanlarına Ait Twitter Hesaplarının Tespit Edilmesi

Bu araştırmada PKK terör örgütü sempatizanlarına ait Twitter hesaplarının tespiti amacıyla "kartopu örnekleme" yöntemi kullanılmıştır. Kartopu örnekleme yöntemi, araştırma evrenini oluşturan alt elemanlara ulaşmanın mümkün olmadığı, ya da araştırma evreni hakkındaki bilgilerin daha az olduğu durumlarda kullanılmaktadır. Kartopu örnekleme yöntemiyle, verinin elde edilebileceği kişiler bulunup, bu kişilerden araştırma evrenine ulaşmak hedeflenmektedir (Baltacı, 2018: 253).

Kartopu örnekleme yöntemi çerçevesinde, ayrıntısı ile aktarılacağı üzere öncelikle PKK terör örgütüne müzahir Twitter etiketleri tespit edilmiş, daha sonra bu etiketleri esas alarak paylaşım yapan muhtemel sempatizanlar bulunmaya çalışılmıştır. Müteakip aşamada ise kesinlikle PKK sempatizanı olduğu düşünülen hesapların takip ettiği (following) hesaplara ait bilgiler toplanarak, kartopu şeklinde veriler çoğaltılmış, araştırmanın örnekleme oluşturulmuştur.

⁶⁹ <https://www.wordclouds.com/>

Sosyal medya uygulamalarından Twitter üzerinde PKK terör örgütü sempaticanlarını tespit edebilmek maksadıyla 01 Aralık 2020 tarihinde anonim bir Twitter hesabı oluşturulmuştur. Anonim bir Twitter hesabı açılmasının nedeni, PKK sempaticanlarının daha kolay tespit edilebilmesi; PKK sempaticanlarının bulunduđu grupların izlenebilmesidir. Araştırmanın tamamlanmasını müteakip açılan anonim Twitter hesabı kapatılmıştır.

Araştırmanın evrenini oluşturan “PKK sempaticanlarına ait Twitter hesaplarının” tamamını tez kapsamında inceleyebilmek mümkün görünmemektedir. Bu maksatla araştırmanın örneklemini oluşturmak için incelenecek Twitter hesap sayısı 50 hesap ile sınırlandırılmıştır. Örneklemin 50 adet Twitter hesabı ile sınırlandırılmasının temel nedeni, tespit edilen Twitter hesaplarına ilişkin tasnif ve ayıklama işlemlerinin manuel olarak, elle yapılacak olması, elle yapılan işlemin bilgisayar destekli işlemlere göre uzun bir zaman dilimini kapsayacak olmasıdır. Zira kartopu örnekleme yöntemi neticesinde, PKK sempaticanı olduđu değerlendirilen hesapların takip ettikleri hesaplar da örnekleme dâhil edilecektir. Araştırma süresince elde edilen tecrübe neticesinde, 50 Twitter hesabından oluşan bir veri setinin kartopu örnekleme yöntemi ile 70 katına kadar çıkabileceği, bunun neticesinde ise yaklaşık 3.500 - 4.000 Twitter hesabının incelenmesi gerekebileceği öngörülmektedir.

İkinci neden ise, Twitter verilerinin toplanması maksadıyla kullanılacak NodeXL Pro uygulamasının belirli bir düğüm sayısı aşıldığında veriyi elde etmekte zorlanması hatta veri toplama işlemini yarıda bırakmasıdır. Araştırma süresince yapılan denemelerde NodeXL Pro ile Twitter’den en fazla 9.999 kullanıcıya ait verinin toplanmasının mümkün olduđu ancak uygulamada 3.000’den fazla kullanıcının verilerine erişimde gerekli zamanın bazı durumlarda günlerle ifade edilebildiği ve hatta toplama işleminin tamamlanamadığı tecrübe edilmiştir.

Birinci aşamada, PKK terör örgütünün Twitter’daki sempaticanlarından 50’sini tespit edebilmek maksadıyla, son dönemlerde sempaticanlar tarafından açıldığı değerlendirilen; #SayinÖcalan, #PKK43yasında, #PKKisNotTerrorist, #BijiSerokApo, #PkkHalktırHalkBurada, #DelistPKK, #GlobalFreedom4OcalanDay, #YpsParastinaGele etiketleri, 01 Ocak 2021 ile 31 Ocak 2021 arasındaki dönemde, açılan anonim Twitter hesabı üzerinden incelenmiştir. Belirtilen etiketler kullanılarak paylaşılan tweetler ve paylaşım yapan hesaplar, bilgisayar yardımı olmaksızın manuel olarak incelenmiştir.

İnceleme öncesinde, söz konusu hesapların PKK terör örgütü sempatzanı olup olmadığını anlamak için kriterler belirlenmiş, bu kriterlere uygun görülen Twitter hesapları araştırma kapsamına dâhil edilmiştir. Belirlenen kriterlerden birincisi Twitter hesabı profil ve kapak fotoğraflarının; Abdullah Öcalan, PKK flaması, kamuoyunda bilinen ve kahramanlaştırılmış PKK'lı teröristleri, terör örgütü kıyafeti giyen şahısları, PKK'yı simgeleyen işaretleri içermesidir. İkinci kriter ise hesap içeriklerinde PKK terör örgütünü ya da terör örgütü liderini destekleyen paylaşımların mevcut olmasıdır. Yöntemin belki de en zaman alıcı bölümü PKK terör örgütü sempatzanlarına ait Twitter hesaplarının tespiti ve ayıklanması aşamasıdır. Bu çalışma sonucunda 50 adet Twitter hesabı tespit edilmiş ve 20 gün süreyle izlemeye alınmıştır.

İnceleme süreci sonunda; 13 hesabın askıya alınarak erişiminin engellendiği, 8 Twitter hesabının ise hesabını koruma altına aldığı⁷⁰ görülmüştür. Yapılan ilk inceleme sonucunda söz konusu 21 hesap, 50 hesaplık veri setinden çıkarılmış, toplamda 29 adet hesap kalmıştır. Hesapların tespit ve ayıklanması aşamasında ikinci olarak; 20.000'den fazla takipçisi olan, 2.000'den fazla hesabı takip eden hesaplar veri setinden ayrılmıştır. Bu işlemin temel nedeni; terör örgütlerinin güvenlik güçlerince takibe alınmaktan kaçınmak maksadıyla çok sayıda ilgisiz hesabı takip etmeleri, kendilerini çok sayıda hesap tarafından takip ettirmeye çalışmalarıdır (Berger ve Morgan, 2015: 41). Bu kapsamda yapılan ayıklama işleminin ardından 7 hesap daha veri setinden ayrılmıştır. Birinci aşamada PKK terör örgütü sempatzanı olarak değerlendirilen toplam 22 adet çekirdek hesap kalmıştır. Çekirdek hesaplar, PKK terör örgütü sempatzanı oldukları, belirlenen kriterler çerçevesinde doğrulanan ve uygulamalar vasıtasıyla veri elde etmeye imkân tanıyan hesaplardır.

Belirlenen 22 adet çekirdek Twitter hesabına ait kullanıcı bilgileri, TweetBeaver uygulaması kullanılarak toplanmıştır. Elde edilen kullanıcı verilerinden 22 adet hesabın toplam 9.905 kişi tarafından takip edildiği, ortalama olarak bir hesabın 450 kişi tarafından takip edildiği tespit edilmiştir. 22 adet PKK terör örgütü sempatzanı Twitter hesabından toplamda 4.699 adet tweet paylaşımı yapıldığı, bir kullanıcının ortalama 213 tweet paylaşımı yaptığı hesaplanmıştır. İncelenen 22 adet Twitter hesabının toplamda 3.529 kişiyi, ortalama olarak bir hesabın 160 kişiyi takip ettiği bilgisine ulaşılmıştır.

⁷⁰ Twitter'da bir hesap sahibinin hesabını koruma altına alması neticesinde, kendisini takip edenler haricinde kalanlar bu kişinin paylaşımlarını görememektedir. Aynı şekilde hesap koruma altına alındığında bu hesaba ait verilerin bu tezde kullanılan uygulamalarla toplanması da mümkün olmamaktadır. Bu nedenle koruma altına alınan hesaplar veri setinden çıkartılmak zorunda kalmıştır.

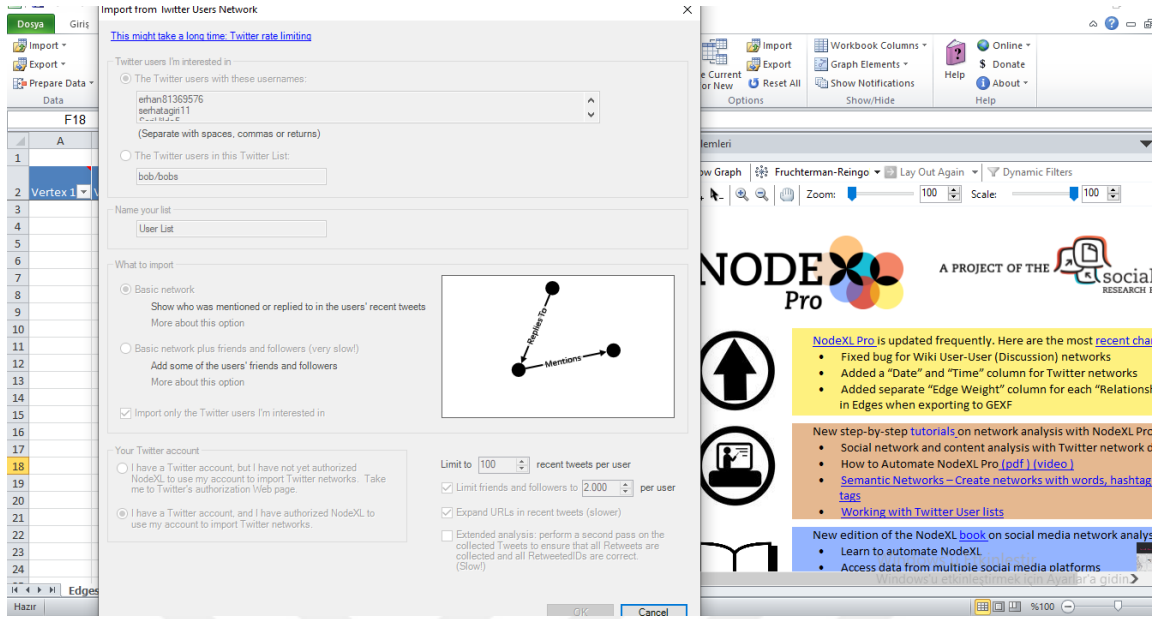
3.5.3. Yöntem Uygulaması İkinci Aşama: Çekirdek Twitter Hesapların Takip Ettiği Hesapların Tespiti, Ayıklanması ve Verilerin Toplanması

Yöntemin ikinci aşamasında, PKK terör örgütü sempatzanı 22 Twitter çekirdek hesabın takip ettiği 3.529 kişinin tespit ve ayıklanması işlemi gerçekleştirilmiştir. TweetBeaver uygulaması kullanılarak 22 adet hesabın, takip ettiği hesaplara ait bilgiler toplanmıştır. Ayıklama işleminin birinci safhasında, 3.529 hesap içerisinde mükerrer olan hesaplar tespit edilmiş ve veri setinden çıkartılmıştır. Bu durum 22 hesap sahibinin aynı kişileri takip etmesinden kaynaklanmaktadır. Manuel olarak yapılan incelemenin ardından mükerrer hesapların ayıklanması neticesinde örneklem içerisinde, 22 çekirdek hesap da dâhil olmak üzere toplamda 1.618 Twitter hesabına ulaşılmıştır.

Ayıklama işleminin ikinci safhasında, veri setindeki 1.618 adet hesap, PKK terör örgütü sempatzanı olup olmadığı açısından incelemeye alınmıştır. Bu maksatla, PKK terör örgütü sempatzanı Twitter hesaplarının tespiti için daha önce kullanılan kriterlere sadık kalınmış, hesapların profil fotoğrafları, profil bilgileri ve yaptıkları paylaşımlar incelenmiştir. 1.618 Twitter hesabı içerisinde haber ajansları, devlete ait hesaplar, siyasi parti temsilcileri, yabancı devlet başkanları, sanatçılar gibi tüm Twitter kullanıcıları tarafından takip edilmesi olağan hesapların bulunduğu görülmüş, bu hesaplar veri setinden çıkartılmıştır. Manuel olarak yapılan bu işlem neticesinde, 171 hesap daha veri setinden çıkartılmış, sonuç olarak 22 adet hesaptan yola çıkılarak toplamda 1.447 hesaplık PKK terör örgütü sempatzanı veri setine ulaşılmıştır.

Örneklem olarak alınan 1.447 adetlik hesaba ait Twitter verilerinin toplanması maksadıyla NodeXL Pro uygulaması kullanılmıştır. NodeXL Pro'nun Şekil 3.14.'te görülen "Twitter Kullanıcıları Ağından İthal Et (Import From Twitter Users Network)" fonksiyonu kullanılarak 1.447 adet hesaba ait veriler toplanmıştır. Bu veriler toplanırken, PKK terör örgütü sempatzanlarının son dönem gündemlerini tespit edebilmek üzere son olarak paylaştıkları 100 adet tweetin toplanmasına yönelik işlem yapılmıştır. Bu işlemin sonucunda 1.447 adet Twitter hesabı ve bu hesapların paylaştığı 125.564 adet tweetin oluşturduğu sosyal ağa ilişkin veriler elde edilmiştir. NodeXL Pro'da yapılan bu işlem 9 saat 25 dakika sürmüştür.

Şekil 3.14. NodeXL Pro ile Twitter Kullanıcı Ağına Ait Verilerin Toplanması



3.5.4. Yöntem Uygulaması Üçüncü Aşama: Toplanan Verilerin NodeXL Pro Uygulaması ile Analiz Edilmesi

Üçüncü aşamada, elde edilen 1.447 adet PKK terör örgütü sempatzanının Twitter hesaplarına ait veriler NodeXL Pro uygulaması kullanarak analiz edilmiştir. Bu maksatla öncelikle veri setine ait ölçütler NodeXL Pro uygulamasına hesaplatılmıştır. Bu hesaplamalar sonucunda PKK terör örgütü sempatzanı Twitter hesaplarının oluşturduğu sosyal ağa ait ölçütler elde edilmiştir. NodeXL Pro tarafından hesaplanan ölçütler tablosuna ait ekran görüntüsü Şekil 3.15'te görülmektedir.

Şekil 3.15. NodeXL Pro Tarafından Hesaplanan Ölçütler Tablosu

In-Degree	Out-Degree	Betweenness Centrality	Closeness Centrality	Eigenvector Centrality	PageRank	Clustering Coefficient	Reciprocated Vertex Pair Ratio
22	17	4208,503	0,000	0,001	1,466	0,070	0,276
49	21	14084,198	0,000	0,001	2,620	0,072	0,259
53	17	13999,880	0,000	0,001	2,657	0,040	0,153
1	25	1671,850	0,000	0,002	1,027	0,101	0,000
21	1	542,950	0,000	0,001	0,908	0,029	0,000
31	1	5068,883	0,000	0,001	1,480	0,057	0,000
49	31	8449,914	0,000	0,003	2,773	0,064	0,083
94	31	15977,741	0,000	0,005	4,205	0,055	0,070
63	18	6641,888	0,000	0,003	2,716	0,052	0,129
139	4	34261,580	0,000	0,004	5,466	0,026	0,014
4	10	1854,618	0,000	0,000	0,743	0,015	0,000
12	10	948,280	0,000	0,000	1,037	0,150	0,000
28	4	1452,049	0,000	0,001	1,259	0,036	0,034
36	3	2314,388	0,000	0,001	1,607	0,020	0,000
27	13	2849,397	0,000	0,001	1,608	0,053	0,000
76	9	12654,464	0,000	0,002	3,159	0,059	0,051
55	8	6170,426	0,000	0,001	2,293	0,076	0,109
20	5	701,444	0,000	0,001	0,985	0,056	0,045
30	1	1558,618	0,000	0,001	1,268	0,055	0,000
94	11	15575,366	0,000	0,003	3,944	0,017	0,030
1	24	1835,816	0,000	0,001	1,026	0,077	0,000
39	1	2093,448	0,000	0,001	1,582	0,028	0,000
27	7	4298,954	0,000	0,001	1,435	0,061	0,032
21	4	1409,702	0,000	0,001	1,051	0,053	0,000
38	3	2874,143	0,000	0,001	1,673	0,009	0,026
58	10	14937,138	0,000	0,001	3,036	0,024	0,015
4	14	198,675	0,000	0,001	0,708	0,133	0,067

Tüm ölçütler (overall metrics) hesaplamasından elde edilen sonuçlara göre Twitter’da yer alan bir grup PKK terör örgütü sempatzanının örneklem olarak ele alındığı bu sosyal ağ yönlü (directed) bir ağdır. Söz konusu ağ içerisinde, veri setindeki PKK terör örgütü sempatzanı Twitter hesabı sayısı olan 1.447 adet düğümün yer aldığı, ağ içerisinde düğümleri birbirine bağlayan 15.067 adet kenarın bulunduğu görülmektedir.

Ağ içerisindeki tek düğüm bağlantılı bileşenler (single-vertex connected components) sayısı 153’tür. Tek düğüm bağlantılı bileşenler ağdaki diğer düğümlerle aynı konuyu konuşan ancak kendi başlarına hareket eden, diğer düğümlerle bağı bulunmayan izole kullanıcılardır. Twitter ağlarındaki bu kişiler, kendisinden söz edilmeyen, bir paylaşımı yanıtlanmayan veya başkasının paylaşımını tekrar paylaşmayan (retweet) kişilerdir (Hansen vd., 2020: 170). Örneklem olarak araştırılan ağda 1.447 adet düğüm bulunduğu düşünüldüğünde, örneklemin %10,5’inin (153) diğerlerine bağlı olmaksızın, münferit hareket ettikleri anlaşılmaktadır.

Bir ağdaki bireyler arasında mevcut bağlantı sayısı ile; aynı ağdaki tüm bireylerin birbirine bağlı olduğu varsayıldığında ortaya çıkan tüm bağlantıların sayısına oranını gösteren yoğunluk ölçütü (Hansen vd., 2020: 82), bu ağ için 0,0065’tir. Ağ yoğunluk değerleri sıfır ile bir arasında değişmekte ve tüm olası kenarların yüzdesi olarak değerlendirilmektedir. Bir ağın yoğun bir şekilde birbirine bağlı olma derecesi, hesaplanan yoğunluk değerinin 1’e yakın bir değer alması, ağ içerisindeki bilgi akış hızını etkilemektedir. Yoğunluk değeri yüksek olan ağlarda bireyler birbirlerine daha sıkı şekilde bağlı olup, bu ağlarda bilginin transfer oranı daha yüksek olmaktadır. Twitter’da yoğunluk arttıkça bilginin yayılma hızı da artmaktadır (Hansen vd., 2020: 170).

PKK terör örgütü sempatzanlarının teşkil ettiği Twitter ağı yoğunluk değerinin 0,0065 olarak hesaplanması, bu değer 0’a daha yakın olması, örneklem ağındaki kişilerin birbirlerine güvenmediğini, sadece kendilerine yakın gördükleri kişilerden aldıkları bilgiyi transfer ettiklerini gösterdiği değerlendirilmektedir. Bununla birlikte ağ boyutu büyüdükçe yoğunluğun azalmasının muhtemel olduğu da göz önünde bulundurulmalıdır.

PKK sempatzanlarının Twitter’da oluşturduğu örnek ağda “maksimum jeodezik mesafe / çap (maximum geodesic distance / diameter) değeri 10, ortalama jeodezik mesafe ise 2,9502 şeklinde hesaplanmıştır. Jeodezik mesafe, iki kişi arasındaki en kısa yolun uzunluğudur. Kenarları yollar ve köşeleri evler olarak düşünürseniz, jeodezik mesafe kişinin mümkün olan en kısa yoldan gittiğini varsayarak, bir kişinin bir evden diğerine gitmek için kat etmesi gereken yol olacaktır. Bir ağın maksimum jeodezik mesafesi veya

ağın çapı, ağdaki en büyük jeodezik mesafe ya da birbirinden en uzak iki düğüm arasındaki mesafeyi göstermektedir. Bir ağdaki jeodezik mesafe ne kadar küçük ise, ağdaki bireylerin birbirine yakınlık derecesi o kadar yüksek anlamına gelmektedir (Hansen vd., 2020: 82). Araştırmanın konusu olan PKK terör örgütü sempatizanlarının oluşturduğu ağda jeodezik mesafenin 2,9502 olarak hesaplanması, ağdaki bireylerin birbirlerini tanıdıklarını ya da en azından ortak arkadaşları vasıtasıyla tanıştıkları anlamına gelmektedir.

Twitter verilerini sosyal ağ analizi ile araştırmak kullanıcıları ağdaki bağlantılarına göre karakterize etmemizi sağlamaktadır. Twitter kullanıcılarının ağda ne kadar merkezi olduklarını ölçmek, etkili kullanıcıları ve bunların birbirleriyle olan bağlantılarını ortaya çıkarmak için sosyal ağ analizine ihtiyaç duyulmaktadır. Twitter’da paylaşım yapan kullanıcıların etkinliğini araştırmak üzere kullanılan en önemli ölçütler iç derece merkeziliği ve dış derece merkeziliği ölçütleridir.

İç derece merkeziliği, diğer Twitter kullanıcılarının bir düğüm (bir kullanıcı) ile kurduğu ilişkiyi gösteren kenarların sayısını ölçmektedir. Örneğin, bir Twitter kullanıcısı, bir konu hakkında paylaşılan tweetlerde diğer kullanıcılar tarafından çok kez bahsedildiyse, bahsedilen kişinin iç derece merkeziliği ölçüsü yüksek olacaktır. Dış derece merkeziliği ise, bir düğümün diğer kullanıcılarla oluşturduğu kenar sayısını saymaktadır. Örneğin, bir Twitter kullanıcısı paylaştığı bir tweetinde diğer kullanıcılardan bahsetmişse, diğerlerinden bahseden kullanıcının dış derece merkeziliği ölçüsü yüksek olacaktır (Hansen vd., 2020: 166). Örneklerle de belirtildiği üzere iç derece merkeziliği ölçütü bir sosyal ağ içerisinde en çok etkileşimi alan Twitter kullanıcısını, dış derece merkeziliği ölçütü ise diğer kullanıcılarla en çok ilişki kuran kişiyi ön plana çıkartmaktadır.

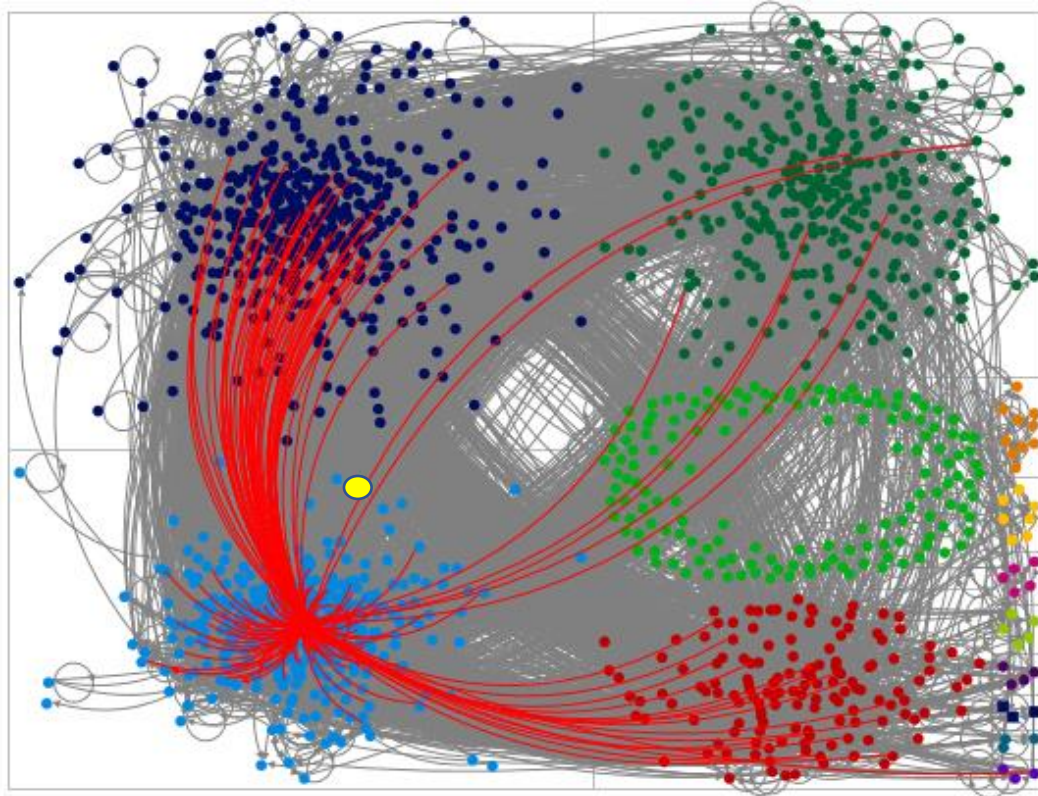
Yüksek iç derece merkeziliğine sahip kullanıcılar, konuyla ilgili sohbete katılan kullanıcı topluluğu arasında tweetleriyle dikkat çekmektedirler. Yüksek iç derece merkeziliğine sahip olanlar, iletişimin merkezi olarak düşünülebilmektedir. Araştırmanın konusu olan PKK terör örgütü sempatizanlarının Twitter ağı verilerine göre iç derece merkeziliği puanı en yüksek olan kullanıcı 212 puanla 47 numaralı kullanıcıdır.

Bu aşamada, araştırmada örneklem olarak Twitter uygulamasından bir grup kullanıcının seçildiğini ancak etik açıdan kullanıcılara ait kimlik bilgisi veya hesap ismi gibi bilgilere tez metni içerisinde yer verilmediğini, verilerin tez hazırlığı yapılan bilgisayarda saklı tutulduğunu belirtmekte fayda görülmektedir. Bu nedenle iç derece merkeziliği en yüksek kullanıcı 47 numaralı kullanıcı olarak ifade edilmiştir. Kullanıcılara verilen bu numara, NodeXL Pro uygulaması tarafından her bir düğüme otomatik olarak

verilen numara olup, çalışmanın bundan sonraki bölümünde diğer kullanıcılar da benzer şekilde numara ile isimlendirilecektir.

PKK terör örgütü sempatizanlarının oluşturduğu Twitter ağında en yüksek iç derece merkeziliğine sahip olan 47 numaralı kullanıcının ağ içerisindeki yeri Şekil 3.16.'da sarı yuvarlak ile işaretlenmiştir. Şekilde 1.447 kullanıcının teşkil ettiği ağın NodeXL Pro uygulamasının Fruchterman-Reingold algoritması kullanılarak hazırlanmıştır. Fruchterman-Reingold algoritması kullanılmasının temel nedeni, söz konu algoritmanın, ağın net bir görünümünü sağlamak için düğümleri kenarların minimum düzeyde kesişeceği şekilde dağıtan, hızlı ve etkili bir düzen algoritması olmasıdır (Tunalı ve Güvenoğlu, 2019: 179). Şekildeki kırmızı çizgiler 47 numaralı kullanıcıdan diğer kullanıcılara doğru uzanan bağlantı kenarlarını temsil etmektedir. Şekilden de anlaşılacağı üzere 47 numaralı Twitter kullanıcısının örneklem olarak seçilen ağdaki nüfuz etkisi oldukça yüksektir.

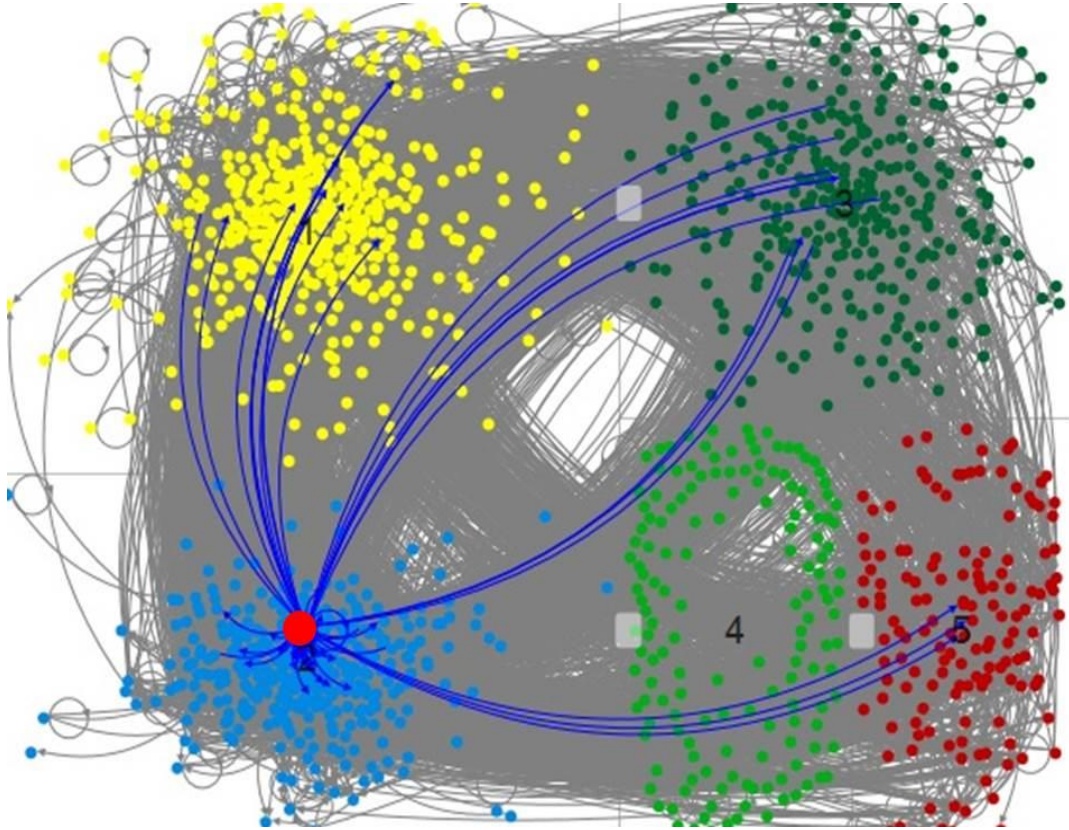
Şekil 3.16. İç Derece Merkeziliği Derecesi En Yüksek Kullanıcı



Dış derece merkeziliği bir Twitter kullanıcısının topluluğa erişim gücünü hesaplamaktadır. Yüksek dış derece merkeziliği değeri, bir kullanıcının bir konu hakkında çok fazla tweet attığını, diğer kullanıcılardan bahsederek veya diğer kullanıcıların tweetlerini yanıtlayarak kullanıcıların dikkatini çekmeyi amaçladığını göstermektedir. Bu durumda, dış derece merkeziliği, bir kullanıcının topluluk üyeleriyle başlattığı etkileşim

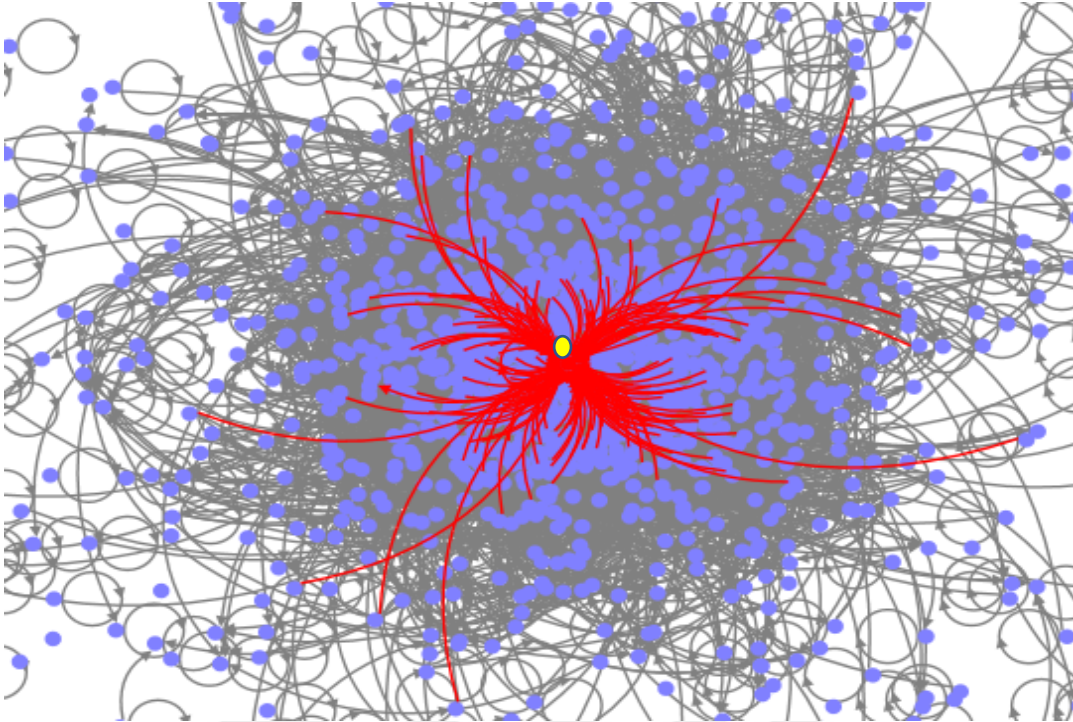
düzeyini hesaplamaktadır (Hansen vd., 2020: 167). Araştırmanın örnekleminde dış derece merkeziliği değeri en yüksek olan kullanıcı 46 puan ile 469 numaralı kullanıcıdır. PKK terör örgütü sempatisanlarının oluşturduğu Twitter ağında en yüksek dış derece merkeziliğine sahip olan 469 numaralı kullanıcının ağ içerisindeki yeri Şekil 3.17.'de kırmızı yuvarlak ile işaretlenmiştir.

Şekil 3.17. Dış Derece Merkeziliği Derecesi En Yüksek Kullanıcı



Arasındalık merkeziliği (betweenness centrality) algoritması da bir sosyal ağ içerisindeki ilişkilerin en ortasında yer alan düğümü / kullanıcıyı tespit etmektedir. Arasındalık merkeziliği, bir düğümün ağdaki “göbek” rolünü ne ölçüde oynadığını ölçmektedir. Arasındalık merkeziliği yüksek olan kullanıcılar, genellikle farklı gruplarda yani ağ kümelerinde bulunan kullanıcıları birbirine bağlamakta, bu durum da gruplar arasındaki bilgi akışını açıklamaya yardımcı olmaktadır (Hansen vd., 2020: 168). Araştırmanın konusu olan PKK terör örgütü sempatisanlarının oluşturduğu ağda arasındalık merkeziliği değeri 73967,8 ile en yüksek olan kişi 7 numaralı kullanıcıdır. Bu kapsamda 7 numaralı kullanıcının PKK terör örgütü sempatisanları ağı içerisinde “göbek” görevi gördüğü, bu kullanıcının iletişimin merkezinde yer aldığı görülmektedir. Şekil 3.18.'de 7 numaralı kullanıcının ağın üzerindeki yeri görülmektedir.

Şekil 3.18. Arasındalık Merkezliği Derecesi En Yüksek Kullanıcı



Yönsüz ağlar için özvektör merkeziliği, yönlü ağlar için ise sayfa değeri (page rank) olarak ifade edilen algoritmalar ile ağdaki en önemli düğüm bulunabilmektedir. PKK terör örgütü sempatizanlarının oluşturduğu Twitter ağı örneklemini yönlü bir ağ olduğundan, bu ağdaki kanaat önderlerini bulabilmek amacıyla “sayfa değeri” hesaplanmıştır. Buna göre örneklemin 8,277 puanlı en yüksek sayfa değeri, arasındalık merkeziliği değeri de en yüksek olarak hesaplanan 7 numaralı kullanıcıdır. Bu hesaplama 7 numaralı kullanıcının ağdaki kanaat önderi olduğunu ortaya koymaktadır. Sayfa değeri en yüksek olan ikinci kullanıcı ise, 8,117 puanı ile aynı zamanda en yüksek iç derece merkeziliği değerine de sahip olan 47 numaralı kullanıcıdır.

Sosyal ağlarda sıklıkla, yoğun şekilde birbirine bağlı kullanıcılardan oluşan daha küçük alt gruplar ya da kümeler (clusters) ortaya çıkmaktadır. Topluluklar olarak da anılan kümeler, birbirine diğerlerine göre daha çok bağlı olan düğümlerin oluşturduğu alt grupları ifade etmektedir. Twitter kullanıcılarının oluşturduğu kümeler, Twitter’daki kullanıcılar arasında bilgi akışının ve etkileşimin sınırlarını tanımlamaktadır. NodeXL Pro üç farklı algoritma ile bir ağda bulunan grupları hesaplayabilmektedir (Hansen vd., 2020: 170-171). Tez kapsamında, büyük ve karmaşık ağ yapılarına ait grupları hesaplayabilen “Clauaset-Newman-Moore” algoritması kullanılmıştır.

PKK terör örgütü sempatizanlarının Twitter’da teşkil ettiği 1.447 kişiden oluşan ağın gruplara ayrılması için NodeXL Pro’nun “gruplar” sekmesinden, “grupları kümelere göre

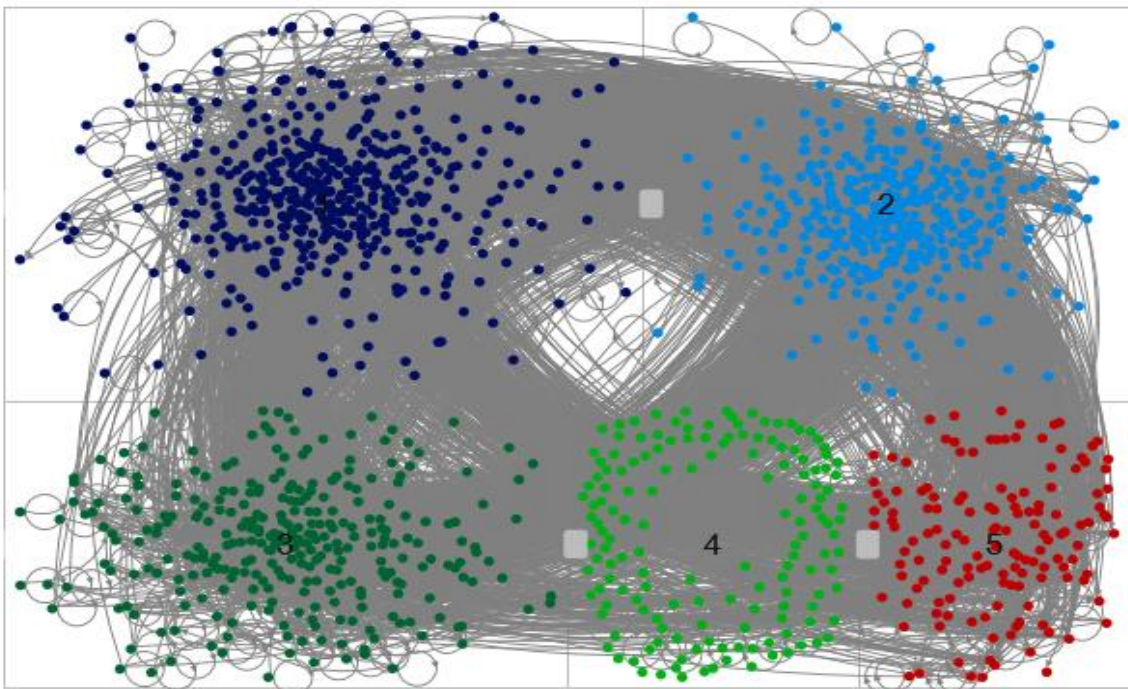
ayır” sekmeleri seçilmiş, sonuç olarak NodeXL Pro örneklem ağını 13 ayrı gruba ayırmıştır. NodeXL Pro, ağı görsel olarak gruplara ayırmakla birlikte aynı zamanda hangi Twitter kullanıcısının hangi grupta bulunduğunu da hesaplayarak göstermekte, grupların ölçütlerini Şekil 3.19.’da görülen biçimde ayrı ayrı hesaplamaktadır.

Şekil 3.19. NodeXL Pro Programı ile Hesaplanan Grup Bilgileri Tablosu

NodeXL Pro										
Tasarım										
O15										
3										
1	A	B	C	D	E	F	K	L	M	N
2	Visual Properties					Labels	Graph Metrics			
3	Group	Vertex Color	Vertex Shape	Visibility	Collapsed?	Label	Vertices	Unique Edges	Edges With Duplicates	Total Edges
4	G1	0, 12, 96	Disk			1	461	3972	0	3972
5	G2	0, 136, 227	Disk				354	4160	0	4160
6	G3	0, 100, 50	Disk				296	1436	0	1436
7	G4	0, 176, 22	Disk	Show			153	91	0	91
8	G5	191, 0, 0	Disk				143	434	0	434
9	G6	230, 120, 0	Disk	Skip			10	27	0	27
10	G7	255, 191, 0	Disk	Skip			7	13	0	13
11	G8	150, 200, 0	Disk	Skip			5	9	0	9
12	G9	200, 0, 120	Disk	Skip			5	9	0	9
13	G10	77, 0, 96	Disk	Skip			4	6	0	6
14	G11	91, 0, 191	Disk	Skip			3	5	0	5
15	G12	0, 98, 130	Disk	Skip			3	4	0	4
16	G13	0, 12, 96	Solid Square	Skip			3	5	0	5

PKK terör örgütü sempatizanlarının Twitter ağında esasen beş ana grupları bulunmaktadır. Diğer gruplar 3 ile 10 kişi arasında değişen sayıdaki kişinin oluşturduğu küçük gruplardır. Ayrıca daha önce de belirtilen 153 kişilik hiçbir gruba bağlı olmayan kişilerin teşkil ettiği tek düğüm bağlantılı bileşenler de ayrı bir grup olarak (G4) gösterilmektedir. Şekil 3.20’de örneklem olarak araştırılan PKK sempatizanları Twitter ağı içerisindeki beş ana grubun gösterildiği ağ görülmektedir.

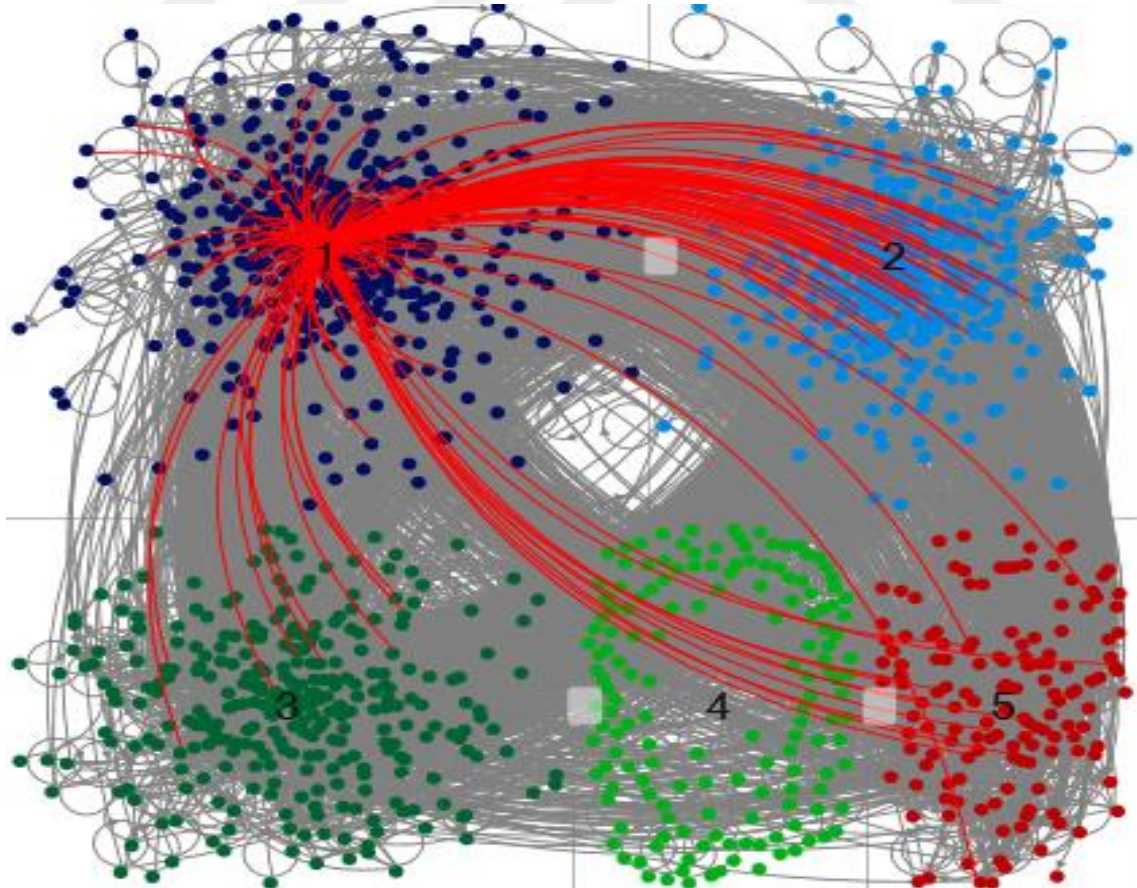
Şekil 3.20. PKK Terör Örgütü Sempatizanlarının Twitter Ağına Ait Gruplar



NodeXL Pro tarafından hesaplanan gruplara ait ölçütlerden, en büyük ağın 461 düğümünden oluşan 1 numaralı ağ olduğu, en fazla bağlantının ise 4.160 kenara sahip 2 numaralı grup olduğu görülmektedir. Bu sonuç, en çok Twitter kullanıcısı bulunan grubun 1 numaralı grup olduğunu, en sıkı ilişkilere sahip grubun ise 2 numaralı grup olduğunu ortaya koymaktadır.

Grupların kanaat önderlerini bulabilmek amacıyla sayfa değerine göre kullanıcılar sıralandığında; 1 numaralı grupta 8,277371 sayfa değeri ile 7 numaralı; 2 numaralı grupta 8,116802 sayfa değeri ile 47 numaralı; 3 numaralı grupta 3,596129 sayfa değeri ile 22 numaralı; 5 numaralı grupta 3,49105 sayfa değeri ile 4 numaralı Twitter kullanıcısının kanaat önderleri olduğu görülmektedir. Ağa ait alt gruplardaki kanaat önderleri aynı zamanda diğer gruplara da nüfuz eden önemli aktörlerdir. 4 numaralı grup 153 kişilik bağlantısız kişilerden oluştuğu için, bu grupta kanaat önderi bulunmamaktadır. PKK terör örgütü sempatizanlarının teşkil ettiği Twitter ağındaki 1 numaralı grupta bulunan kanaat önderi, 7 numaralı Twitter kullanıcısının ağ içerisindeki diğer gruplara erişimini gösteren grafik Şekil 3.21.'de görülmektedir.

Şekil 3.21. 1 Numaralı Grup Kanaat Önderinin Diğer Gruplara Erişimi



Ağıdaki gruplarda yer alan kullanıcıların diğer gruplardaki kullanıcılarla etkileşimini incelemek üzere ise grup kenarları ölçütleri incelenmiştir. NodeXL Pro tarafından hesaplanan bu ölçütlere göre 1 numaralı gruptan 2 numaralı gruba yönelen 977 kenar ya da başka bir deyişle 1 numaralı gruptan 2 numaralı gruba 977 adet bağlantı bulunmaktadır. 1 numaralı gruptan 3 numaralı gruba 197; 5 numaralı gruba 260 adet bağlantı bulunmaktadır. Tüm grupların bağlantı dereceleri Çizelge 3.2.’de görülmektedir.

Çizelge 3.2. Gruplar Arasındaki Bağlantılar Tablosu

	Grup 1	Grup 2	Grup 3	Grup 5
Grup 1	3.972	977	197	260
Grup 2	1.295	4.160	429	279
Grup 3	292	380	1.436	36
Grup 5	296	261	58	434

Çizelge 3.2.’de 1 numaralı grubun kendi içerisindeki bağlantı sayısı, grubun kendine ait satır ve sütununun kesiştiği kutucukta 3.972 olarak görülmektedir. Örneğin 2 numaralı grubun kendi içerisindeki bağlantı sayısı ise 4.160’tır. Çizelgeden gruplar arası en fazla bağlantının 2 numaralı gruptan 1 numaralı gruba doğru ve 1.295 adet olduğu görülmektedir. Bu veriler 2 numaralı grubun 1 numaralı grupta bulunan kullanıcılarla yoğun ilişki içerisinde olduğuna işaret etmektedir.

PKK terör örgütü sempatanlarının sosyal ağ analizine ilişkin veriler NodeXL Pro uygulaması ile toplanmış, veriler NodeXL Pro algoritmaları ile analiz edilmiş, bu veriler doğrultusunda ölçütler hesaplanmıştır. NodeXL Pro sosyal ağ analizine ilişkin oldukça kullanıcı dostu bir uygulama olup elde ettiği veriler doğrultusunda aynı zamanda sosyal ağları görselleştirebilmektedir. Ancak NodeXL Pro uygulaması ile sosyal ağların görselleştirilmesi çok başarılı değildir. Bu nedenle birçok araştırmacı sosyal ağlar üzerinden veri elde etmek için NodeXL Pro, verileri görselleştirmek için ise Gephi programını kullanmaktadır.

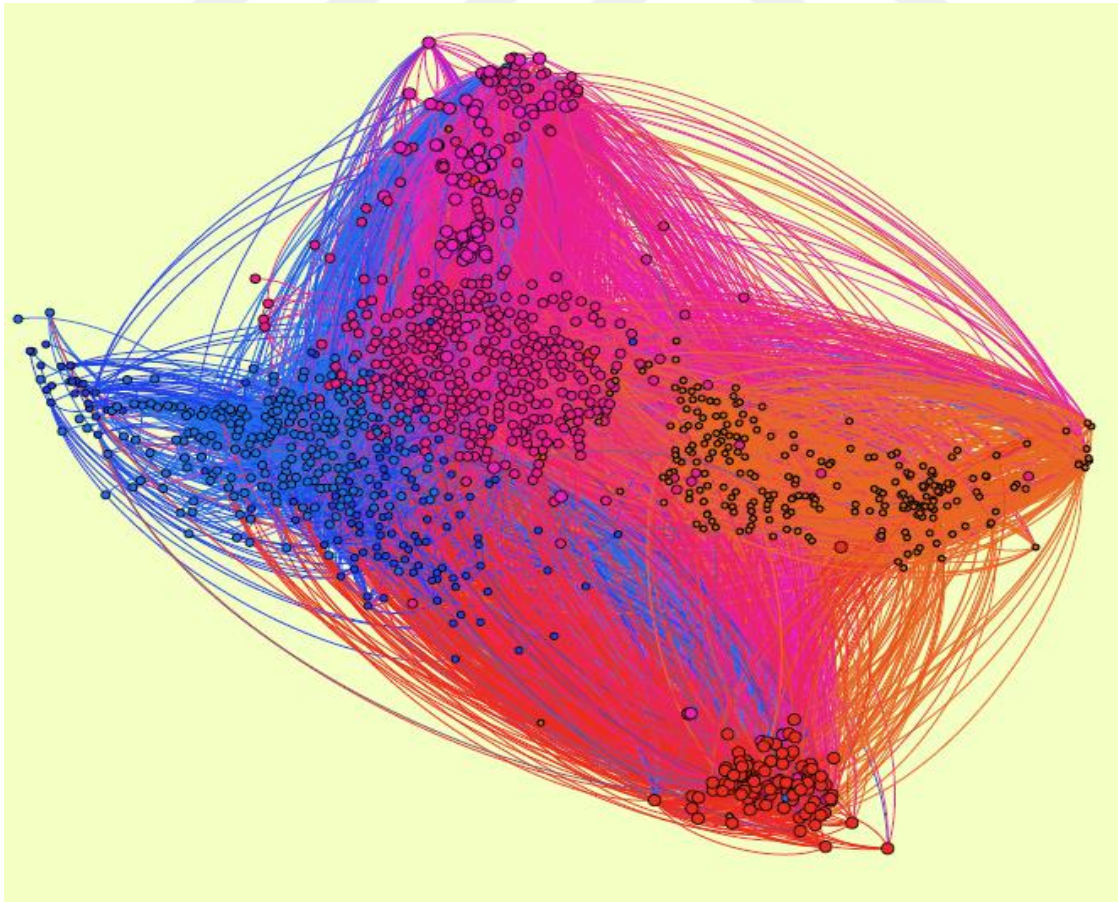
Tıpkı NodeXL Pro gibi Gephi programı da ağlarla ilgili verilere ilişkin ölçütleri hesaplayabilmekte, bu verileri analiz edebilmektedir. Ancak tercihen kullanımı daha kolay olduğundan bu çalışmada analiz maksadıyla da NodeXL Pro tercih edilmiştir. Zira

NodeXL Pro ile yapılan hesaplamalar ile Gephi ile yapılan hesaplamalar arasında oldukça küçük ve yok sayılabilecek farklılıklar olduğu da çalışma süresince test edilmiştir.

1.447 Twitter kullanıcısının oluşturduğu PKK terör örgütü sempatizanları ağını daha görsel bir hale getirmek üzere Gephi 0.8 Alpha programı kullanılmıştır. Gephi ayrıca karmaşık veri setleriyle kolay bir çalışma alanı sunabilmektedir (Bastian vd., 2009: 1). Gephi, NodeXL Pro uygulamasına göre daha hızlı hesaplamalar ve görselleştirmeler yapabilmektedir. PKK terör örgütü sempatizanları Twitter ağı, Gephi uygulamasında Force Atlas algoritması kullanılarak ve küçük gruplar filtre edilerek görselleştirilmiştir.

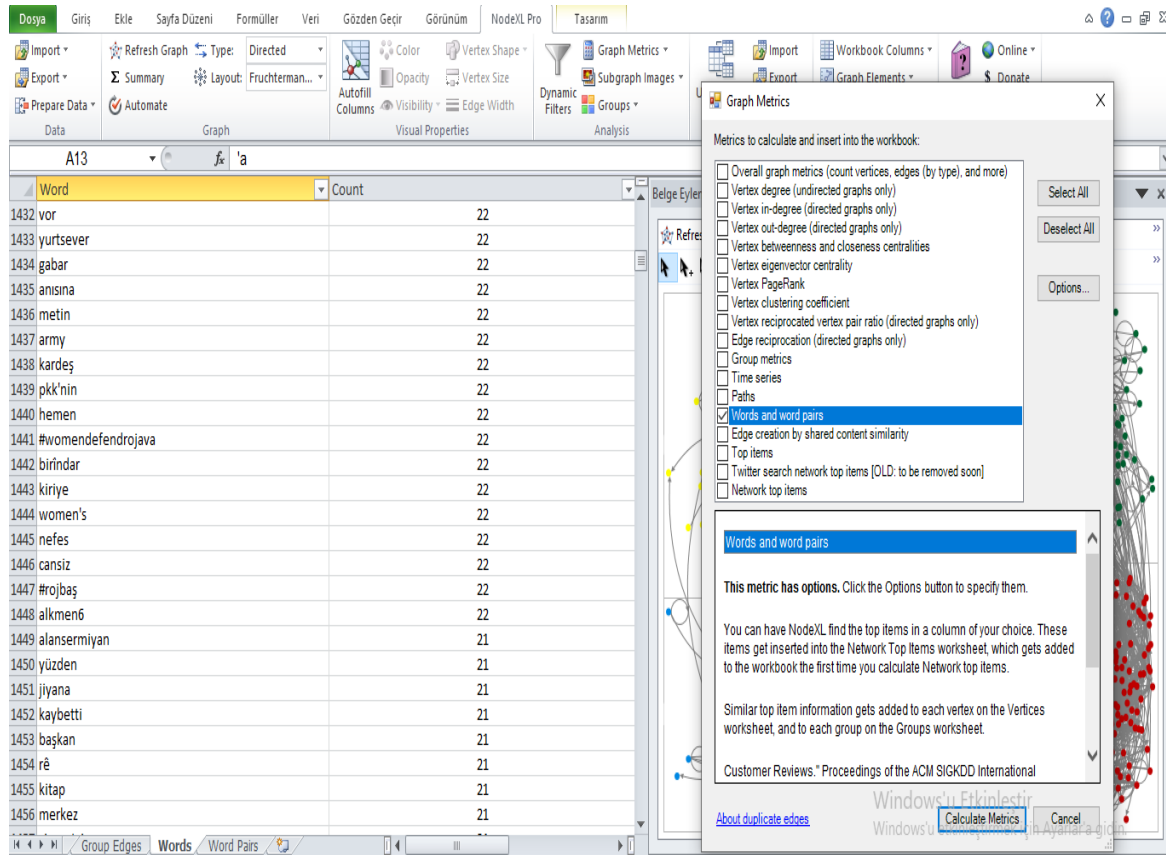
Şekil 3.22.'de görüldüğü üzere Gephi, NodeXL Pro'ya kıyasla sosyal ağları daha çekici bir hale getirebilmektedir. Gephi uygulaması, PKK terör örgütü sempatizanlarının oluşturduğu Twitter ağını mavi, kırmızı, pembe ve kahverengi renklerle temsil edilen gruplara ayırmış, gruplar arası bağları da renkli bağlantılarla göstermiştir. Bu araştırmada, sosyal ağ analizine ilişkin ölçüt hesaplamaları NodeXL Pro ile yapıldığından Gephi ile aynı işlemler tekrar edilmemiştir.

Şekil 3.22. PKK Terör Örgütü Sempatizanları Twitter Ağının Gephi ile Görselleştirilmesi



PKK terör örgütü sempatizanlarının Twitter ağına ilişkin içerik analizini yine NodeXL Pro ile hesaplanan kelime sayıları üzerinden yapabilmek mümkündür. NodeXL Pro, PKK terör örgütü sempatizanlarının paylaştığı 125.564 adet tweetin içerisindeki kelimeleri sayılabilmektedir. NodeXL Pro programının ölçütler sekmesinden, Şekil 3.23.'de görüldüğü üzere kelimeler ve kelime çiftleri seçeneği seçilerek yapılan hesaplama sonucunda, paylaşılan tweetler içerisindeki kelimelerin sayısına erişilebilmektedir.

Şekil 3.23. NodeXL Pro ile Kelime Sayılarının Hesaplanması



NodeXL Pro ile hesaplanan kelime tekrarı verilerinden belirlenen sosyal ağ içerisinde konuşulan ve paylaşılan gündem maddelerini belirleyebilmek, ağdaki kişilerin düşüncelerini değerlendirmek mümkün olabilmektedir. NodeXL Pro tarafından hesaplanan, en çok tekrar edilen ilk 20 kelimeye ilişkin veriler Çizelge 3.3.'te görülmektedir. Burada mutlaka belirtilmesi gereken husus, NodeXL Pro'nun belirlenen metin belgesi içerisinde kelime sayımı yaparken; metin içerisinde geçen tek harfleri, bağlaçları, zarfları ve rakamları da kelime olarak saydığıdır. Bu araştırmada da kelime sayım sonuçlarında 3.134 kez tekrar edilen kelime “ve” kelimesi olarak tespit edilmiş ancak ve bağlacı konu kapsamında anlam ifade etmediğinden dikkate alınmamıştır.

Çizelge 3.3. Ağda En Çok Kullanılan Kelimeler

S.No.	Sık Tekrar Edilen Kelime	Tekrar Sayısı	S.No.	Sık Tekrar Edilen Kelime	Tekrar Sayısı
1	Kobane + Kobani	643+78 =721	11	AKP	189
2	Kürt	572	12	Kürdistan	187
3	#direniş60ıncıgünde	532	13	Heval	169
4	Türk	352	14	Rojava	166
5	KDP	334	15	Öcalan	160
6	PKK	320	16	T.C.	158
7	Özgürlük	242	17	Tecrit	148
8	HDP	222	18	Halk	147
9	Apo	212	19	Gözaltı	133
10	Direnış	194	20	ABD	116

Örneklem olarak belirlenen Twitter kullanıcı ağında paylaşılan tweetlerde en çok kullanılan kelimeler, “Kobane veya Kobani” kelimesidir. Aynı anlama gelen Kobani kelimesinin 78, Kobane kelimesinin ise 643 kez, toplamda 721 kez tekrar edildiği görülmektedir. Tweet metinleri bu kelimeler kapsamında analiz edildiğinde, Suriye’nin kuzeyinde yer alan ve Türkçesi Ayn El Arap olan Kobani isimli yerleşim yerinin 26 Ocak 2015 tarihinde DEAŞ terör örgütünden kurtarılmasının yıldönümü nedeniyle bu kelimeler çerçevesinde gündem oluşturulduğu anlaşılmaktadır. Suriye’nin kuzeyine ilişkin PKK terör örgütü sempatanlarının bu derecede yoğun paylaşımları, terör örgütü PKK’nın Suriye kolu PYD’nin terör örgütü ile aynı çatı altında olduğunun da bir göstergesidir.

PKK terör örgütü sempatanlarının oluşturduğu ağda en çok tekrar eden ikinci kelime “Kürt”, dördüncü kelime ise “Türk” kelimeleridir. PKK terör örgütü sempatanlarının oluşturduğu ağda en çok tekrar eden ikinci kelime “Kürt”, dördüncü kelime ise “Türk” kelimeleridir. Ağ içerisinde atılan tweetlerde sıklıkla kullanılan bu kelimeler, günlük iletişimde sıklıkla kullanıldığından ve bir gündem maddesi teşkil etmek üzere kullanılmadıkları için değerlendirmeye alınmamışlardır.

NodeXL Pro tarafından 1.447 PKK terör örgütü sempatzanlarının Twitter paylaşımları üzerinden yapılan analiz neticesinde, örneklem olarak seçilen ağ içerisinde en çok tekrar eden üçüncü ifadenin, aynı zamanda bir etiket olan “#direniş60ıncıgünde” ifadesi olduğu görülmektedir. #direniş60ıncıgünde ifadesinin tweet metinleri içerisindeki tekrar sayısı, NodeXL Pro tarafından 532 olarak hesaplanmıştır. Bu etiketin paylaşıldığı tweetler incelendiğinde, PKK terör örgütü sempatzanlarının en yoğun gündemlerinin terör örgütü liderinin hapisane koşullarını protesto edenlerin başlattığı açlık grevi eylemleri olduğu anlaşılmaktadır. Tweet metinleri içerisinde söz konusu açlık grevleri ile ilgili olarak İngilizce ve Türkçe paylaşımların yapıldığı da görülmektedir. Bu paylaşımlar PKK terör örgütü sempatzanlarının terör örgütü liderinin hapisane şartlarını ulusal ve uluslararası kamuoyunun gündemine taşımaya çalıştıklarına işaret etmektedir.

PKK terör örgütü sempatizanları ağı tarafından paylaşılan tweetlerde en çok tekrar edilen kelimelerden bir diğeri, 334 tekrar sayısı ile KDP kelimesidir. KDP, Irak'ta mevcut "Kürdistan Demokratik Partisinin" kısaltmasıdır. KDP kelimesinin geçtiği tweet içerikleri incelendiğinde bu paylaşımların, araştırmanın yapıldığı dönemlerde Irak'ın kuzeyinde PKK terör örgütü ile Irak Kuzeyi Bölgesel Yönetimi ve Irak Merkezi Hükümeti güvenlik güçleri arasında yaşanan çatışmalara yönelik olarak, sempatizanların verdiği olumsuz tepkiden kaynaklanan paylaşımlar olduğu görülmektedir. PKK terör örgütü sempatizanlarının KDP'yi gündeme taşıyarak, Irak kuzeyinde terör örgütü üzerinde oluşturulan baskıyı hafifletmeye çalıştığı değerlendirilmektedir.

Şekil 3.24. PKK Terör Örgütü Sempatizanlarının Gündemi Kelime Bulutu



Şekil 3.24.'te görüldüğü üzere, PKK terör örgütü sempatizanları ağında oluşturulan gündem maddelerini görselleştirmek, PKK sempatizanlarının tweet metinlerden kelime

bulutları oluşturabilmek için internet üzerinde çevrimiçi çalışabilen WordClouds uygulaması kullanılmıştır.

Araştırma döneminde PKK terör örgütü sempatizanlarının paylaşmış olduğu tweetlerin içeriğinde sık kullanılan kelimeler, kullanım sıklığına göre büyükten küçüğe doğru Şekil 3.24.'te resmedilmektedir. Kelime bulutu içerisinde yer alan kelimelerin, NodeXL Pro tarafından hesaplanan ve Tablo 3'te gösterilen kelimeler ile paralellik arz ettiği de görülmektedir. Kelime bulutlarının hem analizciye, hem de karar alıcılara sunduğu görsellik ile gündemin daha kolay anlaşılmasını sağladığı değerlendirilmektedir.

PKK terör örgütü sempatizanlarının Twitter'da teşkil ettikleri sosyal ağın analizi sürecinde bazı zorluklar ve sınırlılıklarla da karşılaşmıştır. En büyük zorluklardan birisi, kolluk kuvvetlerinin sosyal medyada terör örgütlerine yönelik aldıkları tedbirler neticesinde, analiz edilmek üzere veri setine dâhil edilen Twitter hesaplarının engellenmesi ve kapatılmasıdır. Analizin bir süreç olduğu göz önüne alındığında, engellenen ve kapatılan hesapların sayısının artması veri setinin daralmasına, sürecin başa dönmesine neden olabilmektedir.

Benzer olarak araştırmayı kısıtlayan bir diğer husus ise veri setine dâhil edilen Twitter hesabının kullanıcısı tarafından koruma altına alınması ya da kapatılmasıdır. Twitter hesabı kullanıcısı tarafından koruma altına alındığında hesaba ilişkin verilere erişilememekte, bu nedenle veri seti tamamlanamamaktadır.

Analiz sürecine ilişkin bir diğer kısıtlılık sosyal ağ analizi için kullanılan programların kapasitelerine ilişkindir. Örneğin, bu araştırmada Twitter'dan veri toplamak için kullanılan NodeXL Pro uygulaması ile en fazla 9.999 kullanıcının verilerine erişilebilmektedir. Esasen milyonlarca kullanıcısı olan bir sosyal medya uygulaması ile ilgili bir araştırmada daha fazla miktarda kullanıcıya ilişkin verinin toplanmasının mümkün olması gerekmektedir. Veri seti belirtilen sayıdaki kullanıcıdan elde edilmeye çalışıldığında ise Twitter politikaları ve kullanılan programların yetersizliği nedeniyle çok uzun bir süre almaktadır.

Terör örgütü sempatizanlarının Twitter üzerinde oluşturdukları sosyal ağların analizinde karşılaşılan başka bir zorluk, sosyal medyanın doğasından kaynaklanan bir hususla ilgilidir. Sosyal medya kullanıcısı kendi kararı ile bir paylaşım yapabildiği gibi kendi isteğiyle bu paylaşımı silebilmektedir. Terör örgütü sempatizanlarının Twitter'da yapılan paylaşımlarını silmeleri, veri setinin daralmasına neden olmaktadır.

Araştırmaya yönelik bir diğer kısıtlılık ise sosyal medya uygulamalarının manipülasyona açık olması, kullanıcıların kimlik belirtme zorunluluğu olmaması, kullanıcıların yaptıkları paylaşımların gerçekliğini sorgulama ihtiyacı duymamasıdır. Bu nedenle veri setine dâhil edilen Twitter hesaplarına ilişkin kriterlerin belirlenmesi ve birkaç kez kontrol edilerek amaca uygun hesapların belirlenmesi önem arz etmekte, bu ise uzun bir zaman dilimine ihtiyaç duyulmasına neden olmaktadır.

Twitter hesaplarının teşkil ettiği bir sosyal ağı analiz etmenin bir diğer zorluğu ise terör örgütü sempatzanlarının bazı tedbirler alarak güvenlik güçlerinin takibinden kurtulmaya çalışmalarıdır. Örneğin, terör örgütü sempatzanlarının büyük bir kısmı terör örgütüyle ilgili ve ilgisiz çok sayıda Twitter hesabını takip ederek bu kişilerle etkileşime girmekte, kalabalığa karışarak takipten kurtulmaya çalışmaktadırlar. Bu durum özellikle manuel yöntemlerle hesapların teşhisinde zorluklar yaratmaktadır.

Sosyal ağ analizinin nasıl yapılacağı, sosyal ağ analizinde kullanılacak bilgisayar destekli uygulamaların nasıl kullanılacağı gibi hususların öğrenilmesi de ayrıca bir zaman ve çaba gerektirmektedir. Bu nedenle sosyal ağ analizine bir miktar kaynak ve personel ayırmak gerekebilmektedir.

3.5.5. PKK Terör Örgütü Sempatzanları Sosyal Ağ Analizi Uygulamasının Sosyal Medya İstihbaratı Kapsamında Değerlendirilmesi

SOMİS'in aşamaları; yönlendirme ve planlama, toplama ve tasnif, analiz, teyit ve dağıtım safhalarını içermektedir. PKK sempatzanlarının oluşturduğu Twitter ağından SOMİS elde edilmesi için gerçekleştirilen uygulamada da teyit ve dağıtım safhaları hariç olmak üzere diğer safhaların gerekleri yerine getirilmiştir. Bunlardan birincisi olan yönlendirme ve planlama safhasında; araştırma öncelikle PKK terör örgütüne yönlendirilmiş, PKK terör örgütünün sosyal medya uygulamalarından Twitter'daki örgütlenme şeklinin tespiti amaç edinilmiştir. Yine bu safhada PKK sempatzanlarının Twitter ağından SOMİS elde edebilmek üzere hangi uygulamaların kullanılacağı, ağın kaç kullanıcı ile sınırlandırılacağı, bu ağdaki gündem maddelerinin nasıl tespit edileceği, ağın sosyogram olarak nasıl gösterileceği gibi hususlar planlanmıştır.

SOMİS'in ikinci safhası olan toplama ve tasnif safhası kapsamında; ilk olarak Twitter'daki PKK sempatzanlarının tespitine çalışılmıştır. Bu maksatla kartopu örnekleme yöntemi kullanılmıştır. Öncelikle terör örgütü sempatzanlarının paylaşım yaptığı Twitter etiketleri tespit edilmiş, sonrasında bu etiketler çerçevesinde paylaşım

yapan muhtemel terör örgütü sempatzanları bulunmaya çalışılmıştır. Bu hesaplara ulaşıldıktan sonra müteakip aşamada kesinlikle PKK terör örgütü sempatzanı olduğu düşünülen 22 adet çekirdek hesaba ulaşılmış, buradan 22 adet Twitter hesabının takip ettiği toplam 3.529 kişiye ulaşılmıştır.

Tasnif işlemi kapsamında ilk olarak 3.529 hesap içerisinde mükerrer olan hesaplar tespit edilmiş ve veri setinden çıkartılmıştır. 22 hesap sahibinin takip ettiği aynı kişilerin tasnif edilmesinin ardından, 22 adet çekirdek hesap sahibi de dâhil olmak üzere toplamda 1.618 Twitter hesabına ulaşılmıştır. Tasnif işlemi burada sonlandırılmamış, 1.618 adet Twitter hesabı içerisinde bulunan haber ajansları, devlete ait hesaplar, siyasi parti temsilcileri, yabancı devlet başkanları gibi kullanıcılar da ayıklanmış ve sonuç olarak 22 adet hesaptan yola çıkılarak toplamda 1.447 hesaplık PKK terör örgütü sempatzanı veri seti örneklemeine ulaşılmıştır.

SOMİS toplama ve tasnif safhasının bir sonraki aşamasında NodeXL Pro uygulaması kullanılarak, örneklem olarak alınan 1.447 adetlik hesaba ait Twitter verileri toplanmıştır. Bu veriler içerisindeki ağdaki kişilerin paylaştığı 125.564 adet tweetin içeriği, bu tweetlerin kimler tarafından tekrar paylaşıldığı, tweet içeriklerinde kimlerin etiketlendiği, birbirleri ile etkileşime giren gruplar, ağa ait ölçüt hesaplamaları, paylaşımlar içerisinde en çok kullanılan kelimeler ve miktarları bilgileri yer almaktadır.

SOMİS'in bir sonraki ve en önemli safhası elde edilen verilerin analizi safhasıdır. PKK terör örgütü sempatzanlarının oluşturduğu ağın analiz işlemleri NodeXL Pro uygulaması ile yapılmıştır. Analiz sonucu elde edilen verilerden terör örgütünün örneklem olarak alınan bölümünde 1.447 Twitter kullanıcısının birbirlerini takip ettikleri, birbirlerinin paylaşımlarını tekrar paylaştıkları, birbirlerinin paylaşımlarını beğendikleri, paylaşım metinlerinin içerisinde birbirlerini etiketledikleri, kısaca bir etkileşim ağı oluşturdukları görülmüştür.

SOMİS analizi kapsamında elde edilen ölçütlerden birisi ağın iç derece merkezliği derecesidir. İç derece merkeziliği ölçütü sosyal ağ içerisinde en çok etkileşimi alan, başka kullanıcılar tarafından paylaşımı en çok beğenilen, yaptığı paylaşım tekraren en çok paylaşılan, diğerlerinin paylaşımında en çok adı geçen kişiyi göstermektedir. Bu ölçüt Twitter paylaşımını dikkat çekecek şekilde hazırlayan, gündemi yaratabilen kişileri tespit edebilmemize yaramaktadır. PKK terör örgütü sempatzanlarının teşkil ettiği Twitter ağına iç derece merkeziliği puanı en yüksek olan kullanıcı 47 numaralı kullanıcı olup, incelenen ağda gündem yaratabilen kişidir.

Yüksek dış derece merkeziliği ölçütü, bir kullanıcının bir konu hakkında çok fazla sayıda tweet attığını, diğer kullanıcılardan bahsederek, onların tweetlerini yanıtlayarak, diğerlerinin tweetlerini tekrar paylaşarak kullanıcıların dikkatini çeken kişiye işaret etmektedir. PKK terör örgütü sempatizanlarının teşkil ettiği Twitter ağına dış derece merkeziliği puanı en yüksek olan, kullanıcıların dikkatini en çok çekebilen kişi 469 numaralı kullanıcıdır.

SOMİS analizinde elde edilen bir diğer ölçüt arasındalık merkeziliği ölçütü olmuştur. Bu ölçüt sosyal ağ içerisindeki ilişkilerin en ortasında yer alan kişiyi tespit etmektedir. PKK terör örgütü sempatizanlarının oluşturduğu ağda arasındalık merkeziliği değeri en yüksek olan kişi 7 numaralı kullanıcıdır. 7 numaralı kullanıcının PKK terör örgütü sempatizanları ağı içerisinde iletişimin merkezinde, ağın tam ortasında yer aldığı anlaşılmaktadır.

SOMİS çerçevesinde, PKK terör örgütü sempatizanları ağına kanaat önderlerinin kim olduğunu tespit edebilmek maksadıyla sayfa değeri ölçütü hesaplanmıştır. NodeXL Pro ile yapılan sayfa değeri hesaplamasına göre 7 numaralı kullanıcı, PKK terör örgütü sempatizanları ağının kanaat önderi olarak tespit edilmiştir. 7 numaralı kullanıcının arasındalık merkeziliği değeri de en yüksek kişi olması, araştırılan ağda bir iletişim ağının merkezinde yer alması, bu kişinin kanaat önderi olduğunu da doğrulamaktadır. Bu sonuç bize, 7 numaralı kullanıcıya fiziki olarak ulaşmanın mümkün olması halinde yakalanması gerektiğini, bu şahsın ele geçirildiği durumda söz konusu iletişim ağındaki işleyişin sekteye uğrayacağını göstermektedir. 7 numaralı kullanıcının fiziki olarak ele geçirilememesi durumunda ise bu kişinin sosyal medya hesabına erişimin engellenmesi, söz konusu ağın faaliyetlerini engelleyecektir. Bununla birlikte, SOMİS sayesinde bir ağda merkezi konumda bulunan kişi etkisiz hale getirilmeden izlemeye devam edilerek terör örgütü hakkında farkındalık daha fazla artırılabilir.

Elde edilen verilerden, PKK terör örgütü sempatizanlarının Twitter ağına beş ana grup teşkil ettikleri de anlaşılmaktadır. Bu gruplar ağdaki Twitter kullanıcılarının birbirleriyle etkileşim oranlarına göre NodeXL Pro uygulaması tarafından oluşturulmaktadır. SOMİS kapsamında değerlendirildiğinde, sanal bir ortamda birbirlerine daha yakın ve daha fazla etkileşim halinde olan sosyal medya kullanıcılarının gruplandırılmasının önemli olduğu düşünülmektedir. Bu gruplar zamanın ve eldeki imkânların el verdiği ölçüde ayrı ayrı da incelenebilecektir.

SOMİS analizinde kullanılan bir diğer yöntem olan içerik analiziyle, tweet metinleri içerisindeki genel eğilimleri ve temel düşünce kalıpları ortaya çıkarılabilmektedir. PKK terör örgütü sempaticanları ağında paylaşılan 125.564 adet tweetin içerik analizi sonuçlarına göre, araştırmanın yapıldığı dönemde bu ağı en önemli gündem maddesinin Suriye'nin kuzeyinde yer alan Ayn El Arap isimli yerleşim yerinin DEAŞ terör örgütünden kurtarılmasının yıldönümü olduğu görülmektedir. İkinci sıradaki gündem maddesi ise terör örgütü liderinin hapisane koşullarını kamuoyu gündemine taşımayı amaçlayan açıklık grevleri olduğu görülmektedir. PKK sempaticanları ağıının bir diğer gündem maddesi de Irak'ın kuzeyinde terör örgütüne karşı askeri tedbirleri artıran KDP'ye karşı oluşturulan gündemdir.

SOMİS ile terör örgütü sempaticanları ağıındaki gündem maddelerini tespit etmek terör örgütünün güncel konulara yönelik eğilimini, bireyleri radikalleştirmek için kullandığı argümanları, toplumu provoke etmek ve devlete karşı hareketlendirmek maksadıyla ürettiği gerekçeleri, kamu düzenini bozabilecek şekilde yakın gelecekte planladığı gösteri, yürüyüş, eylem gibi faaliyetleri anlayabilmeyi sağlamaktadır.

SOMİS'in amaçlarından birisi olarak belirtildiği şekilde terör örgütünün olası niyetini öğrenmek, terör örgütünün davranışlarına ilişkin emareleri tespit edebilmek oldukça önemlidir. Örneğin, 1.447 kişilik PKK terör örgütü sempaticanları örneğine dâhil edilen 615 numaralı kullanıcının 18 Ocak 2021 tarihinde, "Tekrardan şehir savaşları kaçınılmaz" içeriğiyle paylaştığı tweet, terör örgütünün gelecekte terörü meskûn mahallere yeniden taşıma niyetini ortaya koyabilmektedir.

Her ne kadar paylaşılan bir tweet içeriği ile terör örgütünün geleceğe yönelik niyet ve maksadının ortaya konulması güç olsa da bunun bir emare olabileceği göz önünde bulundurulmalı, bu paylaşıma benzer başka paylaşımların tespiti, terörün meskûn mahallerde sürdürülmesine yönelik paylaşımların sayıca artması, terör örgütü lider kadrosunun bu yöndeki açıklamalarının sıklaşması gibi durumlarda konunun diğer istihbarat yöntemleriyle desteklenmesi önem taşımaktadır.

SOMİS ile elde edilen tweet içeriklerinden ulaşılan bir diğer sonuç ise PKK terör örgütü sempaticanlarının, bireylerin çevrimiçi radikalleşmeleri maksadıyla paylaşımlar yapmalarıdır. Bu kapsamda terör örgütü sempaticanlarının sıklıkla Türk-Kürt ayrımı yaratmaya çalıştıkları, Türklerin Kürtleri ortadan kaldırmak istediğini öne sürerek nefret tohumları ektikleri, terör örgütü faaliyetlerini devlete açılmış bir savaş olarak göstermeye

gayret ettikleri, terör örgütü mensuplarından etkisiz hale getirilenlerin intikamlarının alınması gerektiğini ifade ederek şiddete yönelttikleri de görülmektedir.



SONUÇ VE DEĞERLENDİRME

Terörizm ilk ortaya çıktığı günlerden itibaren değişen şartlara göre sürekli kendisini yenilemiş, kendisine yeni alanlar açmış, yeni yöntemler geliştirmiştir. Teknolojide yaşanan gelişmelerin rüzgârını arkasına alan terör örgütleri her türlü teknolojik yeniliği kullanarak imkân ve kabiliyetlerini artırmışlardır. Terör örgütleri teknolojideki gelişimi; terör eylemi türlerini çeşitlendirmek, daha geniş bir alanda etki üretmek, örgütler arasında iş birliğini geliştirmek için kullanmışlardır. Yerleşim yerlerinde ve kırsal alanda görülen terörizm faaliyetleri, teknolojik gelişmelerle birlikte siber alanda da yerini almaya başlamıştır.

1990'lardan itibaren interneti kendi faaliyetleri ekseninde kullanmaya başlayan terör örgütleri, bu alandaki gelişmeler çerçevesinde 2000'lerin başından itibaren sosyal medya araçlarıyla tanışmış, faaliyetlerinin bir kısmını bu araçlarla yürütmeye başlamışlardır. Gerçek hayatta olduğu gibi bireylerin bir arada bulunabildiği, fikirlerini paylaşabildiği, bir etkileşim mekanizması kurabildiği sosyal medya araçları, terör örgütü sempatanları arasında da sosyal ağların oluşturulmasını sağlamıştır.

Bilginin oldukça hızlı bir biçimde aktarılmasına, terör örgütü elemanlarının ve sempatanlarının kendilerini gizleyebilecek şekilde sanal ortamlarda yer almasına imkân sağlayan, hemen hemen hiçbir maliyeti bulunmayan sosyal medya, terörizm için uygun fırsat alanları yaratmıştır.

Sanal ortamlarda teknolojinin sunduğu fırsatları değerlendiren terör örgütleri sosyal medyayı, yeni terör örgütü elemanları temin etmek, propaganda yapmak, terör örgütüne destek sağlamak, bilgi alışverişinde bulunmak, terör örgütüne mali destek sağlamak maksadıyla kullanmaktadırlar.

Teknolojinin hayatın tüm alanına yayılmasıyla birlikte devletler de, terörizmle mücadelede daha teknolojik silahlar, terör örgütlerinin takibine yönelik daha teknolojik teçhizat kullanmaya başlamışlardır. Teknolojideki gelişmelere paralel olarak, bir yandan terör örgütleri teknolojik eylem ve iletişim yöntemlerini geliştirirken, devletler de daha teknoloji yoğun bir mücadeleye başlamış, terörizmle mücadele yöntem ve araçlarını geliştirmişlerdir.

Bu kapsamda; diplomasi, ceza adalet sistemi, siyasal ve sosyo-ekonomik tedbirler, istihbarat ve askeri kuvvet kullanımı şeklinde sıralanabilen terörizmle mücadele araçları içerisinde askeri kuvvet kullanımı ve istihbaratın teknolojinin ilerlemesine paralel olarak en çok değişim gösteren araçlar olduklarını söyleyebilmek de mümkündür. Terörizmle

mücadele araçlarından istihbarat, terörizmden kaynaklanan tehdidin karar alıcılar tarafından anlaşılması, terör örgütlerinin kapasiteleri hakkında bilgi elde edilmesi, örgütlenme biçimleri, terör eylemlerinin önceden tespit edilerek önlenmesi, terör örgütü taktik ve tekniklerinin belirlenmesi, iletişim yöntemlerinin açığa çıkarılması, terör örgütü mensuplarının yerlerinin tespit edilmesi ve etkisiz hale getirilmesinde büyük önemi haizdir.

Terörizmle mücadele araçlarından hangisi veya hangileri kullanılırsa kullanılsın bu araçların etkinliğinin artırılması için ihtiyaç duyulan istihbarat; terörizmin ortaya çıkmasından önce, terörizmle mücadele süresince ve mücadelenin sonrasında devam eden en önemli terörizmle mücadele aracıdır. Terör örgütlerinin eylem ve hareket tarzlarının tahmin edilebilmesi, terör örgütlerine yönelik etkin operasyonların düzenlenebilmesi, dahası terör eylemlerinin sürpriz etkisinin en aza indirilebilmesi için etkin bir istihbarat sistemi kurulması gerekmektedir. Gelişen teknoloji çerçevesinde terörizmle mücadele istihbaratı da bilgisayar sistemlerinin daha fazla kullanıldığı, verinin tasnif ve analizinde bilgisayar uygulamalarının daha ağırlıklı yer aldığı bir hal almaktadır.

Günlük hayatın bir parçası haline gelen sosyal medya ağlarında paylaşılan verinin büyüklüğü ve bu verinin bir kısmının suç örgütlerince meydana getirildiği göz önünde bulundurulduğunda, günümüzde sosyal medya araçlarından istihbarat elde etmenin ne kadar elzem olduğu anlaşılmaktadır.

Bununla birlikte sosyal medya istihbaratı, çok kaynaklı istihbarat çerçevesinde ele alınmıştır. Başta insan istihbaratı, sinyal istihbaratı, karşı istihbarat, görüntü istihbaratı, coğrafi istihbarat gibi farklı istihbarat disiplinlerini kapsayan çok kaynaklı istihbarat anlayışının sosyal medya istihbaratını da kapsama alanına dâhil ettiği görülmektedir. Bu kapsamda, sosyal medya istihbaratının diğer istihbarat disiplinleri ile eşgüdüm içerisinde faaliyet gösterdiği, diğer istihbarat disiplinleri gibi sosyal medya istihbaratının da kendi yöntemleriyle ürettiği istihbarat ile diğer disiplinlerin açıklarını kapattığı değerlendirilmektedir. Çok kaynaklı istihbarat çerçevesinde, sosyal medya istihbaratının istihbarat resmindeki boşlukları tamamlayan parçalı bilgiler sağladığı, bu nedenle istihbarat toplama planının bir parçası olarak ele alınması gerektiği düşünülmektedir.

Sosyal medya istihbaratı ayrıca “ne oldu”, “ne zaman oldu”, “kim yaptı” gibi temel sorulara cevap vererek kolluk kuvvetlerini bilgilendirmekte, kolluk kuvvetlerinin durumsal farkındalıklarını artırmaktadır. Terörizmle mücadele kapsamında sosyal medya istihbaratı ayrıca, terör örgütlerinin kendi içerisinde ve diğer örgütlerle ilişki modellerini

anlayabilmek, terör örgütlerinin propagandalarını tespit edebilmek, terör eylemi öncesi davranışlara ilişkin emareleri ortaya koyabilmek, sanal alanda radikalleşmeyi önleyebilmek amacıyla kullanılabilir. Terörizmle mücadelede sosyal medya istihbaratı; terör örgütleri sempatanlarının teşkil ettiği sosyal medya ağlarını içeriden gözetlemek, örgüt içi davranışları tespit edebilmek, örgütlerin bir eylem hazırlığında olduğunu önceden tespit edebilmek için de elverişli ortamlar yaratmaktadır.

Terörizmle mücadelede sosyal medya istihbaratı sürecinin; yönlendirme ve planlama, verilerin toplanması, analiz, istihbaratın teyit edilmesi ve dağıtım safhalarından oluşması öngörülmüştür. İstihbarat sürecinin en önemli safhası olan analiz safhasında; duygu analizi; anlam analizi; olay tahmin analizi; netnografi analizi; içerik analizi; sosyal ağ analizi yöntemlerinden biri veya birkaçı bir arada kullanılabilir.

Sosyal ağ analizi, birçok kişinin bir araya gelmesiyle oluşan sosyal gruplar içerisindeki bireylerin birbirleriyle ilişkilerini ve davranış modellerini araştırmak üzere kullanılan bir yöntemdir. Sosyal ağlarda yer alan düğümler ve bu düğümler arasındaki bağlantıların analizi anlamına gelen sosyal ağ analizi, sosyal medya üzerinde oluşan ağları incelemektedir. Sosyal ağların analizi sosyal medyanın günlük hayatımıza girmesiyle birlikte daha fazla görünürlük kazanmaya başlamıştır.

Sosyal ağ analiziyle karmaşık yapıdaki bir ağın tanımlaması, görselleştirmesi ve modellenmesi mümkün olabilmekte, söz konusu ağın yapısının anlaşılması hedeflenmektedir. Sosyal ağ analizi ile ağın bütün yapısı, ağ içindeki alt kümeler ve ağ içerisindeki düğümlerin ayrı ayrı ya da hep birlikte incelenmesi mümkün olabilmektedir. Başka bir deyişle, tek tek veya kümeler halinde ağı oluşturan parçalar ya da ağın bütünü sosyal ağ analizinin araştırma alanı içerisinde düşünülebilmektedir.

Sosyal ağ analizi; bir grubun oluşumu, grup içindeki bireylerin uyumu, bireylerin grup içindeki rolleri, bireylerin grup içindeki etkilerini açıklamaya yardımcı olabilmektedir. Sosyal ağ analizi kullanılarak, bir grupta önemli rolleri üstlenen bireylerin ortaya çıkarılması, incelenen bireylerin ne tür roller oynadıkları, ağ içerisinde bulunan alt gruplar ve bu grupların üyelerinin kimler olduğu, alt gruplar arasındaki bağlantıların varlığı, grupları birbirine bağlayan ve göbek rolünü üstlenen bireylerin kimler olduğu sorularına yanıt bulunabilmektedir.

Sosyal ağ analizi; özellikle dışa kapalı ve gizli örgütlerin ağ yapılanmasını meydana çıkarabilmek, bu ağ içerisindeki alt grupları belirleyebilmek, ağ içerisindeki önemli

bireyleri tespit edebilmek amacıyla terörizmle mücadelede kullanılabilir. Terörizmle mücadelede sosyal medya istihbaratının analiz safhasında kullanılabilecek yöntemlerden birisi olan sosyal ağ analizi yöntemiyle; terör örgütü sempatizanlarının oluşturduğu ağların merkezilik, gruplaşma, kümelenme, bilgi akışının yönü gibi farklı açılardan analiz edilmesi mümkün olabilmektedir.

Gizli faaliyet gösteren örgütlerin ağ yapılarının analizi, bu örgütlerin eleman temini faaliyetlerinin açığa çıkarılması, örgütlerin motivasyonlarının anlaşılması, terör faaliyetlerinde kilit rol oynayan kişilerin tespiti, örgüt içerisindeki bireyler arası ilişkilerin tanımlanması, ağın ortadan kaldırılması için zayıf noktaların belirlenebilmesi sosyal ağ analizi ile mümkün olabilmektedir.

Terörizmle mücadele istihbaratı kapsamında sosyal ağ analizi; terör örgütlerinin teşkil ettiği ağların merkezinde yer alan şahısları, örgütten koparılması durumunda örgütü işlevsiz hale getirebilecek kişileri, örgüt içinde belirlenen bir kişinin hangi rolleri üstlendiğini, bir terör ağı içerisinde hangi iletişim bağlantılarının takip edilmesi gerektiği gibi kritik bilgileri sağlayabilmekte, karar alıcılara terörizmle mücadele konusunda destek vermektedir.

Bu noktada mutlak suretle, sosyal ağ analizinin terörizmle mücadelede kullanılabilecek araçlardan yalnızca birisi olduğunu, sosyal ağ analizinin, terörizmle ilgili bilinmeyenlerin yalnızca bir kısmını bulmaya yardımcı olacağını belirtmek gerekmektedir. Terörizmle mücadelede, terör örgütü sempatizanlarının meydana getirdiği ağların anlaşılmasında, gündemlerinin belirlenmesinde, ağ içerisinde etkin kişilerin tespitinde, bu ağların nasıl etkisiz hale getirileceğine ilişkin kararların alınmasında sosyal ağ analizi yönteminin kullanılabileceği sonucuna varılmıştır.

Tezin temel araştırma problemi; “Sosyal medya üzerinden verilerin toplanması, toplanan verilerin sosyal ağ analizi yöntemi ile analizi şeklinde yürütülecek sosyal medya istihbaratı çalışmaları, PKK terör örgütüyle mücadelede hangi katkıları sağlayabilir?” şeklinde oluşturulmuştur. Yöntem uygulamasının sonucunda tezin başlangıç aşamasında oluşturulan araştırma problemi ve alt problemlere ilişkin cevaplar aranmıştır. Bu çerçevede, PKK terör örgütüyle mücadelede sosyal medya istihbaratının, çok kaynaklı istihbarat kapsamında değerlendirilebileceği, PKK ile ilgili istihbarat resminin eksik parçalarını tamamlamak üzere sosyal medya istihbaratının önemli katkılar sunabileceği sonucuna ulaşılmıştır. Örneğin sosyal ağ analizi neticesinde terör örgütünün Twitter ağında etkin rol oynayan şahısların tespit edilebileceği, bu ağdaki grupların belirlenebileceği,

kanaat önderlerinin ortaya çıkarılabileceği, örgütün gündem maddelerinin öğrenilebileceği sonucuna varılmıştır.

Ayrıca tezin araştırma deseninin hazırlanması sürecinde oluşturulan alt araştırma problemleri çerçevesinde, terörizmle mücadele istihbaratı kapsamında sosyal medyanın PKK terör örgütü başta olmak üzere terör örgütleri hakkında veri elde etmek maksadıyla kullanılabilecek en uygun araçlardan birisi olduğu cevabına erişilmiştir.

Ürettiği büyük verinin devasa boyutlara ulaşan hacmi, güncel olaylara ilişkin sürekli veri üretmesi, bir olaya yönelik olarak terör örgütlerinin bakış açısına yer vermesi, örgütlerin geleceğe yönelik niyetlerini açığa vurabilmesi, terör örgütü liderlerinin düşüncelerine yer vermesi, yeni elemanlar temin etmek üzere bireylere çağrıda bulunması ve yön vermesi, özellikle gençlerin radikalleşmesi için paylaşımların bulunması nedeniyle sosyal medyanın terör örgütleri hakkında istihbarat üretmek üzere uygun bir araç olduğu sonucuna ulaşılmıştır.

Araştırmanın alt problemleri çerçevesinde sosyal ağ analizinin terörizmle mücadele istihbaratının analiz basamağı olarak kullanılabileceği sonucuna varılmıştır. Sosyal medya istihbaratının analiz safhasında kullanılabilecek duygu, anlam, olay tahmin, netnografi ve içerik analizlerinin yanı sıra sosyal ağ analizinin de istihbarat analizi yöntemi olarak kullanılabileceği görülmektedir.

Sosyal ağ analizinin; karmaşık bilgileri anlamlandırmada, terör örgütü ağ yapılarının belirlenmesinde, ağların içerisinde yer alan irili ufaklı grupların tespitinde, ağ içerisindeki kişilerin birbirleriyle bağlantılarının ortaya konulmasında, alt gruplar arasındaki ilişkilerin modellenmesinde kullanılabileceği sonucuna varılmıştır.

Sosyal medya istihbaratının terörizmle mücadelede kullanımının birkaç farklı yöntemi olduğu görülmüştür. Terör örgütleri hakkında bilgi elde etmenin en etkin yolu insan istihbaratı yönteminin kullanılması iken, terör örgütlerine sızmak ve örgüt içerisinde doğrudan bilgi almak her zaman mümkün olmamaktadır. Ancak sosyal medyada yer alan terör örgütü mensupları ve sempatizanları arasında sızmak, terör örgütü sempatizanlarının teşkil ettiği ağlar içerisinde yer almak, bu sayede terör örgütlerinin içerisinde doğrudan bilgi edinebilmenin sosyal medya istihbaratıyla mümkün olduğu sonucuna erişilmiştir.

Sosyal medyadan elde edilecek istihbaratın terörizmle mücadelede kullanımının, ikinci şekli; terör örgütü gündemlerinin, propaganda temalarının tespit edilmesi olduğu

sonucu karşımıza çıkmaktadır. Terör örgütü sempatizanlarının gündemlerini öğrenerek terör örgütü hakkında farkındalığın artırılabilceği, terör örgütlerinin daha iyi anlaşılabilceği, bu sayede terör örgütünün gelecekte yapabileceklerine ilişkin çıkarımlarda bulunulabilceği sonucuna varılmıştır.

Üçüncü olarak, sosyal medya istihbaratı ile terör örgütlerinin eleman temini gayretlerine ilişkin bilgilere erişilebildiği görülmüştür. Her ne kadar terör örgütleri gizli örgütlenmeler olsalar da bazı faaliyetleri için görünürlüklerinin en üst seviyelere çıktığı, bu faaliyetlerden birisinin de eleman temini faaliyeti olduğu görülmektedir. Hem DEAŞ hem de PKK terör örgütü örneklerinde olduğu üzere, terör örgütlerine yeni eleman temini faaliyetlerinin sosyal medya istihbaratı ile açığa çıkarılabilceği sonucu elde edilmiştir.

Dördüncüsü, sosyal medya istihbaratı ile terör örgütü mensuplarının ve sempatizanlarının teşkil ettiği ağ içerisinde mevcut grupları, bu grupların birbirleriyle ilişkilerini, ağ içerisinde kilit konumda bulunan şahısları, gruplar arasında bağlantı konumunda olan bireyleri, hangi kişiler ağdan kopartılırsa terör örgütü iletişim ve propaganda ağının işleyişinin sekteye uğrayabileceğinin tespiti de mümkün olabilmektedir. Bu kapsamda, sosyal medyada terör örgütü propagandası yapanların tamamına ait hesapların takibi veya askıya alınması mümkün olamayacağından, tespit edilen kilit hesaplara işlem yapılmasının terör örgütlerinin sanal alanda oluşturduğu ağların işleyişini etkileyebileceği, terörizmle mücadele eden kolluk kuvvetlerinin işlerinin de bu sayede kolaylaşacağı sonuna varılmıştır.

Tezin araştırma deseni oluşturulurken, ortaya konulan temel varsayım; “PKK terör örgütü sempatizanlarının Twitter uygulaması üzerindeki varlığının sosyal medya istihbaratı kapsamında sosyal ağ analizi yöntemiyle incelenmesi neticesinde, terör örgütünün propaganda ve haberleşme ağının ortaya çıkarılabilceği” şeklinde ortaya konulmuştur. Araştırmanın sonucunda varsayımın doğrulandığı, PKK terör örgütü sempatizanlarının teşkil ettiği sosyal medya ağlarından örgütün propaganda ve haberleşme ağlarının kolaylıkla tespit edilebildiği sonucuna erişilmiştir.

Araştırmanın bir diğer varsayımı ise; “Twitter’den üretilecek sosyal medya istihbaratı sayesinde PKK terör örgütü faaliyetleri hakkında güvenlik güçlerinin farkındalığının en üst seviyeye çıkarılabilceği” şeklinde oluşturulmuştur. Araştırma sonucunda, PKK terör örgütü sempatizanlarının belirlenen etiketler yani gündemler hakkında hangi yönde tepki verdiklerinin, ana gündemlerinin ne olduğunun tespit edilebildiği görülmektedir. Terör örgütü gündeminin tespit edilmesi durumunda kolluk

kuvvetlerinin örgüt hakkındaki farkındalığının en üst seviyeye çıkarılabileceği sonucuna ulaşılmıştır.

Tezin son varsayımı ise “PKK terör örgütü Twitter hesaplarının teşkil ettiği ağların takibi sayesinde örgütün geleceğe yönelik muhtemel faaliyetlerinin tahmin edilebileceği” şeklindedir. Yöntem uygulamasının sonucunda, sosyal medya istihbaratıyla terör örgütünün geleceğe yönelik niyetinin tespitinin mümkün olabileceği ancak bunun için terör örgütü sempatizanlarının sosyal medya hesaplarının sürekli takibine, bu takip için gelişmiş bilgisayar sistemleri ve yazılımların kullanımına ihtiyaç duyulduğu sonucuna varılmıştır. Yöntem uygulamasında bahsedilen, PKK terör örgütü sempatizanlarının terörü meskûn mahallere yeniden taşıma niyetine işaret eden paylaşım, 125.564 adet tweetin içerik analizinin manuel olarak, yalnızca bir kişi tarafından yapılan inceleme neticesinde tespit edilmiştir. Araştırmada örneklemin daraltıldığı, istihbarat birimlerince bu örneklemin çok daha büyüğüne ilişkin verilerin analiz edilebileceği göz önünde bulundurulduğunda, terör örgütünün gelecek niyetine ilişkin emarelere ulaşılmasının mümkün olabileceği değerlendirilmektedir.

PKK terör örgütü sempatizanlarının Twitter üzerinde teşkil ettikleri ağda gündemi oluşturabilen, ağ içerisinde en çok etkileşimi alan, başka kullanıcılar tarafından paylaşımı en çok beğenilen, yaptığı paylaşım tekraren en çok paylaşılan, diğerlerinin paylaşımında en çok adı geçen kişinin tespit edilebildiği görülmüştür. Ayrıca uygulamada; bir konu hakkında çok fazla sayıda tweet atan, paylaşımlarında diğer kullanıcılardan bahsederek, onların tweetlerini yanıtlayarak, diğerlerinin tweetlerini tekrar paylaşarak kullanıcıların dikkatini çeken kişiye de ulaşmak mümkün olmuştur.

Araştırmanın uygulama safhasında PKK terör örgütü sempatizanları ağı içerisinde iletişimin merkezinde, ağın tam ortasında yer alan kişi bulunabilmiş, bu kişinin aynı zamanda incelenen ağda kanaat önderi olduğu sonucuna varılmıştır. PKK terör örgütü sempatizanlarına ilişkin araştırmada ayrıca ağ içerisinde alt grupların bulunduğu, her grup içerisinde ayrı ayrı olmak üzere kanaat önderlerinin bulunduğu da görülmüştür. Sosyal medya istihbaratı ile ulaşılabilen bu kişilerin takip edilmesiyle terör örgütüne ilişkin farkındalığın daha da artırılabilceği, bu kişilerin fiziki konumlarının bulunabileceği ve etkisiz hale getirilebileceği ya da bu kişiye ait hesapların askıya alınabileceği sonucuna varılmıştır.

Sosyal medya istihbaratı çerçevesinde araştırmanın uygulama safhasında içerik analiziyle tweet metinleri içerisindeki genel eğilimler ve temel düşünce kalıpları da ortaya

çıkarılabilmektedir. Son olarak uygulama sonucunda, terör örgütü sempatzanlarının Twitter paylaşımlarında kutuplaştırıcı temalar kullanarak gençler arasında radikalleşmeyi artırmaya çalıştığı sonucuna erişilmiştir. Bu tespitler neticesinde istihbarat birimlerinin terör örgütü söylemlerine yönelik karşı söylemler üretebilecekleri / ürettirebilecekleri ve radikalleşmenin önüne geçebilmek için yürütülen çabalara katkı sunabilecekleri değerlendirilmektedir.

Terörizmle mücadelede sosyal medya istihbaratı üretiminin araştırılması süresince bir takım güçlükler ve sınırlılıklarla da karşılaşmıştır. Örneğin, terör örgütü sempatzanlarının teşkil ettiği ağların analizi için gerekli verileri toplama konusunda bazı zorluklarla karşılaşıldığı belirtilmelidir. Sosyal medyada terör örgütü sempatzanlarının oluşturduğu ağların analiz edilmesi için gerekli veriler toplanırken verilerin güvenilirliği konusunda tereddütler yaşanabilmektedir. Bu tereddütlerin giderilebilmesi için bazı kriterlerin belirlenmesi, bu kriterler doğrultusunda verilerin güvenilirliğinin test edilmesi, bunu sağlayabilmek için ise analistin belirli bir tecrübe seviyesine sahip olması gerekebilmektedir.

En büyük zorluklardan birisi, sosyal medyada terör örgütlerine yönelik alınan karşı tedbirler neticesinde, araştırmaya dâhil edilen Twitter hesaplarının süreç içerisinde engellenmesi ve kapatılmasıdır. Engellenen ve kapatılan hesapların sayısının artması veri setinin daralmasına ya da sürecin tekrar edilebilmesine neden olabilmektedir.

Analiz sürecine ilişkin bir diğer kısıtlılık sosyal ağ analizi maksadıyla kullanılan bilgisayar programlarının ve kullanılan bilgisayarın kapasiteleriyle ilgilidir. Bu çalışmada Twitter'dan veri toplamak ve toplanan verileri analiz etmek için kullanılan NodeXL Pro uygulaması ile en fazla 9.999 kullanıcının verilerine erişilebilmekte, analiz süreci saatlerce sürebilmektedir. Bu nedenle istihbarat birimlerince bu tür araştırmaların yapılması için süratli ve kapasite sorunu olmayan bilgisayar yazılımları hazırlatılmalıdır.

Örneğin, bu çalışmada seçilen örneklem; araştırmada kullanılan bilgisayar sisteminin kullanıcı seviyesinde olması, araştırmanın bir ekip yerine bir kişi tarafından yapılması, araştırmanın bazı basamaklarının manuel olarak yapılması gibi nedenlerle az sayıda kullanıcıdan oluşturulmuştur. İstihbarat örgütleri gibi büyük organizasyonlar tarafından benzer bir yöntemin kullanılması gerektiğinde gelişmiş bilgisayar sistemlerinin kullanılması, bu çalışmada manuel olarak yapılmaya çalışılan ayıklama basamağı için bilgisayar yazılımları hazırlanması mümkün olacaktır. Bu durumda çok daha büyük bir

örneklem üzerinden veri elde etmenin mümkün olabileceği, daha büyük bir örneklemde daha anlamlı sonuçlara ulaşılabileceği değerlendirilmektedir.

Sosyal medya istihbaratı sürecine yönelik bir diğer sınırlılık ise sosyal medya uygulamalarını kullanan kişilerin kimlik belirtme zorunluluklarının bulunmaması, kullanıcıların doğru olamayan içerikleri paylaşabilmeleridir. Bu nedenle incelenen sosyal medya hesaplarına ilişkin doğrulama kriterlerinin belirlenmesi ve kullanılması gerektiği, elde edilen istihbaratın diğer istihbarat yöntemleriyle teyit edilmesi gerektiği değerlendirilmektedir.

Sosyal medya istihbaratı kapsamında, sosyal ağ analizi gibi yöntemlerin nasıl uygulanacağı, sosyal ağ analizinde kullanılacak bilgisayar destekli uygulamaların nasıl kullanılacağı gibi hususların öğrenilmesi de ayrıca zaman ve çaba gerektirmektedir. Bu nedenle sosyal ağ analizine bir miktar kaynak ve personel ayırmak gerekebilmektedir.

Bu çalışma, terörizmle mücadele kapsamında sosyal medyadan üretilen istihbaratın, diğer istihbarat disiplinleri ile birlikte kullanılabileceğini, sosyal medya istihbaratının diğer istihbarat disiplinlerine katkı sunabileceğini ortaya koymaktadır. Teknolojideki gelişmelere paralel olarak istihbarat disiplinindeki gelişmelere ayak uydurabilmenin önemli olduğu, bu kapsamda terörizmle mücadelede de sosyal medya istihbaratına ağırlık verilmesi gerektiği, bu disiplinin tamamlayıcı bir istihbarat disiplini olarak kullanılması hususunun göz önünde bulundurulması gerektiği düşünülmektedir. Ayrıca sosyal medya istihbaratının geleceğin istihbarat disiplinlerinden birisi olacağı, bu disiplinin açık kaynak istihbaratından ayrı olarak değerlendirilmesi gerektiği kıymetlendirilmektedir. Sonuç olarak; sosyal medya istihbaratının terörizmle mücadelede farklı bakış açıları sunabileceği, terörizmle mücadeleye diğer istihbarat disiplinleri ile birlikte katkı sağlayabileceği değerlendirilmektedir.

Terörizmle mücadelede sosyal medya istihbaratı kapsamında yapılabilecek müteakip çalışmalarda; terör örgütü sempatizanlarının sosyal medya üzerinde oluşan ağların duygu analizi yöntemiyle incelenebileceği, sosyal medya paylaşımlarının sürekli şekilde makine öğrenmesiyle takip edilmesi ve örgütlerin geleceğe ilişkin niyetlerinin ortaya çıkarılabilmesine yönelik araştırmalar yapılabileceği değerlendirilmektedir.



KAYNAKÇA

- Adalı, E. (2016). Doğal dil işleme. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 5(2): 1-19.
- Agarwal, S., Sureka, A. ve Goyal, V. (2015). Open source social media analytics for intelligence and security informatics applications. *International Conference on Big Data Analytics* içinde (ss. 21-37). Springer. doi: 10.1007/978-3-319-27057-9_2.
- Aguirre, A. P. (2009). The Philippine response to terrorism. *Journal of Policing, Intelligence and Counter Terrorism*, 4(1): 47-63. doi:10.1080/18335300.2009.9686923.
- Ağcasulu, H. (2018). Sosyal bilimlerde ilişkileri inceleyen bir yöntem: Sosyal ağ analizi. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 22 (Özel Sayı 2): 1915-1933.
- Akay, E. Ç. (2018). Ekonometride yeni bir ufuk: Büyük veri ve makine öğrenmesi. *Sosyal Bilimler Araştırma Dergisi*, 7(2): 41-53.
- Akhgar, B. (2017). OSINT as an integral part of the national security apparatus. Akhgar, B., Bayerl, P. S., & Sampson, F. (Ed.). *Open Source Intelligence Investigation: From Strategy to Implementation* içinde (ss. 3-10). Springer Yayınları.
- Aköz, S. (2020). *Siyasi istihbarat*. Gazi Kitabevi.
- Al-Danani, A. M. ve Amor, R. B. (2020). Using social media websites to promote terrorism issues-a study of site users'sample. *International Journal of Research*, 8(5): 55-77, doi: 10.29121/granthaalayah.v8.i5.2020.62.
- Altındağ, N. (2020). Türkiye'nin PKK bölücü terör örgütü ile mücadelesine dair bir analiz. *Anadolu Strateji Dergisi*, 2(1): 33-48.
- Amble, J.C. (2012). Combating terrorism in the new media environment. *Studies in Conflict & Terrorism*, 35(5): 339-353, doi: 10.1080/1057610X.2012.666819.
- Andrei, E. A. (2015). The role of OSINT collection in intelligence and the future of intelligent search. *Redefining Community in Intercultural Context*, 4(1): 193-196.
- Antonius, N. ve Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The international technology management review*, 3(1): 42-53.
- Arıboğan, D. Ü. (2007). *Terör korku hali*. Profil Yayıncılık.
- Arquilla, J. ve Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation.
- Badey, T. J. (1998). US anti-terrorism policy: The Clinton administration. *Contemporary Security Policy*, 19(2): 50-70. doi:10.1080/13523269808404190.
- Baharççek, A. (2000). Etnik terör ve etnik terörle mücadele sorunu. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 10(1): 11-27.
- Baltacı, A. (2018). Nitel araştırmalarda örnekleme yöntemleri ve örnek hacmi sorunsalı üzerine kavramsal bir inceleme. *Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 7(1): 231-274.
- Bányász, P. (2018). Social media and terrorism. *Academic and Applied Research in Military Science*, 17(3): 47-62.

- Barbier, G. ve Liu, H. (2011). Data mining in social media. Aggarwal, C.C. (Ed.) *Social Network Data Analytics* içinde. (ss.327-352). Springer.
- Bartlett, J. ve Reynolds, L. (2015). *The state of the art 2015: a literature review of social media intelligence capabilities for counter-terrorism*. Demos.
- Bastian M., Heymann S. ve Jacomy M. (2009). Gephi: an open source software for exploring and manipulating networks. *International AAAI Conference on Weblogs and Social Media*. Erişim tarihi: 11 Ocak 2021, <https://gephi.org/publications/gephi-bastian-feb09.pdf>.
- Başbuğ, İ. (2011). *Terör örgütlerinin sonu*. Remzi Kitabevi.
- Bean, H. (2011). *No more secrets: Open source information and the reshaping of U.S. intelligence*. Praeger.
- Behera, R.K, Jena, M., Naik, D., Sahoo, B. ve Kumar Rath,S.K. (2018). Linkage-based social network analysis in distributed platform. Panda, M., Abraham, A. ve Hassanien, A.E. (Ed.). *Big data analytics: A social network approach* içinde. (ss.1-25). CRC Press.
- Benhiba, L., Loutfi, A., Abdou, M. ve Idrissi, J. (2017). A classification of healthcare social network analysis applications. (*Biostec 2017*): 147-158. doi:10.5220/0006168001470158.
- Berger, J.M. ve Morgan, J. (2015). The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter. *Analysis Paper No.20, Center for Middle East Policy at Brookings*.
- Berkowitz, B. (2002). Intelligence and the war on terrorism. *Orbis*, 46(2): 289-300.
- Bertram, L. (2016). Terrorism, the internet and the social media advantage: exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism. *Journal for Deradicalization*, (7): 225-252.
- Bimfort, M.T. (1958). A definition of intelligence. *Studies in Intelligence*, 2(4): 75-78.
- Bonner, D. (1992). United Kingdom: The United Kingdom response to terrorism. *Terrorism and Political Violence*, 4(4): 171–205. doi:10.1080/09546559208427180.
- Boyd, D. M. ve Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1): 210-230. doi:10.1111/j.1083-6101.2007.00393.x.
- Bremer, L. P. (1989). Continuing the fight against terrorism. *Terrorism*, 12(2): 81–87. doi:10.1080/10576108908435770.
- Bremer, L. P. (1992). The West's counter-terrorist strategy. *Terrorism and Political Violence*, 4(4): 255–262. doi:10.1080/09546559208427185.
- Bright, D. A., Hughes, C. E., ve Chalmers, J. (2011). Illuminating dark networks: a social network analysis of an Australian drug trafficking syndicate. *Crime, Law and Social Change*, 57(2): 151-176. doi:10.1007/s10611-011-9336-z.
- Bright, J., Margetts, H., Hale,S. ve Yasserli, T. (2014). *The use of social media for research and analysis: a feasibility study*. Erişim tarihi: 03 Kasım 2020 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387591/use-of-social-media-for-research-and-analysis.pdf.

- Buzan, B. (2006). Will the “global war on terrorism” be the new Cold War? *International Affairs*, 82(6): 1101–1118. doi:10.1111/j.1468-2346.2006.00590.x.
- Byman, D. (2005). Confronting Syrian-backed terrorism. *The Washington Quarterly*, 28(3): 99-113, doi: 10.1162/0163660054026498.
- Byman, D. (2006). Friends like these: Counterinsurgency and the war on terrorism. *International Security*, 31(2): 79–115. doi:10.1162/isec.2006.31.2.79.
- Byman, D. (2013). The intelligence war on terrorism. *Intelligence and National Security*, 29(6): 837-863. doi: 10.1080/02684527.2013.851876.
- Byman, D. (2018). *An intelligence reserve corps to counter terrorist use of the internet. AEGIS Paper Series*. Hoover Institution. Erişim tarihi: 12 Kasım 2020 https://www.hoover.org/sites/default/files/research/docs/byman_webready.pdf.
- Cardona, M. (1992). The European response to terrorism. *Terrorism and Political Violence*, 4(4): 245–254. doi:10.1080/09546559208427184.
- Carr, C. (1996). Terrorism as warfare: The lessons of military history. *World Policy Journal*, 13(4): 1-12.
- Carter, B. A. (2017). *Analyzing the criminal justice and military models of counterterrorism: Evidence from the United States*. (Yayımlanmamış Doktora Tezi). Kansas Üniversitesi.
- Carter, C. R., Ellram, L. M., ve Tate, W. (2007). The use of social network analysis in logistics research. *Journal of Business Logistics*, 28(1): 137–168. doi:10.1002/j.2158-1592.2007.tb00235.x.
- Carter, J., Maher, S. ve Neumann, P. (2014). *#Greenbirds: Measuring importance and influence in Syrian foreign fighter networks*. Erişim tarihi: 01 Kasım 2020, <https://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Influence-in-Syrian-Foreign-Fighter-Networks.pdf>. 1-32.
- Celaya, F. (2009). The terrorist threat is being materially and normatively shaped by national and global institutions of law and order: Spain and beyond. *Athena Intelligence Journal*, 4(1): 7-34.
- Chalk, P. (1995). The liberal democratic response to terrorism. *Terrorism and Political Violence*, 7(4): 10–44. doi:10.1080/09546559508427316.
- Chatfield, A.T., Reddick, C.G. ve Brajawidagda, U. (2015). Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided twitter networks. *Proceedings of the 16th Annual International Conference on Digital Government Research*. 239-249. doi: 10.1145/2757401.2757408.
- Chauhan, S. ve Panda, N. K. (2015). *Hacking web intelligence*. Syngress.
- Cidell, J. (2010). Content clouds as exploratory qualitative data analysis. *Area*, 42(4): 514-523. doi: 10.1111/j.1475-4762.2010.00952.x.
- Clifton, A. ve Webster, G.D. (2017). An introduction to social network analysis for personality and social psychologists. *Social Psychological and Personality Science*, 8(4): 442-453. doi: 10.1177/1948550617709114.
- Cohen-Almagor, R. (2017). Jihad online: how do terrorists use the internet? Freire, F. C., Araújo, X. R., Fernández, V. A. M., & García, X. L. (Ed.). *Media and Metamedia Management* içinde (ss. 55-66). Springer International Publishing.

- Constantinides, E. ve Fountain, S. J. (2008). Web 2.0: Conceptual foundations and marketing issues. *Journal of Direct, Data and Digital Marketing Practice*, 9(3): 231-244.
- Crelinsten, R.D ve Schmid, A.P. (1992). Western responses to terrorism: A twenty-five year balance sheet. *Terrorism and Political Violence*, 4(4): 307-340. doi: 10.1080/09546559208427189.
- Crenshaw, M. (1987). Theories of terrorism: Instrumental and organizational approaches. *Journal of Strategic Studies*, 10(4): 13-31, doi:10.1080/01402398708437313.
- Crenshaw, M. (1999). Martha Crenshaw on how terrorism ends. *How terrorism ends special report*. United States Institute of Peace. https://www.files.ethz.ch/isn/39859/1999_may_sr48.pdf.
- Cronin, A.K. (2003). Behind the curve: Globalization and international terrorism. *International security*, 27(3): 30-58.
- Cronin, A.K. (2009). *How terrorism ends: Understanding the decline and demise of terrorist campaigns*. Princeton University Press.
- Cronin, A.K. (2010). The evolution of counterterrorism: Will tactics Trump strategy? *International Affairs*, 86(4): 837-856. doi:10.1111/j.1468-2346.2010.00915.x.
- Cronin, A. K. (2012). U.S. grand strategy and counterterrorism. *Orbis*, 56(2): 192-214. doi:10.1016/j.orbis.2012.01.004.
- Cross, R., Parker, A., Prusak, L. ve Borgatti, S. (2001). Knowing what we know: Supporting knowledge creation and sharing in social networks. *Organizational Dynamics*, 30(2): 100-120. doi: 10.1016/S0090-2616(01)00046-8.
- Çetin, Ş. E. ve Ayhan, A. (2020). Katılımcı kültür olgusu bağlamında sosyal medya: Netnografik bir analiz. *Intermedia International E-journal*, 7(12): 47-69. doi: 10.21645/intermedia.2020.66.
- Çitlioğlu, E. (2011). *İnsanı, dünyayı terörizmi anlamak*. Destek Yayınevi.
- Dahl, E. J. (2005). Warning of terror: Explaining the failure of intelligence against terrorism. *Journal of Strategic Studies*, 28(1): 31-55.
- Dean, G. ve Bell, P. (2012). The dark side of social media: Review of online terrorism. *Pakistan Journal of Criminology*, 3(4): 1-24.
- Demir, C. K. (2015). Terörizmle mücadelede örgütsel yaşam evreleri yaklaşımı. *Güvenlik Stratejileri Dergisi*, 11(22): 131-166.
- Demir, C. K. (2017). *Sebeplerinden mücadele yöntemlerine etnik ayrılıkçı terörizm: PIRA, ETA, PKK*. Nobel Akademik Yayıncılık.
- Demir, C. K. (2018). Terörizm ve terörizmle mücadele. Sarı, G. ve Demir, C.K. (Ed.) *Teoriden uygulamaya güvenlik üzerine içinde*. (ss. 159-206). Gazi Kitabevi.
- DePaolo, C. A. ve Wilkinson, K. (2014). Get your head into the clouds: Using word clouds for analyzing qualitative assessment data. *TechTrends*, 58(3): 38-44. doi: 10.1007/s11528-014-0750-9.
- Department of Homeland Security. (2010). *Terrorist use of social networking facebook case study*. Erişim tarihi: 06 Kasım 2020, <https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/>.

- Dietrich, F. (2013). Anti-terrorism policies and the risk of provoking. *Journal of Theoretical Politics*, 26(3): 405–441. doi:10.1177/0951629813505721.
- Dupont, A. (2003) Intelligence for the twenty-first century. *Intelligence and National Security*, 18(4): 15-39, doi:10.1080/02684520310001688862.
- Duyvesteyn, I. (2008). Great expectations: the use of armed force to combat terrorism. *Small Wars & Insurgencies*, 19(3): 328-351. doi:10.1080/09592310802228666.
- Ekşim, A. ve Civelek, İ. (2019). Twitter tweetleri üzerinden açık kaynak istihbaratı tabanlı yarı otomatik siber güvenlik modeli. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 7(1): 827-836.
- Emre, İ.E. ve Erol, Ç.S. (2017). Veri analizinde istatistik mi veri madenciliği mi? *International Journal of Informatics Technologies*, 10(2): 161-167. doi: 10.17671/gazibtd.309297.
- Enders, W., Sandler, T., ve Cauley, J. (1990). UN conventions, technology and retaliation in the fight against terrorism: An econometric evaluation. *Terrorism and Political Violence*, 2(1): 83–105. doi:10.1080/09546559008427052.
- Enders, W. ve Sandler, T. (2000). Is transnational terrorism becoming more threatening? A time-series investigation. *Journal of Conflict Resolution*, 44(3): 307-332.
- Ergürel, D. (22 Aralık 2015). *Askeri istihbarat sosyal medyada*. Erişim tarihi: 10 Kasım 2020, <https://medium.com/turkce/askeri-istihbarat-sosyal-medyada-2327f071a98d>.
- Evans, R. (2013). *Social media intelligence: Current approaches & emerging opportunities*. IHS White Paper. Erişim tarihi: 8 Kasım 2020, <https://nebula.wsimg.com/5a9a81c29f616cba7a515ab16c0a58cc?AccessKeyId=D535D04439DEB65C2F17&disposition=0&alloworigin=1>.
- Fabe, A. P. H. (2017). Countering terrorism in Sri Lanka. Romaniuk, S.N., Grice, F., Irrera, D. ve Webb, S. (Ed). *The Palgrave Handbook of Global Counterterrorism Policy* içinde (ss. 635-648). Palgrave Macmillan.
- Falode, A.J. (2018). Terrorism 4.0: A global and structural analysis. *Open Political Science Journal*, 1: 153-163.
- Faria, J. R. (2006). Terrorist innovations and anti-terrorist policies. *Terrorism and Political Violence*, 18(1): 47-56.
- Fassrainer, V. (2020). Tweeting terror live: Al-Shabaab's use of Twitter during the Westgate attack and implications for counterterrorism communications. *Military Review*, 100(2): 85-95.
- Flavius-Cristian, M. ve Andreea, C. M. (2013). The role of intelligence in the fight against terror. *European Scientific Journal*, 9(2): 1-11.
- Fornacciari, P., Mordonini, M. ve Tomaiuolo, M. (2015). *Social network and sentiment analysis on Twitter: Towards a combined approach*. 53-64. Erişim tarihi: 25 Aralık 2020, <http://www.ce.unipr.it/people/tomamic/files/kdweb15-fmt.pdf>.
- Fredericks, K.A. ve Durland, M.M. (2005). The historical evolution and basic concepts of social network analysis. *New Directions for Evaluation*, 107: 15–23. doi:10.1002/ev.158.
- Freedman, L. (2002). The coming war on terrorism. *The Political Quarterly*, 73(1): 40–56. doi:10.1111/1467-923x.73.s1.5.

- Freeman, L. C. (2004). *The development of social network analysis: A study in the sociology of science*. Empirical Press.
- Friedman, L. ve Friedman, H. (2008). The new media technologies: Overview and research framework. *SSRN Electronic Journal*. doi:10.2139/ssrn.1116771.
- Friedman, R.S. (2004). Open-source intelligence: A review essay. George, R.Z. ve Robert D. Kline, R.D. (Ed). *Intelligence and the national security strategist: Enduring issues and challenges* içinde. (ss. 273–278). National Defense University Press.
- Gendron, A. (2010). Confronting terrorism in Saudi Arabia. *International Journal of Intelligence and Counter Intelligence*, 23(3): 487-508, doi: 10.1080/08850601003780946.
- Gill, P. ve Phythian, M. (2018). *Intelligence in an insecure world*. Polity Press.
- Goepner, E. W. (2016). Measuring the effectiveness of America's war on terror. *Parameters*, 46(1): 107-120.
- Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, 78(6): 1360-1380.
- Gregory, S. (2003). France and the war on terrorism. *Terrorism and Political Violence*, 15(1): 124–147. doi:10.1080/09546550312331292987.
- Gregory, S. (2007). The ISI and the war on terrorism. *Studies in Conflict & Terrorism*, 30(12): 1013–1031. doi:10.1080/10576100701670862.
- Guillaume, G. (1992). France and the fight against terrorism. *Terrorism and Political Violence*, 4(4): 131–135. doi:10.1080/09546559208427177.
- Gülpınar Demirci, V. (2020). Ağ bilimi. Gülpınar Demirci, V. ve Çilingirtürk, A.M. (Ed.). *Sosyal ağ analizi yöntem ve işletme uygulamaları* içinde (ss.8-89). Ekin Basım Yayın Dağıtım.
- Gülpınar Demirci, V. ve Çilingirtürk, A.M. (Ed.) (2020). *Sosyal ağ analizi yöntem ve işletme uygulamaları*. Ekin Basım Yayın Dağıtım.
- Güneş, E. (2019). Terörizmle mücadelede yeni bir trend olarak terör örgütleriyle görüşme tekniği: PKK/KCK örneği. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, 6(2): 266-286.
- Gürsakar, N. ve Uça Güneş, E.P. (2016). Sosyal ağ analizi. *Anadolu Üniversitesi yayını* No: 3388.
- Hamill, J.T., Deckro, R.F., Chrissis, J.W. ve Mills, R.F. (2008). Analysis of layered social networks. *Professional Journal of Joint Information Operations*. 27-33.
- Hanlon, L. (2007). UK anti-terrorism legislation: Still disproportionate? *The International Journal of Human Rights*, 11(4): 481–515. doi:10.1080/13642980701659997.
- Hansen, D.L., Shneiderman, B., Smith, M.A. ve Himelboim, I. (2020). *Analyzing social media networks with NodeXL: Insights from a connected world*. Morgan Kaufmann.
- Hardy, C., Harley, B. ve Phillips, N. (2004). Discourse analysis and content analysis: Two solitudes. *Qualitative Methods*, 2(1): 19-22. doi: 10.5281/zenodo.998649.
- Hassan, N. ve Hijazi, R. (2018). Social Media Intelligence. Hassan, N. ve Hijazi, R. (Ed.) *Open Source Intelligence Methods and Tools* içinde (ss. 203-260). Apress.

- Haythornthwaite, C., Wellman, B., & Mantel, M. (1995). Work relationships and media use: A social network analysis. *Group Decision and Negotiation*, 4(3), 193–211. doi:10.1007/bf01384688.
- Hellmich, C. (2012). Fighting Al Qaeda in Yemen? Rethinking the nature of the Islamist threat and the effectiveness of U.S. Counterterrorism Strategy. *Studies in Conflict & Terrorism*, 35(9): 618–633. doi:10.1080/1057610x.2012.702669.
- Henne, P. S. (2019). Assessing the impact of the global war on terrorism on terrorism threats in Muslim countries. *Terrorism and Political Violence*, 1–19, doi:10.1080/09546553.2019.1632833.
- Himmelboim, I. ve Smith, M.A. (2017). NodeXL. *The International Encyclopedia of Communication Research Methods*, 1(3): 1–4. doi:10.1002/9781118901731.iecrm0167.
- Hobbs, C., Moran, M. ve Salisbury, D. (Ed.). (2014). *Open source intelligence in the twenty-first century: new approaches and opportunities*. Springer.
- Hoffman, B. (2006). *Inside terrorism*. Columbia University Press.
- Hoffman, B. (2009). A counterterrorism strategy for the Obama administration. *Terrorism and Political Violence*, 21(3): 359–377. doi:10.1080/09546550902950316.
- Hossain, M. S. (2015). Social media and terrorism: Threats and challenges to the modern era. *South Asian Survey*, 22(2): 136–155. doi: 10.1177/0971523117753280.
- Hughbank, R. J. ve Githens, D. (2010). Intelligence and its role in protecting against terrorism. *Journal of Strategic Security*, 3(1): 31–38. doi: 10.5038/1944-0472.3.1.3.
- Introcaso, D. M. (2005). The value of social network analysis in health care delivery. *New Directions for Evaluation*, 2005(107): 95–98. doi:10.1002/ev.164.
- Ishengoma, F. R. (2014). Online social networks and terrorism 2.0 in developing countries. *International Journal of Computer Science & Network Solution*, 1(4): 1–12.
- Ivan, A. L., Iov, C. A., Lutai, R. C. ve Grad, M. N. (2015). Social media intelligence: opportunities and limitations. *Centre for European Studies Working Papers*, 7(2a): 505–510.
- Jenkins, B. M. (1977). *Combating international terrorism: The Role of Congress*. RAND: 1.
- Jiao, Y., Yang, J. ve Xu, S. (2013). A study of the impact of social media characteristics on customer adoption intention of social media. In *International Academic Workshop on Social Science (IAW-SC-13)*: 1095–1099. doi: 10.2991/iaw-sc.2013.252.
- Johnson, L. K. (1986). Making the intelligence “Cycle” work. *International Journal of Intelligence and Counter Intelligence*, 1(4): 1–23. doi:10.1080/08850608608435033.
- Johnson, L. K. (Ed.). (2007). *Handbook of intelligence studies*. Routledge.
- Joyner, C. C. (1988). In search of an anti-terrorism policy: Lessons from the Reagan era. *Terrorism*, 11(1): 29–42. doi:10.1080/10576108808435697.
- Ju, Y., Li, Q., Liu, H., Cui, X., ve Wang, Zh. (2020). Study on application of open source intelligence from social media in the military. *Journal of Physics: Conference Series*. (1507): 1–11. doi: 10.1088/1742-6596/1507/5/052017.

- Kadushin, C. (2005). Who benefits from network analysis: Ethics of social network research. *Social Networks*, 27(2): 139-153. doi: 10.1016/j.socnet.2005.01.005.
- Kahn, D. (2008). An historical theory of intelligence. Gill, P., Marrin, S. ve Phythian, M. (Ed.). *Intelligence theory: Key questions and debates* içinde. (ss.4-15). Routledge.
- Kalpakis, G., Tsikrika, T., Gialampoukidis, I., Papadopoulos, S., Vrochidis, S. ve Kompatsiaris, I. (2018). Analysis of suspended terrorism-related content on social media. Leventakis, G. ve Habermeld, M. R. (Ed.). *Community-Oriented Policing and Technological Innovations* içinde (ss. 107-118). Springer.
- Kanat, S. , Kodaman, T. ve İren, A. A. (2016). İnsani güvenlik ve terörizmle mücadele. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 21(2): 567-588.
- Kaplan, A. M. ve Haenlein, M. (2010). Users of the World, unite! The challenges and opportunities of social media. *Business horizons*, 53(1): 59-68.
- Karaağaç, Y. (2018). *Geçmişten geleceğe istihbarat gizli servisler, örtülü operasyonlar ve savaş stratejileri*. İskenderiye Kitap.
- Karmon, E. (2002). The role of intelligence in counter-terrorism. *The Korean Journal of Defense Analysis*, 14(1): 119-139.
- Keatinge, T. ve Keen, F. (2018). Social media and (counter) terrorist finance: A fund-raising and disruption tool. *Studies in Conflict & Terrorism*, 42(1-2): 178-205 doi:10.1080/1057610X.2018.1513698.
- Kent, S. (1965). *Strategic intelligence for American world policy*. Archon Books.
- Kent, S. (2003). *Stratejik istihbarat*. Özbek, Y. B. ve Arıcı, N. (çev.). Asam Yayınları.
- Kerstetter, W. A. (1979). Terrorism and intelligence. *Terrorism*, 3(1-2): 109-115, doi:10.1080/10576107908435447.
- Khondker, H. H. (2011). Role of the new media in the Arab Spring. *Globalizations*, 8(5), 675–679. doi:10.1080/14747731.2011.621287.
- Kılınç, O. ve Arıcı, A. (2020). Sosyal ağlarda büyük veri: Teknoloji markaları üzerine bir araştırma. *Connectist: İstanbul University Journal of Communication Sciences*, 58: 201-240. doi: 10.26650/CONNECTIST2020-0082.
- Kırcı, P. ve Gülbak, E. (2020). Instagram verileri ile duygu analizi. *Avrupa Bilim ve Teknoloji Dergisi*, (Özel Sayı): 360-364. doi: 10.31590/ejosat.780129.
- Kızılkaya, Y. M. ve Oğuzlar, A. (2017). Tweetlerin etkinliğinin sosyal ağlar ile irdelenmesi. *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(2): 135-150.
- Knoke, D. ve Kuklinski, J.H. (1982). *Network analysis: Quantitative application in the Social sciences*. SAGE Publications.
- Knox, E. G. (2014). The slippery slope of material support prosecutions: Social media support to terrorists. *Hastings Law Journal*, 66(1): 295-330.
- Koschade, S. (2006). A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict & Terrorism*, 29(6): 559-575. doi: 10.1080/10576100600798418.
- Koshland, Jr, D. E. (1995). The importance of intelligence. *Science*, 267(5196): 311.

- Kozinets, R.V. (1997). I want to believe: A netnography of the X-Philes' subculture of consumption. *Advances In Consumer Research*, 24(1): 470-475.
- Kruys, G. P. (2007). *The role of intelligence in countering terrorism and insurgency*. Institute for Strategic Studies University of Pretoria. ss.83-103. Erişim tarihi: 01 Ekim 2020, [https://repository.up.ac.za/bitstream/handle/2263/5638/Kruys_Role\(2007\).pdf?sequence=1](https://repository.up.ac.za/bitstream/handle/2263/5638/Kruys_Role(2007).pdf?sequence=1).
- Küçük, M.E. ve Al, U. (2001). Metadata kavramı. *Bilgi Dünyası*, 2(2): 169-187. doi:10.15612/BD.2001.470.
- Lai, L.S. ve To, W.M. (2015). Content analysis of social media: A grounded theory approach. *Journal of Electronic Commerce Research*, 16(2): 138-152.
- Laqueur, W. (1996). Postmodern terrorism. *Foreign Affairs*, 75(5): 24-36. Erişim adresi: <https://www.jstor.org/stable/20047741>.
- Lasley, J. ve Guffey, J. (2017). A U.S. military perspective on the promise of situational crime prevention for combating terrorism. *Journal of Policing, Intelligence and Counter Terrorism*, 12(2): 85-104, doi: 10.1080/18335330.2017.1351031.
- Lazer, D., Pentland, A., Adamic, L., Aral, S., Barabasi, A.L., Brewer, D., Christakis, N., Contractor, N., Fowler, J., Gutmann, M., Jebara, T., King, G., Macy, M., Roy, D. & Van Alstyne, M. (2009). Social science. *Computational social science*, 323(5915): 721-723.
- Lewis, S. C. ve Reese, S. D. (2009). What is the war on terror? Framing through the eyes of journalists. *Journalism & Mass Communication Quarterly*, 86(1): 85-102. doi:10.1177/107769900908600106.
- Livingstone, S. (1999). New media, new audiences? *New Media & Society*, 1(1): 59-66. doi:10.1177/1461444899001001010.
- Lowenthal, M.M. (2004). Open-source intelligence: New myths, new realities. George, R.Z. ve Robert D. Kline, R.D. (Ed.). *Intelligence and the national security strategist: Enduring issues and challenges* içinde. (ss. 273-278). National Defense University Press.
- Lowenthal, M. M. (2009). *Intelligence from secrets to policy*. Fourth Edition. CQ Press.
- Luque, J., Martinez Tyson, D., Lee, J.-H., Gwede, C., Vadaparampil, S., Noel-Thomas, S. ve Meade, C. (2010). Using social network analysis to evaluate community capacity building of a regional community cancer network. *Journal of Community Psychology*, 38(5): 656-668. doi:10.1002/jcop.20386.
- Macfarlane, L. (1992). Human rights and the fight against terrorism in Northern Ireland. *Terrorism and Political Violence*, 4(1): 89-99. doi:10.1080/09546559208427139.
- Mahood, M.E.K. (2014). *Socmint: Following and liking social media intelligence*. Canadian Forces College. Erişim tarihi: 08 Kasım 2020, <https://www.cfc.forces.gc.ca/259/290/317/305/mahood.pdf>.
- Marion, L. S., Garfield, E., Hargens, L. L., Lievrouw, L. A., White, H. D. ve Wilson, C. S. (2005). Social network analysis and citation network analysis: Complementary approaches to the study of scientific communication. *Proceedings of the American Society for Information Science and Technology*, 40(1): 486-487. doi:10.1002/meet.1450400186.

- Marotta, E. (1999). Europol's role in anti-terrorism policing. *Terrorism and Political Violence*, 11(4): 15–18. doi:10.1080/09546559908427527.
- Marsden, P. V. (2011). Survey methods for network data. J. Scott ve P.J. Carrington (Ed.) *The SAGE handbook of social network analysis* içinde (ss.370–388). SAGE Publications.
- Masood, T. (2012). Pakistan's fight against terrorism. *Defence Against Terrorism Review*, 4(1): 13-30.
- Mayfield, A. (2008). *What is social media?* Erişim tarihi: 2 Kasım 2020, https://www.icrossing.com/uk/sites/default/files_uk/insight_pdf_files/What%20is%20Social%20Media_iCrossing_ebook.pdf.
- McFadden, C. (02 Temmuz 2020). *A chronological history of social media*. Erişim tarihi: 11 Nisan 2021. <https://interestingengineering.com/a-chronological-history-of-social-media>.
- 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*, 3(2): 5-25.
- Milgram, S. (1967). The small world problem. *Psychology Today*, 2(1): 60-67.
- Miller, G. D. (2007). Confronting terrorisms: Group motivation and successful state policies. *Terrorism and Political Violence*, 19(3): 331-350.
- Minchev, Z. (2015). Modern terrorism as hybrid threat and digital challenge. *J Def Manag* 5 (129): 1-2 doi:10.4172/2167-0374.1000129
- Moreno, J. L. (1934). *Who shall survive?: A new approach to the problem of human interrelations*. Nervous And Mental Disease Publishing Co.
- Morris, D.R. (2009). Surprise and terrorism: A conceptual framework. *Journal of Strategic Studies*, 32(1): 1-27. doi:10.1080/01402390802407392.
- Mullins, S. (2013). Social network analysis and terrorism: an introduction to the special issue. *Behavioral Sciences of Terrorism and Political Aggression*, 5(2): 67-69, doi:10.1080/19434472.2012.731697.
- Murphy, J.F. (1990). The need for international cooperation in combating terrorism, *Terrorism*, 13(6): 381-396, doi: 10.1080/10576109008435847.
- Nair, M. (2011). Understanding and measuring the value of social media. *Journal of Corporate Accounting & Finance*, 22(3), 45–51. doi:10.1002/jcaf.20674.
- Newsome, B. (2006). Expatriate games: Interorganizational coordination and international counterterrorism. *Coastal Management*, 29(1): 75-89.
- O'Brien, W.V. (1985). Counterterrorism: Lessons from Israel. *Strategic Review* 13(4): 32–44.
- Oh, O., Agrawal, M. ve Rao, H. R. (2011). Information control and terrorism: Tracking the Mumbai terrorist attack through twitter. *Information Systems Frontiers*, 13(1): 33-43.
- Omand, D., Bartlett, J. ve Miller, C. (2012a). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, 27(6): 801-823. doi: 10.1080/02684527.2012.716965.
- Omand, D., Bartlett, J. ve Miller, C. (2012b). *#Intelligence*. Demos Yayınları.

- Omand, D. (2013). Is it time to move beyond the Intelligence Cycle? A UK practitioner perspective. Phythian, M. (Ed.) *Understanding the intelligence cycle* içinde (ss.136-149). Routledge.
- Omand, D., Miller, C. ve 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* içinde (ss.24-43). Springer.
- Omand, D. (2017). Social media intelligence (SOCMINT). Dover, R., Dylan, H. ve Goodman, M.S. (Ed). *The Palgrave handbook of security, risk and intelligence* içinde (ss. 355-371). Palgrave Macmillan Yayınları.
- Omelicheva, M.Y. (2007). Combating terrorism in Central Asia: Explaining differences in states' responses to terror. *Terrorism and Political Violence*, 19(3): 369-393, doi: 10.1080/09546550701424075.
- O'reilly, T. (2007). What is web 2.0: Design patterns and business models for the next generation of software. *Communications & Strategies*, (1): 17-37.
- Özbölük, T. ve Dursun, Y. (2015). Pazarlama araştırmalarında paradigmal dönüşüm ve etnografinin dijital evrimi: Netnografi. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (46): 227-247.
- Özcan, N.A. (19 Şubat 2016). *Terörle mücadele ve istihbarat*. Erişim tarihi: 06 Ekim 2020. <https://www.milliyet.com.tr/yazarlar/nihat-ali-ozcan/terorle-mucadele-ve-istihbarat-2196597>.
- Özdağ, Ü. (2018). *İstihbarat teorisi*. Kripto Yayınları.
- Özkaya, E. (2017). The use of social media for terrorism. *NATO Defence Against Terrorism Review*, 9: 47-59.
- Öztürk, Z.A. (14 Ekim 2020). *GB, TB, PB... ne kadar veri taşıyabiliyor?* Erişim tarihi: 01 Aralık 2020, https://www.chip.com.tr/haber/gb-tb-pb-ne-kadar-veri-tasiyabiliyor_35472.html.
- Pastor-Galindo, J., Nespole, P., Mármol, F. G. ve Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *Emerging Approaches to Cyber Security*, 10282-10304. doi: 10.1109/ACCESS.2020.2965257.
- Pedahzur, A., Eubank, W. ve Weinberg, L. (2002). The war on terrorism and the decline of terrorist group formation: A research note. *Terrorism and Political Violence*, 14(3): 141–147. doi:10.1080/714005625.
- Pelzer, R. (2018). Policing of terrorism using data from social media. *European Journal for Security Research*, 3(2): 163-179.
- Phillips, D. ve Young, P. (2009). *Online public relations: A practical guide to developing an online strategy in the world of social media*. Kogan Page Publishers.
- Pillar, P.R. (2001). *Terrorism and US foreign policy*. Brookings Institution Press.
- Pillar, P.R. (2004). Intelligence. Cronin, A. K. ve Ludes, J. M. (Ed.) *Attacking terrorism: Elements of a grand strategy* içinde. (ss.115-139). Georgetown University Press.

- Pollard, N. (2009). On counterterrorism and intelligence. G. Treverton & W. Agrell (Ed.), *National Intelligence Systems: Current Research and Future Prospects* içinde (ss. 117-146). Cambridge University Press. doi:10.1017/CBO9781139174541.007.
- Porta, D. D. (1992). Institutional responses to terrorism: The Italian case. *Terrorism and Political Violence*, 4(4): 151–170. doi:10.1080/09546559208427179.
- Reese, S.D. ve Lewis, S.C. (2009). Framing the war on terror: The internalization of policy in the US press. *Journalism*, 10(6): 777-797.
- Reinares, F. (2009). After the Madrid bombings: Internal security reforms and prevention of global terrorism in Spain. *Studies in Conflict & Terrorism*, 32(5): 367-388, doi: 10.1080/10576100902836767.
- Ressler, S. (2006). Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs*, 2(2): 1-10.
- Richardson, L. (2006). *What terrorists want: Understanding the enemy, containing the threat*. Random House.
- Robertson, K. G. (1987). Intelligence, terrorism and civil liberties. *Journal of Conflict Studies*, 7(2): 43-62.
- Rodewig, C. (8 Mart 2012). *Geotagging poses security risks*. Erişim tarihi: 27 Kasım 2020, https://www.army.mil/article/75165/geotagging_poses_security_risks.
- Romanov, V.A. (1990). The United Nations and the problem of combatting international terrorism. *Terrorism and Political Violence*, 2(3): 289-304, doi:10.1080/09546559008427067.
- Saiya, N. (2020). Confronting apocalyptic terrorism: Lessons from France and Japan. *Studies in Conflict & Terrorism*, 43(9): 775-795. doi: 10.1080/1057610X.2018.1499694.
- Sampson, F. (2016). Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings. *The Police Journal*, 90(1): 1-15. doi: 10.1177/0032258X16671031.
- Sancak, K. (2019). Uluslararası terörle mücadelede yumuşak güç ve kamu diplomasisi bağlamında medyanın önemi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 33(1): 359-372.
- Sandler, T. (2011). The many faces of counterterrorism: an introduction. *Public Choice*, 149(3-4): 225–234. doi:10.1007/s11127-011-9883-y.
- Saraçoğlu, M. Y. (2016). NATO'nun bariyerleri: Terörizmle mücadelede yaşanan dönüşüm ve ittifakın etkinliğini azaltan faktörler. *Güvenlik Bilimleri Dergisi*, 5(1): 75-108.
- Saran, U. (02 Mayıs 2016). *Terörle mücadele mi teröristle mücadele mi?* <http://www.aljazeera.com.tr/gorus/terorle-mucadele-mi-teroristle-mucadele-mi>.
- Schmid, A.P. (2004). Prevention of terrorism: towards a multi-pronged approach. Bjørge, T. (Ed.). *Root causes of terrorism: Myths, reality and ways forward* içinde (ss.223-240). Routledge.
- Schmid, A. P. (Ed.). (2011). *The Routledge handbook of terrorism research*. Taylor & Francis.

- Schoder, D., Gloor, P. A., & Metaxas, P. T. (2013). Social media and collective intelligence - ongoing and future research streams. *KI-Künstliche Intelligenz*, 27(1): 9-15. doi: 10.1007/s13218-012-0228-x.
- Schwartz, D. M. ve Rouselle, T. D. A. (2008). Using social network analysis to target criminal networks. *Trends in Organized Crime*, 12(2): 188-207. doi:10.1007/s12117-008-9046-9.
- 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*. John Wiley & Sons.
- Scott, J. (2011). Social network analysis: Developments, advances, and prospects. *Social Network Analysis And Mining*, 1(1): 21-26. doi:10.1007/s13278-010-0012-6.
- Sederberg, P. C. (1995). Conciliation as counter-terrorist strategy. *Journal of Peace Research*, 32(3): 295-312.
- Seker, S. E. (2015). Çizge teorisi (graph theory). *Yönetim Bilişim Sistemleri Ansiklopedisi*, 2(2): 17-29.
- Sert Eteman, F., Tüzüntürk, S. ve Gürsakal, N. (2014). NodeXL ile sosyal ağ analizi: #akademikzam örneği. *Ekonometri, Yöneylem Araştırması ve İstatistik Sempozyumu*, (15): 1-21.
- Shah, D. V., Cappella, J. N., ve Neuman, W. R. (2015). Big data, digital media, and computational social science. *The ANNALS of the American Academy of Political and Social Science*, 659(1), 6-13. doi:10.1177/0002716215572084.
- Shulsky, A.N. ve Schmitt, G.J. (2002). *Silent warfare: Understanding the world of intelligence*. Potomac Books.
- Shultz, R. (1978). Conceptualizing political terrorism: A typology. *Journal of International Affairs*, 32(1). 7-15.
- Sims, J. (2009). Defending adaptive realism. Intelligence theory comes of age. Gill, P., Marrin, S., ve Phythian, M. (Ed.). *Intelligence Theory: Key questions and debates* içinde (ss.151- 165). Routledge.
- Sinclair, G. (2014). Confronting terrorism: British experiences past and present. *Crime, History & Societies*, 18(2): 117-122.
- Singer, P. W. ve Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan Books.
- Smith, M. ve Dingley, J. (2009) Countering terrorism in Northern Ireland: The role of intelligence. *Small Wars & Insurgencies*. 20(3-4): 551-573, doi:10.1080/09592310903027132.
- Sparrow, M.K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social networks*, 13(3): 251-274.
- Steele, R.D. (2007). Open source intelligence. Johnson, L.K. (Ed.) *Handbook of Intelligence Studies* içinde ss.130-147. Routledge.
- Steve, S. (2000). An overview of content analysis. *Practical Assessment, Research, and Evaluation*, 7, Article 17: 1-6. doi:10.7275/z6fm-2e34.
- Strang, S. J. (2014). Network analysis in criminal intelligence. Masys, A.J. (Ed.) *Networks and network analysis for defence and security* içinde (ss.1-26) Springer.

- Strom, K. J. ve Eyerman, J. (2007). Interagency coordination in response to terrorism: Promising practices and barriers identified in four countries. *Criminal Justice Studies*, 20(2): 131–147. doi:10.1080/14786010701396871.
- Sulc, L. (1987). Terrorism and the importance of intelligence. *Terrorism*, 10(2): 133-138, doi:10.1080/10576108708435655.
- Šubelj, L., Furlan, Š., & Bajec, M. (2011). An expert system for detecting automobile insurance fraud using social network analysis. *Expert Systems with Applications*, 38(1): 1039–1052. doi:10.1016/j.eswa.2010.07.143.
- Süperhaber. (13 Şubat 2019). *TSK'dan Kıbrıs'a tank sevkiyatı iddiası*. Erişim tarihi: 24 Kasım 2020, <https://www.superhaber.tv/tskdan-kibrisa-leopard-2a4-tank-sevkiyatı-haber-174824>.
- Şuşnea, E. ve Iftene, A. (2018). The significance of online monitoring activities for the social media intelligence (SOCMINT). *Proceedings of the Conference on Mathematical Foundations of Informatics MFOI'2018*. 230-240.
- Taprial, V. ve Kanwar, P. (2012). Understanding social media. Bookboon.
- Taylor, A. (24 Kasım 2014). *How Western foreign fighters are being recruited online to join Kurds against Islamic State*. Erişim tarihi: 25 Aralık 2020, <https://www.washingtonpost.com/news/worldviews/wp/2014/11/24/how-western-foreign-fighters-are-being-recruited-online-to-join-kurds-against-islamic-state/>.
- Ter Wal, A. L. J. ve Boschma, R. A. (2008). Applying social network analysis in economic geography: framing some key analytic issues. *The Annals of Regional Science*, 43(3): 739–756. doi:10.1007/s00168-008-0258-3.
- The Camstoll Group. (2016). *Use of social media by terrorist fundraisers & financiers*. Erişim tarihi: 15 Kasım 2020, <https://www.camstoll.com/wp-content/uploads/2016/04/Social-Media-Report-4.22.16.pdf>.
- Thompson, E. (2019). *US citizenship and immigration services' effort to identify terrorism threats: Is social media intelligence (SOCMINT) the next tool?* Doctoral dissertation. Monterey, CA; Naval Postgraduate School.
- Thornton, T.P. (1964). Terror as a weapon of political agitation. Eckstein, H. (Ed.), *Internal war: problems and approaches* içinde. (ss.71-99). The Free Press.
- Treverton, G.F. (2008). Intelligence analysis: Between politicization and irrelevance. Roger Z. George and James B. Bruce (Ed.) *Analyzing Intelligence: Origins, Obstacles, and Innovations* içinde (ss. 91- 104). Georgetown University Press.
- Treverton, G.F. ve Miles, R. (2014). *Social media and intelligence*. Elanders Sverige AB.
- Trinquier, R. (2006). *Modern warfare: A French view of counterinsurgency*. Greenwood Publishing Group.
- Tripathy, B.K., Sooraj, T.R. ve Mohanty, R.K. (2018). Big data techniques in social network analysis. Panda, M., Abraham, A. ve Hassanien, A.E. (Ed.). *Big data analytics: A social network approach* içinde. (ss.47-67). CRC Press.
- Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies*, 18(4-5): 530-547. doi: 10.1177/1367549415577396.
- Tunalı, V. (2016). *Sosyal ağ analizine giriş*. Nobel Yayıncılık.

- Tunalı, V. ve Güvenoğlu, E. (2019). Complex network analysis approach to examining undergraduate program preferences. *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, 8(1), 176-186.
- Twitter. (2020). *Twitter'in API'leri hakkında*. Erişim tarihi: 30 Kasım 2020, <https://help.twitter.com/tr/rules-and-policies/twitter-api>.
- Tylutki, K. (2018). The information of a mass destruction range-OSINT in intelligence activities. *Internal Security Review*. 10(19): 384-404.
- UK Ministry of Defence. (2011). *Understanding and intelligence support to joint operations*. Joint Doctrine Publication 2, 3rd Edition.
- US Army Headquarters. (2006). *FM 2-22.3. Human intelligence collector operations*.
- US Army Headquarters. (2019). *ADP 2.0. Intelligence*. Army Publications.
- US Army Joint Chiefs of Staff. (1998). *JP 3-07.2 Joint Tactics, Techniques and Procedures for Antiterrorism*. Army Publications.
- US Army Joint Chiefs of Staff. (2014). *JP 3-07-2 Antiterrorism*. Army Publications.
- Van Duijn, M. A. ve Vermunt, J. K. (2006). What is special about social network analysis. *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences*, 2(1): 2- 6. doi: 10.1027/1614-1881.2.1.2.
- Wagner, A. (2007). Intelligence for counter-terrorism: Technology and methods. *Journal of Policing, Intelligence and Counter Terrorism*, 2(2): 48-61, doi: 10.1080/18335300.2007.9686897.
- Walker, C. (2009). Legal aspects of counter-terrorism & Intelligence in the prevention of terrorism. Fernández Sánchez, P.A. (Ed.) *International Legal Dimension of Terrorism* içinde (ss.149-172). Martinus Nijhoff Publishers.
- Walter, E.V. (1964). Violence and the process of terror. *American Sociological Review*, 29(2), Spring 1964: 248-257.
- Wang, J.C. ve Chiu, C.C. (2008). Recommending trusted online auction sellers using social network analysis. *Expert Systems with Applications*, 34(3), 1666–1679. doi:10.1016/j.eswa.2007.01.045.
- Wardlaw, G. (1989). *Political terrorism: Theory, tactics and counter-measures*. Cambridge University Press.
- Warner, M. (2002). Wanted: A definition of intelligence. *Studies in Intelligence*, 46,(3).
- Warren, M. ve Leitch, S. (2016). The Syrian electronic army – a hacktivist group. *Journal of Information, Communication and Ethics in Society*, 14(2): 200–212. doi:10.1108/jices-12-2015-0042.
- Waskiewicz, T. ve LaMonica, P. (2008). Developing an intelligence analysis process through social network analysis. Blowers, M. ve Sisti, A.F. (Ed.). *Evolutionary and Bio-Inspired Computation: Theory and Applications II* içinde, (ss.1-7). Society of Photo Optical.
- Waskiewicz, T. (2012). *Friend of a friend influence in terrorist social networks*. In *Proceedings on the International Conference on Artificial Intelligence*. Erişim tarihi: 14 Kasım 2020, <https://www.semanticscholar.org/paper/Friend-of-a-Friend-Influence-in-Terrorist-Social-Waskiewicz/d7c798764c632e33675ef3b18594b08e40f94393>.

- Wasserman, S. ve Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge university press.
- We Are Social. (2020). *Digital around the World in April 2020*. Erişim Tarihi: 03 Kasım 2020, <https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020>.
- Weil, A. (2017). The Red Army Faction: Understanding measured government response to an adaptive terrorist threat. *Cornell International Affairs Review*, Vol X: 129-159.
- Weimann, G. (2004). *How modern terrorism uses the internet*. Special Report 116. Erişim tarihi: 05 Kasım 2020, <https://www.usip.org/sites/default/files/sr116.pdf>.
- Weimann, G. (2010). Terror on Facebook, Twitter and Youtube. *The Brown Journal of World Affairs*, Vol. 16, No. 2. ss.45-54.
- Weimann, G. (2014). *New terrorism and new media*. Commons Lab of the Woodrow Wilson International Center for Scholars: 1-20.
- Weinberg, T. (2009). *The new community rules: Marketing on the social web*. O'Reilly Yayınları.
- Welch, C. (2013). *AP Twitter account hacked, makes false claim of explosions at White House*. Erişim tarihi: 05 Kasım 2020, <https://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured>.
- Wilcox, P.C. (1997). The western alliance and the challenge of combating terrorism. *Terrorism and Political Violence*, 9(4): 1-7, doi: 10.1080/0954659708427427.
- Wilkinson, P. (1979). *Terrorism and the liberal state*. New York University Press.
- Wilkinson, P. (1993). Aviation security the fight against terrorism. *Interdisciplinary Science Reviews*, 18(2): 163–173. doi:10.1179/isr.1993.18.2.163.
- Wilkinson, P. (1996). The role of the military in combatting terrorism in a democratic society. *Terrorism and Political Violence*, 8(3): 1-11, doi: 10.1080/09546559608427360.
- Wilkinson, P. (2000). The strategic implications of terrorism. M.L. Sondhi (Ed.) *Terrorism & Political Violence. A Sourcebook* içinde (ss.19-49). Har-Anand Publications.
- Wilkinson, P. (2006). *Terrorism versus democracy: The liberal state response. 2'nd edition*. Taylor & Francis.
- Wilkinson, P. (2011). *Terrorism versus democracy: The liberal state response. 3'rd edition*. Taylor & Francis.
- Winkler, T. H., Ebnöther, A. H. ve Hansson, M. B. (Ed.). (2005). *Combating terrorism and its implications for the security sector*. Elanders Gotab.
- Wirtz, J.J. (2008). Theory of Surprise. Gill, P., Marrin, S. ve Phythian, M. (Ed.). *Intelligence theory: Key questions and debates* içinde. (ss.73-86). Routledge.
- Wu, P. (2015). Impossible to regulate: Social media, terrorists, and the role for the UN. *Chicago Journal of International Law*, 16,1. ss.281-311.
- Yalçinkaya, H., Özyer, T. ve Çelik, B. (2016). Türkçe konuşan DEAŞ destekçileri üzerine Twitter sosyal ağ analizi. *ORSAM Rapor*. No: 205.
- Yılmaz, S. (2011). *Terör ve Türkiye*. Kum Saati Yayınları.

- Zeng, D., Chen, H., Lusch, R. ve Li, S.H. (2010). Social media analytics and intelligence. *IEEE Intelligent Systems*, 25(6): 13–16. doi:10.1109/mis.2010.151.
- Zgryziewicz, R. (2016). *DAESH recruitment how the group attracts supporters*. NATO Strategic Communications Centre of Excellence. Eriřim tarihi: 12 Kasım 2020, <https://www.stratcomcoe.org/daesh-recruitment-how-group-attracts-supporters-0>.



EKLER

EK-1 SOSYAL AĞ ANALİZİNDE KULLANILAN ÖLÇÜTLER

S.No.	Ölçüt	Açıklama
1.	Düğüm sayısı	Ağdaki varlıkların sayısını göstermektedir.
2.	Bağlantı ya da kenar sayısı	Düğümlerin aralarındaki bağlantıların sayısını göstermektedir.
3.	Yoğunluk	Ağda mevcut kenar sayısının, en fazla olası kenar sayısına oranıdır. Yoğunluk, bir ağın ortalama gücüdür.
4.	Merkezlilik (<i>centrality</i>)	Bir ağda yer alan düğüm ve bağlantıların önem derecesini ortaya koymaya çalışan göstergedir.
5.	İç derece merkeziliği (<i>in-degree centrality</i>)	Bir ağ içerisinde en çok etkileşimi alan düğümü öne çıkaran algoritmadır.
6.	Dış derece merkeziliği (<i>out-degree centrality</i>)	Diğer düğümlerle en çok ilişki kuran düğümü ön plana çıkarmaktadır.
7.	Arasındalık merkeziliği (<i>betweenness centrality</i>)	Ağ içerisindeki ilişkilerin en ortasında yer alan düğümü göstermektedir.
8.	Özvektör merkeziliği (<i>eigenvector centrality</i>)	Ağ içerisinde en çok etki sahibi olan, sosyal ağdaki kanaat önderlerini tespit etmek için en önemli düğümü öne çıkartan göstergedir. Özvektör merkeziliği yönsüz ağlar için kullanılan ölçüttür.
9.	Sayfa değeri (<i>PageRank</i>)	Özvektör merkeziliği ile aynı özelliklere sahip ölçüt olup yönlü ağlar için kullanılan ölçüttür.
10.	Yakınlık merkeziliği (<i>closeness centrality</i>)	Düğüm arasındaki ortalama mesafeyi ve bir düğüm ile diğer düğümler arasındaki ortalama mesafeyi ölçmektedir.
11.	Jeodezik mesafe	Ağda bulunan iki kişi arasındaki en kısa yolun uzunluğudur.
12.	Maksimum jeodezik mesafe (<i>ağın çapı</i>)	Birbirinden en uzak iki düğüm arasındaki mesafeyi göstermektedir.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : BURAL, Erol Başaran
 Uyruğu : Türkiye Cumhuriyeti
 Doğum Tarihi ve Yeri :
 Medeni Hali :
 Telefon :
 Faks :
 E-posta :

Eğitim Derecesi	Okul/Program	Mezuniyet yılı
Yüksek lisans	Jandarma ve Sahil Güvenlik Akademisi	2021
Yüksek lisans	Gazi Üniversitesi	2003
Lisans	Kara Harp Okulu	1992
Lise	Kuleli Askeri Lisesi	1988
İş Deneyimi, Yıl	Çalıştığı Yer	Görev
24	Kara Kuvvetleri Komutanlığı	Emekli

Yabancı Diller

İngilizce

Yayınlar

1. Bural, E.B. (2021). *Amerika Birleşik Devletlerinde “Beyazların Üstünlüğü” Hareketleri: Nükleer Silah Tümeni Örnek Olay İncelemesi*. Güvenlik Bilimleri Dergisi, 10(1). doi: 10.28956/gbd.843025.
2. Bural, E.B. (2020). Yeni Nesil Terörizm Paradigması. Imıl, M. (Ed.) *Yeni Nesil Terörizm* içinde (ss.11-34). Nobel Yayınevi.
3. Bural, E.B. (2019). Terör Örgütleri ve Propaganda. Imıl, M. (Ed.) *Propaganda ve Algı Yönetimi* içinde (ss. 53-120). Orion Yayınevi.

Hobiler



JSGA'lı, Her Zaman Yurt, Ulus ve Cumhuriyete Aşk
ve Sadakatle Bağlı Tevazu, Fedakârlık ve Feragat
Örneğidir