T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANA BİLİM DALI
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER YÜKSEK LİSANS PROGRAMI

Açık Kaynak İstihbarati Bağlamında Yeni Bir Veri Kaynağı Olarak Sosyal Medya

Yüksek Lisans Tezi

Ahmet Emin CERRAH
100022612

İstanbul, 2022

T.C.

İSTANBUL TİCARET ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANA BİLİM DALI

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER YÜKSEK LİSANS PROGRAMI

Açık Kaynak İstihbarati Bağlamında Yeni Bir Veri Kaynağı Olarak Sosyal Medya

Yüksek Lisans Tezi

Ahmet Emin CERRAH

100022612

Tez Danışmanı: Prof. Dr. Oya DAĞLAR MACAR

İstanbul, 2022

ETİK BEYAN

Hazırlamış olduğum tez özgün bir çalışma olup YÖK ve İstanbul Ticaret Üniversitesi Lisansüstü Yönetmelikleri'ne uygun olarak hazırlanmıştır. Ayrıca, bu çalışmayı yaparken bilimsel etik kurallarına tamamıyla uyduğumu; yararlandığım tüm kaynakları gösterdiğimi ve hiçbir kaynaktan yaptığım ayrıntılı alıntı olmadığını beyan ederim. Turnitin intihal programından alınan rapora göre tezimin benzerlik oranı %13'tür. Bu tezin ihtiva ettiği tüm hususlar şahsi görüşüm olup İstanbul Ticaret Üniversitesi'nin resmi görüşünü yansıtmamaktadır.

Ahmet Emin CERRAH

Özet

Sosyal medya kullanımının ciddi düzeyde artışı ile meydana gelen veri potansiyeli, yeni bir istihbarat disiplini olarak sosyal medya istihbaratını (SOCMINT) ortaya çıkarmıştır. Sosyal medya platformlarından ihtiyaçlar doğrultusunda anlık veya sistematik şekilde veri toplanarak, toplanan bu verilerin kullanımını öngören SOCMINT'in, kitlelerin duygusal analizini yapmak, suç motivasyonunu öğrenmek ve önleyici faaliyetlerde bulunmak gibi faydaları bulunmaktadır.

Geleneksel yöntemlerin sosyal medya istihbaratındaki aşamalara uyum sağlama kabiliyeti yetersiz kaldığı için bu disiplinde, makine öğrenmesi ve yapay zeka gibi araçlar kullanılmaktadır. SOCMINT'in sunmuş olduğu avantajlar kadar veri kirliliği, sosyal medya jargonunun tanımlanması, algı yönetimi, oto-sansür tepkisi, verilerin doğrulanması ve nitelikli personel ihtiyacı gibi geliştirilmesi veya çözümlenmesi gereken dezavantajları da bulunmaktadır.

Bu bağlamda hazırlanan bu çalışma; kullanıcıların, özel şirketlerin, STK'lerin, terör örgütlerinin, organize suç örgütleri ve uyuşturucu kartellerinin kendi amaç ve çıkarları doğrultusunda kullanmakta olduğu sosyal medya platformlarının, istihbarat birimleri aracılığıyla devletler tarafından da ihtiyaçlar doğrultusunda kullanılabileceğini analiz etmektedir. Sosyal medyanın kavramsal çerçevesinin, dünya genelinde ve Türkiye özelinde kullanımının, olumlu ve olumsuz taraflarının, SOCMINT sürecinin işleyişinin ve bu disiplinin faydalarının nitel araştırma yöntemlerinden kaynak taramasıyla ele alan çalışmanın sonucunda; gerekli teknik imkânlar, nitelikli personeller ve diğer istihbarat disiplinleriyle eş güdümlü yönetilen faaliyetler ile sosyal medya üzerinden toplanacak verilerin istihbarat sürecinde etkili bir biçimde kullanılabileceği tespit edilmiştir.

Anahtar Kelimeler: *İstihbarat, Açık Kaynak İstihbaratı, Sosyal Medya, SOCMINT*

Abstract

The immense potential of data, which stems from the dramatic increase in the use of social media, has created social media intelligence (SOCMINT) as a new type of discipline in the field of intelligence. SOCMINT has certain benefits, such as analyzing emotions of the masses, or learning and preventing motivations behind criminal activities by collecting data from social media platforms momentarily or systematically in parallel with the requirements.

Since the capability of traditional methods to adapt to the social media intelligence processes is insufficient, this discipline makes use of tools such as machine learning and AI. However, SOCMINT also has certain disadvantages, which require to be improved or settled, such as data pollution, detecting social media slang, perception management, reactions to self-censorship, verification of data and the need for qualified staff.

In this regard, this research paper argues that social media platforms are not only benefited by common users, private companies, NGOs, terrorist groups, organized crime groups or drug cartels, but also by governments through intelligence units in parallel with their requirements. As a result of this research, which examines the conceptual framework of social media, its use across the globe and in Turkey, its advantages and disadvantages, how the SOCMINT process works and the advantages of this discipline by using qualitative research methods and literature review, it is concluded that data gathered from social media in conjunction with certain technical means, qualified staff and operations carried out in coordination with other intelligence disciplines can be used effectively during the intelligence process.

Key Words: *Intelligence, Open-Source Intelligence, Social Media, SOCMINT*

TEŞEKKÜR

Yüksek lisans eğitimi ve tez yazım sürecimde her türlü destekte bulunup tez çalışmamda vermiş olduğu destek ve katkılarından ötürü danışman hocam Prof. Dr. Oya DAĞLAR MACAR'a şükranlarımı sunuyorum. Bu süreçte gerek maddi gerek ise manevi desteklerini benden esirgemeyen, haklarını asla ödeyemeyeceğim annem ile babama da sevgi ve saygılarımı iletiyorum.

Ahmet Emin CERRAH

Eylül-2022

İÇİNDEKİLER

TABLO LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

ACOUSTINT: Akustik İstihbarat (Acoustic Intelligence)

AİHM: Avrupa İnsan Hakları Mahkemesi

ARPANET: Gelişmiş Araştırma Projeleri Dairesi Ağı (Advanced Research Projects Agency Network)

CSE: Kanada İletişim Güvenliği Kurumu (Communications Security Establishment)

GCHQ: İngiliz İletişim Merkezi (Government Communications Headquarters)

GCSB: Yeni Zelanda Haberleşme Güvenlik Bürosu (Government Communications Security Bureau)

DARPA: Gelişmiş Savunma Araştırma Projeleri Ajansı (Defence Advanced Research Projects Agency)

DAEŞ: Irak-Şam İslam Devleti

DNI: Milli İstihbarat Müdürü (Director of National Intelligence)

DOT: ABD Ulaştırma Bakanlığı (Department of Transportation)

DSD: Avustralya Savunma Sinyalleri Direktörlüğü (Defence Signals Directorate)

DTO: Uyuşturucu Kaçakçılığı Örgütleri (Drug Trafficking Organizations)

FTP: Dosya Aktarım Kuralı (File Transfer Protocol)

GEOINT: Coğrafi İstihbarat (Geographic Intelligence)

HMIC: Her Majesty's Inspectorate of Constabulary

HUMINT: İnsani İstihbarat (Human Intelligence)

IMINT: Görüntü İstihbaratı (Imagery Intelligence)

İHA: İnsansız Hava Aracı

JIPOE: Joint Intelligence Preparation of the Operational Environment

KVKK: Kişisel Verilerin Korunması Kanunu

MI6: İngiliz Dış İstihbarat Servisi (The Secret Intelligence Service)

MİT: Millî İstihbarat Teşkilâtı

MRE: Yenilebilir Yemek (Meal Ready to Eat)

NATO: Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization)

NSA: Ulusal Güvenlik Ajansı (National Security Agency))

NUCINT: Nükleer İstihbarat (Nuclear Intelligence)

OSINT: Açık Kaynak İstihbaratı (Open Source Intelligence)

PKK: Kürdistan İşçi Partisi (Partîya Karkerên Kurdistanê)

RADINT: Radar İstihbaratı (Radar Intelligence)

RTÜK: Radyo ve Televizyon Üst Kurulu

SIGINT: Sinyal İstihbaratı (Signal Intelligence)

SİHA: Silahlı İnsansız Hava Aracı

SOCINT: Sosyo-kültürel İstihbarat (Sociocultural Intelligence)

SOCMINT: Sosyal Medya İstihbaratı (Social Media Intelligence)

TCO: Uluslararası Suç Örgütü (Transnational Criminal Organization)

TDK: Türk Dil Kurumu

TSA: ABD Ulaştırma Güvenlik İdaresi (Transportation Security Administration)

TT: Twitter Trendleri (Trend Topic)

VPN: Sanal Özel Ağ (Virtual Private Network)

WHO: Dünya Sağlık Örgütü (World Health Organization)

WWW: World Wide Web

YPG: Halk Koruma Birlikleri (Yekîneyên Parastina Gel)

GİRİŞ

İnsanların, tarihin her döneminde farklı amaçlar doğrultusunda ve farklı rakiplere karşı strateji ihtiyacı bulunmuştur. İlk Çağlarda avcılık ile hayatta kalan toplulukların, hayvanların izlerini takip ederek gerçekleştirdiği faaliyetler, kabaca istihbaratın ilk kullanımı olarak nitelendirilmektedir. İnsanlar, başarılı sonuçlar elde edebilmek için oluşturacakları stratejileri ise bilginin kazandırmış olduğu avantajlar ile şekillendirmiştir. Bu çerçevede 21. yüzyıla kadarki süreçte istihbarat genel olarak askerî alana hizmet etmiştir. "Düşman ordusu nerede konuşlandı? Ne kadar mühimmatları var? Asker sayıları kaç? İkmal birlikleri için coğrafi konum ne kadar müsait?" gibi sorulara cevap veren istihbarat faaliyetleri, günümüzde çok daha geniş yelpazede bilgi toplamayı amaçlamaktadır.

Bu süreç içerisinde, istihbarat birimleri teknolojik gelişmeleri yakından takip ederek faaliyetlerine uygun şekilde entegre etmiştir. Ateşin icat edilmesi ile dumanla haberleşme, yazının icat edilmesi ile kriptografi, kervansaray ve limanların casuslar tarafından bilgi toplamak için kullanılması, haberleşme ve posta ağları, bilginin hızlı iletilmesi için gizli yollar, tarihteki belli başlı örneklerden birkaçıdır. Her ne kadar sabır ve gizlilik gerektiren bir süreç olsa da önleyici faaliyet niteliğinden dolayı istihbaratta bilginin hızlı şekilde gerekli yerlere ulaşması önemli bir ihtiyaç olmuştur. Özellikle XVIII. yüzyılda başlayan Endüstri Devrimi'nin etkileri istihbarat faaliyetlerine de yansımıştır.

Teknolojik gelişmeler ile geleneksel istihbarat toplama yöntemi olan insani istihbarat dışında da yeni yöntemler ortaya çıkmıştır. Bu bağlamda birçok farklı aracı veri toplamak için kullanan istihbarat birimlerinin açık kaynaklardan yararlanması da yeni bir yöntem değildir. Yararlanılan ulusal ve yerel gazeteler, dergiler, arşivler, katalog ve broşürler, radyo ve televizyon yayınları gibi açık kaynaklara ek olarak günümüzde internet ve sosyal medya platformları da OSINT (open source intelligence) faaliyetlerinde kullanılmaktadır.

Teknolojik gelişmeleri faaliyetlerine entegre ederek veri toplama yöntemlerini çeşitlendiren istihbarat birimleri, sunmuş olduğu muazzam veri kapasitesi ve hızlı bilgi akışı sebebiyle internet ve sosyal medyayı da etkin bir biçimde kullanmaya başlamıştır.

Bu bağlamda hazırlanan tez çalışmasının temel amacı, açık kaynak istihbaratı kapsamında sosyal medyanın veri kaynağı olarak kullanımının incelenmesidir.

Çalışmada, açık kaynak sosyal medya verilerinin istihbarat sürecine tabi tutularak, diğer istihbarat disiplinleriyle eş güdümlü bir biçimde kullanımının mümkün olduğu hipotezi test edilmiştir. Bunun yanı sıra hipotezin test edilmesinde şu sorulara da cevap aranmıştır:

- Sosyal medyada kolektif bir bilinç oluşturulabilir mi?
- Kullanıcıların veri güvenliği devletler için ulusal tehdit niteliği taşımakta mıdır?
- SOCMINT tek başına istihbarat faaliyeti yürütebilecek kapasitede midir?

Bu bağlamda hazırlanan tez çalışmasında nitel araştırma yöntemlerinden kaynak tarama yöntemi kullanılmıştır. Çalışmanın verileri çevrimiçi kütüphanelerden, akademik veri tabanlarından, medya kuruluşlarının resmî internet arşivlerinden, çevrimiçi devlet arşivlerinden, resmî kurumların yayınlamış olduğu raporlardan, akademik çalışmalardan, kitap, makale ve dergilerden birincil ve ikincil kaynak kullanımına özen gösterilerek toplanmıştır.

Nitelikli bir girizgâh oluşturmak ve istihbaratın, güvenlik ve strateji kavramlarının her ikisini de bünyesinde barındırması nedeniyle ilk bölümde bu iki kavram detaylı bir şekilde ele alınmıştır. Çalışmanın alanyazın kısmı olan ikinci bölüme, istihbarat kavramı açıklanarak başlanmıştır. Yabancı literatürlerde birçok önemli çalışma ve kaynak bulunmasına karşılık diğer disiplinler kadar bilimsel çalışması bulunmayan istihbarat alanının teorik gelişimi yine bu bölümde kısaca ele alınmıştır. Ana konusu açık kaynak istihbarat ve SOCMINT (social media intelligence) olan çalışmanın omurgasını oluşturma amacıyla istihbarat sürecinin nasıl işlediği, çalışmada bahsedilecek SOCMINT dışındaki HUMINT (human intelligence), SIGINT (signal intelligence), IMINT (imagery intelligence) gibi temel veri toplama yöntemlerinin açıklamaları, hizmet ve faaliyet alanlarına göre istihbarat çeşitleri çalışmanın bütününü bozmayacak şekilde olabildiğince detaylı şekilde bu bölümde ele alınmıştır. Veri toplama yöntemlerinin ülkelerin teknik imkânlarına bağlı olarak çeşitlilik gösterebilmesinden dolayı çalışmanın bu bölümünde açıklanan "temel" yöntemler istihbaratın tüm veri toplama yöntemlerini kapsamamaktadır. Bölümün sonunda ise açık kaynak istihbaratının (OSINT) kavramı, kapsamı ve faaliyet kabiliyetleri açıklanmıştır.

Çalışmanın amaç ve hipotezinin test edileceği üçüncü bölüme ise "web 1.0" ve "web 2.0" kavramları açıklanarak başlanmıştır. İnsanların ihtiyaçları doğrultusunda internetin

ne gibi dönüşümler geçirdiği ve geçirmesi öngörülen değişimler incelenmiştir. Bu bölümde kavramsal çerçevelerin ele alındığı başlıklar dışındaki tüm bölümlerde belirli sorunsallara cevap aranmıştır. Sosyal medyanın tanımı, oluşumu ve platformları ele alındıktan sonra yeni medya olarak nitelendirilen sosyal medyanın geleneksel medyadan farkları ele alınmıştır. Bu bölümde, insanların ve basın yayın kuruluşlarının yeni medyayı tercih etmesindeki motivasyonlar incelenmiştir. Sosyal medyanın kullanımı bölümünde ise OSINT çerçevesinde sosyal medya verilerinin nasıl bir potansiyeli olduğu ifade edilmiştir. Dünya genelinde ve Türkiye özelinde 2020-2021 yılları sosyal medya ve internet kullanım verileri karşılaştırmalı olarak ele alınmıştır. Kamu kurumları ve siyasetçilerin sosyal medya kullanımı aynı şekilde veriler ışığında ele alınarak, dijitalleşme ve internet kullanımının artış göstermesinin devlet nezdinde halkla ilişkiler bağlamında ne gibi dönüşümler yaptığı incelenmiştir. Son olarak terör örgütleri ve uyuşturucu kartellerinin sosyal medya kullanımı, bu yapıların açık kaynak üzerinden veri paylaşımındaki motivasyonları örnekler üzerinden açıklanarak, kolluk kuvvetleri ve istihbarat birimleri için kullanılabilir veri potansiyeli incelenmiştir.

İnternet ve sosyal medyanın çok fazla oranda avantajı olmakla birlikte bir o kadar da olumsuz tarafları bulunmaktadır. Çalışmanın bu bölümünde, veri toplama aşamasında gerekli birimlere veya kullanılan yapay zekâ algoritmalarına engel olabilecek bilgi kirliliği tehdidi, kullanıcıların ve şirketlerin veri güvenliğini hedef alan veri hırsızlıkları ve siber güvenlik zafiyetleri, kullanıcıların dolandırılması amacıyla yürütülen sosyal mühendislik faaliyetleri, kitleleri harekete geçirmek ve yeni toplumsal hareketler için sosyal medyayı bir zemin olarak kullanma amacıyla algı yönetimi ve gözetim toplumunun oto-sansüre karşı göstereceği tepki ile güvenlik birimlerinin elde edebileceği potansiyel verinin azalması gibi OSINT ve SOCMINT sürecini olumsuz etkileyebilecek faktörler ele alınmıştır. Fakat sosyal medyanın zararları sadece bu çalışmada belirtilen konularla sınırlı değildir. Sosyal medya bağımlılığı veya siber zorbalık gibi tehditler, çalışmanın amaç bütünlüğünü sağlamadığı için kapsam dışı bırakılmıştır.

Sosyal medya istihbaratı (SOCMINT) başlığında SOCMINT'in tanımı ve kapsamı açıklanarak, veriden istihbarat bilgisi elde etmeyi öngören süreç, sosyal medya istihbarat çarkı üzerinden incelenmiştir. Bu bağlamda sürecin aşamaları ele alınarak veri toplama aşaması ve bu aşamada kullanılan araçlar, örnekler ve görseller üzerinden

açıklanmıştır. İşleme ve analiz aşamasında yararlanılan algoritmalara değinilerek, sosyal medya istihbaratının hukuki zemini ve bu yöntemin faydaları açıklanmıştır.

1. İSTİHBARAT İLE İLİŞKİLİ KAVRAMLAR

1.1. Güvenlik

Güvenlik kavramı, Latince; endişesiz, kaygısız, güvenli anlamına gelen "*sēcūrus"* kelimesinden türetilmiştir ve kökeni; güvenlik, emniyet anlamına gelen "*securitas"* kelimesine dayanmaktadır.[1] TDK'nin tanımı olarak ise; "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" anlamına gelmektedir.[2] Fakat strateji ve istihbarat gibi kavramların nasıl genel geçer bir tanımı yapılamamış ise güvenlik kavramı da aynı şekilde sabit bir tanıma sahip değildir. Farklı dönemlerde farklı şekillerde açıklanmış olmasının en büyük sebeplerinden bir tanesi ise güvenlik kavramının bir sebebin sonucu olmasından kaynaklanmaktadır. Yüzyıllar öncesinde yaşamış toplumların güvenlik anlayışıyla günümüz güvenlik anlayışı pek tabii ki bir olamaz. Avcılık, toplayıcılıkla hayatını devam ettiren bir toplumdaki güvenlik ihtiyaçları, o dönemin değişkenleri ve 21. yüzyılda, metropolde yaşayan bir topluluğun güvenlik anlayışı bambaşkadır. Bu yüzden güvenlik kavramının tanımı zamana, mekâna ve durumlara göre değişebilen bir yapıya sahiptir.

Güvenlik kavramı, tarih boyunca farklı zümreler tarafından tartışma alanı olarak kabul görmüştür. Güvenliğin bireysel mi, devlet boyutunda mı yoksa uluslararası alanda mı ele alınacağı tartışmaların boyutunu daha da büyütmüştür. Birey için de ulus için de uluslararası sistem için de güvenlik en önemli ölçüttür çünkü güvenliği sağlayamamanın sonu bireyin veya devletin hayatının son bulması ile neticelenmektedir. Uluslararası ilişkiler literatüründe güvenliğin sıkça "ulusal güvenlik" olarak tehdit ve tehlikelere karşı askerî/stratejik müdahaleler olarak açıklandığı görülmektedir. Realist paradigma uluslararası sistemi güç mücadelelerinin, çıkar çatışmalarının olduğu anarşik bir yapıya benzetmiştir. Tehdit ve tehlikenin uluslararası sistemin yapısından kaynaklı olduğunu savunan yapısal realistler ise bu anarşik yapının tarihte ve günümüzde nasıl tezahür

[1] Etimoloji Türkçe, (Çevrimiçi) https://www.etimolojiturkce.com/kelime/sigorta, (Erişim tarihi: 20 Nisan 2020)

[2] TDK, **Türk Dil Kurumu Sözlükleri**, (Çevrimiçi) https://sozluk.gov.tr (Erişim tarihi: 20 Nisan, 2020).

ediyorsa gelecekte de aynı şekilde ortaya çıkma eğiliminde olduğunu savunmuştur.[3] Bu bağlamda bir tehdit veya tehlike ortadan kaldırıldığında yeni bir tehdit ile karşılaşma ihtimali çok yüksektir çünkü uluslararası sistem yapısı gereği böylesine bir durum için uygun ortam oluşturmaktadır.

Walter Lippmann, bir ulusun temel değerlerini feda etme tehlikesi yaşamadığı ölçüde güvende olduğunu ifade ederek güvenliği ulusal çıkarlar boyutunda ele almıştır.[4] Arnold Wolfers ise güvenliğin, bir ulusun az ya da çok sahip olabileceği veya az ya da çok sahip olmayı arzuladığı bir değer olduğunu ve bu açıdan uluslararası ilişkilerde büyük öneme sahip olan güç ve zenginlik değerleriyle ortak yöne sahip olduğunu ifade etmiştir. Zenginliğin ulusun sahip olduğu materyaller ile ölçülebildiğini, gücün ise diğer aktörlerin hareketlerini kontrol etme yetisi olduğunu savunurken, güvenliğin nesnel anlamda, elde edilen değerlere yönelik hiçbir tehdidin olmaması ile öznel anlamda, bu tür değerlerin saldırıya uğrayacağına dair korkunun olmaması ile ölçüldüğünü fakat her iki açıdan da ulusun güvenliğinin, bir tarafta neredeyse tamamen güvensiz ve güvensizlik korkusuyla diğer tarafta ise tamamen güvenli ve korkudan uzak bir şekilde geniş bir yelpazede yer aldığını vurgulamıştır.[5]

Bu bağlamda güvenlik kavramı üzerine çalışan düşünürlerin ve akademisyenlerin çoğunun tehdit, tehlike ve risk kavramlarını sıkça kullandığı görülmektedir. Basit bir örnek üzerinden anlatmak gerekirse; komşunuzun evinde silah bulundurması, risk, ev sahibinin o silahı eline alması; tehlike, o silahı size doğrultarak vuruş pozisyonuna getirmesi ise tehdittir. Fakat bu noktada dikkat edilmesi gereken durum, komşunuzun bu silahı size ateş etmek amacıyla eline almamış olma ihtimalidir. Belki de sadece silahın mekanizmasını kontrol etmek için böyle bir eylemde bulunmuştur. Bu sebeple karar aşamasına gelindiğinde olgu ve algı ayrımının çok iyi yapılması gerekmektedir.[6] Güvenlik kavramının kendimizi tehdit altında hissettiğimizde aldığımız önlemler bütünü veya korunma içgüdüsü olmasından dolayı son kararın verilmeden önce çok ince bir şekilde analiz edilmesi elzemdir. Tehdidin şiddeti, karar verme mekanizmasının

[3] John Baylis, "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler**, 2008, Y. 5, S. 18, s. 72.

[4] Walter Lippmann, **U.S. Foreign Policy: Shield of the Republic**, Boston: Little, Brown and Company, 1943, pp. 50-51.

[5] Arnold Wolfers, ""National Secutiy" as an Ambiguous Symbol", **Political Science Quarterly**, 1952, Vol. 67, No. 4, pp. 484-485.

[6] Beril Dedeoğlu, **Uluslararası Güvenlik ve Strateji**, İstanbul: Yeni Yüzyıl Yayınları, 2014, ss. 27-33.

yavaşlamasına sebebiyet verebilir ve korunma içgüdüsü ile aslında tehlike arz etmeyen durumlar için boşa kaynak harcama ihtimali doğurabilir. Yok olma tehlikesiyle karşı karşıya gelindiği zaman dürtüsel hareket ederek yanlış tepkiler verilmemesi için algı ve olgu ayrımını doğru analiz etmek, önlemi alırken sarf edeceğimiz kaynakların doğru kullanılması bağlamında yardımcı olacaktır. Peki bu durum uluslararası ilişkilerde nasıl meydana gelebilir?

İran'ın nükleer zenginleştirme programları yürüttüğü bilinmektedir ve bu çalışmaların nükleer silah üretme ihtimaline karşılık diğer devletler tarafından politikalar üretilmektedir. İran'ın nükleer silahlara sahip olmasının Türkiye açısından risk oluşturup oluşturmadığına, Türkiye'nin beklentileri, İran ile ilişkileri ve bundan sonra uygulayacağı politikalarına bağlı olarak karar verilir. Türkiye, İran'ın elde edeceği nükleer güç ile çevresini tehdit edeceği algısına sahip ise bu gelişmeyi risk kategorisinde değerlendirebilir. Tam aksine, İran'da bu çalışmaların yapılmasının Türkiye'de de nükleer çalışmalarını başlatmasına zemin hazırlayacağı beklentisi olursa, o zaman bu süreç bir risk değil fırsat olarak değerlendirilebilir. İran'ın nükleer silah üretme niyeti bilinmeden, ne zaman üreteceği öngörülemeden ve üretirse ne gibi tehditler oluşturacağından emin olunmadan nükleer çalışmaları risk kategorisine koymak, komşunun evindeki silah örneği ile aynı kapıya çıkmaktadır. Sürecin tehlikeye ve tehdide dönüşmesi ise, nükleer çalışmaların hızlanması, silahlanmanın artması, tatbikatların daha sık yapılması ve dış politikada da sertlik yanlısı tutumun benimsenmesi gibi göstergelere bağlıdır.[7]

2019 senesinde ABD ve Türkiye arasında yaşanan S400 sorunu da güvenlik sorunu kategorisinde yer almaktadır. Bölgesel tehditlerin artması ve 2012 yılında Türkiye'nin NATO müttefiki olan ABD ile Almanya'nın Suriye'ye karşı kurmuş olduğu Patriot hava savunma sistemlerini geri çekmesi ile bir güvenlik tehdidi ile karşılaşan Türkiye Cumhuriyeti, bu tehdidi ortadan kaldırabilmek için hava savunma sistemi almak istemiş fakat Barack Obama dönemindeki ABD, Patriot hava savunma sistemlerinin satışını Türkiye'nin istediği şartlardan ötürü gerçekleştirmemiştir. Tehdidi ortadan kaldırmak için planladığı güvenlik önlemlerini alamayınca Türkiye'de başka bir alternatif olarak Rusya'dan S400 hava savunma sistemleri üzerinde anlaşmaya varmış fakat hem NATO üyesi olmayan Rusya'dan NATO'ya uyumsuz bir hava sistemi aldığı gerekçesiyle hem

[7] Dedeoğlu, **a.g.e.,** s. 33.

de F35 savaş uçağı projesinde hâlihazırda bulunduğu için ABD tarafından Türkiye'ye S400 savunma sistemlerini almakta ısrar etmesi durumunda yaptırım uygulanacağı ve Türkiye'yi F35 programından çıkarmak durumunda kalacakları belirtilmiş ve iki devlet arasında savunma sistemleri üzerinden bir kriz yaşanmıştır.[8] Bu örnekte de görüldüğü gibi uluslararası ilişkilerde güvenlik kavramı aslında subjektif bir kavramdır. Bir aktörün güvenlik kaygısı ile aldığı önlemler diğer aktör veya aktörler için yeni bir tehdit olgusu oluşturabilmektedir. Bu bağlamda güvenliğin sadece askerî ve teknik boyutu değil aynı zamanda stratejik ve diplomatik bir boyutu da bulunmaktadır.

Korunma içgüdüsü sadece devletlerin arasına mesafeler koyulmasına sebebiyet vermez aksine birlik olmalarını da sağlayabilir. Bunun belki de en önemli örnekleri ise NATO ve Varşova Paktı'dır. II. Dünya Savaşı'nın bitmesiyle Sovyetler Birliği ile baş başa kalan Avrupa, Sovyetlerin Berlin'i abluka altına alması ile ciddi bir güvenlik tehdidiyle karşı karşıya gelmiş ve askerî açıdan Sovyetlere nazaran eksik olmasından dolayı ABD ile ortak birlik kurma amacıyla birtakım diplomatik görüşmeler gerçekleştirmiştir. Bu görüşmelerin neticesinde "barış için ortaklık" mottosuyla 1949 yılında NATO kurulmuştur. NATO'nun temel amacı sadece Sovyetler Birliği tehdidine karşı birlik olmak değil genel anlamda tüm üye ülkelerin politik ve askerî özgürlüğünü temin edecek bir kolektif güvenlik örgütü olmaktır.[9]

NATO gibi bir birliğin kendilerine karşı kurulması da Sovyetler Birliği açısından bir tehdit oluşturmuştur ve NATO'nun Avrupa'da artan askerî ve ekonomik faaliyetlerine karşılık Sovyetler de Varşova Paktı'nı kurmuşlardır. Fakat Varşova Paktı'nın sonu NATO'nunkinden çok daha farklı bitmiş ve Soğuk Savaş döneminin sembolü hâline gelen Berlin Duvarı'nın 1991 yılında yıkılması ve akabinde SSCB'nin dağılması ile Varşova Paktı'nın da varlığının sonu gelmiştir.

Soğuk Savaş'ın bitmesi uluslararası sistemde ve devletlerin güvenliğe bakış açısında birçok yeniliğe sebep olmuştur. Dünya artık iki gücün çatışmasından, tek kutuplu bir düzene geçiş yapmış ve Soğuk Savaş dönemi boyunca güvenlik anlayışının salt askerî anlamda tezahür etmesiyle tarafları ciddi anlamda silahlanmaya itmesinden kaynaklı olarak güvenlik çalışmaları askeri çerçevede sıkışmıştır. XXI. yüzyılda küreselleşmenin

[8] Hikmet Yalçinkaya, 'Türkiye Neden S-400 alıyor? 'sorusuna verilebilecek en net 'Patriot 'yanıtı, 2019, (Çevrimiçi) https://www.gzt.com/jurnalist/turkiye-neden-s-400-aliyor-sorusuna-verilebilecek-en-net-patriot-yaniti-3494789 (Erişim tarihi: 21 Nisan 2020).

[9] NATO, (Çevrimiçi) https://www.nato.int/nato-welcome/index_tr.html (Erişim tarihi: 21 Nisan, 2020)

etkileri, dijitalleşme ve teknolojinin hızla ilerlemesi ise güvenlik kavramı açısından farklı çalışma alanları ortaya çıkartmıştır ve bunlara misal olarak gösterilebilecek kavramlardan bir tanesi olan "Dijital Güvenlik" kavramı literatüre kazandırılmıştır. Başlangıçta devletler tarafından ciddi bir sorun olarak algılanmasa da kısa sürede dijitalleşmenin ivme kazanması ve gerek kişisel gerek kurumsal gerek ise devlet bilgilerinin sanal ortama aktarılması ile bu alan, bireyler, özel şirketler ve devletler için yeni bir tehdit olgusu oluşturmuştur.

Kısacası güvenlik kavramının tanımlaması teorik olarak nasıl değişkenlik gösterebiliyorsa aynı şekilde pratik olarak da bu değişken yapıya sahiptir. Bölümün başında bahsi geçen olgu ve algı analizinin önemi aslında kısa vadede devletlerin ulusal çıkarları doğrultusunda güvenliğe bakış açılarını göstermektedir. Bunu bir örnekle açıklamak gerekirse; yine çalışmada bahsi geçen S400 krizinde, Türkiye'nin Almanya ve ABD'nin Patriot hava savunma sistemlerini çekmesine üzerine bir güvenlik açığı ile karşı karşıya kalması Türkiye açısından bir olgudur. Sınır komşusu olan Suriye'de hâlihazırda devam eden bir iç savaş ve terör gruplarının varlığı dolayısı ile güvenliği tahsis etme amacı güderek envanterinde hava savunma sistemi bulundurma niyeti, kaynakları bu amaç doğrultusunda harcaması için sağlıklı bir seçenektir. Fakat bir devletin tamamen kurgusal ve hakkında bilimsel hiçbir bir kanıtın bulunmadığı (örneğin; uzaylı istilası) bir duruma karşılık savunma harcaması yapması ise sadece algıdır ve bu doğrultuda harcanacak kaynaklar olgu-algı analizinden sonra mantıksız görülecektir. Bu yüzden çoğunlukla tehdit, tehlike veya risk faktörlerinin meydana çıkmasından sonra güvenlik önlemlerinin alındığı görülmektedir. İlk ortaya çıktığı dönemlerde internet, devletler tarafından tehlike arz etmeyen bir platform olarak değerlendirilmiş fakat virüsler, siber dolandırıcılık, siber zorbalık, bilgi kirliliği ve toplum mühendislikleri gibi tehditler ortaya çıkınca ulusal güvenliği tehdit eden bir yapı olarak tanımlanıp müdahale gereği duyulmuştur. 2020 yılında yaşanan Covid-19 küresel salgını gibi bu duruma benzer birçok farklı örnek sunmak mümkündür. Bu yüzden güvenlik kavramı bir insan gibi bünyesine yeni çalışma alanları katmaya devam edecektir. Günümüzde güvenlik sorunu olarak algılanmayan durumların, yakın gelecekte ulusal krizler çıkartabilecek düzeyde güvenlik sıkıntıları doğurması olanaksız değildir.

1.2. Strateji

TDK tanımı: "Bir ulusun veya uluslar topluluğunun, barış ve savaşta benimsenen politikalara destek vermek amacıyla politik, ekonomik, psikolojik ve askerî güçleri bir arada kullanma bilimi ve sanatı"[10] olan strateji kavramının tanımlanması birçok düşünür tarafından farklı şekillerde açıklanmıştır. Savaş stratejilerinin en eski ve hâlâ önde gelenleri arasında bulunan teorisyeni Sun Tzu, "Savaş bir ülkenin baş sorunu, ölüm kalım yeri, var olma ya da yok olma yoludur; 'muhasebesiz olmaz'."[11] diyerek stratejisi olmadan savaşa girecek ordunun hazin sonuçlar ile karşılaşacağını belirtmiştir.[12] Her ne kadar Sun Tzu'dan bu yana Machiavelli gibi birçok farklı düşünür tarafından strateji konusu dile getirilmiş olsa da bu çalışmada modern strateji kavramının öncüleri olan Carl Von Clausewitz ve Antoine Henri Jomini'nin prensipleri ele alınmıştır. Clausewitz stratejiyi, "Muharebenin savaşın amaçlarına hizmet edecek şekilde kullanılmasıdır." şeklinde açıklayıp, stratejinin muharebe alanına hizmet ettiğini, strateji teorisinin ise bu faaliyetlerin başlıca araçlarını ele almak zorunda olduğunu ifade etmiştir. [13] Bu durumda savaş alanına ve muharebenin seyrine etki eden bu araçların neler olduğu, giderilmesi gereken başka bir soru işaretidir. Stratejik planlamada, muharebe alanına istenilen sonucu elde etmek için uygulanan planı başarılı kılabilmek için birden çok parametreyi hesaba katmak gerekmektedir (Asker sayısı, askerlerin konumlandırılması, çevresel faktörler, dönemin teknolojik aletleri, istihbarat faaliyetleri, manevi değerler vb.). Hannibal Barca'nın stratejisinde istihbarat faaliyetlerinin yanı sıra psikolojik savaş ve propaganda yolunu da izlemiş olması,[14] Wu Ch'nin, güneyinde ki Wu devletine karşı

---

[10] TDK, (Çevrimiçi) https://sozluk.gov.tr (Erişim tarihi: 21 Nisan 2020).

[11] Sun Tzu durum değerlendirmesini yaparken 5 temel prensibin hesaba katılmasını söylemiştir. Bunlar: Yol, gök, yer, komutan ve kuraldır. Yol denen şey, haklı yöneticisi ile aynı şeyi paylaştırır. Ancak bu takdirde birlikte ölebilirler, birlikte yaşayabilirler ve halk kendini feda etmekten korkmaz. Gök denen şey, karanlık-aydınlık, soğuk-sıcak, zaman-mevsimdir. Yer denen şey, uzaklık-yakınlık, tehlikelilik-güvenlilik, genişlik-darlık, kurtuluşsuzluk-kurtuluşluluktur. Komutan denen şey, erdemlilik, güvenirlilik, insancıllık, cesaret, ciddiyettir. Kural denen şey, askerî birliklerin örgütlenme biçimi, subayların rütbelendirilmesi, ikmal yolları ve askerî harcamadır. (Kaynak: Sun Tzu, **Savaş Sanatı** (Pulat Oktan, Giray Fidan, Çev.), İstanbul: Türkiye İş Bankası Yayınları, 2019, s. 1)

[12] Tzu, **a.g.e.,** s. 1

[13] Carl Von Clausewitz, **Savaş Üzerine**, Eriş Yayınları, 2003, s. 148

[14] Rose Mary Sheldon, "Hannibal as a Spy Chief, Leid,schrift", 2015, S. 3, ss. 30-31. (Hannibal Barca'nın başka bir savaş taktiği de psikolojik harp idi. Hannibal bu yöntemi İtalya'da Roma'yı müttefiklerinden ayırmak için kullanmıştı. O dönemde İtalya'nın çoğu Roma toprağı değil, Roma egemenliği altındaki bağımsız, özerk devletlerdi. Hannibal, Roma ile bu özerk devletlerin arasını açmayı hedeflemişti. İtalyan topraklarına geldiği an ilk olarak buraya İtalya'nın yerli halkları ile savaşmaya değil aksine onları Roma'nın zulmünden kurtarmaya geldiğini söyledi. Her savaştan sonra esirler arasında Romalı

düzenlediği seferde, farklı kuvvetlerin nasıl bir arada kullanılacağını ve nasıl düzen içinde savaşılacağını göstermesi,[15] dinî ideolojilerin ön plana çıktığı Haçlı Seferleri, Napolyon Savaşları, dünya savaşları ve soğuk savaş döneminde birbirinden farklı teknikler, stratejiler kullanılmış ve farklı doktrinler ortaya çıkmıştır. Fakat uygulanma yöntemleri farklılık gösterse dahi değişmeyen şey, stratejik davranışın doğası ve amacıdır. Özneler ve nesneler ne kadar değişse de savaş stratejisinin temel amacı; sınırlı kaynaklar ile "Sizden daha üstün olma ihtimali olan/olmayan bir rakibe karşı nasıl galip gelinir?" sorusuna cevap niteliği taşıyan bir planlama yapmaktır.

Antoine Henri Jomini, stratejiyi savaş sanatının beş ana unsurundan birisi olarak kabul etmiştir. Stratejiyi bir ordunun araziye indiği andan itibaren sefer planının işleyişi şeklinde açıklayan Jomini, lojistik, ikmal depoları, stratejik noktalar, savunma veya saldırı şeklinin avantajları ve dezavantajları, ordunun ve düşmanın psikolojik durumu hatta ve hatta devlet başkanının savaşın karakteri üzerinde mutabık kalması gibi tüm detayları strateji başlığı altında ele almıştır.[16] Fransız İhtilali'nin gerçekleştiği yıllarda doğup Napolyon Savaşları'na çocukken tanıklık eden Jomini, Napoleonik metotlar konusunda en önde gelen yazarlardan bir tanesidir. Belki de bu yüzdendir ki Jomini'nin strateji anlayışında komutanların önemi çok büyüktür. Jomini, bahsi geçen savaş sanatının beş unsurunun ilk üçü üzerinde durmuştur. Bunlar; strateji, lojistik ve büyük taktiktir. Savaş alanında büyük resmi görüp, olağan durumu bir bütün olarak yorumlaması ve uygulamasını bu duruma göre yapması gereken komutanlar, büyük taktiğin uygulanmasında ve askerlerin yönlendirilmesinde kilit rol oynamaktadır. Jomini, strateji ve taktiklerin çokça öne çıktığı Yedi Yıl Savaşları'nda, savaş tarihinin önde gelen komutanları arasında bulunan Friedrich'e de atıfta bulunmuştur. Jomini'ye göre komutanın savaş kararı verildiği an savunma mı yoksa taarruza yönelik strateji mi güdeceği hayati önem taşımaktadır ve Friedrich bu dengeyi muhteşem bir şekilde

---

olmayanları herhangi bir fidye almaksızın serbest bıraktı ve Hannibal'ın politik hedeflerini ve cömertliğini insanların ağızdan ağıza birbirine aktarmasını bekledi. İzlediği bu politika yerel birlikleri toplamasında ve Roma'yı müttefiklerinden ayırma konusunda gayet etkili olmuştu.)

[15] Christon I. Archer, John R. Ferris, Holger H. Herwig, &, Timothy H. E. Travers, **Dünya Savaş Tarihi**, (Cem Demirkan, çev.), Tümzamanlar Yayıncılık, 2006, s. 57.

[16] Antoine Henri Jomini, **Savaş Sanatı – Prensipler / Ana Hatlar** (A. Tunçer Büyükonat, çev.), İstanbul: Doruk Yayımcılık, 2013, s. 69-75

kurarak tedafüi-taarruzun[17] muhteşem bir örneğini sergilemiştir. Buradan yola çıkarak Jomini, komutanın en büyük yetilerinden birisinde; saldırı ve savunma stratejisini nerede ve nasıl kullanılacağını bilmesi olduğunu ifade etmiştir.[18] Jomini komutanların önemini konusunda haksız değildir. Strateji çalışmalarında tarih çok önemli bir yer kaplamaktadır. Geçmişte yaşanmış savaş ve muharebelerde kullanılan taktikler ve stratejiler üstünden yıllar geçmiş olsa dahi günümüzde hâlâ ders niteliğinde okutulmaktadır. A. Safa Özkaya tarafından yerli bir öğreti olarak ortaya koyulan "Dört Yön Doktrini"nin temel unsurlarından bir tanesi olan entelektüel-kültürel zekâ bağlamında elde edilen bilgiler ile komutanın savaş alanındaki önemi bir kez daha vurgulanmıştır. Hint ordusu ile olan savaşında Timur'un fillerin ateşten korkması gibi basit bir bilgiyi stratejik bir şekilde kullanarak savaşın gidişatını tamamen değiştirip, muharebe başlar başlamaz düşman ordusunun sıklet merkezini kendi sıklet merkezi hâline getirmesi, komutanın sahip olduğu entelektüel zekânın muharebenin sonucunu nasıl etkileyebileceğini göstermektedir.[19]

Kısaca, sadece eski dönemlerde değil, modern strateji kuramı öncülerinin de stratejiyi genel olarak savaş ve muharebe alanı ile ilişkilendirmiş ve bu bağlamda ele almış olduğu görülmektedir. Bunun sebebini Sun Tzu'nun bölümün başında bahsi geçen savaş hakkında söylediği cümlelerden çıkarabiliriz. Fetihler dönemi olmasından mütevellit eski dönemlerde strateji kavramının ağırlıklı olarak savaş alanında değerlendirilmesi çok olağan bir durumdur. Fakat ilerleyen dönemlerde farklı değişkenlerin uluslararası sisteme entegre olması ile strateji çalışmalarının yelpazesinde de bu duruma bağlı olarak gelişmeler görülmüştür.

Çalışmanın bu bölümünde stratejik yaklaşımın tarihsel boyutu ile birlikte incelenmesi; birçok farklı zümre tarafından yöneltilen, "Stratejinin kökeni hangi döneme dayanmaktadır?" gibi soruların cevaplanmasını amaçlamaktadır. Yapılan eylemin adı bizzat strateji olarak adlandırılmasa da tarihin en eski zamanlarına kadar stratejinin

[17] Tedafüi-taarruz olarak adlandırılan bu savaş planı, taarruzdan sonra savunmaya çekilen ordunun pasif bir tutum sergileyip düşmanın saldırmasını beklemekten ziyade savunmaya geçen tarafın gücünü toplayıp her fırsatta düşmanın zayıf noktalarına saldırmasını, bu tutumun hem taktiksel hem de stratejik kazanımlar getireceğini öngören bir stratejidir. (Kaynak: Antoine Henri Jomini, a.g.e., ss. 76-77.)

[18] Jomini, **a.g.e.,** ss. 69-77.

[19] A. Safa Özkaya, **Hunlar'dan Günümüze Türk Askerî Kültürü**, İstanbul: Kronik Kitap, 2019, ss. 104-126.

örneklerini görmek mümkündür. Bu sorunsala ithafen, Lawrence Freedman, stratejinin primatların sosyal gruplar oluşturduğu zamandan beri var olduğunu ifade etmektedir.[20] Klasik dönemlerde muharebe alanındaki stratejiyi başarılı kılmak için birden çok parametreyi hesaba katmak gerekiyordu. Günümüzde ise strateji kavramının anlamı ve rolü önceki dönemlere göre oldukça değişmiş, askerî güç ve üstünlüğü elde etmeye odaklanan savaş teorilerinin klasik anlayışından sıyrılarak, belirli bir amaç doğrultusunda kısa, orta ve uzun vadeli olarak sürekli geliştirilen ve koşullara göre yeniden şekillenen, kendi içerisinde çok yönlü ve kapsamlı parametreleri içeren bir yaklaşım modeline dönüşmüştür.[21] XXI. yüzyıl strateji anlayışı sadece muharebe perspektifinden yorumlanmaya çalışılsa dahi çok fazla alanla karşı karşıya kalındığını çünkü savaşların çeşidinin teknolojinin gelişmesi ile bir hayli artmış olduğu görülmektedir. Artık sadece kara veya deniz savaşları değil, siber savaşlar, propaganda savaşları, kimlik ve kültür savaşları, nükleer savaşlar, mezhep savaşları, döviz-kur savaşları, petrol savaşları gibi stratejinin kullanılacağı birçok alan ortaya çıkmıştır.

Enformasyon çağında yaşanan gelişmeler strateji anlayışını da etkilemiştir ve strateji artık sadece devletlerin enstrümanı olmaktan çıkıp şahısların ve özel şirketlerin de kullanmaya başladığı bir kavram hâline gelmiştir. Satış ve pazarlama stratejileri, muhasebe stratejileri, stratejik karar alma süreci, kısa ve uzun vadeli yapılan planlar özel şirketlerin stratejiyi kullanım biçimlerine basit örnekler olarak verilebilse de stratejik düşüncenin özel kurumların bünyesine geçmesinin asıl nedeni rekabettir. Aslında devletlerin yüzyıllardır stratejiyi kullanmasındaki en basit neden de budur. Muharebeler, güç mücadeleleri, çıkar çatışmaları, devletler arasında yaşanan büyük rekabet yarışlarıdır ve strateji ise bu yarışı kazanacak olan tarafın doğru kaynakları, doğru miktarda, nasıl, nerede ve ne zaman kullanması gerektiğini öngören bir şematiktir. Kısacası stratejinin, tarihte rekabet alanının askerî kısmında tezahür etmesindeki en büyük sebeplerden bir tanesi; stratejik düşüncenin uygulanabileceği alanların çeşitliliğinin günümüze kıyasla daha az olmasından kaynaklanmaktadır.

[20] Lawrence Freedman, **Strateji**, İstanbul: Alfa Basım Yayım Dağıtım, 2014, s. 137.

[21] Merve Seren, **Stratejik İstihbarat ve Ulusal Güvenlik**, Ankara: Orion Kitabevi, 2017, s. 62.

2. İSTİHBARAT

2.1. İstihbarat Teorisi

İstihbarat, kelime kökeni olarak Arapça istihbar kelimesinin çoğulu olarak karşımıza çıkmakta ve yeni öğrenilen bilgiler, haberler, duyumlar anlamına gelmektedir.[22] İngilizce ve Fransızcada ise "intelligence" kelimesi ile ifade edilen ve anlamı "akıl, zekâ" olan istihbaratı MİT: "Devlet tarafından belirlenen ihtiyaçlara karşılık olarak çeşitli kaynaklardan derlenen haber, bilgi ve dokümanların işlenmesi sonucu elde edilen üründür."[23] şeklinde açıklarken, ABD'nin 2004 yılında kabul ettiği İstihbarat Reformu ve Terörizmin Önlenmesi Yasası ile atanan Ulusal İstihbarat Direktörü[24] ise: "ABD'nin içinden veya dışından, ABD'yi, Amerikan halkını, mülkleri, çıkarları: kitle imha silahlarının geliştirilmesini, çoğaltılmasını, kullanılmasını veya Amerika'yı ve halkını tehdit edecek diğer tüm konuları içeren bilgilerdir." şeklinde tanımlamıştır.[25]

Her istihbarat teşkilatının istihbarat tanımına bakış açısında farklılıklar görmemiz mümkündür. MİT kendi tanımını yaparken, Amerikan ve İngiliz istihbaratları kavram hakkında daha farklı tanımlar getirecektir. Teşkilatların istihbaratı farklı tanımlamalar ile açıklamasının sebebi ülkelerin ulusal güvenlik, savunma ve strateji alanında izlediği politikaların farklılık göstermesinden kaynaklanmaktadır. Bu yüzden bu alanlarda izledikleri politikaların etkisinde kalarak da istihbarat kültürlerini birbirlerinden farklı tarzda şekillendirmektedirler.[26]

Bu bağlamda istihbarat teorisinin geliştirilmesinde de farklı tanımlar ortaya çıkmıştır. Bunlardan bir tanesi istihbarat analizinin babası olarak nitelendirilen Sherman Kent

---

[22] TDK, **Türk Dil Kurumu Sözlükleri**, (Çevrimiçi) https://sozluk.gov.tr (Erişim tarihi: 22 Nisan 2020).

[23] MİT, (Çevrimiçi) https://mit.gov.tr/isth-olusum.html (Erişim tarihi: 22 Nisan 2020).

[24] Bkz. Title 1 – Reform of the Intelligence Community, SEC. 1001. Subtitle A – Establishment of Director of National Security (DNI), (Çevrimiçi) https://web.archive.org/web/20151211013650/http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-irtpa (Erişim tarihi: 22 Nisan 2020).

[25] DNI, (Çevrimiçi) https://www.dni.gov/index.php/what-we-do/what-is-intelligence (Erişim tarihi: 22 Nisan 2020).

[26] Philip H. J. Davies, "Ideas of Intelligence: Divergent National Concepts and Institutions", Harvard International Review, (October 1 2002), p. 66.

tarafından yapılmıştır: "İstihbaratı; devlet kararlarında etkili olan sivillerin ve askerlerin ulusal refahı korumak için sahip olması gereken bilgidir."[27] şeklinde açıklayan Kent, daha kapsamlı olarak istihbaratı üç aşama olarak ele almıştır. Bu aşamaları bilgi, organizasyon ve faaliyet olarak belirleyen Kent, tanımlamış olduğu bilgiyi, bütün verileri kapsayan ve oldukça geniş bir anlamda çeşitli enformasyon olarak betimleyip "Yüksek Düzey Pozitif Dış İstihbarat"[28] olarak adlandırmıştır. Bahsi geçen bilginin toplama işlemini bir organizasyonun yaptığını ve bu organizasyonu da aktif kişilerin oluşturduğu fiziksel bir yapı olarak tanımlamıştır. Son olarak da istihbarat kelimesini, sadece bilgiyi ve bu bilgiyi toplayacak organizasyonu adlandırmak için değil aynı zamanda bu organizasyonun faaliyetlerini de kapsayacak şekilde açıklamıştır.[29] Sherman Kent'in tanımı istihbarat konusundaki başka bir gözlemci olan Abraham Shulsky tarafından sıkça eleştirilmiştir.

İstihbaratı, "Bir devletin ulusal güvenlik çıkarlarını daha da ileriye taşımak ve gerçek ya da potansiyel rakiplerin tehditleriyle mücadele etmek için oluşturulacak politikaların uygulanması ile ilgili bilgilerdir."[30] şeklinde ifade eden Shulsky, Sherman Kent'in kullandığı "Yüksek Düzey Pozitif Dış İstihbarat" kavramını istihbaratı tanımlamak için yetersiz bulmaktadır. Kent'in tanımında yüksek düzeyde olmayan operasyonel ve taktik istihbaratın, dış istihbarat olmayan iç istihbaratın ve pozitif olmayan karşı istihbaratın yer almadığını ve Kent'in sadece bunların dışında kalanları ulusal refahı ve güvenliği tehdit eden unsurlar olarak ele almasını eleştirmektedir. Sherman Kent'in yazmış olduğu "Strategic Intelligence for American World Policy" kitabının başlığından da anlaşılabileceği üzere genel anlamda bir istihbarat teorisini tanımlamaktan ziyade

---

[27] Sherman Kent, **Strategic Intelligence for American Foreign Policy,** Princeton-New Jersey: Princeton University Press, 1949 s. Vii.

[28]" Buradaki 'Pozitif Dış İstihbarat', amaç, kapsam ve özü itibariyle yabancı ülkeleri tanımlar. Ne ABD ne de ona bağlı bölgeler sahip oldukları bu istihbarat türünün ilgi alanına girmez. Keza polisin görev alanı da kapsam dışıdır. Çünkü özellikle "pozitif" kelimesini kullanmasının sebebi söz konusu istihbaratın "kontr-entelijans, kontr-espiyonaj" veya ülkenin iç işleyişi sonucunda ortaya çıkan hainlerin veya ithal edilen yabancı ajanların ortaya çıkarılması amacı ile yapılan her türlü istihbarat eyleminden farklı olduğunu belirtmektir. "Yüksek düzey" kelimesi ise, operasyonel istihbarat, taktik istihbarat ve küçük askerî yapıların savaş sırasında kullandığı muharebe istihbaratını kavram dışında bırakmak için kullanmıştır. Geriye kalan ülkenin refahı ve güvenliği açısından vazgeçilmez olan bilgi ise Kent'in bahsettiği bilgidir." (Kaynak: Sherman Kent, **Stratejik İstihbarat** (B. Yasemin Özbek, Nazlım Şüküroğlu Arıca, çev.), Ankara: Avrasya Stratejik Araştırmalar Merkezi Yayınları, 2003, ss. 1-2.

[29] Kent**, a.g.e.,** ss. 1, 51, 136.

[30] Abraham N. Shulsky, **Silent Warfare: Understanding the World of Intelligence** (5th ed.), Washington D.C.: Potomac Books, s. 1.

ABD'ye göre istihbaratın ne olduğuna ve ABD'nin ihtiyaçlarına göre yazıldığını ifade etmektedir. Kent'in istihbarat tanımının çok dar bir tanım olduğunu belirten Shulsky, bu tanımın sadece barış zamanına hitap ettiğini, savaş zamanında ise istihbaratın askerî ve stratejik kararlar verilmesi için destekleyici bir unsur olmasının yanı sıra sahada askerleri operasyonel olarak da destekleyecek bir etken olduğunu savunmaktadır. Bunlara ek olarak gizlilik ilkesinin istihbarat anlayışının temel esaslarından olduğunu savunan Shulsky, gizlilik ile uğraşmanın istihbaratın doğal bir parçasını olmadığını söyleyen Sherman Kent'i yine sert bir şekilde eleştirmiştir.[31]

Mark Lowenthal ise: "İstihbarat, ulusal güvenlik için önemli olan spesifik bilgilerin talep edilmesi, toplanması, analiz edilmesi ve karar verici mercilere sunulması sürecidir; bu sürecin ürünleri; istihbarat faaliyetleri ile sürecin ve bilgilerin korunması ve işlerin yasal makamların talep ettiği şekilde yürütülmesidir." şeklinde bir tanımlama getirmiştir.[32] Lowenthal tanımı biraz daha açarak istihbaratı sadece ulusal güvenliği korumak için elde edilecek bir bilgi bağlamında açıklamaktan ziyade tanımın içine istihbarat sürecini de dâhil etmiş ve bu faaliyetlerin yasal düzlemde yapılması gerektiğini vurgulamıştır.

İstihbarata dair detaylı tanımlardan bir tanesi de Ümit Özdağ tarafından getirilmiştir. Özdağ kavramı; "İstihbarat, ulaşılabilen bütün açık, yarı açık ve/veya gizli kaynaklardan her türlü aracın kullanılması sonucunda elde edilen her türlü veri, malumat ve bilginin ulusal genel veya ulusal özel plandaki politikaların gerçekleştirilmesi ve ulusal politikalara zarar verilmesinin engellenmesi amacı ile toplandıktan sonra önemine ve doğruluğuna göre sınıflandırılması, karşılaştırılması, analiz edilerek değerlendirilmesi süreci sonucunda ulaşılan bilgidir" [33] şeklinde açıklamıştır. Özdağ burada basit veya çok genel bir tanım getirmektense istihbarat kavramını derinlemesine ele almış ve tanımında "bilgiyi" de kendi içinde detaylandırmıştır. İstihbaratın sadece ulusal politikaların gerçekleştirilmesinde değil aynı zamanda bu politikaların korunmasını da amaçladığını ifade ettiği istihbarat kavramının, toplanan ham verinin detaylı bir şekilde işlenerek kullanılabilir bilgiye dönüştürüldüğü süreci de tanımında belirtmiştir.

---

[31] Abraham N. Shulsky, **a.g.e.,** s. 169-172.

[32] Mark M. Lowenthal, **Intelligence: From Secrets to Policy**, Washington, DC: Congressional Quarterly Press, 2002, s.8.

[33] Ümit Özdağ, **İstihbarat Teorisi**, Ankara: Kripto Kitaplar, 2014, s. 31.

Aktarılmış olan farklı tanımlamaların ışığında, istihbarat teşkilatlarının, akademisyenlerin ve istihbarat üzerine çalışanların istihbarat kavramına farklı tanımlar getirmiş olması, istihbarat kavramının kalıplaşmış, sabit bir tanımının olmadığını göstermektedir. İstihbarat gibi kompleks bir çalışma alanına evrensel bir tanım getirmek düşünüldüğü kadar kolay bir eylem değildir. İstihbarat, akla ilk olarak James Bond gibi karakterleri getirse de teori ve organizasyon olarak bunlardan çok uzak bir kavramdır. Bir disiplini evrensel bir teori ile açıklamak, evreni tek bir tanımla anlatmaya çalışmaya benzer, yani eksik kalacaktır. Dolayısı ile istihbarat teorisinin geliştirilmesi sürecinde birçok farklı tanım ve bakış açısı ortaya çıkmıştır.

2005 yılında ise istihbarat teorisini geliştirme girişimleri akademik anlamda çok farklı bir boyuta evirilmiştir. Henüz Soğuk Savaş'ın bitmesinin üzerinden fazla bir zaman geçmemiş iken 11 Eylül 2001 tarihinde ABD'nin "engelleyemediği" terörist saldırısı istihbarat kavramına bakış açısını da değiştirmiş ve istihbarat teorisi açısından bir dönüm noktası olmuştur. Birçok farklı zümre tarafından istihbarat başarısızlığı olarak eleştirilen bu saldırının üstüne Irak'la, kitle imha silahları ile ilgili krizin de çıkması, istihbarata karşı bakış açısının bir kez daha değerlendirmeye alınmasına zemin hazırlamıştır. Ulusal İstihbarat Direktörü'nün yardımcısı ve Deborah Barger'ın çalışmalarıyla istihbaratın kavramsal ve teorik temelini anlamak ve geliştirmek için RAND Corp.[34] ile birlikte DNI ofisi bir *workshop* oluşturmuştur. Fakat bir kavramı geliştirmek için önce geliştireceğiniz kavramı anlamanız gerekmektedir. Bu atölyenin ürünleri olarak yapılan tartışmaların ve panellerin neticesinde literatüre istihbarat teorisi bağlamında birçok eser kazandırılmış ve 2008 yılında Peter Gill, Mark Phythian ve Stephen Marrin'in *Intelligence Theory: Key Questions and Debates* adlı kitabı çıkarılmıştır.[35] 2005 yılına kadar istihbarat ve güvenlik literatürlerinde istihbarat teorisine dair pek çok eser bulunmamasına karşın, 2005 yılında ortak bir çalışma olarak yapılan bu *workshop*'un ardından istihbarat teorisi üzerine yapılan akademik çalışmalarda ciddi bir artış görülmüştür.[36]

---

[34] Genel merkezi ABD, Kaliforniya'da bulunan kâr amacı gütmeden dünya genelinde siyasi araştırmalar ve analizler yapan kuruluş, RAND Corp. Resmî web sitesi, https://www.rand.org/about/history.html (Erişim tarihi: 1 Mayıs 2020).

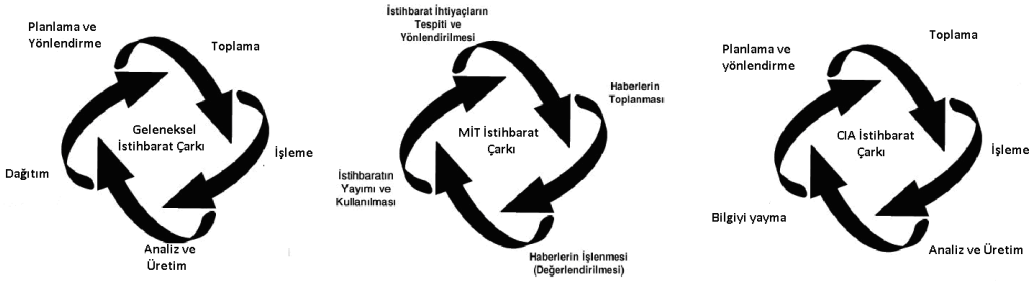
[35] Peter Gill, Mark Phythian, Mark & Stephen Marrin, **Intelligence Theory: Key Questions and Debates**, Studies in Intelligence Series, 2008.

[36] Stephen Marrin, "Evaluating Intelligence Theories: Current State of Play", **Intelligence and National Security**, 2018, Vol. 33, No. 4, s. 479.

Bu bağlamda istihbaratın tanımını yapmakta nasıl farklı fikirler ortaya çıkmışsa istihbarat sürecine de farklı açılardan yaklaşan akademisyenlerin ve teşkilatların birbirlerinden farklı istihbarat çarklarını ortaya çıkardığı görülmektedir.

2.1.1. İstihbarat Çarkları

İhtiyaç duyulan amacın tespit edilmesi, ihtiyaçların tespitine göre veri toplanması, verinin enformasyona ve bilgiye dönüştürülmesi, bilginin de analiz ve işleme ile istihbarat bilgisine dönüştürülüp gerekli alanlarda kullanılmasını kapsayan sürecin tamamına istihbarat çarkı denir. Çark benzetmesi bu sürecin hiçbir zaman bitmemesinden ve sürekli devam etmesinden kaynaklanmaktadır. Bu çarkların ana modeli ise "Geleneksel İstihbarat Çarkı"dır. Basitçe beş aşamadan oluşan geleneksel istihbarat çarkına yönelik eleştirilerin artması ve alternatif modelleri ortaya çıkarmıştır. Gregory F. Treverton, Mark M. Lowenthal, Douglas H. Dearth, Geraint Evans, Robert M. Clark, Arthur S. Hulnick gibi istihbarat kökenli kişiler ve akademisyenler geleneksel istihbarat çarkının süreci anlatmak için yeterli, fakat sistemi tasvir etmek için yetersiz kaldığını ifade etmişlerdir.[37]



Şekil 1: Geleneksel İstihbarat Çarkı, MİT İstihbarat Çarkı, CIA İstihbarat Çarkı

Kaynak: MİT, (Çevrimiçi) https://www.mit.gov.tr/t-cark.html (Erişim Tarihi: 05 Eylül 2022); CIA (Çevrimiçi) https://www.cia.gov/spy-kids/parents-teachers/docs/Briefing-intelligence-cycle.pdf (Erişim Tarihi: 5 Eylül 2022).

Yukarıda Şekil-1 ile gösterilen istihbarat çarkı örnekleri çoğaltılabilmektedir. NATO'nun istihbarat çarkı, Kanada istihbarat çarkı hatta ve hatta istihbarat teorileri üzerine çalışan akademisyenlerin birçoğunun geliştirmiş olduğu istihbarat çarkı modellleri mevcuttur.[38] Şekillerde görüldüğü gibi MİT, istihbaratın çarkını dört aşamalı olarak tanımlarken, CIA neredeyse geleneksel çarkın birebir aynı modelini

[37] Seren**, a.g.e**., ss. 256-257.

[38] Bkz. Lowenthal, Treverton, Clark…

uygulamaktadır. Yani işleyiş biçimleri farklılıklar gösterse de istihbarat çarkları hiç bitmeyen planlama, toplama, işleme, analiz etme ve amaca ulaşma sürecini temsil eden bir mekanizmadır.

2.2. İstihbarat Toplama Yöntemleri

İstihbarat ürününü elde edebilmek için ham verilerin belli işlemler sonucu bilgiye dönüştürülmesi ve bu bilgilerin analiz, işleme ile istihbarata dönüştürülmesi gerekmektedir. Bu verilere veya bilgilere ulaşmak için ise pek çok farklı yöntem kullanılmaktadır. İstihbarat toplama, hedeflerin bilgisi olmadan yapılan kapalı veya açık eylemler olmakla beraber istihbarat çarklarında olduğu gibi, faaliyeti yürüten kurumun ihtiyaçlarına, imkânlarına ve daha birçok parametreye göre değişkenlik gösterebilen bir yapısı bulunmaktadır. Bu bağlamda istihbarat toplama yöntemlerinin genel geçer bir şematiği olmamasından kaynaklı olarak birçok farklı çeşit karşımıza çıkabilmektedir. Bu çalışmada istihbarat toplama yöntemleri bağlamında aşağıdaki temel model kullanılmıştır;

I. Sinyal İstihbarat (Sigint),
II. Görüntü İstihbaratı (Imint),
III. İnsani İstihbarat (Humint),
IV. Nükleer İstihbarat (Nucint),
V. Radar İstihbarat (Radint),
VI. Akustik İstihbarat (Acoustint),[39]
VII. Açık Kaynak İstihbaratı (OSINT)

İstihbarat süresince vazgeçilmez bir diğer kaynak ise istihbarat arşividir. İstihbarat teşkilatının arşivi olmadan analizcilerin kurumsal veya bireysel hafızalarından söz etmek mümkün değildir. Arşiv olmadan yeni gelen verilerin, haberlerin ve bilgilerin geçmiştekilerle karşılaştırılması mümkün değildir. Bir üniversite için kütüphane ne ise istihbarat teşkilatı için arşiv de tam olarak odur.[40]

[39] Michael Herman, **Intelligence Power in Peace and War**, Cambridge University Press, 1996, s. 81.

[40] Özdağ, **a.g.e.,** ss. 81-82.

2.2.1. Sinyal İstihbarat

Sinyal istihbaratı hedef devletin muharebe elektronik sistemleri tarafından yayımlanan elektromanyetik enerjinin alınması, kaydedilmesi, değerlendirilmesi ve yorumlanması ile elde edilen istihbarattır.[41]

XIX. yüzyılın ikinci yarısından sonra hükûmet dışı aktörlerin diplomatik telgraflara erişim sağlaması ile XX. yüzyılın en verimli istihbarat kaynağı olmuştur.[42] İstihbarat toplama metotları arasındaki en yararlı yöntemlerden biri olup hükûmetlere önemli kararlar alınırken yeni bakış açıları kazandırabilmektedir. Sinyal istihbaratı hedeflenen sinyalin türüne bağlı olarak çeşitli şekillerde toplanabilmektedir. NSA ham sinyal istihbaratını toplamakta ve daha sonra çevirmenler, kriptologlar, analistler ve diğer teknik uzmanlar ile bu ham veriyi tüm kaynak analistlerinin kullanabileceği bir ürüne dönüştürmektedir.[43]

Bu yöntemin en önemli örneklerinden bir tanesi Echelon projesidir. Echelon, dünya çapında elektronik iletişimi toplu olarak ele geçirip analiz eden istasyonlardan, uydulardan ve diğer dinleme noktalarından oluşan küresel bir gözetim ağıdır. Beş farklı ülkenin sinyal istihbarat teşkilatının ortak katılımı ile oluşturulmuştur; ABD'yi temsilen NSA; Birleşik Krallığı temsilen GCHQ; Kanada'yı temsilen CSE; Avustralya'ya temsilen DSD ve son olarak Yeni Zelanda'yı temsilen GCSB. Operasyonun kontrolü ise NSA'ya aittir ki bu bu durum bir dönem İngiltere'yi rahatsız etmiş ve ABD ile aralarında Echelon operasyonu bağlamında bir anlaşma yapmaya götürmüştür.[44] Yıllar boyunca telefon konuşmalarını, radyo dalgalarını, kablosuz bağlantıları, e-mailleri, faksları, telgrafları ve daha birçok iletişim trafiğini izleyebilen uydu ağı Echelon, Büyük Britanya'daki bir çocuğa giden doğum günü telgrafından, Berlin Duvarı'nda Doğu Almanya askerlerinin telsiz konuşmalarına kadar her şeyi sistem tarafından kayıt etmektedir.[45]

---

[41] Özdağ, **a.g.e.**, s.122.

[42] Herman**, a.g.e.**, ss. 66-67.

[43] CIA, (Çevrimiçi) https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence-1.html (Erişim tarihi: 26 Nisan 2020).

[44] Bkz. UKUSA Agreement

[45] K. Lee Lerner, & Brenda Wilmoth Lerner, (2004), Encyclopedia of Espionage, Intelligence and Security, Vol I, Detroit, Thomson Gale, s. 370-371

Sinyal istihbaratının güçlü yanları olduğu gibi, zayıf yanları da bulunmaktadır. Pahalı olmasının yanı sıra, ileri teknoloji ve uzman personele gerek duyan bu sistem uzun zaman almakta ve planlama ile arşivlenmesi oldukça zordur. Üstelik hedef ülkenin muharebe elektronik sistemleri ile diğer iletişim sistemlerinin çökmesi/susması hâlinde veri erişimi kesilmektedir. Bu gibi programlara karşı önlem almak amacıyla terör örgütlerinin -özellikle lider kadroları- telefon, telsiz vb. sinyal istihbaratına yakalanan araçlar kullanmadıkları zaman ulaşılmaları ve tespit edilmeleri çok zor olmaktadır.[46]

2.2.2. Görüntü İstihbarat

Uçaklara veya uydulara yerleştirilen fotoğraf makineleri aracılığıyla çekilen görüntüler üzerinden elde edilen istihbarat yöntemidir. Bu yöntemde de görüntülerden elde edilecek faydayı etkileyen bazı faktörler bulunmaktadır. Bunlardan birisi çözünürlüktür. Minimum boyuttaki bir hedefin görüntü yorumlayıcıları tarafından ölçülebilir ve tespit edilebilir olması, bunun için de çözünürlük kalitesinin yüksek olması gerekmektedir. Çözünürlük ne kadar yüksek olursa görüntü o kadar detaylı olur, görüntü ne kadar detaylı olursa istenilen bilgi de o kadar kolay elde edilir. Aynı şekilde hava şartları, görüntünün gece ya da gündüz vaktinde, yüksek veya alçak irtifadan çekilmiş olması da bu faktörler arasındadır. Çekimin yapıldığı ekipmanın kalitesi ve renk tonları da belirleyici etkenlerdendir.[47]

Görüntü istihbarat yöntemi I. Dünya Savaşı'ndan bu yana aktif bir şekilde kullanılmakta ve istihbarat faaliyetlerine destekleyici anlamda ciddi faydalar sağlamaktadır. ABD ve Sovyetler arasında yaşanan Küba Füze Krizi'nde Lockheed U-2 casus uçaklarının çekmiş olduğu fotoğraflar krizin büyümesinde çok etkili olmuştur.[48] Keza bu casus uçaklarından birisinin Sovyet topraklarında düşürülmesi de yine ABD ve Sovyetler arasında başka bir krizin çıkmasına sebebiyet vermiştir.[49]

Görüntü istihbaratındaki fotoğrafların çoğu uçaklar veya uydular kullanılarak elde edilirken günümüzde *drone*lar ve insansız hava araçları da bu amaçla yaygın olarak kullanılmaya başlanmıştır. Silahlı *drone* ve İHA'ların dışında üzerlerine kamera

---

[46] Özdağ, **a.g.e.**, s. 125.

[47] Michael Herman, **Strategic Intelligence: Understandig the Hidden Side of Goverment**, Wesport-London: Prager Security International, 2007, s. 63.

[48] Henry Rubenstein, "DC Power and Cooling Towers", Aktaran: Central Intelligence Agency, Studies in Intelligence, **Archival Record**, 1971, Vol. 16, No. 3, s. 81.

[49] Bkz. U-2 Krizi

yerleştirilmiş casus *drone* ve İHA'lar askerî istihbarat toplama amacı ile belirlenen yerlerde çekim amaçlı kullanılmaktadır. TSK'nin Fırat'ın doğusunda yürüttüğü Barış Pınarı Harekâtı'nda, Rasulayn'da bulunan PKK/YPG'li teröristlerin lastik yakarak İHA'ların görüntü elde etmesini engellemesi,[50] yukarıda belirtilmiş olunan görüntünün kalitesini etkileyen faktörlere basit bir örnek olabilir.

Görüntü istihbaratın diğer yöntemlerden farkı ise sürekliliğin olmamasıdır. İhtiyaç hâlinde hedefin nerede konuşlandığı, elinde ne gibi mühimmatlar olduğu vb. gibi bilgilerin edinilip, görüntü yorumlayıcılar tarafından analiz edilmesi ve yeniden ihtiyaç duyulması hâlinde tekrar başvurulan bir sürecin ürünü olmasıdır.

2.2.3. İnsani İstihbarat

İstihbarat denilince zihinlerde ilk canlanan veri toplama yöntemi insani istihbarattır. Bu disiplinde, kabaca kendi devleti hakkında bilgiye erişimi olan yabancı bir yetkiliyi tespit edip ikna ederek ondan hedeflenen bilgiyi alınabileceği gibi bilginin kaynağı insanlardır. Fakat bu yöntemde bilgi, sadece yabancı yetkililer aracılığıyla elde edilmemektedir. Özellikle savaş zamanlarında duyum alma veya gözlem yapma şansı olan sivillerden de insani istihbarat yöntemi ile bilgi alınabilmektedir (Gemiler ne zaman limana gelecek, tanklar nereden hareket etti, ne yöne doğru gittiler gibi.). Hatta bazen hakkında bilgi almak istenilen kişinin veya istenilen bilgiye sahip olan kişinin bir yakın arkadaşı veya akrabasını kullanarak da istihbarat toplanabilmektedir (Terör örgütü mensupları veya uluslararası silah kaçakçıları).[51]

Bu bilgi toplama yönteminde genellikle iki aktif rol bulunmaktadır. Birincisi; istihbarat teşkilatının görevlendirdiği istihbarat *case officerı*, ikincisi; istihbarat personeline bilgi akışını sağlayacak muhbir, kaynaktır.[52] İstihbarat görevlisi faaliyetlerini açık veya kapalı şekilde yönetebilmektedir. Bilgi akışını diplomatik kimlik ve görüşmeler ile elde edebilmesinin yanı sıra espiyonaj yani casusluk faaliyetleri ile de aktif bir şekilde faaliyet gösterebilir.

İnsani istihbaratın gelişen teknolojiye rağmen önemini hiç kaybetmemesinin yanı sıra birtakım dezavantajları da bulunmaktadır. Bunlardan en önemlisi ise bilginin

---

[50] DHA, 2018, (Çevrimiçi) https://www.dha.com.tr/yurt/turkiyeye-roket-atan-sivil-kiyafetli-teroristler-boyle-goruntulendi/haber-1564458/video/ (Erişim tarihi: 27 Nisan 2020).

[51] Abraham N. Shulsky & Gary J. Schmitt, **Silent Warfare: Understanding the World of Intelligence** (3rd ed.), Washington DC: University of Nebraska Press, 2002, s. 11-12.

[52] Shulsky and Schmitt, **a.g.e.,** s. 11.

doğruluğudur. İstihbarat görevlisinin kaynaktan alacağı bilgiyi teşkilatına bildirmesi ve o bilgi üzerinden strateji yürütülmesi için doğruluğundan emin olunması gerekmektedir. Kullanılan muhbirin iki taraflı ajanlık faaliyeti yürütüyor olabileceği gibi daha sonradan taraf değiştirme ihtimali de göz önünde bulundurulmalıdır. Örneğin: 1980'lerde ABD ordusuna katılan ve Fort Bragg'da[53] ABD Özel Kuvvetleri tarafından İslami terörizme karşı eğitim alan eski Mısır ordusu subayı Ali Mohamed, Brooklyn'de Al Kifah Mülteci Merkezi'nin içine sızarak casusluk faaliyetlerinde bulunmuş ve burada teröristlerle etkileşime girmiştir. Buradaki görüşmelerinin etkisinde kalarak Mohamed daha sonrasında taraf değiştirmiş ve Usame Bin Ladin'e katılmıştır. ABD'li yetkililer tarafından yakalanan Mohamed, Al-Kaide'nin ABD'nin Afrika'daki iki elçiliği bombalama planlarını itiraf etmiştir. Fakat bu itiraf için biraz geç kalınmıştır çünkü Mohamed plana dair bildiklerini 1999 yılında söylemiştir yani saldırılar gerçekleştikten tam bir yıl sonra.[54]

Her ne kadar teknolojinin gelişmesi ile geçmiş tarihe nazaran XXI. yüzyılda insani istihbarat yönteminin öneminin azaldığı düşünülse de bu ifadenin doğru olduğu pek söylenemez. Özelikle terörizmin bölgesel bir tehdit olmakla beraber küresel bir tehlikeye dönüşmesi insani istihbarat ihtiyacını her zaman gerektirecektir. Dönemin süper gücü olan ABD'nin, teknik imkânlara sahip olmasına rağmen insani istihbarat eksikliğinden dolayı 11 Eylül saldırılarını engelleyememesi istihbarat faaliyetlerinde HUMINT'in önemini göstermektedir. Bu bağlamda istihbarat disiplinleri arasında da en önemli veri toplama yöntemi insani istihbarattır. Teknolojik imkânlar ne kadar yüksek düzeyde olursa olsun spesifik bilgilerin elde edilmesinde ve verilerin doğrulanmasında HUMINT ihtiyacı olacaktır. Sonuç olarak bir istihbarat servisinin asıl gücü sahip olduğu HUMINT gücüyle doğru orantılıdır.

2.2.4. Nükleer İstihbarat

Nükleer istihbarat, nükleer patlamaların tespiti, yer altı sismografik hareketlerin kayıt altına alınmasını ve havadaki gama ışınlarından yakın mesafedeki nükleer malzemelerin varlığını tespit etme amacıyla yerleştirilmiş uydular vasıtası ile uygulanan istihbarat yöntemidir.[55]

---

[53] ABD Ordusunun Kuzey Carolina'da bulunan askerî üssü.

[54] K. Lee Lerner and Brenda Wilmoth Lerner, **Encylopedia of Espionage**, Intelligence and Security Vol. II, Detroit: Thomson Gale, 2004, s. 89.

[55] Herman, **a.g.e.,** s. 78.

2.2.5. Radar İstihbarat

Alan takibi için geliştirilmiş olanlar dâhil, uzun menzilli radarlar (Bkz. Ufuk Ötesi Radar) aracılığı ile yapılan istihbarat yöntemidir. Soğuk Savaş döneminde füze ve uçak saldırılarını önceden uyarma sistemi olarak kullanılmıştır.[56]

2.2.6. Akustik İstihbarat

Akustik istihbarat, denizaltındaki sonik dalgaları algılayan araçlar ile veri toplanarak yapılan istihbarat yöntemidir. En ilginç örneklerinden bir tanesi; Soğuk Savaş döneminde CIA'nin Sovyet denizaltılarını dinlemek için yunus balıklarını eğitip akustik sinyallerini yakalamalarını sağlamasıdır.[57]

2.3. Ölçeklerine Göre İstihbarat

İstihbarat faaliyetleri neticesinde toplanacak bilginin faydalanılabileceği üç farklı hizmet alanı vardır.[58] Bunlar:

I. Stratejik İstihbarat,
II. Taktik İstihbarat,
III. Operasyonel İstihbarat

Stratejik istihbarat, uzun vadeli tahmin, öngörüler ve daha geniş bir hizmet alanına sahipken, taktik istihbarat sonuca ulaşmak için kısıtlı zamanda faydalanılan istihbarat alanıdır. Operasyonel istihbarat ise hâlihazırda devam eden ya da başlatılacak bir operasyon için taktik istihbarattan daha kapsamlı bilgi sunan istihbarat alanıdır.[59]

2.3.1. Stratejik İstihbarat

İstihbaratın bir üst formu olarak değerlendirilen[60] stratejik istihbaratın teori babası Sherman Kent, *Stratejik İstihbarat* eserinde; devlet liderlerinin, ulusal amaçlara ulaşmak ve ulusal güvenliği sağlamak için alacağı kararlarda yanılgıya düşmelerini ve

---

[56] Herman**, a.g.e.,** pp. 78-79.

[57] Paul Handley, Cats, Dolphins and One Smart Raven: The CIA's Secret Animal Spies,Yahoo! News, 2019, (Çevrimiçi) https://news.yahoo.com/cats-dolphins-one-smart-raven-cias-secret-animal-013906580.html (Erişim tarihi: 28 Nisan 2020).

[58] Bkz. Ümit Özdağ bu hizmet alanlarını dört şekilde ele almıştır. Stratejik, Operasyonel, Taktik ve Entegre İstihbarat.

[59] Hank Prunckun, **Handbook of Scientific Methods of Inquiry for Intelligence Analysis**, Plymouth, UK: The Scarescrow Press Inc., 2010, s. 6.

[60] Prunckun, **a.g.e.,** p.6.

hata yapmalarını engellemek için rakip ülkeler hakkında ihtiyaç duydukları raporsal bilgilerin tümünü "Stratejik İstihbarat" olarak tanımlamıştır.[61]

Tanımı biraz daha açacak olursak, stratejik istihbarat, devletin karar verici mercilerini, verecekleri karardan önce olabilecek olaylarla, ihtimallerle ilgili bilgilendirerek kararı vermeden önce destekleyici bir unsur görevi yapmakla birlikte analiz ve öngörü ile uygulanan politika sonrası hakkında çıkarımlar yapmaktadır. Bu bağlamda stratejik istihbaratın nihai hedefi hakkında bilgiye ihtiyaç duyduğunuz rakibin imkânlarını ve zayıflıklarını tespit edip, nasıl bir politika izleyeceğini öğrenmektir.[62]

Stratejik istihbaratın uygulandığı alanları biraz daha detaylı anlatmak gerekirse; bir terör örgütü yapılanmasının liderleri ile ilişkileri, bu liderin öldürülmesi veya yakalanması sonucunda verebilecekleri tepki, örgütün hiyerarşik düzeni gereği liderin yokluğunda yerine kimin geçeceği, bu yerine geçecek şahsın hangi zümrelerle ne gibi ilişkileri olduğu ve bu gibi olayların ülkenize geri dönüşünün nasıl olacağı gibi soruların cevapları stratejik istihbarat ile bulunabilmektedir. Pek tabii stratejik istihbarat sadece terörle mücadele veya askerî anlamında değil, diplomatik alanda barış zamanında da kullanılabilecek bir yöntemdir. Başka bir ülkenin diplomatik kadrosu için de stratejik istihbarat yöntemi ile bilgiler ve öngörüler edinilebilir. Bir başkanın veya yeni bir bakanın atanması ile de yukarıdaki sorulan soruların benzerlerine cevaplar aranabilmektedir.

2.3.2. Taktik İstihbarat

Taktik istihbarat kısaca muharebe alanı istihbaratıdır. Çoğunlukla askerî amaçlara ve ihtiyaçlara hizmet eder. Harekâtın planlanması, birliklerin konuşlanacağı yerlerin güvenliği, hava ve arazi hakkındaki bilgiler, lojistik imkânlar, düşman birliğinin nerede bulunduğu, insan gücü, teçhizatlar, düşmanın güçlü ve zayıf noktaları vb. gibi bilgileri toplayıp karar alıcıların hizmetine sunar. Terörle mücadele bağlamında taktik istihbaratın önemi her ülke için çok kritiktir. Teknolojinin gelişmesi ve yeni imkânların ortaya çıkması ile envantere katılan insansız keşif araçları ise taktik istihbarata yeni bir boyut kazandırmıştır.[63]

---

[61] Kent**, a.g.e.,** pp. 1-5.

[62] Özdağ, **a.g.e.,** s. 132.

[63] Seren, **a.g.e.,** s. 272.

2.3.3. Operasyonel İstihbarat

Operasyonel istihbarat, karar vericilere muharebe alanından daha kapsamlı ve geniş bir hizmet sunar. Taktik istihbaratı, terör örgütünün karargâhının nerede olduğunu, ellerinde ne gibi silahlar bulunduğunu cevaplarken, operasyonel istihbarat terör örgütünün amacının, niyetlerinin ne olduğuna, iletişim ağlarına veya örgütün finans kaynağına odaklanır. Operasyonel istihbarat faaliyetleri bağlamında karşımıza çıkan analitik süreçlerden birisi de JIPOE'dir (Joint Intelligence Preparation of the Operational Environment). İstihbarat çarklarında olduğu gibi sürekli devam eden bir süreci temsil eden JIPOE, operasyonel alandaki karar vericilere istihbarat, değerlendirme ve tahmin hizmeti sunar.[64]

Şekil 2: JIPOE

Kaynak: https://www.thelightningpress.com/joint-intelligence-preparation-operational-environment-jipoe/ (Erişim tarihi: 03 Mayıs 2020)

2.4. Hizmet Alanlarına Göre İstihbarat

İstihbarat, faaliyet açısından çok geniş bir yapıya sahiptir. İstihbarat faaliyetleri sadece diplomatik, askerî veya güvenlik meseleleri için yapılmamakla beraber istihbaratın belli başlı faaliyet alanları bulunmamaktadır. İstihbaratın çalışma alanı çok kapsamlı ve bir o kadar da esnektir. Bu bağlamda aşağıda verilen istihbarat alanları istihbarat faaliyetlerinin yapıldığı tüm alanları değil sadece bir kısmını kapsamaktadır.

I. Siyasi İstihbarat,

II. Askerî İstihbarat,

[64] JP 3-18, Joint Forcible Entry Operations CH 1, (11 Mayıs 2017).

III. Ekonomik İstihbarat,
IV. Sosyal İstihbarat,
V. Coğrafi İstihbarat,
VI. Biyografik İstihbarat,
VII. Ulaşım ve İletişim İstihbaratı,
VIII. Bilim ve Teknoloji İstihbaratı,
IX. Siber İstihbarat[65]

2.4.1. Siyasi İstihbarat

Bir ülkenin, tarihiyle, siyasi ve anayasal yapısıyla, inanç sistemiyle, etnik yapısıyla, politik partiler ve seçim süreçleriyle yani genel anlamda ülkenin siyasal yapısıyla ilgili bilgileri hedef alan istihbarat alanıdır. Tarihten bugüne kadar devletlerin politikalarında kritik bir rol oynayan siyasi istihbarat, bir nevi hedef devletin detaylı şekilde profilini çıkarmaya yönelik bir operasyondur. XXI. yüzyılda artan küresel terör tehditler, bölgesel çatışmalar, ekonomik ve toplumsal krizler siyasi istihbaratın önemini arttırmaktadır.[66]

Ümit Özdağ, siyasi istihbarat analizcisinin hedefindeki ülkeyi incelerken göz önünde bulundurulması gereken 11 unsur olduğunu belirtmiştir. Bunlar:

I. Tarih,
II. Anayasal yapı,
III. Hükûmetin etkinliği,
IV. Dış politika,
V. Politik partiler,
VI. Politik kültür,
VII. Baskı grupları,
VIII. Seçim süreci,
IX. Yıkıcı ve bölücü faaliyetler,
X. İncelenen ülkede istihbarat ve polis servislerinin konumudur.[67]

[65] Özdağ, **a.g.e.,** s. 62.

[66] Seren, **a.g.e.,** s. 279.

[67] Özdağ, **a.g.e.,** ss. 65-70.

2.4.1.1. Tarih

"İnsanlık Laboratuvarı" olarak betimlenen tarih, bir ülkenin yapısını anlayabilmek adına çok önemli veriler sunmaktadır. Ülkelere ve toplumlara kimlik kazandırmasının yanı sıra, ülke ve toplumların var oluşunda da önemli bir rol oynamaktadır. Peter N. Stearns, "Neden Tarih Öğreniyoruz?" isimli makalesinde tarihin, insanları ve toplumları anlamaya, geçmişin, bugünü ve yarını etkileyeceğini bu sebeple de yaşadığımız toplumların bugüne nasıl geldiğini analiz etmeye yaradığını aktarmaktadır. ABD kongresinde bir siyasi parti egemenliğinde değişiklik olması sonucunda başka bir eyalette gençlerin intihar oranlarındaki artışa ya da Orta Doğu'da çatışmaların artmasına değinerek, geçmişte yaşanan olayların nasıl etkiler yarattığını anlayarak olayların nasıl şekilleneceğini anlayabileceğimizi savunmaktadır.[68] Tarihin, devletleri ve toplumları anlama, ne gibi eğilimleri olduğu, hayallerinin ve hedeflerinin ne olduğuna yönelik çıkarımlarda bulunma konusundaki önemi göz önünde bulundurulduğunda, siyasi istihbarat açısından da ne kadar önemli bir bilgi kaynağı olduğunu rahatlıkla söylenebilmektir.

2.4.1.2.Anayasal Yapı

Anayasanın iki temel blok üzerine kurulu olduğunu söyleyebiliriz. Bunlar; bir yandan devletin yapısı, işleyişi ve bunların ana prensiplerini belirler ve organların birbirleriyle olan ilişkilerini kurala bağlarken, diğer yandan da hakları ve özgürlükleri tanımlayarak benimser.[69] Yani devlet organlarının yapısı hakkında bilgi edinmek, yasama, yürütme ve yargının halka sunduğu hak ve özgürlükleri ve aynı zamanda yetkilerini anlayabilmek adına anayasal yapı, istihbarat analizcisi için önemli bir kaynaktır. Buna ek olarak anayasal yapının halka sunduğu hak ve özgürlüklerin, adaletin tahsis edilmesin de izlediği yolun ve şeffaflığının halkın gözünde nasıl bir konumda olduğu da araştırma ve analiz konuları arasında mutlaka bulunmalıdır.

2.4.1.3. Hükûmetin Etkinliği

Devletin siyasal yapısında hükûmetlerin rolü çok büyüktür. Bu yüzden siyasi istihbarat analizcisinin hükûmetlerin etkinliği hakkında yapacağı gözlemler de öngörülerine büyük katkıda bulunacaktır. Hükûmetlerin ideolojisi, icraatları ve popülist söylemleri

---

[68] Peter N. Stearn, **Why Study History?,** 1998, (Çevrimiçi) https://www.sd162.org/cms/lib/IL02218050/Centricity/Domain/534/Why%20Study%20History%20-%20Sterns.pdf, (Erişim tarihi: 30 Nisan 2020), ss. 1-2.

[69] Uygar Coşkun, "Dünden Bugüne Anayasacılık", **Hukuk Gündemi Dergisi**, 2008, S. 9, ss. 95-96.

arasındaki orantı, hükûmet kadrosunda bulunan kişilerin yolsuzluk ile bağlantıları, kriz yönetimi kabiliyetleri gibi konular analizcinin araştırma alanları arasındadır.

2.4.1.4. Dış Politika

Dış politika analizi, devletlerin çıkarlarını (özellikle de bölgesel), niyetlerini, bölgede kendilerine hangi unsurları tehdit veya tehlike olarak gördüklerini, hangi devletler, örgütler veya kuruluşlar ile potansiyel müttefik/düşman olabileceklerine dair unsurları tespit etmemize imkân sağlamaktadır. Ülkenin dış politika tarihi, yapmış oldukları anlaşmalar ve ittifaklar, analizcinin dış politika hususunda ihtiyacı olan araştırma konuları arasındadır. Fakat bir devletin izleyeceği politikaları veya stratejileri öngörebilmek için sadece diplomatik kaynakları incelemek yeterli olmamaktadır. Ulusun okul kitaplarından, gayri resmî bilimsel literatürünün taranmasına kadar birçok alan, en az diplomatik araştırmalar kadar fayda sağlayacaktır. Bu tür araştırma araçları ile devletin düşünce yapısını ve temel ideolojisini anlamak mümkün olacaktır. Aynı zamanda ülkede bulunan küçük radikal grupların ideolojileri ve görüşleri de önem arz etmektedir. Zira bu grupların söylemleri, uygun koşulların oluşması ile yerleşik sistem tarafından kabul görebilmektedir.[70]

2.4.1.5. Politik Partiler

Eski dönemlerde imparatorlar, krallar ve mensup oldukları hanedanlar ile yönetilen devletler, Fransız İhtilali ve daha sonrasında monarşik siyasal yapıya karşı yapılan devrimler sonucunda yerini demokratik siyasi partilere bırakmıştır. Her siyasi partinin amacı devlet yönetiminde söz sahibi olmaktır. Parti mensupları halkın her kesiminden olabileceği gibi tek bir kesimden de oluşabilir ve her siyasi partinin mutlaka bir ideolojisi bulunmaktadır. Bu bağlamda, siyasi istihbarat analizcisinin politik partileri araştırırken partilerin ideolojilerini, parti mensuplarını, halkın hitap ettikleri kesimini, etkinlik güçlerini, finans kaynaklarını analiz kapsamına alması büyük önem taşımaktadır.

2.4.1.6. Politik Kültür

Politik kültür kavramı, bu alanda yapılan çalışmaların öncüsü olarak sayılan Gabriel Abraham Almond tarafından *Comparative Political Systems* kitabında şu şekilde tanımlanmıştır:

---

[70] Özdağ**, a.g.e.,** s. 66-67

> *"Her siyasal sistem, siyasi eyleme yönelik belirli bir yönelim örüntüsünde bulunur. Bunu, siyasal kültür olarak adlandırmayı daha uygun olduğunu gördüm. Siyasal kültür kavramına ilişkin iki nokta vardır. Birincisi, bu kavram belirli bir politik sisteme ya da topluma uymamaktadır. İkincisi ise, siyasal kültür her ne kadar genel anlamda kültür ile ilişkili olsa da onunla aynı şey değildir. Çünkü siyasal yönelim, kültürün standartları ve değerleriyle olduğu kadar, biliş, akıl ve dışsal durumlara uyumu da içermektedir. Bu nedenle kültürün farklı bir parçasıdır ve kendine has bir özerkliğe sahiptir.*[71]

Kısacası siyasal kültür: "Toplum üyelerinin politik sisteme yönelik kavrayışları, kanaatleri ve değerlendirmelerinin içselleştirilmesidir."[72] Bu bağlamda siyasi istihbarat analizcisi, hedef ülkenin politik kültürüne dair incelemelerde bulunurken ülkenin genel kültürüne de hâkim olması gerekmektedir. Politik kültür siyasi istihbarat analizcisine, inanç, fikir ve toplumsal değerlerin siyasal süreç üzerindeki etkisi, toplumsal var oluşun anlamı, toplumsal öncelikler ve güncel sorunlar gibi bilgileri sunmaktadır.[73]

2.4.1.7. Baskı Grupları

Baskı grupları, siyasal karar alma sürecinde siyasal iktidar ve bürokrasi üzerinde çeşitli yöntem ve araçlarla doğrudan etkili olmaya ve dahası baskı kurmaya çalışan organizasyonlardır. [74] Baskı grupları arasındaki organizasyonlara barolar, işçi sendikaları, ticaret odaları örnek olarak gösterilebilir.[75] Siyasal sistemi doğrudan veya dolaylı bir şekilde etkileme gücüne sahip bu grupların analizi; organizasyonların amacını, finans kaynaklarını, yöntemlerini ve siyasal sistemi etkileme kabiliyetlerini kapsamaktadır ve istihbarat analizcisi için önemli unsurlardan bir tanesidir.

2.4.1.8. Seçim Süreci

Seçim süreci, siyasal aktörlerin aktif bir şekilde faaliyet gösterdiği ve halkın faaliyetlere verdikleri tepkilerin yoğun şekilde yaşandığı bir dönemdir. Siyasi istihbarat

---

[71] Gabriel A. Almond, "Comparative Political Systems", **The Journal of Politics**, 1956, Vol. 18, No. 3, p. 396.

[72] Gabriel A. Almond, Sidney Verba, **The Civic Culture: Political Attitudes and Democracy in Five Nations**, New Jersey: Princeson University Pres, 1963, s. 14.

[73] ÖZDAĞ, Ümit, (2014), a.g.e. s. 67-68

[74] AKTAN, C. Can, (2007), Hakan Ay, Hilmi Çoban, "Siyasal Karar Alma Sürecinde Çıkar Grupları" içinde: C. Can Aktan, Dilek Dileyici, Modern Politik İktisat: Kamu Tercihi, Ankara, Seçkin Yayınları, s. 205

[75] "Ümit Özdağ'a göre mafya örgütlenmeleri de son dönemlerde baskı grupları arasında değerlendirilmektedir.", (Kaynak: ÖZDAĞ, Ümit, (2014), a.g.e. s. 68)

analizcisinin, hedef ülkedeki seçim süreçlerini doğru bir şekilde analiz etmesi, siyasal aktörlerin hareket kabiliyetlerini çözümlemenin yanı sıra halkın beklentileri ve tepkileri açısında da önemli bulgular elde etmesine fayda sağlamaktadır.

2.4.1.9. Yıkıcı ve Bölücü Faaliyetler

XXI. yüzyılda terör ve organize suç faaliyetleri küresel boyutta olduğu gibi bölgesel anlamda da birçok devlete güvenlik sorunları yaşatmaktadır. Hedef aldıkları ülkenin bütünlüğünü bozma, temel hakları gasp etme veya yıkma eğilimi olan bu grupların eylem kapasitesi, gücü, ideolojisi, büyüklükleri ve amaçları hakkında gerekli bilgileri, kamuoyu tepkisi ve hedef devletin tehdit karşısındaki hareket ve karşılık verme kapasitesi ile birlikte analiz etmek, hedef devletin ulusal çıkarları ve güvenliği idame ettirebilmesi doğrultusunda ne kadar potansiyeli olduğu sonucunu sunacaktır.

2.4.1.10. İncelenen Ülkede İstihbarat ve Polis Servislerinin Konumu

Bilgi toplanma amacı ile araştırılan ve analiz edilen hedef ülkedeki kolluk kuvvetlerinin ve istihbarat servislerinin etkinliği, konumu, tarafsızlığı, hükûmete olan yakınlığı ve bağlılığı incelenmesi gereken unsurlardan bir tanesidir.[76]

2.4.2. Askerî İstihbarat

İstihbaratın en geniş ve önemli çalışma alanlarından birisi askerî istihbarattır. Özellikle dünya savaşları ve Soğuk Savaş döneminde savaş alanlarının genişlemesi ve kullanılan askerî teknolojilerin gelişmesine paralel olarak askerî istihbaratın önemi de artmıştır. Askerî istihbarat genel olarak, savaş zamanında askerî operasyonları yürütme amacını kapsarken, barış zamanında, orduların kendi askerî güçlerini planlamasını veya yabancı askerî kurumlar hakkındaki bilgileri kapsamaktadır.[77] Aynı zamanda, saldırı operasyonunun gerçekleşebileceği düşüncesi ile kumandana, düşmanın kapasitesi, gücü ve alanın fiziki niteliklerine dair bilgi sağlaması ve kumandana savaş hâlinde neler ile karşılaşabileceğini savaşa girmeden bildirmesi, askerî istihbaratın hazırlayıcı bir özelliğinin olduğunun göstergesidir.[78]

Askerî istihbarat, sadece savaş anında veya savaş alanında düşman tehdidinin/tehlikesinin açığa çıkarılmasını değil, aynı zamanda terörle mücadele veya

[76] Özdağ, **a.g.e.,** s. 70.

[77] Shulsky, Schmitt**, a.g.e.,** p. 54.

[78] Kent**, a.g.e.,** pp. 201-202.

karşı ayaklanma politikalarını da destekleyecek önemli unsurlardan bir tanesidir.[79] Zira söz konusu istihbarat alanı karşı ayaklanma olduğu durumlarda, artık devletin veya ordunun karşısında başka bir devlet veya ordu değil halk bulunmaktadır. Bu bağlamda askerî istihbaratın sunacağı bilgi, ayaklanmanın çatışmayı ortadan kaldırarak sonlandırmasında büyük rol oynayacaktır.

Fakat stratejik anlamda galip gelebilmek için rakibin sadece askerî yapısını incelemek yeterli olmayacaktır. Tek başına askerî güç bir ülkenin millî gücünü anlamamız için yeterli veri sunmayacaktır. Ümit Özdağ, millî gücün formülünü şu şekilde paylaşmıştır:

MG= (Ü + N + E + A) * (S + Mİ)

Ü: Ülkenin Büyüklüğü

N: Nüfus

E: Ekonomik Güç

A: Askerî Güç

S: Ülkenin Stratejik Hedefi

Mİ: Millî İrade[80]

Bu bağlamda askerî stratejik istihbarat çerçevesinde yapılacak faaliyetlerde hedef ülkenin askerî gücü, incelenmesi gereken tek unsur değildir. Örneğin 1945 yılında başlayıp 1975 yılında son bulan, ABD'nin son 10 yılında dâhil olduğu ve sonucunun ABD açısından hezimetle sonuçlandığı Vietnam Savaşı, ABD'ye hem sınır ötesi operasyonlarında hem de istihbarat faaliyetlerinde unutamayacağı birkaç ders vermiştir. İkinci Dünya Savaşı'nın bitmesi ve Soğuk Savaş'ın başlaması ile komünist yayılmacılığını ulusal güvenliğine direkt tehdit olarak gören ABD, Vietnam'da bulunan komünist güçlerin Fransa'yı bozguna uğratmasına sessiz kalmayarak komünizm tehlikesine karşı Güney Vietnam tarafına destek vererek savaşa dâhil olmuştur. ABD'nin, düşman savaş düzeniyle, casusluk oranlarıyla, Güney'de kontrol edilen insan sayısıyla ilgili elinde sağlam istihbarat bulunmamasına hatta 1967 yılının başlarına kadar CIA'nin Viet Cong Güvenlik Servisi'nin varlığından dahi haberi olmamasına karşılık sayılar ve askerî üstünlük üzerinden yaptığı hesaplamalar ile Vietnam Savaşı'na dâhil olması,[81] harcanan tonlarca miktar bomba, yapılan uçak ve helikopter yardımları

[79] Seren, **a.g.e.,** s. 281.

[80] Özdağ, **a.g.e.,** s. 60.

[81] Central Intelligence Agency Collection, **The Vietnam Center and Sam Johnson Vietnam Archive**, Texas Tech University, s. 2

ve portakal gazlarıyla[82] yapılan operasyonlara rağmen, on binlerce ABD askerinin ve milyonlarca insanın ölümüyle sonuçlanıp ABD'nin hem Vietnam'da hem de yapılan protestolar ile kendi ülkesinde güven kaybetmesiyle sonuçlanmıştır. Sadece sayılar ve askerî güç üzerinden yapılan hesaplamaların, halkın sosyolojik yapısını, bölgenin demografik yapısını, komünist bölgenin destek aldığı Sovyetler ve Çin'in bölgeye ne kadar hâkim olduğunu ve savaşın gidişatını etkileyen diğer birçok parametreyi kapsamaması, savaşın ABD için bir hüsranla sonuçlanmasına sebep olmuştur.

2.4.3. Ekonomik İstihbarat

Siyasi ve askerî alanlarda olduğu gibi ekonomik alan da hükûmetlerin karar alma aşamasında istihbarat faaliyetleri ile desteklenmektedir. Millî gücün önemli unsurlarından bir tanesinin ekonomik güç olmasına karşın özellikle dünya savaşları ve Soğuk Savaş döneminde devletler nezdinde güçlü olmak, askerî güç ile bağdaştırılmış fakat Soğuk Savaş'ın bitimi ve küreselleşmenin etkileriyle artık güçlü olmak için sağlam bir ekonomiye ihtiyaç duyulduğu kabul edilmiştir. Hatta 2018 yılında ABD ile Çin arasında başlayan "ticaret savaşları" ile ekonomi âdeta yeni bir savaş alanı hâline gelmiştir. Ekonominin gerek askerî gerek stratejik olarak ülkenin alacağı kararlarda ve uygulayacağı politikalarda belirleyici bir özelliği olduğunu göz önünde bulundurursak, ekonomik istihbaratın da ne denli önemli bir rolü olduğu rahatlıkla anlaşılabilmektedir.

Ekonomik istihbarat, doğrudan ya da dolaylı olarak, bilgi toplama işleminin hedefindeki ülkenin ekonomisinin göreceli verimliliğini, rekabetçi konumunu, finansal, ticari ve hatta hükûmet bilgilerini kapsayan istihbarat alanıdır.[83] Bunlara ek olarak yine hedef ülkenin tarım ve sanayi kapasitesi, ham madde kaynakları, ihracat ve ithalat hacmi, pazar payı, kendi kendine yetebilme kapasitesi, ülke ekonomisinde söz sahibi olan kişi ve kişiler, bu kişilerin hükûmet ile olan ilişkisi, finans ve borsa sektörü ekonomik istihbaratın odaklandığı alanlar arasındadır. Özellikle XXI. yüzyıl itibari ile ivme kazanan ekonomik ve teknolojik gelişmeler neticesinde çeşitli sektörlerin özelleştirilmesi, yerli/yabancı şirketlerin sektörel pay oranları, ülkelere gelen yabancı

[82] Ağaçlar üzerinde pusu kuran Vietnam askerlerinin ABD ordusuna verdiği zayiatı önlemek için ABD'nin kullandığı kimyasal maddedir. Bitkilerin yapraklarının dökülmesine sebep olan gazın ismi yaprak dökücü, kimyasalın depolandığı kutuların üzerindeki sarı banttan gelmektedir ve geliştirilmesi sırasında ABD ordusu tarafından "Agent Orange" kod adı verilmiştir. Tabii ki kimyasal maddenin tek zarar verdiği bitkiler değildir, insanlar üzerinde de kas ve kemik bozukluklarından, felç etkisine kadar yan etkileri bulunmaktadır. Detaylı bilgi için Bkz. Lerner, Lerner**, a.g.e.,** pp. 9-10.

[83] Evan H. Potter, **Economic Intelligence and National Security**, Canada: Carleton University Press, 1998, s. vii.

yatırımcılar, yabancılara yapılan arazi satışları vb. hususlar, ekonomik istihbarat açısından ihmal edilemez konulardır.[84]

Her ülkenin farklı ekonomik istihbarat sisteminin bulunması, devletlerin nihai amacı olan ekonomik güvenliğine kendi ekonomik gücü ve sistemi vasıtasıyla ulaşmasına bağlıdır. Örneğin, Almanya'nın ekonomik istihbarat sisteminin merkezini ticaret odaları ve özel sektör oluşturup, sistemin yapısı daha çok kapalı yollarla agresif bir ekonomik istihbarat toplama programını ve bireysel firmalar düzeyinde ekonomik istihbaratın önemi konusunda yüksek düzeyde farkındalığı kapsarken, Britanya'da, sistemin kilit rolünü ticaret ve endüstri bakanlığı oluştururken büyük ölçüde açık yollarla ekonomik istihbarat toplama yöntemi benimsenmiş, kamu ve özel sektör üyeleri ile ekonomik istihbarat üreticileri arasında orta düzeyde bir iş birliği sağlanmıştır.[85]

Kısacası, Soğuk Savaş'ın bitimi ve küreselleşmenin etkisiyle yeni bir mücadele sahasına dönüşen ekonomi alanı, ülkelerin ulusal çıkarları doğrultusunda kilit bir rol oynamaktadır. Bu bağlamda ülkeler böylesine önem arz eden bir alan doğrultusunda gerek içeride gerek ise dışarıda meydana gelen gelişmeleri yakından takip edip, bilgi sahibi olmak istemektedirler. Ekonomik istihbarat ise bu çerçevede devletlere hem gelişmelere vâkıf olmak hususunda hem ulusal çıkarlarını gözetmek hem de rakip devletlerin stratejik hamlelerini öğrenip ekonomik güvenliğini sağlamlaştırma hususunda hizmet sunmaktadır.

2.4.4. Sosyal İstihbarat

XXI. yüzyılda, uluslararası sistemin geçmişte yaşamış olduğu dönüm noktalarının etkisi ile güvenlik, tehdit gibi kavramların yapısında meydana gelen büyük çaplı değişimler sonucunda, geleneksel güvenlik anlayışında pek karşılığı bulunmayan devlet dışı aktörler, gerekli müdahaleler yapılmadığı veya eksik kaldığı takdirde devletler açısından ciddi anlamda tehdit hâline dönüşen toplumsal hareketler, güvenlik disiplininde sosyal bilimlere ihtiyaç duyulduğunun sinyallerini vermeye başlamıştır. Bu bağlamda toplumların yapısı, kültürleri, inançları, değerleri vb. hakkındaki bilgileri hedef alan sosyal istihbarat, oldukça geniş bir bilgi kaynağına sahiptir. Ümit Özdağ'a göre sosyal istihbaratın sekiz temel unsuru bulunmaktadır, bunlar:

---

[84] Seren, **a.g.e.,** s. 285.

[85] Potter, **a.g.e.,** s. 54-56.

I. Nüfus (Yerleşim, artış oranı, yaş ve cinsiyet yapısı, iş gücü, göç, askerlik çağındaki erkek nüfus, ırk grupları, etnik gruplar),
II. Sosyal karakteristikler (Etniklik, aşiretçilik, sosyal skala, resmi ve gayri resmî örgütler, sosyal hareketlilik, mülkiyet düzeni uygulaması),
III. Kamuoyu ve bu çerçevede basın-yayın araçları,
IV. Eğitim,
V. Din (Dinin yapısı, dinî grupların karar alma süresine etkileri, dinî gruplarla devlet arasındaki çatışmalar, dinî gruplar arası ilişkiler),
VI. Sağlık ve sosyal güvenlik sistemi,
VII. Genel kültürel özellikler,
VIII. Zihniyet analizi.[86]

Sadece bu kategorileştirmeye bakıldığında dahi sosyal istihbarat kapsamında bulunan bilgi çeşitliğinin ne denli fazla olduğu anlaşılmaktadır. Sosyal istihbarat, başka bir ülkenin sosyolojik yapısını anlamak için kullanılabileceği gibi bir ülkenin kendi iç sorunlarını çözme amacıyla da kullanılabilmektedir.

Sosyal istihbaratın önemli alanlarından bir tanesini de "kültürel istihbarat" oluşturmaktadır. Farklı kültürlerin karmaşık yapısını kapsayan kültürel istihbarat, sınır içi veya sınır dışı operasyonlarda önemli destekleyici unsurlardan bir tanesidir. Askerî uzmanlar, Jacob Kipp, Lester Grau, Karl Prinslow ve Captain Don Smith, etnografik ve kültürel istihbarat olmadan yapılan bir askerî operasyonu, ellerimizi kullanmadan yapılan bir eve benzetmiştir, yani; yüksek derecede başarısızlık ihtimali olan, boşa harcanmış ve son derece yavaş bir süreçtir. Fakat bir inşaatta başarısızlık, zaman ve malzeme kaybına sebep olurken, savaş alanındaki başarısızlık sivil ve askerî can kaybına ve kaybeden taraf için ciddi jeopolitik sonuçlar anlamına gelmektedir.[87] Bu bağlamda, -özellikle- sınır ötesine yapılan operasyonlarda karar vericilerin bölgenin kültürel yapısıyla ilgili bilgilere hâkim olmaları operasyonun neticesi açısından hayati önem taşımaktadır.

İstihbarat toplama açısından birçok farklı seçeneğin olmasına karşılık SOCINT (sosyo-kültürel istihbarat) yönteminin diğerlerinden farklı olarak sınırsız bilgi toplama imkânı

[86] Özdağ, **a.g.e.,** ss. 84-85.

[87] Kipp, Grau, Prinslow, and Smith, "The Human Terrain System: A CORDS for the 21st Century", **Military Review**, (September-October, 2006), p. 8.

olduğu fikrini ortaya atan Kerry Patton, SOCINT'in metodoloji ve analiz bağlamında kritik önem taşıyan yeni bir istihbarat disiplini olduğunu ifade etmiştir.[88] 11 Eylül 2001 saldırılarından sonra Afganistan'ı işgal eden ABD'nin bölgede savaştan etkilenen sivil Afganlar için kargo uçaklarından MRE (Meals Ready to Eat) paletlerini bıraktıklarını, bunun Afgan halkı için bir iyi niyet gösterisi ve jest olduğunu düşünen ABD'nin yemek paletlerinin çoğunlukla domuz eti bulundurduğunu, Afgan halkının ise Müslüman olması ve İslam'da domuz etinin haram olması sebebiyle bu jestin çok trajik bir şekilde olumsuz sonuçlanmış olmasının SOCINT eksikliğine bağlayan Kerry Patton, karar vericilerin bölge ile alakalı farkındalığa sahip olamadıklarını, istihbarat servisinde resmî bir SOCINT unsuru kurulmuş olsaydı bu durumun hafifletilebileceğini ifade etmiştir.[89]

Özetle, sosyo-kültürel verilerin ve analizlerin ulusal güvenlik ve stratejik politikalar açısından kritik bir önemi olmasından kaynaklı olarak; sosyo-kültürel istihbarat perspektifine uygun bir yaklaşım modeli benimseyen istihbarat kurumları bünyelerinde psikolog, siyaset bilimci, sosyolog, teolog, antropolog, istatistikçi, sosyal psikolog, etnograf gibi farklı meslek ve uzmanlık gruplarından gelen personel bulundurmakta veya bu alanlarda bilgi üreten üniversiteler, düşünce kuruluşları ve enstitülerle yakın iş birliği içerisinde hareket etmektedirler.[90]

2.4.5. Coğrafi İstihbarat

Ögdülmiş, karargâh yerinin belirlenmesi konusuna önem vererek, karargâh kurulurken öncü birliklerin bölgenin suyunun ve otunu iyice incelemesi gerektiğini ifade etmiştir. Uçurum, bataklık, orman ve dağlık alanlarda ne tür tuzaklarla karşılaşacaklarını bilmedikleri için bu topraklardan orduyu geçirirken yanlarında mutlaka yöresel kılavuzlar bulundurarak ellerindeki olanakları avantaja çevirmişlerdir.[91] Tarihten bugüne kadar coğrafya, askerî stratejilerin oluşturulması açsından büyük önem taşıyan bir unsur olmuştur. Toplum yapısını, kültürünü şekillendirebileceği gibi askerî operasyonlarda da sağlam öngörülerin oluşturulmasında etkili bir faktördür.

Askerî açıdan son derece önemli olan bu unsur hakkındaki bilgi hizmetini ise coğrafi istihbarat sunmaktadır. Askerî istihbaratın en eski yöntemlerinden birisi olan coğrafi

---

[88] Kerry Patton, **Sociocultural Intelligence: A New Discipline in Intelligence Studies**, London: The Continuum International Publishing Group, 2010, s. 12.

[89] Patton, **a.g.e.,** s. 22.

[90] Seren, **a.g.e.,** ss. 290-291.

[91] Erkan Göksu, **Kutadgu Bilig'e Göre Türk Savaş Sanatı**, İstanbul: Kronik Kitap, 2018, s. 88.

istihbarat, planlama sürecinde ve operasyonel personelin ihtiyaçlarının karşılanması doğrultusunda önem arz eden, doğru kullanılması, yönlendirilmesi ve kontrol edilmesi hâlinde kaynakların boşa kullanılmasını engelleyecek bir yöntem çeşididir. Coğrafi istihbarat, araştırılacak ülkenin arazi yapısını, limanlarını ve sahillerini, demir yollarını, kara yollarını, iç su yolu taşımacılığını, hava sahasını, iklimini,[92] haritalamasını, fotografisini, coğrafi alanların isimlerini ve hava hedefi unsurları gibi değişkenleri kapsamaktadır.[93] Bu alanların her birinin incelenip analiz edilmesi ve karşılaşılabilecek olası sorunların çözüme kavuşturulması askerî operasyon sürecinin başarısına doğrudan etki etmektedir.

Buna ek olarak coğrafi istihbarat sadece askerî alanda hizmet sunmamakla beraber birçok farklı istihbarat yönteminde destekleyici unsur olarak kullanılabilmektedir. Örneğin biyografik istihbaratın veri toplama aşamasında doğum yerlerinin tespiti; siyasi istihbaratta uluslararası ve idari sınırlarla ilgili problemler ve bölgelere göre farklılık gösteren seçim sonuçlarının saptanmasında; sosyal istihbaratta yerleşim düzenleri, nüfus dağılımının haritalanması ve etnik ve dinî grupların dağılımında; ekonomik istihbaratta ticaret ve üretim merkezlerinin konumlandırılmasında; bilimsel istihbaratta ise jeofizik, jeololoji, klimatoloji, meteoroloji ve sismoloji gibi bilgilere coğrafi istihbarat aracılığı ile ulaşılmaktadır.[94]

2.4.6. Biyografik İstihbarat

Biyografik istihbarat, hakkında bilgi edinilmesi gereken kişinin profilini çıkartmak amacıyla gerek açık gerek ise kapalı kaynaklardan veri toplama yöntemidir. Bu kişiler devlet liderleri, generaller, komutanlar, politikacılar, casuslar olabileceği gibi organize suç örgütlerinin veya terörist grupların üyeleri veya liderleri, akademisyenler, sanatçılar ve iş adamları da olabilmektedir. Kısacası, gerekli spesifik bilgi doğrultusunda, bilgiyi

---

[92] Her ne kadar iklim değişkeninin coğrafi istihbarat bağlamında zamanla önemini yitirmiş olduğu tartışılsa da 2. Dünya Savaşı'nda Nazi Almanya'sının Rus cephesinde hezeyana uğramasının en büyük sebeplerinden bir tanesini hava koşulları oluşturmaktadır. Bu bağlamda iklim ve hava şartları coğrafi istihbarat açısından son derece etkili bir parametredir.

[93] K.C. Duncan, "Geographic Intelligence", **Center for the Study of Intelligence**, Vol. 3, No. 2, (Çevrimiçi) https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no2/html/v03i2a03p_0001.htm (Erişim tarihi: 20 Mayıs 2020).

[94] CIA, **Geographic Intelligence**, (Çevrimiçi) https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no4/html/v07i4a14p_0001.htm (Erişim tarihi: 20 Mayıs 2020), (Aktaran, Seren, **a.g.e.,** s. 292)

elde edebilme amacı için analiz edilmesi gereken şahsın mevki veya konumu değişkenlik gösterebilmektedir.

Henner Hess'in mafya faaliyetleri ile ilgili yaptığı çalışmada; mafyaların tekel olana kadar dikkat çekmemeye çalıştıklarını fakat buna karşılık polis raporları ve mahkeme kayıtlarının mafyaların hayatından çok işledikleri suçlara odaklandığını belirtmiş, mafya yapılanmasının oluşumunun bir yaşam süresi aldığını ve bu ontolojik gelişimin en iyi şekilde anlaşılmasının bir hayat hikâyesi veya biyografi yoluyla olacağını çünkü mafya oluşumlarının gelişiminde hayatlarının belirli noktalarında belirli süreçlerden geçtiklerini ifade etmiştir.[95] Bu bağlamda biyografik istihbarat, kişi ile ilgili bilgilerin incelenmesinin kişinin ölümüne, etkisiz hâle getirilmesine veya bilgiye artık ihtiyaç duyulmayacağı bir zamana kadar devam eden uzun vadeli bir süreçtir.

Biyografik istihbarat salt belirli bir alana odaklanmaktan ziyade taktik, operasyonel ve stratejik istihbarat çeşitlerinin tamamına bilgi hizmeti sunabilmektedir. Bir komutanın kişilik analizi ile operasyon sürecinde ne gibi manevralar yapabileceğinin öngörülerini yapabileceği gibi bu bir siyasi lider içinde uygulanabilmektedir. Örneğin: Suriye lideri Hafız Esad'ın idrar örneğini çalarak teste tabi tutan MOSSAD'ın, analiz sonuçlarından Hafız Esad'ın hangi ilaçları kullandığını ve ne kadar ömrü kalmış olabileceğini, geriye kalan bu yaşam süresinde Golan Tepeleri hususunda ne yapacağını öngörmeye çalışması biyografik istihbarat örneklerinden bir tanesidir.[96] Lider analizleri bağlamında son derece etkili hizmet sunan biyografik istihbaratın önemi günden güne artmaktadır. Fidel Castro'nun 1959 yıllarında kendisini milliyetçi olarak tanımlaması hatta ABD'de miting dahi yapmış olmasının ardından komünist söylemler ile Küba'yı Sovyet tarzı bir sosyalizme çevireceğini belirtmesi, ABD'nin biyografik istihbarat açısından zayıf kalması ve Castro'nun niyetlerini önceden öngörememelerinden kaynaklı olarak müdahalesini geciktirmiştir.[97]

Biyografik istihbarat çerçevesinde toplanacak bilgiler kapalı kaynaklardan olduğu gibi açık kaynaklardan da elde edilebilmektedir. Açık kaynaklardan yapılacak istihbaratın ilk aşaması -var ise- daha önceden yayınlanmış biyografilerin temin edilmesi ve

---

[95] Henner Hess, **Mafia & Mafiosi Origin, Power and Myth**, Avustralya: Crawford House Publishing, 1998, s. 48.

[96] Özdağ, **a.g.e.,** s. 104-105.

[97] Bruce W. Watson, Intelligence, **Encyclopedia Britannica**, 2012, (Çevrimiçi) https://www.britannica.com/topic/intelligence-military (Erişim tarihi: 21 Mayıs 2020).

incelenmesidir. Sonraki adım ise açık kaynaklardan elde edilen bilgilerin önceden hazırlanmış biyografiye işlenmesidir. Biyografik istihbarat formu oluştururken bir devlet başkanın, generalin veya mafya liderinin gereken temel bilgileri pek farklılık göstermemektedir. Aşağıda ayrıntıya girmeyi hedeflemeyen bir biyografik istihbarat formu örnek olarak hazırlanmıştır:[98]

[98] Özdağ, **a.g.e.,** s. 104.

Tablo 1: Örnek Biyografik İstihbarat Formu

Adı	
Soyadı	
Anne-Baba adı	
Doğum yeri ve yılı	
Boyu, kilosu	
Seç ve ten rengi	
Hangi vatandaşlığı taşıdığı	
Etnik ve dinî/mezhepsel kimliği	
Aşiret/kan mensubiyeti (varsa)	
Eğitimi	
İdeolojik geçmişi ve konumu	
Mensup olduğu siyasal parti, dernek ve gruplar	
Cinsel eğilim ve seks yaşamı	
Psikolojik durumu	
Geçirdiği kazalar	
Geçirdiği hastalıklar	
Kalıcı hastalığı var mı?	
Yabancı servislerle ilişkisi var mı?	
Yakın çevresindeki şahsiyetler	
Okuduğu Gazeteler	
En çok sevdiği yazar	
Hobileri	
Fobileri	

Kaynak: Ümit Özdağ, İstihbarat Teorisi, Ankara: Kripto Kitaplar, 2014, s. 104.

Ayrıca siyaset bilimi, siyasi tarih, uluslararası ilişkiler, sosyoloji, psikoloji ve tarih gibi farklı disiplin dallarında yapılan akademik çalışmalarında, biyografik istihbarat açısından kapsamlı ve detaylı bilgiler barındıran önemli açık kaynaklar olduğu göz önünde bulundurulmalıdır. D. N. Verkhoturov'un "Atambayev'in Gölgesi Altında Kırgızistan", Yael S. Aronoff'un "İsrail Başbakanlarının Politik Psikolojisi: Muhafazakârların Barışa Karar Kıldıkları Zaman" ile Guy Ziv'in "Şahinler Neden Güvercin Oldular: Peres ve İsrail Dış Politikasının Değişimi" başlıklı eserler örnek olarak gösterilebilir.[99]

2.4.7. Ulaşım ve İletişim İstihbaratı

Ulaşım istihbaratı, ülkelerin kara yolları, demir yolları, deniz yolları, limanları ve hava sahası gibi ulaşım yollarına dair bilgilerle ilgilenen istihbarat çeşididir. Barış zamanlarda sivil ve ticari güvenlik önlemleri çerçevesinde kullanılan ulaşım istihbaratı, savaş zamanında ise operasyon alanlarına lojistik destek sağlama amaçlı veya düşman hedefin ikmal noktalarını, lojistik imkânlarını tespit etme amacıyla kullanılmaktadır.

Soğuk Savaş Dönemi'nde ABD kongresinin kararıyla 1966 yılında kurulup 1967 yılında göreve başlayan DOT (Department of Transportation), ekonomik, çevresel ve ulusal güvenlik ihtiyaçları çerçevesinde, verimli ulusal ulaşım sistemleri sağlama amacıyla politikalar geliştirip uygulamayı hedeflemektedir. Kara yolları ve demir yollarının yanı sıra, 11 Eylül 2001 terörist saldırılarından sonra sahil güvenlik ve hava güvenliğini sağlamakla görevli TSA (Transportation Security Administration) birimi de DOT'un bünyesinde bulunan birimlerden bir tanesidir.[100] TSA'nın bu bağlamda İstihbarat servislerinin ulaşım güvenliği hususunda ihtiyacı olan bilgileri toplama ve imkânlar dâhilinde analiz edip istihbarat servisleriyle paylaşma yetkisi bulunmaktadır.

İletişim istihbaratı ise radyo, televizyon, telefon, telgraf, denizaltı kablo ve ilgili iletişim medyası da dâhil olmak üzere, sivil ve askerî iletişim merkezi ve sistemlerine yönelik olarak yapılan istihbarat çeşididir.[101] Yine savaş ve barış zamanında ulusal tehdit oluşturabilecek faaliyetleri tespit etme ve önleme amacı güden iletişim istihbaratın,

---

[99] Seren, **a.g.e.,** s. 294.

[100] K. Lee Lerner and Brenda Wilmoth Lerner, **Encyclopedia of Espionage, Intelligence and Security Vol III**, Detroit: Thomson Gale, 2004, s. 168.

[101] Özdağ, **a.g.e.,** s. 106.

teknolojik gelişmeler sonucunda kullanılan araçların çeşitlenmesi ile (internet, uzay ve uydu teknolojisi vb.) faaliyet alanı genişlemiştir.[102]

2.4.8. Bilimsel ve Teknik İstihbarat

Bilimsel ve teknik istihbarat, bir ülkenin bilim ve mühendislik kapasitesi ile ilgili bilgileri kapsayan istihbarat çeşididir. İstihbarat toplama araçları bilimsel ve teknolojik gelişmelerden büyük ölçüde etkilenmiştir ve etkilenmektedir. Bilimsel ve teknik alanlardaki bilgiler sadece devletlerin değil özel firmaların da vazgeçilmez kaynaklarındandır. Çalışmanın başında da belirtildiği gibi bilgiyi kontrol etmek gücü kontrol etmek demektir. Bu bağlamda bir ülkenin veyahut özel bir firmanın hangi teknolojiye sahip olduğu, hangi projelere imza atacağı, AR-GE çalışmaları ve bu çalışmalara ayırdığı bütçenin miktarı gibi veriler son derece önem arz etmektedir. Türkiye'nin 2019 yılında yerli elektrikli otomobil projesinin tanıtılması ve 2021 yılında fabrika açılısının yapılıp ilk serinin 2022 yılında tamamlanacağını duyurması üzerine Almanya menşeli Volkswagen firmasının 2025 yılına kadar 1 milyon elektrikli araç üretme hedefini 2023 yılına çekme kararı bilimsel ve teknik istihbarat örneklerinden bir tanesidir.[103]

II. Dünya Savaşı döneminde, Almanların Fransız topraklarının Normandiya bölgesinde bulunan Bruneval lokasyonuna kurdukları radar istasyonuna yapılan operasyon bilimsel ve teknik istihbarat açısından mükemmel örneklerden bir tanesidir. Keşif uçaklarının görüntü istihbarat yöntemi ile elde ettikleri fotoğraflardan bölgede Almanya'nın hâlihazırda keşfedilmiş radarlarının dışında başka bir ekipmanın daha fark edilmesi üzerine, İngiliz bilim insanları bu istasyonlardan bir tanesine operasyon yapılmasını ve içeride saklanan teknolojiyi analiz edip anlayabilmek adına radarın bazı parçalarının getirilmesini talep etmiştir. Bu talep üzerine yapılan kısa eğitimler sonucunda bölgeye bir paraşüt çıkartması yapan İngiliz birliği, istasyona başarıyla girip ekipteki teknisyenler sayesinde radarları inaktif duruma getirerek istenilen parçaları istasyondan esir aldıkları bir Alman teknisyen ile beraber geri getirmeyi başarmışlardır. Operasyonun başarısı, sistemi daha iyi çözümleyebilmek adına getirilen Alman

---

[102] Seren, **a.g.e.,** s. 299.

[103] Faruk Can, Volkswagen 1 Milyon Elektrikli Araç Hedefini İki Yıl Erkene Aldı, **Euronews**, 2019, (Çevrimiçi) https://tr.euronews.com/2019/12/27/volkswagen-1-milyon-elektrikli-araci-hedefini-iki-yil-erkene-aldi (Erişim tarihi: 24 Mayıs 2020).

teknisyen ile beraber İngiliz bilim insanlarının düşman birliklerinin radar teknoloji potansiyelini anlayıp önlem alabilmelerine olanak sağlamıştır.[104]

XXI. yüzyılda ise artan biyolojik hastalıkların sonuncusu olarak 2019 yılının sonlarında Çin'in Vuhan kentinde ortaya çıkan Covid-19 virüsü günümüz tarihi: 5 Mayıs 2021 itibari ile dünya genelinde 154,4 milyon vakaya ve 3,2 milyon kişinin ölümüne sebep olmuştur.[105] Daha öncesinde yine bir Korona Virüs çeşidi olarak ortaya çıkan SARS, H1N1 ve H5N1 virüsleri gibi Covid-19 virüsü de birçok tartışmayı beraberinde getirmiştir. Dönemin ABD başkanı Donald Trump'un virüsü "Çin Virüsü" olarak lanse etmesi ve ABD'nin virüsün Çin tarafından kasıtlı olarak yapıldığını ve Vuhan kentinde bulunan Viroloji Enstitüsünü işaret ederek WHO'ya yapılan ödeneği kesmesi birçok kesim tarafından tepki çekmekle beraber bir o kadar kesim tarafından da desteklenmiştir. Her ne kadar ABD Ulusal İstihbarat Direktörlüğünün, "Covid-19'un insan eliyle üretilmiş ya da genetiğiyle oynanmış bir virüs olmadığını saptadık." açıklaması virüsü Çin'in yaptığına dair komplo teorilerini çürütmüş olsa da hâlâ virüsün kaynağı ve akıbeti bilinmemekle beraber özellikle XXI. yüzyılda artış gösteren biyolojik tehditlerin bilimsel ve teknik istihbaratın önemini ve ihtiyacını bir kez daha göstermektedir.[106]

Bu bağlamda günümüz güvenlik tehditlerinden bir tanesini de akıllı arabalar oluşturmaktadır. Yeni nesil arabalara entegre edilen sürücü destek sistemleri, otomatik pilot özellikleri gibi yenilikler, siyasi liderlerin akıllı araba yazılımlarının *hack*lenmesi ile suikasta uğrama tehdidini doğurmaktadır. Bu tehdit sadece istihbarat servisleri ve özel firmalar için önem arz etmemekle beraber teknoloji ve IT şirketlerini de derinden ilgilendirmektedir. Dünyanın önde gelen Telekom firmalarından "Deutche Telekom"un alt şirketi olan T-Systems, bu tehdit karşısında teknisyen ekiplerine beyaz şapkalı *hacker*ları da dâhil etmeye başlamıştır. Bu çerçevede büyük çaplı AR-GE çalışmaları ile beyaz şapkalı *hacker*lardan arabaların sistemine sızıp nasıl bir tehdit ile karşı karşıya olunduğunu anlamaya çalışan güvenlik şirketleri, araç sistemine sızılarak, arabaların

---

[104] CIA, "Scientific Intelligence", **Studies Archiev Indexes**, Vol 6, No. 3, (8 Mayıs 2007), (Çevrimiçi) https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no3/html/v06i3a05p_0001.htm (Erişim tarihi: 24 Mayıs 2020).

[105] Google İstatistik, (Çevrimiçi) https://news.google.com/covid19/map?hl=tr&gl=TR&ceid=TR%3Atr (Erişim tarihi: 05 Mayıs 2021).

[106] CNN, Koronavirüs 'Çin'de bir laboratuvarda üretildiği 'iddiaları: Kim, ne dedi?, 2020, (Çevrimiçi) https://www.bbc.com/turkce/haberler-dunya-52596250 (Erişim tarihi: 24 Mayıs 2020).

direksiyonunun kitlenip, araçların şarampolden yuvarlanabileceğini tespit etmiş olup bu tehdide karşı ciddi önlem çalışmalarına başlamışlardır.[107]

2.4.9. Siber İstihbarat

Enformasyon çağının teknolojik gelişmelerinden bir tanesi olan internet, bilgi akışının hızlılığı, serbestliği ve özellikle ilk dönemlerindeki denetlenme eksikliğinden ötürü güvenlik, akabinde strateji kavramlarına yeni bir alan olarak dâhil olmuştur. Bilgiyi kontrol etmenin gücü elde tutmak anlamına geldiği enformasyon çağında, kişisel yazışmaların, devlet veri tabanlarının, arşivlerin, banka hesap bilgilerinin ve daha birçok kritik verinin dijitalleşmesi ile siber âlemin güvenliği yeni bir sorunsal hâline gelmiştir. Sonuç olarak hem güvenlik bağlamında bu yeni tehdit unsuruna karşılık hem de strateji bağlamında yeni bir veri toplama merkezi olarak siber istihbarat kavramı ortaya çıkmıştır. Farklı şekillerde kullanılan siber istihbarat yöntemi sadece açık kaynaklardan yararlanmamakla beraber *hack* ve sızma eylemleriyle kapalı kaynaklardan da yararlanmayı öngörmektedir.[108] Genel anlamda istihbarat etiğinden bahsetmek bile yürütülen faaliyetin amacına ve büyüklüğüne göre ciddi tartışmalara sebebiyet verirken, siber âlemde istihbarat servislerinin sadece açık kaynaklardan yararlanmasını beklemek de bir o kadar tartışmaya açık olacaktır. Devlet karar vericilerine, tehdidin boyutuna göre sadece bilgi akışı sağlamakla kalmayıp aynı zamanda psikolojik harekâtlar ve propaganda faaliyetleri gibi örtülü operasyonlarda siber uzayda yapılan faaliyetler arasındadır.[109]

Siber istihbarat yöntemini kullanan devletin elinde bulundurduğu imkânlar dâhilinde etkisinin daha fazla olmasının yanı sıra, 21. yüzyılda devletlerin askeriye de dâhil olmak üzere birçok kritik kolunun siber sistemlere geçmesi ile beraber birçok devletin bu yönteme başvurması siber savaş kavramını meydana getirmiştir. Harp bu boyuta da taşınmış ve sanıldığının aksine buradaki etkisi devletler açısından çok daha büyük

---

[107] Yeni Çağ Gazetesi, Siber Saldırıların Yeni Hedefi "Bağlı Arabalar", 2019, (Çevrimiçi) https://www.yenicaggazetesi.com.tr/siber-saldirilarin-yeni-hedefi-bagli-arabalar-247079h.htm (Erişim tarihi: 24 Mayıs 2020).

[108] James A. Lewis, Assesing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Washington DC, Center for Strategic and International Studies, (December, 2002), s. 9, (Çevrimiçi) https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (Erişim tarihi: 15 Kasım 2020).

[109] Gökhan Bayraktar, Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat, Güvenlik Stratejileri, 2014, C. 10, S. 20, s. 130.

olmaktadır. Bu çerçevede devletler sadece kendi personelleri ile faaliyetler yürütmekle kalmayıp "beyaz şapkalı *hacker*ları da" devşirmeye başlamışlardır.[110]

2.5. Açık Kaynak İstihbaratı (OSINT)

Açık kaynak istihbaratı (OSINT), herkese açık kaynaklardan erişilebilecek ham verilerin toplanması, sınıflandırılması, kıymetlendirilmesi ve analiz edilmesi gibi işlemlerden geçirilerek istihbarat bilgisi elde etmeyi amaçlayan bir disiplindir.[111] Bu noktada istihbarat bilgisinin normal veri veya bilgiden ayırt edilmesi önemlidir. Herkesin açık kaynaklardan rahatlıkla elde edebileceği veriler belirli aşamalardan geçmediği müddetçe istihbarat bilgisi olarak kullanılamamaktadır. Açık kaynaklar kısaca, gazeteler, dergiler, ansiklopediler, televizyon ve radyo yayınları olabileceği gibi günümüzde en çok kullanılan internet ve sosyal medya platformları da birer açık kaynaktır.[112]

11 Eylül saldırılarına kadar istihbarat birimleri açık kaynakları ellerinde bulunan bilgilere tamamlayıcı bir unsur olarak kullanmaktaydı. Fakat 11 Eylül saldırılarından sonra güvenlik ve istihbarat metodoloji gibi dönüşüme uğrayan birçok kavram gibi açık kaynakların sistematik olarak kullanılmasına karşı da yeni bir bakış açısı gelişmiştir. Özellikle internet üzerinden veri madenciliği ile cihatçı grupların para ve üye toplamak gibi faaliyetlerinde haber siteleri, sohbet odaları, sosyal ağ siteleri gibi platformları etkin bir biçimde kullandıklarının öğrenilmesi açık kaynakların önemini bir kez daha göstermiştir.[113]

Bazı zümreler OSINT'in açık kaynaklardan elde etmeyi öngördüğü bilgilerin gizlice toplanmamasından dolayı bir istihbarat yöntemi olmadığını savunurken, Mark Lowenthal, OSINT'in farklı bir disiplin olmadığını, bunun aksine diğer istihbarat yöntemlerinin bir yüzü olduğunu ifade etmiştir.[114] Benzer şekilde Stephen C. Mercado'da, OSINT'in insani istihbarat (HUMINT), görüntü istihbarat (IMINT) ve

---

[110] Sevgi Ceren Gökkoyun ve Sefa Şengül, Siber Âlemin Muhafızları: Beyaz Şapkalı Hackerlar, Anadolu Ajansı, Ankara, 2019, (Çevrimiçi) https://www.aa.com.tr/tr/bilim-teknoloji/siber-alemin-muhafizlari-beyaz-sapkali-hackerlar/1417719 (Erişim tarihi: 15 Kasım 2020).

[111] Dokman Tomislav and Ivanjko TOMISLAV, Open Source Intelligence (OSINT): Issues and Trends, **INFuture2019: Knowledge in the Digital Age**, 2020, No. 23, p. 1.

[112] Girdin**, a.g.e.,** s. 417.

[113] Prunckun, **a.g.e.,** s. 74.

[114] Mark Lowenthal, "OSINT: The State of the Art, the Artless State", **Studies in Intelligence**, 2001, Vol. 45, No. 3, p. 63.

sinyal istihbarat (SIGINT) gibi kapalı faaliyetlerin açık yüzü olduğunu savunmuştur.[115] İstihbarat disiplinlerinin nasıl tanımlandığı önemli konulardan bir tanesidir. Çünkü yapılan tanım istihbarat servisinin süreci nasıl sürdüreceğini göstermektedir. Lowenthal ve Mercado'nun tanımları bu noktada yanlış bir tespit yapmamaktadır. İstihbarat yöntemlerinin birbirinden tamamen bağımsız olduğu durumlar çok nadirdir. Örneğin, coğrafi istihbarat (GEOINT), günümüzde ticari uyduların kullanımının artması -hatta ücretli veya ücretsiz şekilde açık kaynaktan elde edilebilecek görüntüler sunması- ile bu disiplinin aynı zamanda OSINT olabileceğini, sosyal medya verilerinin yapay zekâ algoritmaları ve teknik araçlarla toplanarak işlenmesinin sinyal istihbaratının (SIGINT), bireyler ve kitleler hakkında veri elde edilmesinin de insani istihbaratın (HUMINT) bir çeşit OSINT olduğunu göstermektedir.[116]

Bu bağlamda açık kaynak istihbaratının uygulanmasında mevcut dört aşama bulunmaktadır. Bunlar; toplama, işleme, analiz ve üretimdir. Toplama aşaması istihbarat birimlerinin işine yarayabilecek potansiyel verilerin tanımlanmasını, toplanmasını ve arşivlenmesini öngörmektedir. Bu toplama işlemi fiziksel olabileceği gibi elektronik olarak da gerçekleştirilebilir. Önceleri açık kaynak verilerinin toplanması için fiziksel olarak bir personelin bu işlemi yapması gerekirken, internet ve sosyal medya gibi günümüz imkânları çoğu açık kaynak verinin çevrimiçi olarak erişilebilmesine imkân tanımaktadır. İkinci aşama işlenme ise verilerin doğrulanmasını ve kullanılabilir hâle getirilmesini içermektedir. Doğrulama diğer istihbarat disiplinlerine başvurarak yapılabilirken, verilerin kullanılabilir hâle getirilmesi orijinal dillerinden çevirisini veya görsel nitelikte olan verilerin kullanılabilir bilgiye dönüştürülmesini kapsamaktadır. [117]

Analiz aşaması bu aşamaya getirilen verilerin ne anlama geldiğinin ve istihbarat birimlerinin ihtiyaçları doğrultusunda ne gibi değeri olduğunu belirlemeye çalışmaktadır. Arthur Hulnick, OSINT verilerinin kullanımında karşılaşılan en büyük zorluklardan bir tanesinin, kamuya açık olan bu büyük hacimli verilerin güvenilirlik derecelerinin belirlenmesi olduğunu ifade etmiş, OSINT verilerinin analizi sırasında

---

[115] Stephen C. Mercado, "Sailing the Sea of OSINT in the Information Age", **Studies in Intelligence**, 2004, Vol. 48, No. 3, s. 3.

[116] Heather J Williams. and Ilana Blum, **Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise,** Santa Monica California: RAND Corporation, 2018, s. 7-8

[117] Williams, Blum, **a.g.e.,** pp. 14-15.

"iyi" ve "kötü" bilginin ayırt edilmesine ciddi mesailer harcanması gerektiğinin altını çizmiştir.[118] Son aşama üretim ise geleneksel modeldeki bilginin kullanılabilir bir şekilde karar vericilere/tüketiciye sunulduğu aşamadır.

Günümüz şartlarında bilginin kullanımı, yayımı hatta muhafazası için dahi dijital ortamların kullanılması, açık kaynak istihbaratının potansiyel veri toplama kabiliyetini yüksek düzeyde arttırmıştır. Sadece kişi veya kitleler hakkında değil devletlerin açık kaynaklardan yayınladıkları politikalar veya askerî raporlar ile veri yelpazesi genişlemiştir. Yakın tarihte (II. Dünya Savaşı dönemleri vb. gibi) radyo yayınları gibi kaynaklardan hedef ülkelerin politikaları konusunda ciddi stratejik çıkarımlar elde edilmesine olanak sağlayan açık kaynak istihbaratı, günümüzde internet ve sosyal ve medyanın yaygınlaşması ile daha da önemli bir konuma gelmiştir. İnternetteki birçok hizmetin ve sosyal medya platformlarının kâr amacı güden kuruluşlar olduğunu göz önünde bulundurduğumuzda ortaya çıkan bu rekabet ortamı veri potansiyelindeki çeşitliliğide beraberinde getirmiştir. Örneğin; Bir arama motoru olarak başlayan Google şirketi, Google Earth gibi açık kaynaktan coğrafi konumlara erişim sağlayan, yapay zekâ projeleri geliştiren bir şirket haline gelmiştir. Bunun yanı sıra devletlerin ciddi bütçeler ayırıp taktik amaçlarla görüntü alabilmesini sağlayan uyduların kâr amaçlı şirketler tarafından da kullanılıp belirli ücretler karşılığında kullanıcılara uydu görüntüsü alma imkânı sunduğu görülmektedir.[119]

Sonuç olarak açık kaynak istihbaratı ile kaynaklar daha sınırlı kullanılarak "tamamlayıcı" özellikte veriler elde edilebilmektedir. Diğer veri toplama yöntemlerinin eksik kaldığı durumlarda OSINT verileri devreye girebilir, ucuz maliyeti ve verileri ulaşımın daha kolay olması sebebiyle tercih edilebilir fakat elde edilecek veriler işlevsel potansiyelleri yüksek olsa dahi hem teyit edilmeye muhtaç verilerdir hem de istihbarat faaliyetlerinin ana hedeflerinden bir tanesi olan "mahrem bilgiye ulaşma" amacı OSINT faaliyetleri ile etkin biçimde elde edilememektedir.

---

[118] Arthur S. Hulnick, "The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?", **The Oxford Handbook of National Security Intelligence** içinde, New York: Oxford University Press, 2010

[119] Bkz. https://www.planet.com – https:/www.dynacrop.space -

3. SOSYAL MEDYA VE İSTİHBARAT

3.1. Web 1.0 – Web 2.0 Kavramları

Teknolojik gelişmelerin sürekli olarak gelişerek geçmiş olduğu evrelerin bir benzeri internet ürününde de yaşanmıştır. Web 1.0 dönemi olarak adlandırılan 1990 yıllarda internetin karakteristik özellikleri daha çok geleneksel medyayı anımsatmaktadır. Statik, katılımın sınırlı olduğu, kullanıcıların uzmanların veya programcıların hazırladığı web siteler ile etkileşime girdiği bir sistem olarak karşımıza çıkmıştır. Fakat değişen dünya standartlarını karşılamakta yetersiz olan web 1.0 dönemi, yerini web. 2.0 dönemine bırakmıştır. Statik web sitelerinden oluşan web 1.0'ın aksine web 2.0 daha dinamik ve çok katılımlı bir ortam sunmaktadır. 20 yıl öncesinde internette bir içerik paylaşmak isteyen bir kullanıcının asgari düzeyde programlama ve grafik yeteneklerine, paylaşacağı içeriği yükleme için FTP yazılımına ve bunları yapabilecek bir sunucuya ihtiyacı varken günümüzde teknik bilgilere hâkim olmayan kişilerin sadece sosyal medya platformlarında profil oluşturarak yüzbinlerce insanla düşüncelerini paylaştığı, görsel içerikleri paylaştığı görülmektedir.[120]

Web 2.0 kavramı ilk olarak Ekim 2004 yılında bir konferansta kullanılmıştır. Burada web 2.0 ilk ilkesi "platform olarak web" şeklinde belirtilmiştir. Web 2.0'ın özetle amaçladığı şey aslında bu cümleden ibarettir. İnterneti bir köprü olarak kullanıp, kullanıcıların içeriklerle etkileşime girerek yeni sitelere ulaşmasını veya yeni sitelere katıldıkça farklı insanlar ile etkileşime girmesini sağlamaktadır. Sosyal medya platformları, iletişim araçları, *viki*ler, *online* anket ve *quiz*ler gibi araçlarla kullanıcıların birbirleriyle olan etkileşimleri ile ortaya çıkan sistemi tanımlamaktadır. [121] Küreselleşmenin meydana getirdiği ihtiyaçları web 1.0'ın karşılayamaması ile ortaya çıkan web 2.0 dönemi, 15 yıllık bir süreç içerisinde muazzam derecede gelişmiş ve

[120] Jane Bozarth, **Social Media for Trainers – Techniques for Enhancing and Extending Learning**, San Francisco CA: Pfeiffer, 2010, s. 11-13.

[121] Tim O'Reilly, What is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software, Oreilly.com, 2005, (Çevrimiçi) https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1 (Erişim tarihi: 26 Nisan 2021).

günümüzde *Facebook, Twitter, Instagram, YouTube* gibi milyarca dolar sermayesi olan büyük sosyal ağ şirketlerini karşımıza çıkarmıştır.

Günümüzde konuşulan bir başka kavram ise web 3.0'dır. Web'in kısa bir tarihine bakacak olursak, verilerin statik olarak sunulduğu web 1.0'dan kullanıcıların verilerle daha dinamik etkileşimlerde bulunabildiği web 2.0 dönemine geçilmiştir. Günümüzde temeli yavaş yavaş atılmaya başlanan web 3.0 dönemi ise büyük oranda yapay zekâ ve makine öğrenmesi üzerine kurulu bir internet teknolojisidir. Makine öğrenmesi ve yapay zekâ algoritmaları ile kullanıcılara hitap eden kişiselleştirilmiş içerikleri daha hızlı bir şekilde sunmayı amaçlamaktadır. Henüz tam olarak tanımlanmış olmasa da birçok alanda kullanılmaya *blockchain* teknolojisi, büyük veri analizleri yapan algoritmalar ve makine öğrenimi web 3.0 döneminin zeminini hazırlamaktadır.[122]

3.2. Sosyal Medya Kavramı

Günümüzde rahatlıkla erişim sağlayıp veri paylaşımı yapabildiğimiz sosyal medya platformları için siber âlemin en gözde ürünüdür diyebiliriz. Her ne kadar yakın tarihte ortaya çıktığı sanılsa da aslında internetin orijini Soğuk Savaş dönemine dayanmaktadır. Soğuk Savaş dönemi iki süper gücün arasındaki silahlanma yarışının yanı sıra aynı zamanda bilim ve teknoloji yarışı özelliği de taşımaktadır ve internetin doğuşuna bu rekabet ortamı olanak sağlamıştır. SSCB'nin 4 Ekim 1957 yılında Sputnik-1 uydusunu uzaya göndermesiyle iki süper güç arasındaki yarış daha da kızışmış ve hamle yapma sırası doğal olarak ABD'ye geçmiştir. ABD Savunma Bakanlığının bir kolu olan DARPA, 1969 yılında paket iletim sistemini geliştirerek ARPANET projesini hayata geçirmiştir.[123] Bilginin taşınması, paylaşılması ve muhafazası bağlamında geleneksel yöntemlerden sıyrılarak siber alanı kullanmayı öngören ARPANET projesi tek merkez kullanmaktan ziyade farklı noktalarda çok merkezli bir sistem üzerine inşa edilip herhangi bir noktanın saldırıya maruz kalması durumunda sistemin aksamadan devam etmesini engellemeyi amaçlamaktaydı. Bu yüzden günümüzde internetin çok merkezli bir yapıya sahip olmasının nedeni internetin ilk kurulduğu bu dönemlerde siber

---

[122] Binance Academy, **İnternetin Evrimi - Web 3.0 Nedir?,** 2021, (Çevrimiçi) https://academy.binance.com/tr/articles/the-evolution-of-the-internet-web-3-0-explained (Erişim tarihi 26 Nisan 2021).

[123] İTÜBİDB, **İnternet'in Tarihçesi**, 07 Eylül 2013, (Çevrimiçi) https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet%27in-tarih%C3%A7esi (Erişim tarihi: 11 Ekim 2020).

güvenlik tehditlerinden ziyade fiziki güvenlik düşünülerek hareket edilmesinden kaynaklanmaktadır.[124]

İnternetin varlığı 1969 yılına dayansa da bireysel kullanıcılara açılması 1989 yılında İngiliz bilim insanı Tim Berners-Lee tarafından World Wide Web'in yani WWW uzantısının icadıyla gerçekleşmiştir. 1991 yılında bu icadın tanıtılmasıyla internet artık bireylerin bilgisayarlarında bulunan internet tarayıcıları aracılığıyla erişim sağlayabileceği global bir ağ hâline gelmiştir.[125] Topluma arz edilmesiyle pozitif anlamda eğlence ve ticaret mecrasına, negatif anlamda ise hızlı gelişimi ve denetlenme sorunlarından kaynaklı olarak beraberinde ciddi tehditleri getirecek olan internetin, bölümün başında belirtildiği üzere son yıllarda en çok ilgi gören ürünü ise sosyal medya platformları olmuştur.

Geleneksel medyaya alternatif olarak kullanılmaya başlayıp hızla popülarite kazanan, birçok iletişim uzmanı tarafından "Yeni Medya" olarak adlandırılan sosyal medyanın tanımlaması ise A. Kazım Kirtiş ve Filiz Karahan tarafından; "Kabaca, internet kullanıcılarının birbirleriyle çevrimiçi etkileşimde bulundukları ve *blog*lar oluşturup, oluşturulan bu *blog*lara yorum yapma, içerik paylaşma veya *Facebook*, *MySpace* gibi sosyal ağ siteleri aracılığıyla arkadaşlarla iletişim kurma gibi etkinlikleri içeren farklı yolları ifade etmektedir." şeklinde açıklanmıştır.[126]

Sosyal medya hakkında net bir çıkış tarihi verilememesinin yanı sıra, gelişen iletişim imkânları ve teknolojiye paralel olarak farklı platformlarda farklı içerikler sunarak karşımıza çıkmakta olduğu görülmektedir. Başlangıçta eğlence ve ticari imkânlarla popüler olmayı başaran sosyal medya, günden güne kullanıcı sayısının, pazar hacmi ve rekabetin artması ile devasa bir bilgi ve iletişim sistemine evirilmiştir. Örneğin *Instagram* platformunda sadece resim, video, hikâye ve e-ticaret hizmetleri sunulurken, aynı firmanın sahibi olduğu bir başka platform *Facebook*'ta bu özelliklerin yanı sıra yazı, durum vb. özellikler bulunmakta, buna karşılık kullanıcı sayısı ve elde ettikleri

---

[124] Nezir Akyeşilmen, **Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik**, Ankara: Orion Kitabevi, 2018, s. 26.

[125] SIU, "A Brief History of IT", **IT Computer Technical Support Newsletter**, 2016, Vol. 2, No. 29, (Çevrimiçi) https://ehs.siu.edu/_common/documents/IT%20newsletter/vol-2-no-29.pdf (Erişim tarihi: 11 Ekim 2020) .

[126] A. Kazım Kirtiş ve Filiz Karahan, "To Be or Not To Be in Social Media Arena as the Most Cost-Efficient Marketing Strategy after the Global Recession", **Procedia Social and Behavioral Sciences**, 2011, Vol. 24, s. 262.

gelir birbirleri ile rekabet edebilecek düzeydedir. Her ne kadar tek tek incelenemeyecek kadar fazla sosyal medya platformu bulunsa da markalaşmış ve dünya çapında ciddi kullanıcı sayısına ulaşmış platformları ve sosyal medya platformlarının çeşitlerinin incelenmesi ve sonucunda farklılıkları ile benzerliklerinin tahlil edilmesinde fayda bulunmaktadır.

3.2.1. Sosyal Medya Platformları

3.2.1.1. Bloglar

Basit anlamda *blog*lar genellikle *blog* yazarının ilgisini çeken, uzmanlık alanı olan veya hayal gücünü kapsayan, belirli periyotlarla, kısa ve düzenli olarak güncellenen web sayfalarını temsil etmektedir. *Blog*lar özellikle 1990'ların sonlarına doğru *blog* sayfalarının kullanımının artış göstermesiyle beraber dergiler ve web günlükler olarak da yaygınlaşmaya başlamıştır. Genellikle belli kategorileri bulunan ve okurların dikkatini bu şekilde spesifik konular hakkında yazılan yazılara çekmeyi öngören *blog*ların konuları zamanla çok daha geniş bir yelpazeyi içerecek kadar genişlemiştir.[127] Bunun yanı sıra okurların *blog*larda bulunan yazılara veya fotoğraflara yorum yaparak geri bildirimde bulunabilmesi ise ilerleyen süreçte kurumsal *blog*ların ortaya çıkmasına uygun ortamı hazırlamıştır.

3.2.1.2. Forumlar

Forum, internete bağlı kullanıcıların, çeşitli konular çerçevesinde tartışabildikleri alanlardır. Sohbet (IRC, chat) odalarından farkı bu alanlarda insanların fikirlerini birbirlerine farklı zamanlarda iletebilmeleridir.[128] Her ne kadar aralarında üyelik istemeyen forum siteleri bulunsada, forum sitelerinin çoğunluğunda üyelik sistemi mevcuttur ve üye olduktan sonra kendinize bir *nickname* (takma isim) belirleyip forum sitesi içinde açılan başlıklara belirlemiş olduğunuz bu lakap ile katılım gösterirsiniz. Tabii ki kullanıcıların internet gibi bir alanda takma isimle katılım gösterdiği bir platformda oluşabilecek kaosu engellemek için *admin*, *co-admin* veya moderatörler gibi görevli kişiler bulunmaktadır. Çünkü her forum sitesinin kendi içinde belirlemiş olduğu bazı kuralları vardır ve üyeler bu kuralların dışında çıktığında yetkililer tarafından süreli veya süresiz olarak uzaklaştırılabilir. Forumlarda *blog*larda olduğundan daha farklı bir

---

[127] Steve Jones, **Encyclopedia of New Media: An Essential Reference to Communication and Technology**, Thousand Oaks, CA: SAGE Publications, 2003, s. 33.

[128] Hamza Çakır ve Hakan Topçu, "Bir İletişim Dili Olarak İnternet", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 2005, C. 1, S. 19, s. 93.

kategori sistemi mevcuttur. Siyasi konular ile alakalı bir *blog*a girdiğinizde sadece bu konudaki içeriklere ulaşabiliyorken, forum sitesinden her konunun ayrı bir başlığı bulunmaktadır. Üyeler içerik eklemek veya hâlihazırda eklenmiş içerikler ile etkileşime girmek için bu başlıkları ziyaret edebilmektedir. Benzer veya aynı içerik paylaşılması durumunda, site içindeki kirliliği engellemek için yine görevli kişiler başlığı kaldırabilir veya yanlış bir konu altında açılmış ise açılan bu başlığı doğru kategorinin altına taşıyabilmektedir. Böylelikle minimal düzeyde bir kontrol mekanizması ile üyelerin birbirleri ile etkileşime girebileceği ve bilgi alışverişi yapabileceği bir platform sağlanmış olmaktadır.

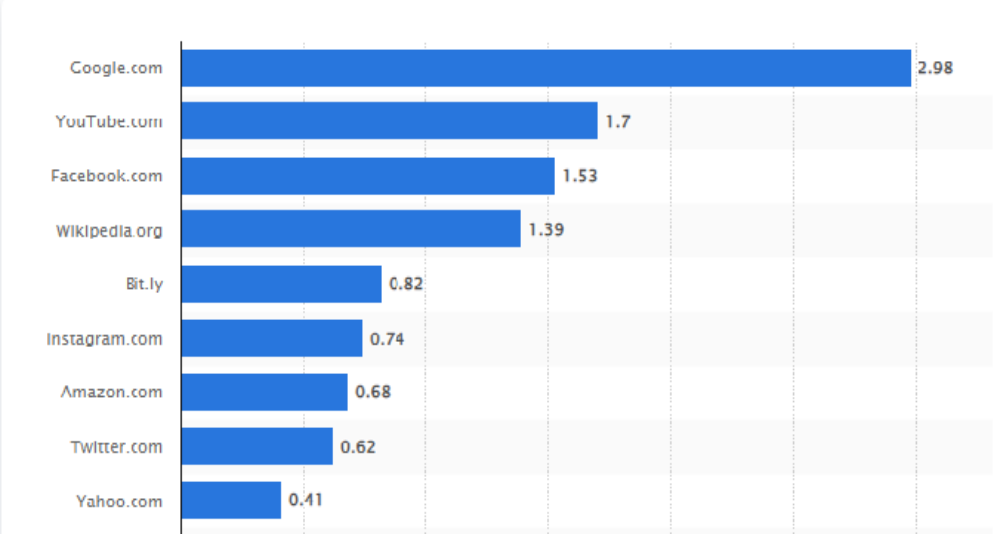
3.2.1.3. Ansiklopediler

Bilgiye ulaşmak için geleneksel yöntemlerden birisi olan ansiklopedi ve sözlükler, neredeyse her dönem insanların merak ettiği konulara dair kapsamlı bilgilere ulaşabildikleri kaynaklar olmuşlardır.[129] Günümüzde ise bu temel kaynaklar *Wikipedia, Britannica* gibi *online* ansiklopediler ile devam etmektedir. O hâlde *online* ansiklopediler nasıl sosyal medya platformu olarak tanımlanabilir? Geleneksel ansiklopedilerin aksine *Wikipedia* gibi internet ansiklopedileri, kullanıcıların sürekli ekleme ve düzenlemeler yapabildiği, bağımsız ve ücretsiz bir platform özelliği taşımaktadır. Yani siteye üye olan her kullanıcı burada yazar olarak katkıda bulunabilir veya hâlihazırda yazılmış bilgileri değiştirip düzenleyebilir. Böylelikle yaşanan tüm gelişmelerin anında sisteme girilmesini amaçlayan bu platform, oluşabilecek bilgi kirliliği veya "değiştirme savaşlarını" editörleri ile engellemeyi öngörmektedir.[130] İnternetin en büyük getirilerinden bir tanesi olan "bilgiye hızlı erişimi" kolaylaştırması ile popüler olan *online* ansiklopedilere gösterilen katılımı Aralık 2020 verileri çok net bir şekilde göstermektedir.

[129] Engin Cihad Tekin, "Kitap Tarihi Araştırmalarının Önemli Bir Alanı: Ansiklopedilerin Gelişimi ve Ansiklopedi Kültürü Araştırmalarının Önemi", **ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi**, 2020, C. 11, S. 2, s. 196.

[130] WIKIPEDIA, Vikipedi, https://tr.wikipedia.org/wiki/Vikipedi (Erişim: 14 Nisan 2021).

3.2.1.4 Twitter



Şekil 3: Statista, Most Popular Websites Worldwide as of December 2021, by unique visits (in millions), TWITTER

Kaynak: https://www.statista.com/statistics/1201889/most-visited-websites-worldwide-unique-visits/, (Erişim: 05 Eylül 2022).

Twitter son zamanlarda kullanıcıların haber, eğlence, siyaset veya popüler kültür hatta ruh hâlleri gibi birçok alanda görüşlerini paylaştığı ve tartıştığı sosyal bir platform olarak karşımıza çıkmaktadır. 280 karakter sınırlaması ile gönderilen *tweet*lerin gayet basit bir ara yüz aracılığı ile kullanıcıların takipçilerine ve yapılan paylaşımın yayılmasıyla takipçisi olmayan kişilere dahi anlık iletilmesini sağlamaktadır. *Google* ve *Bing* gibi hizmetler ile koordineli bir şekilde çalışılması sonucunda hem *Twitter* dışında yapılan aramalar sonucunda paylaşımlara ulaşım sağlanması hem de kullanıcıların bilmediği bir dilde paylaşılan *tweet*lerin kendi dillerine çevrilmesi sağlanmaktadır.[131]

Sosyal medyanın "yeni medya" olarak adlandırılmasındaki en büyük etkenlerden bir tanesi *Twitter* gibi platformların dünya çapında anlık bilgi paylaşımı yapılmasını sağlayan bu altyapısı olduğu gerçeğidir. Çünkü sunulan bu imkânlar sayesinde bilgisayar, akıllı telefon veyahut tablet aracılığı ile internet erişimi ve sosyal medya

[131] Benevenuto Fabricio, Magno Gabriel, Rodrigues Tiago & Almeida Virgilio, **Detecting spammers on Twitter**. 2010, (Çevrimiçi) https://homepages.dcc.ufmg.br/~fabricio/download/ceas10.pdf (Erişim: 15 Nisan 2021).

hesabı olan herkes potansiyel birer gazeteci olabilmektedir. Bu bağlamda ele alındığında *Twitter* devasa bir bilgi transferine ev sahipliği yapmaktadır. Sadece bununla da sınırlı olmayıp aynı zamanda kitlelere ulaşmak için en hızlı yollardan bir tanesi olmuştur. Günümüzde hemen hemen her siyasetçinin veya devlet kurumunun bir *Twitter* hesabı bulunmakta ve halkla ilişkiler aracı olarak kullanılmaktadır.

Özellikle açık kaynak istihbaratı açısından ciddi derecede veri sunmasının yanı sıra, geleneksel yöntemlere nazaran *Twitter* ve diğer sosyal medya platformlarından elde edilen bu verilerin teyit edilme ihtiyacı çok daha fazladır. Örneğin; 2020 yılında Hong Kong uydu televizyonu müdür yardımcısı olan Shijian Xingzou'nun *Twitter*'ın Çin versiyonu olan *Weibo* sitesindeki hesabından Kuzey Kore lideri Kim Jong Un'un öldüğünü söylemesi ile beraber *Twitter*'da teyit edilmemiş bu iddia uzun bir süre tartışma konusu olmuştu.[132] Haber sonradan yalanlansa da belirli bir süre *Twitter* ve diğer sosyal medya platformlarındaki gündemi işgal etmeyi başarmıştır. Kısacası *Twitter*, anlık bilgi transferi açısından muazzam bir zemin sunmasına karşılık, teyit edilmesi gereken, algıya açık bilgilerin önüne geçememektedir.

3.2.1.4. Facebook

Facebook, 2004 yılında kurulmuş ABD merkezli bir sosyal ağ sitesidir. Kabaca anlatmak gerekirse, bireyler site üzerinden belirli kişisel bilgilerini girerek (isim-soy isim, doğum tarihi, cinsiyet, e-posta, telefon numarası vb.) hesap oluşturabilmektedir. Platform aslında son derece standartlaştırılmış kullanıcı hesaplarını öngörmektedir. Yani birden fazla özellik ekranda aynı yerde bulunarak aranan verileri tanımayı ve bulmayı kolaylaştırmaktadır. Facebook hesaplarında iki önemli sayfa bulunmakta; bunlar "*timeline*" da denilen ana sayfa ve "*Wall* (duvar)" denilen profil sayfasıdır. Duvar olarak adlandırılan profil sayfası daha çok kullanıcıların kendilerini tanıttıkları bölümdür. Profil resmi, kapak fotoğrafı, isteğe bağlı olarak doğum tarihi, yaşadığı şehir, okuduğu okul gibi bazı bilgileri içeren bir künye ve yapılan beğeniler ile takip ettikleri sayfalar sunulmaktadır. Yine bu bölümde "durum güncellemeleri" adlı kısımda kişiler istedikleri içeriği (yazılı veya görsel şeklinde) paylaşabilmekte ve profillerindeki arkadaşları (yapılan paylaşımın gizlilik kısıtlaması yapılmamış ise herkes) bu

[132] Business Today, **Is Kim Jong Un Dead? Twitter abuzz with rumours of North Korean leader's demişe**, 26 Nisan 2020, (Çevrimiçi) https://www.businesstoday.in/current/world/kim-jong-un-dead-twitter-abuzz-with-rumours-of-north-korean-leader-demise/story/402024.html (Erişim: 15 Nisan 2021).

güncellemelere beğenerek veya yorum yaparak etkileşimde bulunabilmektedir. *Timeline* olarak da adlandırılan ana sayfa kısmında ise kullanıcılar kendi yaptıkları paylaşımlar gibi arkadaşları ve takip ettikleri sayfaların paylaşımlarının tamamı bulunmaktadır. Yapılan paylaşımların kronolojik olarak yansıtılmasından kaynaklı olarak *timeline* ismi kullanılmaktadır.[133]

Birçok sosyal medya platformunda olduğu gibi algıya açık paylaşımlar *Facebook* sitesinde de ciddi sorunlara yol açmıştır. 2020 yılı ABD seçimlerinde manipülatif paylaşımlar ile gündeme gelen *Facebook* sitesi, yayınladığı bir raporda *Facebook* ve *Instagram* platformlarından toplamda 265.000 içeriğin seçmenlere müdahale edildiği gerekçesiyle kaldırılmış, 3,3 milyon reklam gönderimi ise bilinçli olarak ABD sosyal sorunlarını ve seçimlerini hedef aldığı gerekçesiyle reddedildiği bildirmiştir. Yine aynı raporda 2019 yılından itibaren Rusya, Çin ve İran ülkelerinin desteklediği sahte hesaplar ile yapılan manipülatif paylaşımların ABD'li vatandaşlara yönelik aldatıcı ve güven sarsıcı etkileri tespit edilip engellendiğinden bahsedilmiştir.[134]

Tüm bunların yanı sıra, aynı *Twitter* platformunda olduğu gibi *Facebook* sitesi de kullanıcılara dair muazzam bir veriye sahip ve bu verilerin analizinde ne gibi sonuçlar elde edilebileceği hâlâ süregelen bir tartışma konusu. Stanford ve Cambridge üniversitelerinden araştırmacıların yapmış olduğu, 17.000 katılımcının spesifik bir anketi tamamladıktan sonra *Facebook* profillerindeki beğenilerini araştırmacılarla paylaşıp, kullanıcıların kişiliklerini analiz etmeyi öngören aynı anketi kişilerin yakın çevresine de uyguladıktan sonra elde ettikleri sonuç bu tartışmaların önemini niteleyecek düzeydedir. Anketlerden ve beğenilerden yeterince veri elde ettikten sonra, *Facebook* algoritması kişinin özelliklerini çevresindeki insanlara kıyasla daha iyi tahmin edebilmekteydi. Algoritmanın kullanıcıyı bir iş arkadaşından daha iyi tanıması için 10, bir oda arkadaşından daha iyi tanıması için 70, ebeveyni veya kardeşi için 150, eşinden daha iyi tanıyabilmesi için ise 300 beğeni yeterliydi.[135] Kısacası basit bir

---

[133] Ralf Caers, Tim Feyter, Marijke Couck, Talia Stough, Claudia Vigna & Cind Du Bois,"Facebook: A literature review**", New Media & Society**. 2013, 15, pp. 983-984.

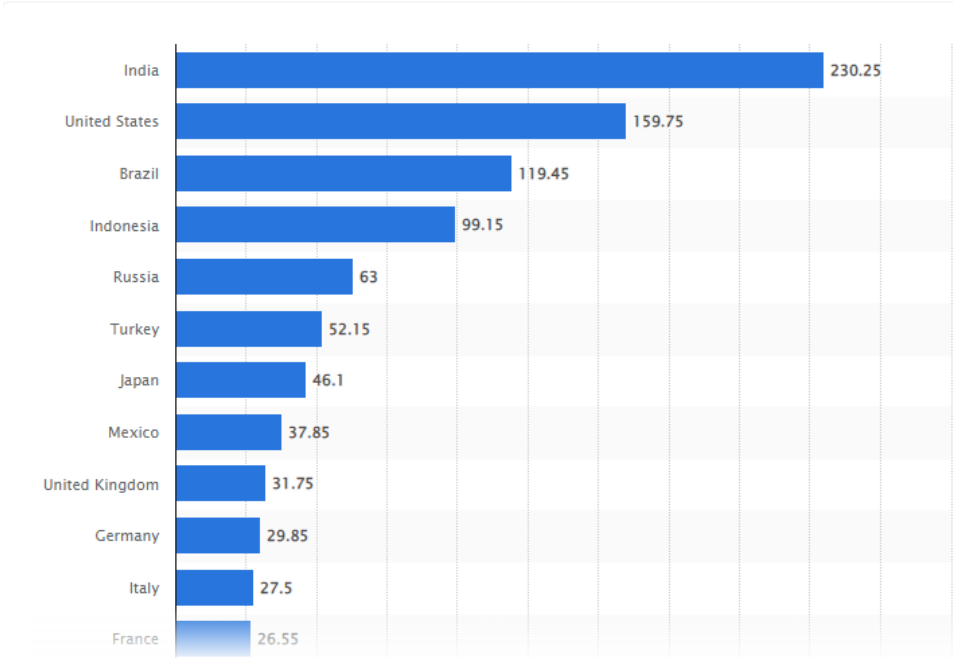
[134] About.fb.com., **A Look at Facebook and US 2020 Elections**, Aralık 2020, (Çevrimiçi) https://about.fb.com/wp-content/uploads/2020/12/US-2020-Elections-Report.pdf (Erişim: 16 Nisan 2021).

[135] Douglas Ouenqua, Facebook Knows You Better Than Anyone Else, **The New York Times,** 2015, (Çevrimiçi) https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html (Erişim tarihi: 16 Nisan 2021).

şekilde üye olup profilinizi oluşturduğunuz bir sosyal ağ sitesi, sitede yapılan beğeniler ile kullanıcı hakkında eşinin onu tanıdığından daha iyi analiz edebilecek kadar veriye ulaşabilmektedir.

3.2.1.5. Instagram

Instagram platformu, kullanıcıların oluşturmuş oldukları profillerinde fotoğraflarını, video kayıtlarını ve anlık görüntülerini arkadaşları veya açık hesap özelliği ile herkesle paylaşmalarını sağlayan bir uygulama.[136] Fakat bu özelliklerin neredeyse tamamı diğer platformlarda da bulunmasına rağmen *Instagram*'ın bu kadar tercih edilmesinin sebebi nedir?



Şekil 4: *Eylül 2022 tarihli ülkelere göre Instagram kullanıcı sa*yıları (milyon)

Kaynak: https://www.statista.com/statistics/578364/countries-with-most-instagram-users/ (Erişim: 05 Eylül 2022)

Ocak 2021 yılına ait veriler, sadece Türkiye'de 46 milyon kullanıcısı olan *Instagram* uygulamasının ülke nüfusunun yarısından fazlası tarafından kullanıldığını göstermektedir (birden fazla hesap kullanan bireyler ve sahte hesaplar dahilinde sadece sayısal olarak yapılmış bir çıkarım). Uygulamada yapılan eylemler aslında pek de yabancı olunmayan davranışlar. Bu uygulamayı kabaca yakın tarihlerde misafirliğe giden akrabaların veya dostların birbirlerine fotoğraf albümlerini göstermesinin dijital

[136] Janabeth Ward, "A Content Analysis of Celebrity Instagram Posts and Parasocial Interaction", **Elon Journal of Undergraduate Research in Communications**, 2016, Vol. 7, No. 1, p. 1.

versiyonu olarak tanımlayabiliriz. Böylelikle sanal ortamda yapmış olduğunuz aktiviteleri, bulunduğunuz ortamı, hobilerinizi veya evcil hayvanlarınızı insanlarla paylaşmanıza olanak sağlamaktadır. Bunlara ek olarak filtre ve efekt uygulamalarıyla platformu daha eğlenceli bir hâle getirerek popülaritesini arttırmaktadır. Diğer platformlardan farklı olarak, siyasetten olabildiğince uzak, daha çok eğlence ve ticaret alanlarına hitap eden *Instagram* uygulamasının sunduğu hizmetler diğer platformlarla benzer nitelikte olsa da tercih edilmesine yol açmaktadır. Ayrıca birçok meşhur kişinin bu uygulamayı aktif olarak kullanması, yeni bir meslek kolu olarak karşımıza çıkan *influencer*ların bu uygulama vasıtasıyla gelir elde edip popüler olması, özellikle gençler tarafından *Instagram* uygulamasının tercih edilmesine etkili olmaktadır.

3.2.1.6. Tiktok

Veri gizliliği ile ilgili birçok sosyal medya platformu zaman zaman tartışmaya açılsa da günümüzde bu tarz tartışmalara en çok konu olan uygulama *Tiktok* olmuştur. Çin'de *Douyin* olarak bilinen bu uygulama şu an ki *Tiktok* uygulamasının öncüsü niteliğindedir. 2016 yılında dünyanın en değerli *start-up*'ı olan *ByteDance* tarafından piyasaya sürülmüş ve 2018 yılında *Musical.ly* ile birleşerek denizaşırı ilk çıkışını yapmıştır. Fakat uygulamanın tek tartışıldığı konu veri gizliliği değildir. Geçtiğimiz yıllarda Hindistan'daki milletvekilleri tarafından kültürel bozulmayı ve açık içeriği sebebiyetiyle uygulamaya kısa süreliğine yasaklama getirilmiştir. ABD'nin Federal Ticaret Komisyonu ise çocukların mahremiyet yasasını ihlal ettiği gerekçesiyle 5,7 milyon dolar para cezasını çarptırmıştır. Bunun yanı sıra güvenlik endişeleri de ABD hükûmetinin inceleme başlatmasına neden olmuş, uygulanan sansür politikaları ciddi eleştirilere sebebiyet vermiştir.[137] Apple firması tarafından geliştirilen iOS 14 platformu ile *Tiktok* şirketinin veri saklama işlemi yaptığı iddiası ise uygulamayı bir kez daha tartışmaya açmıştır. Yapılan herhangi bir arama veya kopyala-yapıştır işleminde kullanılan kelimelerin *Tiktok* uygulaması tarafından kayıt altına alınıp şirketin daha çok kullanıcının uygulamayı tercih etmesi için analiz amaçlı kullandığı iddiaları, (her ne kadar şirket bu iddiaları reddetse de) birçok kullanıcının ve resmî makamların tepkisini çekmiştir.[138]

---

[137]Katie Sehl, Everything Brands Needs to Know About Tiktok in 2020, **Hootsuite**, 2020, (Çevrimiçi) https://blog.hootsuite.com/what-is-tiktok/ (Erişim tarihi: 16 Nisan 2021).

[138] Ecevit Bıktım, Tiktok Veri Hırsızlığı ile Gündemde, **CNN Türk,** 2020, (Çevrimiçi) https://www.cnnturk.com/teknoloji/tiktok-veri-hirsizligi-ile-gundemde (Erişim tarihi: 16 Nisan 2021).

Bütün bu tartışmalara konu olan *Tiktok* ise basitçe kullanıcıların 15 saniyelik dikey videolar çekip paylaştığı bir uygulamadır. Kullanıcılar başka bir videoya geçmezse çekilen videolar *loop* özelliği ile bittiği anda tekrar başlama özelliği göstermektedir. Ayrıca kullanıcılar başka videolar ile kendi videolarını birleştirerek bu süreyi 60 saniyeye çıkartabilmektedir. Uygulama bu kısa süreli videolarda kullanıcılara daha eğlenceli içerik sunabilmek için müzik örnekleri, filtreler, hızlı kesimler ve çıkartmalar gibi yaratıcı eklentiler içermektedir. Tüm bu tartışmalara ve devlet müdahalelerine rağmen *Tiktok* uygulaması ciddi bir büyüme kaydetmiş ve Ad Age tarafından Ekim 2019'da yayınlanan bir rapora göre *Tiktok* ve Çince versiyonu olan *Douyin* uygulaması dünya çapında 800 milyon kullanıcıya ulaşmıştır.[139]

3.2.2. Yeni Medyanın Geleneksel Medyadan Farkları

Günümüzde teknolojik gelişmelerin etkisi ile iletişim sektöründe "Yeni Medya" ve "Bilgi Teknolojileri" sistemlerinin hâkimiyeti görülmektedir. Özellikle bireylerin internet erişimine ve teknolojiye kolayca ulaşabilmeleri ile sadece habercilik alanında değil eğlence ve kültürel alanlarda da yeni medya etkisini göstermektedir. Bu bağlamda yeni medya hakkında çok sayıda çalışma hazırlanmış ve farklı tanımlamalar getirilmeye çalışılmıştır. Örneğin Marshall Mcluhan ve Bruce R. Powers, günümüz teknolojilerinin nicel görsel uzam ile nitel işitsel uzam olmak üzere iki farklı mantığı doğurduğunu ve iletişim sistemlerinin "Global Köy" kavramını ortaya çıkartıp bu iki görüşün her zaman ve her yerde iletişim kurabilme imkânlarını ifade etmişlerdir.[140] Yeni medya kavramını ilk kullanan kişi olan Marshall Mcluhan, bu kavram ile aslında iletişim sistemlerini kastetmiştir.

Lev Manovich ise yeni medyayı farklı bir perspektiften açıklamıştır. Yeni medya alanında yapmış olduğu çalışmalarından bir tanesinde yeni medyanın kültürel çevreden ana akıma geçmesinin yaklaşık on yıl aldığını, ABD'deki SIGGRAPH ve Avusturya'daki Ars Electronica'nın 1970'li yıllarda bilgisayarlar ile çalışan sanatçıların yıllık yaptıkları buluşmaların ise yeni medya açısından bir milat olduğunu, gelişimini tamamlamasının ise 1980'li yılları bulduğunu ifade etmiştir. Manovich yeni medyayı alanında ilgili insanların tartıştıkları ve bilgi paylaşımı yaptıkları ortam olarak açıklamış

[139] Andrew Meola, Analyzing Tiktok User Growth and Usage Patterns in 2020, Insider, 2020, (Çevrimiçi) https://www.businessinsider.com/tiktok-marketing-trends-predictions-2020 (Erişim tarihi: 16 Nisan 2021).

[140] Marshall Mcluham and Bruce R. Powers, **Global Köy**, İstanbul: Scala Yayıncılık, 2020, s. 9-20.

ve siber kültür, bilgisayar teknolojisi, yazılım ile kontrol edilen veriler, manuel yapılan algoritmaların bilgisayar teknolojisiyle yapılması vb. gibi kavramlarla birlikte ele almıştır.[141]

Buradaki asıl sorunsal ise neden "Yeni Medya" olarak adlandırılıyor olmasıdır. Bu sorun doğal olarak öncelikle yeni olanın geleneksel olandan farklarının açıklanması ihtiyacını doğurmaktadır. Çalışmada bahsi geçen ARPANET projesinin ardından internetin bireylerin kullanımına açılması ile mesafeleri ortadan kaldıran, çok kısa zamanda bireylerin çok daha kolay bir biçimde iletişim kurmasını sağlayan bu sistem beraberinde iki farklı görüşü de meydana getirmiştir. Bunlardan birincisi bu teknolojinin demokratikleşmesi ile insan haklarına ve özgürlüklere katkı sağlayabileceği yönündeyken diğer görüş, bu özgür gibi görünen ortamın arkasında yönetimsel güçlerin iktidarını pekiştirdiği düşüncesidir.[142]

Yeni medyanın özgürlükçü yapısı tamamen bir illüzyondan ibaret demek çok yanlış bir tespit olacaktır. Çünkü geleneksel medya ile karşılaştırıldığında en çok göze çarpan özelliklerinden bir tanesi bu olmaktadır. Geleneksel medya merkeziyetçi bir yapıya sahipken yeni medya merkezî olmayan bir sistemdir. Geleneksel medyanın bu yapısı zaman ile tekelci bir sistemi de karşımıza çıkarmıştır. Özellikle habercilik alanında somut olarak basımı yapılan gazete, dergi gibi iletişim araçlarının hem maliyeti hem de stresli iş yükünden ötürü sistem bir süre sonra geleneksel medyayı ticari çıkarlar güden bir duruma getirmiştir. Fakat bunun aksine yeni medya hem kullanıcının ücretsiz hem de çok daha hızlı şekilde bilgiye ulaştığı bir sistemi sunmaktadır. Geleneksel medyanın bu konu bakımından yeni medya karşısında son derece zayıf kaldığını 8 Kasım 2020 tarihinde Türkiye Hazine ve Maliye Bakanı Berat Albayrak'ın *Instagram* üzerinden duyurduğu istifasından çok daha iyi okuyabiliriz. Sosyal medyada ardı arkası kesilmeyen ve gündemden düşmeye haber konusu, geleneksel medyada yerini dahi bulamamıştı. Teyit edilme ihtiyacı bulunan haberin bir gün sonrasında hiçbir gazetede

---

[141] Lev Manovich, **New Media From Borges to HTML**, The MIT Press, 2003, s. 1-20.

[142] Tayfun Yücesoy, **Bireyden Kitleye Sosyal Medya Devrimleri ve Ötesine Kuramsal Yaklaşımlar**, İstanbul: Duvar Yayınları, 2020, s. 12-13.

haber yapılmaması ise geleneksel medya – yeni medya karşılaştırmasını bir kez daha gündeme getirmiştir.[143]

Yeni medyanın erişim kapasitesi geleneksel medyaya göre çok daha fazladır. Ulaşımının geleneksel medyaya kıyasla daha kolay ve kitlelere erişim açısından daha fazla imkâna sahip olmasının en büyük etkenlerinden bir tanesi de kartopu efektidir. Geleneksel medyada bireyin bir gazetede okuduğu ve televizyonda izlediği haberi paylaşabileceği insan sayısı kısıtlıyken, yeni medyada okunan bir haberi paylaşarak yayımını hızlandırabilme imkânı çok daha fazladır. Bu aynı bir kartopunun yuvarlanarak daha da büyük bir hâle gelmesi gibi paylaşılan bir içeriğin kullanıcıların etkileşimi ile daha büyük kitlelere ulaşmasını sağlamaktadır. Geleneksel medya belli periyotlarında yayım ve yayın yapmasına karşılık yeni medyada bilgiye her an her yerde ulaşabilmektesinizdir. Bunun yanı sıra yeni medya arşivcilik açısından da çok daha uygun imkânlar sunmaktadır. Kullanıcılar okudukları veya izledikleri bir içeriği kolaylıkla kayıt altına alıp muhafaza edebilmektedirler.

Celalettin Aktaş, geleneksel medya ile yeni medya karşılaştırmasında yeni medyanın merkeziyetçi olmayan, asenkronik, çok sayıda yayın-yayım kaynağı bulunan, küresel ve çeşitlendirilmiş içeriği bulunan yapısına dikkat çekerek bu farklılıkları aşağıdaki tabloda göstermiştir.[144]

[143] JOURNO, Berat Albayrak istifa haberleri: Eski medya sustu, "yeni medya" coştu, uluslararası medya gazetecilik yaptı, 2020, (Çevrimiçi) https://journo.com.tr/berat-albayrak-istifa-haberleri (Erişim tarihi: 17 Nisan 2021).

[144] Celalettin Aktaş, Yeni Medyanın Geleneksel Medya ile Karşılaştırılması, (Çevrimiçi) https://personel.klu.edu.tr/dosyalar/kullanicilar/suleyman.ozcan/dosyalar/dosya_ve_belgeler/ileti%C5%9Fim/Makale%202%20Yeni%20medya-Geleneksel%20medya.pdf (Erişim tarihi: 17 Nisan 2021).

Tablo 2: **Yeni Medya ile Geleneksel Medya Arasındaki Farklılıklar**

	Geleneksel Medya	Yeni Medya
Kanal	Az sayıda	Çok sayıda
Kontrol	Gönderen	Alıcı
İletim	Tek yönlü	İki yönlü, etkileşimli
İçerik	Sınırlı	Çeşitlendirilmiş
Kapsama Alanı	Bölgesel, küresel	Küresel
Toplumsal Kontrol	Kanunlar, meslek ve ahlâk ilkeleri, halk eğitimi	Teknik aygıtlar, izleme
Zaman	Senkron	Asenkron
Yapısı	Merkeziyetçi (bir noktan-çok noktaya)	Merkeziyetçi olmayan (çok noktadan-çok noktaya)

Kaynak: AKTAŞ, Celalettin, Yeni Medyanın Geleneksel Medya ile Karşılaştırılması, Akademik Sosyal Araştırmalar Dergisi, Yıl:6, Sayı:36, Nisan 2019, s. 227-239 https://www.academia.edu/41216983/Geleneksel_Medya_ile_Yeni_Medyan%C4%B1n_Kar%C5%9F%C4%B1la%C5%9Ft%C4%B1r%C4%B1lmas%C4%B1_Kuramsal_Bir_Analiz_%C3%87al%C4%B1%C5%9Fmas%C4%B1

Bu yeniliklere geleneksel medyanın da yavaş yavaş uyum sağlamak zorunda olduğunu, faaliyetlerinin büyük bir kısmını dijital alana taşıdıklarından çıkarabiliriz. Televizyon kanallarında yayınlanan program veya dizilerin aynı zamanda kendi *YouTube* kanallarında paylaşılması, her haber kuruluşunun tüm sosyal ağlarda hesaplarının bulunması ve haber içeriklerini bu platformlardan da paylaşmaları bunlara örnek olarak verilebilmektedir. Ayrıca yukarıda bahsedilen ticari çıkarlarını internet ortamında daha iyi muhafaza edebileceği gerçeği de bulunmaktadır.

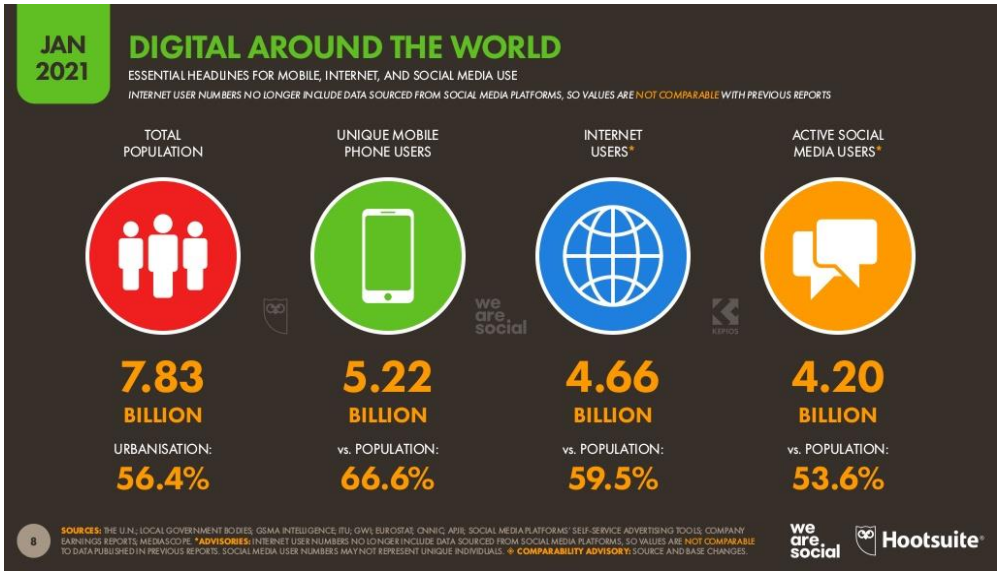
3.2.3. Sosyal Medyanın Kullanımı

Hızla popüler olması ve kolay erişilebilirliği ile her yaştan insanın sosyal medya platformlarını kullanması, günümüz dünyasında âdeta bir gereklilik hâline gelmiştir. Aynı zamanda sunduğu ticari imkânlar, e-ticaret ile e-ihracat gelişmeleri ve halka ilişkiler alanındaki kitlelere ulaşma kapasitesi sebebiyle özel şirketler de bu alanda kurumsal olarak varlıklarını göstermek istemişlerdir. Kullanıcı sayısı arttıkça ve sosyal medyada iletişime geçilebilecek kitleler büyüdükçe kendi PR politikaları çerçevesinde birçok farklı grup sosyal medyayı aktif olarak kullanır hâle gelmiştir. Günümüz sosyal medya kullanıcılarına bakıldığında bireysel kullanıcıları, özel şirketleri, devlet kurumlarını, devlet dışı aktörleri, sosyal hizmet birimlerini hatta ve hatta uyuşturucu

kartelleri ve terör örgütleri gibi yapılanmaları dahi görebilmekteyiz. Bu bağlamda sosyal medyadaki verilerden ve elde edilen bu verilerin istihbarat faaliyetlerinde kullanımından bahsetmeden önce dünyada, Türkiye'de ve bahsi geçen diğer aktörler açısından sosyal medya kullanımının potansiyeline bakmakta fayda görülmektedir.

3.2.3.1. Dünyada Sosyal Medya Kullanımı

Sosyal medya kullanımı hakkındaki güncel verilerin ve kullanım oranındaki artışını daha iyi anlaşılması için Wearesocial ve Hootsuite şirketlerinin senelik olarak hazırladığı internet ve sosyal medya kullanımları hakkındaki detaylı raporların 2020 ve 2021 senelerine ait verileri karşılaştırmalı olarak ele alınacaktır.

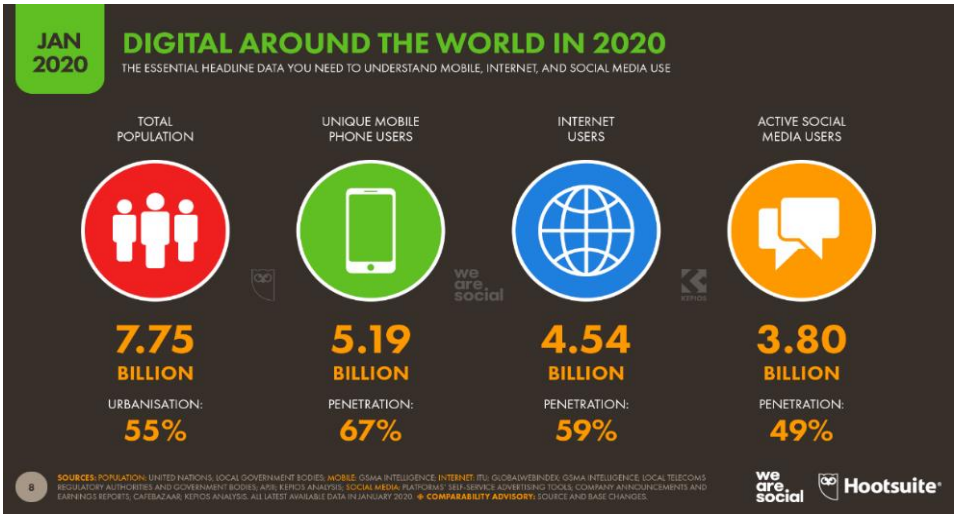


Şekil 5*:* 2021 Dünya Genelinde İnternet ve Sosyal Medya Kullanımı, Wearesocial ve Hootsuite

Kaynak: Wearesocial, Digital 2021, https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media (Erişim: 18 Nisan 2021) [145]

2021 verilerine göre; 7,83 milyar olan dünya nüfusunun %59,5'ine tekabül eden 4,66 milyar birey internet, %53,6'sına tekabül eden 4,2 milyar birey ise aktif olarak sosyal medyayı kullanmaktadır. Raporun sunduğu veriler ışığında basitçe dünyanın yarısı aktif olarak sosyal medya kullanıcısıdır diyebiliriz.

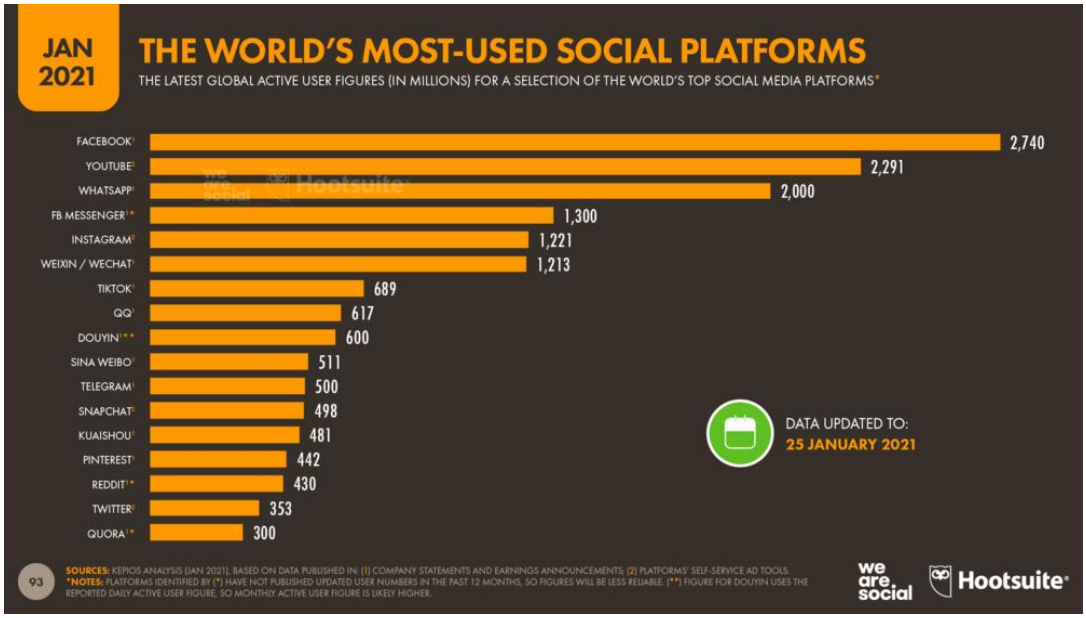
[145] Önceki senelerin raporlarına kıyasla 2021 yılı raporunda internet kullanıcıları sayılarında sosyal medya platformlarından elde edilen veriler dâhil edilemediğinden dolayı eski raporlarla kıyaslanması sağlıklı sonuçlar sunmayacaktır. Fakat yine de çalışmada 2020 yılı verileri paylaşılacaktır.



Şekil 6: 2020 Dünya Genelinde İnternet ve Sosyal Medya Kullanımı, Wearesocial ve Hootsuite

Kaynak: Wearesocial, Digital 2020, https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media (Erişim: 18 Nisan 2021).

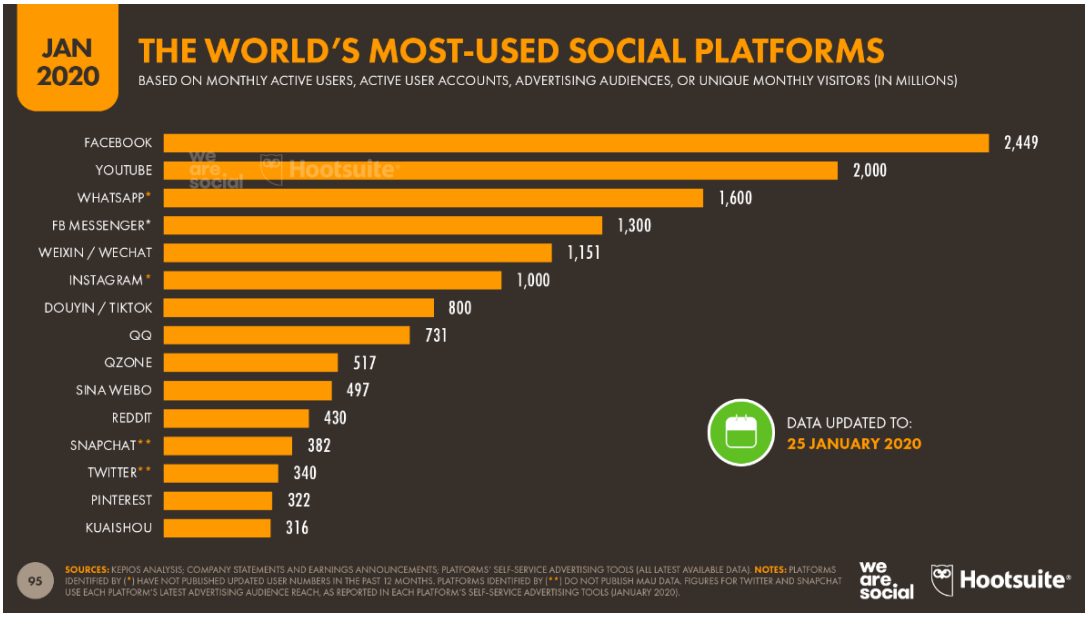
2020 yılında ise bu rakamlar; 7,75 milyar dünya nüfusunun %59'una tekabül eden 4,54 milyar birey internet, %49'una tekabül eden 3,8 milyar birey ise aktif sosyal medya kullanıcısı olarak karşımıza çıkmaktadır. Yani 2020 yılından itibaren dünya nüfusu 80 milyon, internet kullanıcısı 12 milyon, aktif sosyal medya kullanıcısı ise 40 milyon artış göstermiştir. 2021 yılında dünya genelinde en çok kullanılan sosyal medya platformları ise şu şekildedir:



Şekil 7: 2021 Dünya Genelinde En Çok Kullanılan Sosyal Medya Platformları

Kaynak: Wearesocial, Digital 2021 **https://datareportal.com/reports/digital-2021-global-overview-report** (Erişim tarihi: 18 Nisan 2021)

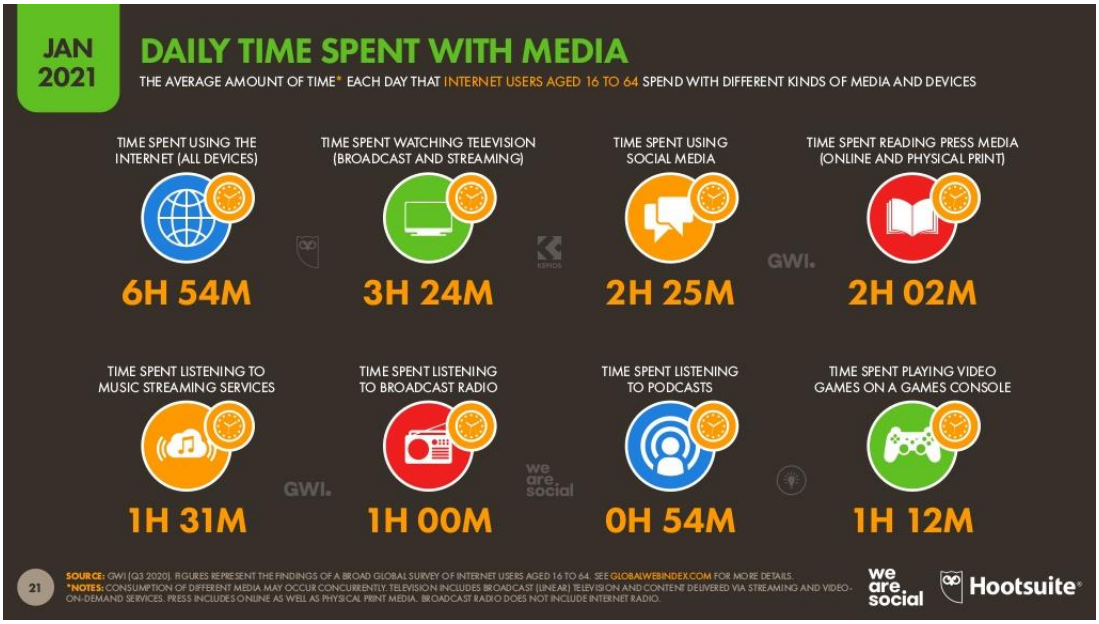
Veri güvenliği konusundaki zafiyetleri hakkında en çok hedef olan *Facebook* platformu 2 milyar 740 milyon kullanıcı ile en fazla tercih edilen sosyal medya platformu iken anlık haber paylaşımlarının ve siyasi figürlerin aktif olarak kullandığı *Twitter* platformu 353 milyon kullanıcı ile listenin sonlarında yer almaktadır. Çin'in siber güvenlik politikası ile birçok sosyal medya platformuna erişimi yasaklayıp bu platformların yerli versiyonlarını kullanıma açmasının, listedeki Çin menşeili sosyal medya platformlarına bakılarak başarılı sonuçlar vermekte olduğunu söyleyebiliriz. *Tiktok* uygulamasının Çin versiyonu olan *Douyin* 600 milyon kullanıcıya sahip iken, başka bir video paylaşım uygulaması olan Kuasishou'nun 481 milyon, *WhatsApp* uygulamasının alternatifi olarak piyasaya sürdüğü *WeChat* uygulamasının 1 milyar 213 milyon, *Twitter*'ın alternatifi olan *Sina Weibo* sitesinin ise 511 milyon aktif kullanıcıya sahip olduğu görülmektedir. Tabii ki burada nüfus etkeni de göz ardı edilmemelidir. Ülke içinde VPN kullanmadan Amerikan menşeili şirketlere erişim olmadığı için 1,4 milyar nüfuslu bir ülkenin kendi alternatif markalarının ortaya böyle bir tablo çıkarması gayet doğaldır. Burada bir diğer ilginç nokta ise *Telegram* markasının bulunmasıdır. 2020 verilerine bakıldığında *Telegram* markası listede bulunmamakta iken 2021 yılında 500 milyon aktif kullanıcı gibi ciddi bir sayıya ulaşmıştır.



Şekil 8: 2020 Dünya Genelinde En Çok Kullanılan Sosyal Medya Platformları

Kaynak: Wearesocial, Digital 2020, **https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media** (Erişim tarihi: 18 Nisan 2021)

2014 yılında *Facebook* tarafından satın alınan *WhatsApp* uygulamasının 2021 yılında "Gizlilik Sözleşmesi" kriziyle ciddi tartışmalara konu olması kullanıcıları doğal olarak alternatif arayışlarını sevk etmiştir. 2021 ve 2020 verilerine bakıldığında aktif *Facebook* kullanıcı sayısının 300 milyona yakın oranda düştüğü görülmektedir. *Facebook* firması bu açığı sahip olduğu diğer markalar ile koordineli bir şekilde çalışarak kapatma politikasına yönelmiş ve *WhatsApp* uygulamasının gizlilik sözleşmesinde yer alan kullanıcı bilgilerini yeni bir sözleşme aracılığıyla *Facebook* ile paylaşmasını istemiştir. Yeni sözleşmenin kabul edilmemesi durumunda ise sözleşmeyi kabul etmeyen kullanıcıların 8 Şubat 2021 tarihinde uygulamayı kullanamayacaklarını belirtmiştir. Bu durum kullanıcılar açısından ciddi bir krize sebebiyet vermiş ve sosyal medya platformlarında günlerce gündem olmuştur. Neticesinde kullanıcılar veri gizliliği açısından daha güvenilir alternatifler aramaya başlamış ve *Telegram*, *Signal* gibi uygulamalara yönelmişlerdir. [146]



Şekil 9: 2021 Medya İçin Harcanan Günlük Süre

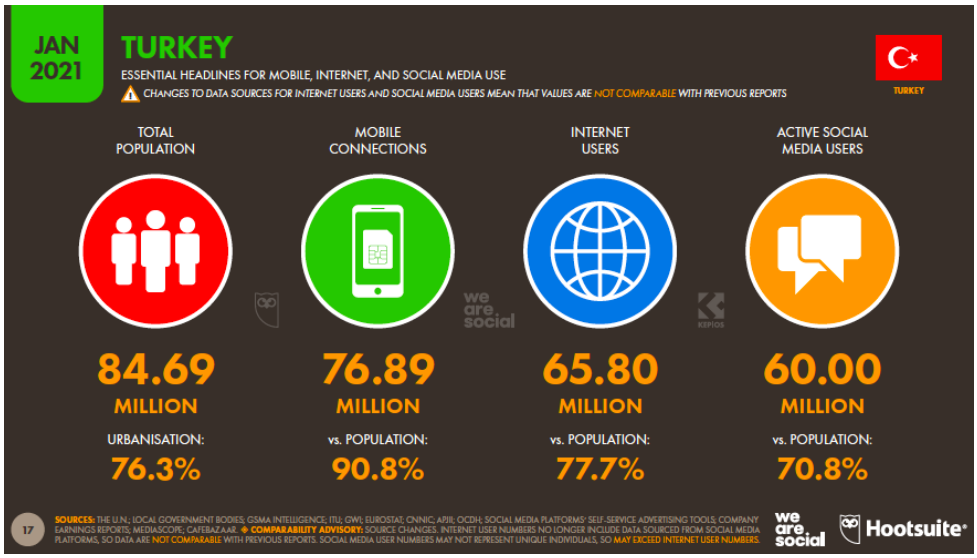
Kaynak: Wearesocial, Digital 2021, **https://wearesocial.com/digital-2021** (Erişim tarihi: 18 Nisan 2021).

[146] HABERTURK, WhatsApp sözleşmesi 2021 nedir, ne anlama geliyor? WhatsApp gizlilik sözleşmesi nasıl iptal edilir?, 2021 (Çevrimiçi) https://www.haberturk.com/whatsapp-sozlesmesi-nedir-ne-anlama-geliyor-whatapp-gizlilik-sozlesmesi-nasil-iptal-edilir-2932352-teknoloji (Erişim tarihi: 18 Nisan 2021),

Son olarak ise 16 ila 64 yaş arasındaki kullanıcıların internet ve sosyal medya gibi araçlara günlük ortalama harcadıkları vakit; internet için 6 saat 54 dakika, sosyal medya için 2 saat 25 dakika, video oyunları için 1 saat 12 dakika, *podcast* için 54 dakika, radyo yayınları için 1 saat, televizyon için ise 3 saat 24 dakika olarak gözlemlenmiştir.

3.2.3.2. Türkiye'de Sosyal Medya Kullanımı

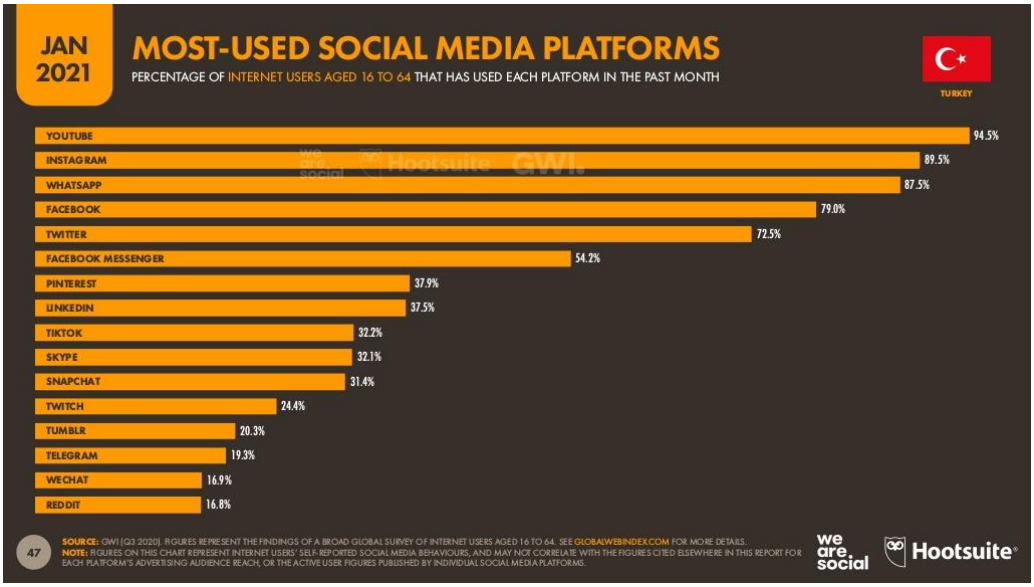
Türkiye'de birçok ülke gibi internet ve sosyal medya kullanımında yenilikleri yakalayabilmiştir. Dijitalleşmenin etkisiyle kamu bünyesinde birçok işlemin internet ve mobil uygulamalar üzerinden yapılmaya başlaması da insanların siber alana yönelimini desteklemiştir. Bu bağlamda dünyada internet ve sosyal medya kullanım verileri incelendiği gibi Türkiye'deki verilere bakmak da faydalı olacaktır.



Şekil 10: 2021 Türkiye'de İnternet ve Sosyal Medya Kullanımı

Kaynak: Wearesocial, Digital 2021: Turkey, **https://datareportal.com/reports/digital-2021-turkey,** (Erişim tarihi: 19 Nisan 2021)

Ocak 2021 yılı itibariyle 84,69 milyon nüfusu olan Türkiye'nin, nüfusunun %77,7'lik kısmını temsil eden 65,80 milyon vatandaşı internet, %70,8'lik kısmını temsil eden 60 milyon vatandaşı ise sosyal medyayı aktif bir biçimde kullanmaktadır. Bu sayılar son derece ciddi bir veri potansiyelini temsil etmektedir. Henüz okula başlamamış küçük çocuklar ve yaşlı nüfus da dâhil olmak üzere 84,69 milyon olan nüfusun 60 milyonu sosyal medyada veri paylaşımı yapmaktadır.



Şekil 11: 2021 Türkiye'de En Çok Kullanılan Sosyal Medya Platformları

Kaynak: Wearesocial, Digital 2021: Turkey, **https://datareportal.com/reports/digital-2021-turkey**, (Erişim tarihi: 19 Nisan 2021)

Fakat dünya genelindeki verilere kıyasla Türkiye'de tablo biraz daha farklı gözükmektedir. Her ne kadar *Facebook* ve *Twitter*'ın son derece fazla kullanıcısı olsa da 16 ila 64 yaş arasındaki sosyal medya kullanıcıların en çok *YouTube* ve *Instagram* gibi ana teması eğlence olan platformları tercih ettiği görülmektedir. Dünya'da sosyal medya kullanımı başlıklı bölümde belirtilen *WhatsApp* gizlilik sözleşmesi krizinde ise Türkiye nezdinde yine farklı bir sonuç ortaya çıkmaktadır. AB'de geçerli olan "Genel Veri Koruma Yönetmeliği" nedeniyle bahsi geçen gizlilik sözleşmesi Avrupa'daki ülkelere "kabul etmezseniz uygulamayı kullanamazsınız" şeklinde dayatılamıyor.[147] Kullanıcıların uygulamayı kullanmasının önünde sözleşmeyi kabul edip etmemek gibi bir engelleri bulunmuyor. Türkiye dâhil olmak üzere belli başlı ülkelerde bu sözleşme krizi yaşanmış olmasına rağmen Türkiye'de en çok kullanılan sosyal medya platformlarının arasında *WhatsApp* 3. sırada iken listenin devamında alternatif olarak sunulan *Telegram* veya *Signal* gibi uygulamalar gözükmemekte, aksine Çin menşeili *WeChat* uygulaması diğer platformlara göre çok az kullanıcısı olsa da listede yer edinebilmektedir. Fakat yine de buradan Türkiye'deki kullanıcıların veri gizliliği konusunda bilinçsizce davrandığı sonucunu çıkarmak hatalı bir tespit olacaktır çünkü sosyal medya platformları üzerinden gösterilen tepkiler üzerine *Facebook* şirketi

[147] TRT Haber, WhatsApp'ın Yeni Şartları Avrupa Birliği'nde Geçerli Değil, 2021, (Çevrimiçi) https://www.trthaber.com/haber/bilim-teknoloji/whatsappin-yeni-sartlari-avrupa-birliginde-gecerli-degil-547606.html (Erişim tarihi: 19 Nisan 2021).

WhatsApp uygulamasının gizlilik sözleşmesi hakkında yeni bir bilgilendirme açıklaması yapmak ve sözleşme şartlarında bulunan 8 Şubat tarihini 15 Mayıs'a ertelemek durumunda kalmıştır. Akabinde devlet kurumları devreye girerek Facebook şirketinin yapmakta olduğu paylaşım politikasının hukuksuz olduğunu belirterek mesajlaşma servisi için inceleme başlatmıştır.[148]

İnternet ve sosyal medya kullanımının yanı sıra, Türkiye'deki 16 ila 64 yaş aralığındaki kullanıcılarının günlük 7 saat 57 dakikasını internette, 2 saat 57 dakikasını sosyal medyada, 36 dakikasını *podcast* yayınlarını dinlemek, 39 dakikasını radyo yayınlarını dinlemek, 58 dakikasını video oyunu oynamak, 3 saat 13 dakikasını ise televizyon izlemek için harcadığı tespit edilmiştir.[149]

3.2.3.3. Devlet Kurumları ve Siyasetçilerin Sosyal Medya Kullanımı

Vatandaşların kullanıcı sayısı arttıkça sosyal medya alanı devlet kurumları açısından da içinde bulunulması gereken bir mekân hâline gelmiştir. Esasında bunu devletin içgüdüsel bir eylemi olarak da tanımlayabiliriz. Vatandaşlık dediğimiz kavram aslında devlet ile birey arasında yapılan zımni bir sözleşmedir. Bu anlaşmanın öngördüğü şekilde devlet vatandaşlarının güvenliğini, eğitim, sosyal, sağlık ve hukuksal hakları gibi temel hak ve hürriyetlerini güvence altına alacağının teminatını verip karşılığında vatandaşı olacak bireyin devleti ve kanunlarını tanımasını istemektedir. Bu çerçeveden bakıldığında günümüzde sanal olduğu kadar gerçek de olan siber âlemin içinde de bu yükümlülükleri yerine getirmesi gerekmektedir. Ayrıca hızlı iletişimin verdiği imkânlar dâhilinde kitlelere ulaşma imkânı çok daha verimli olacaktır. Diğer yandan siyasetçiler açısından ise âdeta sanal bir miting ortamı oluşturan sosyal medya gerek halkla ilişkiler çalışmaları bağlamında gerek ise bireyler ile anlık etkileşimde bulunma kabiliyeti sayesinde sosyal medyadan yararlanmaktadır.

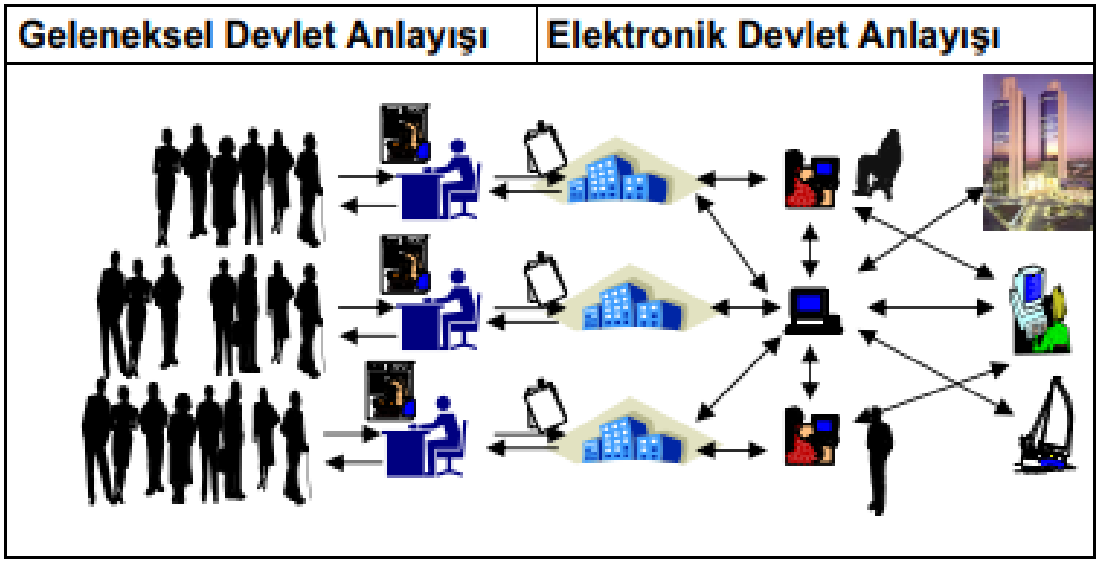
Küreselleşme ve dijitalleşme ile artık kamu sektörü de ciddi değişimlere gitmesi gerektiğinin farkına varmıştır. Hızla değişen dünya standartlarında geleneksel devlet modelinin kamu yönetimi gerek hizmet kalitesi gerekse hız konusunda yetersiz kalmaya başlamıştır. Bu bağlamda *e-government* sistemi geleneksel kamu yönetimine alternatif olarak ortaya çıkmıştır. Geleneksel kamu yönetimi vatandaşlar ile yüz yüze etkileşimde

---

[148] SHIFDELETE, WhatsApp'tan İlk Geri Adım!, 2021, (Çevrimiçi) https://shiftdelete.net/son-dakika-whatsapp-sozlesme-tarihini-erteledi (Erişim tarihi: 19 Nisan 2020).

[149] Simon Kemp, **Wearesocial**, Digital 2021: Turkey, 2021, (Çevrimiçi) https://datareportal.com/reports/digital-2021-turkey (Erişim tarihi: 19 Nisan 2021).

bulunup yapılacak eylemleri kâğıt işleri ile uzun ve yorucu bir şekilde halletmeyi öngörürken, e-devlet[150] sistemi bu işlemlerin tamamının dijital ortamda yapılıp hem zamandan hem mekândan tasarruf edilmesi imkânını sunmaktadır.[151]



Şekil 12: Geleneksel Devlet Anlayışı ile Elektronik Devlet Anlayışı Karşılaştırması

Kaynak: Kadir Pamukoğlu ve Mustafa Ocak, Bilişim Teknolojilerinin Devletin Etkinliğindeki Rolü ve İnternet Üzerinden Satış Uygulaması, https://www.harita.gov.tr/uploads/files/articles/bilisim-teknolojilerinin-devletin-etkinligindeki-rolu-ve-internet-uzerinden-satis--1068.pdf (Erişim tarihi: 19 Nisan 2021).

Fakat nasıl ki son derece statik olan web 1.0 teknolojik gelişmeler ve yenilikler ile web 2.0'a evirildiyse, *e-government* sistemi de sosyal medya araçlarını da kapsayan web 2.0 gibi *e-government* 2.0 kavramını karşımıza getirmiştir. Bu bağlamda *e-government* 2.0 kavramı bünyesine sosyal web gibi özelliklerin entegre edilmesini öngörmektedir. Vatandaşların sürece katılımını arttırmak, çevrimiçi kamu hizmetlerinin kalitesini iyileştirmek, hızlı bir şekilde geri dönüş almak gibi imkânları sağlamaktadır. Aynı zamanda bu tarz bir sistemin hem daha şeffaf hem de daha demokratik olduğu

[150] Türkiye'deki örneği için bkz. https://www.turkiye.gov.tr/

[151] Kadir Pamukoğlu ve Mustafa Ocak, Bilişim Teknolojilerinin Devletin Etkinliğindeki Rolü ve İnternet Üzerinden Satış Uygulaması, (Çevrimiçi) https://www.harita.gov.tr/uploads/files/articles/bilisim-teknolojilerinin-devletin-etkinligindeki-rolu-ve-internet-uzerinden-satis--1068.pdf , (Erişim tarihi: 19 Nisan 2021), s. 59.

düşünülmektedir. [152] Bu bağlamda Türkiye Cumhuriyeti 65. hükûmetinin kamu yönetiminde sosyal medya kullanıma dair sosyal medya hesapları bu tabloda görülmektedir:

Tablo 3: Türkiye Cumhuriyeti 66. Hükûmetinin Sosyal Medya Hesapları

Bakanlık Adı	Facebook	Twitter	Youtube	Instagram	Tiktok	LinkedIn	Google+
Adalet Bakanlığı	✓	✓	✓	✓	X	✓	✓
Aile ve Sosyal Hizmetler Bakanlığı	✓	✓	✓	✓	X	✓	✓
Çalışma ve Sosyal Güvenlik Bakanlığı	✓	✓	✓	✓	X	✓	✓
Çevre, Şehircilik ve İklim Değişikliği Bakanlığı	✓	✓	✓	✓	X	✓	✓
Dışişleri Bakanlığı	✓	✓	✓	✓	X	✓	✓
Enerji ve Tabii Kaynaklar Bakanlığı	✓	✓	✓	✓	X	✓	X
Gençlik ve Spor Bakanlığı	✓	✓	✓	✓	✓	✓	✓
Hazine ve Maliye Bakanlığı	✓	✓	✓	✓	X	✓	✓
İçişleri Bakanlığı	✓	✓	✓	✓	X	✓	✓
Kültür ve Turizm Bakanlığı	✓	✓	✓	✓	X	✓	✓
Milli Eğitim Bakanlığı	✓	✓	✓	✓	X	✓	✓
Milli Savunma Bakanlığı	✓	✓	✓	✓	X	X	X
Sağlık Bakanlığı	✓	✓	✓	✓	X	✓	X
Sanayi ve Teknoloji Bakanlığı	✓	✓	✓	✓	X	✓	✓
Tarım ve Orman Bakanlığı	✓	✓	✓	✓	X	✓	✓
Ticaret Bakanlığı	✓	✓	✓	✓	X	✓	✓
Ulaştırma ve Altyapı Bakanlığı	✓	✓	✓	✓	X	✓	✓

Siyasetçilerin kullanımı da benzer amaçlar ve motivasyonlar barındırmaktadır. Toplumla sürekli olarak iletişim hâlinde olmak, kitlelere daha kolay ulaşabilmek, hızlı geri dönüşler ve toplumun katılımı vb. gibi. Bunun en güncel örneğini ABD Başkanı Donald Trump olarak gösterebiliriz. Başkanlık döneminde özellikle *Twitter* platformunu aktif bir şekilde kullanmasından dolayı söylemleri sürekli olarak gündemde yer bulmaktaydı. Sadece halkla ilişkiler alanında değil dış politika alanında da sürekli olarak kontrolsüz bir biçimde sosyal medya hesabından paylaşım yapması kendi ülkesinde bulunan diplomatları da rahatsız etmiştir.[153]

Web 1.0 olanaklarından siyasal partilerde faydalanmış ve siyasal amaçları doğrultusunda web siteler aracılığı ile kitlelere ulaşmayı amaçlamıştır. Fakat nasıl ki web 1.0'ın sunmuş olduğu statik web siteleri bir süre sonra kullanıcıların talep ettiği iletişim imkânlarını tam anlamıyla sunamamış ve neticesinde *blog*lar ve sosyal ağ

[152] Imed Boughzala, Marijn Janseen & Saïd Assar, E-Government 2.0: Back to Reality, a 2.0 Application to Vet, 2015, (Çevrimiçi) https://www.researchgate.net/publication/278652082_E-Government_20_Back_to_Reality_a_20_Application_to_Vet (Erişim tarihi: 19 Nisan 2021), s. 1-12.

[153] William Gallo, Trump'ın Dış Politikada Twitter Kullanımı Endişe Yaratıyor, Amerika'nın Sesi, 2016, (Çevrimiçi) https://www.amerikaninsesi.com/a/trumpin-dis-politikada-twitter-kullanimi-endise-yaratiyor/3622423.html (Erişim tarihi: 19 Nisan 2021).

siteleri ortaya çıkmışsa, siyasi oluşumlarda halkla ilişkiler amacıyla kurmuş oldukları web sitelerinden tam anlamıyla verim alamadıklarını ve internet ortamında bir dönüşüm olduğunu fark ettiklerinde sosyal medyayı etkin bir biçimde kullanmaya başlamışlardır. Bu sebeple sosyal medya, özellikle seçim kampanyalarında etkili bir iletişim aracı olması sebebiyle seçmenlerle etkileşim hâlinde olmak ve siyasal propaganda faaliyetlerini yürütmek için siyasetçiler tarafından aktif bir şekilde kullanılmıştır.[154]

Dolayısıyla internet ortamında yaşanan değişim, dönüşüm ve gelişmelerin yansımaları, faaliyetlerinde bu alandan yararlanan neredeyse tüm alanları etkilemiştir. Web 2.0 gelişmeleri ile *e-government* 2.0 uygulamalarına geçiş yapan kamu hizmetleri gibi siyasal iletişim alanı da siyasal iletişim 2.0 dönüşümü yaşamıştır. Geleneksel medyanın kullanıldığı siyasal iletişime karşılık sosyal medyanın kullanıldığı siyasal iletişim 2.0'da iletişim maliyetleri son derece düşük iken geri bildirim oranları daha yüksek, iletişim şekli iki yönlü ve diyalog üzerine kurulu iken mesajların hem kitlesel hem bireysel nitelikte olduğu görülmektedir.[155]

Sosyal medyayı çok daha aktif kullanan ve dijital yerli [156] olarak nitelendirilen kuşakların oy kullanacak ve siyasi karar vericilerden talepte bulunacak olgunluğa eriştikleri göz önünde bulundurulduğunda, sosyal medyanın siyasal iletişim boyutunda çok daha aktif olacağı görülmektedir.

3.2.3.4. Terör Örgütleri ve Uyuşturucu Kartellerinin Sosyal Medya Kullanımı

Sosyal medyanın sunmuş olduğu iletişim imkânlarından yararlananlar tabii ki sadece devlet kurumları, siyasetçiler veya özel sektör değildir. Terör örgütleri kendi ideolojilerini veya inançlarını kitlelere duyurabilmek için aktif bir şekilde sosyal medya platformlarını kullanmaktadır. İdeolojik paylaşımların dışında uyuşturucu kartelleri gibi yapmış oldukları silahlı eylemlerin veya kaçırdıkları rehinelerin görüntülü

---

[154] Ümit Arklan, "Sosyal Medyanın Siyasal Amaçlı Kullanımı: Ağ Kuşağının Kullanım Alışkanlıkları Üzerine Bir Araştırma", **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, 2016, C. 4, S. 2, s. 622.

[155] Mustafa Bostancı, **Sosyal Medya ve Siyaset**, Konya: Palet Yayınları, 2015, s. 93.

[156] Dijital dünyada doğmuş ve büyümüş olan, internet, video oyunları ve dijital diller konusunda "native speaker" olarak nitelendirilen nesil (Y ve Z kuşağı) için kullanılan "dijital yerli" kavramı ve dijitalleşmeden önce doğmuş fakat bir noktada bu gelişmeler ile etkileşime geçmiş olan nesil (X kuşağı) için kullanılan "dijital göçmen" kavramları hakkında daha fazla bilgi için bkz. Marc Prensky, "Digital Natives, Digital Immigrants, On the Horizon", **MCB University Press,** 2016, Vol. 9, No. 5, pp. 1-2.

paylaşımlarını da korku ve kaos oluşturmak için yine bu platformlar üzerinden paylaştıkları görülmektedir.

Soğuk Savaş sonrası dönemde küreselleşmenin de etkisiyle karşımıza çıkan yeni kavramlardan bir tanesi uluslararası terörizm olmuştur. Bölgesel etkisinin yanı sıra kitle imha silahlarına erişim sağlayabilmek için organize suç örgütleriyle iş birliği kuran terör örgütlerinin faaliyetleri artık küresel boyuta ulaşmıştır. Bununla birlikte propagandalarını yapabilmek için yazılı ve görsel medyayı kullanan terör örgütleri, çağın önemli gelişmelerinden bir tanesi olan internet ile sosyal medyayı da bu iletişim araçlarından bir tanesi olarak kullanmaya başlamıştır. Bu durum doğal olarak hem geleneksel hem yeni medya hakkındaki tartışmaları da beraberinde getirmiştir. Medyada terör örgütü propagandalarına yer verilerek terörist faaliyetlere bir nevi destek verildiği hakkında sıkı eleştiriler getirilmiştir.[157]

Terör gruplarının medya ağlarında bu şekilde propaganda yapmalarındaki motivasyon şu şekilde özetlenebilir:

- Yaptıkları eylemlerin propagandasını yapmak ve kitleler üzerinde korku oluşturmak,
- Kendi amaçları doğrultusunda geniş kitleleri mobilize etmek ve aynı zamanda uluslararası alanda haklılıklarına vurgulamak,
- Devletlerin ve güvenlik güçlerinin terörle mücadele politikalarını haksız ve anti-demokratik ve hukuk dışı olarak göstermek,
- Sözde mücadelelerine karşı sempatizan kitleyi arttırmak,
- Sermayesini arttırmak,
- Terör örgütüne mensup üyelerine moral ve cesaret vermek.[158]

Örneğin DAEŞ terör örgütü başta *YouTube* olmak üzere birçok sosyal medya platformundan yararlanarak milyonlarca kişiye propaganda videosu gönderebilmektedir. Kimi zaman kısa çatışma anları ve infaz videolarını kimi zaman ise örgütün kontrol ettiği şehirlerdeki günlük yaşama dair kısa kesitleri kullanmıştır. Bir önceki bölümde bahsi geçen geleneksel medyanın merkeziyetçi yapısına karşılık sosyal medyanın merkeziyetçi olmayan dinamik yapısı, paylaşılan bu uygunsuz içeriklerin en kısa sürede

[157] Hüseyin Kazan, "Terör-Medya İlişkisi ve Medyada Terör Haberciliği", **Güvenlik Stratejileri**, 2015, C. 12, S. 24, ss. 116-121.

[158] Paul Wilkinson, "The Media and Terrorism: A Reassessment", **Terrorism and Political Violence**, 2007, Vol. 9, No. 2, s. 56-57.

siteden kaldırılmasına rağmen birçok kullanıcı tarafından paylaşılıp binlerce kişiye ulaşmasına imkân sağlamaktadır. Silinen videoların tekrar yüklenmesinin önüne geçilecek bir sistem yapısı da bulunmadığı için yapılması planlanan propaganda varlığını sürdürebilmektedir.[159]

DAEŞ'e veya Irak-Suriye'de bulunan radikal gruplara katılan militanlar hakkında The Soufan Group (TSG) tarafından hazırlanan raporda 100'ün üzerinde ülkeden 30.000'in üzerinde terör örgütü üyesi bulunduğu belirtilmiştir. Bunların 5000'e yakınının Batı Avrupa'dan, 4700'ünün eski Sovyet Cumhuriyeti'nden, 280'inin Kuzey Amerika'dan, 875'inin Balkanlardan, 8000'inin Kuzeybatı Afrika bölgesinden, 8240'ının Orta Doğu'dan, 900'ünün ise Güneydoğu Asya'dan olduğu ifade edilmiştir. Bu verilere bakıldığında dünyanın neredeyse her bölgesinden sempatizan kazanan örgütün medya propagandalarından başarılı sonuç elde ettiği görülmektedir. [160]

Terör örgütlerine benzer amaçlarla sosyal medyayı kullanana TCO (Transnational Criminal Organisations) ve DTO'ların (Drug Trafficking Organisations) ise farklı motivasyonları bulunmaktadır. Carlo Morselli'nin sosyal medyanın suç gruplarının işleyişini ve faaliyetlerini anlamaya nasıl yardımcı olabileceği ve yeni iletişim teknolojilerinin bu tarz gruplar tarafından kullanılmasının oluşturduğu mevcut ve potansiyel tehditleri araştırma amacıyla, *Facebook*, *Twitter* ve *MySpace* gibi sosyal ağ sitelerinde bazı anahtar kelimeler kullanarak yaptığı filtremeler ile hazırladığı çalışmasında bu tarz yapılanmaların sosyal medyayı üye kazanmak için yapmadığını tespit etmiştir. Ayrıca sosyal medyada çete hesaplarına ziyarette bulunan üyelerin kandırılarak veya manipüle edilerek etkileşimde bulunduğuna dair hiçbir kanıt olmadığını ancak katılım gösterenlerin bu tarz gruplara meraklarını göstererek yorumlarını ve fikirlerini paylaştıklarını ifade etmiştir. Uyuşturucu kartelleri ve çetelerin bu tarz propagandaları daha çok itibarlarını artırmak ve çete kültürünü tanıtmak için yaptığı gözlemlenmiştir.[161]

---

[159] Ceyhun Kaan Karakaş, "DAEŞ Propagandasında Yeni Medya Kullanımı", **Marmara İletişim Dergisi**, 2017, C. 2, S. 1-1, s. 37-38

[160] THE SOUFAN GROUP, Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq, 2015, (Çevrimiçi) https://www.cvereferenceguide.org/sites/default/files/resources/TSG_ForeignFightersUpdate3.pdf (Erişim Tarihi 20 Nisan 2021), s. 5.

[161] Carlo Morselli, "Gangs and Social Networking", **Organized Crime Research Brief**, 2010, Vol. 13, No. 1, p.2.

TCO ve DTO'lar ile Meksika'daki uyuşturucu kartelleri ve kartellere bağlı çetelere üye kişilerin sosyal medya kullanımının doğasını ve kapsamını belirlemek amacıyla örneklemler üzerinden açık kaynaklı ve istihbarat odaklı metotlar kullanılarak hazırlanan bir başka çalışmada ise benzer bulgulara rastlanmıştır. Kartellerin üye devşirmenin aksine kendi aralarında iletişim kurmak için sosyal medya platformlarını kullandıkları tespit edilmiştir. Grup toplantıları veya yapılacak eylemlerin planlaması için sosyal medya platformu üzerinden haberleşme ağını kurduklarını bu yüzden kartel üyelerinin sosyal medya hareketlerinin takibi ile elde edilecek açık kaynaklı verilerin istihbarat sürecinde potansiyel faydası bulunduğu ifade edilmiştir. Elde edilebilecek verilerin kartellerin söylemlerini ve yapısal durumlarını inceleyen kolluk kuvvetleri ve istihbarat personelleri açısından çıkarımları olduğu belirtilmiştir. Bunun yanı sıra sosyal medya kaynaklarındaki potansiyel yanlış bilgilerin oluşturabileceği sorunlara dikkat çekilerek, insani istihbarat yöntemi, şüpheli itiraflar, tanık ifadeleri, IP adresi ve kimlik doğrulaması gibi teknik desteklerle elde edilen verilerin doğrulanması gerektiği ifade edilmiştir.[162]

3.2.4. Sosyal Medyanın Olumlu ve Olumsuz Tarafları

Bir önceki başlıklarda sosyal medyanın iletişim açısından ne tür imkânlar sunduğundan bahsedilmiştir. Gelişmelerden anlık olarak haberdar olmak, kullanıcılar ile etkileşimde bulunup hâlihazırda tanıdığınız insanlar ile yeniden bir araya gelmek veya yeni insanlar tanımak gibi fırsatların yanı sıra ticari açıdan da büyük bir pazar hâline gelmiştir.

Markaların sosyal medya aracılığı ile ürün tanıtımlarını veya reklamlarını daha uygun maliyetlerle kitlelere ulaştırma imkânları, e-ticaret ve e-ihracat gibi sektörlerin büyümesi, girişimcilerin sosyal medyanın global etkisinden yararlanarak yeni müşteri portföylerine ulaşabilmesi bu pazarın daha da genişlemesini sağlamıştır. Sosyal medya, pazarlamanın 4P'sinin[163] tutundurma aşamasının yeni bir elemanı olarak karşımıza çıkmaktadır. Firmalar sosyal medyada kendi reklamlarını yapabilmekte, millî ve kültürel değerleri olan özel günlerde kutlama mesajları yayınlayarak müşteriler ile satış dışı etkileşimde bulunarak halkla ilişkiler kampanyalarını yürütebilmekte, kişisel satışa katkı sağlayabilmekte aynı zamanda doğrudan pazarlama etkinliklerini

[162] Justin Nix, Michael Smith, Matthew Petrocelli, Jeff Rojek & Victor Manjarrez Jr, "The Use of Social Media by Alleged Members of Mexican Cartels and Affiliated Drug Trafficking Organizations", **Journal of Homeland Security and Emergency Management**, 2016, Vol. 13, No. 3, pp. 395-418.

[163] Product (ürün), Price (fiyat), Place (Dağıtım), Promotion (Tutundurma)

yürütebilmektedir.[164] Bunun yanı sıra farklı reklam politikaları uygulayarak sosyal medyada geniş kitlelere hitap eden fenomenler aracılığı ile ürün tanıtımlarını gerçekleştirebilmektedir. Ayrıca e-ticaretin sunmuş olduğu düşük maliyetler sebebiyle bu alanda yapılan satışların tüketiciye daha uygun fiyatlara sunulması, tüketicilerin bu alana daha çok yönelmesinde etkili olmaktadır.

Sosyal medyanın belki de saymakla bitirilemeyecek kadar fazla olan olumlu taraflarının yanı sıra bir de olumsuz tarafları bulunmaktadır. Sosyal medyanın gelişim sürecinde özellikle bu olumsuz taraflar pek konuşulmamaktaydı. Fakat günümüzde bu olumsuzluklar artık kullanıcıları rahatsız veya tedirgin etmesi sebebiyle sık sık tartışmaya açılır hâle gelmiştir.

3.2.5. Sosyal Medya Tehditleri

3.2.5.1. Bilgi Kirliliği

Sosyal medya, kitlelerin yaşamlarında meydana getirmiş olduğu yenilikler ile kullanıcılara özgürlüklerle dolu bir alan sunmuş ve kitlelerin kendi sözcüleri olabilmesine imkân tanımıştır. Bu sayede milyonlarca kullanıcı kendi fikirlerini ve düşüncelerini dürüstçe ve korkusuzca ifade edebilme olanağı bulmuştur. Birçok zümre tarafından tartışmaya açılan sosyal medyadaki ifade özgürlüğünün âdeta bedeli olarak karşımıza bilgi kirliliği sorunu çıkmaktadır.[165]

Sosyal, kültürel, siyasi veya ekonomik herhangi bir konuyu kendi fikirleri çerçevesinde paylaşan kullanıcılar "kasıtlı veya kasıtsız" bir şekilde bilgiyi deformasyona uğratabilmektedir. Buna ek olarak sosyal ağları hızlı bilgi alabilmek için kullanan bireylerin, edinilen bilgiyi ikinci hatta üçüncü bir kaynaktan teyit etme motivasyonu bulunmadığı için her geçen gün kullanıcı sayısı artan sosyal ağlara paralel olarak bilgi kirliliği de artış göstermektedir. Ayrıca sosyal medyada paylaşılan içeriklerin *photoshop*, kırpma veya montajlama yöntemleri ile sunulmaları da zaman zaman görülmektedir.[166]

---

[164] Yüksel Köksal ve Şuayip Özdemir, "Bir İletişim Aracı Olarak Sosyal Medya'nın Tutundurma Karması İçerisindeki Yeri Üzerine Bir İnceleme", **Süleyman Demirel Üniversitesi İİBF Fakültesi Dergisi**, 2013, C. 18, S. 1, s. 334.

[165] Ramesh Pandita, "Information Pollution, a Mounting Threat: Internet a Major Casuality", **J. Of infosci. Theory and Practice**, 2014, Vol. 2, No. 4, s. 52-53.

[166] Merve Seren, Tolga Çelik, Nedim Özgeldi & Elif M. Dumankaya, Sosyal Medya El Kitabı, Ankara: Orion Kitabevi, 2018, s. 61.

3.2.5.2. Kişisel Verilerin Korunması

Sosyal medya sitelerinde profil veya üyelik oluşturulacağı zaman her platformun kullanıcılardan talep ettiği belli başlı bilgiler bulunmaktadır. Bunlardan bazıları; isim-soy isim, e-posta adresi, telefon numarası, rehber, adres bilgileri, cihaz kimliği, satın alma geçmişi, fotoğraf ve videolar olabilir. Bununla birlikte profil oluşturulduktan sonra yapılan paylaşımlarda kullanıcının vermiş olduğu bu bilgilerin üstüne paylaştığı ekstra verilerdir. Milyonlarca kullanıcının sosyal medya platformlarının veri tabanına kendi rızaları ile verdiği bu verilerin korunması ise bir başka sorundur. Devletler bireylerin siber alanda paylaşmış olduğu verileri kanunlar, firmalar ise güvenlik sözleşmeleri ile güvence altına almaktadır. Durum teoride böyle olsa da pratikte tam anlamıyla beklenileni karşılamamaktadır.

Türkiye'de veri güvenliği için oluşturulan "Kişisel Verilerin Korunması Kanunu"; *Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları* belirlemeyi amaçlamaktadır.[167] Her ne kadar kanunlarda amaç, kapsam ve tanımlar yapılıp cezai yaptırımlar belirlenmiş olsa da veri hırsızlığı gibi nedenlerle yapılan siber saldırıların %23'ünün kimliği belirsiz *hacker*lar tarafından yapıldığı PwC, CIO ve CSO'nun 2018 yılında yapmış olduğu raporda belirtilmiştir.[168] Ayrıca veri ihlali konusunda hedef olan firmaların gerek siber saldırılara karşı yeterliliğinin gerek ise siber güvenlik bilincinin yeterli olmadığı tespit edilmiştir.[169]

Siber saldırılar hemen hemen her gün birçok firmanın tecrübe etmek zorunda kaldığı ciddi bir tehdit hâline gelmiştir. Ayrıca bu saldırıların hedefi küçük ve büyük firma gözetmeksizin gerçekleşmektedir. Söz konusu durumlarda akla ilk gelen örnek 2014 yılında yaşanan Facebook Cambridge Analytica krizidir. Cambridge Üniversitesi'nde öğretim üyesi olan Aleksandr Kogan, 2014 yılında ABD seçmeni hakkında ayrıntılı profil çıkarmayı hedefleyen bir anket uygulaması geliştirmiştir. Anket uygulaması

---

[167] RESMİ GAZETE, Kişisel Verilerin Korunması Kanunu, Resmî Gazete Sayısı: 29677, 2016 https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 (Erişim tarihi: 21 Nisan 2021).

[168] PwC, CIO ve CSO, **The Global State of Information Security Survey**, 2018, (Çevrimiçi) https://www.pwc.com.tr/gsiss2018-en (Erişim tarihi 21 Nisan 2021).

[169] Ebru Yıldırım Yeniman, "Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması", **Mesleki Bilimler Dergisi (MBD)**, 2018, C. 7, S. 2, s. 32.

sadece sizin *Facebook* bilgilerinize değil arkadaşlarınızın verilerini de sizin vasıtasınız ile toplamaktaydı. Toplamda elde edilen 50 milyon kişilik kullanıcı verisi Cambridge Analytica'ya satılıp o dönemden itibaren başkan adaylarının seçim kampanyalarında kullanılmaya başlanmıştır.[170] Bir başka örnek ise 2016 yılında *Yahoo* firmasının yaşamış olduğu siber saldırıdır. Bu vakada ise çok basit bir çözüm bulunmasına karşılık gerekli adımlar atılamamıştır. *Yahoo*'nun CEO'su saldırı gerçekleştikten sonra tüm şifreleri otomatik olarak yenilemiş olsaydı kullanıcıların verilerini güvence altına alabilirdi fakat kullanıcıların yeni şifre oluşturma zorunda kalmasından ötürü rahatsız olup firmayı kullanmayı bırakacaklarından endişelenmiştir. Bu bağlamda siber saldırıların tek nedeni yetersiz altyapı değil aynı zamanda bilinçli personellerin de bulunmasıdır.

3.2.5.3. Sosyal Mühendislik

Siber alanda gerçekleşen saldırılar akıllara ilk olarak teknik saldırıları getirmekte ve daha sağlam altyapılar ve güvenlik duvarları ile bu sorunların vereceği hasarın azaltılabileceği düşünülmektedir. Fakat sosyal ve psikolojik siber saldırılar olan toplum mühendisliklerini bu önlemler engelleyememektedir. Sosyal mühendisliği bir vaka ile açıklamak daha faydalı olacaktır. 15 yaşında lise öğrencisi olan Kane Gamble iki arkadaşı ile dönemin CIA Başkanı, Ulusal Güvenlik Danışmanı, eski istihbarat müdürü ve FBI'ın bilim ve teknoloji bölümü başkan yardımcısı dâhil birçok ABD hükûmet yöneticisinin e-posta ve sosyal medya hesaplarını *hack*lemiştir. Fakat Gamble ve arkadaşları bunu teknik yollar ile değil sadece toplum mühendisliği olarak adlandırılan ikna etme, dolandırma ile başarmıştır.[171] Siber güvenlik konusunda en zayıf halka olan kullanıcıların [172] hatalarından yararlanılan bu yöntem ile Irak ve Afganistan operasyonlarına dair birçok askerî belge ve istihbarat raporlarını elde edip sonrasında ifşa edilmesini sağlamışlardır. Gamble öncelikle CIA Başkanı John Brennan'ı hedef alır ve telefon numarasını elde eder. Kane Gable kendisini hem John Brennan'ın kullanmış

---

[170] Burak Budak, Bilmeniz Gerekenler: Cambridge Analytica Hikayesi, Facebook ve Büyük Veri, **Webrazzi**, 2018, (Çevrimiçi) https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri/ (Erişim tarihi: 21 Nisan 2021).

[171] THE GUARDIAN, **Two Years** '**Detention for UK Teenager Who** '**Cyberterrorised** '**US Officials,** 2018, (Çevrimiçi) https://www.theguardian.com/technology/2018/apr/20/two-years-detention-for-uk-teenager-who-cyberterrorised-us-officials-kane-gamble (Erişim tarihi: 21 Nisan 2021).

[172] Nezir Akyeşilmen, **Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik**, Ankara: Orion Kitabevi, 2018, s. 8.

olduğu telefon şirketi Verizon çalışanı hem de John Brennan'ın kendisi olarak tanıtarak John Brennan'a ait e-posta ve *iCloud* hesaplarına erişim sağlar.[173]

Bu vakada görüldüğü üzere sosyal mühendislikte teknik imkânlar son derece sınırlı kullanılmaktadır. Bu bağlamda sosyal mühendislik bir kişiyi kendi çıkarlarına uygun ya da aykırı bir eylemi gerçekleştirme yolunda etkileyen her türlü davranış olarak tanımlayabiliriz. Siber alan ise bu yöntemin uygulanabilmesi için muazzam bir zemin hazırlamaktadır. İrtibata geçilecek hedef ile yüz yüze görüşmeden farklı bir kimliğe bürünerek eylem gerçekleştirilebilir. Ayrıca sosyal mühendislik için can damarı denilecek "bilginin" elde edilebileceği en uygun ortamlardan bir tanesidir. Elde edilen her yeni bilgi sosyal mühendislik sürecine katkı sağlamaktadır ve sosyal mühendislik eylemi yapacak kişinin veri toplama yöntemi ne olursa olsun temel düşüncesi "hiçbir bilgi gereksiz değildir" olmalıdır.[174] Sosyal mühendislik faaliyetlerinde hedef ile bire bir temasa geçme zorunluluğu da bulunmamaktadır. Son yıllarda sıkça kullanılan ve otomatik olarak birçok kullanıcıya gönderilen *spam* e-postaları da birçok hesabın ele geçirilmesinde etkili olmaktadır.

[173] JUDICIARY OF ENGLAND AND WALES, (2018), The Queen -v- Kane Gamble, Sentencing Remarks of the Hon. Mr Justice Haddon-Cave, (Çevrimiçi) https://www.judiciary.uk/wp-content/uploads/2018/04/r-v-gamble-sentencing.pdf (Erişim tarihi: 21 Nisan 2021), s. 2-3.

[174] Paul F. Kelly, Sosyal Mühendisin Maskesini Düşürmek, İstanbul: Paloma Yayınevi, 2018, ss. 47-49.

Tablo 4: İkna Yoluyla Dolandırıcılık Süreci

SUÇUN HAZIRLIK HAREKETLERİ	SUÇUN İCRASI	SUÇUN SONUÇLANMASI
Gizlenmeye Uygun Lokasyonlarda Sahte Çağrı Merkezinin Belirlenmesi	Mobil Telefonlardan İletişimin Başlatılması	Hesap ve Kredi Kartı Bilgilerinin Elde Edilmesi
Fiziki Şartların Oluşturulması	**Vaatler Yöntemi** Kurgu Teklifler ve Senaryoların Kullanılması **Korkutma Yöntemi** Kamu ve Özel Sektör Görevlileri Unvan ve Sıfatlarının Kullanılması **Yardım Kampanyaları Yöntemi** Sözde Yardım Kampanyalarının Düzenlenmesi	Mobil Telefonlara Şifre Gönderilmesi ve Tuşlanma Talebinin İletilmesi • Şifrenin Tuşlanması ile Ödeme Talimatı • Hesaba Transfer/EFT/Havale Talimatı • E-ticaret Sitelerinden Alışveriş Talimatı
Teknik Altyapının Oluşturulması • VoIP Teknoloji Kullanımı	İkna İletişiminin Sürdürülmesi	İkna Dolandırıcılığının Gerçekleşmesi
Örgüt Üyesi Seçimi ve Eğitimi Son Hesap Sahiplerinin Tespiti Kişilere Ait Özel Verilerin Elde Edilmesi • Dark Web – Insider Faktörü • Phishing Siteler – Veri Çöplüğü Analizi		İkna Dolandırıcılığını Sonlandırılması • Banka Şubelerinden Mevduatın Çekilmesi • Başka Hesaba Transfer/EFT/ Havale Edilmesi

Kaynak: Atalay Bahar, "İkna Yoluyla Dolandırıcılık: Dolandırıcılık Faaliyetlerinde İkna ve Etkili İletişim Yöntemlerinin Tespiti Üzerine Bir Araştırma", **Türkiye İletişim Araştırmaları Dergisi**, 2018, S. 35, s. 145.

3.2.5.4. Algı Yönetimi

Yeni medyanın önceki bölümlerde bahsedilmiş olan olumlu ve olumsuz taraflarına ek olarak toplumsal hareketlerin genişlemesi ve yayılmasında da uygun imkânlar sunduğu görülmektedir. Toplumsal hareketlerin en önemli özelliklerinden bir tanesi kolektif bilincin oluşturulmasıdır. İşçi ve milliyetçi hareketlerin ağırlıklı olduğu eski toplumsal hareketler ile daha çok 1970'lerde ortaya çıkan çevre, insan hakları, barış ve feminizm gibi temaların bulunduğu yeni toplumsal hareketler, eylemlerini ve propagandalarını geleneksel yöntemlerle yürüterek kitlelere ulaşmayı ve söylemelerini dile getirmeyi amaçlamaktaydı. Yeni medya ise toplumsal hareketlerin oluşturması gereken kolektif bilincin kitlelere yayılması konusunda etkili teknolojik imkânlar sunmaktadır. Bunun en büyük örneği yakın tarihte gerçekleşen Arap Baharı'dır.

Kısaca özetleyecek olursak, Tunus'taki ekonomik ve işsizlik sıkıntılarının üstüne yolsuzluk iddialarının çıkması başlayan süreçte, üniversite mezunu işsiz bir gencin hayatını devam ettirebilmek için seyyar satıcılık yaptığı el arabasının polisler tarafından el konulması üzerine 18 Aralık 2010 tarihinde kendini yakması ile olaylar başlamıştır. *Facebook*, *Twitter* ve *YouTube* gibi sosyal medya platformlarının Arap Baharı

sürecindeki en etkili iletişim araçlarından bir tanesi olması, bilginin protestocular arasında hızlı dolaşımına katkı sağlaması tansiyonu daha da yükseltmiştir. Komşu ülkelere de sıçrayan Arap Baharı hareketinin neticesinde Tunus, Libya, Mısır, Ürdün gibi ülkelerde yönetim değişikliği yaşanmış Suriye'de ise günümüzde hâlen devam eden iç savaş başlamıştır.[175]

Yeni medya araçlarının Arap Baharı sürecinde etkisi yadsınamayacak düzeyde olsa da sosyal medya bağlamında pek çok tartışmayı beraberinde getirmiştir. Her ne kadar bu argümanla alakalı bilimsel kanıtlar henüz bulunmasa da bir kesim Arap Baharı gibi hareketlerin sosyal medya üzerinden kasıtlı olarak kışkırtıldığını savunurken, diğer bir kesim toplumsal hareketlerin dijitalleşme öncesi dönemlerdeki varlığına atıfta bulunarak sosyal medyaya biçilen bu büyük rolün abartıldığı, bir başka kesim ise sosyal medya ağlarının toplumsal hareketlerin kitlelere ulaşabilmesi için iletişim araçları olduğu yönündedir.

Evgeny Morozov, "Facebook ve Twitter Sadece Devrimcilerin Gittiği Yerlerdir" başlıklı yazısında siber-ütopyacıların Arap Baharı hareketlerinin sosyal ağlar tarafından yönlendirildiğini düşünerek gerçek dünya aktivizmini görmezden geldiklerini ifade etmiştir. Yani bu tarz protesto gösterilerinin kamuya mal edilip, organize edilmesi için internet ve sosyal ağların kullanıldığı argümanının geçerli olabilmesi için halkı aktivist ağlar tarafından düzenlenen bu hareketlerin arka planında bir koordinasyon olup olmadığının ortaya çıkarılmasıdır. [176] Sosyal medya ağlarının Arap Baharı hareketlerinde protestoculara sunduğu bilgi akışı ve iletişim imkânları yadsınamaz bir gerçektir. Fakat Morozov'un yazısında belirttiği gibi bu tip toplumsal hareketler sosyal ağlar üzerinden kendi kendiliğine oluşmamaktadır. Kolektif bir bilinç oluşturulabildiği doğrudur fakat bu bilincin oluşturulmasındaki planlama ve koordinasyon sanal olmayan yöntemler ile başlamıştır.[177]

---

[175]İsmet Göçer ve Sertan Çınar, "Arap Baharı'nın Nedenleri, Uluslararası İlişkiler Boyutu ve Türkiye'nin Dış Ticaret ve Turizm Gelirlerine Etkileri", **KAÜ İİBF Dergisi**, 2015, C. 6, S. 10, ss. 54-55.

[176] Evgeny Morozov, Facebook and Twitter are Just Places Revolutionaries Go, **The Guardian**, 2011, (Çevrimiçi) https://www.theguardian.com/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians (Erişim tarihi: 22 Nisan 2021).

[177] NYTIMES, **A Tunisian-Egyptian Link That Shook Arab History**, 2011, (Çevrimiçi) https://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?_r=0 (Erişim tarihi: 21 Nisan 2021).

Malcolm Gladwell ise benzer bir şekilde *Facebook* icat edilmeden önce de devrimlerin yapıldığını, 1980'lerde Doğu Almanya'da neredeyse hiç kimsenin cep telefonu yokken Leipzig merkezinde yüz binlerce insanın neredeyse bir yüz yıl daha süreceği düşünülen rejimi devirdiklerini ifade etmiştir. Nihayetinde protestocuların organize olmak için kullandığı iletişim araçlarından çok protesto amaçlarının önemli olduğunu vurgulamıştır.[178]

Kitlelerin sosyal ağlar üzerinden bu şekilde organize edilmesi doğal olarak algı yönetimi konusunu gündeme getirmiştir. ABD Savunma Bakanlığı'nın algı yönetimi için yapmış olduğu tanımlama şu şekildedir: *"Kitlelerin duygu, düşünce, amaç, mantık, istihbarat sistemleri ve liderlerini etkileyerek seçili bilgilerin yayılması ve/veya durdurulması: bunun sonucunda hedef davranış ve düşüncelerinin hedefleyenin istekleri doğrultusunda yönlendirilmesi. Algı yönetimi gerçekler, yansıtma, yanıltma ve psikolojik operasyonların bir bütünüdür."*[179] Bu bağlamda sosyal medyanın sunmuş olduğu imkânlar ile eylemlerin maliyetleri düşmüştür. Bireysel katılımın kolaylaşması ve artması ile yeni toplumsal hareketlerin başarıya ulaşması artmıştır.[180] Tabii ki sosyal medyanın sunmuş olduğu bu imkânlar sadece aktivistlerin değil aynı zamanda araştırmacıların ve istihbarat personellerinin de işini kolaylaştırmaktadır. Ben Zimmer bu konu hakkında *Twitter* ve *Facebook* gibi sosyal paylaşım sitelerinin dilbilim, sosyoloji ve psikoloji gibi alanlarda çalışma yapan bilim insanları için de altın değerinde olduğunu, uzun zaman alan zahmetli veri toplama işlemleri yerine araştırmacıların bu verilere sosyal medya platformlarından erişebileceğini belirtmiş ve *Twitteroloji* adı verilen bu çalışmanın küresel ölçekte belli halkların ruh hâlini analiz etmek için kullanıldığını ifade etmiştir.[181]

---

[178] Malcolm, Gladwell, Does Egypt Need Twitter?, **Newyorker**, 2011, (Çevrimiçi) https://www.newyorker.com/news/news-desk/does-egypt-need-twitter (Erişim tarihi: 21 Nisan 2021).

[179] US DEPARTMENT OF DEFENCE, **Perception Management**, (Çevrimiçi) https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4039 (Erişim tarihi: 21 Nisan 2021).

[180] Yücesoy, **a.g.e.,** s. 154.

[181] Deborah McMurray, Have Heard About "Twitterology?" It's the Latest How Now Science, **Lexisnexis**, 2011, (Çevrimiçi) https://www.lexisnexis.com/legalnewsroom/legal-business/b/technology/posts/have-you-heard-about-quot-twitterology-quot-it-s-the-latest-hot-new-science (Erişim tarihi: 21 Nisan 2021).

3.2.5.5. Gözetim Toplumu

İktidar, tarih boyunca ismi ve şekli değişse de sürekli var olan, etrafında olan gelişmelerden sürekli olarak haberdar olmak isteyen ve bu yüzden gelişmeleri denetleyip gözetleyen bir güçtür. Bu gözetim motivasyonu ilerleyen zamanda Foucault'nun metafor olarak kullanacağı, 1785 yılında "Panoptikon" olarak anılan ve Jeremy Bentham tarafından tasarlanan yapı ile açıklanabilir. Kelime kökeni olarak bütün anlamında gelen "pan" ve gözlemlemek anlamına gelen "opticon" kelimelerinden türeyen kavram, "Bütünü Gözetlemek" anlamına gelmektedir. Bahsi geçen bu yapı gözetleyicinin merkezde olduğu yuvarlak bir şekilde tasarlanmıştır. Ana binada içe ve dışa bakan hücreler, yapının tam ortasında ise tüm hücreleri gözetleyebilen bir kule bulunmaktadır. Özel şekilde tasarlanan bu yapıda gözetleyen tüm hücreleri görebilirken, hücrelerin içinden gözetleyen görülememektedir. Bu da gözetleyenin görünmezliği ilkesini temsil eden iktidar rolünü temsil etmektedir.[182]

Şekil 13: Panoptikon Yapı

Kaynak: Mvreview, **Foucault's Panopticon and Understanding Power**, 2018, https://mvreview.home.blog/2018/07/22/foucaults-panopticon/ (Erişim tarihi: 21 Nisan 2021)

Michel Foucault ise bu hapishane yapısını okul, hastane ve fabrikayı da (çünkü ileride Jeremy Bentham bu yapılarda da aynı uygulamayı yapmıştır) dâhil ederek iktidarın

[182] Gizem Özdel, "Foucault Bağlamında İktidarın Görünmezliği ve "Panoptikon" ile "İktidarın Gözü" Göstergeleri", **The Turkish Online Journal of Design, Art and Communication**, 2012, C. 2, S. 1, ss. 22-24.

gözetimini açıklarken bir metafor olarak kullanmıştır. Yapıda gözetleme kulesinin hiçbir şekilde görülememesinin gözetleyenin görünmezliği açısından son derece önemli olduğunu ve bunun tutukluda sürekli olarak gözetleniyor etkisi bırakarak hiçbir sert müdahalede bulunmadan mahkûmu iyi davranmaya, deliyi sakin olmayan, işçiyi çalıştırmaya, okul çocuğunu özenli olmaya, hastayı ise tedavi olmaya sevk edeceğini ifade etmiştir.[183]

Günümüzde ise değişen şartlar ve imkânlar ile gözetleme yöntemleri de değişime uğramış ve çeşitlenmiştir. Bentham'ın panoptikon yapısı yerini televizyon, kamera sistemleri ve internet almıştır. Fakat günümüzde kullanılan bu uygulamalar panoptikon yapıya kıyasla farklı özelliklere sahiptir. Panoptikonun katı gözetiminden ziyade günümüz gözetimini tanımlayan sinoptikon ve omniptikon kavramlarında gözetim gözetlenen tarafından gönüllü bir şekilde kabul edilmektedir. Azınlığın çoğunluğu gözetlediği panoptikonun tam aksine günümüzde televizyon gibi medya yayınlarıyla karşımıza çıkan sinoptikon kavramında çoğunluk azınlığı izlemektedir. Yani özel alanı kamusal alanda yok etmeyi amaçlayan panoptikon, yerini kamusal alanın aşınarak yok olmasını amaçlayan sinoptikona bırakmıştır. Bu şekilde gözetim toplumsal rıza ile durmaksızın devam ederek küresel gözetimde gönüllük durumu ortaya çıkarmaktadır.[184] Azınlığın çoğunluğu izlediği panoptikon kavramı çoğunluğu azınlığı izlediği sinoptikon kavramına, sinoptikon kavramı da günümüzde kullanılan sosyal ağlar ile herkesin herkesi izleyebildiği omniptikon kavramına evirilmiştir.[185] Yani iktidar, sosyal ağ siteleri ve kullanıcıları, sosyal ağ siteleri kullanıcıları, kullanıcılar da birbirilerini izleyebilmektedir. Son iki modelde gözetimde gönüllüğünün haz almaya evirildiği görülmektedir. Fakat bununla beraber kullanıcılar yaptıkları paylaşımların diğer herkes tarafından izlenildiğinin farkındadır ve bu yüzden gerek yaşanabilecek cezai yaptırımlardan gerek ise toplumsal baskıdan çekindikleri için dikkatli hareket etmektedirler.

---

[183] Michel Foucault, **Hapishanenin Doğuşu**, Ankara: İmge Kitabevi, 1992, s. 251-254.

[184] Selin Okmeydan Bitirim, „Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon 've 'Omniptikon'a", **Online Academic Journal of Information Technology**, 2017, C. 8, S. 30, s. 58-60.

[185] Nihal Şener Kocabay, "Eğlencenin Gözetleme Hâli ya da Eğlence Endüstrisinde "Görünen" ve "Gören" Olmak", **TRT Akademi**, 2016, C. 1, S. 6, s. 60.

İnternet ve onun bir ürünü olan sosyal medyanın karakteristik özelliklerinin en başında gelen özgürlük temasından kaynaklı olarak her ne kadar gözetimde gönüllülük olsa da yer yer sansür uygulamaları veya cezai yaptırımlar sebebiyle tartışmalar çıkmaktadır. Örneğin 2018 yılında internet üzerinden yapılacak yayınların RTÜK denetimine alınması kararı sosyal medyada ciddi tepkilere yol açmış ve "Türkiye'de artık internet özgür değil" şeklinde kampanyalar yapılmıştır.[186] Buradaki motivasyon çalışmanın bu bölümünde bahsi geçen iktidarın gözetleme motivasyonundan kaynaklanmaktadır. Omniptikon kavramında herkesin herkesi gözetlemesinden kaynaklı olarak, Türkiye'de günlük erişimi 1 milyonun üzerinden olan sosyal ağ sağlayıcılarının Türkiye'de temsilcilik açması zorunluluğu ve belirlenen süre içerisinde açmamaları hâlinde para cezası, reklam yasağı ve internet yavaşlatması gibi cezai yaptırımların uygulanacak olması tepkilere yol açmıştır.[187] Kullanıcı sayısı, elde ettikleri gelir ve geçmiş dönemlerde yaşanan veri ihlalleri ile siber güvenlik krizleri göz önünde bulundurulduğunda, açılması istenilen temsilcilikler ile iktidar aynı zamanda sosyal ağ sağlayıcılarını da gözetleme motivasyonu bulundurmaktadır. Bu gibi durumlar, internet kullanıcılarının sanal alemdeki özgürlüklerinin kısıtlandığı düşüncesini oluşturacak ve yapacakları paylaşımlarda daha dikkatli olmalarına yol açacaktır. Sonuç olarak uygulanan bu sansür politikalarının da direkt olarak elde edinilebilecek potansiyel veri oranına etkisi görülecektir.

3.3. Sosyal Medya İstihbaratı (SOCMINT)

Tarihten bu yana insanoğlu istihbarat amacıyla teknolojik imkânlardan sürekli olarak yararlanmıştır. İnşa etmiş oldukları yol sistemleri ve kervansaraylar, postacılık, ateş işaretleri, ses sinyalleri, su saatleri, yazının icat edilmesi ile kriptografi, haberleşmek için hayvanların kullanılması bunlardan birkaçıdır.[188] Günümüz teknolojik gelişmelerinden internet ve sosyal medya da bu bağlamda istihbarat amaçlı veri toplama imkânları sunmaktadır. Sosyal medya istihbaratı (SOCMINT) ise istihbarat sürecinde

---

[186] DW, **İnternet Denetimine Sosyal Medyada Tepki**, 2018, (Çevrimiçi) https://www.dw.com/tr/internet-denetimine-sosyal-medyada-tepki/a-43080811 (Erişim tarihi: 21 Nisan 2021).

[187] TRT HABER, Hangi Dijital Medya Platformları Türkiye'de Temsilcilik Açıyor?, 2021, (Çevrimiçi) https://www.trthaber.com/haber/bilim-teknoloji/hangi-dijital-medya-platformlari-turkiyede-temsilcilik-aciyor-545811.html (Erişim tarihi: 21 Nisan 2021).

[188] Rose Mary Sheldon, **Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages**, North Carolina: Mc Farland & Company, Inc Publishers, 2003, s. 18-19.

yeni bir veri toplama yöntemi olarak karşımıza çıkmaktadır. Temel olarak sosyal medya ortamından elde edilen verilerin ve bireylerin düşünceleri veya davranışlarını karakterize edebilecek durumların tanımlanması ve anlaşılabilmesi için açık kaynak istihbaratından (OSINT) ve web madenciliği tekniklerinden yararlanılarak analitik bir biçimde kullanımını öngörmektedir.[189]

Bu bağlamda sosyal medyanın kullanımı ve potansiyel veri kapasitesi çalışmanın önceki bölümlerinde paylaşılmış ve sosyal medyanın muazzam bir veri imkânı sunduğu görülmüştür. Fakat istihbarat sürecinde ihtiyaç duyulan sadece ham veri veya enformasyon değildir. İhtiyaçları asıl karşılayacak olan bunların tasnifleme, işleme ve analiz gibi süreçlerden geçirilmesi sonucu elde edilen bilgidir. Bu çerçevede sosyal medyanın kapasitesine bakıldığında geleneksel yöntemler kullanılarak belirtilen işlemlerin uygulanamayacağı kadar fazla veri olduğu görülmektedir. Bu durumu tanımlamak için kullanılan "Büyük Veri" terimi; hem yüksek düzeyde karmaşıklığa sahip büyük hacimli verileri hem de bu verileri gelişmiş teknik ve teknolojik imkânlar ile anlamlı hâle getirecek analitik metotları tanımlamaktadır.[190] Yani anlamsız bir şekilde yığılmış binlerce verinin anlamlı hâle dönüştürülmüş biçimidir. Bu sebeple büyük verinin analize hazır hâle getirilmesi için yapay zekâ raporlama araçları kullanılmaktadır. Bunlardan en önemlisi, algoritmalara kalıpları tanımanın ve insanların bilgi parçalarının içindeki görmediği anlamların öğretildiği bir yapay zekâ çeşidi olan makine öğrenmesidir. Makine öğreniminin önemli uygulamalarından biri olan "Sentiment Analysis" ise hedef/hedeflerin duygu ve duyarlılık analizini yapmaktadır. Algoritmaya duyguların metinsel örnekleri tanımlandıktan sonra bu duyguyu araması istendiğinde veri hacimlerini otomatik olarak sınıflandırabilmektedir. Yapılan bu duygu analizi işlemleri ile sosyal medya kullanıcılarının hangi siyasi partiye nasıl duygular beslediği, ruh hâli veya suç potansiyeli öğrenilebilmektedir.[191] Buna benzer bir uygulama olan *Facebook* algoritmasından çalışmanın önceki bölümlerinde bahsedilmiştir.

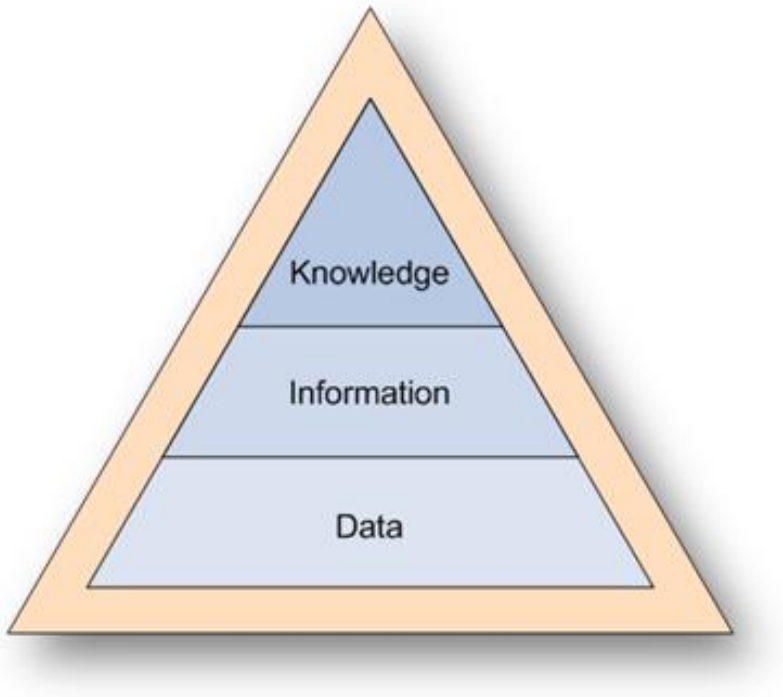
---

[189] Elena ŞUŞNEA And Adrian IFTENE, The Significance of Monitoring Activities fort he Social Media Intelligence (SOCMINT), **MFOI**, 2018, s. 231.

[190] GOV.UK, Emerging Technologies: Big Data, Hm Government Horizon Scanning Programme, 2014, https://www.gov.uk/government/publications/emerging-technologies-big-data (Erişim tarihi: 22 Nisan 2021), s. 2.

[191] Sir David Omand, Jamie Bartlett & Carl Miller, "Introducing Social Media Intelligence (SOCMINT)", **Intelligence and National Security**, 2012, Vol. 27, No. 6, s. 810-811.

Yapay zekâ uygulamaları her ne kadar verilerin toplanması, sınıflandırılması ve analizi konusunda ciddi katkılar sunuyor olsa da verinin bilgiye dönüştürülmesi sürecinde tek başına yeterli olamamaktadır.



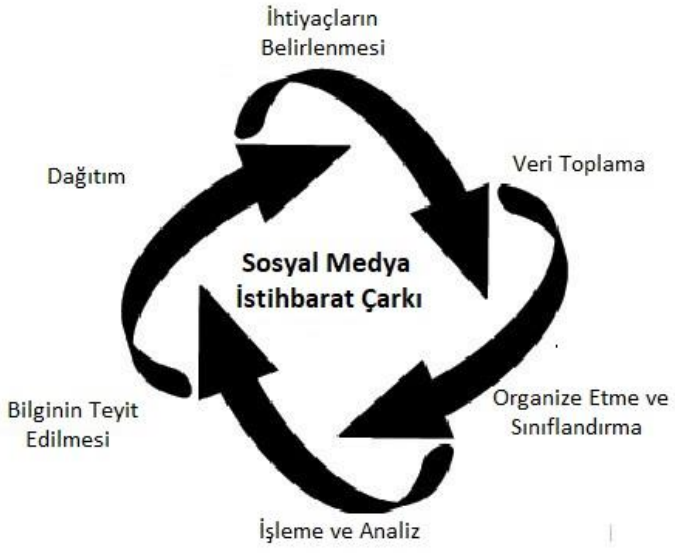
Şekil 14: Veri, Enformasyon ve Bilgi Hiyerarşisi

Kaynak: Gollner.ca, **Putting Content In Its Place,** 2014, https://www.gollner.ca/2014/04/putting-content-in-its-place.html (Erişim tarihi: 23 Nisan 2021).

Şekilde gösterilen piramitte veri veya büyük veri en alt kısımda bulunmaktadır. Veri, toplama, organize etme ve sınıflandırma işleminden sonra enformasyon hâlini alır. Analiz edilip özetlenen enformasyon ise bilgiye dönüştürülür ve karar vericilere dağıtımı sağlanır. Yapay zekâ algoritmalarının ve modüllerin analiz edilmeye hazır hâle getirdikleri veriler insani faktörlerden ötürü başarılı sonuçlar vermeyebilir. ABD'de Ismaaiyl Brinsley'in *Instagram* hesabından gümüş bir silah paylaşarak polisleri tehdit ettiği paylaşımından sonra iki polisi öldürmesi haberinin üzerine, müşterileri için sosyal medya analizleri yapan Recorded Future Inc. şirketinin kurucu ortağı Christopher Ahlberg'in, "İstediğiniz tüm teknolojiyi satın alabilirsiniz ancak zekice şeyler bulmak istiyorsanız, onu kullanacak akıllı insanlara sahip olmalısınız." açıklaması yapay zeka teknolojisi kadar kaliteli personelin önemini de göstermektedir. Sonuç olarak elde edilen bilginin nasıl kullanılacağına dair nihai kararı insan aklı verecektir.

3.3.1. Sosyal Medya İstihbarat Çarkı

İstihbarat kavramının açıklandığı çalışmanın ikinci bölümünde istihbarat çarklarına da yer verilmiştir. Şekil 14'te ise geleneksel istihbarat çark modelinden yararlanılarak hazırlanmış sosyal medya istihbarat çarkı gösterilmektedir.



Şekil 15: Sosyal Medya İstihbarat Çarkı

İstihbarat çarklarında ihtiyaçlar ve uygulanan politikalar doğrultusunda farklılık olmasından kaynaklı olarak sosyal medya istihbarat çarkının da kendi özellikleri bulunmaktadır. Temel olarak geleneksel model ile benzeşiyor olsa da sosyal medya istihbarat çarkında veri toplama işleminden sonra sosyal medyadaki veri kirliliğinden ötürü toplanan verilerin organize edilmesi ve sınıflandırılması aşaması bulunmaktadır. İşleme ve analiz sürecinden sonra ise sosyal medya bilgilerinin HUMINT kaynaklarından doğrulanması gerekmektedir. Geleneksel istihbarat modelinde HUMINT yöntemi ile toplanan bilgilerin dahi doğru kaynaklardan elde edilmesi kritik önem taşımakta iken sosyal medyadan toplanan verilerin teyit edilmesi, algı-olgu kavramlarının daha iyi analiz edilip, kaynakların doğru kullanılmasını sağlayacaktır.

3.3.1.1. İhtiyaçların Belirlenmesi

Sosyal medya istihbarat sürecinin ilk aşaması olan ihtiyaçların belirlenmesi; spesifik bir alanda ihtiyaç duyulan bilgiye sosyal medya vasıtası ile erişim elde edinilebileceğinin tespiti sonucunda SOCMINT'in uygulanmasına karar verilmesidir. Sosyal medyadan elde edilecek verilerin çok çeşitli olmasından kaynaklı olarak amaçlarda bu duruma

paralel birçok farklı alan da ortaya çıkabilmektedir. İstihbaratın önleyici bir faaliyet olmasından dolayı bu ihtiyaçlar toplumda travma etkisi yaratabilecek bir olaya kamuoyunu tepkisini ölçmek veya önlem almak olabileceği gibi, doğal afet sonucunda zarar gören insanlara ulaşma ve yardım etme amacıyla dahi kullanılabilir.

Örneğin; ABD'nin Ohio eyaletinde yaşanan Chardon Lisesi silahlı saldırısı esnasında öğrenciler içerideki durumlarını *Twitter* üzerinden bildirmiştir.[192] Aynı olayda silahlı saldırıyı gerçekleştiren şahıs okula gelmeden önce *Twitter* üzerinden, zorbalığa uğradığını ve okula bir silah getireceğine dair *tweet* atmış fakat kimse bunu dikkate almamıştır.[193] Bu olay örneklem olarak alınacak olursa; SOCMINT yöntemi, ihtiyaçların belirlenmesi aşamasında olayın gerçekleştiği zaman diliminde okul içinde bulunan öğretmen, öğrenci ve personellerin sosyal medya hesaplarının incelenmesini öngörmektedir.

3.3.1.2. Veri Toplama

Sosyal medya istihbaratında ihtiyaçların spesifik olarak belirlenmesinden sonraki süreçte dahi erişilebilecek veri sayısı muazzam derecedir. 6-11 Ağustos 2011 tarihinde Londra'da gerçekleşen isyanlarda ilgili materyaller için sosyal medya üzerinden veri toplama işleminin zorluğunu profesyonel bir istihbarat personeli; Britanya Kütüphanesi'nde indeks olmaksızın bir kitabın belirli bir sayfasını aramaya benzetmiştir. Polis memurlarından birisi ise çok fazla veri paylaşımı yapılmasından kaynaklı olarak bir *tweet*i okumayı bitiremeden sayfanın en altına düştüğünü belirtmiştir.[194]

ABD'nin büyük tepkilere sebebiyet veren Prizma ve İngiliz gizli servisinin uyguladığı izleme programlarında genel bir izleme ve takip etme politikası yürütüldüğü için kısıtlı bir zaman söz konusu değildir.[195] Fakat kriz anlarında kullanıcılar tarafından veri

---

[192] Lauran Dugan, Twitter Used As Impromptu Emergency Broadcast System During Ohio School Shooting, **Adweek**, 2012, (Çevrimiçi) https://www.adweek.com/performance-marketing/twitter-used-as-impromptu-emergency-broadcast-system-during-ohio-school-shooting/ (Erişim tarihi: 23 Nisan 2021).

[193] Janice D'Arcy, The Ohio School Shooting and Missed Warning Signs on Twitter, 2012, (Çevrimiçi) https://www.washingtonpost.com/blogs/on-parenting/post/the-ohio-school-shooting-and-missed-warning-signs-on-twitter/2012/02/27/gIQABBmUeR_blog.html (Erişim tarihi: 23 Nisan 2021).

[194] HMIC, The Rules of Engagement, A Review of the August 2011 Disorders, (Çevrimiçi) https://www.justiceinspectorates.gov.uk/hmicfrs/media/a-review-of-the-august-2011-disorders-20111220.pdf (Erişim tarihi: 23 Nisan 2021), s. 31 – 2.22.

[195] TERRAMEDUSA, **Casuslukta İngilizce Asaleti: SOCMINT**, 2013, (Çevrimiçi) https://terramedusa.com/casuslukta-ingiliz-asaleti-socmint/ (Erişim tarihi: 23 Nisan 2021).

girişinin artması geleneksel metotları işlevsiz bırakmaktadır. Sonuç olarak önleyici bir faaliyet olan istihbarat için zaman -özellikle kritik dönemlerde- çok önemli bir etkendir. Bu yüzden teknik imkânlar sadece verilerin analizinde değil toplama işleminde de kullanılmaktadır. Bu sebeple veri trafiğinin fazla olduğu zaman dilimlerinde "ileri teknoloji yapay zekâ algoritmaları" dışında da bazı araçlar bulunmaktadır.

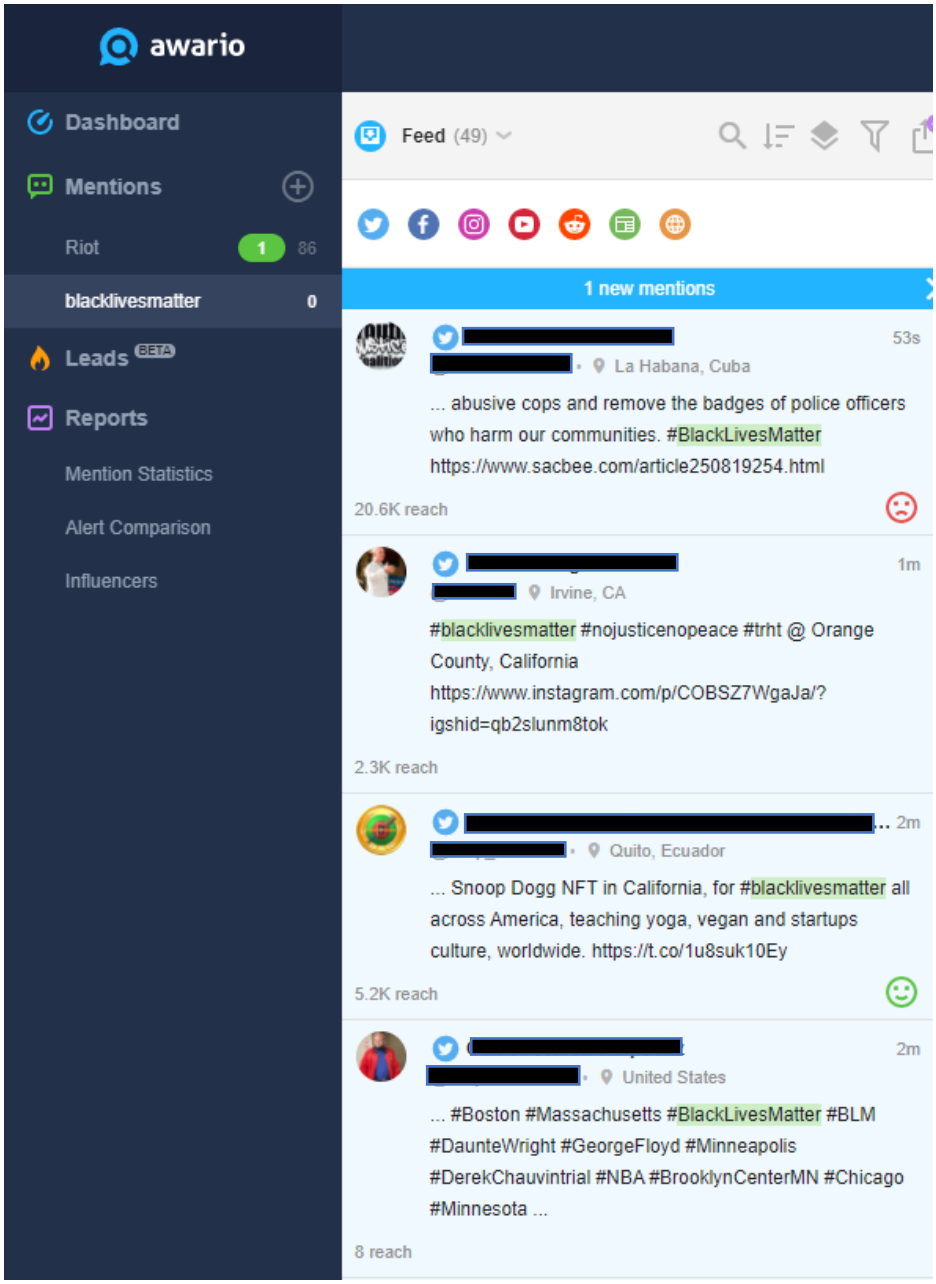
3.3.1.2.1.Google Alerts

Günümüz itibari ile en iyi arama motoru olan *Google*'ın sunmuş olduğu bu araç, çok basit bir şekilde e-posta adresinizi kullanarak veri toplamanıza imkân sunmaktadır. *Google Alerts*, spesifik olarak belirlediğiniz bir kelimenin internette kullanımı hâlinde size e-posta olarak bildirimde bulunan bir sistemdir. Kullanıcılar bu uygulamayı birçok farklı amaçla kullanabilmektedir. Örneğin; ticari amaçlar için kendi markanız veya ürününüz için oluşturacağınız *Google* Uyarısı, markanız veya ürününüz hakkında size anlık *feedback* imkânı sunacaktır. Habercilik, hobiler hatta iş aramak için bile veri toplamada faydalı olabilmektedir.[196]

3.3.1.2.2.Awarıo

Awario aracı ise yine seçeceğiniz bir kelime ile *Twitter, Facebook, Instagram, Youtube* ve *Reddit* gibi sosyal medya sitelerinde seçmiş olduğunuz kelimenin kullanıldığı paylaşımları göstermektedir.

[196] Elisa Gabbert, "How Do Google Alerts Work? Why Are They Not Working?", **Wordstream**, 2020, (Çevrimiçi) https://www.wordstream.com/blog/ws/2012/04/10/google-alerts (Erişim tarihi: 23 Nisan 2021).



Şekil 16: Awario Kelime Filtreleme

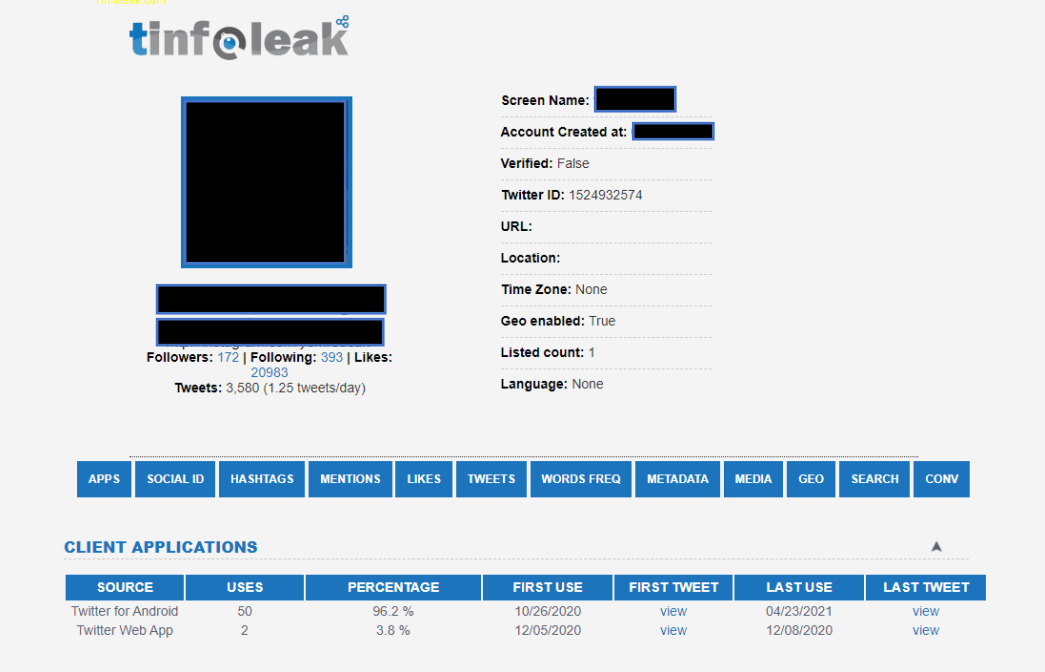
Kaynak: https://app.awario.com, (Erişim tarihi: 23 Nisan 2021)

Uygulama içerisinde "riot" ve "blacklivesmatter" kelimelerinin aratılması ile elde edilen sonuçlar gösterilmiştir.

3.3.1.2.3.Tinfoleak

Sosyal medya istihbaratı kitlelerin veya genel bir durumun analizini yapmak için veri toplayabileceği gibi belirli kişiler hakkında da bilgi toplamayı amaçlayabilir. *Tinfoleak* aracı ise bu tarz bir amaç için kişilerin Twitter profil analizini yapmaya yarayan bir

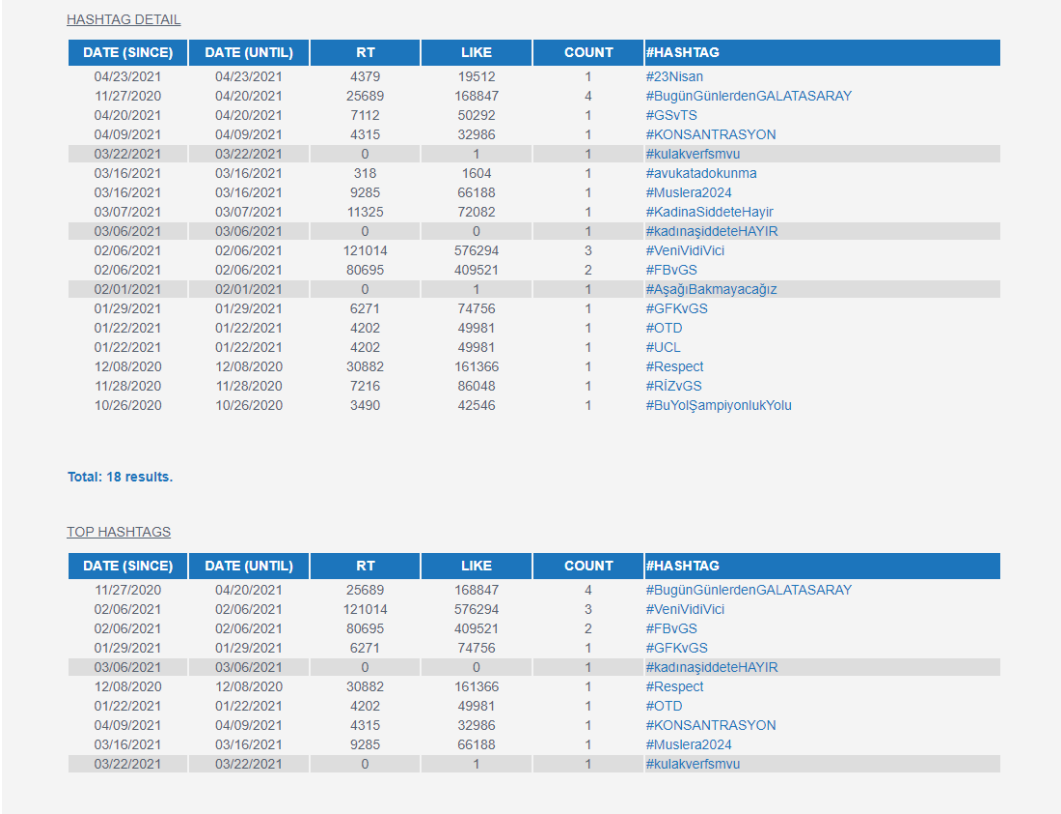
uygulamadır. Tamamen ücretsiz ver herkesin erişimine açık olan bu uygulamanın örnek çalışması Şekil 16'da paylaşılmıştır.



Şekil 17: Tinfoleak Örnek Çalışma

Kaynak: https://tinfoleak.com

Takip edilecek hesap hakkında birçok veri sunan *Tinfoleak* uygulaması basit bir şekilde kişinin kullanıcı adının girilmesi ile detaylı bir rapor sunmaktadır. Bu raporda *Twitter* ID olarak yazan 1524932574 numarası kullanıcı profilinin değişmeyen ID numarasıdır. Yani ilerleyen süreçte kullanıcı adı veya isim değiştirilse de hesaba bu ID numarası ile ulaşılabilmektedir.



HASHTAG DETAIL

DATE (SINCE)	DATE (UNTIL)	RT	LIKE	COUNT	#HASHTAG
04/23/2021	04/23/2021	4379	19512	1	#23Nisan
11/27/2020	04/20/2021	25689	168847	4	#BugünGünlerdenGALATASARAY
04/20/2021	04/20/2021	7112	50292	1	#GSvTS
04/09/2021	04/09/2021	4315	32986	1	#KONSANTRASYON
03/22/2021	03/22/2021	0	1	1	#kulakverfsmvu
03/16/2021	03/16/2021	318	1604	1	#avukatadokunma
03/16/2021	03/16/2021	9285	66188	1	#Muslera2024
03/07/2021	03/07/2021	11325	72082	1	#KadinaSiddeteHayir
03/06/2021	03/06/2021	0	0	1	#kadınaşiddeteHAYIR
02/06/2021	02/06/2021	121014	576294	3	#VeniVidiVici
02/06/2021	02/06/2021	80695	409521	2	#FBvGS
02/01/2021	02/01/2021	0	1	1	#AşağıBakmayacağız
01/29/2021	01/29/2021	6271	74756	1	#GFKvGS
01/22/2021	01/22/2021	4202	49981	1	#OTD
01/22/2021	01/22/2021	4202	49981	1	#UCL
12/08/2020	12/08/2020	30882	161366	1	#Respect
11/28/2020	11/28/2020	7216	86048	1	#RİZvGS
10/26/2020	10/26/2020	3490	42546	1	#BuYolŞampiyonlukYolu

Total: 18 results.

TOP HASHTAGS

DATE (SINCE)	DATE (UNTIL)	RT	LIKE	COUNT	#HASHTAG
11/27/2020	04/20/2021	25689	168847	4	#BugünGünlerdenGALATASARAY
02/06/2021	02/06/2021	121014	576294	3	#VeniVidiVici
02/06/2021	02/06/2021	80695	409521	2	#FBvGS
01/29/2021	01/29/2021	6271	74756	1	#GFKvGS
03/06/2021	03/06/2021	0	0	1	#kadınaşiddeteHAYIR
12/08/2020	12/08/2020	30882	161366	1	#Respect
01/22/2021	01/22/2021	4202	49981	1	#OTD
04/09/2021	04/09/2021	4315	32986	1	#KONSANTRASYON
03/16/2021	03/16/2021	9285	66188	1	#Muslera2024
03/22/2021	03/22/2021	0	1	1	#kulakverfsmvu

Şekil 18: Tinfoleak Örnek Çalışma 2

Kaynak: https://tinfoleak.com

Raporun devamında kullanıcının hangi *hashtag*lere katıldığı, en çok hangi kullanıcılar ile etkileşimde olduğu, *geo-location* bilgileri ve en çok kullandığı kelimeler gibi veriler de sunulmaktadır. Bu uygulama aracılığıyla örneklem olarak kullanılan hesabın verileri hedef kişi hakkında önemli bilgiler sunarken, çalışmanın alanyazın kısmında bahsi geçen veri toplama yöntemi biyografik istihbarat için de destekleyici bir potansiyel taşımaktadır.

3.3.1.3. Organize Etmek ve Sınıflandırmak

Veri toplama işleminde kullanılan araçlar ne kadar etkin olursa olsun veri kirliliğinden kaynaklı olarak birçok gereksiz bilgi araya sızacaktır. İhtiyaçlar doğrultusunda farklı algoritma ve araçlardan yararlanılarak elde edilen verilerin analiz sürecine geçilmeden önce filtreme ve ayıklama gibi süreçlerden geçirilerek organize edilmesi ve sınıflandırılması gerekmektedir. Örneğin Türkiye'deki *Twitter* trendleri üzerinden bilgi çıkarımı yapılması üzerine hazırlanan bir çalışmada, 1 aylık süre makasında 62.273 adet veri elde edilmiş ve bu veriler analiz sürecine geçirilmeden önce "Tweetler", "Etiketler" ve "Cevaplar" olmak üzere üç gruba ayrılmıştır. Kendi içinde incelenen ve

değerlendirilen bu verilerin sonucu olarak 22.626 adet *tweet*, 38.766 adet etiket ve 796 adet cevaplama verisi ortaya çıkmış, işe yaramayacak 85 veri ise silinmiştir. *Tweet*lerin bütün hâlinde analiz edilmesi sonucunda çok fazla Uniform Resource Locator (URL) bulunmuştur. Bu durum Türkiye'deki Trending Topic (TT) listelerinin çoğunluğunun reklam amaçlı kullanıldığını göstermektedir. Bu sebeple elde edilen verilerden bazı anlamları bilgilere ulaşılabildiğinin fakat gerçek verilere ulaşabilmek için verilerin öncelikle kendi içerisinde temizlenmesi gerektiğinin sonucuna varılmıştır.[197]

Bu bağlamda birçok bot hesabının reklam amaçlı *trend topic*leri kullanması ve akabinde bilgi kirliliğine sebep olması SOCMINT sürecini olumsuz etkileyen faktörlerden bir tanesidir. Bu yüzden sürecin sonunda sağlıklı sonuçlar alabilmek için elde edilen verilerin reklam vb. içerikli kirli bilgilerden arındırılıp analiz sürecine hazır hâle getirilmesi kritik önem taşımaktadır.

3.3.1.4. İşleme ve Analiz

Makine öğrenmesi ve *sentiment analysis* gibi yapay zekâ algoritmalarına bölümün başında değinilmiştir. Bu bölümde bahsi geçen yapay zekâ algoritmaları, analiz sürecinde kullanılabilecek diğer araçlar ve insan faktörü detaylı bir şekilde ele alınacaktır. Ham veri ile enformasyonun güvenilirliği ve doğruluğu tam olarak netleştirilemediği için istihbarat sürecinde etkin bir biçimde kullanımı ancak doğru şekilde analiz edilmesi ile sağlanabilir. Sosyal medya verilerinin analiz edilme süreci, diğer veri toplama yöntemlerine göre daha kompleks bir yapıya sahiptir. SOCMINT analiz süreci, büyük veri kümelerinin geleneksel biçimde personeller tarafından yürütülmesinden ziyade daha hızlı ve kapsamlı olan, insan varlığının rutin katılımı olmadan otomatik olarak hesaplamalar yapabilen yapay zekâ algoritmalarının daha etkili olduğu bir alandır.[198]

Bu çerçevede dil ve kültür büyük önem taşımaktadır. Çünkü hem veri toplama hem de analiz sürecinde yapay zekâya kelime veya kalıp tanımlamaları yapılırken günlük dilin tercih edilmesi elde edilecek sonucu etkileyebilmektedir.[199] Günlük yaşamda dahi dil ve kültür farklılıklardan ötürü bir duyguyu veya olayı anlatım biçimi kişiden kişiye değişiklik gösterebilmekteyken internet gibi kendi jargonu olan bir ortamda analistlerin

---

[197] Serkan Savaş ve, Nurettin Topaloğlu, "Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri", **8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, 2015, s. 65-67.

[198] Omand, vd., **a.g.e.**, s. 810.

[199] Omand, vd., **a.g.e.**, s. 812-813.

bu duruma yetkin olması gerekmektedir. Misal vermek gerekirse; ELI5 kelimesi normal birisi için hiçbir anlam taşımıyorken, internet ortamında bir şey anlaşılamadığında daha basitçe anlatılmasının istendiği "Explain Like I'm 5" kalıbının karşılığıdır. IMHO (In My Humble Opinion), TBH (To be Honest) veya TL; DR (Too Long; Didn't Read) gibi kısaltma kalıpları internette yaygın bir biçimde kullanılan jargonu temsil etmektedir. Bu bağlamda SOCMINT analistlerinin faydalanabileceği siber uzay ve sosyal medya sözlüğü çalışması da yapılmalıdır. Çünkü personeller dahi internet jargonuna hâkim değilken bu gibi kalıpların yapay zekâyı tanımlanmasını beklemek pek sağlıklı olmayacaktır.

Neredeyse çok yeni olan SOCMINT yönteminin bahsi geçen alanlarda dezavantajları olduğu gibi kitlelerin ruh hâlini ve duygularını izleyerek potansiyel asayiş sorunlarını tahmin etmek gibi avantajları da bulunmaktadır. Bu çerçevede devlet kurumlarına yardımcı olabilecek hâlihazırda sosyal medya analizi yapan özel şirketler bulunmaktadır. HMIC'nin (Kraliyet Polis Teşkilatı Müfettişliği) veri analizi alanında çalışan Vega and Autonomy ve Dettica yaptığı görüşmeler sonucunda sosyal medya analizinin birtakım faydaları olduğu tespit edilmiştir. Bunlar kısaca: ayrıntılı analiz için her mesajı okuma zorunluluğu olmadan hızlı bir şekilde belirli mesaj gruplarını tarama, iletişimde ruh hâlini ve duyguyu ölçmek, verilerin anahtar kelimeler ve sözcük grupları üzerinden taranması, farklı kaynaklara tek noktadan erişim, sosyal medya kullanımındaki anormallikleri ve olağan dışı davranışları tespit etme karar verme sürecini destelemek için gelişmeleri takip etmek.[200]

Bu bağlamda sosyal medya verilerinin analizinde kullanılan araçların; ses, video, metin veya veri görüntülerinde bağlantıları tanımlayan sistemleri arayarak veri havuzunda depolayan multimedya analizi, verilerin analizi yoluyla dilleri öğrenen çok dilli analiz, isimleri ve yerleri coğrafi konumlara dönüştüren coğrafi kodlama, çevrimiçi sohbetlerin kilit kullanıcılarını ve yapılarını tanımlayan sosyal ağ analizi gibi işlevleri bulunmaktadır.[201]

[200] HMIC, **a.g.e.,** s. 36-37.

[201] HMIC, **a.g.e.,** s. 37.

3.3.1.4.1.Sosyal Medya Verilerinin Analizinde Kullanılan Algoritmalar ve Araçlar

3.3.1.4.1.1.Nodexl

Kabaca, internet âlemi milyarca kullanıcı arasındaki trilyonlarca bağlantıdan meydana gelmektedir. Kullanıcının internete bağlandıktan sonra yapmış olduğunu tüm eylemler (etkileşimler, beğeniler, sohbetler vb.) onu diğer tüm kullanıcılarla, paylaşımlarla, mekânlar ve nesneler ile birbirine görünmeyen bir bağ ile bağlayan muazzam bir ağı oluşturmaktadır. İnternet üzerinden veri toplayarak bu görünmeyen bağları görmek ve analiz etmek için ileri düzey programlama ve veri yönetimi bilgisi gerekmektedir.[202] NodeXL ise neredeyse hiçbir programlama becerisi istemeden kullanıcıların sosyal ağ analizi yapmasını sağlayan bir yazılımdır. Microsoft Excel'in (2007, 2010, 2013 ve 2016) bir eklentisi olarak çalışan yazılım *Twitter*, *Facebook*, *YouTube* ve *Flickr* gibi sosyal medya sitelerindeki verilerin analizini sağlamaktadır. Yapılan ağ analizini görsel olarak sunan NodeXL yazılımı, verilerin filtrelenmesi, seçimi, kümelenmesi ve sıralanması gibi imkânlar sunmaktadır.[203]

Bu vasıtayla ağ analizi, sosyal ilişkilerin gizli kalmış yapılarını görmek ve anlamak için kullanılmaktadır. Böylece kişiler arasındaki enformel sosyal ilişkilerin karmaşık yapısı istatiksel ağ yöntemleri ile analiz edilir.[204] Ağ analizi yöntemi sosyal medya üzerinden analiz yapabileceği gibi ABD seçimlerindeki senato oylamasını analize tabi tutarak hangi senatörün parti üyeliğini değiştireceğini dair ilginç bilgiler sunabilmektedir.

3.3.1.4.1.2.Polinode

Polinode, NodeXL yazılımına benzer şekilde ağ verilerini toplamaya, analiz etmeye ve istenildiği takdirde bulut sistemi üzerinde muhafaza edilmesine yaramaktadır. E-posta, anlık mesajlaşmalar, performans incelemeleri ve sosyal ağ siteleri gibi mevcut tüm ağ verilerini toplayarak aradığınız spesifik bir soruya cevap vermeye yaramaktadır. Bu soru, "Kiminle ve ne sıklıkla çalışıyor? Tavsiye almak için kimlerden yararlanır?" gibi

---

[202] Fatma Sert, Selim Tüzüntürk & Necmi Gürsakal, **NodeXL ile Sosyal Ağ Analizi: #akademikzam Örneği,** 2014, (Çevrimiçi) https://www.researchgate.net/profile/Fatma-Sert-Eteman/publication/301650244_NodeXL_ile_Sosyal_Ag_Analizi_akademikzam_Ornegi/links/571fc5e108aeaced788ac917/NodeXL-ile-Sosyal-Ag-Analizi-akademikzam-Oernegi.pdf (Erişim tarihi: 24 Nisan 2021), s. 3.

[203] NodeXL, **CodePlex Archive**, (Çevrimiçi) https://archive.codeplex.com/?p=nodexl (Erişim tarihi: 24 Nisan 2021).

[204] Sert, vd.**, a.g.e.,** s. 1.

bir kişi veya firma hakkında sorulara yanıt verebilirken, insanlar arasındaki ilişkileri de analiz etme imkânı sunmaktadır.[205]

3.3.1.4.1.3.Palantir

Palantir Technologies ABD menşeli bir yazılım şirketidir. Çoğunlukla Palantir Gotham, Palantir Foundry ve Palantir Metropolis projeleri ile gündeme gelmekte ve veri analizi konusunda sayılı şirketlerdendir. Palantir Gotham uygulaması ABD İstihbarat Topluluğu ve ABD Savunma Bakanlığında terörle mücadele analistleri tarafından kullanılmaktadır. Yazılım, iş birliğine dayalı analiz ve raporlama için eş zamanlı düzenlemeye olanak tanımaktadır. Şirketin yazılımsal altyapısı birçok farklı alanda hizmet sunmaktadır. Yapay zekâ ve makine öğrenimi kurmak, eğitmek, değerlendirmek ve altyapıyı iyileştirmek için araçlar sağlamakta, büyük ölçekli verileri kullanışlı hâle getirerek analistlerin verileri doğrulamak için harcayacağı vakti verileri anlamak ve kullanmak için harcamasına olanak tanımaktadır.[206]

3.3.1.4.1.4.Senticnet

İnternetteki sosyal veriler her ne kadar insanlar tarafından rahatlıkla anlaşılabilir olsa da aynı şey makineler için geçerli değildir. Bu çerçevede makine öğrenmesini dilbilim ve anlambilim ile birlikte kullanarak kelimeler ve kelimeler ile iletilen duygular arasındaki bilişsel ve duyuşsal boşluğu kapatmak için fikir madenciliği ve duygu analizi için kullanılan bir sistem olan SenticNet 2 geliştirilmiştir.[207]

Sistem basitçe, yapay zekâya bir metin hâlinde duyguları tanımlayarak istenilen verileri, pozitif, negatif veya nötr şeklinde analiz etmesini sağlamaktadır. Duygu analizi pek çok farklı alanda hizmet sunabilmektedir. Bir firma yeni çıkaracağı ürünü ile ilgili sosyal medya üzerinden müşterilerinin geri dönüşlerini analiz edebilir veya bir siyasetçi seçim kampanyası hakkında seçmenlerin ne düşündüğünü bu analiz yöntemi ile öğrenebilmektedir. Fakat sosyal medya platformlarında *emoji* ve kısaltmalar ile kullanılan dilin analizin sonucunu etkileme potansiyeli bulunmaktadır.

---

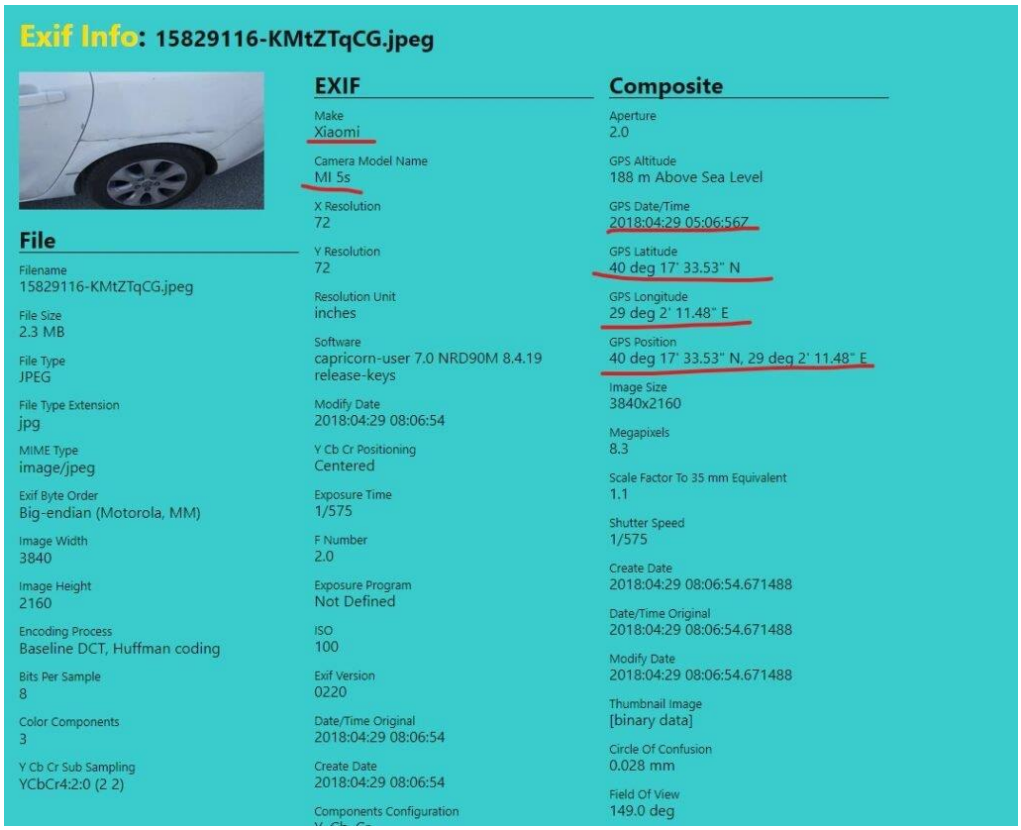
[205] Polinode, **What is Polinode? What Can I Use It For?,** (Çevrimiçi) https://www.polinode.com/#:~:text=Polinode%20allows%20you%20to%20import,visualize%20it%20and%20analyze%20it.&text=Most%20often%20Polinode%20is%20used%20within%20organizations%20for%20organizational%20network%20analysis (Erişim tarihi: 24 Nisan 2021).

[206] PALANTIR, **Intelligence**,(Çevrimiçi) https://www.palantir.com/solutions/intelligence/ (Erişim tarihi: 24 Nisan 2021).

[207] Erik Cambria, Catherine Havasi & Amir Hussain, **SenticNet 2: A Semantic and Affective Resource for Opinion Mining and Sentiment Analysis**, Association for the Advancement of Artificial Intelligence (aaai.org), 2012, s. 202.

3.3.1.4.1.5.Exif Araçları

Fotoğrafların GPS, tarih, kullanılan cihaz gibi bilgilerinin analizinde kullanılan *exif* araçları eskisi kadar yaygın olmayan bir yöntemdir. Çünkü sosyal ağlar üzerinden yüklenilen görsellerin *exif* bilgileri sosyal ağlar tarafından görsel yüklendiği zaman silinmektedir. Fakat bazı araçlar ile bu bilgilere ulaşılabilmektedir. Sosyal medya yönetim aracı olan Hootsuite, bu araç vasıtasıyla yapılan görsel yüklemelerinde görsellerin orijinallerini OW.LY domaininde saklamaktadır. Bu şekilde görselin *exif* bilgilerine erişim sağlanabilir ve *exif* analizinden birçok veri elde edilebilmektedir.[208]



Şekil 19: *Exif Analizi*

Kaynak: ÖNAL, Emre, a.g.e.

Analizden sonra fotoğrafın hangi ekipmanla hangi tarihte çekildiği ve çekildiği yerin GPS koordinat bilgileri gibi verilere ulaşılabilmektedir. Koordinat bilgilerinin basitçe GPS'e girilmesi ile de haritada lokasyona erişilebilir.

[208] Emre Önal, **SOCMINT Kullanımı ve Örnekler**, 2019, (Çevrimiçi) https://www.blog.emreonal.com.tr/socmint-kullanimi-ve-ornekler/ (Erişim tarihi: 24 Nisan 2021).

3.3.1.5. Bilginin Teyit Edilmesi

İstihbarat sürecinde veri toplama yöntemlerinin tamamı için kritik önem taşıyan faktörlerden bir tanesi de bilginin doğruluğudur. Özellikle sosyal medyanın yanlış yönlendirmeler, hatalı bilgiler, kasıtlı çarpıtmalar, algı ve bilgi kirliliği gibi karakteristik özelliklerinden kaynaklı metodolojik engeller bulunmaktadır. Bu nedenle SOCMINT'ten elde edilen verileri analiz edecek personel için verilerin doğrulanması son derece önemlidir. Bu doğrulama işlemine "caydırıcı etki" gibi engel teşkil edebilecek bazı durumlar söz konusu olabilir. Kullanıcıların oto-sansüre karşı gösterebileceği tepkiler çalışmanın "Gözetim Toplumu" başlığında ele alınmıştır. Bu tarz durumlarda gözlemlendiğini anlayan kullanıcılar verilerinin toplanıp analiz edilmesine tepki gösterebilir, protesto edebilir veya paylaşımları daha kısıtlı ve dikkatli bir şekilde yapabilir. Bu durum sosyal medya üzerinden elde edilecek verilerin oranına direkt olarak etki edecek ve SOCMINT'in işlevine zarar verecek potansiyeli sahiptir.[209] Sonuç olarak insanlar sosyal medyaya ne kadar bağlı kalırsa, istihbarat servislerinin faydalanabileceği veri miktarı da o kadar fazla olacaktır.

Kriz durumlarında sosyal medya üzerinden algı amaçlı yanlış bilgiler yayılabilmektedir. Bunlar kasıtlı olarak yapılabileceği gibi paylaşılan habere bilinçsizce katılım gösterenlerin desteğiyle kar topu etkisi gösterebilmektedir. 2011 yılı Londra protestolarında sosyal medya üzerinden paylaşılan asılsız bilgileri derleyerek analiz eden The Guardian gazetesinin paylaşmış olduğu raporda; isyancılar hayvanat bahçelerine saldırarak hayvanları serbest bıraktı, isyancılar McDonald's'ta kendilerine yemek yapıyorlar, polis 16 yaşındaki bir kız çocuğunu darp etti, London Eye ateşe verildi, isyancılar Birmingham'daki çocuk hastanesine saldırdı, Londra'da askerler sokağa indi ve Miss Selfridge mağazası kundaklandı gibi asılsız haberlerin paylaşıldığı ve milyonlarca etkileşim aldığı görülmüştür.[210] Bu yüzden gerekli müdahaleler yapılmadan önce SOCMINT yönteminden elde edilen verilerin mutlaka doğrulanması gerekmektedir. En eski fakat en güvenilir yöntem olan HUMINT (insani istihbarat) yöntemi bu doğrulama işlemi için etkin bir biçimde kullanılabilir.

---

[209] LSE, **Policy Engagement Network**, Interception Modernisation Programme, 2009, s. 56-57.

[210] The Guardian, **How Riot Rumours Spread on Twitter**, 2011, (Çevrimiçi) https://www.theguardian.com/uk/interactive/2011/dec/07/london-riots-twitter (Erişim tarihi: 24 Nisan 2021).

Bu durum tam tersi şekilde gerçekleşerek HUMINT'in tamamlayıcısı olarak SOCMINT yöntemi de kullanılabilir. Bir dönem internette yayıncılık yapan kişileri yetkililere sahte ihbarlarda bulunarak silahlı timlerin gönderilmesi üzerine ortaya çıkan SWATTING terimi birçok insanın mağdur olmasına sebebiyet vermiştir. İhbar geldiği anda canlı yayında olan birçok yayıncı izleyicileri önünde tutuklanmıştır.[211] Özellikle SWATTING gibi olası sahte ihbarların önüne SOCMINT faaliyeti ile geçilebilir.

3.3.1.6. Dağıtım

Dağıtım istihbarat sürecinin son aşamasıdır. Toplanan verilerin işlemlerden geçirilerek karar vericilerin ihtiyaç duyduğu bilgi hâline getirilip sunulmasını öngörmektedir. İstihbaratın yayımı ve dağıtımındaki en önemli faktör, bilgiyi etkili bir şekilde iletmektir. Bu brifing metin şeklinde yazılı veya görsel şekilde sunum olarak yapılabileceği gibi sözlü olarak da yapılabilmektedir. Kompleks durumlarda bilginin anlaşılabilirliği kişiden kişiye değişebileceği için raporlar dikkatli ve özenli bir şekilde hazırlanmalıdır.

3.3.2. Sosyal Medya İstihbaratında Yasallık

İstihbarat süreci hakkında bilinen en büyük yanlışlardan birisi personellerin hukuk dışı faaliyetlerde bulunabileceğidir. Hollywood etkisinden kaynaklanan bu algının aksine istihbarat personeli her devlet çalışanı gibi kanunlar tarafından denetlenen bir memurdur. Bu bağlamda Türkiye Cumhuriyeti'nin istihbarat servisi Millî İstihbarat Teşkilatının kamu idarelerinin bağlı olduğu denetim mekanizmaları 2937 numaralı Kanun'da belirtilmiştir. [212] Bu bağlamda SOCMINT yöntemi her ne kadar açık kaynaklardan yararlanıyor olsa da vatandaşların mahremiyetine ve veri gizliliği politikalarına uygun şekilde yürütülmesi gerekmektedir. Bu bağlamda AİHM (Avrupa İnsan Hakları Mahkemesi), 1981 yılında yapılan Avrupa Konseyi Kongresi'nde kişisel verileri "kimliği belirli veya belirlenebilir kişiler ile ilgili bilgi" olarak tanımlamış ve özel hayatın gizliliği ile ilgili 8. Madde'de "1. Herkesin özel hayatına, aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkı vardır, 2. Bu yasal hak

---

[211] Rob Kalaijan, 5 Streamers Who Were SWATTED During a Live Stream, **Sportskeeda**, 2021, (Çevrimiçi) https://www.sportskeeda.com/esports/5-streamers-swatted-live-stream#:~:text=Swatting%20is%20when%20a%20person,get%20caught%20live%20on%20stream (Erişim tarihi: 24 Nisan 2021).

[212] T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi, Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu, 2937 sayılı Kanun, (Çevrimiçi) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf (Erişim tarihi: 24 Nisan 2021), (Erişim tarihi: 24 Nisan 2021).

doğrultusunda, ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzensizliğin ve suçun önlenmesi, sağlığın, ahlakın veya başkalarının haklarının korunması dışında bu hakkın kullanımına hiçbir kamu müdahalesi olmayacaktır." ifadeleriyle güvence altına alınmıştır.[213]

Bu madde ile kişisel verilerin "keyfî müdahalelere" karşı güvence altına alınmasıyla birlikte spesifik ihtiyaçlar doğrultusunda kullanılabileceği de belirtilmiştir. Bu da geleneksel güvenlik modelinde olduğu gibi meşru şiddet tekelinin devletler tarafından kullanılabilir olduğunu göstermektedir. Kişisel Verilerin Korunması Kanunu'nda ise kişisel veriler için benzer bir tanım yapılmaktadır; "Kimliği belirli veya belirlenebilir nitelikteki gerçek kişiye ilişkin her türlü bilgidir." Burada gerçek kişi ibaresi ile tüzel kişilerin verilerinin kanun kapsamı dışında kaldığı görülmektedir. Ayrıca "her türlü bilgi" ifadesinin çok geniş bir kapsamı bulunmakta ve hangi bilgilerin kişisel veri olarak kabul edileceğine ilişkin bir esas belirtilmemektedir. Bu sebeple önemli olan verinin herhangi bir gerçek kişi ile ilişkilendiriliyor veya o gerçek kişiyi tanımlayabilir olmasıdır.[214]

Bu bağlamda kişilerin verilerinin işlenmesine onay verdiği "açık rıza" kavramına da değinilmelidir. Açık rıza kavramının geçerliliği için veri sorumluları tarafından detaylandırılması ve belirli bir duruma özgülenmiş olması gerekmektedir. Yani, "Sizlere daha kaliteli hizmet sunabilmek için verilerinizin işlenmesine onay veriyor musunuz?" şeklinde alınacak beyan kanunen geçerli olmayacaktır.[215] Buna bir örnek olarak *Facebook* şirketinin kullanıcılarından aldığı yasal izinler şu şekilde ifade edilmiştir;

> "*Fikrî mülkiyet hakları kapsamındaki içerikleri Ürünlerimizde veya Ürünlerimizle bağlantılı şekilde paylaştığınızda, yayınladığınızda veya yüklediğinizde; içeriklerinizi barındırmamız, kullanmamız, dağıtmamız, değiştirmemiz, çalıştırmamız, kopyalamamız, herkese açık olarak sunmamız veya göstermemiz, çevirisini yapmamız ve*

[213] Europen Court of Human Rights, Internet: Case-law of the European Court of Human Rights, Data-Protection and Retention Issues Relevant for the Internet, 2015, (Çevrimiçi) https://www.echr.coe.int/documents/research_report_internet_eng.pdf (Erişim tarihi: 25 Nisan 2021), s. 7/62.

[214] KVKK, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, 2018, s. 21.

[215] KVKK, **a.g.e.,** s. 23.

türevlerini oluşturmamız için bize münhasır olmayan, devredilebilir, alt lisanslanabilir, telifsiz ve uluslararası bir lisans vermiş olursunuz. Bu bağlamda örneğin Facebook'ta bir fotoğraf paylaştığınızda, bu fotoğrafı saklamamıza, kopyalamamıza ve hizmetimizi veya kullandığınız diğer Facebook Ürünlerini destekleyen hizmet sağlayıcıları gibi başkalarıyla paylaşmamıza (yine ayarlarınız doğrultusunda) izin vermiş olursunuz. Bu lisans, içerikleriniz sistemlerimizden silindiğinde sona erer."[216]

Bir başka sorunsal ise kullanıcıların profillerini herkese açık hâle getirmesinin tek başına verilerin işlenmesine açık rıza gösterip göstermemesidir. Bu çerçevede yine KVKK'nın 5. Madde'sinin d. bendinde "ilgili kişinin kendisi tarafından alenileştirilmiş olması" açık rıza aranmadan kişisel verilerin işlenmesini mümkün kılacağı belirtilmiştir.[217] Yani, ilgili kişinin paylaşmış olduğu verileri alenileştirmesi, bu verileri ne amaçlı paylaştığını belirtmesiyle gerçekleşmektedir. Örneğin; kişinin ikinci el eşya satışı yapmak için bir sosyal ağ sitesinde kişisel telefon numarasını paylaşmasındaki amaç potansiyel alıcıların kendisi ile iletişime geçmek için kullanmasıdır. Telefon numarası bir başkası tarafından bu amaçla kullanılırsa yasal, fakat alınan bu verinin başka amaçlarla kullanılması yasal olmayacaktır.[218]

Genel anlamda siber uzay, özelinde ise sosyal medya kompleks yapılara sahip olduğu için bu alanların hukuki zeminini oturtmak oldukça zordur. Gerçek hayatta bir kişinin yaşını öğrenip bunu başkalarıyla paylaşmak suç teşkil etmezken siber uzayda bu durum veri hırsızlığı olarak nitelendirilebilir. Bu bağlamda insan haklarına uygun bir şekilde, kamuoyu güvenine ve toplumsal düzene zarar vermeden SOCMINT yönteminin hukuki zemininin oluşturulması gerekmektedir. Hangi durumlarda bu yönteme başvurulacağı, ne gibi verilere nasıl erişim sağlanabileceği gibi yasal yetkilerin hukuken belirlenmesi gerekmektedir. SOCMINT'in kullanılabilecek bir yöntem olmasıyla beraber maruz

---

[216] FACEBOOK, **Hizmet Koşulları**, (Çevrimiçi) https://www.facebook.com/legal/terms/update (Erişim tarihi: 25 Nisan 2021).

[217] KVKK, **a.g.e.,** s. 24

[218] KVKK, "Alenileştirme" Hakkında Kamuoyu Duyurusu, 2020, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU (Erişim tarihi: 25 Nisan 2020).

kalınacak bir yöntem olması da göz önünde bulundurulur ve bilişim hukuku bağlamında henüz nitelikli bir zemin oluşturulamadığı hesaba katılırsa, siber güvenlik konusunda en zayıf halka olan kullanıcıların ve şirketlerin veri mahremiyeti konusunda bilgilendirilmesi gerekmektedir.

3.3.3. Sosyal Medya İstihbaratının Faydaları

Kabaca emekleme aşamasında olan sosyal medya istihbaratının, dünya genelinde ciddi oranda artış gösteren kullanımı ve bu ortamdan elde edebilecek verilerin önemli derecede fazla olması sebebiyle bazı faydaları bulunmaktadır. Önleyici bir faaliyet olan istihbarat sürecine, suç ile ilgili verileri eylemin gerçekleşmesinden önce sağlama potansiyeli olan SOCMINT'in operasyonel faydalarının yanı sıra düzenli olarak analiz yapmaya elverişli veriler sayesinde mevcut durum hakkında çıkarımlar yapmaya ve geleceğe dair öngörülerde bulunmaya imkân sağlamaktadır. Çalışmanın önceki bölümlerinde basitçe değinilen faydalar bu bölümde üç başlık altında incelenecektir. Bunlar gerçek-zamanlı durumsal farkındalık, gruplara katılım ve suçun önlenmesi ve kovuşturulması için motivasyonun belirlenmesidir.[219]

3.3.3.1. Gerçek-Zamanlı Durumsal Farkındalık

Durumsal farkındalık kavramı ilk olarak Alman havacı Oswalde Boelke tarafından düşmandan önce mevcut durumun farkına vararak üstünlük kazanmak amacı ile kullanılmıştır. [220] Çevresel faktörler ve olayların zaman-mekân ilişkisine göre algılanmasıyla hem mevcut durumu tanımlama hem de gelecek hakkında öngörüde bulunma imkânı tanımaktadır. Yeni medyada haberlerin yayılmasının ve oluşturduğu etkinin geleneksel medyaya göre daha fazla olması sebebiyle sorunun tespit edilmesi, veri akışının çok daha hızlı olduğu sosyal medya üzerinden etkin bir biçimde yapılabilmektedir.

Örneğin; coğrafi konum tekniğiyle paylaşım yapanların yerinin tespit edilmesi, belirli bir konumda olası şiddetle ilgili paylaşımların artması ile bölgeye daha hızlı ve daha etkili bir durum müdahalesi yapma imkânı tanımaktadır.[221] Yapılan bir çalışmada, sosyal medya paylaşımlarının bir sistem aracılığıyla sorulara tabi tutularak durumsal farkındalık oluşturmanın mümkün olup olmayacağı test edilmiştir. Örneklem olarak

---

[219] Omand, vd., **a.g.e.,** s. 805-806

[220] Faruk Dinç, **Durumsal Farkındalık**, Anka Enstitüsü, 2018, (Çevrimiçi) http://ankaenstitusu.com/durumsal-farkindalik/ (Erişim tarihi: 25 Nisan 2021).

[221] Omand, vd., **a.g.e.,** s. 806.

Boston maratonun bombalanmasında yaklaşık yarım milyon kadar *tweet* kullanılmış ve sistem elde etmiş olduğu bu *tweet*lere, "Henüz patlamamış başka bombaların nerede olduğu bildiriliyor? Bu mesajlar ne zaman yayıldı? Bu mesajlar ne sıklıkla yayıldı?" gibi sorular sorulmuştur. Sonuç olarak ise, sistem *tweet*lere sormuş olduğu bu sorular ile ana akım medyanın haberi yayınlamasından 11 dakika önce sonuca ulaşmış ve geleneksel medyada bahsedilmeyen St. Ignatius Kilisesi ve Mandarin Oriental Hotel'i gibi insanların olaydan sonra toplandığı lokasyonları da tespit etmiştir.[222]

3.3.3.2. Gruplara Katılım

Pek çok farklı amaç için kullanılsa da sosyal medya temel olarak kitleleri bir araya getiren iletişim aracıdır. Birbirini tanıyan veya tanımayan milyonlarca insanın fikirlerini paylaştığı bu ortam, benzer ilgi alanları veya hobileri olan kitlelerin gruplar oluşturmasına olanak tanımaktadır. Sosyal medyada yüz yüze iletişimden farklı olarak kullanıcılar profilleri -ki bu anonim olabilir- veya takma isimleriyle iletişim kurabilmelerinden ötürü bu alanda daha cüretkâr olabilmektedirler. Fakat sosyal medyada oluşturulan bu grupların hepsi futbol takımları, arabalar veya popüler kültür ile alakalı içerikler paylaşmamaktadır. Çalışmanın Terör Örgütleri ve Uyuşturucu Kartellerinin Sosyal Medya Kullanımı başlıklı bölümünde birçok organize suç örgütünün, kartellerin ve terör örgütlerinin hem propaganda yapmak hem de yeni üyeler kazanmak gibi amaçlarla sosyal medya platformları kullandığı belirtilmiştir.

Bu gibi durumlar emniyet veya istihbarat personelleri için gruplara katılım sağlayarak gözlem yapabilme ve hedef oluşumlar hakkında bilgi edinme imkânı sunmaktadır. Belirli grupların faaliyetlerini veya davranışlarını daha iyi anlayabilmek için gerekli yasal izinler alındıktan sonra bu grupların içine girerek ne gibi motivasyonlarının olduğunu, olaylara ne gibi tepkiler verdiklerini, söylem ve argümanlarının neler olduğunu ve hatta daha spesifik bir şekilde olası eylem ve gösteri planlarına ilişkin bilgilere SOCMINT yöntemiyle ulaşabilmektedir.[223]

3.3.3.3. Suçun Önlenmesi ve Kovuşturulması İçin Motivasyonun Belirlenmesi

Suçun önlenmesi ile ilgili birçok çalışma ve sınıflandırma yapılmıştır. Paul J. Brantingham ve Frederic L. Faust'un yapmış olduğu sınıflandırma üç aşamadan

---

[222] Brian Ulıcny, Jakub Moskal & Mieczyslaw M. Kokar, Situational Awareness from Social Media, STIDS, 2013, (Çevrimiçi) https://vistology.com/wp-content/uploads/2016/02/STIDS2013_T12_UlicnyEtAl.pdf (Erişim tarihi: 25 Nisan 2021), s. 87-93.

[223] Omand, vd., **a.g.e.,** s. 806.

oluşmaktadır. İlk aşamada suç işleme potansiyeli bulunan kişilere müdahale etmek gibi bir durum yoktur. Bu önleyici faaliyette suça zemin hazırlayan koşullar hedef alınmaktadır. İkinci aşama ise suç işleme eğilimi olan kişi veya kişilere erken müdahale öngörülmektedir. Son aşama ise sabıkalı kişilerin tekrar suç işleme ihtimallerini önlemektir. Yani suçun tekrarını önleme amacı bulunmaktadır.[224]

Kişileri suç işlemeye yönelten fiziksel ve sosyal koşulların sosyal medya üzerinden analiz edilmesi yüksek teknik kabiliyet ve teknolojik imkân isteyen bir süreç olacaktır. İnsanların suçu neden işlediğini anlayabilmek için çok detaylı analizlerin yapılması gerekmektedir. SOCMINT yönteminin buna uygun kabiliyetinin olmasıyla birlikte sürekli olarak izleme yapan yapay zekâ ihtiyacı bulunmaktadır.

Suç işleme eğilimi olan kişiler ve sabıkalıların sosyal medya verilerinden veya gruplara katılımda olduğu gibi bulunduğu gruplardaki söylemlerinden ve etkileşimde bulunduğu kullanıcılardan motivasyonu anlaşılabilir.

Örneğin; Meksikalı Jose Rodrigo Arechiga Gamboa, uyuşturucu kaçakçılığı yapan Sinaloa Karteli'nin üyesidir. Gamboa, "El Chino Antrax" kullanıcı ismiyle *Twitter* sayfasında lüks yaşamı ve silahlı paylaşımları ile sosyal medyada kısa sürede ünlenmiştir. Paylaşımları sebebiyle kolluk kuvvetlerinin dikkatini üzerine çeken Gamboa'nın izini süren polisler sosyal medya hesapları üzerinden elde ettikleri ipuçları ile uyuşturucu kaçakçısını Hollanda'ya sahte kimlik ile giriş yapmaya çalışırken yakalamıştır. Kartelin başkan yardımcısı olan babası Serafin Zambada Ortiz ise sadece lüks yaşamını paylaşmakla kalmayarak iş yaptıkları ortaklarını da paylaştığı her fotoğrafa etiketlemiştir. Oğlu gibi babası da yaptığı paylaşımlardan bir ay sonra kolluk kuvvetleri tarafından yakalanmıştır.[225] Yakalanan kartel üyelerinin beraber fotoğraf paylaştıkları kişiler veya etkileşimde bulundukları kullanıcılar bu bağlamda Kartel hakkında daha detaylı verilere ulaşılmasına olanak sağlayacaktır.

---

[224] Paul J. Brantingham and Frederic L. Faust, "A Conseptual Model of Crime Prevention", **Crime & Delinquency**, 1976, Vol. 22, No. 3, s. 290.

[225] Jordyn Taylor, "Mexican Cartel Members Post Drug Photos on Social Media, Get Arrested", **Observer**, 2014, (Çevrimiçi) https://observer.com/2014/01/mexican-cartel-members-post-drug-photos-on-social-media-get-arrested/ (Erişim tarihi: 25 Nisan 2021).

SONUÇ

Uluslararası ilişkilerin baş aktörleri olan devletler için pek çok farklı değişken varlığını sürdürebilmesi için önem taşımaktadır. Güvenlik ise bunların en başında gelmektedir. Bunu sağlayabilmek için devletler, hâkim oldukları alan içerisinde mutlak kontrol ve gözetim içgüdüsüyle hareket ederler. Bununla da yetinmekle kalmayarak çevresindeki gelişmelerden ve değişimlerden de haberdar olma motivasyonları bulunmaktadır. Fakat siber uzayın yapısına bakıldığında geleneksel dünya sisteminden çok daha farklı bir yapı karşımıza çıkmaktadır. Gerçek dünyadan çok daha kompleks ve kaotik olan bu yapı, devletlerin hareket kabiliyetini kısıtlamakla birlikte onların *reel* dünyada karşılaştığı tehditleri dönüştürerek tam olarak hâkim olamadıkları bu alanda yeni bir meydan okuma olarak karşılarına çıkarmaktadır.

Bu çerçevede devletlerin karşısına çıkan bu meydan okumalardan en önemlisi internet ve sosyal medyadır. *Reel* dünyada 5 kişilik bir ayrılıkçı grubun iktidara verebileceği zarar çok kısıtlıyken, siber uzayın tanımış olduğu imkânlar doğrultusunda 5 kişilik bir *hacker* grubu devletin işlevini aksatabilecek düzeyde zarar verebilmektedir. 11 Eylül saldırılarının sonucu olarak değişen dünya düzeni ve uluslararası ilişkiler alanına kazandırdığı yeni kavramlar, dijitalleşme ve siber devrimler ile siber uzayda gelenekselden farklı şekillerde tezahür etmektedir.

Önleyici bir faaliyet olan istihbarat, her teknolojik gelişme gibi internet ve sosyal medyanın imkânlarından da yararlanmaktadır. Özellikle sosyal medyanın sunmuş olduğu büyük veri grupları istihbarat verisi niteliğinde olmasa dahi ipucu niteliği taşıyabilmektedir. Bu bağlamda hazırlanan tez çalışmasının sonucu olarak sosyal medya üzerinden elde edilen verilerin belirli aşamalardan geçirilip diğer istihbarat disiplinleriyle teyit edilmesiyle istihbarat sürecinde kullanılabileceği tespit edilmiştir. Fakat henüz çok yeni bir yöntem çeşidi olan SOCMINT'in sunmuş olduğu bu imkânlara karşılık bazı dezavantajları bulunmaktadır. İlk olarak belirtilmesi gereken nokta SOCMINT'in "tek başına" bir istihbarat yöntemi olarak kullanılmasının uygun olmayacağıdır. Sosyal medyanın muazzam bir veri potansiyeli olmasına karşılık, buradan elde edilecek verilerin güvenirliliği diğer istihbarat disiplinlerine göre çok daha

şüphelidir. Bu yüzden elde edilen verilerin mutlaka diğer veri toplama yöntemlerinden yararlanılarak teyit edilmesi gerekmektedir.

Dünya nüfusunun %53,6'sına tekabül eden 4,20 milyar kullanıcının sürekli olarak veri girişi yapıyor olmasının sosyal medya platformları üzerinden uygulanacak SOCMINT faaliyetlerine olumsuz etkisi olacaktır. Bu durum sosyal medyanın yapısında çok fazla veri bulundurması ve verilerin analiz edilmesinde geleneksel yöntemlerden faydalanılmasına engel olmaktadır. Büyük veri kümeleri arasından ihtiyaç duyulan spesifik verilerin ayıklanması ve sınıflandırılması makine öğrenmesi ve yapay zekâ algoritmalarına ihtiyaç duyulduğunu göstermektedir. Aynı zamanda sosyal medyada kullanılan jargonun ve kısaltmaların gerek makine öğrenmesi ve yapay zekâ algoritmalarına tanımlanması gerek ise istihbarat analizcileri tarafından doğru algılanabilmesi için bu alanda çalışacak personellerin sosyal medya ve internet jargonuna hâkim kişilerden oluşması gerekmektedir. Sonuç olarak veri toplama, sınıflandırma ve analiz etme aşamalarında algoritmalardan yararlanılacak olsa da nihai kararı verecek olan insan aklıdır. Bu bağlamda SOCMINT yönteminin uygun bir şekilde kullanımı için teknik imkânlar ve nitelikle personellere ihtiyaç duyulmaktadır.

Hali hazırda yapay zekâ ve makine öğrenmesi gibi çalışmaları yürüten özel yazılım şirketleri, SOCMINT yöntemi açısından yetkinliği tam anlamda kazanamamış istihbarat servisleri için faydalanılabilecek birer destekleyici unsur potansiyeli taşımaktadır. Bunun yanı sıra sosyal medya üzerinden planlı ve organize bir şekilde kolektif bir bilincin oluşturulabileceği tespit edilmiştir. Söylemlerin kitlelere hızlı bir şekilde aktarılmasını sağlama imkânından ötürü yeni toplumsal hareketlerin argümanlarını sosyal medya üzerinden yürütmesi, sosyal medyanın etkileşim üzerine kurulu yapısında kar topu etkisi oluşturarak kısa sürede geleneksel yöntemlerin ulaşamayacağı sayıdaki kitlere ulaşmasına olanak sağlamaktadır. Kasıtlı veya kasıtsız olarak paylaşımlar üzerinde oynamalar yapılmasının argümanların kitleler üzerindeki tesirinin daha etkili bir biçimde yayılmasına neden olmaktadır. Örneklem olarak incelenen Arap Baharı hareketlerinde, sosyal medyanın bir iletişim aracı olarak kullanıldığı ve kolektif bilincin buradaki *blog* yazıları ve paylaşımlar ile oluşturulabildiği görülmüştür.

İnternetin özgürlükçü mottolarından kaynaklı olarak devletlerin buradaki gözlem faaliyetlerinin olabildiğince hassas ve yasalara uygun şekilde yapılması gerekmektedir. Panoptikon gözetim metaforunda olduğu gibi gözetleyenin görünmezliği ilkesi SOCMINT faaliyetinde elde edilebilecek veri miktarına doğrudan etki edecektir.

Toplumun sosyal medya üzerinden gözlemlendiği ve buradaki yaptıkları paylaşımlar sebebiyle cezai yaptırımlara maruz kalabileceği düşüncesi insanların şahsi olarak oto-sansür uygulamalarına sebebiyet verebilir. Bu durumda direkt olarak istihbarat birimlerinin sosyal medyada toplayabileceği potansiyeli verilerin azalmasına neden olacaktır.

Çalışmanın saptamış olduğu olgulardan bir tanesi de siber güvenlik konusunda kullanıcıların ve özel şirket personellerinin yeterince bilinçli olmadığıdır. Sanal dünyanın artık gerçek bir dünya şekilde algılanması gerektiği bilinci topluma aktartılmalıdır. Nasıl ki bir insan doğduğu gibi bir ülkenin vatandaşı oluyorsa, kullanıcılar da internete bağlandığı an aslında dijital bir vatandaşlık almaktadır. Bu bağlamda *reel* dünyada küçük yaşta sosyal bilgiler ve vatandaşlık gibi dersler ile bireylerin topluma ve kanunlara sorumlulukları öğretiliyor ise yine küçük yaşta siber dünyanın gerekliliklerinin öğretilmesi gerekmektedir. İnternet kullanımının 6 ila 7 yaşlarına kadar düştüğünü göz önünde bulunduracak olursak, ilkokullarda internet ve sosyal medya kullanımına dair eğitimler verilmesi kritik önem taşımaktadır. Veri güvenliği, internetteki tehditler ve siber zorbalık gibi bilinçlendirici faaliyetler gelecek nesillerin interneti ve sosyal medyayı daha kontrollü ve güvenli bir biçimde kullanmasına olanak sağlayacaktır. Keza aynı durum şirket çalışanları için de geçerli olmaktadır. Şirketlerde personellerin ve yönetim ekiplerinin bilinçlenmesi için siber güvenlik eğitimleri verilmesi, ilerleyen süreçte yaşanabilecek siber saldırılara karşı daha bilinçli ve soğukkanlı müdahalelerde bulunulmasına yarayacaktır. Bunlara ek olarak bilişim hukuku açısından da birçok ülkenin henüz uygun zemini oluşturamadığı görülmüştür. Bu bağlamda hem veri güvenliği açısından siber saldırılara karşı cezai yaptırımların netleştirilmesi hem de SOCMINT yönteminin uygulanabilmesi için yasal zemininin oluşturulup amaç ve kapsamlarının belirlenmesi gerekmektedir.

Bunların yanı sıra SOCMINT faaliyetlerinin istihbarat birimleri açısından birçok faydası olabileceği tespit edilmiştir. Sosyal medya verilerinin sistematik bir biçimde takip edilmesi durumsal farkındalık oluşturulmasında etkili olacaktır. Böylelikle hem istihbaratın önleyici faaliyet niteliği uygulanabilir hem de geleceğe dair öngörülerde bulunulabilir. Ayrıca deprem, sel veya hortum gibi doğal afetlerde müdahalelerin hızlı bir şekilde doğru noktalara yapılmasına imkân sağlayabilir. Gruplara katılım eylemi ile güvenlik birimleri sosyal medya üzerinden hedef oluşumlar hakkında bilgi edinme imkânı bulmaktadır. Bu durum gelecek dönemde planlanan bir eylem hakkında bilgi

verebileceği gibi gözlemlenen yapının argümanları ve söylemleri hakkında veriler de sunmaktadır. SOCMINT yöntemi ile suç potansiyeli olan kişiler ve etkileşimde olduğu kullanıcılar gözleme tabi tutularak suç motivasyonu anlaşılabilir ve gerekli durumlarda önleyici müdahalelerde bulunulabilir. Örneklem olarak incelenen Meksika karteline bağlı bir uyuşturucu kaçakçısının sosyal medya üzerinden paylaştığı içeriklerden yapmış oldukları faaliyet ve iş ortakları tespit edilmiş olup, sistematik inceleme sonrasında edilen veriler ışığında havalimanında sahte kimlikle çıkış yapmaya çalışırken tutuklanması gerçekleştirilmiştir.

Aynı zamanda makine öğrenmesi ve *sentiment analysis* algoritmalarıyla sosyal medya üzerinden duygu analizleri yapılabilmekte ve kullanıcıların spesifik olaylar karşısındaki tepkileri ölçülebilmektedir. Bu uygulama potansiyel yağmalama veya protesto gibi eylemlerin önceden tespit edilebilmesine olanak sağlamaktadır.

Sonuç olarak SOCMINT uygulamasının istihbarat sürecinde kullanılabilecek etkin bilgilere ulaşabileceği tespit edilmiştir. Fakat "etkin" bir biçimde kullanılabilmesi için uygun bir hukuki zemine, yapay zekâ ve makine öğrenmesi gibi teknik imkânlara, nitelikli personellere ve bunlarından hepsinden daha önemlisi elde edilen bilgileri doğrulayabilecek HUMINT desteğine ihtiyacı bulunmaktadır. İstihbarat çalışmalarında unutulmaması gereken en önemli konulardan bir tanesi HUMINT'in önemidir. Teknik imkânlar ne kadar fazla olursa olsun bir istihbarat servisinin asıl gücünü insani istihbarat kabiliyeti göstermektedir. Neticede SOCMINT yöntemi gibi birçok istihbarat disiplini ihtiyaç duyulan verileri toplayabilir, fakat bu bilgileri teyit edebilecek veya kapalı kapılar ardındaki spesifik bilgileri aktarabilecek olan HUMINT'tir.

KAYNAKÇA

AKYEŞİLMEN, Nezir. **Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik**. Ankara: Orion Kitabevi. 2018.

ALMOND, Gabriel A. "Comparative Political Systems". **The Journal of Politics**. 1956. Vol.18. No.3. pp. 391-409.

ALMOND, Gabriel A. Sidney Verba. **The Civic Culture: Political Attitudes and Democracy in Five Nations**. New Jersey: Princeton University Press. 1963.

ARCHER, Christon I., ve FERRIS, John R., ve HERWIG, Holger H., ve TRAVERS, Timothy H.E. **Dünya Savaş Tarihi**. (C. Demirkan, Çev.). İstanbul: Tümzamanlar Yayıncılık. 2006

ARKLAN, Ümit. "Sosyal Medyanın Siyasal Amaçlı Kullanımı: Ağ Kuşağının Kullanım Alışkanlıkları Üzerine Bir Araştırma". **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**. 2016. Y.2, S.4. pp. 618-657.

AKTAN, C. Can ve DİLEYİCİ Dilek. "Siyasal Karar Alma Sürecinde Çıkar Grupları". Modern Politik İktisat: Kamu Tercihi içinde. Ankara: Seçkin Yayınları. 2007.

BAYLIS, John. "Uluslararası İlişkilerde Güvenlik Kavramı". **Uluslararası İlişkiler**. 2008. Y.5, S. 18. pp. 69-85.

BAYRAKTAR, Gökhan. "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat". **Güvenlik Stratejileri**. 2014. Y.10, S.20

BOSTANCI, Mustafa. **Sosyal Medya ve Siyaset**. Konya: Palet Yayınları. 2015

BOZARTH, Jane. **Social Media for Trainers – Techniques for Enhancing and Extending Learning**. San Francisco CA: Pfeiffer. 2010.

BRANTINGHAM, Paul J., & FAUST, Frederic L. A. "Conseptual Model of Crime Prevention". **Crime & Delinquency**. 1976. Vol.22, No.3. pp. 284-296.

CAERS, Ralf & FEYTER, Tim & COUCK, Marijke & STOUGH, Talia & VIGNA, Claudia & DU BOIS, Cind. "Facebook: A Literature Review". **New Media & Society**. 2013. Vol.15, No.6. pp. 982-1002.

CAMBRIA, Erik & HAVASI, Catherine & HUSSAIN, Amir. "SenticNet 2: A Semantic and Affective Resource for Opinion Mining and Sentiment Analysis". **Twenty-Fifth International Florida Artificial Intelligence Research Society Conference**. Association for the Advancement of Artificial Intelligence. 2012.

Central Intelligence Agency Collection. **The Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University.**

CLAUSEWITZ, Carl Von. **Savaş Üzerine.** Eriş Yayınları. 2003

ÇAKIR, Hamza ve TOPÇU, Hakan. "Bir İletişim Dili Olarak İnternet". **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**. 2005. Y. 1. S. 19. ss. 71-96.

COŞKUN, Uygar. "Dünden Bugüne Anayasacılık". **Hukuk Gündemi Dergisi**. 2008. S. 9.

DAVIES, Philip H. J. "Ideas of Intelligence: Divergent National Concepts and Institutions". **Harvard International Review.** (October 1 2002). Vol. 24. No. 3. pp. 62-66.

DEDEOĞLU, Beril. **Uluslararası Güvenlik ve Strateji**. İstanbul: Yeni Yüzyıl Yayınları. 2014.

FREEDMAN, Lawrence. **Strateji**. İstanbul: Alfa Basım Yayım Dağıtım. 2014.

FOUCAULT, Michel. **Hapishanenin Doğuşu**. Ankara: İmge Kitabevi. 1992.

GILL, Peter, PHYTHIAN, Mark & MARRIN, Stephen. **Intelligence Theory: Key Questions and Debates**. Studies in Intelligence Series. London: Routledge. 2008

GİRGİN, Kemal. **Modern İstihbarat ve Türkiye**. İstanbul: Okumuş Adam Yayıncılık. 2003.

GÖÇER, İsmet ve ÇINAR, Sertan. "Arap Baharı'nın Nedenleri, Uluslararası İlişkiler Boyutu ve Türkiye'nin Dış Ticaret ve Turizm Gelirlerine Etkileri". **KAÜ İİBF Dergisi**. 2015. Y. 6. S. 10. ss. 51-68.

GÖKSU, Erkan. **Kutadgu Bilig'e Göre Türk Savaş Sanatı**. İstanbul: Kronik Kitap. 2018.

HERMAN, Michael. **Intelligence Power in Peace and War.** Cambridge University Press. 1996.

HERMAN, Michael. **Strategic Intelligence: Understanding the Hidden Side of Goverment**. Wesport-London: Prager Security International. 2007.

HESS, Henner. **Mafia & Mafiosi Origin, Power and Myth**. Avustralya: Crawford House Publishing. 1998.

JOHNSON, Loch K. The Oxford Handbook of National Security Intelligence". The Dilemma of Open Source Intelligence. Is OSINT Really Intelligence içinde. New York: Oxford University Press. 2010.

JOMINI, Antoine Henri. **Savaş Sanatı-Prensipler/Ana Hatlar.** (A. Tunçer Büyükonat, Çev.). İstanbul: Doruk Yayımcılık. 2013.

JONES, Steve. **Encyclopedia of New Media: An Essential Reference to Communication and Technology.** Thousand Oaks, CA: SAGE Publications. 2003

JP 3-18. Joint Forcible Entry Operations CH 1. 2017.

KARAKAŞ, Ceyhun Kaan. "DAEŞ Propagandasında Yeni Medya Kullanımı". **Marmara İletişim Dergisi.** 2017. Y. 2. S. 28. ss. 33-46.

KAZAN, Hüseyin. "Terör-Medya İlişkisi ve Medyada Terör Haberciliği". **Güvenlik Stratejileri**. 2015. Y. 12. S. 24. ss. 109-146.

KELLY, Paul F. **Sosyal Mühendisin Maskesini Düşürmek**. İstanbul: Paloma Yayınevi. 2018.

KENT, Sherman. **Stratejik İstihbarat**. (B. Y. Özbek ve N. Ş. Arıca, Çev.). Ankara: Avrasya Stratejik Araştırmalar Merkezi Yayınları. 2003.

KENT, Sherman. **Strategic Intelligence for American Foreign Policy**. Princeton-New Jersey: Princeton University Press. 1949.

KIPP, Jacob, GRAU, Lester, PRINSLOW, Karl & SMITH, Captain. **The Human Terrain System: A CORDS for the 21st Century**. Military Review September-October. 2006.

KİRTİŞ, A. Kazım ve KARAHAN, Filiz. "To Be or Not To Be in Social Media Arena as the Most Cost-Efficient Marketing Strategy after the Global Recession". **Procedia Social and Behavioral Sciences.** 2011. Vol. 24. Pp. 260-268.

KÖKSAL, Yüksel ve ÖZDEMİR, Şuayip. "Bir İletişim Aracı Olarak Sosyal Medya'nın Tutundurma Karması İçerisindeki Yeri Üzerine Bir İnceleme". **Süleyman Demirel Üniversitesi İİBF Fakültesi Dergisi**, 2013. Y. 18, S. 1. Ss. 323-337.

LERNER, K. Lee ve LERNER, Brenda Wilmoth. **Encyclopedia of Espionage, Intelligence and Security Vol I**. Detroit: Thomson Gale. 2004.

LERNER, K. Lee ve LERNER, Brenda Wilmoth. **Encyclopedia of Espionage, Intelligence and Security Vol I**I. Detroit: Thomson Gale. 2004.

LERNER, K. Lee ve LERNER, Brenda Wilmoth. **Encyclopedia of Espionage, Intelligence and Security Vol III**. Detroit: Thomson Gale. 2004.

LIPPMANN, Walter. **U.S. Foreign Policy: Shield of the Republic**, Boston: Little, Brown and Company. 1943.

LOWENTHAL, Mark. "OSINT: The State of the Art, the Artless State". **Studies in Intelligence.** 2001. Vol. 45, No. 3

LOWENTHAL, Mark M. Intelligence: From Secrets to Policy. Washington, DC: Congressional Quarterly Press. 2002.

LSE. Policy Engagement Network. **Interception Modernisation Programme**. 2009.

MANOVICH, Lev. **New Media From Borges to HTML.** The MIT Press. 2003.

MARRIN, Stephen. Evaluating Intelligence Theories: Current State of Play. **Intelligence and National Security.** 2018.

MCLUHAN, Marshall ve POWERS, Bruce R. **Global Köy**. İstanbul: Scala Yayıncılık. 2020.

MERCADO, Stephen C. "Sailing the Sea of OSINT in the Information Age". **Studies in Intelligence**. 2004. V. 48. No. 3. pp. 45-55.

MORSELLI, Carlo. "Gangs and Social Networking". **Organized Crime Research Brief**. 2010. Vol. 13 No. 1, pp. 2.

NIX, Justin, SMITH, Michael, PETROCELLI, Matthew, ROJEK, Jeff, & MANJARREZ JR, Victor. "The Use of Social Media by Alleged Members of Mexican Cartels and Affiliated Drug Trafficking Organizations". **Journal of Homeland Security and Emergency Management**. 2016. Vol. 13. No. 3. pp. 395-418.

OKMEYDAN BİTİRİM, Selin. "Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon 've 'Omniptikon'a". **Online Academic Journal of Information Technology**. 2017. Y. 8. S. 30. ss. 45-69.

OMAND, Sir David, BARTLETT, Jamie, & MILLER, Carl. "Introducing Social Media Intelligence (SOCMINT)". **Intelligence and National Security**. 2012. Vol. 27. No. 6. pp. 801-823.

ÖZDAĞ, Ümit. **İstihbarat Teorisi.** Ankara: Kripto Kitaplar. 2014.

ÖZDEL, Gizem. "Foucault Bağlamında İktidarın Görünmezliği ve "Panoptikon" ile "İktidarın Gözü" Göstergeleri". **The Turkish Online Journal of Design, Art and Communication**. 2012. Y. 2. S. 1. ss. 22-29.

ÖZKAYA, A. Safa. **Hunlar'dan Günümüze Türk Askeri Kültürü.** İstanbul: Kronik Kitap. 2019.

PANDITA, Ramesh. "Information Pollution, a Mounting Threat: Internet a Major Casuality". **J. Of infosci. Theory and Practice**. 2014. Vol. 2. No. 4. pp. 49-60.

PATTON, Kerry. **Sociocultural Intelligence: A New Discipline in Intelligence Studies**. London: The Continuum International Publishing Group. 2010.

POTTER, Evan H. **Economic Intelligence and National Security**. Canada: Carleton University Press. 1998

PRENSKY, Marc. "Digital Natives, Digital Immigrants, On the Horizon". **MCB University Press**. 2001. Vol. 9. No. 5. Pp. 1-15.

PRUNCKUN, Hank. **Handbook of Scientific Methods of Inquiry for Intelligence Analysis**. Plymouth, UK: The Scarescrow Pres, Inc. 2010

RUBENSTEIN, Henry. "DC Power and Cooling Towers, Aktaran: Central Intelligence Agency". **Studies in Intelligence, Archival Record**. 1972. Vol. 16. No. 3.

SEREN, Merve, (2017), Stratejik İstihbarat ve Ulusal Güvenlik, Orion Kitabevi, Ankara

SEREN, Merve, ÇELİK, Tolga, ÖZGELDİ, Nedim ve DUMANKAYA, Elif M. **Sosyal Medya El Kitabı**. Ankara: Orion Kitabevi. 2018.

SHULSKY, Abraham N., & SCHMITT, Gary J. **Silent Warfare: Understanding the World of Intelligence** (3rd ed.). Washington DC: University of Nebraska Press. 2002.

SHELDON, Rose Mary. **Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages**. North Carolina: Mc Farland & Company, Inc Publishers. 2003.

SHELDON, Rose Mary. "Hannibal as a Spy Chief". **Leidschrift**. 2015. Vol. 30. No. 3. pp. 25-46.

ŞENER KOCABAY, Nihal. "Eğlencenin Gözetleme Hali ya da Eğlence Endüstrisinde "Görünen" ve "Gören" Olmak". **TRT Akademi**. Y. 1. S. 6. (Ocak 2016). ss. 50-70.

ŞUŞNEA, Elena, & IFTENE, Adrian. "The Significance of Monitoring Activities for the Social Media Intelligence (SOCMINT)". **MFOI**. Chisinau, Moldova. (July 2-6 2018). pp. 230-240.

TEKİN, Engin Cihad. "Kitap Tarihi Araştırmalarının Önemli Bir Alanı: Ansiklopedilerin Gelişimi ve Ansiklopedi Kültürü Araştırmalarının Önemi". **ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi**. 2020. Y. 11. S. 2. ss. 195-214.

TOMISLAV, Dokman, & TOMISLAV, Ivanjko. "Open Source Intelligence (OSINT): Issues and Trends". **INFuture2019: Knowledge in the Digital Age.** 2020. 23.

TZU, Sun. **Savaş Sanatı**. (P. Oktan ve G. Fidan, Çev.). İstanbul: Türkiye İş Bankası Yayınları. 2019.

WARD, Janabeth. "A Content Analysis of Celebrity Instagram Posts and Parasocial Interaction". **Elon Journal of Undergraduate Research in Communications**. 2016. Vol. 7. No. 1. pp. 1.

WILKINSON, Paul. "The Media and Terrorism: A Reassessment". **Terrorism and Political Violence**. 2007. Vol.9. No.2. pp. 51-64.

WILLIAMS, Heather J. ve BLUM, Ilana. **Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise**. Santa Monica California: RAND Corporation. 2018

WOLFERS, Arnold." National Security" as an Ambiguous Symbol". **Political Science Quarterly**. 1952. Vol. 67. No. 4. pp. 481-502.

YILDIRIM YENİMAN, Ebru. "Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması". **Mesleki Bilimler Dergisi (MBD)**. 2018. Y. 7. S. 2. ss. 24-33.

YÜCESOY, Tayfun. **Bireyden Kitleye Sosyal Medya Devrimleri ve Ötesine Kuramsal Yaklaşımlar**. İstanbul: Duvar Yayınları. 2020.

SAVAŞ, Serkan ve TOPALOĞLU, Nurettin. "Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri". **8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**. 2015.

WEB KAYNAKLARI

About.fb.com. **A Look at Facebook and US 2020 Elections.** (December, 2020). https://about.fb.com/wp-content/uploads/2020/12/US-2020-Elections-Report.pdf

AKTAŞ, Celalettin Aktaş. Yeni Medyanın Geleneksel Medya ile Karşılaştırılması. https://personel.klu.edu.tr/dosyalar/kullanicilar/suleyman.ozcan/dosyalar/dosya_ve_belgeler/iletişim%C5%9Fim/Makale%202%20Yeni%20medya-Geleneksel%20medya.pdf

AWARIO, https://app.awario.com

BIKTIM, Ecevit. Tiktok Veri Hırsızlığı ile Gündemde. **CNN Türk**. 2020. https://www.cnnturk.com/teknoloji/tiktok-veri-hirsizligi-ile-gundemde

BINANCE ACADEMY. **İnternetin Evrimi - Web 3.0 Nedir?**. 2021. https://academy.binance.com/tr/articles/the-evolution-of-the-internet-web-3-0-explained

BUDAK, Burak. Bilmeniz Gerekenler: Cambridge Analytica Hikayesi, Facebook ve Büyük Veri. **Webrazzi**. 2018. https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri/

Business Today. **Is Kim Jong Un Dead? Twitter abuzz with rumours of North Korean leader's demişe.** (26 Nisan 2020). https://www.businesstoday.in/current/world/kim-jong-un-dead-twitter-abuzz-with-rumours-of-north-korean-leader-demise/story/402024.html

BOUGHZALA, Imed, JANSEEN, Marijn, & ASSAR, Saïd. E-Government 2.0: Back to Reality, a 2.0 Application to Vet. 2015.https://www.researchgate.net/publication/278652082_E-Government_20_Back_to_Reality_a_20_Application_to_Vet s. 1-12.

CAN, Faruk. Volkswagen 1 Milyon Elektrikli Araç Hedefini İki Yıl Erkene Aldı. **Euronews**. 2019. https://tr.euronews.com/2019/12/27/volkswagen-1-milyon-elektrikli-araci-hedefini-iki-yil-erkene-aldi

CIA Resmî web sitesi. https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence-1.html

CIA Resmî web sitesi. **Geographic Intelligence**. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no4/html/v07i4a14p_0001.htm

CIA Resmî web sitesi. "Scientific Intelligence". **Studies Archiev Indexes**. 2007. Vol. 6. No. 3. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no3/html/v06i3a05p_0001.htm

CNN Resmî web sitesi. **Koronavirüs 'Çin'de bir laboratuvarda üretildiği 'iddiaları: Kim, ne dedi?** 2020. https://www.bbc.com/turkce/haberler-dunya-52596250

D'ARCY, Janice. The Ohio School Shooting and Missed Warning Signs on Twitter. 2012. https://www.washingtonpost.com/blogs/on-parenting/post/the-ohio-school-shooting-and-missed-warning-signs-on-twitter/2012/02/27/gIQABBmUeR_blog.html

DİNÇ, Faruk. Durumsal Farkındalık. **Anka Enstitüsü**. 2018. http://ankaenstitusu.com/durumsal-farkindalik/

DNI Resmî web sitesi. https://www.dni.gov/index.php/what-we-do/what-is-intelligence

DHA Resmî web sitesi. 2018. https://www.dha.com.tr/yurt/turkiyeye-roket-atan-sivil-kiyafetli-teroristler-boyle-goruntulendi/haber-1564458/video/

DUGAN, Lauran. Twitter Used As Impromptu Emergency Broadcast System During Ohio School Shooting. **Adweek**. 2012. https://www.adweek.com/performance-marketing/twitter-used-as-impromptu-emergency-broadcast-system-during-ohio-school-shooting/

DUNCAN, K.C. "Geographic Intelligence". **Center for the Study of Intelligence**. (). Vol. 3. No.2.https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no2/html/v03i2a03p_0001.htm

DW. İnternet Denetimine Sosyal Medyada Tepki. 2018. https://www.dw.com/tr/internet-denetimine-sosyal-medyada-tepki/a-43080811

Etimoloji Türkçe web sitesi. https://www.etimolojiturkce.com/kelime/sigorta

Europen Court of Human Rights. Internet: Case-law of the European Court of Human Rights, **Data-Protection and Retention Issues Relevant for the Internet**, 2015. https://www.echr.coe.int/documents/research_report_internet_eng.pdf

FABRICIO, Benevenuto, GABRIEL, Magno, TIAGO, Rodrigues & VIRGILIO, Almeida. Detecting spammers on Twitter. 2010. https://homepages.dcc.ufmg.br/~fabricio/download/ceas10.pdf

FACEBOOK. Hizmet Koşulları. https://www.facebook.com/legal/terms/update

GABBERT, Elisa. How Do Google Alerts Work? Why Are They Not Working? **Wordstream**. 2020. https://www.wordstream.com/blog/ws/2012/04/10/google-alerts

GALLO, William. Trump'ın Dış Politikada Twitter Kullanımı Endişe Yaratıyor. **Amerika'nın Sesi.** 2016. https://www.amerikaninsesi.com/a/trumpin-dis-politikada-twitter-kullanimi-endise-yaratiyor/3622423.html

GLADWELL, Malcolm. Does Egypt Need Twitter? **Newyorker**. 2011. https://www.newyorker.com/news/news-desk/does-egypt-need-twitter

Gollner.ca. Putting Content In Its Place. 2014. https://www.gollner.ca/2014/04/putting-content-in-its-place.html

Google İstatstik. https://news.google.com/covid19/map?hl=tr&gl=TR&ceid=TR%3Atr

GOV.UK. Emerging Technologies: Big Data. **Hm Government Horizon Scanning Programme**. 2014. https://www.gov.uk/government/publications/emerging-technologies-big-data

GÖKKOYUN, Sevgi Ceren ve ŞENGÜL, Sefa. Siber Âlemin Muhafızları: Beyaz Şapkalı Hackerlar. **Anadolu Ajansı**. Ankara. 2019. https://www.aa.com.tr/tr/bilim-teknoloji/siber-alemin-muhafizlari-beyaz-sapkali-hackerlar/1417719

HABERTURK. **WhatsApp sözleşmesi 2021 nedir, ne anlama geliyor? WhatsApp gizlilik sözleşmesi nasıl iptal edilir?** 2021. https://www.haberturk.com/whatsapp-sozlesmesi-nedir-ne-anlama-geliyor-whatapp-gizlilik-sozlesmesi-nasil-iptal-edilir-2932352-teknoloji

HANDLEY, Paul. Cats, Dolphins and One Smart Raven: The CIA's Secret Animal Spies. **Yahoo! News.** 2019**.** https://news.yahoo.com/cats-dolphins-one-smart-raven-cias-secret-animal-013906580.html

HMIC. The Rules of Engagement. **A Review of the August 2011 Disorders**. s. 31-2.22. https://www.justiceinspectorates.gov.uk/hmicfrs/media/a-review-of-the-august-2011-disorders-20111220.pdf

İTÜBİDB. İnternet'in Tarihçesi. 2013. https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet%27in-tarih%C3%A7esi

JOURNO. **Berat Albayrak istifa haberleri: Eski medya sustu, "Yeni medya" coştu, uluslararası medya gazetecilik yaptı**. 2020. https://journo.com.tr/berat-albayrak-istifa-haberleri

JUDICIARY OF ENGLAND AND WALES. The Queen -v- Kane Gamble, Sentencing Remarks of the Hon. Mr Justice Haddon-Cave. 2018. https://www.judiciary.uk/wp-content/uploads/2018/04/r-v-gamble-sentencing.pdf

KALAIJAN, Rob. 5 Streamers Who Were SWATTED During a Live Stream. **Sportskeeda**. 2021. https://www.sportskeeda.com/esports/5-streamers-swatted-live-stream#:~:text=Swatting%20is%20when%20a%20person,get%20caught%20live%20on%20stream

KEPP, Simon. Digital 2020. **Wearesocial ve Hootsuit**e. 2020. https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

KEMP, Simon. Digital 2021: Turkey. **Wearesocial ve Hootsuite**. 2021. https://datareportal.com/reports/digital-2021-turkey

KEMP, Simon. Digital 2021. **Wearesocial ve Hootsuite.** 2021. https://wearesocial.com/digital-2021

KVKK. Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular. 2018. s. 21. https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular

KVKK. "Alenileştirme" Hakkında Kamuoyu Duyurusu. 2018. https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU

LEWIS, James A. Assesing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington DC, Center for Strategic and International Studies. (December, 2002). s. 9. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

MCMURRAY, Deborah. Have Heard About "Twitterology?" It's the Latest How Now Science. **Lexisnexis**. 2011. https://www.lexisnexis.com/legalnewsroom/legal-business/b/technology/posts/have-you-heard-about-quot-twitterology-quot-it-s-the-latest-hot-new-science

MEOLA, Andrew. Analyzing Tiktok User Growth and Usage Patterns in 2020. **Insider**. 2020. https://www.businessinsider.com/tiktok-marketing-trends-predictions-2020

MİT Resmî Web Sitesi. https://mit.gov.tr/isth-olusum.html

MOROZOV, Evgeny. Facebook and Twitter are Just Places Revolutionaries Go, **Theguardian**, 2011. https://www.theguardian.com/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians

MYREVIEW. Foucault's Panopticon and Understanding Power. 2018. https://mvreview.home.blog/2018/07/22/foucaults-panopticon/

NATO. https://www.nato.int/nato-welcome/index_tr.html

NodeXL. **CodePlex Archive**. https://archive.codeplex.com/?p=nodexl

NYTIMES. A Tunisian-Egyptian Link That Shook Arab History. 2011. https://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?_r=0

O'REILLY, Tim. What is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software. **Oreilly.com**. 2005 https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1

OUENQUA, Douglas. Facebook Knows You Better Than Anyone Else. **The New York Times**. 2015. https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html

ÖNAL, Emre. SOCMINT Kullanımı ve Örnekler. 2019. https://www.blog.emreonal.com.tr/socmint-kullanimi-ve-ornekler/

PALANTIR. **Intelligence**. Palantir.com. https://www.palantir.com/solutions/intelligence/

PAMUKOĞLU, Kadir ve OCAK, Mustafa. Bilişim Teknolojilerinin Devletin Etkinliğindeki Rolü ve İnternet Üzerinden Satış Uygulaması. https://www.harita.gov.tr/uploads/files/articles/bilisim-teknolojilerinin-devletin-etkinligindeki-rolu-ve-internet-uzerinden-satis--1068.pdf

POLINODE. What is Polinode? What Can I Use It For?. https://www.polinode.com/#:~:text=Polinode%20allows%20you%20to%20import,visualize%20it%20and%20analyze%20it.&text=Most%20often%20Polinode%20is%20used%20within%20organizations%20for%20organizational%20network%20analysis

PwC, CIO & CSO. The Global State of Information Security Survey. 2018. https://www.pwc.com.tr/gsiss2018-en

RAND Corp. https://www.rand.org/about/history.html

RESMİ GAZETE. Kişisel Verilerin Korunması Kanunu, Resmî Gazete Sayısı: 29677. 2016. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

SEHL, Katie. Everything Brands Needs to Know About Tiktok in 2020. **Hootsuite**. 2020. https://blog.hootsuite.com/what-is-tiktok/

SERT, Fatma, TÜZÜNTÜRK, Selim & GÜRSAKAL, Necmi. NodeXL ile Sosyal Ağ Analizi: #akademikzam Örneği. 2014. https://www.researchgate.net/profile/Fatma-Sert-Eteman/publication/301650244_NodeXL_ile_Sosyal_Ag_Analizi_akademikzam_Ornegi/links/571fc5e108aeaced788ac917/NodeXL-ile-Sosyal-Ag-Analizi-akademikzam-Oernegi.pdf

SHIFDELETE. WhatsApp'tan İlk Geri Adım! 2021 https://shiftdelete.net/son-dakika-whatsapp-sozlesme-tarihini-erteledi

SIU. A Brief History of IT. **IT Computer Technical Support Newsletter**. 2016. Vol. 2. No. 29. https://ehs.siu.edu/_common/documents/IT%20newsletter/vol-2-no-29.pdf

Statista. **Most popular websites worldwide as of December 2020, by unique visits**. 2021. https://www.statista.com/statistics/1201889/most-visited-websites-worldwide-unique-visits/

Statista. **Leading countries based on Instagram audience size as of January 2021.** 2021. https://www.statista.com/statistics/578364/countries-with-most-instagram-users/

STEARN, Peter N. **Why Study History?** 1998. https://www.sd162.org/cms/lib/IL02218050/Centricity/Domain/534/Why%20Study%20History%20-%20Sterns.pdf

TAYLOR, Jordyn. Mexican Cartel Members Post Drug Photos on Social Media, Get Arrested. **Observer**. 2014. https://observer.com/2014/01/mexican-cartel-members-post-drug-photos-on-social-media-get-arrested/

T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi. **Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu.** Kanun No: 2937. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf

TDK, **Türk Dil Kurumu Sözlükleri**. https://sozluk.gov.tr

TERRAMEDUSA. **Casuslukta İngilizce Asaleti: SOCMINT**. 2013. https://terramedusa.com/casuslukta-ingiliz-asaleti-socmint/ (Erişim tarihi: 21 Nisan 2021).

THE GUARDIAN. **How Riot Rumours Spread on Twitter.** 2011. https://www.theguardian.com/uk/interactive/2011/dec/07/london-riots-twitter (Erişim tarihi: 21 Nisan 2021).

THE GUARDIAN. **Two Years 'Detention for UK Teenager Who 'Cyberterrorised 'US Officials.** 2018**.** https://www.theguardian.com/technology/2018/apr/20/two-years-detention-for-uk-teenager-who-cyberterrorised-us-officials-kane-gamble (Erişim tarihi: 21 Nisan 2021),

THE SOUFAN GROUP. **Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq.** 2015 https://www.cvereferenceguide.org/sites/default/files/resources/TSG_ForeignFightersUpdate3.pdf (Erişim tarihi: 21 Nisan 2021).

TINFOLEAK. https://www.tinfoleak.com

Title 1 - Reform of the Intelligence Community, SEC. 1001. Subtitle A - Establishment of Director of National Security (DNI).https://web.archive.org/web/20151211013650/http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-irtpa (Erişim tarihi: 21 Nisan 2021).

TRT HABER. **WhatsApp'ın Yeni Şartları Avrupa Birliği'nde Geçerli Değil.** 2021 https://www.trthaber.com/haber/bilim-teknoloji/whatsappin-yeni-sartlari-avrupa-birliginde-gecerli-degil-547606.html (Erişim tarihi: 21 Nisan 2021).

TRT HABER **Hangi Dijital Medya Platformları Türkiye'de Temsilcilik Açıyor?** 2021. https://www.trthaber.com/haber/bilim-teknoloji/hangi-dijital-medya-platformlari-turkiyede-temsilcilik-aciyor-545811.html (Erişim tarihi: 21 Nisan 2021).

ULICNY, Brian, MOSKAL, Jakub, & KOKAR, Mieczyslaw M. "Situational Awareness from Social Media". **STIDS**. 2013. https://vistology.com/wp-content/uploads/2016/02/STIDS2013_T12_UlicnyEtAl.pdf (Erişim Tarihi: 21 Nisan 2021).

US DEPARTMENT OF DEFENCE. **Perception Management**. https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4039 (Erişim tarihi: 21 Nisan 2021).

WATSON, Bruce W. (2012). Intelligence. **Encyclopedia Britannica.** https://www.britannica.com/topic/intelligence-military (Erişim Tarihi: 21 Nisan 2021).

WIKIPEDIA. **Vikipedi**. https://tr.wikipedia.org/wiki/Vikipedi

YALÇINKAYA, Hikmet.' Türkiye Neden S-400 alıyor? 'sorusuna verilebilecek en net 'Patriot ' yanıtı. gzt.com. 2019. https://www.gzt.com/jurnalist/turkiye-neden-s-400-aliyor-sorusuna-verilebilecek-en-net-patriot-yaniti-3494789 (Erişim Tarihi: 21 Nisan 2021).

Yeni Çağ Gazetesi Resmî web sitesi. **Siber Saldırıların Yeni Hedefi "Bağlı Arabalar".** 2019. https://www.yenicaggazetesi.com.tr/siber-saldirilarin-yeni-hedefi-bagli-arabalar-247079h.html (Erişim Tarihi: 21 Nisan 2021).