Teknoloji, günümüzde hayatın hemen her alanına tamamen nüfuz ve etki etmiştir. Eğitim, sağlık, ticaret ve güvenlik gibi temel kamu politikalarında teknolojik gelişmeler belirleyici bir faktör haline gelmiştir. Yeni teknolojilerin kamu politikalarında katılımı ve denetimi, şeffaflığı ve hesap verebilirliği artırması, daha hızlı, daha düşük-maliyetli ve sürdürülebilir politikaların önünü açması önemli kazanımlardır. Öte yandan teknolojik gelişmelerin neden ve sonuçları ile hayatımıza somut etkilerini anlayabilmek için bazı önemli soruları kendimize sormamız gerekmektedir: Genelde devlet yönetimini özelde ise kamu politikalarını dönüştüren yeni teknoloji ve iş yapma biçimleri nelerdir? Dünyada ve Türkiye'de bilinmesi gereken başarılı örnekler hangileridir? Bu teknolojiler hangi sorunları çözmekte, ne gibi yeni sorunların ortaya çıkmasına neden olmaktadır? Uygulamada karşılaşılan sorunlar nelerdir ve bunlar nasıl çözülebilir? En önemlisi, Türkiye'nin teknoloji politikaları nasıl tasarlanmalı ve uygulanmalıdır?

Bu kitapta, konusunda uzman bilim insanları tarafından yazılan bölümlerde; açık veri, akıllı kent, bilgi yönetimi, büyük veri, insan-makine etkileşimi, insansız ve otonom araçlar, kameralı güvenlik sistemleri, nesnelerin interneti, oyunlaştırma, sağlık bilişimi, siber güvenlik, sosyal medya, trol olgusu, yapay zekâ ve yaşayan laboratuvarları gibi konular detaylı bir şekilde analiz edilmiştir. Alan yazında yeni teknoloji ve iş yapma biçimlerinin kamu politikalarına etkilerini sistematik bir biçimde incelemesi açısından bir ilk olan bu kitabın öncelikle bu konuya ilgi duyan araştırmacılara, lisans ve lisansüstü düzeyde bir ders ve referans kitabı olarak okuyuculara ve bu konulardan faydalanmalarını umduğumuz politika yapıcılara yararlı olmasını diliyoruz.

ISBN 978-625-7727-28-0
9 786257 727280

Gazi Kitabevi

Merkez	Mağaza
53. Sok. No: 29 Bahçelievler / ANKARA Tel : (0 312) 223 77 73 - 223 77 17 Faks: (0 312) 215 14 50	Dögol Caddesi No: 49/B Beşevler / ANKARA Tel : (0 312) 213 32 82 - 213 56 37 Faks: (0 312) 213 91 83

info@gazikitabevi.com.tr • www.gazikitabevi.com.tr

TEKNOLOJİ VE KAMU POLİTİKALARI

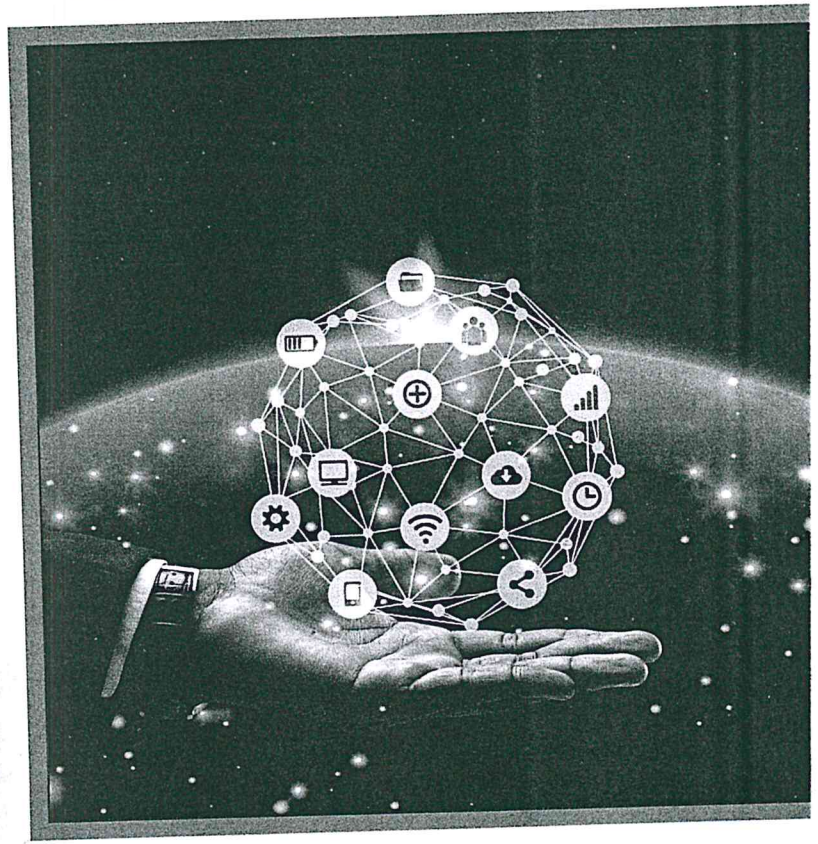
Prof. Dr. Mete YILDIZ
Doç. Dr. Cenay BABAOĞLU

Gazi Kitabevi

TEKNOLOJİ VE KAMU POLİTİKALARI

Derleyenler

Prof. Dr. Mete YILDIZ - Doç. Dr. Cenay BABAOĞLU



Gazi Kitabevi

Gazi
Kitabevi

"En İyi Akademi, Bir Kitaplıktır."

TEKNOLOJİ VE KAMU POLİTİKALARI
Yeni Teknoloji ve İş Yapma Biçimlerinin Kamu Yönetimi ve Politikalarına Etkisi

Prof. Dr. Mete YILDIZ
Doç. Dr. Cenay BABAOĞLU

ISBN • 978-625-7727-28-0
Baskı • Ekim, Ankara, 2020

Dizgi/Mizanpaj • Gazi Kitabevi
Kapak Tasarım • Gazi Kitabevi

Gazi Kitabevi Tic. Ltd. Şti.
Yayıncı Sertifika No: 44884

Merkez
Bahçelievler Mah. 53. Sok. No: 29 Çankaya/ANKARA
0.312 223 77 73 - 0.312 223 77 17
0.312 215 14 50
www.gazikitabevi.com.tr
info@gazikitabevi.com.tr

Mağaza
Dögol Cad. No: 49/B Beşevler/ANKARA
0.312 213 32 82 - 0.312 213 56 37
0.312 213 91 83

Sosyal Medya
gazikitabevi
gazikitabevi
gazikitabevi

İlksan Matbaası Ltd. Şti. Matbaa
Sertifika No: 47073

aa
İvedik Organize San. Bölgesi Ağaç İşleri San. Sit. 521 Sk. No: 35 İvedik/ANKARA

Üzerimde büyük emekleri olan Robert Agranoff, Şinasi Aksoy, Juliet Musso, Aykut Polatoğlu ve Muhittin Acar'a en içten teşekkürlerimle...

Mete Yıldız

Desteklerini hep arkamda hissettiğim anneme ve babama...

Cenay Babaoğlu

BÖLÜM 1

YENİ TEKNOLOJİ VE İŞ YAPIŞ BİÇİMLERİNİN KAMU POLİTİKALARINA ETKİLERİ: GENEL BİR ÇERÇEVE

Mete YILDIZ[1]

Sanayi Devrimi'nden bu yana teknolojik gelişmeler doğumdan ölüme hayatımızın her dönemini ve tüm idari, siyasi, toplumsal ve ekonomik faaliyet alanlarını hızla dönüştürmektedir. İçinde bulunduğumuz 21. Yüzyılın ilk çeyreğinde yeni teknoloji ve iş yapış biçimlerinin söz konusu etkisi daha da güçlenerek genişlemiş ve çeşitlenmiştir. Hatta öldükten sonra bile teknolojinin ölen kişinin hayatı üzerindeki etkisi bir süre daha devam etmektedir. Örneğin, sosyal medya platformlarındaki hesaplar, kullanıcısı öldükten sonra bile, daha önceden kullanıcı tarafından belirlenen bir "hesap varisi"ne devredilerek kullanıma ve dolayısıyla yaşamaya devam edebilmektedirler. Benzer şekilde, ölen kişinin mezarını ziyarete giden yakınları büyükşehir mezarlıklarındaki kabrin yerini, mezarlık girişindeki belediye kiosklarından da hizmet veren Mezarlık Bilgi Sistemleri yardımıyla yaptıkları arama yoluyla bulabilmektedirler.

Bugün artık hayatın hiçbir alanı kalmamıştır ki, teknoloji ona neredeyse tamamen nüfuz ve etki etmemiş olsun. Eğitim, sağlık, ticaret ve güvenlik gibi hayatın çeşitli alanlarında teknolojik gelişmeler giderek daha da

Savunma Sanayi Başkanlığı (2018). *Savunma Sanayi Sektörel Strateji Dokümanı (2018-2022)* https://www.ssb.gov.tr/Images/Uploads/MyContents/F_20190402102925477924.pdf, Erişim Tarihi: 12.08.2020.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020). *Hakkımızda*, https://cbddo.gov.tr/hakkimizda/, Erişim Tarihi 15.08.2020.

TUSAŞ (2020). *ANKA-S Projesi*, https://www.tusas.com/haber/anka-s-projesi, Erişim Tarihi: 10.08.2020.

Yalçın, H. ve Erboğa A. (2017), "Milli İHA Siyasi İradeyle Üretildi", *Kriter Dergisi*, 2(14), https://kriterdergi.com/soylesi/milli-iha-siyasi-iradeyle-uretildi, Erişim Tarihi: 22.08.2020.

Yıldız, Mete ve Ekmekçioğlu, Alper (2018), "İnsansız Hava Araçlarının Askeri ve Sivil Alanlarda Kullanımı: ABD ve Türkiye Örnekleri ve Bazı Politika Önerileri", *Türk İdare Dergisi*, 486, s. 169-227.

Yüksekbilgili, Zeynep ve Yüksekbilgili, Gözde (2018), "Endüstri 4.0 Bağlamında Türkiye'nin Yerine İlişkin Güncel ve Gelecek Eksenli Bir Analiz", *İktisat İşletme ve Finans*, 10.29106/fesa.412009, Erişim Tarihi: 15.07.2020.

Zhang, Tao ve Qing, Li (2017), "Current Trends in the Development of Intelligent Unmanned Autonomous Systems", *Frontiers of Information Technology & Electronic Engineering*, 18(1), s. 68-85.

BÖLÜM 14

SOSYAL MEDYA VE GÜVENLİK POLİTİKALARI

Kamil DEMİRHAN[1]

Ali ÇAĞLAR[2]

BÖLÜM TANITIMI

Bu çalışmanın, sosyal medyanın günümüzdeki etkilerini anlama, eğlence ve ticaret gibi popüler kullanım alanlarının ve amaçlarının ötesinde, siyaset ve yönetimle ilgili alanlarda farklı kullanım amaç ve biçimlerini öğrenme, bunlar üzerine düşünme ve analiz etme sürecinde katkı sağlaması umulmaktadır. Çalışmanın amacı, sosyal medya istihbaratı bağlamında sosyal medyanın ulusal güvenlik bakımından sağladığı olanakları ve riskleri değerlendirmektir. Bununla birlikte, emniyet güçlerinin sosyal medya istihbaratı uygulama ve politikalarına ilişkin literatürün sınırlı olması nedeniyle, Türkiye'de bu konuyla ilgili akademik alandaki boşluğa dikkat çekmeyi de amaçlamaktadır. Çalışmada, ilk önce sosyal medya istihbaratı kavramı açıklanmıştır. İkinci ve üçüncü kısımda sosyal medya istihbaratının kamu güvenliği bakımından sağladığı olanaklar ve riskler, dünyadaki örnekler üzerinden açıklanmıştır. Dördüncü kısımda, Türkiye'de sosyal medyanın, kamu güvenliği bağlamında polis tarafından kullanımı, konuyla

[1] Doç. Dr., Zonguldak Bülent Ecevit Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi Bölümü Öğretim Üyesi, 67100, ZONGULDAK. E-posta: demirhankamil@beun.edu.tr

[2] Prof. Dr., Hacettepe Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi Bölümü Öğretim Üyesi, 06800, Beytepe/ ANKARA. E-posta: acaglar@hacettepe.edu.tr

ilgili haberler üzerinden incelenmiştir. Son olarak, sosyal medya istihbaratının meşruiyeti bireysel haklar, özgürlük, gözetim ve güvenlik bağlamında değerlendirilmiştir. Çalışma, sosyal medyanın ulusal güvenlik bakımından olanaklar sağlamakla birlikte, sosyal medyanın küresel düzeyde bir çekişme ve rekabet alanı olması nedeniyle birtakım riskler de barındırdığına dikkat çekmektedir. Bu çalışmada, Türkiye'de konuyla ilgili haberler üzerinden yapılan incelemede, sosyal medya ve kamu güvenliği bağlamında sosyal medyanın polis tarafından kullanımına ilişkin uygulamaların "sanal devriye" ve "siber polis" kavramları çerçevesinde kamuoyuna yansıdığı görülmektedir.

Anahtar Kelimeler: Sosyal Medya İstihbaratı, Kamu Güvenliği, Terör, Sanal Devriye, Siber Polis

Öğrenme Çıktıları

- Bu bölüm ile sosyal medyanın güvenlik politikaları açısından önemi hakkında bilgi edinilir.
- Bu bölüm kapsamında sosyal medya istihbaratı yaklaşımı hakkında bilgi edinilir.
- Türkiye'de ulusal güvenlik açısından sosyal medyanın oynadığı rol ve yapılması gerekenler ile farklı ülkelerdeki yaklaşımlar hakkında bilgi edinilir.

GİRİŞ

Sosyal medya, dünyada çok sayıda kişinin bilgi paylaştığı sözlükler, bloglar, haber, resim, video paylaşım platformları ile insanlar, gruplar, örgütler ve kurumlar arasında etkileşim ve iletişim kurulan sosyal ağ sitelerinden oluşmaktadır (Fuchs, 2013). Sosyal medyanın gelişiminde geleneksel Web 1.0 teknolojilerinden etkileşime imkân tanıyan Web 2.0 teknolojilerine geçiş etkili olmuştur. Web 2.0 terimi ilk olarak 2004 yılında, Tim O'Reilly tarafından kullanılmıştır. Web 2.0 tek taraflı internet sayfalarından kullanıcıların karşılıklı etkileşim kurabileceği, hizmet sunumu ve katılım gerçekleşebileceği platformlara geçişi ifade etmektedir (O'Reilly, 2012, s. 34). Sosyal medya sitelerinin 2002 yılından itibaren gelişmeye başladığı görülmektedir. Fotolog (2002), LinkedIn (2003), MySpace (2003), Last.FM (2003), Hi5 (2003), Flickr (2004), Facebook (2004), Bebo (2005), YouTube (2006), Twitter (2006), Tumblr (2007), Instagram (2010) Google+ (2011), Pinterest (2011) küresel düzeyde popüler olan sosyal medya platformlarıdır. Sosyal medya, eğlence ve ticaretin yanı sıra; yönetim, katılım, siyasal iletişim, siyasal pazarlama, reklamcılık, diplomasi, acil durum ve kriz yönetimi gibi pek çok alanda kullanılmaktadır.

Sosyal medya platformlarının çok sayıda kullanıcısı bulunmaktadır. Kullanıcılar her an gittikleri yerleri, nerede bulunduklarını ne düşündüklerini ne okuduklarını ne yediklerini ya da ne giyindiklerini, kiminle birlikte vakit geçirdiklerini, hangi taşıtı kullandıklarını, sevdikleri veya sevmedikleri şeyleri sosyal medya platformlarında paylaşmaktadırlar. Sosyal medya platformları diğer kullanıcılara açık alanlardır. Kullanıcılar, birbirlerinin paylaşımlarını görebilmekte; sosyal ağlarında kimlerin olduğu, en son hangi siteye girdikleri, kimi beğendikleri, kimi takip ettikleri ve kim tarafından takip edildiklerini tespit edebilmektedir. Sosyal medya kullanıcıları, örgütlenme, kaynak bulma, haberleşme, propaganda, halkla ilişkiler, deneyim ve uzmanlık paylaşımı, mobilizasyon gibi amaçlarla bu araçlardan faydalanmaktadır. Sosyal medya, geleneksel kitle iletişim araçlarına göre, kolay ulaşılabilir, yayın için büyük ve uzman bir ekip gerektirmeyen, olay merkezli ve olayın tanıklar tarafından aktarımına izin veren, veri paylaşımının hızlı ve yoğun bir şekilde gerçekleştiği, kullanım maliyetleri düşük ve gözetimin sınırlı olduğu, etkileşime imkân tanıyan platformlardan oluşmaktadır.

Sosyal medya istihbaratı; bu açık haberleşme, iletişim ve etkileşim kaynağından sağlanan bilgilerin kamu güvenliği amacıyla toplanması, analizi ve kullanılması anlamına gelmektedir. Sosyal medya istihbaratı, toplumsal ayaklanmalarda, acil durumlarda ve krizlerde yanlış bilgi ve haber paylaşımı ve provokasyonun önlenmesi gibi amaçlarla kullanılabilmektedir. Ayrıca, terörle mücadelede önemli bir rol üstlenmektedir. Sosyal medya bir istihbarat kaynağı olarak kamu güvenliğine katkı sağlarken diğer yandan birtakım riskleri de içerisinde barındırmaktadır. Terör örgütleri sosyal medya üzerinden kaynak sağlamakta, üye bulmakta ve kendi propagandalarını bu araçlar üzerinden yapmaktadır. Ülkeler sosyal medya istihbaratını birbirlerine karşı kullanabilmektedir. Kamuda çalışanlar ya da vatandaşların yaptığı paylaşımlar kamu güvenliğini tehdit edebilecek sonuçlar doğurabilmektedir. Bazı durumlarda da saldırı amacıyla gizli bilgilere ulaşılmakta ve bunların sızdırılması ile ulusal güvenliği tehlikeye düşüren sonuçlar ortaya çıkabilmektedir.

Sosyal medya istihbaratının önemli bir boyutu da devletin sosyal medya iletişimini takip etmesine bağlı olarak ortaya çıkan toplumsal risklerdir.

Bireylerin iletişiminin izlenmesi ve takip edilmesi, hükümetlere karşı bir güvensizliğin doğmasına, bireylerin bu alanda kendilerini kısıtlanmış hissederek tepki duymasına neden olabilmektedir. Bu güven probleminin aşılmasında, prosedürlere uyulması, yasal sınırlar içerisinde kalınması, bireysel hak ve özgürlüklere müdahale edilmemesi ve vatandaşların sosyal medya istihbaratının güvenlik bağlamında kendilerine fayda sağladığına ikna olması önemli bir rol oynamaktadır. Sosyal medya istihbaratının olanak ve risklerine geçmeden önce, sonraki bölümde, sosyal medya istihbaratı kavramı daha ayrıntılı şekilde açıklanmaktadır.

1. SOSYAL MEDYA İSTİHBARATI: KAVRAMSAL ÇERÇEVE

Siber istihbarat, devlet güvenliği açısından saldırı ve sızmaları, kitlelerin hareketlerini önceden bilerek tehlikeleri önleme işlevine sahiptir (Savaş ve Topaloğlu, 2015). Sosyal medya istihbaratı, siber elektronik istihbarat, siber açık kaynak istihbaratı gibi farklı siber istihbarat yöntemlerinden biridir ve bu istihbarat yöntemleriyle ilişki içerisindedir (Bayraktar, 2014: 131). Sosyal medya istihbaratı (SOCMINT – Social Media Intelligence) siber istihbaratın bir parçası, bütünleyicisi olarak, sosyal medyada her an gerçekleşen paylaşımlarda suça ilişkin içeriklerin bulunabileceğinden hareketle, sosyal medya verilerinden program ve algoritmalar kullanarak bilgi ve kanıt bulma, bunları doğrulama, analiz etme ve uygulama süreçlerini ifade etmektedir (Omand, vd., 2012). Sosyal medya istihbaratı kendi içerisinde açık-kaynaklı ve kapalı-kaynaklı olarak birbirinden ayrılmakta olup meşruiyet ve kolaylık açısından açık kaynaklı istihbarat kendi içerisinde daha az sorun taşımaktadır (Omand, vd., 2012:820). Diğer taraftan sosyal medya istihbaratını, siber istihbaratın bir parçası olan sinyal istihbaratının ve açık kaynaklı istihbaratın bir parçası olarak gören yaklaşımlar da mevcuttur. Açık kaynaklı istihbarat Birleşik Krallık, İsveç, Hollanda gibi ülkelerde istihbarat çalışmalarının büyük bir kısmını oluşturmaktadır (Ünver, 2018: 3).

Yoğun ve hızlı bir şekilde gerçekleşen haberleşme faaliyetleri ve kurulan sosyal ağlar sosyal medyada analize açık bir veri yığını, "büyük veri" oluşturmaktadır. Dünya'da ülkelerin güvenlik güçleri özellikle kitlesel ayaklanma ve protesto gibi toplumsal olaylarda ve terörle mücadelede sosyal medyadan faydalanmaktadır. Sosyal medyada olay esnasında kullanıcılar tarafından paylaşılan bilgilerin ve sosyal ağların analizi kamu güvenliğinin sağlanması bakımından etkili olmaktadır. Örneğin, 2011 yılında olimpiyatlar öncesinde Londra'da yaşanan ayaklanmalar sonrasında merkezi polis birimi sosyal medyadan işlenen ve planlanan suçları tespit etmek ve toplumun nabzını ölçmek amacıyla veri toplamış ve bunları analiz ederek -Flickr'da paylaşılan fotoğraflardan şüphelilerin tespiti gibi- kullanmıştır. Sosyal medya yoğun veri akışıyla istihbarat için önemli bir bilgi kaynağı oluştursa da bu verinin yönetilebilirliği önemli bir problemdir. Sosyal medyadaki verinin analizi, istihbarat servisleri için özel bir teknik altyapı ve yüksek kaliteli insan gücünü gerektirmektedir. Sosyal medya, özellikle içerik ve haberlerle ilgili analiz ve bilginin doğrulanması noktasında sorun yaratmaktadır. Bu durum hem insan kaynağını hem de analiz ve filtreleme işlemlerini kolaylaştıracak program desteğini gerektirmektedir (Omand, vd., 2012:802-8). Geliştirilen algoritmalarla bilgisayar tabanlı öğrenme araçları büyük veri setlerinin analizine imkân tanırken, duygu analizi gibi konularda yetersiz kalmaktadır. Bu konuda hem grupların davranış ve normlarını hem de çevrimiçi kültürü, dili ve davranışları analiz edebilen uzman ihtiyacı ortaya çıkmaktadır (Omand, vd., 2012:813). Söz konusu teknik donanım ve uzmanların amacı, değişken, karışık ve büyük veriye dayanan istihbaratın doğru kişiyle güvenli ve stratejik olarak kullanılabilir şekilde iletilmesini sağlamaktır (Omand, vd., 2012).

Sosyal medya istihbaratı kamu güvenliğine katkı sağlarken öne çıkan işlevleri, "olay anında, olay yerinden kitle kaynaklı bilgi sağlamak; sorunun kökenini ve arkasında yatan nedenleri araştırmak ve analiz etmek; sosyal medyada iletişim trafiği üzerinden gelişmekte olan olayları tespit etmek; grupların davranışlarını daha iyi anlayabilmek, tepkilerinin nedenlerini görmek için gruplara özgü iletişim ortamlarına dâhil olmak; suça ilişkin unsurları tespit ederek suçun önlenmesi veya suçun kovuşturulması" (Omand, vd., 2012:802) olarak ifade edilebilir. Sosyal medya istihbaratı ulusal güvenlik bağlamında devletin takip, kontrol ve gözetimi bakımından sorunlar yaratabilmektedir. Sosyal medya istihbaratının meşruiyeti, bu istihbaratın toplumun huzur ve güvenliğine katkı sağlaması ve güvence altında olan diğer kamusal hak ve özgürlüklere engel ya da tehdit teşkil etmemesine bağlıdır (Omand, vd., 2012: 807). Diğer taraftan, sosyal medya istihbaratı yalnızca devlet tarafından değil, resmi olmayan sivil analistler ve özel şirketler tarafından da yapılabilmekte ve sahip oldukları yasal sınırlılıklardan muafiyet, esneklik, otonomluk gibi özellikleriyle bilgi toplama ve analiz faaliyetlerinde önemli avantajlar yaratmaktadır. Ayrıca, resmi olmayan kuruluşlarda Cambridge Analytica, Facebook, Google, Amazon gibi nitelikli analistlerin istihbarat kuruluşlarına oranla daha rahat koşulları nedeniyle daha fazla tercih edildiği de belirtilmektedir (Ünver, 2018: 6).

Sosyal medya, yalnızca ulusal güvenlik için olanaklar yaratmamaktadır. Snowden, Wikileaks ve Cehsea Manning ifşalarında olduğu gibi, sivillerin devlete karşı kullanabileceği ya da devletlerin birbirlerine karşı kullanabileceği bilgilerin bu açık kaynaktan elde edilmesi de söz konusudur. Devlet düzeyindeki sızıntılar hükümetlere ve istihbarat servislerine zarar verebilmektedir (Ünver,2018:7). Cambridge Analytica şirketinin 50 milyonu bulan Facebook kullanıcılarının bilgilerini 2016 Amerika Birleşik Devletleri (ABD) başkanlık seçimlerinde usulsüzce kullanımı bu duruma örnek oluşturmaktadır (Habertürk, 2018). Ayrıca, bu bilinen veya ifşa olmuş kuruluşların yanı sıra henüz ifşa olmamış veya kim tarafından kurulduğu, hangi amaçlarla nasıl kullanıldığını henüz bilmediğimiz oluşumların var olabileceğini de göz önünde bulundurmak gerekir.

2. SOSYAL MEDYA İSTİHBARATININ KAMU GÜVENLİĞİ BAKIMINDAN OLANAKLARI

Sosyal medyanın emniyet güçleri tarafından istihbarat amacıyla kullanımı bazı olanaklar yaratmaktadır. Öne çıkan işlevleri;

i. "İstihbarat kaynağı,
ii. Güvenlik meseleleri ile ilgili gerçek zamanlı bilgilendirme kanalı,
iii. Halkı internetin zararlarından korumak için bilgi kaynağı,
iv. Polis kurumları içerisinde bilgi paylaşımı" şeklinde sıralanmaktadır (Crump, 2012 akt. Özçetin, 2015: 26).

Sosyal medyanın emniyet açısından kullanımında önemli bir anlayış, kalabalıktan anlamlı bilgi edinmek ve toplumu polisin faaliyetlerine katkı sağlamaya yönlendirmek şeklinde ifade edilmektedir. Polisin, sosyal medya istihbaratını kamu güvenliğini sağlamak amacıyla kullanımına ilişkin ilk örneklerden biri, 2011 yılı Ağustos ayında Londra'da Mark Duggan adlı bir kişinin polis tarafından vurulmasıyla, Tottenham'da başlayan iki gün içerisinde şiddet eylemlerine dönüşen protestolardır. Protestolarda eylemciler polise ve özel mülkiyete karşı saldırılara başlamıştır. Ayaklanmalar kısa sürede İngiltere'deki diğer şehirlere de yayılmış, kamu güvenliği bakımından büyük bir risk ortaya çıkarak halkın can ve mal güvenliği endişesi oluşmuştur (HIMC, 2011: 13). Hem polis hem de vatandaşlar en hızlı şekilde iletişim kurmaya yönelmişlerdir. Polis, olayları bastırmak ve kamusal düzene ilişkin riski en aza indirmek üzere ayaklanmanın başladığı gün sosyal medyada takibe başlayarak ayaklanmayı organize edenler ve olası saldırı hedeflerini tespit etmeye çalışmıştır. medya paylaşımları üzerinden tespit edilmiş ve polis bu eylemi engellemiştir. Polisin ihbarlar için oluşturduğu internet sayfasına çok fazla kitle-kaynaklı ihbar gelmiştir. Yoğun ihbar ve iletişimle birlikte, sosyal medya istihbaratının yönetilebilirliği sorunu ortaya çıkmıştır. Twitter'ı takip eden görevli bir polis memuru, *'tweetler o kadar hızlı geliyor ki onları okumaya fırsat kalmadan sayfanın sonuna gidiyor'* diyerek iletişimi takip etmenin zorluğundan bahsetmiştir (HIMC, 2011: 31). Bu noktada, sosyal medya istihbaratının daha önce de söz edilen bilgilerin filtrelenmesi, analiz edilmesi ve anlamlı istihbarata dönüştürülmesi süreçlerinde yardımcı teknik araçlar ve insan kaynağının önemi görülmektedir (HIMC, 2011: 31).

Dünyada ABD, İngiltere, Kanada gibi ülkeler sosyal medya istihbaratını etkin şekilde kullanmaktadır (Baltacı, 2017). Örneğin, ABD'de CIA sosyal medyadan istihbarat toplamak üzere "vengeful librarians – intikamcı kütüphaneciler" olarak isimlendirilen bir grup oluşturmuştur. Bu grup Usame Bin Ladin'in öldürülmesi üzerine dünyada kamuoyunun tepkisini ölçmeye çalışmıştır (Blunden ve Cheung, 2014). İran seçimleri sonrası patlak veren "yeşil devrim" olarak anılan seçim sonuçlarına ilişkin protestolar da bu grup tarafından yakından takip edilmiştir (Dozier, 2011). Açık kaynak istihbaratı yalnızca resmî kurumlar tarafından değil özel şirketler tarafından da gerçekleştirilmektedir. CIA bağlantılı kar amacı gütmeyen stratejik bir kuruluş olarak açıklanan In-Q-Tel (iqt.org, 2020) ve Google'ın içerisinde olduğu özel bir şirket olan *"Recorded Future"* internette gerçek zamanlı veri tarayarak olaylar ve insanlar arasında bağlantı kurmuş ve bu verileri kullanarak geleceğe ilişkin tahminler yapmıştır. ABD merkezli ve çok-uluslu savunma teknolojileri alanında faaliyet gösteren Raytheon aldı şirketin geliştirdiği RİOT (Rapid Information Overlay Technology) adlı program ile Facebook, Twitter, Foursquare gibi web sitelerinde paylaşılan trilyonlarca içerik (fotoğraflar) analiz edilerek insanlarla ilgili nereye gittikleri, kiminle iletişim kurdukları ve bir sonraki adımda ne yapacakları hakkında bilgi toplanmakta ve ulusal güvenlik sistemi inşa edilmektedir. Şirket, endüstri, ulusal laboratuvarla ve ticari ortaklarıyla birlikte büyük veriyi ulusal güvenlik ihtiyaçları doğrultusunda, -hakkında bilgi topladıkları bireylerin ulusal güvenlik riski taşıyıp taşımadığı gibi- kullanılabilir bilgiye dönüştürmek için faaliyet gösterdiğini açıklamaktadır (The Guardian, 2013). ABD Ulusal Güvenlik Ajansı'nın (NSA) kullandığı PRISM uygulaması ile sosyal medya ve e-posta veri tabanlarına ulaşılarak istihbarat toplanmasını sağlamaktadır. ABD İç Güvenlik Bakanlığı (DHS) vatandaşlık başvurusu yapan kişileri değerlendirirken sosyal medya

istihbaratından yararlanmaktadır. ABD İç güvenlik Bakanlığı, Sosyal Ağ İzleme Merkezi üzerinden sosyal medya kullanıcılarını izlemektedir. ABD Polis Teşkilatı da PredPol (Predictive Policing) yazılımıyla sosyal medyadan suçun önceden tahmini ve suçların soruşturulması sürecinde yararlanmaktadır (Baltacı, 2017: 128-132).

Sosyal medya istihbaratının kullanıldığı bir diğer durum, yeni sosyal hareketlerdir. Sosyal medya toplumsal hareketlerin organizasyon ve eylemlerinde etkili olmaktadır. Bir protesto durumunda konuyla ilgili paylaşımda bulunan sosyal medya kullanıcılarının mesajları dakika dakika takip edilerek protestocuların sayısı ve hareketleri ile ilgili bilgi toplanmakta, istihbarat görevlileri olayların öncesinde ve olaylar süresince alandan bilgi sağlamakta hem göstericilerle hem de vatandaşlarla çevrimiçi olarak iletişimini sürdürmektedir (Policeforum, 2013: 15). Örneğin, Kanada'da Toronto polis teşkilatı, suçla mücadelede, suçluların tespiti ve kamuyla iletişim süreçlerinde sosyal medyadan faydalanmıştır. 2010 G20 Zirvesi ve "Toronto'yu İşgal Et – Occupy Toronto" protestolarında polis, protestocuların sosyal medya iletişimlerini takip ederek olası riskleri hesaplamış, ayrıca vatandaşlar ile polis arasında iletişim kurmak için sosyal medyadan yararlanmıştır (Policeforum, 2013).

Dünyada artan terör tehdidiyle birlikte, dijital istihbarat, terörist grupların irtibatlarını tespit etmek ve terörist saldırıları deşifre etmek bakımından daha fazla önem kazanmıştır. Terörist grupların dünyada giderek güç kazanması, tüm ülkelerin kamuoyunda ulusal güvenlik bakımından önemli endişeleri beraberinde getirmiştir. Sosyal medya, terörle mücadelede farklı şekillerde kullanılmaktadır. Örneğin, Nijerya'da Boko Haram'a karşı sosyal medya istihbaratı hükümet tarafından karşı-operasyon, karşı-propaganda, dijital gözetim, haberleşme gibi terörle mücadelede önemli olanaklar sağlamaktadır (Chukwuere ve Onyebukwa, 2018). Sosyal medyanın emniyet güçleri tarafından kullanımı, potansiyel tehditlerin önceden tespitini, terör örgütlerinin üye sağlama yollarını ve kaynaklarının tespitini, saldırı yöntemlerini tespit etme ve bunlara karşılık verirken hangi araçların kullanılabileceğini belirlemede faydalı olmaktadır. Ayrıca, sosyal medya kamu güvenliğini sağlarken yanlış, yalan, yanıltıcı haberler ve bilgilerle mücadelede, kamu diplomasisinde insanların düşünce ve yaklaşımlarını öğrenme ve değiştirmede etkili olmaktadır (Kimutai, 2014: 56-5).

Sosyal medya siber saldırıların tespiti için de etkili bir istihbarat alanı olarak ifade edilmektedir. "Sıfırıncı gün (zero-day) atakların, saldırı gerçekleşmeden ya da henüz çok yayılmadan sosyal medya üzerinden tespit edilebilmesi" bu duruma örnek teşkil etmektedir (Ekşim ve Civelek, 2019: 827). Bir siber saldırı planı yapılırken ya da hazırlık aşamasında, bu planı tasarlayanlar başka kişilerle ilişki kurmakta, özellikle de "karanlık web" olarak da adlandırılan sitelerde takip, siber saldırının hazırlık aşamasındayken tespit edilmesine imkân sağlayabilmektedir. Sosyal medyada tehdit oluşturan paylaşımların tespiti de sosyal medya paylaşımlarının analizinde olduğu gibi bilgisayar destekli analizleri gerektirmekte ve siber tehditlere ilişkin veri toplayan 'makine temelli öğrenme' araçları sosyal medya istihbaratının bir parçası haline gelmektedir. Örneğin, Twitter'da yaklaşık günlük paylaşılan tweet sayısı 500 milyon civarındadır ve CyberTwitter, siber güvenlikle ilgili tweetlerin analizini gerçekleştirilmesine yardımcı bir araç olarak kullanılmaktadır (Ekşim ve Civelek, 2019: 829-830). CyberTwitter uygulamasının ana işlevi Twitter üzerindeki paylaşımları toplama, sınıflandırma ve analiz ederek anlık olarak tehlikelere karşı kullanıcıları uyarmaktır (Mittal, vd. 2016:1). Sosyal medya istihbaratına bağlı oluşan veri çekme, arşiv, analiz, sınıflandırma gibi ihtiyaçlar bu tür uygulamaların önemini arttırmaktadır.

3. SOSYAL MEDYA VE ULUSAL GÜVENLİK BAKIMINDAN RİSKLER

Sosyal medya istihbaratı ulusal güvenlik için emniyet güçlerine yukarıda bahsedildiği gibi önemli imkânlar sağlarken, diğer taraftan risk oluşturan gruplar için bir propaganda alanı sağlamaktadır. Örneğin, terörist gruplar bu alan üzerinden örgütlenerek, kendilerine yeni kaynaklar bulabilmekte, eğitim ve hazırlık faaliyetlerini geliştirmekte ve diğer suç örgütlüleriyle eşgüdüm içerisinde hareket edebilmektedir. Terör örgütleri sosyal medya üzerinden birbirleriyle benzer düşüncelere sahip kişileri bir araya getirmekte, benzer şekilde düşünen insanlarla ve kritik konumdaki üyeleriyle bağlantı kurmak amacıyla sosyal medyayı kullanmakta, sosyal medya terör faaliyetlerini normalleştirilmesine olanak sağlamakta, devlete yönelik karşıt duyguların yayılmasına imkân tanımaktadır (Cox, vd., 2018; Kimutai, 2014). Örneğin, Nijerya'da faaliyet gösteren Boko Haram ile yoğunluklu olarak Somali ve Kenya'da operasyonlar düzenleyen Eş-Şebab terör örgütü, Facebook ve Twitter üzerinden faaliyetlerine ilişkin video ve fotoğrafları paylaşarak ağlar üzerinden kendi gündemlerini küresel düzeyde yaymaktadır (Rodriguez (2014:8). Eş-Şebab, hazırladığı videolarla gençlere hitap etmekte hem Somali diasporası hem de batıdan yeni kişileri bünyesine katmak için çabalamaktadır. Örgütün, Kenya, Nairobi'de 2013 yılında

gerçekleştirilen Westgate alış-veriş merkezinde düzenlediği saldırı Twitter üzerinden gerçek zamanlı olarak bildirilmiştir. Örgüt, olayla ilgili İngilizce çok sayıda tweet paylaşarak, hikâyeyi dünyaya kendisi anlatmış, dikkatleri Kenya hükümetinin yayınından kendi yayınına çekmiştir (Cox, vd., 2018). Boko Haram, özellikle 2015 yılından itibaren İŞİD'e tabi olduktan sonra, yoğunluklu olarak sosyal medyayı kullanmıştır. Kullanım düzeyini belirleyen unsurlardan biri de Afrika'daki internet erişimindeki artış olmuştur. Boko Haram, çoğunlukla Youtube, Twitter, Facebook gibi platformları kullanan gençlere hitap etmekte, yaptıkları başarılı operasyonları, devam eden saldırıları ve rehinelere yaptıklarını sosyal medya üzerinden paylaşmaktadır. Bu paylaşımlar eylemciler, takipçiler ve potansiyel üyeleri hedef almaktadır (Cox, vd., 2018). Örgüt propaganda faaliyetlerinde, Nijerya hükümetini hedef alan paylaşımlarda bulunmakta ve kendi silahlı gücünü göstermektedir. Örgüt sosyal medyadan, İŞİD gibi ortaklarıyla ve farklı ülkelerdeki liderlerle koordinasyon kurmak için de faydalanmaktadır. İŞİD, Eş-Şebab ve Boko Haram'a göre daha geniş bir sosyal medya kullanımına sahiptir. Çoğunlukla, Facebook, Twitter, WhatsApp, Telegram, JustPaste.it, Kik ve Ask.fm gibi platformları kullanmaktadır. Örgüt bu platformlar üzerinden mikro-topluluklar oluşturarak sempatizanlarla iletişim kurmakta, kendisi dışındaki etki kaynaklarını ortadan kaldırmakta ve saldırı planları yapmaktadır (Cox vd., 2018:30-36).

Bir başka güvenlik riski de sosyal medya üzerinden halkın örgütlendiği ve harekete geçtiği toplumsal hareketlerdir. Sosyal medya pek çok toplumsal harekette ve protestoda insanlar arasında haberleşme, örgütlenme, mobilizasyon sürecinde etkili olmuştur. 2009 yılında Londra'da G20 zirvesi protestoları (Ward, 2009), 2009 yılında İran'da ve Moldova'da seçim sonuçlarına ilişkin protestolar (Morozov, 2009b; Rahimi, 2011), 2010 ve 2011 yılı boyunca Kuzey Afrika ve Orta Doğu ülkelerinde yaşanan, "Arap Baharı" olarak adlandırılan protesto ve halk ayaklanmaları (Axford, 2011; Ghannam, 2011), ABD'de 2011 yılında yaşanan "Wall Streeti İşgal Et" olayı (Gaby ve Caren, 2014), 2013 yılında Türkiye'de yaşanan Gezi olayları (Demirhan, 2014), 2014 yılında Hong Kong'da yaşanan "Şemsiye Hareketi" (Kaiman, 2014), 2018 yılında Fransa'da başlayan "Sarı Yelekliler" hareketi (Newton, 2018), 2019 yılında Irak'ta yaşanan protesto (Al-Awsat, 2019) hareketlerinde sosyal medyanın etkili rol oynadığı görülmüş; bu hareketlerin bir kısmı "sosyal medya devrimi" olarak adlandırılmıştır. Sosyal medyaya yönelik kamu politikaları da toplumsal hareketlerde etkili olmaktadır. Protestolarda kamu otoritelerinin internet erişimini yönlendirmek yerine engelleme doğrultusundaki politika, karar ve uygulamaları, ayaklanmaların genişlemesine, hatta çoğu kez de şiddetlenmesine neden olmaktadır. Örneğin Mısır'da, hükümet tarafından halkın internet erişiminin kesilmesi, insanları gelişmelerden haberdar olabilmek için sokağa çıkartmıştır (Assange vd., 2012: 29).

Protesto ve ayaklanmalarda, sosyal medya bir taraftan kaynak sağlama, haberleşme, mobilizasyon, halkla ilişkiler gibi işlevler sağlarken daha stratejik düzeyde göstericiler polis müdahalesini sosyal ağlar ve paylaşımları üzerinden öngörebilmekte, kendi pozisyonlarını polisin hareketlerini tahmin ve tespit ederek değiştirebilmektedir. Buna karşın, bu sosyal ağlar ve paylaşımlar üzerinden polisin istihbarat sağlaması, gösterinin gidişatını takip etmesi ve göstericileri tespit ederek müdahalede bulunması da mümkündür. Mısır'da gerçekleşen ayaklanmaların, eğer ABD'de gerçekleşseydi ve başarısızlıkla sonuçlansaydı sosyal medya paylaşımlarının[3] çok etkili bir istihbarat aracı haline dönüşeceği belirtilmiştir (Assange vd., 2012: 29).

Sosyal medyanın toplumsal hareketlerdeki işlevleri örgütleme, organizasyon gibi her zaman ulusal güvenlik bakımından risk oluşturmayabilir. Sosyal medya katılımın bir aracı olarak da işlevseldir ve sosyal hareketler de toplumsal taleplerin, meşru sınırlar içerisinde ifade edilebilmesi bakımından olanak sunmaktadır. Kamuoyunun çeşitli sorunlar karşısında bilgilenmesi, harekete geçmesi ve gayri resmi iletişim ağları üzerinden karar alıcılara taleplerini iletmesi sosyal medyanın demokratik açıdan sağladığı bir fırsat olarak değerlendirilebilir. Diğer taraftan, sosyal medyanın demokrasiye etkisi konusunda karamsar yaklaşımlar da vardır. Bu yaklaşımlarda, sosyal medya ülkelerin içişlerine karışmak üzere, yabancı ülkelerin kullandığı bir araç olarak görülmekte ve sosyal medya üzerinden örgütlenen hareketler bir risk olarak açıklanmaktadır. Örneğin, karamsar yaklaşımın temsilcilerinden Morozov, İran'da 2009 yılındaki protestolarda, Twitter'da paylaşılan tweetlerin Farsça olmadığını vurgulamaktadır. Morozov'a göre (2009a), Twitter aktivistleri tarafsız kişiler değil, batı yanlısı İngilizce bilen İranlılar ya da İranlı diasporadan oluşmaktadır. Ayrıca paylaşılan tweetlerin büyük bir bölümünün, yerel halkın kendi dilinde değil İngilizce tweetler olduğu vurgulanmıştır. Morozov bu durumu, ayaklanmaların kendiliğinden değil, rakip siyasi güçler tarafından örgütlendiğinin bir göstergesi olarak değerlendirmektedir.

[3] Mısır'da, 16-30 Ocak tarihleri arasında, içinde "Mısır Hareketi" geçen 1,5 milyona yakın tweet paylaşılmıştır (Murthy, 2013: 97).

Bu noktada, sosyal medya istihbaratının ülkelerin birbirlerine karşı kullanma riski belirginleşmektedir. Bu risk, Facebook, Twitter gibi ABD merkezli iletişim alanlarının, Çin'in yaptığı gibi başka ülkeler tarafından güvenlik gerekçeleriyle kullanılmaması durumunu ortaya çıkarmaktadır (Baltacı, 2017). Çin, Facebook, Twitter, Youtube gibi yabancı sosyal medya sitelerine ilişkin güvenlik riski nedeniyle yasaklayıcı politikalar uygularken, Çin'de Twitter'a yakın işlevleri olan Sina Weibo gibi alternatif sosyal medya platformları kullanılmaktadır (Yu vd., 2011; Willnat, vd., 2015).

Sosyal medyanın ulusal güvenlik bakımından oluşturduğu bir diğer risk, ülkelere ilişkin gizli bilgilerin, yazışmaların sızdırılması ve bunların ülkeler üzerinde yarattığı skandal tehdidiyle uluslararası politikada birer silaha dönüşmesidir. Bu tür sızıntılar, ülkelerin iç siyasetlerinde belirleyici olabilmektedir. Örneğin, daha önce bahsedilen toplumsal ayaklanmalarda etkili olmaktadır. Tunus'taki ayaklanmalar, Tunus başkanıyla ilgili ortaya çıkan Wikileaks belgeleri nedeniyle skandal patlak verdikten kısa bir süre sonra başlamıştır (Bachrach, 2011). Wikileaks ile ABD'nin diplomatik yazışmalarına ilişkin binlerce belge, ABD medyasında yer almıştır.

Sosyal medya küresel düzeyde devlet ve devlet dışı aktörler tarafından sürdürülmekte olan bilgi savaşının bir parçasını oluşturmakta ve bu savaşın galibini belirlemede etkili bir araç olmaktadır. Sosyal medyanın kamu kurumlarında çalışanlar tarafından kullanımı bu bilgi savaşı içerisinde ulusal güvenlik risklerini arttırabilmektedir. Bazı hükümetler işyerlerinde Facebook ve Twitter kullanımını yasaklamaktadır (Salik ve Iqbal, 2019). Baltacı (2017:152) özellikle kolluk ve istihbarat personeline yönelik bir risk oluşturabileceğini belirtmiş ve organize suç örgütlerinin bu personelin sosyal medyadaki kişisel bilgilerinden ve eğilimlerinden yararlanarak güvenlik tehdidi oluşturabildiğine dikkat çekmiştir. Sosyal medyada yalnızca suç örgütleri değil yabancı istihbarat örgütleri de faaliyet göstermektedir. Yabancı istihbarat örgütleri ulusal güvenlikle ilgili konularda yaşamsal öneme sahip bilgileri bu açık kaynaklarda yapılan paylaşımlardan elde edebilmektedir. Sosyal medya bu açıdan özellikle düşman lojistiğinin tespiti, operasyonel detaylar, eğitim alanları, mühimmat ve silah gücü, bölükler hakkında yaşamsal bilgiler sunmaktadır (Salik ve Iqbal, 2019). Kimutai, (2014: 46-47). Sosyal medyanın yanlış kullanımına bağlı olarak ulusal güvenlikle ilgili risklerin ortaya çıktığı vurgulanmakta ve kurumların kendi personeline, uzmanlık alanına uygun olarak sosyal medya kullanımına ilişkin eğitim vermesi gerektiğine dikkat çekilmektedir. Örneğin, ABD hükümeti, bu doğrultuda bir strateji geliştirmiş ve sosyal medyanın güvenli kullanımıyla ilgili kendi birimlerine yardımcı olması, kamu görevlilerinin davranışlarına odaklanan ve güvenlik kültürü eksiğini kapatmaya yönelik bir rehber hazırlamıştır. Kimutai (2014) sosyal medya üzerinden oluşabilecek özellikle bilgi istemlerine yönelik iki önemli riske; kimlik hırsızlığı ve kötü / zararlı yazılımlara dikkat çekmiştir.

Sosyal medyadaki bilgi paylaşımı bakımından bir diğer risk, yanlış, yalan veya yönlendirici bilgilerin paylaşılması ve bu bilgilerin çok kısa süre içerisinde yayılmasıyla ortaya çıkan etkilerdir. Örneğin, 2013 yılında ABD'nin kâr amacı gütmeyen haber ajansı "Associated Press"in (AP) Twitter hesabından paylaşılan, "Beyaz Saray'da İki Patlama! Obama Yaralandı" tweeti sonrasında Dow Jones Borsası'nda önemli bir düşüşle 136 milyar dolar civarında bir kayıp yaşanmış, AP kısa sürede Twitter hesabının ele geçirildiğini (heklendiğini) açıklayarak, haberi yalanlamıştır (Fisher, 2013). Bazı organize gruplar, deprem, sel, nükleer tehlike, küresel çapta salgın hastalık gibi acil durum, felaket ya da kriz sorasında harekete geçerek insanları yanlış yönlendirmekte, kurtarma operasyonlarını geciktirmekte veya yanıltmakta; böylece ülkeye zarar vermektedir (Kimutai, 2014: 37). Bu örnekler, sosyal medyanın ve sosyal medyadan sağlanan istihbaratın sağladığı olanakların yanı sıra ulusal güvenlik bakımından önemli riskleri de içerisinde barındırdığını göstermektedir.

4. TÜRKİYE'DE SOSYAL MEDYA'NIN ULUSAL GÜVENLİK AMACIYLA KULLANIMI: "SİBER POLİS" VE "SANAL DEVRİYE"

Türkiye'de sosyal medyanın istihbarat amaçlı kullanımına ilişkin çalışma sayısı az olmakla birlikte; mevcut çalışmalar içerisinde genel olarak polisin sosyal medya kullanımına ilişkin çalışmalar ön plana çıkmaktadır. Özçetin ve Özçetin'in (2015) araştırması, Türkiye'de İl Emniyet Müdürlükleri'nin sosyal medya kullanımını ele alan sınırlı sayıdaki çalışmadan biridir. Polisin Twitter aktivitelerinin incelendiği bu çalışmada, Twitter'ın en fazla suç/olay bilgisi paylaşımı olduğu; ikinci olarak kurumsal bilgilerin paylaşıldığı, üçüncü olarak da toplum destekli polislik, "suçla mücadele ve güvenlik politikası sürecine aktif katılım ve destek" faaliyetlerinin geçekleştirildiği belirtilmiştir. Özçetin ve Özçetin (2015) Türkiye'de polisin sosyal medyanın etkisine ilişkin farkındalığının özellikle Gezi olaylarından sonra başladığını vurgulamış, sosyal medyanın iletişim, etkileşim ve kamuoyu oluşturma özelliklerinin yanı sıra "gözetim ve izleme" potansiyelinin de farkına varmaya başladığını belirtmiştir.

He ne kadar Baltacı (2017: 152) ülkemizde sosyal medya istihbaratının kullanımına ilişkin bir belgeye rastlamadığını belirtmişse de Taşcı ve Can (2015) Emniyet Genel Müdürlüğü'nün Siber suçlarla mücadelede 2003 yılından sonra mevzuat olarak bazı düzenlemeleri yaptığı, 2011 yılı itibariyle de kurumsal yapılanmasını büyük ölçüde tamamladığını açıklamıştır. Türkiye'de 2011 yılında siber suçlarla mücadeleyi tek bir çatı altında toplayarak, etkin bir mücadele için EGM bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı ismiyle kurulan (Taşcı ve Can, 2015) ve 2013 yılında Siber Suçlarla Mücadele Daire Başkanlığı (SSMDB) adını alan kurum, 2018 yılında 2700 personel ile sanal ortamda izleme yaptığını kamuoyu ile paylaşmıştır (Kızılkoyun, 2018).

SSMDB'nın görev ve yetkileri arasında;

- "Her türlü iletişimi dinleme yetkisi,
- Veri, ses ve görüntü kaydı alma yetkisi,
- Siber polisin önemli soruşturmalarda başka bir konumdaki bir bilişim sistemine uzaktan erişim sağlama yetkisi" (Taşcı ve Can, 2015:239) gibi yetkiler sayılmıştır.

SSMDB'ye bağlı olarak kurulan Siber Suçlarla Mücadele Şube Müdürlükleri altında, Adli Bilişim Büro Amirliği, Operasyon Destek Büro Amirliği, Bilgi Teknolojileri Büro Amirliği gibi amirlikler arasında, 'Sanal Devriye Büro Amirliği' de kurulmuş ve önleyici bir birim olarak öngörülmüştür. Bu amirliğin, "emniyet birimlerinin internet üzerindeki varlığını güçlendirmek, suç önleme mesajlarını yaymak ve internet topluluğu ile iletişim içerisinde olmak için sosyal medya platformlarından mümkün olduğunca faydalanmaları" (Taşcı ve Can, 2015: 239) için katkı sağlayacağı belirtilmiştir.

Türkiye'de sosyal medya istihbaratına ilişkin çalışma sayısı az olmakla birlikte, polisin bu alandaki faaliyetlerini incelemek bakımından basında çıkan haberler konuyla ilgili bilgi sağlamaktadır. Yapılan haber incelemelerinde, '*Sanal devriye*' kavramına, TRT Haber'in (2013) Temmuz 2013 tarihindeki haberinde rastlanılmıştır. Bu haberde Emniyet Genel Müdürlüğü (EGM) bünyesinde Sanal Devriye Büro Amirliği kurulduğu bilgisi paylaşılmış ve şu şekilde açıklamalarda bulunulmuştur: *"Sanal Devriye Büro Amirliği ekipleri, internette işlenen 'intihara yönlendirme, cinsel taciz, tehdit, hakaret, şantaj, fuhuşa teşvik ya da aracılık etmek' gibi suç işleyenlerin peşine düştü."* .... *"'651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun' kapsamında görev yapan Sanal Devriye Büro Amirliği, Asayiş Daire Başkanlığı'nın görev alanına giren suçların internet ortamında işlenmesi durumunda, suç unsurları tespit edilerek dijital deliller elde ediyor"* haberiyle, emniyetin internet ortamındaki izleme faaliyetlerinin hangi suçları hedef aldığı ve izleme yapan birimlerin dayandığı mevzuat hakkında bilgi vermektedir. Söz konusu kanun, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşlarına internet ortamındaki içerikleri izleme imkânı vermektedir.

2017 yılında 680 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname'de sanal ortamda takip ile düzenlemeler yapılmıştır. 2018 yılında, 7072 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 26. maddesiyle 2559 sayılı Polis Vazife ve Selahiyet Kanunu'nun ek 6. maddesine eklenen on sekizinci fıkrada, *"Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir"* denilerek, sanal ortamda takibin yasal zemini oluşturulmuştur (Resmi Gazete, 2018). Ancak, 19/02/2020'de Anayasa Mahkemesi, 7072 Sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un bazı kurallarının iptalini gerçekleştirmiş, 7072 sayılı Kanun'un 26. maddesiyle 2559 sayılı Polis Vazife ve Selahiyet Kanunu'nun ek 6. maddesine eklenen on sekizinci fıkrada iptal edilerek, *"Sanal ortamda işlenen suçlar da dahil olmak üzere suç soruşturmasını yapacak yetkili Cumhuriyet başsavcılığının belirlenmesi ve bu konuya ilişkin uyuşmazlıkların çözümü yargı makamlarının görevi"* olduğu belirtilmiştir. Diğer taraftan, 7072 sayılı Kanunun 27. Maddesi ve 2559 sayılı Kanun'un ek 7. Maddesi'nde *"Polis, devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere, ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla iş birliği yapar"* denilerek "sanal ortam" istihbarat toplama alanı içerisinde sayılmıştır.

Konuyla ilgili yapılan haber incelemeleri, sanal devriye ve siber polis faaliyetleri ve bu faaliyetlerin neleri kapsadığı konusunda birtakım bilgiler sağlamaktadır. 15 Haziran 2018 tarihli, Hürriyet Gazetesi (2018a) haberinde

Siber Suçlarla Mücadele Daire Başkanlığı personeli, yasa dışı paylaşımları, terör faaliyetlerini ve devlet büyüklerine hakaretleri sosyal medya dâhil olmak üzere internet ortamında tespit ettiği belirtilmiştir.

30 Mayıs 2018 tarihli CNN Türk (2018) haberine göre, Adana polisi, siber suçlarla mücadele için "sanal devriye ekibi" kurduğunu açıklanmış, haberde 24 saat bu görevlilerin Twitter ve Facebook dâhil olmak üzere internet ve sosyal medyada paylaşılan içerikleri inceledikleri belirtilmiştir.

22 Kasım 2018 tarihinde Hürriyet Gazetesi'nde (2018b), "FBI ve Samsun Siber polisinin Darknet operasyonu: 1 gözaltı" başlıklı haberde, "Darknet ve Deepweb gibi karanlık internet olarak adlandırılan sanal dünyada işlenen suçlardan çocuk istismarı ile ilgili 1 kişinin gözaltına alındığı" bilgisi paylaşılmıştır.

11 Aralık 2018 tarihinde Milliyet Gazetesi'nin (2018) haberine göre, Samsun Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü ekiplerinin yaptıkları sanal devriyede "'Darbeturks.com' isimli internet sitesinde değişik banka ve kurumlara ait sitelerin sahtesini -sahte oltalama sitesi- (phishing script) hazırlayıp satışının yapıldığının" tespit edildiği ve olayla ilgili soruşturma yapıldığı bilgisi paylaşılmıştır.

19 Aralık 2018 tarihinde Milliyet Gazetesi'nin haberinde EGM'nin 2018 yılı içerisinde 11 bin sosyal medya hesabı üzerinde çalışma yaptığı, 7 bin 109 kişinin gözaltına alındığı, suç içerikli paylaşım yapan 2,754 kişinin tutuklandığı açıklanmıştır. Açıklamada, "Siber Suçlarla Mücadele Dairesi Başkanlığı tarafından yapılan çalışmalarda, yaşam hakkı ile kişilerin can ve mal güvenliği, milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesinin yanı sıra sosyal medya ağlarının terör örgütleri ile onların paravan yapılanmaları tarafında suç amacına hizmet eden bir savaş aletine dönüştürülmesi, hedef kitlelerine kendi propagandasını yapmaları, toplumsal infial yaratmaları, üye kazanmaları ve finansal kaynak elde etmeleri, terör olaylarını abartarak ve manipülasyon malzemesi haline getirerek toplumda sansasyonel etki yaratmalarının engellendiği" belirtilmiştir. EGM çalışmalarını internet üzerindeki açık kaynaklarda, aralıksız olarak sürdürüldüğü belirtilmiş bu çalışmalar ise "sanal devriye" terimiyle açıklanmıştır. Bu amaçla, "ödeme sistemleri, bilişim sistemleri, uyuşturucu, silah, DAEŞ, FETÖ/PDY, PKK/KCK, YPG, aşırı sol terör örgütleri, güvenlik, eskort, çocuk istismarı, yasadışı bahis, idari soruşturma ve diğer olaylar" olmak üzere 12 masa kurulduğu açıklanmıştır.

TRT Haber (2019) 25 Mart 2019 tarihinde, "'Sanal Devriye' görevi yürüten siber polislerin geçen yıl yaptığı çalışmalarda, bilişim, ödeme sistemleri ve yasa dışı bahis suçlarından 6 bin şüpheli gözaltına alındı" şeklindeki haberinde EGM Siber Suçlarla Mücadele Daire Başkan Yardımcısı, birçok suçun aynı zamanda siber suçları ilgilendirdiğini, siber suçu içinde barındırdığını belirtmiştir.

NTV'nin 9 Ekim 2019 tarihli haberinde, Emniyet Genel Müdürlüğü'nün "Barış Pınarı Harekâtı üzerinden Türkiye aleyhinde kara propaganda yaparak, halkı kin ve nefrete tahrik eden, güvenlik güçlerinin itibarını zedelemek maksadıyla kaynaksız ve yalan paylaşımlarda bulunan, terör örgütü propagandası yaptığı görülen 78 kişi ile ilgili gerekli yasal işlemlerin başlatıldığı" açıklamasına yer verilmiş ve "Türk Polis Teşkilatı olarak suç ve suçlularla mücadelemizi her alanda sürdürdüğümüz gibi sanal ortamda da sürdürmeye devam edeceğiz" şeklindeki açıklaması aktarılmıştır.

HaberTürk (2019) 28 Kasım 2019 Perşembe günü Elâzığ'da "Barış Pınarı Harekâtı" ile ilgili terör örgütü PYD/YPG'nin amaçları doğrultusunda sosyal medya üzerinden propaganda yapan 6 şüphelinin gözaltına alındığı" haberini vermiştir.

17 Ocak 2020 tarihinde, Anadolu Ajansı'nın haberinde Emniyet Genel Müdürlüğü bünyesinde Siber Operasyon Merkezi'nin açıldığı duyurulmuş, İçişleri Bakanı Süleyman Soylu'nun konuyla ilgili, "Siber saldırılara karşı Siber Operasyon Merkezimizi açtık. Dışarı çıktığımda artık daha huzurluyum" ifadesi aktarılmıştır.

Sosyal medyada gerçekleştirilen paylaşımlar üzerinden terör propagandası yaptığı ya da provokatif paylaşımlarda bulunduğu iddiasıyla açılan soruşturmalar son yıllarda giderek artmıştır. Bu durum emniyet birimlerinin sosyal medyadaki iletişim faaliyetlerini takip ettiğinin, ya da bu alandaki ihbarları dikkate aldığının bir göstergesidir. NTV'nin (2020) haberine göre, Elazığ'da 24 Ocak 2020'de meydana gelen depremden sonra sosyal medya üzerinden yaptığı paylaşımların provokatif niteliği nedeniyle elli kişi hakkında soruşturma açıldığı bildirilmiştir.

Basında yer alan haberler incelendiğinde, Türkiye'de sosyal medyanın, suçluların tespiti amacıyla kullanıldığı görülmektedir. Türkiye'de son yıllarda ülke gündemini ilgilendiren güvenlikle ya da acil durumlarla ilgili olaylarda sosyal medya üzerinden yapılan paylaşımların güvenlik riski olarak değerlendirildiği söylenebilir. Örneğin, İdlib'de 34 Türk askerinin şehit olması sonrasında sosyal medya üzerinden yapılan paylaşımlar incelenerek, 28 Şubat 2020 tarihinde mesaj içerikleri provokatif nitelikte paylaşımlar gerçekleştiren sosyal medya kullanıcıları hakkında Cumhuriyet başsavcılıkları tarafından soruşturmalar başlatılmıştır: A.A'nın 28 Şubat 2020

tarihli haberine göre, Ankara Cumhuriyet Başsavcılığı konuyla ilgili yaptığı açıklamada; "Suriye'nin İdlib şehrinde gerçekleştirilen menfur saldırı sonucu şehit edilen askerlere ait olduğu yönünde sosyal medya üzerinden provokatif amaçlı ve gerçeğe aykırı olarak yayımlanan video, resim ve paylaşımlar hakkında 'halkı kin ve düşmanlığa tahrik veya aşağılama', 'kanunlara uymamaya tahrik' ve 'terör örgütü propagandası yapmak' suçlarından re'sen soruşturma başlatıldığı" bilgisini paylaşmıştır.

Milliyet Gazetesi'nin 07 Mart 2020 tarihli haberinde, emniyetin korona-virüsle ilgili olarak paylaşım yapan hesaplara ilişkin çalışma başlattığı ifade edilmiştir. Konuyla ilgili halkı gerçek olmayan paylaşımlarla panik yaratacak paylaşımların adli mercilere iletileceği belirtilmiştir. Emniyet Genel Müdürlüğü'nün açıklamasında, "Siber Suçlarla Mücadele Daire Başkanlığı ekiplerinin, sosyal medyada milli ve manevi değerlere saldırı, sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge farklılığına dayanarak yapılan hakaret ve saldırılar ile korku ve panik oluşturarak kamu düzenini bozan paylaşım yapan hesapları tespit etmek amacıyla yedi gün 24 saat esasına göre sanal devriye faaliyetleri yürüttüğü" belirtilmiştir.

Habertürk'ün (2016) haberinde "MİT, sosyal paylaşım sitelerine karşı uyardı" başlıklı haberinde, "MİT'in stratejik tüm kurumlarda Facebook ve Twitter gibi sitelere kurum bilgisayarından girilmemesi yönünde uyarıda bulunduğu ve birçok kurumda sosyal medya sitelerine kamu bilgisayarlarından girişi engellediği belirtilmiştir. Türkiye'de haber aramalarında MİT'in sosyal medya istihbarat faaliyetlerine ilişkin bilgi sağlanamamıştır. Basında yer alan haberler değerlendirildiğinde; Türkiye'de polisin, kamu güvenliğini tehlikeye sokabilecek durumlarda sosyal medya üzerinden halka yönelik yönlendirme ve provokasyon amacıyla yapılan faaliyetleri tespit etmek amacıyla bu alanı takip ettiği görülmektedir.

5. GÖZETİM VE TEMEL HAKLAR BAKIMINDAN ELEŞTİRİLER

Sosyal medya istihbaratının bir boyutunu güvenlik diğer boyutunu ise mahremiyet oluşturmaktadır ve bu ikisi arasındaki gerilim, 11 Eylül saldırılarından sonra daha da belirginleşmiştir. Ancak, 2011 yılında Wikileaks adıyla sızan gizli belgeler ve 2013 yılında ABD Merkezi İstihbarat Teşkilatı (CIA) ve Ulusal Güvenlik Dairesi (NSA) eski çalışanı Edward Snowden'ın NSA gibi kurumların gizli iletişimleri takip ettiğinin ortaya çıkması, ulusal güvenlik amacıyla gerçekleştirilen istihbarat

Özellikle, kişisel bilgilerin ve iletişimin gizliliği, özgürlükler ve sivil haklar bağlamında ele alınmıştır (Walsh ve Miller, 2015).

Edward Snowden'ın, dünyada devletlerin iletişimi ve verileri izlediğine ilişkin açıklamaları, vatandaşların kamu otoritelerine karşı tepkisine neden olmuş ve kişisel verilerin gizliliğine ilişkin talepleri gündeme getirmiştir. Bu gözetim hissi aynı zamanda kullanıcıların internetteki davranışlarında birtakım değişiklikler yaratabilmektedir (Bayerl ve Akhgar, 2015: 63). Bu durumun önemli bir sonucu, insanların kendileriyle ilgili doğru bilgileri vermelerinden kaçınmaları, yanlış bilginin artması, doğrulama maliyetlerinin ortaya çıkması olmuştur (Bayerl ve Akhgar, 2015: 63).

İnternette devletlerin iletişim faaliyetlerini izlemesiyle ilgili olarak, Bayerl ve Akhgar'ın (2015: 63) çoğunluğu (%83,9) ABD olmak üzere Hindistan, Kanada, Hırvatistan, Kenya, Romanya gibi ülkelerden katılımcıların bulunduğu ankete dayalı bir araştırmasına göre, katılımcıların neredeyse tamamı az ya da çok, paylaşımlarının ülkelerinde gözetime takıldığını belirtmiştir. Katılımcıların yarıdan fazlası, kendileriyle ilgili "isim" ya da "e-posta adresi" bilgilerini uydurduklarını, yanlış bilgi verdiklerini belirtmiştir. Bayerl ve Akhgarın çalışması (2015: 64), ulusal güvenlik risklerinin, terör tehdidinin ve açık kaynak istihbaratı sayesinde daha güvenli bir ortamın oluşması beklentisinin bireylerin gözetimi kabul etmelerinde etkili olduğunu göstermektedir. Genellikle, gözetime yönelik eleştiriler, hükümete karşı güvensizlik ve ifade özgürlüğüne ilişkin tehdit potansiyeli ile bağlantılıdır.

Özçetin ve Özçetin (2015), polisin sosyal medya üzerinden gerçekleştirdiği toplumla ortak istihbarat paylaşımını, polisin gözetleme ve düzenleme faaliyetlerinin parçası olarak değerlendirmektedir. Gözetim faaliyetlerine gönüllü katılım, sosyal medya tarafından ve aracılığıyla daha yoğun bir şekilde gerçekleşmektedir. Burada vatandaşların üzerinde durduğu konu güvenliktir. Walsh ve Miller (2015), güvenlik ve gizlilik konusunda, istihbarat faaliyetleri bireysel özgürlüklere ilişkin tehditler yaratırken diğer taraftan da istihbaratın kaldırılmasının ulusal güvenlik risklerini ortaya çıkarabileceğini vurgulayarak bu noktada gerçekçi çözümlere ihtiyaç olduğunu vurgulamaktadır. Terörizm gibi insan yaşamına yönelik tehditler karşısında güvenlik ihtiyacı istihbaratın meşruiyet kazanmasında önem taşımaktadır. Sosyal medya istihbaratı bağlamında, gözetim ve sonuçlarından olumsuz etkilenen yalnızca haklar bakımından bireyler değil aynı zamanda mali olarak değer kaybeden Google, Facebook, ...

özgürlük dengesinin kurulması büyük önem arz etmektedir. Bu dengeyi kurarken iletişimin gerçekleştiği sosyal medya platformlarının da sorumluluğu bulunmakta, kişisel verilerin kâr ya da siyasal çıkar amaçlı izinsiz olarak kullanılmaması, şirketlerin kişisel verilerin gizliliğini ihlal etmemesi oldukça önem taşımaktadır.

DEĞERLENDİRME

Sosyal medya istihbaratı, sosyal medyanın yaygın ve yoğun bir şekilde kullanımına ve kullanıcıların her türlü duygu, düşünce, faaliyet, beğeni, ilişki ve kendilerine ilişkin bilgilerin paylaşımına bağlı olarak, devletin güvenlik birimlerinin kamu güvenliği amacıyla, sosyal medyadan bilgi toplaması, sınıflandırması, analiz etmesi ve bunları stratejik olarak kullanması süreçlerinden oluşmaktadır. Bu verilerden hareketle, güvenlik politika ve stratejileri oluşturulmakta ve uygulamalar gerçekleştirilmektedir. Bu çalışmada, sonuç olarak sosyal medya istihbaratının kamu güvenliği bakımından sağladığı olanaklar, aynı zamanda neden olduğu birtakım riskler bir arada değerlendirilmeye çalışılmıştır. Sosyal medya bireyler için kendini ifade etme, sesini duyuramayanlar için sesini duyurma, vatandaşlar için yaşadıkları sorunları ilgililere bildirme, ya da siyasete daha fazla katılma imkânı sağlayan bir alan/araç olarak görülebilir. Kamu politikası aktörleri, sosyal medyayı yalnızca istihbarat amacıyla kullanmamaktadır. Kurumlar için sosyal medya iletişimi toplumla, vatandaşlarla irtibat kurma, kendini anlatma, bilgilendirme, verdikleri hizmetlere ilişkin değerlendirme almanın bir aracıdır. Bu süreçler düşünüldüğünde sosyal medya istihbaratı kamunun sosyal medya kullanımının diğer kullanım amaçlarıyla bağlantılı bir parçası olarak da görülebilir.

Sosyal medyanın kamu otoriteleri tarafından izlenmesi, kamu otoritelerinin temel haklara müdahalesi bağlamında devlet ve toplum ilişkilerinin gerilmesine ve meşruiyet sorununa neden olabilmektedir. Bu noktada, gözetimin güvenlik amacının ötesine geçmemesi önem kazanmaktadır. Dikkat edilmesi gereken bir diğer unsur, gözetimin yalnızca kamu otoritelerinden değil sosyal medya hizmeti sağlayan özel şirketler tarafından da gerçekleştirilmesi ve bu gözetimin kullanıcılar tarafından çok fazla dikkate alınmamasıdır. Bu açıdan, sosyal medya kullanıcılarının, haklarına yönelik hassasiyeti uygulamalarından faydalandıkları sosyal medya şirketlerine karşı da göstermeleri önem taşımaktadır. Bu çalışmanın içerik sınırlılıkları dikkate alınmak kaydıyla, Türkiye'de sosyal medya istihbaratı konusunda çalışma sayısının az ve bu konuda kamu politikalarına [illegible] da sınırlı olduğu tespitini yapmak mümkündür. Türkiye'de sosyal medyanın ulusal güvenlik bağlamında kullanımında polisin etkili olduğu, sosyal medyayı kamu güvenliği amacıyla takip ettiği ve sosyal medyadaki etkinliğinin "sanal devriye" ve "siber polis" kavramlarıyla ifade edildiği görülmektedir. Güvenlik, gözetim ve özgürlük ilişkisi bakımından, Türkiye'de bu alandaki strateji, plan ve uygulamaların, haberlerle sınırlı kalınmayarak, daha çeşitli platformlar üzerinden kamuoyuna duyurulması, anlatılması bu gerilimin çözülmesinde katkı sağlayabilir. Yasal süreçlerle ilgili bilgilendirmelerin gözetim tartışmasının yükselmesine ve güven kaybına olanak vermeden en erken sürede yapılması, kamu personelleri ya da güvenlik çalışanları gibi farklı kullanıcılara hitap eden ve olası sorunları önceden hesaba katan sosyal medya kullanım rehberlerinin hazırlanması, bu alanda fayda sağlayabilir. Bunlardan daha da önemlisi, ülkenin vatandaşları arasında bir farkındalık yaratılarak, vatandaşlarımızın/sosyal medya kullanıcılarının güvenlik tehdidi oluşturan yapılanma ve örgütlenmelere alet olmamaları, kendi bireysel özgürlük ve güvenliklerinin toplumun özgürlük ve güvenliğinden geçiyor olduğunun bilincinde olmaları çok önemlidir. Demokratik şeffaflık, hem güvenlik birimlerine olan güven düzeyini artıracak ve hem de iyi niyetli vatandaşların bireysel mahremiyetlerinin ihlalinin önüne geçilmesini sağlamış olacaktır. Bunu başarmanın tek yolu, siber alanda uzmanlaşmış ve hatta bilgisayar korsanlarından (hackerlardan) daha nitelikli profesyonellerin yetiştirilmesidir. Ayrıca, bu niteliklere sahip profesyonellere, özgürlük – güvenlik dengesi hakkında özel eğitimler verilerek, vatandaşların bireysel hak ve özgürlük ihlallerinin önüne geçilmesini sağlamak olanaklıdır.

Kitap, Film ve Video Önerileri

Gerbaudo, Paolo (2014) Twitler ve Sokaklar. İstanbul: Agora Kitaplığı.

David Fincher (2010) The Social Network (Film).

Bill Condon (2013) The Fifth Estate (Film).

Tartışma Soruları

1. Sosyal medya istihbaratının kamu güvenliği bakımından sağladığı olanakları ve riskleri belirtiniz. Bu olanakları geliştirme ve riskleri en aza indirme konusunda hangi politikaların geliştirilebileceğini tartışınız.
2. Güvenlik ve gözetim gerilimini açıklayınız. Güvenlik ve gözetim dengesinin nasıl sağlanabileceğini tartışınız.

Çoktan Seçmeli Sorular

1. **Aşağıdakilerden hangisinin sosyal medya istihbaratının kullanım amaçlarından biri olduğu söylenemez?**
   a) Kamu güvenliği için saldırı ve sızmaları önlemek
   b) Kitlelerin hareketlerini önceden tespit etmek
   c) Bireylerin özel hayatlarına müdahale etmek
   d) Terörle mücadele etmek
   e) Suçluları tespit etmek

2. **Aşağıdakilerden hangisi sosyal medya istihbaratının aşamalarından biri değildir?**
   a) Sosyal medyadan bilgi ve kanıt toplama
   b) Verileri analiz etme
   c) Bilgiyi stratejik olarak kullanılabilir hale getirme
   d) Bilgiyi ilgili birimlere güvenli olarak iletme
   e) Karşı-operasyon gerçekleştirme

3. **Aşağıdakilerden hangisinin ulusal güvenlik amacıyla gerçekleştirilen sosyal medya istihbaratının işlevlerinden biri olduğu söylenemez?**
   a) Olay yerinden kitle kaynaklı bilgi almak
   b) Bir sorunun kökenini ve nedenlerini anlamak
   c) Sosyal medya iletişim trafiği üzerinden gelişmekte olan sorunları ve boyutlarını tespit etmek
   d) Gruplara özgü iletişim ortamlarına dahil olarak suçu önlemek
   e) Elde edilen bilgileri kullanarak siyasal rakiplerin önüne geçmek

4. **Aşağıdakilerden hangisi sosyal medyanın yarattığı bir risk değildir?**
   a) Sosyal medyanın terör örgütleri tarafından kullanımı
   b) Sosyal medyanın ayaklanmalarda kullanımı
   c) Sosyal medyanın yabancı devletler tarafından kullanımı
   d) Sosyal medyanın toplumsal taleplerin iletilmesi amacıyla kullanımı
   e) Kamu kurumlarında çalışan kişilerin resmi yazışmalarla ilgili [illegible] sosyal medya üzerinden paylaşmaları

5. **Türkiye'de sosyal medyanın emniyet güçleri tarafından kamu güvenliğini sağlamaya yönelik yapı ve uygulamalarıyla ilgili aşağıdakilerden hangisi söylenemez?**
   a) Siber Suçlarla Mücadele Şube Müdürlükleri bu konuda yetkilidir
   b) Sanal devriyelerce sosyal medya üzerinden yapılan suç içerikli paylaşımlar tespit edilerek işlem başlatılmaktadır
   c) 2013 yılından beri polisin internet takip yetkisi bulunmaktadır
   d) Siber suçlarla mücadelede Sanal Devriye Büro Amirliği suçu önleyici bir birim olarak kurulmuştur
   e) Siber Suçlarla Mücadele Daire Başkanlığı, korku ve panik oluşturarak kamu düzenini bozan paylaşım yapan hesapları tespit etmektedir

Yanıtlar: c, e, e, d, b

KAYNAKÇA

Al-Awsat, Asharq (2019). *From Tahrir to Twitter, Iraqi Protests Rely on Social Media Thursday*, https://aawsat.com/english/home/article/1970376/tahrir-twitter-iraqi-protests-rely-social-media. Erişim Tarihi: 10.03.2020.

Anadolu Ajansı (2020). İdlib'de Türk askerine yönelik provokatif sosyal medya paylaşımlarına soruşturma. https://www.aa.com.tr/tr/turkiye/idlibde-turk-askerine-yonelik-provokatif-sosyal-medya-paylasimlarina-sorusturma/1748549. Erişim Tarihi: 05.03.2020.

Assange, J., Appelbaum, J., Müller-Maguhn, A. ve Zimmermann, J. (2012). *Şifrepunk.* (Çev. Ayşe D. Temiz). İstanbul: Metis Yayınları.

Axford, Barrie (2011). "Talk About a Revolution: Social Media and the MENA Uprisings". *Globalizations, 8*(5), s. 681-686.

Bachrach, J. (2011). "WikiHistory: Did the Leaks Inspire the Arab Spring?" *World Affairs Journal.* http://www.worldaffairsjournal.org/article/wikihistorydid-leaks-inspire-arab-spring. Erişim Tarihi: 14.05.2015.

Baltacı, S. (2017). *Sosyal Medya Üzerinden Elde Edilen İstihbaratın Güvenlik Maksatlı Kullanılması*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İliskiler Anabilim Dalı İstihbarat Bilim

Bayerl, Petra Saskia ve Akhgar, Babak (2015). "Legitimacy of surveillance is crucial to safeguarding validity of OSINT data as a tool for law-enforcement agencies." *Communications of the ACM*, https://doi.org/10.1145/2699410, Erişim Tarihi: 10.03.2020.

Bayraktar, Gonca (2014). "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat". *Güvenlik Stratejileri Dergisi, 10*(20), s. 1-149.

Blunden, B. ve Cheung, V. (2014). *Behold a Pale Farce: Cyberwar, Threat Inflation, and The Malware Industrial Complex*. USA: Trine Day

Chukwuere, Joshua Ebere ve Onyebukwa, Chijioke Francis (2018). "The Impacts of Social Media on National Security: A View from the Northern and South-Eastern Region of Nigeria", *International Review of Management and Marketing 8* (5), s. 50-59.

CNN Turk (2018). *Sanal devriye*. https://www.cnnturk.com/turkiye/sanal-devriye-bu-polislerin-gorevi-7-24-sosyal-medyayi-takip-etmek?page=6. Erişim Tarihi: 11.03.2020.

Cox, Kate, Marcellino, William, Bellasio, Jacopo, Ward, Antonia, Galai, Katerina, Meranto, Arya Sofia, Persi, Paoli- Giacomo (2018). *Social Media in Africa A Double-Edged Sword for Security and Development United Nations Development Programme. (UNDP) Regional Centre for Africa.* https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf. Erişim Tarihi: 10.03.2020.

Crump, Jeremy (2012). "What Are the Police Doing on Twitter? Social Media, the Police and the Public". *Policy&Internet, 3*(4), s. 1-27.

Dozier, Kimberly (2011). *CIA following Twitter, Facebook*, https://www.globalresearch.ca/intelligence-and-social-media-cia-is-monitoring-twitter-and-facebook/27480. Erişim Tarihi: 13.03.2020.

Fisher, Max (2013). *Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?* https://www.washingtonpost.com/news/worldviews/ wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/ Erişim Tarihi: 10.03.2020.

Fuchs, Christian (2013). "Class and Exploitation on the internet." Trebor Scholz (ed.) iç. *Digital Labor* (s.211-224). New York: Routledge

HaberTürk (2019). *Elaziğda sosyal medyada terror propagandasi operasyonu.* https://www.haberturk.com/elazig-haberleri/73732363-elazigda-sosyal-medyada-teror-propagandasi-operasyonu-6-gozalti. Erişim Tarihi: 05.03.2020.

Habertürk (2016). MİT, sosyal paylaşım sitelerine karşı uyardı. https://www.haberturk.com/gundem/haber/1199593-mit-sosyal-paylasim-sitelerine-karsi-uyardi. Erişim Tarihi: 05.03.2020.

HaberTürk (2018). *Facebook skandalı büyüyor.* https://www.haberturk.com/facebook-skandali-buyuyor-trump-in-secilmesinde-onemli-rol-oynadik-1884885. Erişim Tarihi: 15.03.2020

HIMC (2011). *The rules of engagement: A review of the August 2011 disorders.* https://www.justiceinspectorates.gov.uk/hmicfrs/media/a-review-of-the-august-2011-disorders-20111220.pdf, Erişim Tarihi: 28.02.2020.

Hürriyet Gazetesi (2018a). 45 milyon sosyal medya hesabına siber göz. https://www.hurriyet.com.tr/gundem/45-milyon-sosyal-medya-hesabina-siber-goz-40868004, Erişim: 11.03.2020.

Hürriyet Gazetesi (2018b). *FBI ve Samsun Siber polisinin Darknet operasyonu.* https://www.hurriyet.com.tr/gundem/fbi-ve-samsun-siber-polisinin-darknet-operasyonu-1-gozalti-41028003. Erişim: 11.03.2020.

Independent (2020). *Emniyet'ten koronavirüs çalışması.* https://www.independentturkish.com/node/143176/siyaset/emniyetten-koronavirus-alarmı-aym-geçen-ay-polisin-sanal-takip-yetkisini. Erişim Tarihi: 05.03.2020.

Iqt.org (2020). In-Q-Tel. https://www.iqt.org/our-history/ Erişim: 12.03.2020

Kaiman, J. (2014). "Hong Kong's umbrella revolution." *The Guardian briefing.* http://www.theguardian.com/world/2014/sep/30/-sp-hong-kongumbrella-revolution-pro-democracy-protests, Erişim Tarihi: 04.04.2015.

Kimutai, J. K. (2014). *Social Media and National Security Threats: A Case Study of Kenya*. A Research Project Submitted In Partial Fulfilment of The Requirements of The Degree of Master of Arts in International Studies, Institute of Diplomacy and International Studies, University of Nairobi. Kenya.

Kızılkoyun, F. (2018). *45 milyon sosyal medya hesabına siber göz.* https://www.hurriyet.com.tr/gundem/45-milyon-sosyal-medya-hesabina-siber-goz-40868004. Erişim Tarihi: 12.03.2020

Milliyet (2018). *Sosyal medyadan suç içerikli paylaşım...* https://www.milliyet.com.tr/gundem/sosyal-medyadan-suc-icerikli-paylasim-yapan-2-bin-754-kisi-tutuklandi-2797868. Erişim Tarihi: 10.03.2020.

Mittal, Sudip, Das Kumar, Mulwady Prajit, Varish Joshi, Anupam ve Finin, Tim (2016). "CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities", *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (ASONAM), San Francisco, CA, 2016, *ss.* 860-867.

Morozov, E. (2009a). Iran: Downside to the Twitter Revolution. *DISSENT,* http://www.evgenymorozov.com/morozov_twitter_dissent.pdf. Erişim Tarihi: 23.10.2014.

Morozov, E. (2009b). "Think Again: Twitter". *Foreignpolicy.* http://www.foreignpolicy.com/articles/2009/08/06/think_again_twitter Erişim: 23.10.2014.

Murthy, D. (2013). *Twitter: Social Communication in the Twitter Age.* UK: Polity.

Newton (2018). *Facebook's role in the French protests has polarized observers Is this a typical democratic protest, or something darker?* By Casey Newton@CaseyNewton. https://www.theverge.com/2018/12/11/18135273/yellow-vest-facebook-france-protests. Erişim Tarihi: 14.03.2020

NTV (2019). *Sosyal medyada 'kara propaganda'dan 78 kişi hakkında yasal işlem başlatıldı.* https://www.ntv.com.tr/turkiye/sosyal-medyada-kara-propagandadan-78-kisi-hakkinda-yasal-islem-baslatildi,7GKygmGVykeD9cEHBTRNJQ. Erişim Tarihi: 09.03.2020.

NTV (2020). Elazığ depremine yönelik provokatif paylaşım yapan 50 şüpheli hakkında soruşturma. https://www.ntv.com.tr/turkiye/elazig-depremine-yonelik-provokatif-paylasim-yapan-50-supheli-hakkinda-sorusturma,sXvsD_WdJ06wpO62g2yHgw. Erişim: 05.03.2020.

Omand, David (2015). *Designing Digital Freedom A Human Rights Agenda for Internet Governance.* CANADA: Centre for International Governance Innovation and the Roval Institute of International

Omand, Sir David, Jamie Bartlett ve Carl Miller, (2012). "Introducing Social Media Intelligence" (SOCMINT). *Intelligence and National Security, 27*(6), s. 801-823.

O'Reilly, Tim (2012). "What is beb 2.0?" Michael Mandiberg (ed.). İç. *The Social Media Reader* (s. 32-52). New York: New York University Press.

Özçetin, Deniz ve Özçetin, Burak (2015). Polis ve Sosyal Medya: Türkiye'de İl Emniyet Müdürlüklerinin Twitter Kullanımı. *Folklore/Edebiyat, 21 (*83).

Policeforum (2013) https://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/social%20media%20and%20tactical%20considerations%20for%20law%20enforcement%202013.pdf. Erişim: 12/03/2020.

Rahimi, B. (2011). "The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran". *The Communication Review, 14* (3), 158-178.

Resmi Gazete (2018). Olağanüstü Hal Kapsaminda Bazi Düzenlemeler Yapilmasi Hakkinda Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun Kanun No. 7072, Kabul Tarihi: 1/2/2018, 8 Mart 2018 Resmi Gazete.

Rodriguez, Richard Michael (2014). *A Spatial Analysis of Boko Haram and Al-Shabaab References in Social Media in sub-Saharan Africa.* A Thesis Submitted to the Graduate Faculty of George Mason University in Partial Fulfillment of the Requirements for the Degree of Master of Science Geo-informatics and Geospatial Intelligence.

Salik, Hammaad ve Iqbal, Zaheema (2019). *Social media icons Social Media and National Security.* https://thegeopolitics.com/social-media-and-national-security/ Erişim: 09.03.2020

Savaş, Serkan ve Topaloğlu, Nurettin (2015). "Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri", ISC Turkey 2015 - VIII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.

Taşcı, U. ve Can, A. (2015). "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014", *Fırat Üniversitesi Sosyal Bilimler Dergisi, 25*(2) s. 229-248, Elazığ.

The Guadian (2013, Şubat 10). Software that tracks people on social media created by defence firm. https://www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence. Erişim: 09.03.2020

TRT Haber (2019). *2018'de "sanal devriye" ile 6 bin şüpheli gözaltına alındı.* https://www.trthaber.com/haber/turkiye/2018de-sanal-devriye-ile-6-bin-supheli-gozaltina-alindi-409637.html. Erişim: 09.03.2020.

TRT Haber (2013). Sanal devriye. https://www.trthaber.com/haber/gundem/polis-artik-sanal-devriye-de-atacak-95756.html. Erişim: 09.03.2020.

Ünver, H. Akın (2018). "Dijital Açık Kaynaklı İstihabarat ve Uluslararası Güvenlik". *Siber Politikalar ve Dijital Demokrasi 7,* Ekonomi ve Dış Politika Araştırma Merkezi.

Walsh, Patrick F. ve Seumas Miller (2016). "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden", Intelligence and National Security, *31*(3):345-368, DOI: 10.1080/02684527.2014.998436.

Ward, M. (2009). Twitter on the front line. BBC. http://news.bbc.co.uk/2/hi/technology/7979378.stm. Erişim: 14.04.2015.

Willnat, Lars, Lu Wei ve Jason Martin (2015). "Politics and Social Media in China". Gary D. Rawnsley, Ming-yeh T. Rawnsley (ed.) iç. *Routledge Handbook of Chinese Media (s. 1-27).* UK: Routledge.

Yu, Louis, Asur, Sitaram ve Huberman, Bernardo A. (2011). "What Trends in Chinese Social Media", *SSRN Electronic Journal.* DOI: 10.2139/ssrn.1888779.

BÖLÜM 15

SİBER GÜVENLİK ve KAMU POLİTİKALARI

Mustafa AFYONLUOĞLU[1]

BÖLÜM TANITIMI

1969'da ARPANET üzerindeki iki düğüm noktası arasında ilk verinin transferi ile birlikte, daha önceki dönemlerde sesli iletişim dünyasına yapılan yetkisiz erişim girişimlerinin, veri iletişimlerine de yönelmesi, elektronik dünyanın dijital saldırılara karşı korunmasını gündeme getirmiş, özellikle 1983'de ARPANET'e ait TCP/IP iletişim protokollerinin standart olması ile birlikte "internet" adı verilen iletişim ağının tüm dünyaya açılması "bilgi toplumu" adıyla yepyeni bir çağı aralamış ve siber dünyanın başlangıcını oluşturmuştur.

Özellikle 1990'lı yıllarda devletler, sağladıkları hizmetleri elektronik ortamda da sunmaya başlayarak "e-Devlet" adı verilen hizmet sunum şekline geçtiklerinde, artık internet üzerindeki veri akışları verimliliğin ve etkili hizmet sunumunun bir anahtarı olarak vatandaşın ve iş dünyasının hayatına yansımaya başlamış, diğer yandan ortaya çıkan bu dijital dünya saldırılar açısından cazip bir alan olarak görülmeye başlanmıştır. İlerleyen dönemde iletişim imkânlarının artması ve ucuzlaması, bilişim cihazlarına erişimin kolaylaşması, mobil cihazların yaygınlaşması ve son olarak sosyal medya araçlarının hızla gelişmesiyle dijital vatandaşlık kavramı gündeme gelmiştir. Artık teknolojinin bireylerin hayatına okul öncesinden itibaren girmesiyle birlikte siber güvenlik, siber farkındalık, siber zorbalık, dijital ayak izleri, mahremiyet, ekran-zaman yönetimi gibi alanlar tüm toplumu ilgilendiren ve