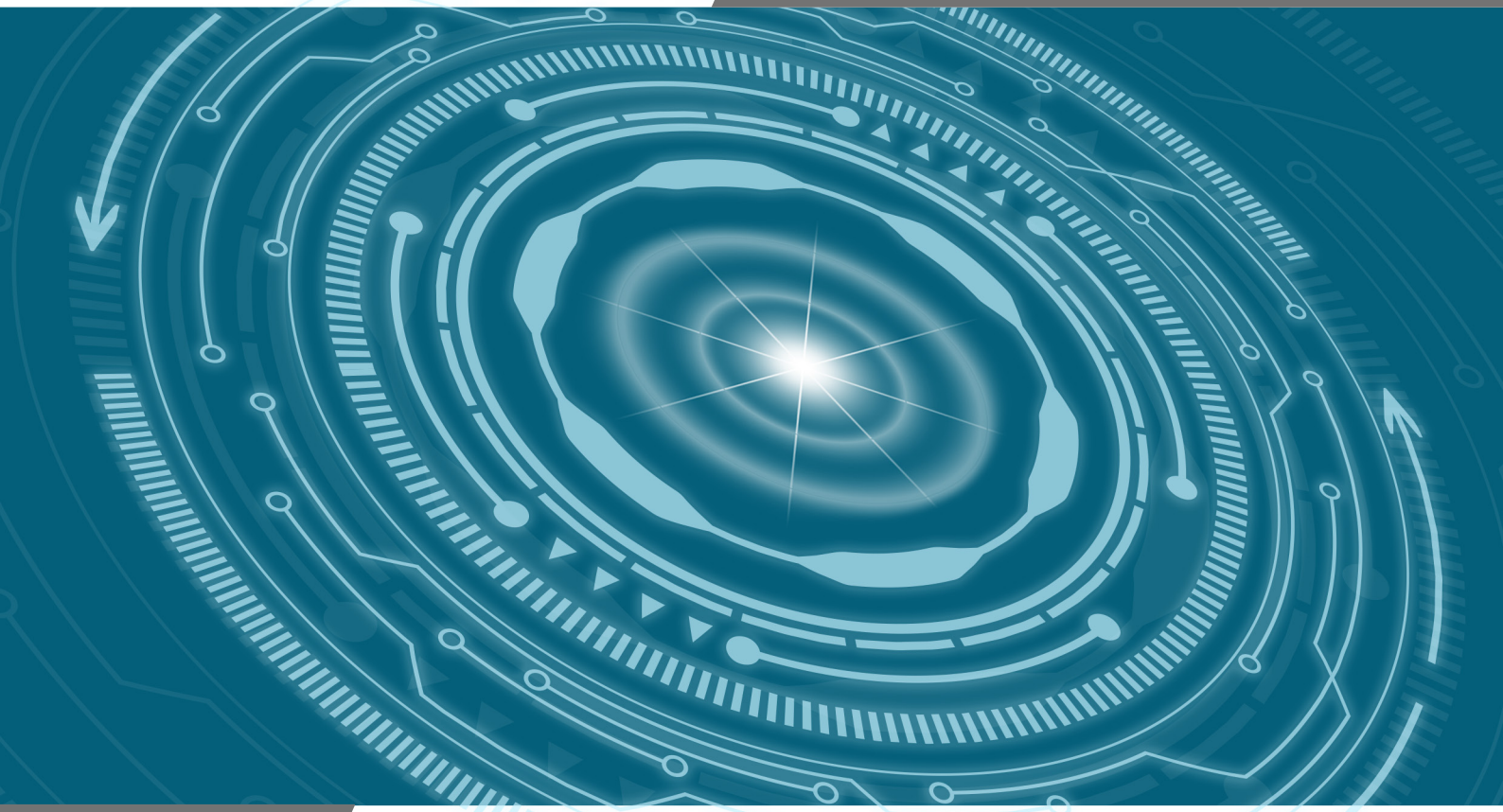
Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

Siber Politikalar ve Dijital Demokrasi 2018/7



Temmuz 2018

# Dijital Açık Kaynaklı İstihbarat ve Uluslararası Güvenlik

**H. Akın Ünver** | EDAM, Oxford CTGA & Kadir Has Üniversitesi

# Dijital Açık Kaynaklı İstihbarat ve Uluslararası Güvenlik

**H. Akın Ünver** | EDAM, Oxford CTGA & Kadir Has Üniversitesi

İstihbarat önemli ve doğası itibariyle sürekli değişken bir idare uygulamasıdır. Bu uygulama tarihsel olarak devletler, tüccarlar ve din adamları ekseninde gelişmiş olsa da, 20. yüzyılın sonları istihbarat ve gözetleme ekipmanlarının özelleştirilmesine ve istihbarat kavramının genişlemesine tanıklık etmiştir. Günümüzde internet, sosyal medya, akıllı telefonlar ve veri bilimi gibi araçlar, acil durumlar ve kriz olaylarıyla ilgili kritik bilgilerin daha fazla açığa çıkmasına ve yayılmasına katkıda bulunmakta, dolayısıyla haberlerin, gizli bilgilerin ve sızıntıların daha hızlı fark edilmesini ve paylaşılmasını sağlamaktadır. Genel olarak, istihbarat, kritik bilgilerin güvenlik ya da avantaj sağlama amaçlarıyla ve metodik bir şekilde toplanması ve analiz edilmesi pratiğidir. Casusluk ya da örtülü operasyonlar ile eş anlamlı olarak kullanılmasına karşın, istihbarat çoğunlukla, çalma yoluyla bu tür bilgileri elde etmek için gizli yöntemler kullanmak yerine, mevcut ve erişilebilir bilgilerinin sistemli bir şekilde toplanması, işlenmesi ve analizine odaklanır. Daha fazla ve daha iyi bilginin toplanmasına yönelik bu eğilim milli güvenlik tarihinin en temel parçası olmuştur. Bu durum, Sun Tzu'nun 'Savaş Sanatı' adlı eserinin, sıkça atıfta bulunulan 'Casusların Kullanımı' başlıklı bölümünden itibaren müteakip siyasetnamelerde açıkça kanıtlanmaktadır: '*Dolayısıyla, bilge egemen ve iyi generalin taarruz etmesini, fetih yapmasını ve sıradan insanların erişemeyeceği başarılar kazanmasını sağlayan* şey *sahip olduğu ön bilgidir*.'[1]

Geleneksel istihbarat anlayışı, yüksek değerli bilgilerin karar vericilere karşılaştırmalı üstünlük sağlayan bir şekilde yöntemli olarak toplanmasına dayanmaktadır.[2] Bu bilgiler yabancı bir ülkenin imkan ve kabiliyetleri, genel küresel olaylar ya da bir ülkenin iç işleri ile ilgili olabilmektedir. Çoğunlukla istihbaratı askeri ya da güvenlik meselelerine indirgeme eğilimi gösterilse de, bu, istihbaratın ticaret, finans, kültür ve eğitim konularında değerini görmezden gelen çok dar bir tanımlamadır. Söz konusu alanlardaki faaliyetler barış zamanlarında uzun vadeli avantajlar elde edilmesini sağlamaktadır. Bu geleneksel istihbarat tanımı, geçersiz hale gelmemiş olsa da, teknolojik ilerlemeler ve daha da önemlisi yeni teknolojilerin daha geniş kitleler için erişilebilir hale gelmesiyle birlikte genişletilmiştir.[3] Tarih boyunca, istihbarat yetkinliği, hem teknoloji hem de insan davranışlarının modellenmesi ile ilgili ustalaşmayı gerekli kılmış, sonuçta her iki alan da istihbaratı diğer alanlardaki faaliyetler için (askeri, politik, ekonomik) bir kuvvet çarpanı haline getirmiştir. Hatalı olarak hesaplanmış kararların azalmasına olanak sağlayan geleneksel işlevlerine ek olarak, modern istihbaratın hedef kitlesi devletlerin ve ticari şirket liderlerinin ötesinde kamuyu kapsayacak şekilde genişlemektedir. İstihbarat artık yalnızca bir uyarı mekanizması değil, aynı zamanda beklenmedik kriz zamanlarında sorunların çözümüne yarayacak bir teknik bilgi birikimi ve doğaçlama önlemler havuzudur.[4]

1 Sun Tzu, The Art Of War (Sterling Publishers Pvt. Ltd, 2005), 92.

2 Loch K. Johnson (ed.), The Oxford Handbook of National Security Intelligence (Oxford University Press, 2010), 4.

3 Johnson, 229.

4 Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds., Routledge Companion to Intelligence Studies (Routledge, 2013), 51.

İstihbarat çalışmaları, diplomasi, güvenlik ve siyaset konularında en heyecan verici araştırma alanlarından biri olmasına karşın, istihbaratın gizlilik içeren doğası nedeniyle metodik çalışılması hep zor olmuştur. Her ne kadar yöntemsel bilgi toplama en önemli güvenlik alanlarından olmuş olsa da, bu alan, gizliliği gereği bilimsel ve akademik titizlikten yoksun kalmıştır.[5] Bu, çoğunlukla tarihsel istihbarat kayıtlarına ya da dar bir istihbarat topluluğunun ötesinde veriye erişimin mümkün olmamasından kaynaklanmıştır. Ancak, Soğuk Savaş'ın sonlarına doğru, özellikle Amerika Birleşik Devletleri başta olmak üzere bu arşivler sivil akademik çalışmaların kullanımına açılmaya başlanmıştır. Bu, büyük ölçüde 1980'lerde ABD ve Birleşik Krallık'taki İkinci Dünya Savaşı istihbarat dosyalarının gizliliğinin kaldırılmasına bağlı olarak gerçekleşmiştir. Söz konusu belgelerin en önemlileri Stratejik Hizmetler Dairesi'ne (OSS) ve İngiliz sinyal istihbaratına ait dökümanlardır.[6] Önceleri yalnızca gizliliği kaldırılmış dökümanlardan oluşan küçük bir koleksiyon ile çalışabilen istihbarat konusunda uzmanlaşmış sivil bilim adamları, 1990'larla birlikte üzerinde çalışabilecekleri çok daha geniş bir veri havuzuna sahip olmuştur. Söz konusu veri erişimi ile birlikte, milli güvenlikte istihbaratın değişen işlevi ve değişen teknolojiler ile haberleşme yöntemlerine nasıl adapte olabileceği ile ilgili ilk teoriler ortaya çıkmıştır.

Genel olarak, istihbarat dört ana süreci içermektedir. Söz konusu süreçlerin ilki olan toplama, bir devletin güvenliği ve/veya göreceli siyasa üstünlüğü ile ilgili anlamlı ve yüksek değerli bilgiye erişim, bu bilgiyi sınıflandırma ve toplama kapasitesidir. Tarihsel olarak istihbarat toplama kapasitesi geniş bir insani ve fiziksel erişim ağını gerektirmiş olsa da, 20. Yüzyıl ile birlikte teknolojik kapasite ile haberleşme ve bilişim alanlarındaki teknik ilerlemere sürekli şekilde adaptasyonu da ağırlıklı olarak içermeye başlamıştır. İkinci ana süreç olan iletim (transmission), hedeflenen sahadan istihbarat merkezine ve oradan iç güvenlik kurumlarına güvenilir kritik bilgi akış kanallarının oluşturulmasını ve çeşitlendirilmesini içermektedir. İstihbarat iletimi, gerek sahadan kuruma bilginin çıkarım ve teslim zincirini oluşturan bir yüksek derecede kalifiye ve güvenilir insan ağına, gerekse dijital istihbaratın hızla teslim edilmesini sağlayan dijital iletim yapılarına ihtiyaç duymaktadır. Dijital veri -görsel, ses, metin – ile ilgilenen istihbarat türlerinde iletim, söz konusu verinin güvenli şekilde depolanması ve gönderilmesi amacıyla, yüksek düzeyli kriptolama ve kripto çözme uygulamalarını gerektirmektedir. Üçüncü ana süreç olan farkındalık yaratma, istihbarat zümresi tarafından karar alıcıların ihtiyaçlarının ve karar alıcılar tarafından önemli karar alanları ile ilgili istihbaratın değerinin anlaşılmasını içermektedir. İstihbarat zümresi ile karar alıcılarının önceliklerinin eşleşmediği ya da siyasi liderliğin istihbarat zümresine güvenmediği teşkilat kültürlerinde farkındalık bileşeni tehlikeye atılmakta, bu durum kriz senaryolarında kilit öneme sahip istihbaratın etkin bir şekilde işlenmesini ve iletilmesini engellemektedir. Son olarak, istihbarat kuruluşlarının, rakiplerini yanlış ve eksik bilgiye yönlendirmelerini sağlayan 'seçici yanıltma' kabiliyetlerine sahip olması gerekmektedir. Bu yetenek istihbarat rakiplerinin dikkatinin kaynak ve zaman harcatacak şekilde dağıtılması ile söz konusu aktörlere karşı göreceli üstünlük sağlanması bakımından gereklidir.[7]

Ülkelerin farklı tehdit algılamalarına ve bilgi arayışı ile gizlilik işleyişi konularında değişken dinamiklere sahip olması sebebiyle, istihbarat kültürler arasında çeşitlilik göstermektedir. Bu nedenle, istihbarat monolitik ve standart bir uygulama olarak düşünülmemelidir. Daha ziyade, karar alma üstünlüğünün elde edilmesinde çok sayıda bilgi toplama mekanizmasının kullanılmasına bağlı olarak siyasi ve kültürel koşullara bağlı farklı yollar bulunmaktadır. İstihbarat kültürünün başlıca etkenlerinden birini rejim tipi oluşturmakta,[8] demokrasiler, yarı-demokrasiler ve otoriter hükümetler bilgiyi farklı bürokratik, yasal ve yasama gözetimi mekanizmaları ile işlemekte ve yönetmektedir.[9] Ayrıca, demokratik istihbarat servisleri otoriter devletler ile karşılaştırıldığında daha fazla özerkliğe sahip olma eğilimi göstermekte, ve yine daha fazla liyakata dayalı işe alım ve terfi sistemlerini işletebilmektedir. Bu durum sözü edilen istihbarat servislerinin çok sayıda tehdit karşısında daha meşru bir zeminde daha çeşitli yetenekler ile hareket etmesine olanak tanımaktadır. Güçlü gözetim mekanizmaları ayrıca yolsuzluğu, kaynak israfını ve kötü yönetimi minimize edebilmekte, dolayısıyla demokratik olarak kontrol edilen istihbarat kuruluşlarının ülke içindeki siyasi

5 Dover, Goodman, and Hillebrand, 71.

6 Dover, Goodman, and Hillebrand, 88.

7 Dover, Goodman, and Hillebrand, 71–83; Johnson, The Oxford Handbook of National Security Intelligence, 113–19.

8 Montgomery McFate, "The Military Utility of Understanding Adversary Culture" (Arlington, VA: DTIC, Office of Naval Research, Ocak 2005), http://www.dtic.mil/docs/citations/ADA479862.

9 Philip H. J. Davies, "Intelligence Culture and Intelligence Failure in Britain and the United States," Cambridge Review of International Affairs 17, no. 3 (Ekim 1, 2004): 495–520, https://doi.org/10.1080/0955757042000298188.

meşruluğunun artmasına izin vermektedir.[10] Dahası, otoriter devletler iç ve dış tehditleri abartılı bir şekilde gösterme eğilimi göstermekte ve savurgan istihbarat servislerini birden fazla ve belirsiz bilgi cephelerine etkisiz bir şekilde yayılmaya zorlamaktadır. Bir başka belirleyici etken kurumsal tarih ve kültürdür.[11] Post-emperyal (daha önce bir imparatorluğun merkezini oluşturmuş) devletler ile diğerleri arasında istihbarat uygulamaları ve bölgesel farkındalık bakımından belirgin farklılıklar bulunmaktadır. Daha uzun süreli istihbarat geleneklerinin varisi olan söz konusu post-emperyal devletler, genellikle önceki emperyal sınırları içinde yer alan devletleri içerecek şekilde daha geniş bölgelerde operasyon yürütme eğilimi göstermektedir.[12] Son olarak, devam eden çatışmalara olan yakınlık çok önemli bir faktördür. Çatışan ya da aktif olarak devam etmekte olan bir iç çatışmaya komşu olan devletler diğerlerine göre daha farklı bir kurumsal kültür ile faaliyet göstermektedir. Örgütsel ve bürokratik istihbarat modellerinin büyük çoğunluğu ülkenin aktif ya da donuk çatışmalara olan angajmanı ve/veya dış barış harekatlarında yer almasına bağlı olarak değişiklik göstermektedir.

## İstihbarat disiplinleri kabaca altı öncelikli ekole ayrılmaktadır:

HUMINT (insan istihbaratı): En eski (ve 19. yüzyıl sonlarına kadar tek) istihbarat ekolü olarak HUMINT tarihsel olarak istihbaratın büyük kısmını oluşturmuştur. Kabaca, HUMINT, politik, askeri, ekonomik veya kültürel öneme sahip bireyler arasındaki sözlü ve sözsüz iletişimsel ilişkilere, ağlara ve etkileşimlere dayanır. Psikoloji, kognitif bilim, sosyoloji, antropoloji ve beşeri bilimler, HUMINT topluluğunun yabancı ülkelerdeki kritik güvenlik olaylarını ve süreçlerini anlamak için kullandığı araçlardan bazılarıdır. Yalnızca büyükelçiler, askeri ateşeler ya da devlet görevlileri değil, aynı zamanda tüccarlar, turistler ve öğrenciler de tarih boyunca insan istihbaratının kültürel ve ulusal alışveriş noktaları olarak hizmet etmiştir. Ayrıca, HUMINT hiçbir şekilde devletlerin tekelinde değildir. Özel şirketler, bankalar, araştırma laboratuvarları ve teknoloji firmaları da rakiplerine karşı finansal ya da bilimsel/teknik üstünlük sağlama amacıyla düzenli insan istihbaratı operasyonları gerçekleştirmektedir.[13]

GEOINT (geospatial intelligence) (coğrafi-konum istihbaratı): Coğrafya'nın farklı yönleri (hava, arazi, su yolları) her zaman istihbarat analizinin önemli değişkenleri olmuş olsalar da, GEOINT özellikle uydular, insansız hava araçları (İHA), ışık tespiti ve ölçümü (LIDAR) ve gözetleme uçakları tarafından sağlanan gerçek zamanlı (ya da yaklaşık olarak) havadan görüntülerin ortaya çıkmasından yararlanmıştır. GEOINT, seçilmiş bir coğrafi alandaki insan faaliyetlerinin ve de kaynakların ve yer altı koşullarının takip edilmesi ve izlenmesine yönelik sabit ya da zaman-frekans görüntü analizi sağlamaktadır. Her ne kadar coğrafi-konum verisi daha önce MASINT ve SIGINT alanlarının kesiştiği bir husus olsa da, özel coğrafi-konumsal araçların kullanılabilirliği Amerika Birleşik Devletleri'nde bulunan National Geospatial Agency (NGA) adlı istihbarat teşkilatının kurulmasını sağlamıştır. Günümüzde, Planet Labs, Terra Bella, BlackSky Global, Orthecast ya da XpressSAR gibi firmalar tarafından sağlanan ticari olarak erişilebilir yüksek çözünürlüklü görüntüler şirketlerin, yardım kuruluşlarının ve bir takım devlet dışı aktörlerin GEOINT imkan ve kabiliyetlerini elde etmesini sağlanmıştır.[14]

MASINT (ölçüm ve akustik istihbaratı): Akustik, radyo frekansı, radyasyon, kimyasal / biyolojik, spektroskopik ve kızıl ötesi imzayı ölçmek için çok çeşitli yüksek teknolojili algılama araçları için bir şemsiye terim olan MASINT, metrik, açısal, uzamsal ve modüler verinin uzaktan algılama yöntemleri ile toplanmasına odaklanmaktadır. 1991 yılından önce, MASINT sistemlerinin çoğu, insan destekli otomatik algılamaya yardımcı olmak için gömülü şablonlar ve akustik kitaplıkları içermiştir. Günümüzde, yapay zeka, makine öğ-

10 Mikael Wigell, "Mapping 'Hybrid Regimes': Regime Types and Concepts in Comparative Politics," Democratization 15, no. 2 (Nisan 1, 2008): 230–50, https://doi.org/10.1080/13510340701846319.

11 Jessica L. Weeks, "Autocratic Audience Costs: Regime Type and Signaling Resolve," International Organization 62, no. 1 (Ocak 2008): 35–64, https://doi.org/10.1017/S0020818308080028.

12 Jeffrey W. Legro, "Culture and Preferences in the International Cooperation Two-Step," American Political Science Review 90, no. 1 (Mart 1996): 118–37, https://doi.org/10.2307/2082802.

13 Jacqueline R. Evans et al., "Criminal versus HUMINT Interrogations: The Importance of Psychological Science to Improving Interrogative Practice," The Journal of Psychiatry & Law 38, no. 1–2 (Mart 1, 2010): 215–49, https://doi.org/10.1177/009318531003800110; Montgomery McFate and Steve Fondacaro, "Cultural Knowledge and Common Sense," Anthropology Today 24, no. 1 (Şubat 1, 2008): 27–27, https://doi.org/10.1111/j.1467-8322.2008.00562.x.

14 Todd S. Bacastow and Dennis Bellafiore, "Redefining Geospatial Intelligence," American Intelligence Journal 27, no. 1 (2009): 38–40; Andy Sanchez, "Leveraging Geospatial Intelligence (GEOINT) in Mission Command" (Arlington, VA: DTIC, Office of Naval Research, Mart 21, 2009), http://www.dtic.mil/docs/citations/ADA506270.

renimi ve büyük akustik tespiti veri kütüphanelerinin yardımıyla, çoğu MASINT sistemi, bir insan operatörünün yardımı olmadan otonom gözetim yapmak üzere geliştirilmiştir. Bugün, MASINT, füzeler, uçaklar veya insansız hava araçlarının tespitinden, afet yardımı, mülteci yardımının izlenmesi ve doğal kaynak - endüstriyel çıktı ölçümlerine kadar çok çeşitli bilgi ortamlarında kullanılabilmektedir.[15]

FININT (finansal istihbarat): Finansal istihbarat, 'parayı takip et' şeklinde ifade edilen mottosuyla, finansal işlemlerin düşman imkan ve kabiliyetlerinin, niyetlerinin ve ağlarının anlaşılması amacı ile takip edilmesi disiplinidir. Terör finansmanı, vergi kaçakçılığı, kara para aklama ya da yasadışı silah ticareti konularına odaklanan finansal istihbarat, öncelikli olarak düşman aktörlerin operasyonlarını ve mevcudatlarını nasıl finanse ettiğinin anlaşılması ve bu süreçlerde yer alan aracı kurum ve/veya kişilerin haritasının çıkartılması ile ilgilenmektedir. FININT, istihbarat disiplininin en çok çeşitlilik gösteren ekollerinden biri olarak birden fazla devlet organına hizmet etmekte ve yalnızca güvenlik ya da kriz zamanı karar alma konularına bağlı kalmamaktadır. Kısıtlı zaman ya da bilgi ile tepki verilmesi gerekli olmayan ve açık kaynaklar ile erişilebilen ekonomik büyüme, sanayi üretimi, mali politikalar ve ekonometrik veriler gibi uzun vadeli trendler finansal istihbaratın yetki ve faaliyet alanı içindedir.[16]

SIGINT (sinyal istihbaratı): Duman, güvercinler, ışık ya da semafor sinyalleri tarihte uzun zaman boyunca kullanılmış haberleşme araçları olsa da, sinyal istihbaratının ortaya çıkması temel olarak telgrafın keşfine dayanmaktadır. Özel bir istihbarat disiplini olarak geçmişi 1850'li yıllara dayanan SIGINT, öncelikli olarak düşmanın mesafeli mesaj iletimlerinin yakalanması ve işlenmesi, ve de dost muhaberelerinin rakipler tarafından yakalanmasını önleme amacı ile kriptolanması ile ilgilenmektedir. Bu faaliyetler düşman elektronik haberleşmesinin dinlenmesi amacı ile iletişim ağlarına ve sinyal iletim kanallarına gizli olarak bağlanılmasını ve mesajların kriptolanması ile kripto çözümünü içeren uygulamaları içermektedir. Haberleşme teknolojilerinin 20. yüzyıl boyunca çok hızlı bir şekilde gelişmesi ile birlikte, sinyal istihbaratı TECHINT (teknik istihbarat), CYBINT (siber istihbarat) ve DNINT (dijital ağ istihbaratı) uygulamalarını içerecek şekilde genişlemiştir. Günümüzde, çok geniş internet ortamına yayılmış bilgi, sosyal medya platformları ve bilgi ve iletişim teknolojileri (BİT) sinyal istihbaratının yetki alanı içindedir. Söz konusu disiplin aynı zamanda botları, trolleri ve yalan haberleri de içeren modern internet tabanlı bilgi harbinin ön saflarındadır.[17]

OSINT (açık kaynaklı istihbarat): Bir istihbarat teşkilatının kapasitesi, öncelikli olarak, kritik bilgiyi ne kadar iyi tespit edip aktarabildiği ile ölçülse de, neyin önemli olduğunu anlama ve bağlamsallaştırma becerisi, açıkta ve kolayca erişilebilir olan hususlar ile ilgili bilgi sahibi olmayı gerektirmektedir. Önemli ve gereksiz bilgileri birbirinden ayırmak için bir istihbarat kuruluşunun öncelikle kendi "bilgi ortamı" için temel teşkil eden faaliyetleri gerçekleştirmesi gerekmektedir. Bu da, "kamusal alanda yasal olarak mevcut olan" ya da "açık alanda gizlenmiş" olan bilgiyi geliştirmek ve toplamak için kurumsal ve örgütsel beceriler geliştirerek yapılabilmektedir. Tarihsel olarak OSINT haber ve bilgi ajansları, kültürel ve diplomatik değişimler ve sosyalleşme ile icra edilmiş olmasına rağmen, giderek daha fazla internet ve BİT tabanlı teknolojik gelişmelere dayalı olarak uygulanmaktadır. Dolayısıyla klasik OSINT ve dijital OSINT farklı olarak ele alınmalıdır.[18]

---

15 Jeffrey T. Richelson, "MASINT: The New Kid in Town," International Journal of Intelligence and CounterIntelligence 14, no. 2 (Nisan 1, 2001): 149–92, https://doi.org/10.1080/088506001300063136; J. Dudczyk, J. Matuszewski, and M. Wnuk, "Applying the Radiated Emission to the Specific Emitter Identification," in 15th International Conference on Microwaves, Radar and Wireless Communications (IEEE Cat. No.04EX824), vol. 2, 2004, 431–434 Vol.2, https://doi.org/10.1109/MIKON.2004.1357058.

16 Donato Masciandaro, "Financial Supervisory Unification and Financial Intelligence Units," Journal of Money Laundering Control 8, no. 4 (Ekim 1, 2005): 354–70, https://doi.org/10.1108/13685200510620858; John Frank Thony, "Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units," European Journal of Crime, Criminal Law and Criminal Justice 4 (1996): 257.

17 Matthew M. Aid, "All Glory Is Fleeting: Sigint and the Fight Against International Terrorism," Intelligence and National Security 18, no. 4 (Aralık 1, 2003): 72–120, https://doi.org/10.1080/02684520310001688880; Martin Rudner, "Britain Betwixt and Between: Uk SIGINT Alliance Strategy's Transatlantic and European Connections," Intelligence and National Security 19, no. 4 (Aralık 1, 2004): 571–609, https://doi.org/10.1080/0268452042000327528.

18 Michael Glassman and Min Ju Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," Computers in Human Behavior 28, no. 2 (Mart 1, 2012): 673–82, https://doi.org/10.1016/j.chb.2011.11.014; Robert W. Pringle, "The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989," International Journal of Intelligence and CounterIntelligence 16, no. 2 (Nisan 1, 2003): 280–89, https://doi.org/10.1080/08850600390198706.

# Dijital OSINT

1953-61 tarihleri arasında ABD Merkez Haber Alma Dairesi (DCI) başkanlığı yapan Allen Dulles tarafından ifade edildiği şekliyle, '*bu açık, normal ve hilesiz araçlar ile elde edilebilen istihbaratın yerinde bir analizi, tahmin ediyorum ki, ulusal siyasamızın yönlendirilmesi için gerekli olan bilginin yüzde 80'inden fazlasını karşılayabilir*'.[19] Dulles tarafından ayrıca vurgulandığı üzere, '*cazibesi ve gizemi nedeniyle, gizli istihbarat olarak adlandırılan faaliyetler gereksiz yere* aşırı şekilde vurgulanmakta',[20] öte yandan istihbaratın toplanması ve işlenmesi çoğunlukla belli diplomatik münasebetler, kişisel ilişkiler, radyo, basın ve bir ülkenin yurtdışında yaşayan diyasporası gibi 'normal yöntemler' aracılığıyla yapılmaktadır. Aynı yüzde 80 kuralı NATO 2002 ve Hulnick 2004'te de belirtilmiş, ancak EUROPOL (Avrupa Birliği Polis Teşkilatı), Birleşik Krallık, İsveç ve Hollanda bakanlıkları ve DIA (Savunma İstihbarat Teşkilatı) için OSINT tüm istihbarat faaliyetlerinin 'en az yüzde 90'ını' oluşturmaktadır.[21] Belirtilen husus, istihbarat faaliyetlerinin çok büyük bir çoğunluğunun, popülerleşmiş ve esrarengizleştirilmiş espiyonaj ve casusluk uygulamaları ile değil, açık kaynakların toplanması ve diğer uygulamalar ile ortaya çıkarılamayan bağlantıların ve nüansların bulunması hususlarına odaklandığı anlamına gelmektedir.

OSINT bir teşkilatın daha geniş alandaki işlevlerinin uygunluğunu ve altyapısını belirlemektedir. Bu nedenle, OSINT uygulamalarının etkili bir şekilde sevk ve idare edilmesi bir istihbarat servisine iki kilit üstünlük sağlamaktadır. Birinci husus olan genel bağlam, stratejik göreliliği belirleyen olaylar, aktörler ve rollerin spektrumu (yani, devam eden olaylarla ilgili olarak bir ülkenin çıkarlarının nasıl tanımlanacağı) ve bunları başarmak için hangi unsurların konuşlandırılacağı ile ilgilidir. Küresel olaylar, süreçler ve önemli aktörlerin açık çıkarları arasındaki nedensel mekanizmalar hakkında bir anlayışa sahip olmayan servisler, sorunları ulusların sınırlarına ulaşmadan önce durdurma veya yönetme becerisine sahip olmadan, ancak tepkisel olarak ele alabilmektedir. Daha da kötüsü bu tepkisellik söz konusu problemler ancak sınırı geçtikten sonra gerçekleşebilmektedir.[22] İkinci olarak, OSINT, bir servise ne tür bilgilerin erişilebilir olduğunun ve hangi bilgilerin bulunmasına odaklanılması gerektiğinin isabetli bir şekilde anlaşılmasını sağlayarak, diğer istihbarat fonksiyonlarını verimli hale getirmektedir. Bu şekilde, istihbarat servisleri diğer işlevleri (özellikle espiyonaj ve bilgi hırsızlığı gibi daha agresif bilgi çıkarım mekanizmalarını) daha tutumlu bir şekilde kullanarak yanlış hesaplama ve diğer ülkelerle yaşanabilecek olası gerilimleri ile ilgili riskleri azaltmaktadır. OSINT ayrıca tahmine dayalı uygulamaları elimine ederek diğer istihbarat işlevlerinin maliyetini azaltmaktadır.[23]

OSINT, iletişim ve şifreleme teknolojilerindeki ilerlemeler ile nüfuz ve etkileri bakımından daha da önemli hale gelmiştir. Alfabenin ve diplomatik yazının icadı, mühürler ve şifreleme mekanizmalarına, yazılı basına, resmi görevlendirme ve moden bürokrasiye, telgrafa, kod yapıcılar ve kod kırıcılara, radyoya, sinyal kesicilere (SIGINT), bilgisayarlara, yüksek hacimli kriptolamaya ve kripto çözümüne olan ihtiyacı ortaya çıkarmıştır. İnternetin, dijital birbirine bağlantılılığın ve sosyal medya platformlarının yaygınlaşması, OSINT'in artan önemine ve diğer istihbarat ekolleri arasında birbiriyle çakışan alanların ortaya çıkmasına yol açmış, aynı zamanda içerik ve haberlerle ilgili doğrulama sorunlarına sebep olmuştur. Bilgide ve veride yaşanan patlama OSINT alanında hem kolaylıklara hem de zorluklara neden olmuştur. Belirtilen kolaylıklar iletişim kanallarının genişlemesinden, zorluklar ise değersiz ve yanıltıcı bilginin benzer şekilde yaygınlaşmasından kaynaklanmaktadır. Bu durum OSINT vazifelerinin salt dijital verinin toplanması ve işlenmesi değil, aynı zamanda doğrulama ve kaynağın tespiti ile ilgili mekanizmaların geliştirilmesi ve hangi içeriğin değersiz olup olmadığının anlaşılması olarak tanımlanmasına yol açmaktadır. İstihbarat servisleri, hangi dijital bilgi veya veri türünün önemli olduğunu bilmek ve internet ile sürekli değişen dağıtma ve depolama modellerini kavramak için teknik altyapıya ve yüksek kaliteli insan gücüne (veya bu işlevlerin tümünün dış kaynaklarından sağlanabilmesi için gerekli yeteneklere) ihtiyaç duymaktadır. Bu amaçla, birçok dijital OSINT servisi internet çalışmaları birimleri oluşturmaya başlamıştır.[24] Ayrıca, istihbarat servisleri tarihsel olarak yaptıları gibi yalnızca kendi aralarında de-

[19] Dover, Goodman, and Hillebrand, Routledge Companion to Intelligence Studies, 125.

[20] Dover, Goodman, and Hillebrand, 125.

[21] Johnson, The Oxford Handbook of National Security Intelligence, 221.

[22] Johnson, 45.

[23] Dover, Goodman, and Hillebrand, Routledge Companion to Intelligence Studies, 14.

[24] Edward J. Appel, Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence, Second Edition (CRC Press, 2014), 157.

ğil, internet kaynaklarının demokratikleşmesi ve geniş kitleler tarafından büyük oranlarda erişilebilir hale gelmesine bağlı olarak, sivil analistler ve özel OSINT şirketleri ile de rekabet etmek zorundadır. Söz konusu iki yeni istihbarat aktörü – sivil vatandaşlar ve özel analistler – resmi istihbarat teşkilatlarının ağır bürokratik yükleri ile bağlantısız olduklarından değişen teknik durumlara hızlı adapte olup, toplama, depolama ve analiz işlevlerini kendi inisiyatifleri ile gerçekleştirebilmektedir. Aynı faaliyetleri yürütebilmek için resmi servisler hukuki meşruluğa ve resmi otoriteye ihtiyaç duymaktadır. Terörle mücadeleden siber güvenliğe ve kitle imha silahlarının izlenmesinden protesto eylemlerinin analizine, teknoloji şirketleri ve siviller birçok resmi OSINT servisi ile aynı veri ve bilgi türlerini kullanmaktadır. Devlet dışı analistler devletler kadar finansan kaynaklara sahip olmasa da, söz konusu açığı otonomluk, hız ve doğaçlama yetenekleri ile kapatabilmektedir.

Sözü edilen genişlemeye eklenen bir başka popülerleşmiş değişken ise büyük veridir (big data). Sıkça vurgulanan 'büyük veri devrimi' sonucunda iki esas yenilik ortaya çıkmaktadır. İlk olarak, veri depolama ve iletim teknolojileri, 3G/4G veri ağlarına erişilebilirlik, Wi-Fi erişimi ve bulut teknolojilerinin yaygınlaşması sonucunda günümüzde eşi görülmemiş hacimlerdeki bilginin üretimi, depolanması ve paylaşımı yapılabilmektedir. Bu durum hem belirli bir veri biriminin (bit) üretiminin, depolanmasının ve iletiminin giderek ucuzlaşmasına, hem de yüksek seviyede granüllü sosyal verinin (özellikle kişisel) üretilmesine ve toplanmasına imkan vermektedir. Neticede, sosyal ve kişisel veri çok amaçlı kullanılabilir hale gelmiştir. Örneğin, vergi ve çalışma verileri satın alma davranışının, sağlık alanındaki seçeneklerin, konaklama seçimlerinin ve seçmen davranışının profilinin çıkarılması için kullanılabilmektedir.[25] Bu çok amaçlı sosyal ve kişisel veriler, Facebook arkadaşları, beğenileri, Twitter retweetleri, Instagram paylaşımları, coğrafi konumlu fotoğraf yüklemeleri ve Snapchat videoları şeklinde kendini gösteren dijital davranış aracılığı ile daha da granüllü hale gelmektedir. Belirtilen durum, hem resmi hem de özel OSINT analistlerinin, bugüne kadarki en geniş, sürekli olarak büyüyen, son derece detaylı ve milyonlarca insana ait davranışsal bilgilerden oluşan veri havuzuna ulaşmasını sağlamaktadır. Son olarak, fitness saatlerinden ev içi akıllı uygulamalara kadar 'nesnelerin interneti' (internet of things, IOT) veri türlerinin yaygınlaşması ile ilintili olarak, sözü edilen bugüne kadar ki en geniş sosyal ve kişisel bilgi havuzu devasa hale gelmekte, aynı zamanda ulusların yüksek çözünülürlüklü profillerinin çıkarılmasını olanaklı hale getirecek kadar detaylı olmaktadır.[26] Bir hasım ülkedeki toplumda kamusal moral, siyasi eğilimler, seçmen davranışı ve toplumsal kuvvetler üzerine çalışan herhangi bir analist için – devlet ya da özel – verinin böylesine yaygınlaşması istihbarat kapasitesi bakımından tarihi öneme sahip bir dönüm noktasıdır. Öte yandan, bütün devletler sözü edilen veriyi etkin bir şekilde edinememektedir. Sözü edilen türde verilerin anlamlı bir şekilde değerli istihbarata dönüştürülebilmesi için bir analistin bilgisayar biliminden veri bilime çeşitli yeteneklere sahip olması gerekmekte, bu noktada devletler genellikle gelişmeleri yakalama konusunda başarısız olmaktadır.

Resmi istihbarat servislerinin birçok sorunundan ilki yeteneğin cezbedilmesi konusudur. Facebook, Google, Amazon ve diğer teknoloji şirketlerinin büyük oranda daha özgür iş ortamlarını, az miktarda hiyerarşi ve daha iyi ücretleri sağlaması ile birlikte, yüksek derecede kalifiye veri analistlerinin büyük kısmı resmi servislere olan ilgisi azalmaktadır.[27] Bu durum devletlerden özel şirketlere kadar dijital istihbarat kuvvetinde siklet merkezinin değişmesine neden olmaktadır. İkinci sorun devletlerin büyük ölçüde bürokratik yapıları için sorunlu olan altyapı geliştirilmesi, uyum sağlama ve iyileştirme hususlarından oluşmaktadır. Yeni donanımlar her zaman maliyetli olmakta, teknoloji dönüşümü (eski ekipmanların düşük maliyet ile yenilenmesi) ya da iyileştirme-modernizasyon süreçleri daha az niceliğe sahip ve daha atik karar alma sistemlerini gerekli kılmaktadır. Teknolojinin iş modelinin bizatihi kendisi devletlerin teknoloji şirketlerinin arkasında kalmasına ve bu şirketlere bağımlı hale gelmesine yol açmaktadır.[28] Üçüncü olarak, OSINT faaliyetlerindeki artan sivilleşme, dijital aktivizmin devletin yanlış yönetimi, yolsuzluk ve siyasi baskı konularının açığa çıkarılmasını ve bu hususlardaki bilginin dağıtılmasını içeren 'direniş olarak

[25] Westin Alan F., "Social and Political Dimensions of Privacy," Journal of Social Issues 59, no. 2 (Nisan 29, 2003): 431–53, https://doi.org/10.1111/1540-4560.00072.

[26] Feng Chen et al., "Data Mining for the Internet of Things: Literature Review and Challenges," International Journal of Distributed Sensor Networks 11, no. 8 (Ağustos 18, 2015): 431047, https://doi.org/10.1155/2015/431047.

[27] Valerio De Stefano, "The Rise of the Just-in-Time Workforce: On-Demand Work, Crowdwork, and Labor Protection in the Gig-Economy," Comparative Labor Law & Policy Journal 37 (2016 2015): 471.

[28] Stefan Tongur and Mats Engwall, "The Business Model Dilemma of Technology Shifts," Technovation 34, no. 9 (Eylül 1, 2014): 525–35, https://doi.org/10.1016/j.technovation.2014.02.006.

bilgi' hareketini yaratmıştır.[29] Bu direniş kültürü, Snowden, Wikileaks ve Chelsea Manning ifşaları ile birlikte devletler tarafından gözetleme konusundaki yetkilerin kötüye kullanımının ortaya çıkarılmasını müteakiben, daha iyi organize olmuş bir dijital kimliğe bürünmüştür. Devletler teorik olarak sözü geçen sivil OSINT havuzunu kullanabilsede, belirtilen topluluğun mevcut kültürü ve kimliği çoğunlukla devlet karşıtıdır.[30] Son olarak, OSINT'in doğası gereği iki ucu keskin bir bıçak olması sebebiyle, devletler, OSINT faaliyetlerinden çıkar sağlayabildikleri oranda muhtemelen zarar da görebilmektedir. Bir devlet, diğer devletleri ya da iç muhalefet gruplarına zarar vermek amacı ile OSINT alanından faydalanmayı denerken, aynı zamanda hedef kitle maliyetleri ve kamuoyu karşısında utanç yaratacak durumlardan zarar görebilir. Sivil veri sızıntıları (oy verme, sağlık, satın alma tarihi verileri vb) bireylere zarar verse de, çoğu sızıntının gizlilik içeren doğasına bağlı olarak, devlet düzeyindeki sızıntılar hükümetlere ve istihbarat servislerine daha fazla zarar verebilmektedir.[31] Bu durum devletlerin dijital kuvvet paritesinde sivillerin gerisinde kalmasına yol açmakta (siviller özellikle hedef alınmadığı sürece) ve devlet ile toplum arasındaki göreli kuvvet dengesini değiştirmektedir. Bu değişiklik, sözü edilen yenilenmiş devlet-toplum güç dengesine bağlı olarak dış aktörlerin bir ulusun iç mekanizmalarını suistimal edebilmesine ve bu süreçlere karışabilmesine olanak vermesinin sonucunda, devletler arasında güvenlik ikilemlerinin doğmasına yol açmaktadır. Bu müdahaleler güçlü ve zayıf devletlere benzer şekilde zarar verebilmektedir. Bahsi geçen konunun en iyi örnek Amerika Birleşik Devletleri seçimlerine sahte haberler ve diğer kamusal olarak erişilebilir haber ve bilgi kaynakları aracılığı ile Rusya tarafından gerçekleştirilen müdahaledir.

[29] Moonsun Choi, Michael Glassman, and Dean Cristol, "What It Means to Be a Citizen in the Internet Age: Development of a Reliable and Valid Digital Citizenship Scale," Computers & Education 107 (Nisan 1, 2017): 100–112, https://doi.org/10.1016/j.compedu.2017.01.002.

[30] Zeynep Tufekci, Twitter and Tear Gas: The Power and Fragility of Networked Protest (New Haven ; London: Yale University Press, 2017).

[31] S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations," IEEE Security Privacy 11, no. 4 (Temmuz 2013): 54–63, https://doi.org/10.1109/MSP.2013.90.

# OSINT Türleri ve Örnekleri

OSINT araçları hızla gelişmekte olsa da, bu alandaki en popüler yöntemler dört ana kategoride toplanabilmektedir: dilbilimsel/metin tabanlı yöntemler, coğrafi bilgi sistemleri (GIS) – uzaktan algılama, ağ bilimi ve görsel adli bilimler.

## a. Dilbilimsel ve Metin Tabanlı Yöntemler

| **Bilgi Kutusu (Terimler)** |
|---|
| - Doğal Dil İşleme (NLP): Kökleri Alan Turing'in 1950 tarihli 'Bilgisayar Mekanizması ve Zeka' başlıklı makalesine (Turing testini ortaya çıkaran) kadar geri giden NLP, öncelikli olarak insan ve makine dilleri arasındaki etkileşim ile ilgilenmektedir. Özünde insan dilleri arasında otomatik hale getirilmiş manike tercümelerine odaklanan NLP, günümüzde yapılandırılmamış ve yapılandırılmamış, çok dilli ve büyük miktarlardaki metinler içinde bulunan düzenlerin ortaya çıkarılmasına odaklanmakta, bunu birimler, anahtar kelimeler, kelime-ifade ilişkileri ve anlamsal – söz bilimsel roller aracılığı ile gerçekleştirmektedir. NLP, otomatik metin özetleme, makine tabanlı duygu analizi, birim ve başlık çıkartma gibi daha modern metin tabanlı yöntemleri uygulayacak şekilde gelişmiştir ve modern metin madenciliği yöntemlerinin temelini oluşturmaktadır. |
| - Gizli Anlamsal İndeksleme (LSI): LSI, örnek bir metinden öğrenerek birden fazla belgedeki 'gizli' kavramları tespit etmeyi amaçlayan makine öğrenimi tabanlı bir metin analizi yöntemidir. Örneğin, 'topçu', 'top mermisi', ve 'bombardıman' metinlerinin birden fazla belge içinde sıkça görülmesi durumunda, sistem bu kelimeleri aynı anlamsal bağlam içinde indekslemekte, aynı zamanda 'top mermisi' (shell) kelimesini 'sahil', 'kum' ya da 'yengeç' ('beach', 'sand', or 'crab') kelimelerini içeren belgelerden ayırmaktadır. LSI, arşiv belgeleri, yasama ile ilgili ya da hukuki belgeler gibi büyük miktarlardaki metinler ile kullanıldığında en iyi sonuçları üretmektedir. |
| - Gizli Dirichlet Tahsisi (LDA): LDA, LSI gibi metin tabanlı bir makine öğrenimi yöntemi olmasına karşın, kelimeleri kullanıcı tarafından tanımlanan klasörler yerine kendi tanımladığı konu modelleri içinde kümelendirmektedir. LDA bir metin içindeki kelimelerin sıklığını ve aralarındaki ilişkileri birlikte ne kadar sık ve hangi bağlamda kullanıldıkları temelinde kontrol etmektedir. |
| - Varlık İsmi Tanımlama ve Çıkarımı: Varlık İsmi Tanımlama bir algoritmanın bir metin dizisini (cümle ya da paragraf) girdi olarak alıp, bu metin dizisinde geçen ilgili isimleri (kişiler, yerler ve teşkilatlar) tespit ettiği bir süreçtir. Haber kanalları ve yayın evleri günlük olarak büyük miktarlarda çevrimiçi içerik yaratmakta ve bu içeriğin doğru şekilde yönetilmesi her bir yayımlanmış metinin en iyi şekilde kullanılması için büyük önem taşımaktadır. Veri İsmi Tanımlama bütün yayımlanmış metinleri otomatik olarak tarayabilmekte bu bu metinler içinde tartışılmış önemli kişi, teşkilat ve yerleri ortaya çıkarabilmektedir. Her bir metin ile ilgili etiketleri bilmek metinlerin belirli hiyerarşilerde otomatik olarak kategorilendirilmesine ve içeriğin sorunsuz bir şekilde bulunmasına yardımcı olmaktadır. |
| - Metin bütüncesi (text corpus): Bir bütünce genellikle metin tabanlı OSINT yöntemleri için ana veri havuzunu oluşturmaktadır. Bütünce istatistik analizlerin yapılmasına yarayan bir kelime ve anahtar kelime koleksiyonudur. Bütünce, dilbilimsel bir araştırmanın yapılması için daha kullanışlı hale getirilmesi amacıyla, sıkça açımlama olarak bilinen bir sürece tabi tutulmaktadır. Bir bütüncenin açımlanmasının örneklerinden biri, her bir kelimenin konuşmanın hangi kısmında yer aldığıyla ilgili bilginin bütünceye etiketler halinde dahil edildiği 'konuşmanın kısmı etiketlendirmesidir'. |
| - N-Gram: Bir dil işleme uygulamasında, bir n-gram bütüncede aranacak sorgu için analiz birimini belirlemektedir. İki kelimenin bir arada aranması durumunda ('conventional' + 'warfare', ya da 'terrorist' + 'attack') bu sorgu bir bi-gram olarak tanımlanmaktadır. Öte yandan bir tri-gram özellikle 'conventional' + 'submarine' + 'warfare', ya da 'terrorist' + 'suicide' + 'attack' kelimelerinin kombinasyonu için yapılan üç kelimeli bir sorgu olmaktadır. |

Dil ve duygu analizi OSINT'in en eski uygulamalarından olmuştur. Liderlik psikolojisi, politik niyet ve organizasyonel uyum ile ilgili sonuçların konuşma ve metinlerden çıkarılması OSINT'in diplomatların ve diğer aracıların önemli bilgileri sentezlemesini sağlayan tarihsel versiyonlarının temel bir uygulamasıdır. Esasında, Soğuk Savaş boyunca, gazetelerin, siyasi liderlik bildirilerinin ve hatta bilimsel yayınların toplanması çatışmanın her iki tarafındaki ülkelerde sıradan bir faaliyet olmuştur.[32] Dahası, Birinci Dünya Savaşı'ndan bu yana, dil bilim, antropoloji ve bölge çalışmaları istihbarat açısından önemli oranda ün kazanmıştır. Bu duruma kanıt teşkil eden olgulardan biri en iyi üniversitelerde kurulan özel bölümler ve bu bölümlerin aldığı önemli miktarlardaki finansal devlet desteğidir.[33]

Metinin dijitalleşmesi ve 'veri olarak metin' yöntemlerinin sosyal bilimlerde popülerleşmesi dilbilimsel OSINT analizi üzerinde doğrudan etki yapmıştır. Niceliksel dil bilimin popülerleşmesi 1960'lara kadar geriye gitse de, metin dosyalarının bilgisayar tabanlı kelime işlemcileri ile büyük oranda dijitalleşmesi ve standartlaşması metin kategorileştirmesi, metin kümelemesi, varlık çıkarımı ve bilişimsel özetleme gibi açık kaynaklı toplamada oldukça önemli ilerlemelere yol açmıştır. Sözü edilen büyük dijitalleşmenin sonucunda, tarihsel arşivler, siyasi metinler ve anılar kelime işleme amacıyla bütünüyle dijitalleşmiş, bu durum dil bilimcilere ve içerik/söylem analistlerine eşi benzeri görülmemiş veri boyutları ve hızlı işleme araçları sağlamıştır. Bu araçlar, web siteleri, bloglar ve sosyal medya gönderileri gibi internet tabanlı metin madenciliği için özellikle değerli olmuştur. Varlığını sürdüren 644 milyon web sitesine ek olarak, büyük hacimli sosyal medya verisi günlük olarak birikmekte, bu birikim tüm dünyada gerçekleştirilen metin tabanlı etkileşimlerin büyük çoğunluğunun aranabilir, tasniflenebilir, ölçülebilir olduğu anlamına gelmektedir. Söz konusu uygulamaların bir kısmı gerçek zamanlı olarak gerçekleşmektedir.

Metin tabanlı OSINT Python, R, MatLab ve Ruby gibi programlama standartları ile yapılabiliyor olsa da, aynı zamanda salt metin tabanlı OSINT'e özel uygulamalar da bulunmaktadır. Popüler olan uygulamalardan bazıları kullanıcıların büyük hacimli metinlerde bağlantıları, düzenleri ve temaları tespit edip görselleştirmesini sağlayan WordStat, RapidMiner, KHCoder ve NVivo yazılımlarıdır. Ek olarak, Gizli Dirichlet Tahsisi (LDA), metin bölümlemesi, Gizli Anlamsal Analiz ve Pachinko Tahsisi gibi istatistiksel konu modellemesine dayanan doğal dil işleme uygulamaları düzen tespiti ve duygu analizi amaçlı makine öğrenimi yaklaşımını mümkün kılmaktadır. Dahası, varlık ismi tanımlama ve ve çıkarımı uygulamaları geçmişe yönelik ya da gerçek zamanlı analiz için büyük hacimli sosyal medya metin verisinin kataloglanmasını, tasnifini ve işlenmesini çok daha kolay hale getirmektedir.

OSINT'in gelecek vadeden uygulamaları, Ashgar (et. al.) tarafından yapılan ve Youtube yorum videolarındaki radikalleşme düzeyinin ölçülmesi amacıyla bu videolardaki düzenlerin tespitini inceleyen araştırmada[34] ya da Hsinchun Chen tarafından yapılan ve Dark Web ve içindeki aşırıcı ağlar ile ilgili metin madenciliğini konu alan ufuk açıcı çalışmada[35] gösterildiği üzere, davranışsal tahmin/tespit analizleridir. Singh et. al. bunu bir adım ileriye götürmüş ve Hindistan Dış İşleri Bakanlığı ile Narenda Modi arasındaki popülerlik dinamiklerini analiz etmek üzere Hindistanlı diplomatların tweetlerini toplayarak diplomatik merkez ile siyasi liderliğe destek hakkında açık şekilde fikir kazanılmasını sağlamıştır.[36] Öte yandan tahminsel analiz ile ilgili olarak Mueller ve Rauch gerçekleşmek üzere olan protesto ve çatışmalarını öngörmeyi amaçlayarak gazete metin madenciliğini kullanmış, öngörü amaçlı ve büyük hacimli 'veri olarak metinden' yararlanan açık bir model üretmiştir.[37]

---

[32] Johnson, The Oxford Handbook of National Security Intelligence, 144.

[33] Osamah F. Khalil, America's Dream Palace: Middle East Expertise and the Rise of the National Security State (Cambridge, Massachusetts: Harvard University Press, 2016).

[34] Muhammad Zubair Asghar et al., "Sentiment Analysis on YouTube: A Brief Survey," ArXiv 1511.09142 (Kasım 29, 2015), http://arxiv.org/abs/1511.09142.

[35] Hsinchun Chen, Dark Web: Exploring and Data Mining the Dark Side of the Web, Integrated Series in Information Systems (New York: Springer-Verlag, 2012), //www.springer.com/gp/book/9781461415565.

[36] V. K. Singh, D. Mahata, and R. Adhikari, "Mining the Blogosphere from a Socio-Political Perspective," in 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010, 365–70, https://doi.org/10.1109/CISIM.2010.5643634.

[37] Hannes Mueller and Christopher Rauh, "Reading Between the Lines: Prediction of Political Violence Using Newspaper Text," American Political Science Review, Aralık 2017, 1–18, https://doi.org/10.1017/S0003055417000570.

## b. Coğrafi-Konum İstihbaratı ve Uzaktan Algılama Araçları

### Bilgi Kutusu (Terimler)

- Vektör ve tarama verisi: GIS yazılımında (Coğrafi Analiz Sistemi, CAS), coğrafi bilgi iki ana veri türü içinde depolanmaktadır. Vektör verisi dünyayı noktalar, çizgiler ve poligonları kullanarak temsil etmektedir. Vektör modelleri ülke sınırları, kara parselleri ve sokaklar gibi belirli sınırlara sahip verinin depolanması için kullanışlıdır. Öte yandan, tarama verisi, dünyanın düzenli karelere ayrılmış hücreler ile yapılan bir temsilidir. Tarama modelleri havadan fotoğraflar, uydu görselleri, kimyasal yoğunlaşmalardan oluşan bir yüzey ya da eğimli bir yüzey gibi sürekli değişkenlik gösteren verilerin depolanması için kullanışlı olmaktadır.

- Taban haritası: Bir taban haritası kullanıcıya bir harita için ortam sağlamaktadır. Vektör ya da tarama verisi bir taban haritasının üzerine bindirilerek kullanılabilmektedir. Taban haritaları haritacının nakletmeye çalıştığı bilgiye dayanan farklı coğrafi-konumsal bilgileri sağlayan referans bilgileri içerebilmektedir.

- Coğrafi kodlama – coğrafi çitleme: Coğrafi kodlama bir koordinat çifti, bir adres ya da bir yer ismi gibi yer tariflerinin yeryüzü yüzeyinde bir lokasyona dönüştürülmesidir. Bir analist belirli bir zamanda bir yer tarifinin girişini yaparak ya da aynı zamanda bir çok yer tarifini kullanarak coğrafi kodlama yapabilmektedir. Sonuç olarak ortaya çıkan lokasyonlar, haritalama ve konum analizi için kullanılabilen ve nitelikli coğrafi özellikler şeklindeki çıktılardır. Öte yandan, coğrafi çitleme, bir uygulama ya da başka bir yazılımın, bir mobil aygıt ya da RFID etiketinin bir coğrafi konum etrafında kurulmuş ve coğrafi çit olarak tanımlanan sanal sınırlar içine girdiğinde ya da bu sınırların dışına çıktığında daha önceden programlanmış bir hareketi gerçekleştirmesini sağlamak üzere GPS, RFID, Wi-Fi ya da hücresel veri kullanan konum tabanlı bir hizmettir. Bir coğrafi çitin nasıl ayarlandığına bağlı olarak bu sistemler push bildirimleri, kısa mesajları ya da uyarıları harekete geçirebilmekte, sosyal medyada hedefli reklamlar gönderebilmekte, araç filolarının takibine izin verebilmekte, belirli teknolojilerin kullanımını engelleyebilmekte ya da konum tabanlı pazarlama verilerini ulaştırabilmektedir.

- Coğrafi Bilgi Sistemleri (GIS): Bir coğrafi bilgi sistemi her tür coğrafi verinin elde edilmesi, depolanması, manipüle edilmesi, analizi, idare edilmesi ve sunulması için tasarlanmış bir sistemdir. Bu teknolojinin anahtar kelimesi coğrafyadır ve bu verinin bir kısmının konumsal olduğu anlamına gelmektedir. Diğer bir deyişle, söz konusu veri bir şekilde yeryüzündeki konumlara atfedilmektedir. Bu veri ile birlikte nitelik (attribute) verisi olarak bilinen genellikle çizelge özellikli olan veri kullanılmaktadır. Nitelik verisi genel olarak konumsal özelliklerin her biri ile ilgili ek bilgi olarak tanımlanabilmektedir.

- LIDAR: Işık Tespiti ve Mesafe Ölçümü anlamına gelen LIDAR, darbeli lazer şeklindeki ışığı yeryüzüne olan mesafenin ölçümü (değişken uzaklıkları) için kullanan bir uzaktan algılama yöntemidir. Bu ışık darbeleri – hava sistemleri tarafından kayıt edilen diğer verile ile birlikte – yeryüzünün şekli ve yüzey özellikleri ile ilgili hassas, üç boyutlu bilgi üretmektedir. Bir LIDAR enstrümanı prensip olarak bir lazerden, bir tarayıcıdan ve bir özel GPS alıcısından oluşmaktadır. Uçaklar ve helikopterler geniş alanlarda LIDAR verisi elde etmek için en çok kullanılan platformlardır.

- Landsat: LANDSAT programı kara gözetlemesi için kullanılan ve bir optik/kızıl ötesi uzaktan algılama uydu serisinden oluşan en eski ve işlevsel uydu görsel programıdır. Bu program 1972 yılında Amerikan Ulusal Havacılık ve Uzay Dairesi (NASA) tarafından başlatılmış, daha sonra operasyonel duruma geldikten sonra Ulusal Okyanus ve Atmosfer Dairesi (NOAA) tarafından devralınmıştır.

- Uzaktan algılama: Uzaktan algılama bilginin fiziksel olarak ilgili konumda bulunmadan elde edilmesi bilimidir. Örneğin, en çok kullanılan üç uzaktan algılama yöntemi uçaklar, uydular ve insansız hava araçları ile gerçekleştirilmektedir. Uzaktan algılama uygulamaları aktif ve pasif olarak iki öncelikli türden oluşmaktadır. Aktif sensörler, kendi enerji kaynaklarını gözledikleri bir nesenin aydınlatılması için kullanmaktadır. Bir aktif sensör soruşturulacak hedef doğrultusunda radyasyon yaymaktadır. Sensör daha sonra hedeften yansıyan ve geri dönen radyasyonu tespit etmekte ve ölçmektedir. Öte yandan, pasif sensörler, gözetlenen nesne ya da manzaradan yayılan ya da yansıyan doğal enerjiyi (radyasyon) tespit etmektedir. Yansıyan güneş ışığı pasif sensörler tarafından en sık ölçülen radyasyon kaynağıdır.

Kartografi de dil gibi eski bir istihbarat ve stratejik analiz ekolüdür ve öncelikli olarak jeopolitik ve coğrafi değişkenler ile sınırlar ve arazinin siyasi etkileri üzerinde çalışmaktadır. Coğrafi bilgi sistemleri – ya da GIS – ve internet tabanlı konum bilgilerinin (giriş ve konum tayin bilgileri) birleşimi analistler tarafından mobilizasyon, büyük hareketlilikler ve çatışmaların da dahil olduğu insan davranışının sosyal ve konumsal dinamiklerinden istifade edilmesine imkan sağlamıştır.[38] Yükseklik, topografya, eğim, kaynaklar, taşıma ve altyapı gibi ek değişkenler ile birlikte, coğrafi-konum istihbaratı (GEOINT) kullanılarak, küçük ve büyük ölçekli insan davranışı analiz edilebilmekte ve anlamlı şekilde modellenebilmektedir.[39] Bu tip analiz çalışmaları için özel GIS platformları mevcut olsa da – ArcGis, QGis – Python ve R (ve hatta Excel) gibi programlama platformları da GIS paketlerini ya da haritalama, coğrafi istatistik ve yakınlık analizini entegre eden eklentilere sahiptir. Planet Labs, Terra Bella, BlackSky Global ve XpressSAR sistemlerinin ek görsel kuvveti ile birlikte, pek çok katman, zaman çerçevesi ve granüllü coğrafi bilgi günümüzde sivil GEOINT analistleri tarafından kullanılabilmektedir.

GEOINT çalışmalarında iki ana veri türü bulunmaktadır: vektör ve tarama. Vektör verisi bir harita üzerinde belirli bir konum ya da bölgenin tayin edilmesi amacıyla poligonların ve koordinatların birleştirilmesi ile oluşmaktadır. Öte yandan, tarama verisi, üç boyutlu analizin oluşturulması için görselleri, yükselti modellerini ve harita işleyicilerini içermektedir. Coğrafi bilgi sistemlerinin artan ünü ile birlikte, internet üzerinde bulunan coğrafi-konum veritabanlarının sayısı önemli oranda artmıştır. Söz konusu veritabanları ayrıca LiDAR (Işık Tespiti ve Mesafe Ölçümü), insansız hava araçları, GPS ve uydular ile desteklenmekte, bununla coğrafi veri setlerinin granüllülüğünün ve boyutunun artırılması amaçlanmaktadır. Kullanılan teknik ne olursa olsun, GEOINT uygulamarının en iyileri yalnızca konum verisini sağlayıp görselleştirmemekte, ayrıca bir politikanın hikayesini anlatmakta ya da diğer yöntemlerin yetersiz kaldığı yerlerde bir stratejik boşluk görebilmektedir. Örneğin, Harvard İnsani İşler Girişimi (HHI) üniversiteler tarafından yönlendirilen GEOINT yaklaşımının ilk örneklerinden biridir. HHI 1999 yılında kurulmuş ve Darfur, Sudan, Çad ve Kongo'da yaşanan kriz ve çatışmaları sahada bulunan unsurlar ile işbirliği içinde haritalandırmak için sivil toplum kuruluşları, BM yardım teşkilatları ve mülteci yardım kuruluşları ile ortaklık yapmıştır.[40] Ayrıca Katrina kasırgası sırasında, gerek ABD yönetimi gerekse sivil toplum analistleri afet müdahalesi ve yardım çalışmaları için farklı GIS yöntemlerini benimsemiştir.[41] Kar amacı gütmeyen bir teknoloji şirketi olan Ushahidi ise Haiti, Şili, Kenya ve İtalya'da seçimlerin gözlemlenmesi ve afet sonrası yardım çalışmalarına odaklanan bir başka devlet dışı OSINT girişimidir. Ushahidi, kriz olayları sırasında kullanılan bir kitle kaynaklı harita olan bir 'kitle haritası' kullanmıştır.[42] Söz konusu kitle kaynaklı harita, şirketin 2007-2008 Kenya krizi sırasında gerçekleştirdiği meşhur olay izleme çalışmasına ek olarak Occupy hareketi ve 2011 yılındaki Londra gösterileri de dahil olmak üzere çeşitli protesto olayları sırasında kullanılmıştır. Daha sonra, Ushahidi tanık ifadelerine dayalı kriz olayları veri toplama çalışmaları için gerekli olan altyapıyı sağlayarak İtalya ve Hindistan'da yapılan seçimlerin gözlemlenmesi için konuşlandırılmıştır.

38 Thomas Zeitzoff, "How Social Media Is Changing Conflict," Journal of Conflict Resolution 61, no. 9 (Ekim 1, 2017): 1970–91, https://doi.org/10.1177/0022002717721392; Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," Perspectives on Politics 13, no. 1 (Mart 2015): 42–54, https://doi.org/10.1017/S1537592714003120.

39 Bacastow and Bellafiore, "Redefining Geospatial Intelligence."

40 Steve Lohr, "In Relief Work, Online Mapping Yet to Attain Full Potential," The New York Times, Mart 28, 2011, sec. Business Day, https://www.nytimes.com/2011/03/28/business/28map.html.

41 Jeffrey Gettleman, "Congo: Rapes by Civilians Rise Sharply, Study Says," The New York Times, Nisan 14, 2010, sec. Africa, https://www.nytimes.com/2010/04/15/world/africa/15briefs-congo.html.

42 Anand Giridharadas, "Ushahidi - Africa's Gift to Silicon Valley: How to Track a Crisis," The New York Times, Mart 13, 2010, sec. Week in Review, https://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html.

## c. Bağlantılar ve Ağlar

**Bilgi Kutusu: Terimler**

- Ağ düğümleri: Bir iletişim ağında, bir ağ düğümü, dağıtımlı ağ rotaları boyunca veriyi alabilen, yaratabilen, depolayabilen ya da gönderebilen bir bağlantı noktasıdır. Her bir ağ düğümü – ister veri aktarımı için bir son nokta isterse bir yeniden dağıtım noktası olarak – dağıtımların tanınmasını, işlenmesini ya da diğer ağ düğümlerine aktarılmasını sağlayan programlanmış ya da tasarlanmış beceriye sahiptir.

- Yoğunluk: Yoğunluk istatistiği bir ağda mevcut olan olası ilişkilerin oranını temsil etmektedir. Değer 0 ile 1 arasında değişmekte, alt limit hiç ilişki içermeyen ağları, üst limit ise bütün olası ilişkileri temsil etmektedir. Değer 1'e yaklaştıkça, ağ daha fazla yoğunlaşmakta ağ içindeki düğümler birbiri ile daha birleşik hale gelmektedir. Yoğun ağlarda bilgi seyrek ağlara göre daha kolay akmaktadır.

- Merkezilik (arasındalık): Ağ analizinde, merkezilik çizge (grafik) içindeki diğer düğümler ile olan bağlantılarının sayısı bakımından en önemli düğümleri tayin etmektedir. OSINT uygulamalarında, ağ merkeziliği çalışmaları genellikle büyük bir grubun en önemli ve en iyi şekilde bağlantılanmış üyelerine odaklanmaktadır. Sosyal ağ analizinde, yüksek merkeziliği olan figürler daha etkili statüye sahip olanlardır.

- Homofili: Ağ homofilisi benzer düğümlerin benzer olmayanlara oranla birbirine eklenme olasılıklarının daha yüksek olduğunu iddia eden bir teoridir. Yoğun ve büyük sosyal ağlarda, homofili ölçümü bir analiste büyük bir nüfus havuzu içindeki bir topluluğu ya da bir grubu kolayca tanımlama imkanı tanımaktadır. Homofili, bilgi ve fikirlerin yayınımındaki hızı belirleyebilmesine bağlı olarak ağ bilimindeki kilit konulardan biridir.

İlişkiler, gruplar ve ağlar OSINT için her zaman önemli olmuştur. Örgütsel liderlik, siyasi karar alma çevreleri ve terörist çevreler istihbarat analizi için merkezi araştırma konularıdır. Klasik ağ teorisi bireyler arasındaki sosyal ağlara (dostluklar, danışmanlık), resmi sözleşmeye bağlı ilişkilere (ittifaklar, ticaret, güvenlik topluluğu) odaklanmaktadır. Ağ teorisini sosyal bilimler, siyaset bilimi ve uluslararası ilişkiler için önemli yapan husus, bu teorinin görünürde karmaşık olan etkileşimlere yapısallık kazandırabilmesi ve siyasi süreçleri mikro, orta ve makro düzeylerde kavramlaştırabilmesi ve teorileştirebilmesidir. Bu duruma uygun olarak, ağ teorisi söz konusu ilişkilerin ve bu ilişkiler üzerindeki içsel ve dışsal baskıların inanışları ve davranışları etkileyebilmesini şart koşmaktadır. Uluslararası ilişkilerin ana akım analiz düzeyleri yaklaşımını benimsemek yerine, ağ teorisi bu analiz düzeyleri arasındaki etkileşime odaklanmakta ve söz konusu etkileşimlerin politikaları ve davranışı nasıl etkilediğini kavramlaştırmayı amaçlamaktadır.[43] Gephi, NetMiner ve iGraph gibi çeşitli uygulamalar büyük ağlar ile çalışmayı ve bu ağları niceliksel yöntemler kullanarak arasındalık, homofili ve merkezilik bakımından ölçümlemeyi kolaylaştırmıştır. Bu durum, geleneksel yöntemler ile karşılaştırıldığında, aşırıcı ve radikal ağların daha kolay görselleştirilmesini ve hiyerarşiler ile nüfuz sahiplerinin çok daha açık bir şekilde bağlamlaştırılmasını mümkün kılmaktadır.[44] Ayrıca, bilişimsel ağ analizi klasik ağ teorisinin genişliğini ve karmaşıklık düzeylerini büyük oranda artırmakta, yalnızca ilişkilerin tayinini yapmaktan öte, yapay zeka, makine öğrenimi ve sinir ağları yaklaşımlarını bu ilişkilerdeki gerçek zamanlı değişiklikleri otomatik olarak yaratmak için kullanmaktadır. Günümüzde, dijital OSINT içinde ağ analizinin en popüler uygulamalarından biri, çok büyük gruplar arasındaki takip, beğeni ve paylaşım ilişkilerini inceleyen sosyal medya analizidir.[45] Daha eski yöntemler ile karşılaştırıldığında, sosyal ağ analizi söz konusu sistemler içindeki nüfuz sahipleri ile hiyerarşilerin daha başarılı şekilde anlaşılmasını mümkün kılmaktadır.

[43] Johnson, The Oxford Handbook of National Security Intelligence, 26.

[44] Matt Apuzzo, "Who Will Become a Terrorist? Research Yields Few Clues," The New York Times, Aralık 21, 2017, sec. World, https://www.nytimes.com/2016/03/28/world/europe/mystery-about-who-will-become-a-terrorist-defies-clear-answers.html.

[45] Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," Studies in Conflict & Terrorism 38, no. 1 (Ocak 2, 2015): 1–22, https://doi.org/10.1080/1057610X.2014.974948.

## d. Görsel ve Video Kullanan Adli Bilimler

### Bilgi Kutusu (Terimler)

- Artefakt: Artefakt bir medyadaki (video, ses, ya da görsel) görünür bozulma ya da görsel hatadır. Aftefakt homojenliği, medya boyunca bu bozulmaların ne kadar eşit dağıldığının ölçülmesi ile yapılan ve bir medya türünün manipüle edilip edilmediğini anlamaya yarayan bir medya adli bilimi aracıdır. Artefakt eşitsizliği genel olarak manipülasyon ya da medya üzerinde oynama ile ilişkilendirilmekte ve makine öğrenimi tabanlı medya adli bilimi araçları ile tespit edilebilmektedir.

- Dijital Adli Bilimler: Dijital medya adli bilimleri alanı silinmiş ve gizlenmiş verinin bulunmasına yönelik bir uğraşı, kullanılan çeşitli araçların arkasındaki temel teknolojilerde hakimiyet ve bilimsel olarak geçerli bilginin sunulması becerisidir. Dijital medya adli bilimleri devletlere ve şirketlere dijital kanıtların özgünlüğünü değerlendirme fırsatı tanıyan büyümekte olan bir bilim dalıdır.

- Fotoğrafik Karşılaştırma: Bir görsel adli bilimler aracı olarak, fotoğrafik karşılaştırma bir görselin özgünlüğünü ya da birden fazla versiyonu üzerindeki değişiklikleri test etmektedir. İnternet üzerinde, fotoğrafik karşılaştırmanın büyük miktarlarda benzer görselleri düzenleyerek orijinal versiyonu bulması gerekmektedir. Özellikle kriz olayları ile ilintili görsellerde ya da yüksek siyasi değere sahip fotoğraflarda, otomatik hale getirilmiş yazılımlar insan gözü tarafından ölçülemeyen eşitsizliği tespit etmek için kullanılabilmektedir.

- Meta Veri: Medya dosyaları, dosyanın içeriğini tarif eden özellikleri barındırmaktadır. Bu özellikler şu şekilde kategorilendirilmektedir:
a) Kodlama algoritması (medya alt türü), video kare büyüklüğü, video kare oranı, ses bit oranı ve ses örnek oranı gibi kodlama parametrelerini tanımlayan medya tipi nitelikleri.
b) Meta veri başlık, sanatçı, fotoğrafçı ve tür gibi medya içeriğini tarif eden bilgileri barındırmaktadır. Bu bilgiye, medya tipi nitelikleri ile karşılaştırıldığında, meta veri ile daha hızlı ulaşılabilmektedir.
c) Kullanım kısıtlamaları ile bilgileri içeren DRM özellikleri. Halihazırda, Medya Vakfı, PKEY_DRM_IsProtected özelliği dışında meta veri aracılığıyla DRM özelliklerini desteklememektedir.

- Fotogrametrik Analiz: Özünde bir MASIN aracı olan fotogrametri fotoğraflardan ölçümleme çıkarma bilimidir. Söz konusu ölçümler kesin koordinatlar ya da medyadaki görseller arasındaki mesafe olabilir. Halihazırda, OSINT analistleri uydu, insansız hava aracı ve LIDAR görselleri ile toplanan iki ve üç boyutlu görselleri kullanarak dijital fotogrametri analizi icra edebilmektedir. Fotogrametri algoritmaları tipik olarak hataların karelerini koordinatlar ya da referans noktalarının göreli yer değişiklikleri üzerinde toplamaya çalışmaktadır.

Wi-Fi ve telefon veri ağı hizmetlerinin daha hızlı ve ucuz hale gelmesine bağlı olarak, çevrimiçi insan haberleşmesi çok hızlı bir şekilde metin tabanlı bir yapıdan medya tabanlı olana evrilmiştir. Whatsapp üzerinde bir ses mesajı göndermek mesajlaşmaktan, ya da bir fotoğraf ya da video göndermek uzun cümle ve paragrafları ifade etmekten daha kolay bulunabilmektedir. Aynı mantık krizler ve acil durumlar için de geçerlidir. Stres altında insanlar, kısa mesajlar ya da çevrimiçi yazılan uzun mesajlar yerine, olayları belgelemek ya da yardım çağırma amacıyla görsel ya da video paylaşmayı tercih etmektedir. Bu nedenle, halen tweetlense, paylaşılsa ve blog sayfaları yazılsa da, dijital haberleşme (özellikle kriz zamanlarında) giderek artan bir şekilde medya tabanlı hale gelmiştir. Stratejik kazanım ve acil durumlarda haberleşme amacı ile fotoğraflar üzerinde yapılan çalışmaların geçmişi 19. Yüzyılın sonlarına dayanıyor olsa da, genel bir pratik olarak video istihbaratı büyük oranda İkinci Dünya Savaşı sonrası bir gayrettir. Günümüzde, sözü edilen görsel medya dijital olarak analiz edilebilmekte, yorumlanabilmekte ve sahadan kilit bilgilerin çıkarılması amacıyla (özellikle fiziksel erişimin sınırlı olduğu çatışma, gösteri ya da afet bölgelerinde) kullanılabilmektedir. Görseller ve videolar harp sahalarında ya da kriz bölgelerinde doğrulama, bildiri, propaganda ve karşı propaganda amaçları ile kullanılabilmekte, ilişkilerin, çıkarların ya da imkan ve kabiliyetlerin kanıtları olarak paylaşılabilmektedir. OSINT için acil durum medyasının değerine bağlı olarak, bu ayrıca manipülasyon ve sahtecilik karşısında en korunmasız alanlardan biridir. Görsel ve videolar

birbirine benzer şekilde taklit edilebilmekte ve kötü amaçla değiştirilebilmekte ve eskimiş medya yeniymiş gibi paylaşılabilmektedir. Bu durum sonuçta devletlerin ve devlet dışı aktörlerin acil durumlarda rakiplerinin yanlış yönlendirilmesine, dikkatlerinin dağıtılmasına ve gözlerinin korkutulmasına yarayacak şekilde kullanılabilmektedir.

Çeşitli özel girişimler, kitle kaynaklı bir OSINT ağı oluşturma amacı ile, web tabanlı görsel ve videoların özel olarak çalışılmasına odaklanmıştır. Söz konusu girişimlerin en ünlüsü Bellingcat bir çevrimiçi soruşturma platformudur. Bellingcat medya tabanlı OSINT'in nasıl icra edileceği ile ilgili çeşitli eğitim materyalleri yayımlamıştır. Bellingcat'in ün kazanmış soruşturmaları Rus askeri birlik hareketlerini, Suriye'nin kimyasal silah kullanımının doğrulanmasını ve bazı hadiselerde gösterici – polis dinamiklerini içermektedir.[46] Bir diğer örnek olan Forensic Architecture, Londra Üniversitesi merkezli ve siyasi öneme sahip fakat iyi belgelenmemiş olayların anlaşılması için fotoğraf, video ve hava platformlarından elde edilen görselleri kullanan bir akademik-aktivist platformdur.[47] Gerek Bellingcat gerekse Forensic Architecture, kanıt yaratma amacıyla, medyanın yöntemli olarak çalışılmasını ve de dağınık görsel kanıtların çok çeşitli kaynaklardan bir araya getirilmesini kullanarak kritik olayları doğrulamayı amaçlamaktadır. Başlangıçta meraklıların bir hobisi olarak görülen medya adli bilimleri OSINT girişimleri resmi istihbarat servislerine göre daha uygun ve etkili hale gelmiş, bu durum Bellingcat ve Forensic Architecture girişimlerinin mahkemeler, Birleşmiş Milletler ve devletler tarafından yönlendirilen insan hakları raporları için kanıt sağlaması ile belirginleşmiştir.[48]

## Kitle Kaynaklı OSINT

Çok sayıda ve kamu tarafından erişilebilir kritik veri türü ile 'sırların sonunun geldiği' ya da 'sır sonrası' bir döneme girilmekte olduğu şeklinde bir yargıya ulaşmak cazip görülebilmektedir. Esasında, Sean P. Larkin Foreign Affairs tarafından yayımlanan 'Şeffaflık Çağı' başlıklı makalesini kaleme aldığında, ticari olarak erişilebilir uydu görsellerinin, insansız hava araçları sensörlerinin, otomatik kriz raporlarının, vatandaş gazetecilerin ve açık kaynak blog yazarlarının sırları anlamsız hale getireceği ile ilgili son derece kararlı bir tutum takınmıştır.[49] Larkin'in görüşü kamuya açık gözetleme araçlarının maliyetinin düşmesine bağlı olarak sırları elde etmenin ve korumanın maliyetinin yükselmekte olduğu yönündedir. Devletlerin krizler, diplomatik gerginlikler ve gösteriler sırasında çerçeve ve hikayeleri (ontolojik güvenlik) yaratma ve sürdürme kabiliyetleri teknoloji ile ciddi oranda darbe almıştır. Özellikle önemli olaylar sırasında sosyal medyanın gücünün küresel olarak keşfedilmesinden bu yana, devletler konvansiyonel haber kaynaklarının ötesinde yeni hikaye ve çerçeve kaynakları ile rekabet etmek zorunda kalmıştır.

Küresel birbirine bağlantılılık ve vatandaşlar tarafından icra edilen muhabirliğin ortaya çıkması yeni bir analist sınıfını doğurmuştur. Bu sınıf benzer şekilde düşünen dijital aktivistlerden devlet kaynaklı hikayelere karşı konulması için yararlanmayı amaçlayan kitle kaynaklı istihbarat ağından oluşmaktadır. Esasında, kitle kaynaklı istihbarat analizini kullanma konusunda ilk denemeyi gerçekleştiren 2009 yılında icra edilen 'Network Challenged' tatbikatı ile Amerika Birleşik Devletleri (DARPA) olmuştur.[50] Söz konusu kitle kaynaklı tatbikat sırasında, OSINT faaliyetlerinde devlet kaynaklı çabalarda karşılaşılan çok sayıda zorluk (doğrulama, olay verisi yaratma, ölçüm gibi) sosyal ağ araçları aracılığı ile çalışan kullanıcılardan oluşan yarı otonom ağ tarafından daha iyi idare edilebilmiştir. Bu tatbikat 'amatörlerin' (istihbarat ve siyasa planlama alanlarında tecrübesi olmayan ya da çok az olan siviller) farklı perspektiflerden bakıldığında hem kullanışlı hem de kullanışsız olduğunu göstermiştir. Kitle kaynaklı istihbarat kesinlikle hızlı, bürokrasi ve katı politikalara bağlı olmayan bir faaliyettir. Öte yandan, söz konusu OSINT me-

46 Pablo Gutierrez and Paul Torpey, "How Digital Detectives Say They Proved Ukraine Attacks Came from Russia," The Guardian, Şubat 17, 2015, sec. World news, http://www.theguardian.com/world/2015/feb/17/ukraine-russia-crossborder-attacks-satellite-evidence.

47 Rowan Moore, "Forensic Architecture: The Detail behind the Devilry," The Observer, Şubat 25, 2018, sec. Art and design, http://www.theguardian.com/artanddesign/2018/feb/25/forensic-architects-eyal-weizman.

48 Dylan Collins, "A US Airstrike Which Killed 38 People Allegedly Hit a Peaceful Mosque in a Syrian Village," Business Insider, Nisan 18, 2017, http://www.businessinsider.com/us-airstrike-allegedly-hit-a-peaceful-mosque-in-a-syrian-village-2017-4.

49 Sean P. Larkin, "The Age of Transparency," Foreign Affairs, Nisan 18, 2016, https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency.

50 Mark Harris, "How A Lone Hacker Shredded the Myth of Crowdsourcing," WIRED, Eylül 2, 2015, https://www.wired.com/2015/02/how-a-lone-hacker-shredded-the-myth-of-crowdsourcing/.

raklılarının bir çoğu yeterli istihbarat eğitimine, siyasa organizasyon becerilerine ve karar alıcılar için siyasa seçeneklerinin hazırlanmasında uyumu sahip olmamıştır. Başka bir deyişle, kitle kaynaklı OSINT odaklanılmış bir olay sırasında (bir kriz gibi) devlet kaynaklı hikayelerin zorlanmasında iyi bir faaliyet olarak görülmekte, ancak düzenli siyasi hususların tayininde ve siyasa önerileri üretmede düzenli, günlük internet verisinin izlenmesi ve toplanması için gerekli kapasiteden yoksun kalmaktadır.[51]

Ek olarak, devletler için kriz olayları sırasında kitle kaynaklı OSINT'in gücünden yararlanmak siyasi olarak zordur. Çoğu dijital OSINT aracının 2011 yılında gerçekleşen Occupy ve Arap Baharı hareketleri sonrasında küresel olarak nasıl yaygınlaştığına bağlı olarak, söz konusu uygulamanın genel tonu hegemonya karşıtı ve muhalif bir hal almıştır.[52] Kitle kaynaklı OSINT'in önceki biçimlerinin çoğu gösteri kitlelerinin yönlendirilmesine, gösteri lojistiğinin organize edilmesine ve polisin ya da devlet istihbarat servislerinin engellenmesine odaklanmıştır. Bu nedenle, OSINT'e güvenmeyen devlet istihbarat servisleri ile devletin niyetlerine güvenmeyen vatandaş kaynaklı analiz çabaları arasında derin bir ayrılık ortaya çıkmıştır. Bu karşılıklı güvensizlik bir kitle kaynaklı OSINT ortamının geliştirilmesine yönelik devlet öncüllü çabalar için çalıştırılabilir bir modeli şimdiye kadar engellemiştir. Bahsi geçen şekilde bir model yakın gelecekte mümkün görülmediğinden, devletler ve vatandaş öncüllü çabalar acil durumlar esnasında kendi araç ve ağlarını kullanmaktadır.

Kitle kaynaklı uygulamalara saha tabanlı olay verisi üreticileri, sahaya yakın veri küratörleri ve saha dışı, uzakta konumlu veri analizcileri dahil olmaktadır. Önceki iyi örneklerden biri 2007-2008 yılları arasında Kenya'da seçimler ile ilgili şiddet olaylarını haritalayana Ushahidi (Svahili dilinde 'tanık' anlamına gelmektedir) platformudur. Ushahidi'nin olay verilerini tespit etme performansı Kenya'daki çatışmanın izlenmesinde resmi istihbarat teşkilatlarından daha iyi bir iş çıkarmış ve sonuçta günümüzde Kenya'de seçimler ile ilgili şiddet olayları üzerine geçerliliğini koruyan birincil veri kaynağı olarak kalmıştır.[53] Ushahidi daha sonra 2010 yılında gerçekleşen Haiti depremi üzerine olay verilerinin mobilizasyonu ve kitle kaynaklı hale getirilmesi amacıyla GeoCommons platformuna geçiş yapmış, yardım ve kurtarma kuruluşlarına mümkün olan en fazla olaya müdahale etmelerinde kayda değer oranda yardımcı olmuştur. Ushahidi zamanla Birleşmiş Milletler İnsani İşler Dairesi (OCHA) ile bir Libya Kriz Haritasının oluşturulmasında ortaklık yapacak kadar önemli hale gelmiş, savaştan etkilenmiş ve yardıma ihtiyacı olan alanlarda saha verilerini toplamıştır.[54] Devletler tarafından sivil öncüllü yardım ve kurtarma OSINT platformlarından ne ölçüde yararlanılabileceği ile ilgili geçmiş örneklerden biri bazı NATO hava unsurlarının söz konusu yardım amaçlı haritayı yer hedeflerinin gözden geçirilmesi ve hava bombardımanlarının zaman planlamasını yapmak için kullanmış olmasıdır.[55]

Bellingcat ve LiveUAMap kitle kaynaklı istihbarata daha geç dahil olmuş sistemlerden ikisidir. Bellingcat 2012 yılında bir blog olarak mütevazi bir başlangıçla, LiveUAMap ise Rusya'nın 2014 yılında Ukrayna'da gerçekleştirdiği askeri müdahalenin erken aşamaları sırasında ortaya çıkmıştır. Bellingcat, 2014 yılında Ukrayna üzerinde MH17 uçağının düşürülmesinde hangi Rus birliklerinin rol oynadığının tespit edilmesi için kitle kaynaklı analistler tarafından OSINT araçlarının kullanılması ile ünlenmiştir.[56] Bu soruşturma, Rusya'nın MH17'nin düşürülmesi olayına dahil olması ile ilgili kanıtların resmi devlet raporlarından daha güçlü bir şekilde ve kamuya açık bilgilerin kullanılarak elde edilmesi sonucunda, OSINT için bir dönüm noktası olmuştur. Sonuçta, Bellingcat'in raporu belirtilen olayla ilgili soruşturmayı yürüten Hollanda mahkemesinin iddianamesine dahil edilmiştir.[57] Daha sonra yine 2014 yılında, Bellingcat misket bombalarının ve diğer uluslararası olarak yasaklanmış geniş alanda etkili silahların kullanımı ile ilgili art arda raporlar yayımlamış, Suriye ordusunun söz konusu yasaklı silahları nasıl ürettiğini, taşıdığını

[51] Larry Greenemeier, "DARPA Verigames Crowdsourced Formal Verification (CSFV) Project," Scientific American, Haziran 9, 2015, https://www.scientificamerican.com/citizen-science/darpa-verigames-crowdsourced-formal-verification-csfv-project/.

[52] Tufekci, Twitter and Tear Gas.

[53] Giridharadas, "Ushahidi - Africa's Gift to Silicon Valley."

[54] John D. Sutter, "Ushahidi: How to 'crowdmap' a Disaster," CNN Labs, Ekim 25, 2010, http://www.cnn.com/2010/TECH/innovation/10/25/crowdmap.disaster.internet/index.html.

[55] Ian Traynor, "Libya: Nato Bombing of Gaddafi Forces 'Relying on Information from Rebels,'" The Guardian, Mayıs18, 2011, sec. World news, http://www.theguardian.com/world/2011/may/18/libya-nato-bombing-benghazi-rebel-leaders.

[56] Max Fisher, "Did Ukraine Rebels Take Credit for Downing MH17?," Vox.com, Temmuz 17, 2014, https://www.vox.com/2014/7/17/5913089/did-this-ukrainian-rebel-commander-take-credit-for-shooting-down-the.

[57] Mark Gibney, "The Downing of MH17: Russian Responsibility?," Human Rights Law Review 15, no. 1 (Mart 1, 2015): 17, https://doi.org/10.1093/hrlr/ngu036.

ve konuşlandırdığını ortaya koymuştur.[58] Daha sonra 2015 yılı içinde, Bellingcat ISİD terör örgütünün değişmekte olan insansız hava araçları taktiklerini ve havadan bomba bırakabilen İHA geliştirme çabalarını ortaya çıkaran ilk OSINT yayın organı olmuştur.[59] Söz konusu girişim elde ettiği ün ve gönüllü sayısı bakımından ciddi anlamda büyümüş, tüm dünyadan kitle kaynaklı olay verisi üreticilerini, video ve görsel analistlerini ve GIS haritacılarını içeren bir ağ inşa etmiştir. Bellingcat ayrıca kullandığı OSINT yöntemlerini öğretmeye başlayarak sivil vatandaşlar tarafından daha fazla yönlendirilen istihbarat üretimini mümkün kılmayı amaçlamıştır.

LiveUAMap ise Bellingcat'e göre biraz daha farklı çalışmaktadır. LiveUAMap neredeyse gerçek zamanlı sosyal medya verilerini toplayarak kullandığı interaktif dünya haritası üzerinde çatışma olaylarını göstermeyi amaçlamaktadır. Söz konusu grup başlangıçta özellikle 2014 yılında Rusya'nın Ukrayna'daki faaliyetlerini izleyen bir yayın organı olarak ortaya çıkmış olsa da, kapsamını Suriye, Irak ve daha sonra dünyanın geri kalan bölgelerini içerecek şekilde genişletmiştir. LiveUAMap, gerçek zamanlı uyarıları üretmek için çok dilde sosyal medya verisini ve aynı zamanda 2013 yılına kadar geri giden olaylar veritabanını kullanan gerçek bir kitle kaynaklı çatışma izleme platformudur. Benzer girişimler ise sivil ve resmi uçakların kod bilgilerini ve varış noktalarını haritalayan ve gösteren FlightTracker, dünyanın ana limanları arasında görev yapan petrol ve doğal gaz tankerlerini izleyen TankerTracker, ve tüm dünyada silahlı kuvvetler ve devlet dışı aktörler tarafından konuşlandırılan muharip ve keşif amaçlı insansız hava araçlarının gerçek zamanlı görsellemesini sağlayan DroneDeploy platformlarıdır.

## OSINT'in Uluslararası Siyasi Neticeleri: Demokrasi ve Güvenlik İkilemi

2017 yılı Kasım ayında, fitness izleme uygulaması ve cihaz üreticisi Strava, kullanıcılarına ait 13 trilyon GPS konum veri noktasından oluşan veri setini kullanıma açmıştır.[60] Başlangıçta insanlara kişisel skorlarını sosyal medyada paylaşarak fitness performansları aracılığıyla sosyalleşmeleri için (ne kadar mesafede ya da ne kadar hızlı koştukları gibi) bir fırsat yaratma girişimi olarak düşünülmüş olsa da, bahsi geçen veri setinin yayımlanması tam bir operasyon güvenliği felaketine dönüşmüştür. Söz konusu bireysel konum veri noktaları, büyük şehirlerdeki popüler koşu rotalarının belirlenmesini sağlamakla birlikte, ayrıca askerlerin Strava kullanımı aracılığıyla tanımlanmamış askeri üsleri de ortaya çıkarmıştır. İnsansız hava aracı ve uydu görsellerinin ticarileşmesi halihazırda tüm dünyada birçok önemli askeri üssün keşfine yol açsa da, Strava verileri bu durumu bir adım daha ileri götürmüş, özellikle çatışma bölgelerindeki gizli askeri üslerin ve söz konusu üslerdeki koşucuların zamanlama, faaliyet tarihi ve rotalaranın gün yüzüne çıkmasına sebep olmuştur. Her ne kadar başlangıçta amaçlanmamış olsa da, bu durum, Amerika Birleşik Devletleri Merkez Komutanlığı sözcülerinden Albay John Thomas tarafından Washington Post gazetesine verilen mülakatta 'söz konusu haritanın olası neticelerinin incelendiğinin' belirtilmesine yol açacak ciddi bir güvenlik açığı olmuştur.[61]

Daha sonra 2018 yılı Mart ayının ortalarında Cambridge Analytica adlı veri analizi şirketinin Trump seçim kampanyası ile yürüttüğü kanun dışı anlaşmalar gün yüzüne çıkmış, bu olay 50 milyon Facebook kullanıcısının profillerinin, kullanıcıların rızası olmadan nasıl toplandığını gözler önüne sermiştir.[62] Facebook, Trump seçim kampanyasının önemli liderlerinden olan Steve Bannon ile yakın iletişim kuran ve

[58] Martin Chulov, "Syria Attack: Nerve Agent Experts Race to Smuggle Bodies out of Douma," The Guardian, Nisan 12, 2018, sec. World news, http://www.theguardian.com/world/2018/apr/12/syria-attack-experts-check-signs-nerve-agent.

[59] Ben Sullivan, "The Islamic State Conducted Hundreds of Drone Strikes in Less Than a Month," Motherboard, Şubat 21, 2017, https://motherboard.vice.com/en_us/article/vvxbp9/the-islamic-state-conducted-hundreds-of-drone-strikes-in-less-than-a-month.

[60] Alex Hern, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases," The Guardian, Ocak 28, 2018, sec. Technology, http://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[61] Andrew Liptak, "Strava's Fitness Tracker Heat Map Reveals the Location of Military Bases," The Verge, Ocak 28, 2018, https://www.theverge.com/2018/1/28/16942626/strava-fitness-tracker-heat-map-military-base-internet-of-things-geolocation.

[62] Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram," Vox, Mart 23, 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

üst düzey bir Cambridge Analytica analisti olan Alenxandr Kogan'a 50 milyon profilin işlenmemiş verilerini sağlayarak söz konusu skandala aktif bir aktör olarak doğrudan dahil olmuştur. Kogan, 'thisismydigitallife' isimli bir Facebook test uygulaması geliştirmiş, bu uygulama verdikleri verilerin daha sonra siyasi bir kampanyada kullanılacağından habersiz 270 bin Facebook kullanıcısı tarafından kullanılmıştır.[63] Kogan, ağ analizi yöntemleri aracılığı ile (arkadaşlar, ilgi alanları, beğeniler) başlangıçtaki 270 bin kullanıcıdan toplamda 50 milyon kullanıcının verilerine ulaşabilmiştir. Daha yakın zamanda, bir grup siyaset bilimci metin tabanlı makine öğrenimi yöntemlerini kullanarak ABD Dışişleri Bakanlığı'nın 1971 yılından itibaren yürüttüğü yazışmaların tasniflendirme paternlerini analiz etmiştir.[64] Bu yazışmalar ABD Dışişleri Bakanlığı ile yabancı bir ülkedeki ABD diplomatik misyonu arasındaki yazışmaları içermiştir. Araştırmacılar, milyonlarca yazışmanın içeriğini inceleyerek, 'gizli', 'özel', 'sınırlı resmi kullanım için' ya da 'tasnif dışı' şeklinde etiketlenen yazışmalarda hangi kelime kombinasyonlarının kullanılma olasılığının yükseldiğini tespit etmiştir. Söz konusu çalışma insan hatasının gizli bilgilerin yanlış tasnif edilmesinde ve sonuçta çok sayıda gizli dökümanın tasnif dışı bırakılmasında önemli ölçüde rol oynadığını ortaya çıkarmıştır. En önemlisi, bahsi geçen çalışma bir belgenin gizli olup olmadığının belirlenmesinde istikrarsız kuralların olduğunu göstermiştir. Araştırmacılara göre bu durum, hem diğer devletler tarafından makine öğrenimi araçlarının kullanılarak tasnif dışı ABD arşivleri aracılığı ile gizli bilgilerin bulunmasına hem de sivil analistlerin aynı veri havuzundan faydalanarak gizli bilgileri kamuya sızdırmasına imkan tanıyacak şartları yaratmaktadır. Belirtilen üç gelişmenin tümü hem devletlerin hem de sivillerin nasıl OSINT'in mağduru olabildiğini ve hiçbir 'tarafın' bu geniş analitik okyanusta gerçek anlamda bir üstünlüğe sahip olamadığını göstermektedir.

Devletlerin organize şiddetin tek meşru kullanıcısı olduğu şeklindeki Weberyan mantık takip edilerek, aynı husus gizlilik alanına da uygulanabilir. Genellikle devletlerin organize ve kurumsal gizliliğin tek meşru sahibi olduğu düşünülmektedir. Demokrasilerde ve otoriter sistemlerde seçmenler, birbirine benzer şekilde, devletlerin milli güvenliğe ilişkin büyük miktarda istihbaratın toplanması, güvenli şekilde işlenmesi ve de bu bilgilerin rakiplerin erişiminden korunması konularında gerekli imkan ve kabiliyetlere sahip olması gerektiğini düşünmektedir. Ancak, demokrasileri otoriter sistemlerden ayıran istihbaratın gözetimi ve bahsi geçen gizliliğin kötüye kullanılmasının engellenmesi hususlarıdır.[65] Vatandaşlar ve iç hedefler böylesine kötüye kullanımların sıklıkla en korumasız ve en kolay hedefleri olmakta, bu durum devletlerin güvenliğin sağlanması için kullandığı karşı istihbarat ve gizlilik biriktirme araçlarının ülke içindeki muhaliflerin izlenmesi ve bastırılması için de kullanılabiliyor olmasından kaynaklanmaktadır.[66] Öte yandan, daha fazla şeffaflık ve hesap verebilirlik istihbarat servislerinin hızını ve operasyon menzillerini azaltmakta, bu durum milli güvenlik üzerinde olumsuz etki yaratmaktadır. Söz konusu durum mahremiyet ve güvenlik arasında orta noktayı bulmaya çalışanlar için kalıtsal nitelikli bir ikilemi üretmektedir. Bir yandan, kontrol edilmeyen istihbarat teşkilatları geniş gözetleme altyapısını kötüye kullanarak bir ülkenin demokratik işleyişlerine zarar vermekte, öte yandan, istihbarat faaliyetlerini daha şeffaf hale getiren politikaların çoğu istihbarat servislerinin etkinliğini, faaliyetlerinin kapsamını ve caydırıcılık kapasitesini devre dışı bırakabilmektedir.[67]

Demokrasilerde gözetime karşı olarak yaygın argüman istihbaratın normal yargı ve yasama aygıtları ile sınırlandırılabilecek sıradan bir siyasi alan olmadığı yönündedir.[68] Ülkeler, istihbarat faaliyetlerinin uzun hukuksal ve parlamenter delil tespitine ve denetlemeye konu edilmesi ile a) kritik öneme sahip bir istihbaratı kaçırabilir, b) otoriter devletlerin istihbarat servisleri karşısında hassas bilgi ile ilintili göreli üstünlüğü kaybedebilir, c) bir saldırının engellenmesinde başarısız olabilir ve bu durum istihbaratın kötüye kullanımı ile karşılaştırıldığında daha ciddi bir kamuoyu tepkisi yaratabilir.[69] Bahsi geçen sınırlamaların hiçbiri (ya da pek azı) ile ilgilen-

63 Carole Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," The Guardian, Mart 18, 2018, sec. News, http://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

64 Renato Rocha Souza et al., "Using Artificial Intelligence to Identify State Secrets," ArXiv 1611.00356 (Kasım 1, 2016), http://arxiv.org/abs/1611.00356.

65 Michael P. Colaresi, Democracy Declassified: The Secrecy Dilemma in National Security (Oxford, UK: Oxford University Press, 2014).

66 Zachary K. Goldman and Samuel J. Rascoff, Global Intelligence Oversight: Governing Security in the Twenty-First Century (Oxford: Oxford University Press, 2016), 14.

67 Goldman and Rascoff, 72.

68 Daniel Baldino, ed., Democratic Oversight of Intelligence Services (Sydney: Federation Press, 2010), 3.

69 Johnson, The Oxford Handbook of National Security Intelligence, 80.

mek zorunda olmayan otoriter bir devlet küresel istihbarat rekabetinin gerekliliklerinin karşılanmasında ve demokrasiler karşısında üstünlük elde etmede kısa vadede daha atik ve hızlı hale gelebilmektedir. Yukarıda sözü edilen argüman bu ve benzeri yönde içeriğe sahiptir. Söz konusu argüman ile ilgili iki esas sorun bulunmaktadır. Birincisi, Desch[70] ve Reiter (et. al.)[71] tarafından ortaya konulduğu üzere, demokrasiler de büyük miktarlarda bilgiyi kamuoyundan gizli tutabilmekte ve ayrıca gözetim mekanizmalarını başarıyla engelleyebilmektedir. Tekrarlayan örneklerin gösterdiği gibi, demokrasiler, otokrasiler kadar tek taraflı ya da dikkatleri başka yöne çekmeye yönelik savaşlara girebilmekte ve bunu yaparken kamuoyunu yanıltmaktadır.[72] İkinci olarak, gözetim mekanizmalarının ya da istihbaratın kötüye kullanılmasına karşı alınan önlemlerin demokrasileri otokrasiler karşısında stratejik olarak daha az avantajlı hale getirdiğini gösteren bir kanıt yoktur. Birkaç aykırı görüş dışında literatürde oluşmuş genel trend hala güçlüdür. Açık bilgi ve daha geniş 'fikirler piyasasına' bağlı olarak, demokrasiler daha az yanlış hesaplama ya yanlış algılama eğilimi göstermekte, birbiriyle savaşmamakta, iç savaşlardan ve iç huzursuzluklardan daha az zarar görmekte ve giriştikleri savaşların çoğunu kazanmaktadır.[73] Sonuç olarak, sorun nedir?

Alınan önlemlerin çoğunlukla istihbaratı etkisiz kılan faktörlerden olmaması gerçeğine bağlı olarak, istihbaratın gözetimi ve stratejik dezavantaj arasındaki nedensel mekanizma son derece zayıftır.[74] Hızlı ve iyi istihbaratın iki farklı husus olması gibi, hızlı istihbarat her zaman iyi politikalara yol açmamaktadır. Demokrasiler alınan önlemler ile koyulan sınırlar sonucunda zaman ya da menzil kaybetse de, söz konusu açığı iki alanda kapatmaktadır. İlk olarak, istihbarat ile ilgili önlemlere ve gözetim mekanizmalarına bağlı olarak, istihbarat servisleri gözetleme-izleme faaliyetlerinin mantıksal temellerini, muhakemesini ve stratejik yararlarını test eden bir gözden geçirme sisteminden geçmek zorundadır.[75] Söz konusu ek gözetim katmanının hataları ya da yanlış kararları erkenden tespit etme olasılığı bulunmakta, bu olasılık istihbarat servislerinin maliyetli bir hata ya da başka bir ülke ile diplomatik gerilimin tırmanmasına yol açacak bir uluslararası hadise ile yüzleşmesini engelleyebilmektedir. İkinci olarak, demokrasiler bir istihbarat topluluğunun ideolojik saflığından daha çok yeteneklerin ve kapasitenin teknik düzeyi ile ilgilenme eğilimi göstermektedir. Çoğu otoriter rejimde, istihbaratta etkili pozisyonlar komiser olarak atananlar ile çok az ve yetersiz operasyonel/teknik uzmanlığı bulunan akrabalar ile doldurulmaktadır.[76] Atamalarda yeteneklerin ikincil öneme sahip olduğu ideoloji ile yönlendirilen istihbarat servislerinde, hızlı karar alımı çoğu zaman maliyetli yanlış hesaplamalar ile sonuçlanmakta, söz konusu maliyetler gözetim mekanizmalarının ve önlemlerin eksikliğinden doğan hız ve menzil üstünlüklerini geçersiz kılmaktadır. Dolayısıyla, demokrasiler daha yavaş istihbarat kararları alsa da, bu kararlar genellikle daha teknokrat eğilimli topluluklar tarafından, karar alma, yargı organları ve teknokratlar arasında daha iyi bir etkileşim ile ve sonuçta daha iyi formüle edilmiş ve kriz çıkarma riski daha düşün politikalar üretecek şekilde alınmaktadır.

Aynı kapasite içinde, devletlerin sıfır toplamlı bilgi ortamında 'gizliliği maksimize eden' aktörler olduğu düşüncesine dayanan 'istihbarat ikilemi' iddia edildiğinden daha az öneme sahip olabilir. İlk olarak, devletler uygun istihbaratı sahip oldukları teknik, insan ve bürokratik altyapı ile işlemekte ve depolamaktadır.[77] Gizli bilgileri altyapılarının izin verdiği ölçütlerin ötesinde topladıklarında yabancı casusluğa karşı koruyamayacak olmalarından dolayı devletler istihbaratı maksimize eden aktörler olamamaktadır. Bu sebeple, devletler elde etmek için altyapılarını kullandıkları bilgi türlerini önceliklendiren ve böylece karar alımı için anlamlı şekilde işlemeye ve bu gizli bilgileri yabancı casusluk faaliyetleri kar-

70 Michael C. Desch, "Democracy and Victory: Why Regime Type Hardly Matters," International Security 27, no. 2 (Ekim 1, 2002): 5–47, https://doi.org/10.1162/016228802760987815.

71 Dan Reiter, Allan C. Stam, and Alexander B. Downes, "Another Skirmish in the Battle over Democracies and War," International Security 34, no. 2 (Eylül 30, 2009): 194–204, https://doi.org/10.1162/isec.2009.34.2.194.

72 Erich Weede, "Democracy and War Involvement," Journal of Conflict Resolution 28, no. 4 (Aralık 1, 1984): 649–64, https://doi.org/10.1177/0022002784028004004; Kenneth A. Schultz, "Do Democratic Institutions Constrain or Inform? Contrasting Two Institutional Perspectives on Democracy and War," International Organization 53, no. 2 (ed 1999): 233–66, https://doi.org/10.1162/002081899550878.

73 Johnson, The Oxford Handbook of National Security Intelligence, 167; Baldino, Democratic Oversight of Intelligence Services, 45; David Lyon, Kirstie Ball, and Kevin D. Haggerty, Routledge Handbook of Surveillance Studies (New York: Routledge, 2012), 51.

74 Hans Born and Ms Marina Caparini, Democratic Control of Intelligence Services: Containing Rogue Elephants (Ashgate Publishing, Ltd., 2013), 4.

75 Baldino, Democratic Oversight of Intelligence Services, 89.

76 Johnson, The Oxford Handbook of National Security Intelligence, 243.

77 Colaresi;, Democracy Declassified, 51.

şısında pareto-optimum bir maliyette tutmaya çalışan gizliliği optimize eden aktörlerdir.

OSINT söz konusu denklemi büyük ölçüde değiştirmiştir. Yüksek kaliteli istihbarat artık yalnızca devletlerden ve güçlü büyük şirketlerden oluşan küçük bir tekelin elinde değildir. Gazeteciler, sivil toplum kuruluşları ve sivil vatandaşlar da, artık önceleri gizli olarak tasniflenen bilgiye erişebilmekte, bu bilgiyi toplayabilmekte, işleyebilmekte ve dağıtabilmektedir.

İstihbaratın ticarileşmesi – gözetleme ekipmanları, sosyal medya analiz servisleri ve programlama devrimi – uluslararası istihbarat rekabetinde yeni güç kaynaklarının ortaya çıkmasına yol açmıştır. Hackerların varlığı artık eskimiş bir haberdir ve söz konusu devlet dışı aktörler halihazırda gerek bağımsız gerekse devlet destekli stratejik rekabette olağan değişkenler haline gelmiştir. OSINT'in gelişmekte olan yeni güç kaynakları hackerların kodlama dehasına sahip olma ihtiyacı duymamaktadır. Ticari uydu görselleri, kolaylıkla satın alınabilen insansız hava araçları, sosyal medya analiz platformları ve biraz boş zaman yeni küresel OSINT sınıfının oluşmasına yardımcı olmuş, bu durum bilgi siyaseti üzerinde orantısız bir etki ile gerçekleşmiştir. Günümüzde, ortalama teknik bilgi düzeyine, temel seviyeden dahi az programlama becerilerine ve dijital medya verilerinin keşfi için meraklı gözlere sahip istekli bireyler küresel kitle kaynaklı OSINT ağının parçası olabilmektedir.

Günümüzde devletler istihbarat rakipleri olarak yalnızca diğer devletler, büyük şirketler ya da hackerlar ile ilgili değil, aynı zamanda bahsi geçen küresel vatandaş gazeteciler, OSINT heveslileri ve sivil veri analizi girişimleri ile ilgili de düşünmek zorundadır. Sözü edilen ağ, devlet destekli bilgi harekatlarının desteklenmesinde ya da bunlara karşı konulmasında, propagandada ve siyasi iletişim harbinde giderek daha etkili hale gelmekte, Bellingcat'in MH17 uçağı ile ilgili adli bilim çalışmasının da gösterdiği gibi, sıklıkla önemli uluslararası öneme sahip kanıtları gün yüzüne çıkarabilmektedir.[78] Devlet-toplum ilişkilerinde gizliliğin rolüne bağlı olarak, devletlerin dijital kitle kaynaklı OSINT'e nasıl yanıt vermesi gerektiği büyük oranda bir rejim türü sorusudur. Normal şartlarda, otoriter rejimlerin kritik bilginin büyüyen demokratikleşmesi karşısında en savunmasız aktörler olduğu düşünülebilir. Sonuçta, böylesi rejimler bilginin büyük kısmını kamuoyundan saklamakta, siyasi bilginin paylaşımında çok az miktarda devlet-toplum etkileşimine sahip olmakta ve istihbaratın kötüye kullanımı ile ilgili hiçbir gözetim mekanizmasını işletmemektedir. Bu rejimler sıklıkla kendi vatandaşları üzerinde ve özellikle karşıt görüşlüleri ve muhalifleri bastırmayı amaçlayarak casusluk faaliyetleri yürütmekte, ve karşıt önlemlerin, kontrol ve denge mekanizmalarının yokluğuna bağlı olarak, milli güvenlik ve istihbarat meselelerinde yapısal yanlış yönetim ve yolsuzluktan zarar görmektedir. Tersine, her ne kadar demokrasiler de ifşa ve sızıntıların yarattığı güçlüklerden zarar görse de, sözü edilen zararların özgür ve adil seçimleri, işleyen bir parlamentoyu ve kamu gözetimi ile ayıplama mekanizmalarını da içeren demokratik yapılara bağlı olarak minimum seviyede kaldığı değerlendirilmektedir.

İstihbaratın gözetimi ve koruma mekanizmaları ile ilgili en büyük eleştiri bu faaliyetlerin istihbarat servislerinin teknoloji ile ne yaptığının anlaşılmasını düzgün bir şekilde anlaşılmasını sağlayacak teknik bilgi birikimi ve arkaplandan yoksun oldukları yönündedir.[79] Bu durumun en iyi örneğini Facebook ile ilgil verdiği ifade sırasında Mark Zuckerberg'e sorulan arkaik ve duyarsız sorular oluşturmuştur.[80] OSINT'in gözetim mekanizmalarına sağlayabileceği önemli bir katkı, söz konusu mekanizmaların çoğunun kendi başlarına gerçekleştiremediği halihazırda mevcut analizin sağlanmasıdır. Açık kaynaklı araçların yöntemli bir analizi aracılığıyla, teknik olarak yeterli bir ağ tabanlı kitle daha kurumsal ancak daha yavaş işleyen gözetim kurumlarını, gizliliğin kötüye kullanımı ile ilgili veri, kanıt ve izleme ölçüleri ile destekleyebilir. Ancak, OSINT otoriter rejimlerin demokratikleşmesini hızlandırabilecek ya da mümkün kılabilecek midir? Bu denklemde gerçek hayatta daha fazla değişkenin bulunması sebebiyle söz konusu olasılık güçlü görünmemektedir. Otoriter rejimler OSINT faaliyetleri sonucunda daha büyük miktarlarda siyasi sırları kaybetse de, bu durumun rejim ya da hükümet değişikliğini, ya da bu geçişi olanaklı kılacak kadar yeterli bir mobilizasyonu yaratabilmesi için bir neden bulunmamaktadır.

Çoğunlukla, demokratik ülkelerdeki sızıntı ve ifşaların – her

[78] MH17 - The Open Source Investigation, Three Years Later," Bellingcat, Temmuz 17, 2017, https://www.bellingcat.com/news/uk-and-europe/2017/07/17/mh17-open-source-investigation-three-years-later/.

[79] Amy B. Zegart, "The Domestic Politics of Irrational Intelligence Oversight," Political Science Quarterly 126, no. 1 (Mart 1, 2011): 1–25, https://doi.org/10.1002/j.1538-165X.2011.tb00692.x.

[80] Emily Stewart, "Lawmakers Seem Confused about What Facebook Does — and How to Fix It," Vox, Nisan 10, 2018, https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations.

ne kadar küçük olursa olsunlar – hükümetlerin istifalarına ya da hükümete olan desteğin büyük miktarda azalmasına sebep olma olasılığı otokrasiler ile karşılaştırıldığında daha fazladır. Tüm kayıplarına rağmen, otoriter devletlerin ifşalar sonucunda karşılaşılabilecek muhtemel zararları sınırlayacak ya da caydıracak sert güç kullanımı taktiklerine başvurma eğilimleri diğer devletlere göre daha ağırlıklıdır.[81] Tüm rejim türlerinde yanlış yönetim ve hesaplamalar ile ilgili ifşaların eleştirisi ve söz konusu ifşalara kamuoyunun tepkisi benzerlik gösterse de, bunların siyasi baskıya dönüşebilme ve bir hükümeti siyasi olarak sarsabilme yetenekleri yapısal olarak birbirinden farklıdır.

O halde, OSINT çağında rejim tipi ile dış politikadaki etkinlik arasındaki ilişki nasıl değerlendirilmelidir? Bu hususta ana akım görüş, alternatif bilginin erişilebilir olmasına bağlı olarak, OSINT'in yaygınlaşmasının devletler için kamuoyunu ya da uluslararası hedef kitlesini aldatmayı zorlaştıracağı yönündedir. En iyi şekliyle, OSINT'in tüm internet ortamında isabetli bilginin daha iyi akışını ve verilen bilgilerin doğruluğunu uygun şekilde kontrol etmeyi mümkün kılarak devletler tarafından yönlendirilen dezenformasyon girişimlerinin propaganda etkilerini geçersiz kılacağı beklenmektedir. Bu durumun, sonuçta OSINT aracılığıyla gerçekleşecek ifşaların göz önünde bulundurulmasıyla, dış politikanın daha dikkatlice oluşturulmasına ve bilinçli dezenformasyon ile temellendirilmemesine sebep olacağı düşünülmektedir. Ancak, belirtilen durum her zaman için geçerli değildir. Bunun sebeplerinden birisi, kriz ve gerginliğin tırmandığı zamanlarda hükümet ve siyasi liderlik için daha büyük bir desteğe ve bu desteğin mobilizasyonuna dönüşen bir seçmen refleksi olan 'toparlanma etkisidir' (rallying effect).[82] Söz konusu etki, çoğu krizin kalıtsal olarak kısa süreli olmasına bağlı olarak, demokrasilerin ve otokrasilerin kısa vadede birbirine benzer şekilde hızlı ve muhtemelen yanlış hesaplanmış kararlar alma olasılığını artırmakta ve bu söz konusu rejimlerin OSINT ile yönlendirilen bilgi ortamında hareket etmelerine rağmen yaşanmaktadır. Gözlemsel çalışmalar ile kanıtlandığı üzere, otoriter devletler de dış politikada hedef kitle açısından zarar görmekte ve demokratik dış politikalar otokrasiler ile karşılaştırıldığında bilginin kullanımının kısıtlandığı ortamlarda her zaman etkili olamamaktadır.[83]

[81] Michael M. Andregg and Peter Gill, "Comparing the Democratization of Intelligence," Intelligence and National Security 29, no. 4 (Temmuz 4, 2014): 487–97, https://doi.org/10.1080/02684527.2014.915174.

[82] John R. Oneal and Anna Lillian Bryan, "The Rally 'round the Flag Effect in U.S. Foreign Policy Crises, 1950–1985," Political Behavior 17, no. 4 (Aralık 1, 1995): 379–401, https://doi.org/10.1007/BF01498516.

[83] Weeks, "Autocratic Audience Costs"; Branislav L. Slantchev, "Politicians, the Media, and Domestic Audience Costs," International Studies Quarterly 50, no. 2 (June 1, 2006): 445–77, https://doi.org/10.1111/j.1468-2478.2006.00409.x; Jessica Chen Weiss, "Authoritarian Signaling, Mass Audiences, and Nationalist Protest in China," International Organization 67, no. 1 (January 2013): 1–35, https://doi.org/10.1017/S0020818312000380.

# Sonuç: Uluslararası Güvenlik için Çıkarımlar

Dijital OSINT ile ilgili yaygın tartışma esas olarak teknolojinin devlet sırlarının doğasını ve devlet işlerinde gizliliğin rolünü nasıl değiştirdiği ile ilgilenmektedir. Bir denge sağlanana kadar, iletişim teknolojileri devletler ve ilgili toplumlar arasında bir muharebe sahası olarak kalmaktadır. İletişim alanında geçmişteki teknolojik ilerlemelerde olduğu gibi – yazılı basın, radyo, televizyon, uydular — internet tabanlı iletişim de önemli toplumsal kuvvetlerin daha fazla özgürlük alanları için mücadele etmesini ve devletlerin söz konusu kuvvetleri bastırmasını olanaklı hale getirmektedir. Devletin bakış açısından OSINT iki sonuca yol açacaktır. Kısa vadeli sonuç yeni iletişim araçları aracılığı ile gerçekleşen ifşaların ve sızıntıların engellenmesi amacıyla askeri ve istihbarat politikalarının gözden geçirilmesi olacaktır. Bu gözden geçirme, önemli siyasi sırları kriptolama ve depolama yollarını değiştirmeyi de içerecek şekilde, akıllı telefon kullanımından sosyal medyada bulunmaya kadar basit bir takım davranışsal ayarlamaları kapsayacaktır. Ancak, uzun vadede sivil vatandaşlar tarafından yönlendirilen OSINT girişimleri hükümet sırlarını ifşa etmeye ve özellikle kriz ve aciliyet zamanlarında hikayeye hakim olmasını engellemeye devam edecektir. Demokrasiler ve otoriter devletler birbirine benzer şekilde olaylar ile ilgili kendi versiyonlarını öne sürmeyi deneyecek, ancak önemli olayların çerçevelenmesinde ve anlatımında bir tekel oluşturmanın giderek zorlaştığını göreceklerdir. Bu durum hükümetleri ya alternatif bilgi ile ilgili kamusal mekanizmaları bastırmaya ya da engellemeye, ya da devlet işlerinde sırlardan yararlanma yollarını değiştirmeye zorlayacaktır. Bu konudaki örneklerden birisi basının, iç sızıntıların ve kamuoyu baskısının, Bush dönemi tutuklu tesislerinin Obama yönetimi tarafından kapatılmasına ve sonuç olarak ABD kongresinin söz konusu tesisleri yasa dışı ilan etmesine sebep olmasıdır. Öte yandan, MH17 uçağının Rusya tarafından düşürülmesine dair ifşalar sonucundaki benzer baskılar, çatışma alanlarında askerlerin cep telefonu kullanımının yasaklanması dışında, Rus yönetiminin davranışını değiştirmemiştir. Benzer olarak, Rus askerlerinin 2014 yılında Kırım'da çektiği selfi fotoğraflarının ifşası Rusya'nın Ukrayna'da giriştiği harekatların gidişatını ve daha geniş isteklerini değiştirmemiştir.

Dolayısıyla, büyük açık kaynaklı analiz faaliyetlerinin yaygınlaşmasının bütün devletler üzerinde aynı etkiyi gösterme olasılığının düşük olduğu değerlendirilmektedir. Aynı zamanda OSINT'in bütün devletleri gizliliğe daha az güvenmeye zorlayacağı ile ilgili kanıt bulunmamaktadır. Büyük olasılıkla, dijital OSINT hedef kitle zararlarına karşı yüksek toleransı olan devletler (otokrasiler) ile söz konusu zararlara daha duyarlı olan devletler (demokrasiler) arasında bir 'gizlilik asimetrisi' yaratacaktır. Sızıntılar, ifşalar ve sivil vatandaşlar tarafından yöneldirilen çabalar baskı, gözaltı, hapis ve sansür gibi iç politika araçları ile geçersiz hale getirebileceğinden, otokrasiler dijital kitle kaynaklı OSINT'i genel düzen içinde giderek daha önemsiz bir husus olarak (belki kritik harekatlar dışında) değerlendirecektir. Öte yandan, demokrasiler, farklı bir rota izlemek zorunda kalacaktır. Söz konusu rota aşağıdaki hususları içeren alternatif siyasa seçeneklerinden oluşacaktır:

- Kamu diplomasisi teşkilatlarının tek yönlü bir tutumdan (devlet görüşünün geniş bir kitleye ulaştırılması gibi), kamuoyu görüş ve hassasiyetlerinin hükümet organlarına iletilmesini içerecek çok yönlü bir tutuma geçecek şekilde yeniden düzenlenmesi, böylece bu organların dijital açık kaynaklı ortama uyumlarının sağlanması.
- Sivil kitle kaynaklı OSINT'in resmi istihbarat çalışmalarına bir ölçüde dahil edilmesi. Bu husus, halihazırda kamuoyu tarafından bilinmeyen sırların miktarının az olduğu, temsil oranı daha yüksek ve daha özgür siyasi sistemler için daha az risk taşımaktadır. Tersine, bahsi geçen düzenleme, 'gizlilik biriktirme' eğilimi gösteren ve kamusal OSINT platformları ile işbirliği yapılması durumunda kaybedecek (sızdıracak) fazla miktarda gizli bilgiye sahip otoriter devletler için daha zordur.
- İstihbarat uygulamalarında yargı ve yasama organlarının daha fazla gözetleme yapmasına izin verilmesi. İstihbarat operasyonlarının önlem mekanizmalarına daha açık ve bu mekanizmalar ile daha fazla işbirliği yapar hale getirilmesiyle, istihbarat servisleri sırlarından bazılarının OSINT araçları ile ifşa olması durumunda hedef kitle maliyetlerinden daha az zarar görebilecektir.

Uzun vadede, internet ve sosyal medya platformları, devletlerin bilgi akışı üzerindeki hakimiyetini tekrar kazandığı bir iş dengesi üzerine yerleşecek, bu durum devletlerin ya büyük teknoloji şirketlerini kontrol etmesi ya da bu şirketler ile sızıntı ve ifşaları minimize eden hukuki alanları tanımlayan bir güç paylaşımı anlaşmasına ulaşması ile gerçekleşecektir. Söz konusu gelişme gerçekleşene kadar, sızıntı ve ifşalar devam ederek devletleri siviller tarafından yönlendirilen analiz girişimleri karşısında dezavantajlı bir

duruma getirecek, ve ayrıca uluslararası güvenlik rekabeti ile istihbarat teşkilatlarının 'gizlilik savaşlarını' sürükleyecek yeni bir güvenlik ikilemi katmanı yaratacaktır. Öte yandan, demokrasilerde dahi kitle maliyetlerinin abartılması için bir neden bulunmamaktadır. Bu durum özellikle çevrimiçi kitlenin dikkat süresinin her zaman kısıtlı kalması ve siyasi angajman ile doğrudan bağlantısının bulunmamasından kaynaklanmaktadır. Sosyal medya angajmanı gerçek siyasi mobilizasyona nadiren dönüşmekte ve bu durum ancak sosyal medya angajmanının, OSINT çabalarının gerçek değişikliklere yol açtığı siyasi, yargısal ya da yasama ile ilgili bir momentumu yarattığı durumlarda mümkün olabilmektedir. Bu nedenle, OSINT girişiği mücadeleleri seçme konusunda giderek tutumlu olmayı giderek daha uygun bir seçenek bir tutum olarak benimseyecek ve çabalarını daha geniş kamuoyu dikkati ve siyasi momentum yaratacak konulara odaklanarak gerçekleştirecektir.

Sonuçta, gizlilik sona ermemekte, ancak gizlilik ile ilgili anlayış ve düşünce açık bilgi platformlarına bağlı olarak çok hızlı bir şekilde değişmektedir. Devletlerin ve toplumların gizli olarak kabul ettiği olay ve hakikatler artık gizli değildir. Bu durum doğal olarak internette neyin saklanması ve neyin açıklanması gerektiği ile ilgili ve söz konusu sırlar açığa çıktığında oluşacak zararın nasıl sınırlı tutulacağı ile ilgili yeniden düşünmeyi gerektirmektedir. Devletler ve vatandaşlar yeni iletişim ve bilgi bulma platformlarına uyum sağlayana kadar, gizlilik son derece bulanık bir kavram olmaya ve devlet-toplum tartışmasının tüm taraflarını etkilemeye devam edecektir.

# Referanslar


Aid, Matthew M. "All Glory Is Fleeting: Sigint and the Fight Against International Terrorism." *Intelligence and National Security* 18, no. 4 (Aralık 1, 2003): 72–120. https://doi.org/10.1080/02684520310001688880.

Andregg, Michael M., and Peter Gill. "Comparing the Democratization of Intelligence." *Intelligence and National Security* 29, no. 4 (July 4, 2014): 487–97. https://doi.org/10.1080/02684527.2014.915174.

Appel, Edward J. *Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence, Second Edition*. CRC Press, 2014.

Apuzzo, Matt. "Who Will Become a Terrorist? Research Yields Few Clues." *The New York Times*, Aralık 21, 2017, sec. World. https://www.nytimes.com/2016/03/28/world/europe/mystery-about-who-will-become-a-terrorist-defies-clear-answers.html.

Asghar, Muhammad Zubair, Shakeel Ahmad, Afsana Marwat, and Fazal Masud Kundi. "Sentiment Analysis on YouTube: A Brief Survey." *ArXiv* 1511.09142 (November 29, 2015). http://arxiv.org/abs/1511.09142.

Bacastow, Todd S., and Dennis Bellafiore. "Redefining Geospatial Intelligence." *American Intelligence Journal* 27, no. 1 (2009): 38–40.

Baldino, Daniel, ed. *Democratic Oversight of Intelligence Services*. Sydney: Federation Press, 2010.

Born, Dr Hans, and Ms Marina Caparini. *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Ashgate Publishing, Ltd., 2013.

Cadwalladr, Carole. "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower." *The Guardian*, Mart 18, 2018, sec. News. http://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." Vox, Mart 23, 2018. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

Chen, Feng, Pan Deng, Jiafu Wan, Daqiang Zhang, Athanasios V. Vasilakos, and Xiaohui Rong. "Data Mining for the Internet of Things: Literature Review and Challenges." *International Journal of Distributed Sensor Networks* 11, no. 8 (Ağustos 18, 2015): 431047. https://doi.org/10.1155/2015/431047.

Chen, Hsinchun. *Dark Web: Exploring and Data Mining the Dark Side of the Web*. Integrated Series in Information Systems. New York: Springer-Verlag, 2012. //www.springer.com/gp/book/9781461415565.

Choi, Moonsun, Michael Glassman, and Dean Cristol. "What It Means to Be a Citizen in the Internet Age: Development of a Reliable and Valid Digital Citizenship Scale." *Computers & Education* 107 (Nisan 1, 2017): 100–112. https://doi.org/10.1016/j.compedu.2017.01.002.

Chulov, Martin. "Syria Attack: Nerve Agent Experts Race to Smuggle Bodies out of Douma." *The Guardian*, Nisan 12, 2018, sec. World news. http://www.theguardian.com/world/2018/apr/12/syria-attack-experts-check-signs-nerve-agent.

Colaresi;, Michael P. *Democracy Declassified: The Secrecy Dilemma in National Security*. Oxford, UK: Oxford University Press, 2014.

Collins, Dylan. "A US Airstrike Which Killed 38 People Allegedly Hit a Peaceful Mosque in a Syrian Village." *Business Insider*, Nisan 18, 2017. http://www.businessinsider.com/us-airstrike-allegedly-hit-a-peaceful-mosque-in-a-syrian-village-2017-4.

Davies, Philip H. J. "Intelligence Culture and Intelligence Failure in Britain and the United States." *Cambridge Review of International Affairs* 17, no. 3 (October 1, 2004): 495–520. https://doi.org/10.1080/0955757042000298188.

De Stefano, Valerio. "The Rise of the Just-in-Time Workforce: On-Demand Work, Crowdwork, and Labor Protection in the Gig-Economy." *Comparative Labor Law & Policy Journal* 37 (2016 2015): 471.

Desch, Michael C. "Democracy and Victory: Why Regime Type Hardly Matters." *International Security* 27, no. 2 (October 1, 2002): 5–47. https://doi.org/10.1162/016228802760987815.

Dover, Robert, Michael S. Goodman, and Claudia Hillebrand, eds. *Routledge Companion to Intelligence Studies*. Routledge, 2013.

Dudczyk, J., J. Matuszewski, and M. Wnuk. "Applying the Radiated Emission to the Specific Emitter Identification." In *15th International Conference on Microwaves, Radar and Wireless Communications (IEEE Cat. No.04EX824)*, 2:431–434 Vol.2, 2004. https://doi.org/10.1109/MIKON.2004.1357058.

Evans, Jacqueline R., Christian A. Meissner, Susan E. Brandon, Melissa B. Russano, and Steve M. Kleinman. "Criminal versus HUMINT Interrogations: The Importance of Psychological Science to Improving Interrogative Practice." *The Journal of Psychiatry & Law* 38, no. 1–2 (Mart 1, 2010): 215–49. https://doi.org/10.1177/009318531003800110.

Fisher, Max. "Did Ukraine Rebels Take Credit for Downing MH17?" Vox.com, July 17, 2014. https://www.vox.com/2014/7/17/5913089/did-this-ukrainian-rebel-commander-take-credit-for-shooting-down-the.

Gettleman, Jeffrey. "Congo: Rapes by Civilians Rise Sharply, Study Says." *The New York Times*, Nisan 14, 2010, sec. Africa. https://www.nytimes.com/2010/04/15/world/africa/15briefs-congo.html.

Gibney, Mark. "The Downing of MH17: Russian Responsibility?" *Human Rights Law Review* 15, no. 1 (Mart 1, 2015): 169–78. https://doi.org/10.1093/hrlr/ngu036.

Giridharadas, Anand. "Ushahidi - Africa's Gift to Silicon Valley: How to Track a Crisis." *The New York Times*, Mart 13, 2010, sec. Week in Review. https://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html.

Glassman, Michael, and Min Ju Kang. "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)." *Computers in Human Behavior* 28, no. 2 (Mart 1, 2012): 673–82. https://doi.org/10.1016/j.chb.2011.11.014.

Goldman, Zachary K., and Samuel J. Rascoff. *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford: Oxford University Press, 2016.

Greenemeier, Larry. "DARPA Verigames Crowdsourced Formal Verification (CSFV) Project." *Scientific American*, June 9, 2015. https://www.scientificamerican.com/citizen-science/darpa-verigames-crowdsourced-formal-verification-csfv-project/.

Gunitsky, Seva. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13, no. 1 (Mart 2015): 42–54. https://doi.org/10.1017/S1537592714003120.

Gutierrez, Pablo, and Paul Torpey. "How Digital Detectives Say They Proved Ukraine Attacks Came from Russia." *The Guardian*, Şubat 17, 2015, sec. World news. http://www.theguardian.com/world/2015/feb/17/ukraine-russia-crossborder-attacks-satellite-evidence.

Harris, Mark. "How A Lone Hacker Shredded the Myth of Crowdsourcing." WIRED, September 2, 2015. https://www.wired.com/2015/02/how-a-lone-hacker-shredded-the-myth-of-crowdsourcing/.

Hern, Alex. "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases." *The Guardian*, Ocak 28, 2018, sec. Technology. http://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

Johnson, Loch K. *The Oxford Handbook of National Security Intelligence*. Oxford University Press, 2010.

Khalil, Osamah F. *America's Dream Palace: Middle East Expertise and the Rise of the National Security State*. Cambridge, Massachusetts: Harvard University Press, 2016.

Klausen, Jytte. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism* 38, no. 1 (Ocak 2, 2015): 1–22. https://doi.org/10.1080/1057610X.2014.974948.

Landau, S. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security Privacy* 11, no. 4 (July 2013): 54–63. https://doi.org/10.1109/MSP.2013.90.

Larkin, Sean P. "The Age of Transparency." *Foreign Affairs*, Nisan 18, 2016. https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency.

Legro, Jeffrey W. "Culture and Preferences in the International Cooperation Two-Step." *American Political Science Review* 90, no. 1 (Mart 1996): 118–37. https://doi.org/10.2307/2082802.

Liptak, Andrew. "Strava's Fitness Tracker Heat Map Reveals the Location of Military Bases." *The Verge*, Ocak 28, 2018. https://www.theverge.com/2018/1/28/16942626/strava-fitness-tracker-heat-map-military-base-internet-of-things-geolocation.

Lohr, Steve. "In Relief Work, Online Mapping Yet to Attain Full Potential." *The New York Times*, Mart 28, 2011, sec. Business Day. https://www.nytimes.com/2011/03/28/business/28map.html.

Lyon, David, Kirstie Ball, and Kevin D. Haggerty. *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012.

Masciandaro, Donato. "Financial Supervisory Unification and Financial Intelligence Units." *Journal of Money Laundering Control* 8, no. 4 (October 1, 2005): 354–70. https://doi.org/10.1108/13685200510620858.

McFate, Montgomery. "The Military Utility of Understanding Adversary Culture." Arlington, VA: DTIC, Office of Naval Research, Ocak 2005. http://www.dtic.mil/docs/citations/ADA479862.

McFate, Montgomery, and Steve Fondacaro. "Cultural Knowledge and Common Sense." *Anthropology Today* 24, no. 1 (Şubat 1, 2008): 27–27. https://doi.org/10.1111/j.1467-8322.2008.00562.x.

"MH17 - The Open Source Investigation, Three Years Later." bellingcat, July 17, 2017. https://www.bellingcat.com/news/uk-and-europe/2017/07/17/mh17-open-source-investigation-three-years-later/.

Moore, Rowan. "Forensic Architecture: The Detail behind the Devilry." *The Observer*, Şubat 25, 2018, sec. Art and design. http://www.theguardian.com/artanddesign/2018/feb/25/forensic-architects-eyal-weizman.

Mueller, Hannes, and Christopher Rauh. "Reading Between the Lines: Prediction of Political Violence Using Newspaper Text." *American Political Science Review*, Aralık 2017, 1–18. https://doi.org/10.1017/S0003055417000570.

Oneal, John R., and Anna Lillian Bryan. "The Rally 'round the Flag Effect in U.S. Foreign Policy Crises, 1950–1985." *Political Behavior* 17, no. 4 (Aralık 1, 1995): 379–401. https://doi.org/10.1007/BF01498516.

Pringle, Robert W. "The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989." *International Journal of Intelligence and CounterIntelligence* 16, no. 2 (Nisan 1, 2003): 280–89. https://doi.org/10.1080/08850600390198706.

Reiter, Dan, Allan C. Stam, and Alexander B. Downes. "Another Skirmish in the Battle over Democracies and War." *International Security* 34, no. 2 (September 30, 2009): 194–204. https://doi.org/10.1162/isec.2009.34.2.194.

Richelson, Jeffrey T. "MASINT: The New Kid in Town." *International Journal of Intelligence and CounterIntelligence* 14, no. 2 (Nisan 1, 2001): 149–92. https://doi.org/10.1080/088506001300063136.

Rudner, Martin. "Britain Betwixt and Between: Uk SIGINT Alliance Strategy's Transatlantic and European Connections." *Intelligence and National Security* 19, no. 4 (Aralık 1, 2004): 571–609. https://doi.org/10.1080/0268452042000327528.

Sanchez, Andy. "Leveraging Geospatial Intelligence (GEOINT) in Mission Command." Arlington, VA: DTIC, Office of Naval Research, Mart 21, 2009. http://www.dtic.mil/docs/citations/ADA506270.

Schultz, Kenneth A. "Do Democratic Institutions Constrain or Inform? Contrasting Two Institutional Perspectives on Democracy and War." *International Organization* 53, no. 2 (ed 1999): 233–66. https://doi.org/10.1162/002081899550878.

Singh, V. K., D. Mahata, and R. Adhikari. "Mining the Blogosphere from a Socio-Political Perspective." In *2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*, 365–70, 2010. https://doi.org/10.1109/CISIM.2010.5643634.

Slantchev, Branislav L. "Politicians, the Media, and Domestic Audience Costs." *International Studies Quarterly* 50, no. 2 (June 1, 2006): 445–77. https://doi.org/10.1111/j.1468-2478.2006.00409.x.

Souza, Renato Rocha, Flavio Codeco Coelho, Rohan Shah, and Matthew Connelly. "Using Artificial Intelligence to Identify State Secrets." *ArXiv* 1611.00356 (November 1, 2016). http://arxiv.org/abs/1611.00356.

Stewart, Emily. "Lawmakers Seem Confused about What Facebook Does — and How to Fix It." *Vox*, Nisan 10, 2018. https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations.

Sullivan, Ben. "The Islamic State Conducted Hundreds of Drone Strikes in Less Than a Month." *Motherboard*, Şubat 21, 2017. https://motherboard.vice.com/en_us/article/vvxbp9/the-islamic-state-conducted-hundreds-of-drone-strikes-in-less-than-a-month.

Sutter, John D. "Ushahidi: How to 'crowdmap' a Disaster." *CNN Labs*, October 25, 2010. http://www.cnn.com/2010/TECH/innovation/10/25/crowdmap.disaster.internet/index.html.

Thony, John Frank. "Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units." *European Journal of Crime, Criminal Law and Criminal Justice* 4 (1996): 257.

Tongur, Stefan, and Mats Engwall. "The Business Model Dilemma of Technology Shifts." *Technovation* 34, no. 9 (September 1, 2014): 525–35. https://doi.org/10.1016/j.technovation.2014.02.006.

Traynor, Ian. "Libya: Nato Bombing of Gaddafi Forces 'Relying on Information from Rebels.'" *The Guardian*, Mayıs18, 2011, sec. World news. http://www.theguardian.com/world/2011/may/18/libya-nato-bombing-benghazi-rebel-leaders.

Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven ; London: Yale University Press, 2017.

Tzu, Sun. *The Art Of War*. Sterling Publishers Pvt. Ltd, 2005.

Weede, Erich. "Democracy and War Involvement." *Journal of Conflict Resolution* 28, no. 4 (Aralık 1, 1984): 649–64. https://doi.org/10.1177/0022002784028004004.

Weeks, Jessica L. "Autocratic Audience Costs: Regime Type and Signaling Resolve." *International Organization* 62, no. 1 (Ocak 2008): 35–64. https://doi.org/10.1017/S0020818308080028.

Weiss, Jessica Chen. "Authoritarian Signaling, Mass Audiences, and Nationalist Protest in China." *International Organization* 67, no. 1 (Ocak 2013): 1–35. https://doi.org/10.1017/S0020818312000380.

Westin Alan F. "Social and Political Dimensions of Privacy." *Journal of Social Issues* 59, no. 2 (Nisan 29, 2003): 431–53. https://doi.org/10.1111/1540-4560.00072.

Wheaton, Sarah. "New Technology Generates Database on Spill Damage." *The New York Times*, Mayıs4, 2010, sec. U.S. https://www.nytimes.com/2010/05/05/us/05brigade.html.

Wigell, Mikael. "Mapping 'Hybrid Regimes': Regime Types and Concepts in Comparative Politics." *Democratization* 15, no. 2 (Nisan 1, 2008): 230–50. https://doi.org/10.1080/13510340701846319.

Zegart, Amy B. "The Domestic Politics of Irrational Intelligence Oversight." *Political Science Quarterly* 126, no. 1 (Mart 1, 2011): 1–25. https://doi.org/10.1002/j.1538-165X.2011.tb00692.x.

Zeitzoff, Thomas. "How Social Media Is Changing Conflict." *Journal of Conflict Resolution* 61, no. 9 (October 1, 2017): 1970–91. https://doi.org/10.1177/0022002717721392.

Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

Siber Politikalar ve Dijital Demokrasi 2018/7

Temmuz 2018

# Dijital Açık Kaynaklı İstihbarat ve Uluslararası Güvenlik

**H. Akın Ünver** | EDAM, Oxford CTGA & Kadir Has Üniversitesi