İstihbarat Çalışmaları ve Araştırmaları Dergisi

Journal of Intelligence Research and Studies

Ocak 2023, Cilt: 2, Sayı: 1, ss.17-38

January 2023, Volume: 2, Issue: 1, pp.17-38

ISSN 2822-3349 (Basılı/Print) **ISSN 2822-3357 (Çevrimiçi/Online)**

Makaleye ait Bilgiler / Article Information

Araştırma Makalesi / Research Article

Makale Başvuru Tarihi / Application Date : 09 Kasım 2022 / 09 November 2022

Makale Kabul Tarihi / Acceptance Date : 05 Aralık 2022 / 05 December 2022

Makalenin Başlığı / Article Title

21'nci Yüzyılda Açık Kaynak İstihbaratı

Open Source Intelligence in the 21th Century

Yazar(lar) / Writer(s)

Tolga ÖKTEN

Atıf Bilgisi / Citation:

Ökten, T. (2023). 21'nci Yüzyılda Açık Kaynak İstihbaratı. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 2(1), ss. 17-38, DOI: http://dx.doi.org/10.29228/icad.9

Ökten, T. (2023). Open Source Intelligence in the 21th Century. *Journal of Intelligence Research and Studies*, 2(1), pp. 17-38, DOI: http://dx.doi.org/10.29228/icad.9

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

Research Center for Defense Against Terrorism and Radicalization Association

Adres/Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı 5387. Cadde No:15A D:58

06800 Çankaya/Ankara

Telefon/Telephone: +90 312 441 11 50

www.icadergisi.com

e-posta/e-mail: editor@icadergisi.com

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2023, 2(1) Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2023, 2(1) Research Article
DOI: http://dx.doi.org/10.29228/icad.9

21'NCİ YÜZYILDA AÇIK KAYNAK İSTİHBARATI

Tolga ÖKTEN[*]

ÖZET

Açık kaynaklar, günümüz istihbarat çalışmalarında yoğun olarak tartışılan bir konu başlığıdır. Birçok profesyonel, istihbaratın mutlaka gizli haber toplama faaliyetlerine dayanması gerektiğini ve bilgiye ulaşmanın kolay ve kısa bir yolu olmayacağını savunmaktadır. Diğerleri içinse açık kaynak istihbaratı yeni bir dönemi işaret etmektedir. Bu makalede, istihbarat çalışmaları literatüründe genelde teknoloji özelde ise açık kaynak başlığı altında yer alan bazı temel konu başlıklarının okuyuculara tanıtılması ve tartışılması amaçlanmıştır. Ayrıca, Türkçe terminoloji oluşturma sürecine de katkı sağlamak istenmektedir. Tartışma başlıkları; istihbaratın demokratikleşmesi, toplama-analiz ikiliği, görev ve kadro tanımlarındaki dönüşüm, açık kaynakların önleyici istihbarattaki güçlü ve zayıf yanları ile istihbarat zafiyeti olarak belirlenmiştir. Bu başlıklar etrafında istihbaratın 21. yüzyıldaki dönüşümü ve yol haritası tartışılmıştır.

Anahtar Kelimeler: *Açık Kaynak, Teknoloji, Dönüşüm, Toplama, Analiz.*

OPEN SOURCE INTELLIGENCE IN THE 21TH CENTURY

ABSTRACT

Open sources are an important topic of discussion in contemporary intelligence studies. Many professionals argue that intelligence should be based on covert intelligence collection methods and there is no easy way or shortcut to access information. For others, open-source intelligence indicates a new era in intelligence. Accordingly, in this study, some of the primary debates in the intelligence studies literature under technology generally and open source specifically are introduced and examined. Besides, it intends to contribute to the efforts of forming Turkish terminology. The main discussion topics are the democratization of intelligence, collection-analysis duality, transformation in job descriptions, strengths and weaknesses of open sources in warning intelligence, and intelligence failure. Around these topics, the transformation and the road map of intelligence are discussed.

Key Words: *Open-Source, Technology, Transformation, Collection, Analysis.*

GİRİŞ

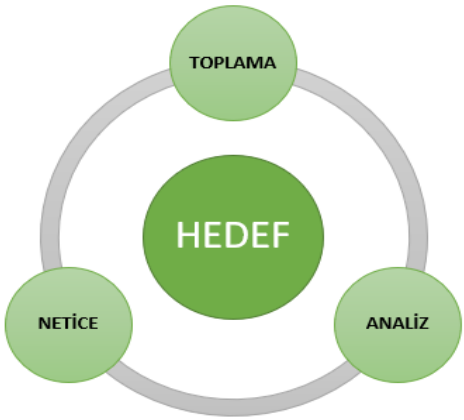
İstihbarat, en basit tanımıyla sistemdeki aktörleri anlamak, etkilemek ve önlemek amacıyla yürütülen gizli faaliyetlerdir. Bunun başarılabilmesi

[*] Öğretim Görevlisi Tolga ÖKTEN, Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar Enstitüsü, tolgaokten1982@gmail.com, ORCID: 0000-0002-6102-7704
Makale Başvuru Tarihi / Application Date: 09 Kasım 2022 / 09 November 2022
Makale Kabul Tarihi / Acceptance Date: 05 Aralık 2022 / 05 December 2022

için siyasi ve bürokratik karar alıcılar tarafından belirlenen önceliklere yönelik olarak yürütülen toplama faaliyeti neticesinde elde edilen bilgilerin[1] analizi ve sürecin zamanında neticelendirilmesi gerekmektedir. İstihbarat çarkı olarak da tanımlanan bu süreç istihbarat mesleğini teorik bir zemine oturtmaktadır.

İstihbarat teşkilatı personelinin temel görevi, hedef öncelikleri çerçevesinde yeni kaynaklar yaratmak, mevcutları yönetmek ve toplanan bilgilerin doğruluğunu ve güvenilirliğini analiz ederek faaliyeti neticelendirmektedir (Şekil-1). Önceliklerin belirlenmesi ve neticelendirme aşaması istihbarat teşkilatlarının karar alıcılar ile arasındaki bağlantıyı oluşturur. Toplama ve analiz ise teşkilatın içine ayna tutar ve mesleğin özünü oluşturmaktadır. Her faaliyetin[2] kendi karakteri olmakla birlikte istihbarat mesleğinin doğası aynıdır ve süreç her birimde genellikle bu şekilde yürütülür.

Şekil 1: İstihbarat Çarkı (Kaynak: Yazar tarafından hazırlanmıştır)



Bilgi farklı kaynaklardan toplanmaktadır. Mesleğin kökeni espiyonaj faaliyeti olarak da adlandırılan insan istihbaratına,[3] diğer bir deyişle casuslara dayanmakla birlikte, teknoloji geliştikçe teknik istihbarat kaynakları da denkleme girmiş ve kaynak çeşitliliği sağlanmıştır. Özellikle

[1] Türk istihbarat literatüründe bilgiye haber de denilmektedir. Bu çalışmada iki terim birbiri yerine kullanılmıştır.
[2] Faaliyet; ülke, bölge, konu, görev vb. farklı başlıklar altında bölümlenebilir.
[3] İnsana dayalı istihbarat İngilizce literatürde Human Intelligence (HUMINT), Türkçe literatürde ise İNİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.

internet teknolojisinde yaşanan gelişmeler, istihbaratın önemli bir parçası olan gizlilik boyutunu aşındırmaya başlamıştır. Günümüzde bilgisayar başından kalkmadan stratejik ve taktik istihbarat öncelikleri hakkında önemli bilgiler toplanabilmekte ve analiz edilebilmektedir. Açık kaynak[1] olarak adlandırılan bu veriler; askeri birliklerin konumlarının tespitinden, savaş suçlarının belgelenmesine, radikalleşme emarelerinin tespitinden, terör eylemlerinin soruşturulmasına kadar geniş bir yelpazede kullanılmaktadır. Ayrıca, stratejik öncelikleri oluşturan, örgüt içerisindeki hizipleşmeler, lider kadrolardaki değişiklikler, alınan siyasi kararlar, diplomatik gelişmeler ve dezenformasyon faaliyetleri de açık kaynaklar üzerinden takip edilerek yorumlanabilmektedir.

Bu çalışmanın amacı 21. yüzyıla damga vuran açık kaynak teknolojisinin istihbarat faaliyeti üzerindeki etkilerinin tartışılmasıdır. Bu kapsamda, istihbarat çalışmaları literatüründe genelde teknoloji özelde ise açık kaynak başlığı altında yer alan bazı temel konu başlıklarının okuyuculara tanıtılması ve tartışılması amaçlanmıştır. Açıklayıcı olması amacıyla, teorik çerçeve, örnek vakalar üzerinden detaylandırılmıştır. Çalışmanın bir diğer amacı da Türkçe terminoloji oluşturma sürecine katkı sağlamaktır.

Makalede öncelikle açık kaynak tanımı kavramsallaştırılmıştır. Sonrasında ortaya çıktığı değerlendirilen etkiler birkaç alt başlık üzerinden tartışılmıştır. Bu alt başlıklar hipotezler üzerinden formüle edilmiştir. Son bölümde ise bulgular özetlenmiştir.

H-1: Açık kaynak teknolojisi istihbarat faaliyetini tabana yayarak alanı demokratikleştirmiştir.

H-2: Açık kaynaklar toplama-analiz ikiliğini analiz lehine azaltmıştır.

H-3: Açık kaynaklar istihbarat teşkilatlarının kadro ve görev tanımlarında dönüşümü tetiklemiştir.

H-4: Açık kaynakların zayıf yanı, proaktif olmaktan ziyade reaktif olması ve bu nedenle önleyici istihbarat faaliyetindeki etkisinin sınırlı kalmasıdır.

H-5: Açık kaynakların terör/güvenlik istihbaratında en fazla potansiyel vaat ettiği nokta siber alan hakimiyeti sağlanmasıdır.

[1] Açık kaynak istihbaratı İngilizce literatürde Open-Source Intelligence (OSINT), Türkçe literatürde ise AKİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.

H-6: Açık kaynakların geriye yönelik çok güçlü bir araştırma yöntemi olması nedeniyle, istihbarat zafiyeti başlığı altındaki öngörü yanılgıları artmıştır.

1. AÇIK KAYNAK İSTİHBARATININ KAVRAMSALLAŞTIRILMASI

Teknik ve insana dayalı bilgi; açık, yarı açık ya da gizli kaynaklara dayanmaktadır. Gizli kaynaklar üzerinden yapılan haber toplama işlemi sadece bir imkân değil aynı zamanda bir yetki meselesidir. Yasa dışı bir faaliyetin içerisinde yer alan insanların para karşılığı çalıştırılması ya da bir hedefin dinlenmesi sürecinin sınırları yasal çerçeveler ile belirlenmektedir. Açık kaynaklar ise herkes tarafından kullanılabilir ve bu nedenle istihbarat mesleğinin görünen yüzüdür.

Açık kaynakların 20. yüzyıl öncesinde fiziki olarak elde edilen yazılı metinlerden oluştuğu görülmektedir. 20. yüzyılda buna elektronik dalgalar üzerinden yayılan radyo ve televizyonlar da eklenmiştir. Bu yüzyılda görüntü[1] ve sinyal istihbaratı[2] alanında çok büyük ilerlemeler yaşanmıştır. 21. yüzyılda ise mecra giderek siber alana doğru kaymıştır. Bu çerçevede günümüzde açık kaynak ile internette bulunan büyük verinin eşanlamlı olarak kullanılmaya başlandığı söylenebilecektir.

Bu noktada internette yer alan bütün bilgiler açık kaynak olarak kabul edilebilir mi sorusu ön plana çıkmaktadır. Bu soru çerçevesinde açık kaynaklar dar ve geniş olarak iki şekilde kavramsallaştırabilecektir (Tablo-1). Dar anlamıyla, sahibi tarafından bilinçli olarak yüklenen bilgilerden oluşmaktadır (Steele, 2019). Bu tanıma üçüncü şahıslar tarafından çalınarak toplumun kullanımına sunulan bilgiler de eklenebilecektir.[3] Arama motorları üzerinden yasal olarak ulaşılabilecek olan; haber programları, uzman görüşlerini içeren röportaj, dergi, kitap ve raporlar, ticari uydu görüntüleri ile internet sitelerine ve sosyal paylaşım platformlarına yüklenen fotoğraf, video vb. yapılandırılmış ve yapılandırılmamış veriler bu tanıma girmektedir. Geniş tanım ise internette kullanıma bilinçli olarak açılmış verilerin yanı sıra, ağ üzerinde bulunan ancak çeşitli şifreleme yöntemleri ile korunan bilgileri de içermektedir. Resmi ve özel kurumlarda bulunan kişisel veriler,

[1] Görüntü istihbaratı İngilizce literatürde Imagery Intelligence (IMINT), Türkçe literatürde ise GÖRİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.
[2] Sinyal istihbaratı İngilizce literatürde Signal Intelligence (SIGINT), Türkçe literatürde ise SİNİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.
[3] İkinci duruma örnek olarak Wikileaks belgeleri verilebilir. Özü itibariyle gizli bilgi olan diplomatik kriptolar Irak'ta görevli bir Amerikan ordu personeli olan Bradley Edward Manning tarafından sızdırılmış ve internette yayımlanmıştır.

banka hesap bilgileri, e-posta ve online konferanslar gibi internet görüşmeleri bu tanıma dahil edilebilecektir. Bu bilgiler yarı açık kaynak olarak da adlandırılabilir.[1] Bu bilgiler kişisel veri düzenlemeleri çerçevesinde korunan ve sadece ilgili kurum yetkililerin sorgulayabileceği bilgilerdir.[2] Geniş kavramsallaştırma açık kaynakların istihbarat faaliyetinde kapladığı yeri çok fazla genişletmiştir. 20. yüzyılda fiziki olarak güvenlikli binalarda ve kasalarda saklanması ve bu yüzden açık olmaması gereken birçok bilgiye günümüzde internet üzerinden ulaşılabilmektedir. Günümüzde, veri bir kez ağa yüklendikten sonra bunlara ulaşılabilmekte ve manipüle edilebilmektedir.

Tablo 1. Açık Kaynak Kavramsallaştırmaları (Kaynak: Yazar tarafından hazırlanmıştır)

DAR KAVRAMSALLAŞTIRMA	GENİŞ KAVRAMSALLAŞTIRMA
Haber programları Uzman görüşleri Dergi, kitap ve raporlar Ticari uydu görüntüleri Yüz tanıma, Flight Radar vb. internet uygulamaları İnternet sitelerine ve sosyal paylaşım platformlarına yüklenen medya	Şifreli sosyal medya hesapları Kamu kuruluşlarının veri tabanlarında bulunan bilgiler Kişisel Verileri Koruma Kanunu kapsamındaki diğer veriler

Bazı senaryolarda akıllı telefon uygulamaları vasıtasıyla, biyografik bilgilerin yanı sıra konum ve görüşme verileri gibi anlık bilgiler elde edilebilmekte ayrıca kişisel bilgisayarların harddiskinde bulunan verilere ulaşılabilmektedir. Ancak bunlar için cihazlara teknik yerleşme yapılmalıdır. Bu faaliyet için ya kullanıcının ya da ikinci bir şahsın telefona virüs programı yüklemesi gerekir. Bilgisayarların harddiskinde, akıllı telefonlarda ya da şifreli hesaplarda bulunan verilere ulaşmak istihbarat teşkilatlarınca sıklıkla uygulanan bir taktiktir.[3] Mahkeme kararı ile yapılan iletişimin dinlemesi faaliyeti gibi bu yöntem de gizli kaynak olarak kabul edilmektedir. Yetkili olmayan şahıslarca yapılması durumunda suç oluşturmaktadır.

[1] Yarı açık kaynaklar literatürde Proprietary Intelligence – PROPINT olarak da adlandırılmaktadır (Denécé, 2014, s.35)
[2] Türkiye'de bu veriler 6698 sayılı Kişisel Verilerin Korunma Kanunu ile korunmaktadır. (www.mevzuat.gov.tr, 2016)
[3] Pegasus yazılımının kullanılması bu duruma örnek olarak verilebilir. (www.europarl.europa.eu, 2022)

Her seviyedeki kullanıcının açık kaynak istihbaratının farklı tonlarında aktif olduğu söylenebilecektir. Amatör seviyedeki kullanıcılar firmaların sağladığı imkanları kullanırken[1], teşkilatların ve diğer profesyonel kullanıcıların yarı açık kaynak olarak tanımlanan alanda daha aktif oldukları görülmektedir.

2. AÇIK KAYNAKLARIN İSTİHBARAT FAALİYETİ ÜZERİNDEKİ ETKİLERİ

Çalışmada açık kaynakların istihbarat üzerindeki etkileri çeşitli alt başlıklarda incelenmiştir. Bu alt başlıklar hipotezler şeklinde tartışılmıştır.

H-1: Açık kaynak teknolojisi istihbarat faaliyetini tabana yayarak alanı demokratikleştirmiştir.

Teknoloji bir işin nasıl yapılacağını ya da yapılmayacağını belirleyen en önemli değişkenlerden bir tanesidir. Bu nedenle sadece istihbaratta değil diğer alanlarda da oyunun kurallarını değiştiren bir etken olarak görülmüştür. İster savaş ister bankacılık olsun işlerin teknoloji sayesinde eskisinden çok daha farklı ve kolay bir şekilde yürütülebileceği görüşü yaygındır.

Açık kaynak teknolojisinin, yarattığı fırsatlar ile istihbarat faaliyetini tabana yayarak alanı demokratikleştirdiği ileri sürülmektedir (Wheaton, 2019). Aslında demokratikleşme, istihbaratın masa başı bir iş haline geldiği anlamına gelmektedir. Bu noktada, bütün bilgiler ulaşılabilir olduğuna göre açık kaynak analizi yapan siviller ve özel sektör bileşenlerinin post-modern istihbaratçılar haline geldiğini ve hedefe yaklaşarak risk almadan, bilgisayar başında istihbarat üretilebileceğini iddia edebilir miyiz sorusu ön plana çıkmaktadır. Konuyu bir metaforla açıklamak gerekirse, bu soru, bütün kaynaklara internetten ulaştıktan sonra zahmet edip kütüphaneye gitmeye gerek var mıdır sorusudur.

Bu noktada, istihbarat analizinin büyük bölümünün açık kaynaklardan yararlanılarak hazırlandığı ve çok az bir kısmının gizli bilgi içerdiği görüşü ön plana çıkmaktadır (Johnson, 2009, s.42).[2] Açık kaynak bilgileri istihbarat mıdır sorusunu bir kenara bırakmak gerekirse bile, bu yanlış bir genelleme ve doğru bilinen bir yanlıştır. Dışa açık bir ülkenin makro ekonomik

[1] Örneğin Flight Radar ve Google Earth açık kaynak analizinde sıklıkla kullanılmaktadır.
[2] Buna karşı çıkan görüşe göre istihbarat faaliyeti mutlaka gizli bilgiye dayanmalıdır ve bilgiye ulaşmak ne kadar zorsa bilgi o kadar değerlidir. Lowenthal bu görüşü eleştirmektedir (Lowenthal, 2008, ss.182-185).

göstergeleri hakkında toplanan veriler açısından bu doğru olabilir ancak örgüt hücrelerine dair toplanan bilginin çok az bir bölümü açık kaynaktan toplanır. Özellikle teknolojinin kullanımının kısıtlı olduğu kırsal alana yönelik taktik istihbarat faaliyeti açısından kullanım alanı çok dardır.

Bu noktada istihbarat ürününün niteliği de önemlidir. Bir konu başlığında hazırlanan ülke analizi açık kaynaklar üzerinden ilerleyebilir ancak eylem ikaz istihbaratında durum karmaşıklaşır. Özellikle önleyici faaliyetleri oluşturan istihbarata karşı koyma ve terörle mücadele konularında açık kaynak bilgileri çok sınırlıdır ve genellikle istihbarat değeri bulunmamaktadır. Bir tepenin ya da sokağın görüntüsüne Google Earth'den ulaşılabilir ancak hücre evinin ya da sığınağın konumunu gösterecek olan birine ihtiyaç vardır. Benzer bir şekilde, bir telefon hattının kimin adına kayıtlı olduğu yarı açık kaynak bilgisidir, ancak hattı kimin kullandığı bilgisi saklanmaktadır ve tespit edilebilmesi için farklı yöntemlere başvurulması gerekir.

Konunun daha iyi anlaşılabilmesi için stratejik-taktik istihbarat önceliği ayrımı yapılması da gerekmektedir. Bir terör örgütünün herhangi bir ülkeyi hedef alacağını ilan etmesi o ülke açısından stratejik bir istihbarat önceliğidir. Diğer taraftan bu karar örgüt açısından da stratejik bir karar olduğu için kamuoyuna ve tabanına medya kanalları üzerinden açıklanmaktadır. Bu tarz bilgiler açık kaynak istihbaratı üzerinden toplanarak analiz edilebilir. Bunlar 5N1K'nın "ne" ve "neden" sorularıdır. Diğer taraftan, saldırının "kim" tarafından, "ne zaman", "nereye" ve "nasıl" yapılacağı taktik istihbarat boyutudur ve bu bilgiler çoğunlukla açık kaynaklarda yer almaz. Aslında, bu tartışma sadece açık kaynak teknolojisi için değil, uydu ve uçak gibi ileri teknoloji ürünü cihazlara dayanan teknik istihbarat faaliyeti için de geçerlidir. Örneğin, Soğuk Savaş boyunca uydu ve U-2'lerden gelen teknik istihbarata dayanılmasının, insan boyutunu ikinci plana atarak Sovyet nükleer silah kapasitesinin tespitinde hatalara yol açtığı belirtilmektedir (Freedman, 1977).

Diğer taraftan açık kaynak teknolojisi stratejik öncelikler açısından kamu ve özel sektör bileşenleri arasında önemli bir iş birliği potansiyeli sunmaktadır (Lahneman, 2016, ss.12-14). Daha önce belirtildiği üzere açık kaynaklar mesleğin görünen yüzüdür ve istihbarat teşkilatları ile sivil araştırmacılar arasındaki sınırı oluşturmaktadır. Bu sınır her geçen gün daha fazla geçirgen hale gelmektedir. Bu çerçevede özellikle stratejik istihbarat

önceliklerinde açık kaynakların rolü ve iş birliği fırsatları giderek artmaktadır. Kabul etmek gerekir ki, stratejik istihbarat analizi sürecinin en önemli aktörleri konu/bölge uzmanlarıdır. Yıllarca aynı konu/bölge üzerinde çalışmış, ilgili ülkelerde bulunmuş, büyük ihtimalle bölge diline, kültürüne ve siyasetine hâkim kişilerdir. Bu noktada istihbaratçılara göre çok daha uzmanlaşabilme potansiyelleri vardır (Johnson, 2009, s.42). Örneğin bir teşkilat mensubuna ekonomi öğretmektense bir ekonomiste analiz edeceği bilgileri vermek daha mantıklıdır. 20. yüzyılda gizli kalması gereken birçok bilgi ve belgeye günümüzde internetten kolaylıkla ulaşılabilmekte bu sayede konu hakkında uzmanlığı bulunan akademisyen ve diğer sivil uzmanların analiz sürecine katkı yapmaları çok daha kolaylaşmaktadır.

H-2: Açık kaynaklar toplama-analiz ikiliğini analiz lehine azaltmıştır.

İstihbarat çalışmaları literatüründe yer alan toplama-analiz ikiliği sadece masa başında yapılan felsefi bir tartışma değil, mesleğin her anında yaşanan bir olgudur. Her iki aşamanın da taraftarları, gelenekleri, teknikleri ve örgütleri vardır.

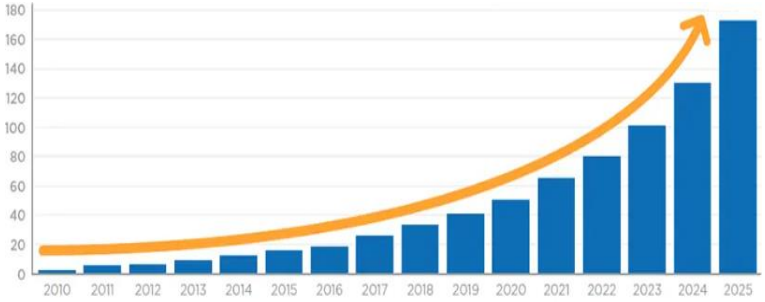
İlk bakışta açık kaynak istihbaratının bir toplama aracı olduğu düşünülebilecektir. Açık kaynak istihbaratını, insan istihbaratı ya da sinyal istihbaratı gibi ayrı bir toplama disiplini olarak kabul eden çalışmalar da bulunmaktadır (Field Manuel 2-0, s.I-30) (Lowenthal, 2008, s.187) (Johnson, 2014, s.9) (Wirtz ve Rosenwasser, 2010, s.726). Diğer taraftan açık kaynak istihbaratı özü itibariyle toplama değil bir analiz faaliyetidir.

Toplama ve analizin aşamalarının merkezinde teknoloji olmasına rağmen, analiz kapasitesi toplama kapasitesine oranla çok daha yavaş ilerlemektedir. Teknoloji veri toplama ve işleme kapasitesini arttırmıştır ancak üretilen istihbarat aynı hızla artmamıştır (Lowenthal, 2008, s.184). Yapay zekâ uygulamaları sayesinde veri madenciliği ve analiz teknikleri sürekli gelişmekte, ancak alınan kararlar eninde sonunda insan zihninin algılama kapasitesine dayanmaktadır. Sistemin toplam kapasitesini de belirleyen bu darboğazı, toplanan veri yığınını analiz edebilecek nitelikteki programlar ve personel oluşturmaktadır. Bu nedenle analiz aşamasının açık kaynak istihbaratının ağırlık merkezini oluşturduğunu söylemek yanlış olmayacaktır.

Analizin artan öneminin en önemli nedeni, açık kaynaklara dayalı toplamanın artık bir yetenekten ziyade standart haline gelmesidir. Gelişen bilgisayar teknolojisi sayesinde hedef ekosistemine yönelik olarak toplama

(bulk collection) rutin bir işlem haline gelmiştir (Gill ve Phythian, 2018, s.322). İnternet ve akıllı telefon teknolojisi ile birlikte bir haber patlaması yaşanmıştır ve toplanan veri her geçen gün çığ gibi büyümektedir. İnternetteki veri sayısı 2010-2018 arasında yaklaşık 30 kat artmıştır ve hızla artmaya devam etmektedir (Grafik-1). 2018'de 33 zetabayt olan verinin 2025'te 175 zetabayta ulaşması beklenmektedir (www.i-scoop.eu). Bu verinin yaklaşık yarısı gerçek zamanlı olarak paylaşılan veridir (www.statista.com). Bu çerçevede internetin istihbarat teşkilatları için bir süper arşiv haline geldiği söylenebilecektir. Teorik olarak internet üzerinden hemen her türlü bilgiye ulaşılabilmektedir. Bu durum sadece istihbarat teşkilatları açısından değil sivil kullanıcılar açısından de geçerlidir. İnternete sahibi tarafından bilinçli şekilde yüklenen ya da başka taraflarca sızdırılan her türlü yapılandırılmış ya da yapılandırılmamış bilgi, bilgisayarı olan her bir kullanıcı için büyük bir veri havuzu oluşturmaktadır.

Grafik 1: İnternetteki Veri Miktarı (www.i-scoop.eu)



Analiz sürecinin amacı ise büyük veriyi yorumlayarak görselleştirmek ve operasyonel hale getirmektir. Bu aşamada da teknolojiye önemli görevler düşmektedir. Özellikle bilgi sistemleri teknolojileri *(Management Information Systems - MIS)*, analizi geçmişten çok daha güçlü hale getirmiştir. 11 Eylül saldırıları bu anlamda milat olarak görülebilir. Daha önce üretim yönetimi, pazar ve müşteri analizi gibi alanlarda kullanılan bu sistemler 11 Eylül sorasında istihbarat alanına hızlı bir giriş yapmıştır. Bu teknolojiler sayesinde; farklı istihbarat ve kolluk birimleri arasındaki bilgi paylaşımı hızlanmakta, arşiv bilgileri farklı kurumların veri tabanlarından çok daha hızlı bir şekilde çekilebilmekte, irtibat ağları ile eylem paternlerinin görselleştirilmesi ve haritalandırılması *(link analysis)* sağlanabilmekte, yarı açık kaynaklarda yer alan bilgiler tek bir ara yüzde toplanabilmektedir. Günümüzde analiz faaliyeti bu tarz kullanıcı dostu işletim sistemleri sayesinde mümkün olmaktadır. Bu kapsamda en önemli analiz araçlarından

bir tanesi sosyal ağ analizidir. Sistemin haritalandırılması ve nodların ve ilişki ağının çözülmesi açısından önemli bir kapasite sunmaktadır. Aslında sosyal ağ analizi yeni bir şey değildir ve henüz bilgisayarlar kullanılmazken bile mekanik olarak yürütülmüştür. Diğer taraftan analiz teknolojilerindeki ilerleme ve sosyal ağın giderek artan bir şekilde fiziki dünyadan açık kaynak olan sanal dünyaya kayması analizin karakterini değiştirmiştir. Diğer taraftan bu başlık altında vurgulandığı üzere analiz kapasitesi hala toplama kapasitesine yetişmekten uzaktır.

Açık kaynaklarda yaşanan bu genişleme ironik bir şekilde analistlerin iş yükünü arttırmıştır. Şu anda sistemde çok fazla uyaran vardır ve bu gürültü içerisinden sinyalleri tespit etmek çok zordur.[1] Her ne kadar algoritmalar vasıtasıyla filtrelenseler de çok fazla gereksiz bilgi akışı mevcuttur. Sıfır hata prensibi nedeniyle her bilgi eninde sonunda incelenmek zorundadır. Bilgisayar üzerinden mesajlar anlık olarak paylaşılmaktadır ancak bilgilerin analiz edilmesi zaman alan bir süreçtir ve analistlerin iş yükü her gün daha da artmaktadır.

20. yüzyıl istihbaratçılığında, haber toplama faaliyetinin istihbarat çarkının en meşakkatli kısmı olduğu görülmektedir. Bir şehrin detaylı haritası, silahın teknik özellikleri, askeri üssün fotoğrafı, siyasi liderlerin biyografilerine ulaşmak mesleğin önemli bir parçası olmuştur. Günümüzde bu bilgilere açık kaynaklardan ulaşmak mümkündür. Bu durum büyük bir bilgi bombardımanına neden olmaktadır. Analizcilerden, bilgisayar ekranından hızla akan mesajlara işlem yapması ve internette yer alan bilgilerin sürekli takip etmesi beklenmektedir. Steril hedef önceliklerine sahip olmak giderek zorlaşmakta ve sayı odaklı bir performans beklentisi yerleşmektedir.

H-3: Açık kaynaklar istihbarat teşkilatlarının kadro ve görev tanımlarında dönüşümü tetiklemiştir.

Geleneksel olarak toplama ile analiz arasında bir duvar bulunmaktadır (Herman, 1998, s.5). Analiz teknolojileri bu duvarı giderek şeffaflaştırmakta, istihbarat personelinin görev tanımları ve kadroları da bu durumdan etkilenmektedir. Bu tartışma 4. Nesil İstihbarat kavramını da gündeme getirmiştir. Bu teoriye göre, yeni dönemde dijital ve biyolojik analiz

[1] Wohlstetter sinyal *(signal)* ve gürültü *(noise)* kavramlarını kullanmaktadır (s.3).

yöntemlerinin iç içe geçmiş ve aradaki fark bulanıklaşmıştır (Younger, 2018).

Öncelikle analizciler giderek kendi toplayıcıları haline gelmektedir (Treverton, 2019, s.145). Gelişen bilgisayar teknolojisi, veri analiz sistemleri ve açık kaynaklar sayesinde günümüzde analizciler giderek daha fazla oranda ihtiyaç duydukları bilgileri kendileri toplayabilmektedir. Farklı kurumların veri tabanlarına tek bir arayüz üzerinden ulaşılabilmesi durumunda fiziki engeller ortadan kalkmakta ve herkes kendi toplayıcısı haline dönüşmektedir. Bu nedenle hedef ülkede maske kimliklerle yaşayan ya da servislere akredite olarak çalışan toplayıcılardan beklenen bilginin içeriği de değişmiştir. Toplayıcılar artık giderek daha fazla gizli bilgi peşinde koşmak zorundadır. İnternetin yetersiz kaldığı noktalara ulaşmak ve faaliyetin içerisinde yer alan gizli bilgiyi elde edecek kaynaklar bulmalıdır. Örnek vermek gerekirse hedef şahsın ikamet adresi ya da telefon numarası bilgisayar başından bulunabilir, ancak hedefe yönelik yürütülecek operasyonel çalışmalar halen toplayıcıların görevidir.

İkinci olarak geleneksel toplama ve analiz görevlerinin yanına farklı görev tanımlarının da eklendiği görülmektedir. İnternet her ne kadar herkese açık olsa da burada yer alan yapılandırılmamış ya da korunan bilginin toplanarak analiz edilebilecek formata getirilmesi ayrı bir meslektir (Shulsky ve Schmitt, 2002, s.41). Yapılandırılmamış verinin işlenmesi analizin ilk aşamasıdır. Bazen istihbarat çarkında tasnifleme olarak da adlandırılır. Bu aşama analizin en zor ve zaman alan aşaması haline geldiği savunulmaktadır (Johnson, 1994, s.19).[1] Öyle ki birçok veri bu aşamayı geçememekte süper arşivin tozlu raflarında kalarak hiçbir zaman kullanılmamaktadır. Bu bilginin işlenmesi analizin bir sonraki aşamasına geçilmesi için şarttır.

Bu çerçevede, teşkilatların konu/bölge uzmanından ziyade teknik analiz uzmanına ihtiyaç duyduğu ve analizin giderek bir teknik görev haline dönüştüğü yorumu da yapılmaktadır (Treverton ve Gabbard, 2008, s.35). 20. yüzyılın aksine günümüzde analiz daha matematiksel hale gelmiştir. Phyton ve R gibi uygulamalar büyük veri setleri, sosyal medya uygulamaları ve haber sitelerinde bulunan büyük verinin tasnif ve analiz edilmesinde büyük kolaylıklar sağlamaktadır. Açık kaynak istihbaratı artık bilgisayar okur yazarlığı ile yürütülecek bir iş olmayı çoktan aşmış ve farklı bir uzmanlık

[1] Johnson bu tespiti dönemin National Security Agency (NSA) Başkanı Mike McConnell'a dayandırmaktadır. NSA Amerikan istihbarat yapılanmasında sinyal istihbaratının toplanmasından sorumlu temel kurumdur.

alanı haline gelmiştir. Bu nedenle günümüzde teknik analiz, veri analizi gibi adlar altında farklı bir görev tanımları, kadrolar ve taktik yenilikler ortaya çıkmıştır. Geleneksel istihbaratçılık yeteneklerinden ziyade bilgisayar diline hâkim olmayı gerektirmektedir. Bu durum geleneksel olarak destek personeli olarak görülen teknik uzmanlar artık avcıya mı dönüşmekte ve istihbarat personeli kaçınılmaz olarak mühendisler arasından mı seçilmeye başlanacak gibi bazı soruları da beraberinde getirmektedir.

Üçüncüsü, teknoloji ve yapay zekâ uygulamaları bazı görev tanımlarını ortadan kaldıracak gibi gözükmektedir. Örneğin analiz sürecinin önemli bir parçası olan tercüme faaliyeti giderek ticari uygulamalar üzerinden gerçekleştirilebilir hale gelmiştir. Kritik dillerdeki çeviriler artık tek bir tuşla anlık olarak yapılabilmektedir. Benzer bir şekilde, sinyal istihbaratından elde edilen konuşmaları yazı formatında yapılandıracak uygulamalar sayesinde bu işle görevli çok sayıdaki personelin de yükü azalacaktır. Bu nedenle geleceğin istihbarat teşkilatlarında yeni görev tanımları ortaya çıktığı gibi bazı görevlerin ortadan kalkması da olasıdır.

H-4: Açık kaynakların zayıf yanı, proaktif olmaktan ziyade reaktif olması ve bu nedenle önleyici istihbarat faaliyetindeki etkisinin sınırlı kalmasıdır.

İstihbaratın kolluk görevinden ve gazetecilik mesleğinden farkı, işlenen bir suçu aydınlatmaktan ziyade suçu işlenmeden öngörmesidir. Geleceğe yönelik tahminde bulunmak istihbarat ile diğer meslekler arasındaki farkı oluşturmaktadır (Hulnick, 1999, s.46). Bu çerçevede açık kaynakların çoğunlukla proaktif değil reaktif olduğu söylenebilecektir. Bu nedenle açık kaynak analizinin belki de en zayıf yanı ileriye dönük değil geriye dönük bilgiler vermesidir.

Özellikle güvenlik/terör istihbaratının ana görevi önleyici istihbarattır. Elde edilecek eylem ikaz istihbaratı *(warning intelligence)* sayesinde eylemlerin planlama aşamasında tespit edilerek gerçekleştirilmeden önlenmesi amaçlanır. Bu süreçte, eylem kapasitesi ve niyeti bulunan hücrelerin tespit edilerek faaliyetin neticelendirilmesi gereklidir. İkaz istihbaratı eylemleri her zaman önleyemese bile, gerekli pasif güvenlik önlemlerin alınarak caydırıcılığın sağlanması ya da direnç *(resilience)* yaratarak yıkıcı etkilerinin azaltılmasını hedefler.

Sofistike eylemler, hücre üyelerinin hataları (Ör. hücre evinde patlama olması), çevredekilerin dikkatini çekmeleri[1] (Ör. yanıcı madde stoklanması) gibi nedenlerle hazırlık aşamasında önlenebilmektedir. Diğer taraftan bu senaryolar genellikle istisnadır ve eylemlerin önlenebilmesi için hücreye sızılması gereklidir. Bu aşamadan sonra bir operasyon kurulur ve süreç neticelendirilir (Woo, 2011, s.51). Yalnız aktörlerin aksine, gizli faaliyet gösteren hücrelerin saldırı planlarını internetten öğrenmek pek mümkün değildir. Sosyal gruplar ya da yalnız aktörler sohbet odalarında ya da sosyal medya hesaplarında eylem hazırlıklarına dair mesajlar paylaşsa da profesyonel hücreler operasyonel güvenliğe riayet etmektedirler.

Bu noktada, ağ analizinin kendine has sınırlılıklarının bulunduğu anlaşılmaktadır. Ağ analizi sistemdeki farklı noktalar arasında içeriğinden bağımsız olarak bir ilişki şeması çıkarmayı amaçlar (Barnea, 2018, s.224). İltisak ağını haritalandırır ancak irtibatın içeriğine dair bir bilgi veremez. Durumun fotoğrafını çeker ancak operasyonel bir planlama için yeterli değildir. Faaliyetin neticelendirilebilmesi için sadece fotoğrafının değil röntgeninin çekilmesi gereklidir. Bu da sadece gizli kaynaklar kullanılarak başarılabilir. Bu nedenle açık kaynaklar hedefleme sürecinin önemli bir parçasıdır ancak mucizevi bir iksir olmaktan uzaktadır.

Bu çerçevede, açık kaynakların önleyici istihbarattan ziyade genellikle soruşturma aşamasında daha etkili olduğu görülmektedir (Krebs, 2016, s.49). Ortada çözülmesi gereken bir suç varsa ipuçlarını açık kaynaklarda ya da gri alanda kalan bilgileri analiz ederek bulmamız mümkündür. Bu durumda suça bir bulmaca olarak bakılır ve kanıt aranır. Henüz işlenmemiş bir suçun önlenmesi ise kaçınılmaz olarak bilinmezlik içerir.[2] Bu bilinmezliğin somutlaştırılabilmesi için hedefe yaklaşarak risk almak gerekir. Bu risk bazen genellikle istihbaratçılar ve onların yönettiği kaynaklar alır.

Diğer taraftan açık kaynak analizinden bahsederken sadece örgüt hücrelerine odaklanmak da doğru değildir. Özellikle istihbarata karşı koyma kapsamında maske kimliklerle faaliyet gösteren illegallerin[3] hareketlerinin takibi ve haber kanallarının ortaya çıkarılması gibi amaçlarla da kullanılabilmektedir. Örneğin Bellingcat, açık ve yarı kaynak analizi

[1] Bu durum literatürde pasif mukavemet olarak adlandırılmaktadır.
[2] Bu konu istihbarat zafiyeti başlığı altında daha detaylı açıklanmıştır.
[3] "İllegal" terimi, derin bir maske hikaye ile hedef ülkede görev yapan istihbarat personelini tanımlamak için kullanılmaktadır. Bunlar teşkilat mensubu olabilecekleri gibi teşkilat personeli tarafından yönetilen elemanlar da olabilirler.

üzerinden çok önemli soruşturmalar yürüterek Rus istihbarat servislerinin yasa dışı faaliyetlerini ortaya çıkarmaktadır. Bu sayede Avrupa'da gerçekleştirilen çok sayıda suikast aydınlığa kavuşturulmuştur. Sergey Skripal'e yönelik suikast girişiminin şüphelileri olan GRU mensupları Anatoliy Chepiga ve Alexander Mishkin'in deşifre edilmesi bu duruma örnek olarak verilebilecektir (Bellingcat. 2018). Eylemciler görev öncesinde tespit edilemeseler de arkalarında çok sayıda dijital ayak izi bırakmışlardır. Kapalı devre kamera görüntüleri, araç plaka kayıtları, uçuş bilgileri ve geçmiş dönemde başkalarına ait sosyal medya hesaplarında yer alan özel fotoğrafları sayesinde tespit edilebilmişlerdir. Aslında Belingcat'in ulaştığı bilgilerin birçoğu dar anlamda açık kaynak bilgisi değildir. Plaka kayıtları, telefon arama ve baz istasyonu bilgiler, pasaport bilgileri, PNR verileri, kamera kayıtları gibi birçok bilgi dış kullanıma kapalıdır. Kurum bu bilgilerin kaynağı olarak yerel ortaklarını göstermektedir. Bu çerçevede yabancı istihbarat servisleri ve Rusya içindeki muhalif yapılarla da yakın temasta oldukları anlaşılmaktadır.

Bellingcat'in açık kaynak analiz faaliyeti soruşturma odaklı olsa da ortaya çıkan bilgilerin önleyici istihbarat açısından bazı fırsatlar yarattığını da kabul etmemiz gerekmektedir. Bellingcat'in Rus illegallerinin kullandıkları pasaport serilerini ifşa etmesi sayesinde hem geçmişe yönelik soruşturmalar yürütülebilmiş hem de halen maske kimlikle faaliyet gösteren illegaller deşifre edilmiştir. Bu illegallerin bir kısmının görevlerini sona erdirerek Rusya'ya geri döndüğü bilinmektedir.[1]

H-5: Açık kaynakların terör/güvenlik istihbaratında en fazla potansiyel vaat ettiği nokta siber alan hakimiyeti sağlanmasıdır.

Bir önceki başlıkta görüldüğü üzer açık kaynakların güvenlik/terör istihbaratındaki rolü tartışmalı bir konudur. Genel kanı bu kaynakların sofistike terör eylemlerini engellemede başarılı olmadığıdır. Diğer taraftan, açık kaynak istihbaratının iddiası, potansiyel eylemcilerin radikalleşme süreçlerinin büyük veri üzerinden takip edilebileceği ve bazı senaryolarda eylemlerin önlenebileceğidir (Ball ve Webster, 2003, s.4).

Radikalleşme emarelerinin tespiti için potansiyel eylemcinin parçası olduğu ekosisteme yani ağa odaklanılması gerekmektedir. Bu hem fiziki

[1] Maria Adela Kuhfeldt River kod adını kullanarak NATO personellerine yaklaşan bir GRU elemanı olduğu iddia edilen Olga Kolobova hakkındaki analiz bu duruma örnek verilebilir (www.bellingcat.com, 2022).

hem de elektronik bir ilişki ağıdır. Ağ üzerindeki noktalar (eylemci, milis, kurye, telefon, bilgisayar, internet sitesi, hücre evi, mağara, vb.) birbirleriyle iltisaklıdır (Arquilla ve Ronfeldt, 2001, s.II-7, Sparrow, 1991, s.257). Bu irtibat arkadaşlık, akrabalık, ideoloji, para, lojistik, irtibat ya da eylem amaçlı olabilir. Ağ üzerindeki bu noktalar arasındaki ilişki arkasında iz bırakmaktadır. Noktaların tespiti yeni hedefler yaratarak deşifre edilen ağı genişletmektedir.

Bir önceki başlıkta belirtildiği gibi ağ analizi sihirli bir çözüm sunmasa da analiz teknolojisinin örgüt ekosisteminin görselleştirilmesi açısından büyük kolaylıklar sağladığı kabul edilmelidir. Bu çerçevede açık kaynak analizinin en güçlü olduğu nokta belki de siber alan hakimiyetinin sağlanmasıdır. Asker ve polis birimlerinin fiziki alan hakimiyeti sağlaması gibi istihbarat teşkilatları da siber alanı örgütlere kapayarak hareketlerini yavaşlatmak ve engellemek zorundadır. Siber devriye[1] olarak da adlandırılan bu görev çerçevesinde sadece internet üzerinden islenen suçların tespiti değil örgütsel faaliyetlerin de kontrolü amaçlanmaktadır. Bu çerçevede örgütsel sitelerin sosyal medya uygulamalarının ve mesaj trafiğinin kontrol altında tutulması ve eylem ya da radikalleşme sinyallerinin tespit edilerek operasyona dönüştürülmesini öngörmektedir.

Radikalleşme emarelerinin tespiti için büyük veri toplanarak süzgeçten geçirilmektedir (Barnea, 2019, ss.440-441). Yapay zekâ uygulamaları bu süreçte büyü bir rol üslenmektedir. Davranış kalıplarını ve kilit söylemleri takip ederek, mekanik olarak takip edilemeyecek bir alanı kontrol altında tutmaktadır. Yapay zekâ uygulamaları ile; radikal söylemler, eylem öncesi hazıklık aşamasındaki sızıntı davranışları, bir konu ya da kişi hakkındaki takıntılı davranışlar ve başka saldırganlarla özdeşleşme çabaları takip edilmektedir (Brynielsson vd., 2013, ss.7-9).[2] Haritalandırma programları ve anahtar kelime sorgulamaları, olağan şüphelilerin takibi ve ikaz emarelerinin toplanması açısından önemli araçlardır.

Bu noktada, özellikle yalnız aktör eylemlerinin engellenmesinde önemli fırsatların söz konusu olduğu söylenebilecektir. Her ne kadar Reina saldırganı Masharipov ya da Paris saldırganı Abdelhamid Abaaoud eylemciler internet üzerinde aktif değillerse de özellikle yalnız aktörlerin

[1] Tanım için bkz. www.egm.gov.tr, 2020
[2] Özellikle aşırı sağ vasat içerisinde Anders Breivik ile özdeşleşme çabalarına sıklıkla rastlanılmaktadır. Breivik'in 22 Temmuz 2011'de Oslo ve Utoya'da gerçekleştirdiği saldırılarda 77 kişi hayatını kaybetmiştir.

eylem öncesinde güçlü sinyaller verdikleri bilinmektedir. Eyleme geçmeden önce ortaya çıkan bu emarelerin tespiti durumunda önleyici adımların atılması mümkündür. Bu kapsamda alan kaplama faaliyetinin nokta operasyona dönüşmesi de mümkündür. Mizansen operasyonlarla *(sting operations)* potansiyel saldırganın kontrollü bir şekilde eylem aşamasına geçirilerek suç üstüne gidilmesi özellikle Amerikan iç istihbarat kurumlarınca sıkça kullanılan bir uygulamadır. Benzer bir şekilde ağ üzerindeki kişilerin motivasyon unsurlarının tespit edilerek, angaje amacıyla kullanılabildiği görülmektedir. Çin'in Linkedln gibi uygulamaları bu amaçla kullandığı bilinmektedir.

H-6: Açık kaynakların geriye yönelik çok güçlü bir araştırma yöntemi olması nedeniyle, istihbarat zafiyeti başlığı altındaki öngörü yanılgıları artmıştır.

Açık kaynak arşivinin bilgisayarı olan herkes tarafından geçmişe yönelik detaylı olarak sorgulanabilmesi, istihbarat zafiyeti *(intelligence failure)* kavramının sıklıkla gündeme gelmesine neden olmuştur. Teknolojinin analiz boyutunu ön plana çıkarması ile bağlantılı olarak, eylemlerin önlenmesindeki başarısızlıklarda oklar giderek daha fazla analiz aşamasına işaret etmeye başlamıştır (Treverton, 2009, s.106). Bunun nedeni bütün bilinmezliklerin cevabının internetin derinliklerinde bir yerde olduğu yanılgısıdır (Treverton vd., 2006, s.14). Zaten eylemciler hakkındaki bilgilere açık kaynaklardan ulaşılabiliyorsa, hata, bu bilgilerin doğru analiz edilememesi nedeniyle oluşmuştur. Özet olarak ortada bir istihbarat zafiyeti bulunmaktadır.

Açık kaynakların geçmişe yönelik sorgulama gücü, sonuç odaklı eleştirilere ve öngörü yanılgılarına *(hindsight bias)* yol açmaktadır. İstihbarat teşkilatları saldırganlar hakkında çok fazla bilgi bulunmasına rağmen saldırıyı engelleyememekle suçlanmaktadır. Çokça vurgulandığı üzere kimse polisin bütün cinayetleri engellemesini beklememekte ama istihbaratın bütün eylemleri önlemesini istemektedirler (Goldman, 2016). Öncelikle şunu belirtmek gerekir ki daha fazla bilgi daha fazla istihbarat anlamına gelmemektedir (Treverton vd., 2006, s.14). Veri toplama ve işleme kapasitesinde yaşanan büyüme hayali bir güvenlik algısı yaratmakta, ancak daha fazla veri daha fazla güvenlik anlamına gelmemektedir. Her ilave bilgi ile operasyonel etkinlik arasında doğrudan bir ilişki mevcut değildir. Bu çerçevede, aslında eylemciler hakkında internette çok fazla bilgi bulunduğu

görülmektedir. Örneğin, 11 Eylül saldırganlarının kendi adlarına kayıtlı adreslerine, ehliyetlerine, kredi kartı bilgilerine ve seyahat geçmişlerine rahatlıkla ulaşılabilmiştir. Bu bilgilere saldırıdan önce de ulaşmak mümkündür ancak nereye bakılması gerektiği bilinmediğinden saldırı öncesinde hiçbir işe yaramamıştır (Treverton, 2009, s.32). Belki de derinlerde bir yerde bütün eylemciler hakkında bilgi bulunmaktadır, ancak bu bilginin değerli olduğuna nasıl karar verileceği sorusu genellikle yanıtsız kalmaktadır.

Bu noktada, realizmin klasik tehdit formülasyonu açıklayıcı bir çerçeve sunmaktadır. Formüle göre, tehditler kapasite ve niyetin etkileşiminden oluşur. Açık kaynaklar kapasite hakkında genellikle doğru ve güvenilir bilgilere ulaşmamızı sağlar. Diğer taraftan niyetleri tespit etmek çok daha zor ve subjektif bir süreçtir (Treverton, 2009, s.138). Rusya nükleer silah kullanacak mı ya da varlığı bilinen bir radikal eylem kararı verecek mi soruları somut verilerin ötesine geçen bir durumdur. Benzer bir şekilde zaten kırsala katılmış kişilerden oluşan bir örgüt grubunun konumunun tespiti ile henüz fikir aşamasında olan bir eylemin önlenmesi farklı özellikteki faaliyetlerdir. Kapasitenin gözlemlenebilmesi gereklidir. Bir silah, ya da insan varlığı kapasitenin kanıtı olabilir. Ancak silahın nerede ve ne zaman kullanılacağı gözlemleyebilmek pek mümkün değildir.

Bu durum istihbarat çalışmaları literatüründe sıkça tartışılan bulmaca-sır *(puzzle-mystery)* farklılığına işaret etmektedir. İlk duruma göre ortada çözülmesi gereken bir bulmaca vardır ve tek gereken şey doğru parçayı doğru yere yerleştirmektedir. Özellikle kapasite boyutunu oluşturan somut eşyalar bulunmayı bekler. Bunlar; eylem malzemesi olan patlayıcılar, bir hücre evi ya da kırsalda bir mağaradadır. Aksi görüş ise eksik parçaların hala keşfedilmeyi beklediğidir. Örnek vermek gerekirse El Kaide liderlerinin Afganistan Pakistan sınırındaki sığınakları bir bulmacanın parçalarıdır. Ancak saldırıların kim tarafından, ne zaman, nereye ve nasıl gerçekleştireceği bir sırdır (Treverton, 2009, s.33-34). 11 Eylül saldırısının lideri Muhammed Atta'nın kimlik bilgilerini bulmak yapbozun parçalarını birleştirmeye benzemektedir. Bu bilgilere açık kaynaklardan ulaşılabilmektedir. Diğer taraftan eylem niyetini öngörebilmek ayrı bir mesleki yeterlilik gerektirmektedir.

Kapasite sorusunun genellikle bir cevabı vardır. Diğer taraftan niyetler konusunda ortada bir cevap değil sadece tahminler olabilir (Treverton, 2009,

s.147). Tahminler demokratik ülkelerde kanıt yerine geçmez. Örneğin 12 Haziran 2016 tarihinde Orlando'daki bir gece kulübüne gerçekleştirdiği saldırıda 49 kişiyi öldüren Omar Mateen gibi yalnız aktörlerin engellenememesi ABD'de geniş şekilde tartışılmıştır. Mateen, saldırı öncesinde, iş yerinde El Kaide ve IŞİD'in gerçekleştirdiği terör eylemlerini öven söylemlerde bulunması nedeniyle FBI tarafından kontrol altında tutulmuş ancak hakkında kanıt bulunamamıştır. Yetkililerce, Mateen gibi yalnız aktörlerin saldırı öncesinde yasalara aykırı hiçbir eyleminin bulunmadığı, Afganistan'a gitmenin ya da Osama bin Laden'i övmenin bir kişiyi istihbarat hedefi haline getireceği, ancak suçlanması ve tutuklanması için yeterli olmayacağı belirtilmiştir (Goldman, 2016). Dönemin FBI Başkanı Comey, teşkilatın yasal sınır olan on ay boyunca Mateen hakkında ön soruşturma yürüttüğünü, ancak herhangi bir eylem emaresine rastlanmadığını, geriye bakınca bu vakada eksik ya da yanlış olan ve farklı yapmaları gereken bir prosedürün bulunmadığını açıklamıştır (Goldman, 2016).

Güvenlik/terör istihbaratında yaşanan kapasite niyet sorunsalında tartışılan bir konu da alan hakimiyeti başlığında vurgulanan mizansen operasyonlardır. Kabul edileceği üzere, geleceği tahmin etmek kolay bir iş değildir. Bu nedenle istihbarat teşkilatlarına sadece geleceği tahmin etmek değil geleceği dizayn etmek gibi bir görev de verilmiştir. Bazı senaryolarda potansiyel eylemciye çözümü sunmak yoluna gidilmektedir. Mizansen operasyonlarda, niyeti hakkında şüphe bulunan potansiyel eylemciye gerekli kapasite sunulmakta ve suçüstü ile sürecin neticelendirilmesi yoluna gidilmektedir. Bu sayede aktör söylemden eylem aşamasına kontrollü bir şekilde geçirilmekte ve sistemden ayıklanmaktadır.

SONUÇ

Bu çalışmada açık kaynak istihbaratı üzerinde istihbarat çalışmaları literatüründe yer alan bazı temel tartışmalara değinilmiştir. Bu tartışmalar; istihbaratın demokratikleşmesi, toplama-analiz ikiliği, görev ve kadro tanımlarındaki dönüşüm, açık kaynakların önleyici istihbarattaki güçlü ve zayıf yanları ile istihbarat zafiyeti başlıklarında incelenmiştir. Şaşırtıcı olmayacak şekilde birçok senaryoda gri alanların bulunduğu görülmüştür.

Öncelikle, insanların sosyal paylaşım platformlarında paylaştıkları görüntü ve mesajlar üzerinden "büyük sonuçlara ulaşmak" istihbaratçılık değildir. Özellikle taktik istihbarat boyutunda hala gizli haber toplama

yöntemleri kullanarak hedefe yaklaşmak gerekmektedir. Diğer taraftan stratejik analiz boyutunda önemli bir demokratikleşme fırsatı yakalandığı da söylenebilecektir. Özellikle dış politika ya da ekonomi gibi alanlarda uzman özel sektör bileşenleri her geçen gün daha fazla bilgiye ulaşabilmekte ve bu da stratejik analizi demokratikleştirmektedir.

İkincisi, açık kaynaklar her ne kadar toplama boyutuyla gündeme gelse de aslında bir analiz meselesidir. Bunun nedeni internet üzerinden yapılan toplama işleminin bir standart haline gelmekle birlikte, analizin halen bir yetenek olmasıdır. Toplanan her bilgi istihbarat anlamına gelmemekte ve analiz aşamasının üstüne ilave sorumluluk olarak binmektedir. Bu nedenle analiz aşamasının öneminin arttığı ve açık kaynakların toplama-analiz ikiliğinde sarkacı analiz boyutuna çevirdiği söylenebilecektir.

Üçüncü olarak açık kaynak teknolojisi istihbarat alanındaki kadroları ve görev tanımlarını da dönüştürmektedir. Teknoloji sayesinde toplama ve analiz arasındaki geçirgenlik artmış ve analizciler giderek kendi toplayıcıları haline gelmiştir. Bu nedenle toplayıcılardan giderek daha fazla gizli ve operasyona dönüştürülebilir bilgi talep edilmektedir. Ayrıca, özellikle analiz boyutunda teknoloji merkezli yeni görev tanımları ortaya çıkarken, tercümanlık gibi bazı kadrolar da önemini yitirmektedir.

Dördüncüsü, açık kaynaklar proaktif olmaktan ziyade reaktiftir. Bu nedenle özellikle güvenlik/terör istihbaratındaki önleyici gücü kısıtlıdır. Diğer taraftan geriye doğru işleyen tahkikat aşaması için çok güçlü bir kabiliyet sunmaktadır.

Beşincisi, önleyici istihbarat açısından birtakım potansiyeller de vaat etmektedir. Siber alan hakimiyeti üzerinden vasatın kontrol edilmesi ve radikalleşme emarelerinin tespiti bu açıdan değerlendirebilir. Özellikle yalnız aktörlerin eylem öncesinde kapasite ve niyeti hakkında sosyal medyada önemli belirtiler verdikleri bilinmektedir.

Son olarak, açık kaynaklar istihbarat zafiyeti konusunun daha sık gündeme gelmesine neden olmuştur. Kuşkusuz ki eylem öncesinde hedef önceliklerinin belirlenmesi, toplama, analiz ya da neticelendirme aşamaları üzerinden hatalar yapılabilir. Diğer taraftan, açık kaynak teknolojisindeki ilerlemenin zafiyet başlığı altında yapılan yorumlardaki öngörü yanılgılarını arttırdığı görülmektedir.

KAYNAKÇA

Ball, K. Webster, F. (2003) The intensification of surveillance. Ball, K. Webster, F. (Ed.). The intensification of surveillance: crime, terrorism and warfare in the information içinde (ss.1-15). Pluto Press.

Barnea, A. (2018). Challenging the "lone wolf" phenomenon in an era of informant. *International Journal of Intelligence and Counterintelligence*. 31(2). 217-234.

Barnea, A. (2019) Big data and counterintelligence in western countries. *International Journal of Intelligence and counterintelligence*. 32(3). 433-447.

Brynielsson, J. Horndahl, A. Johansson, F. Kaati, L. Mårtenson, C. ve Svenson, P. (2013) Harvesting and analysis of weak signals for detecting lone. *Security Informatics*. 2(11). 1-15.

Denécé, E. (2014). The revolution in intelligence affairs: 1989–2003, *International Journal of Intelligence and Counterintelligence*. 27(1): 27-41.

Field manuel 2-0 intelligence. (2007). United States Army Press.

Freedman, L. (1977). U.S. Intelligence and the soviet strategic threat. Princeton University Press.

Gill P. ve Phythian M. (2018). *Intelligence in an Insecure world.* Polity Press Cambridge.

Goldman, A. (2016). Why didn't the F.B.I. stop the New York bombing? Erişim tarihi: 24 Ekim 2018. https://www.nytimes.com/2016/09/22/us/fbi-terror-ahmad-khan-rahami.html.

Herman, M. (1998). Diplomacy and intelligence, *Diplomacy & Statecraft*, 9(2). 1-22.

https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/ Erişim tarihi: 24 Ekim 2018.

https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/?s=03 Erişim tarihi: 24 Ekim 2022.

https://www.egm.gov.tr/02072020-tarihli-basin-aciklamasi Erişim tarihi: 24 Ekim 2022.

https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched Erişim tarihi: 20 Ekim 2022.

https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf Erişim tarihi: 14 Ekim 2022.

https://www.i-scoop.eu/big-data-action-value-context/data-age-2025-datasphere/#:~:text=In%20the%20announcement%20of%20the,a%20yearly%20basis)%20by%202025. Erişim tarihi: 24 Ekim 2022.

https://www.statista.com/statistics/949144/worldwide-global-datasphere-real-time-data-annual-size/ Erişim tarihi: 24 Ekim 2022.

Hulnick, A.S. (1999) Fixing the spy machine: Preparing American intelligence for the twenty-first century. Praeger.

James J. Wirtz, ve Rosenwasser, J.J. (2010). From combined arms to combined intelligence: philosophy, doctrine and operations, *Intelligence and National Security*, 25(6). 725-743.

Johnson, L.K. (2009). Sketches for a theory of strategic intelligence. Gill, P. Marrin,S. ve Phythian, M. (Ed). Intelligence theory key questions and debates içinde. (ss.33-53). Routledge.

Johnson, L.K. (2010). National security intelligence. Johnson, K.L. (Ed). The oxford handbook of national security intelligence içinde. (ss.3-32). Oxford University Press.

Johnson, L.K. (2014). The development of intelligence studies. Dover, R. Goodman, M. ve Hillebrand, C. (Ed). Routledge companion to intelligence studies içinde. (3-22). Routledge.

Joint publication 3-25 countering threat networks. (2016). United States Army Press.

Krebs, V.E. (2002). Mapping networks of terrorist cells. *Connections*. 24(3): 43-52.

Lowenthal, M. (2008). Intelligence: From secrets to policy. CQ Press.

Lahneman, W.J. (2006). The future of intelligence analysis volume I final report. University of Maryland.

Shulsky, A.N. ve Schmitt G.J. (2002). Silent warfare: Understanding the world of intelligence. Potomac Books.

Sparrow, M.K. (1991). Network vulnerabilities and strategic intelligence in law enforcement. *International Journal of Intelligence and counterintelligence*. 5(3). 255-274.

Steele, R.D. (2007). Open source intelligence. Johnson, K.L. (Ed). Handbook of intelligence studies içinde. (ss.129-147). Routledge

Treverton, G.F. Jones, S.G. Boraz, S. Lipscy, P. (2006). Toward a theory of intelligence. RAND Corporation.

Treverton, G.F. C. Gabbard, B. (2008). Assessing the tradecraft of intelligence analysis. RAND Corporation.

Treverton, G.F. (2009). Intelligence for an age of terror. RAND Corporation. Cambridge University Press.

Williams, P. (2001). Transnational criminal networks. Phil Arquilla, J. Ronfeldt, D.F. (Ed). Networks and netwars: The future of terror, crime, and militancy içinde. (ss.61-98). RAND Corporation.

Wheaton, K.J. (2019). How to teach 2500 years of intelligence history in about an hour. Erişim tarihi: 11 Ekim 2022. https://sourcesandmethods.blogspot.com/2019/06/how-to-teach-2500-years-of-intelligence.html.

Wohlstetter, R. (1962). Pearl harbor warning and decision. Stanford University Press.

Woo, G. (2011). Interdiction of plots with multiple operatives. Wiil, U.K. (Ed). Counterterrorism and open-source intelligence içinde. (ss.49-60) Springer-Verlag.

Younger A. MI6 'C' speech on fourth generation espionage, Erişim tarihi: 11 Mayıs 2022. https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage.