İstihbarat Çalışmaları ve Araştırmaları Dergisi

Journal of Intelligence Research and Studies

Haziran 2022, Cilt: 1, Sayı: 1, ss.23-59

June 2022, Volume: 1, Issue: 1, pp.23-59

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

Makaleye ait Bilgiler / Article Information

Araştırma Makalesi / Research Article

Makale Başvuru Tarihi / Application Date : 14 Mart 2022 / 14 March 2022

Makale Kabul Tarihi / Acceptance Date : 07 Mayıs 2022 / 07 May 2022

Makale Yayım Tarihi / Publication Date : 30 Haziran 2022 / 30 June 2022

Makalenin Başlığı / Article Title

Açık Kaynak İstihbaratı ve Askeri İstihbarat

Open-Source Intelligence and Military Intelligence

Yazar(lar) / Writer(s)

Kazım Mehmet EROL

Atıf Bilgisi / Citation:

Erol, K.M. (2022). Açık Kaynak İstihbaratı ve Askeri İstihbarat. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 1(1), ss.23-59, DOI: http://dx.doi.org/10.29228/trad.4

Erol, K.M. (2022). Open-Source Intelligence and Military Intelligence. *Journal of Intelligence Research and Studies*, 1(1), pp. 23-59, DOI: http://dx.doi.org/10.29228/trad.4

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, 2022, 1(1) Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2022, 1(1) Research Article
DOI: http://dx.doi.org/10.29228/icad.3

AÇIK KAYNAK İSTİHBARATI VE ASKERİ İSTİHBARAT

Kazım Mehmet EROL *

ÖZET

İçerisinde bulunduğumuz bilgi çağında, etkisi ve hacmi giderek genişleyen "Açık Kaynak İstihbaratının" (AKİS) istihbarat analizcileri ve toplayıcıları ile karar vericilere büyük oranda yardım ettiği görülmektedir. Farklı dillerde yayımlanan haber kaynaklarından sosyal medya platformlarına, çevrimiçi haritalardan, sivil toplum örgütleri, diplomatik ve askeri kurumların raporlarına kadar AKİS, bize girift ve mozaik bir yapıda istihbarat sağlama imkânı sunmaktadır. İstihbarat, askerî harekâtın planlama sürecini yönlendiren ve destekleyen en önemli güçtür. Kaynakların verimli şekilde kullanılması maksadıyla askeri istihbarat sağlamada toplama gayretleri uygun şekilde planlanmalı ve her aşamada gözden geçirilmelidir. Hibrit savaş, bilgi harekâtı ve siber alan gibi çeşitli ve belirsiz ortamlar, muharebe sahasını daha karmaşık hale getirmiştir. Bütün bu ortamlara yönelik ihtiyaçları karşılama potansiyeli olan ve oldukça geniş imkânlar sunan AKİS'ten faydalanabilmek önemli hale gelmektedir. Bu makalede AKİS'in potansiyelinden askeri istihbarat alanında yeterince faydalanılmadığı ve AKİS'in askeri istihbaratta faydalanıldığı alanlarda uygun süreç ve yöntemlerden eksik olduğu olmak üzere iki önemli sav üzerinde durulmuştur. Çalışmanın amacı AKİS'in uygun metotların uygulanması ve diğer istihbarat disiplinleri ile eşgüdüm halinde kullanılması halinde askeri istihbarat alanında değerli bir disiplin olabileceğini ortaya koymaktır. Bu maksatla öncelikle AKİS ve askeri istihbaratın genel durumu, tarihsel gelişimi, AKİS'in farklı seviyelerde askeri istihbaratta kullanımı ve diğer istihbarat vasıtalarıyla ilişkisi, AKİS süreci, yöntemleri ve uygulamaları incelenmiştir.

Anahtar Kelimeler: *İstihbarat, Açık Kaynak İstihbaratı, Askeri İstihbarat, AKİS Tarihi, AKİS Yöntemleri.*

ABSTRACT

OPEN SOURCE INTELLIGENCE AND MILITARY INTELLIGENCE

In the information age we live in, it is seen that open-source intelligence (OSINT), which become increasingly voluminous and effective, sheds light on issues and assists to elaborate and understand them by all intelligence analysts/collectors and decision-makers. From media sources in different languages to social media platforms and online maps to reports of NGOs and diplomatic/military institutes, OSINT provides with means of obtaining intelligence in a grift and mosaic structure. Intelligence is the main driving and supporting force in the planning process of military operations. In order to exploit the sources more effectively military intelligence collection efforts should be planned and reviewed properly.

* Araştırmacı, Güvenlik Yönetimi (İstihbarat) Bilim Uzmanı, kmerol@hotmail.com, ORCID: 0000-0003-4427-5260

Makale Başvuru Tarihi / Application Date: 14 Mart 2022 / 14 March 2022

Makale Kabul Tarihi / Acceptance Date: 07 Mayıs 2022 / 07 May 2022

Diverse and ominous environments such as hybrid war, information operations and cyberspace complicated the theatre. Therefore, it is becoming increasingly important to be able to adequately benefit from OSINT, which has the potential to meet the needs of all these environments and offers a wide range of opportunities. In this article, two main arguments are emphasized, namely that the current potential of OSINT is not adequately benefited in military intelligence and even in the areas OSINT is utilized in military intelligence it lacks appropriate methods and processes. The aim of the study is to demonstrate that OSINT can be a valuable discipline in the field of military intelligence if appropriate methods are applied and used in coordination with other intelligence disciplines. For this purpose, first of all the general situation of OSINT and military intelligence, its development in the historical process, the use of OSINT in military intelligence at different levels and its relationship with other intelligence tools, and finally the OSINT process, methods and applications were examined.

Keywords: *Intelligence, Open-Source Intelligence, Military Intelligence, History of OSINT, OSINT Methods.*

GİRİŞ

Açık Kaynak İstihbaratı (AKİS); belirli istihbarat ihtiyaçlarını karşılamak maksadıyla genel kamu kullanımına açık veri veya bilginin toplama, analiz, işlem ve yayım süreçlerinden geçirilmesiyle elde edilen istihbarat ürünüdür. AKİS'in, istihbarat toplulukları dışındaki birçok alanda da giderek önem kazandığı ve yaygın kullanıma kavuştuğu bilinmektedir (Böhm ve Lolagar, 2021, s. 1).

AKİS'in istihbarat elde etme gayretleri içerisinde önemli yer tuttuğu görülmektedir. AKİS'in siyasi istihbarat, ekonomik istihbarat, sosyal istihbarat, bilimsel ve teknolojik istihbarat, coğrafi istihbarat, siber istihbarat ve hatta biyografik istihbarat gibi alanlarda kullanımının yaygın olarak benimsendiği birçok örneklerle görülmektedir. Ancak bu durumun askeri istihbarat için de aynı olduğunu söylemek güç olacaktır. Aslında uygun bir teşkilatlanma, işleyiş ve duruma dayalı yöntemlerle AKİS, Askeri İstihbarat için de vazgeçilmez bir vasıta olabilmektedir.

Silahlı kuvvetler tarafından kullanılan istihbarat anlamına gelen Askeri İstihbarattan söz edildiğinde, ilk akla gelen istihbarat toplama teknikleri sırasıyla; İnsan İstihbaratı (İNİS), Görüntü İstihbaratı (GÖRİS) ve Sinyal İstihbaratı (SİNİS) vasıtaları olmaktadır (Gudgin, 1999, ss. 106-107). İstihbarat toplulukları, çağın değişen şartlarına paralel olarak hızlı bir evrilme içerisindedir. İNİS, GÖRİS ve SİNİS gibi istihbarat disiplinlerinde önemli gelişmeler olduğu görülmekle birlikte, şüphesiz en büyük atılım AKİS alanında olmuştur. Müşterek ve hibrit savaşın askeri operasyonlarda

etkisinin yoğun olarak görüldüğü günümüzde, askeri istihbarat çağa ayak uydurmak, imkân ve kabiliyetlerini geliştirmek durumunda kalmaktadır.

Askeri İstihbarat açısından AKİS; hızlı bir şekilde elde edilmesi ve maliyetsiz olması sayesinde analizcilere ve komutan/karar alıcılara planlamaya yönelik öngörü sağlaması, aşina olunmayan bir bölgeye yönelik harekât söz konusu olduğunda medya, harita uygulamaları, akademisyen ve diğer uzmanların ürünlerinden faydalanılarak ilk aşamada istihbarat elde edilmesi, uygun toplama planıyla AKİS ile elde edilecek istihbarattan diğer vasıtalardan tasarrufa gidilerek asıl istihbarat ihtiyaçlarında sıklet merkezi sağlanması ve son olarak müşterek ve birleşik harekâtlarda gizli istihbarat paylaşılmasının sakınca yaratacağı durumlarda tek vasıta olması hasebiyle ön plana çıkmaktadır (JMITC, 1996, s.78).

İçerisinde bulunduğumuz bilgi çağında çevrimiçi ve sosyal medya platformları üzerinden devasa boyutlara ulaşan veri girişleri sonucu ortaya çıkan bilgi yığınlarının, AKİS'in istihbarat örgütleri ve güvenlik uzmanları tarafından uygulanmasını ve kontrol etmesini zorlaştırması, bu durumu yasa dışı gruplar ve örgütlerin istismarına açık hale sokmaktadır. AKİS'in karanlık tarafı ile ilgili vurgulanması gereken diğer bir husus da istihbarat örgütleri ve güvenlik uzmanlarının kullanımına açık olan bu disiplinin, aynı seviyede terör ve suç örgütleri ile diğer devlet dışı silahlı grupların da kullanımına açık olmasıdır.

Konu kapsamında yapılan literatür taramasında; "Açık Kaynak İstihbaratı" kapsamında 61uluslararası ve 4 ulusal tez, yaklaşık 300 uluslararası ve 9 ulusal makale ile 15 uluslararası kitap tespit edilirken ulusal alanda kitaba rastlanmamıştır. "Askeri İstihbarat" kapsamında uluslararası alanda yaklaşık 32 ve ulusal 1 tez, uluslararası alanda yaklaşık 50 ve ulusal 9 makale ile uluslararası alanda 10 kitap ve 1 ulusal kitap tespit edilirken, her iki konuyu birlikte işleyen uluslararası ve ulusal alanda herhangi bir teze veya kitaba rastlanmazken, uluslararası alanda 1 kitap, 1 tez ve yaklaşık 8 adet makaleye rastlanmıştır. Bu çalışmanın özgün yanı, açık kaynak istihbaratı ve askeri istihbaratın aynı çerçevede ele alınarak arasındaki ilişkinin ve metodolojinin ortaya dökülmesidir. Bu doğrultuda literatüre katkı sunulması hedeflenmiştir.

Bu makalede; birincisi "AKİS'in mevcut potansiyelinden askeri istihbarat alanında yeterince faydalanılıyor mu?" ve ikincisi "AKİS hangi

yöntemler ve nasıl bir süreç kullanılarak askeri istihbaratta faydalı olabilir?" olmak üzere iki sorunun cevabı bulunmaya çalışılacaktır.

Bu minvalde birinci bölümde; öncelikle AKİS ve askeri istihbaratın tarihsel süreçte ilişkisi ve gelişimi, ikinci bölümde; AKİS'in farklı seviyelerde askeri istihbarat alanında kullanımı ve diğer istihbarat vasıtalarıyla ilişkisi, üçüncü bölümde ise; AKİS süreci, yöntemleri ve uygulamaları kapsamında AKİS'i oluşturan terimler ve kavramsal çerçeve, AKİS'in avantaj ve dezavantajları, AKİS çarkı, AKİS'te güvenirlik testi ve sınıflandırma ve son olarak AKİS toplama yöntemleri incelenmiştir.

1. AKİS VE ASKERİ İSTİHBARATIN TARİHSEL SÜREÇTE GELİŞİMİ

Dünya tarihinde istihbaratın silahlı kuvvetler için kullanılması, savaş tarihi kadar eski olmakla birlikte, askeri istihbaratın da bu sanatın en eski hali olduğu kabul edilmektedir. İstihbaratın gelişimi içerisinde Askeri istihbarat ve açık kaynak istihbaratı yan yana görülmektedir, ancak özellikle modern çağda askeri istihbarat ile AKİS ilişkisinin bilginin yaygın olarak elde edilmesinin sonucu olarak güçlü örneklerinin ortaya çıktığı görülmektedir.

AKİS günümüzün dijital dünyasıyla beraber gelen sosyal medya, internet, açık kaynak yazılımları ile birlikte daha fazla bilinmeye başlansa da asıl yaygın kullanımı Birinci ve İkinci Dünya savaşlarında politik istihbarat ve daha çok askeri istihbarat sağlamak maksadıyla takip edilen gazete haberlerinin kesilerek tasnif edilmesine dayanmaktadır (Böhm ve Lolagar, 2021, s. 2).

15'inci yüzyılda matbaanın ortaya çıkması, bilginin ve düşüncelerin yayılma hızını artırması neticesinde, kriptolama/şifreleme ve açık kaynak istihbaratı gibi beklenmedik istihbarat sanatları ortaya çıkmıştır. (Andrew, 2018, s. 126). Rönesans dönemi ve Venedik ile başlayan ticari ve politik istihbaratta yaşanan gelişmelerin temel kaynağını, casuslar ve kurulan ticari ağlar üzerinden hareket eden tüccarların getirdiği "avvisi" olarak adlandırılan haber bültenleri sayesinde elde edilen açık kaynak istihbaratı oluşturmuştur. (Infelise, 2002, ss.1-3).

1800'lü yıllarda savaş öncesi kapsamlı hazırlık yapmalarıyla bilinen Napolyon ve Büyük Frederick, genelkurmay benzeri karargâh teşkilatlanmalarına gitmiş ve böylece istihbarat, karargâh birimlerinden biri

haline gelmiştir. Yine Napolyon'a karşı savaşmış olan Clausewitz "Savaş Üzerine" adlı eserinde bilgi ve istihbaratın önemine dair birçok bölüm ele almış, savaşta belirsizlik ve karmaşanın azaltılmasını vurgulamıştır. Görüldüğü üzere askeri istihbaratın kurumsallaşmasının temelleri böylece atılmaya başlanmıştır (Akad, 2018, ss.26-33). Diğer taraftan Napolyon açık kaynak istihbaratına gizli kaynaklardan daha çok önem vermiştir. Napolyon'un bir taraftan istihbarat raporlarının olduğu kadar gazetelerin dikkatle okuması, diğer taraftan bu alanda gizliliğe önem vermesi önemli örneklerdir (Hanley, 2005, s.13).

Tarihte ilk defa, devlet yetkilileri 19'uncu yüzyılda muharebe alanında yaşanan gelişmeleri ve önemli olayları askeri istihbarat raporlarından önce açık kaynaklardan öğrenmeye başlamıştır (Andrew, 2018, s.404). Bu dönemde istihbarat alanında teknolojiden de faydalanılmaya başlandığı görülmüştür. Dönemin iletişim imkânları olan demiryolları ve telgraf haberleşme sistemi, etkin bir şekilde kullanılmıştır (Özdağ, 2013, s.48).

İstihbarat çalışmalarında geleneksel yöntemlerle yeni yöntemlerin birleştiği I. Dünya Savaşı istihbaratla bilim arasında bağlantı kurmuştur. Dünyanın hava keşfi ve SİNİS yöntemlerinin kullandığı istihbarat çağına girdiği bu savaşta, en hızlı gelişen istihbarat alanları SİNİS ve ELİS olmuştur (Akad, 2018, s.221). Tabi ki bu dönemde AKİS'in kullanmaya yönelik gelişmelere değinmeden geçilemeyecektir. Gazeteler, kitaplar ve seyahat notları gibi basılı yayımlar sayesinde istihbarat toplama ve analizi gerçekleştirilebilmiştir.

II. Dünya Savaşı istihbaratın teknolojiden en çok faydalanmaya başladığı dönem olarak nitelendirilebilir. SİNİS ve GÖRİS gibi yöntemler İNİS ile birlikte kullanılmaya başlanmıştır. Bu dönemde Almanya'nın askeri istihbaratının temelini açık kaynaklar oluşturmuştur. İstihbarat konusunda Sovyetlerden ziyade Fransa'ya ağırlık veren Almanlar için Fransa Ordusu hakkında istihbarat elde etmek için açık kaynaklar kapalı kaynaklardan daha kıymetli veriler sunmuştur (Andrew, 2018, s.454). Britanya konusunda da "Alman Savaş Ofisi" basılı yayınlardan elde edilen istihbaratın casuslardan elde edilenlerden daha doğru olduğuna kanaat getirmiştir (Andrew, 2018, s.474). Yine 1900'lerde Britanya'nın Kahire'de bulunan "Askeri İstihbarat Ofisi" GÖRİS, SİNİS, İNİS ve AKİS kaynaklarından elde edilen istihbaratı analiz ederek, günlük ve değerlendirme raporları halinde hükümete yayımlamıştır (Andrew, 2018, s.532).

1939'da Birleşik Krallık'ta kurulan, devlet ve sivil kurumlarca desteklenen, "BBC Monitoring" servisi öncü bir kurum olmuştur (Hassan ve Hijazi, 2018, s.7). Modern dönemde AKİS'in kurumsallaşmasında öncülük eden ülke ABD olmuştur. 1930'larda Princeton Üniversitesinde yabancı radyo kanallarını takip etmek için ve 1941 yılında yabancı medya veri ve bilgilerinin toplanması ve analiz edilmesi maksadıyla kurulan "Yabancı Medya Takip Servisi" (Foreign Media Monitoring Service), 1947'de Yabancı Medya İstihbarat Servisi (Foreign Media Intelligence Service), müteakiben ABD'de meydana gelen 9/11 saldırısına yönelik oluşturulan komisyonun AKİS elde etmek maksadıyla istihbarat ajansı oluşturulması yönündeki raporunun ardından 2005'te oluşturulan "Açık Kaynak Servisi" *(Open Source Center)* bu alanda ilk defa teşkil edilen kurumsal yapılar olmuştur.

Soğuk Savaş döneminde Anglo-Amerikan istihbarat ittifakı istihbarat alanında teknolojik ve organizasyonel reformlarla Sovyetler'in askeri kabiliyetleri ve konuş durumları hakkında, açık kaynak istihbaratı ile imkân kabiliyet ve niyetleri hakkında istihbarat sağlarken, bu ittifakın istihbarat toplama kabiliyetlerine erişemeyen Sovyetler Birliği, Çin ve diğer Sovyetler gelişmiş casusların yanı sıra AKİS Batı'nın silah sistemlerindeki gelişmeleri ve istihbarat toplama yetenekleri konusunda istihbarat sağlamada temel vasıta olmuştur. ABD'nin uzay çalışmalarını da söz konusu devletler AKİS üzerinden takip etmişlerdir (Mercado, 2010, s.2). Yine Soğuk Savaş döneminde liderlerin basın açıklamaları, demeçleri ve röportajları, özellikle ABD ve Rusya'nın silah sistemleri hakkında basına yansıyan haber ve görüntüler ile söz konusu ülkelerin gövde gösterisi kapsamında icra ettikleri askeri geçit törenleri ülkelerin imkân ve kabiliyetleri, niyet ve maksatları ile gelecek vizyonları hakkında önemli açık kaynak istihbaratı sağlamıştır.

II. Dünya Savaşı ve Soğuk Savaşı döneminde hedef ülkelerden ajanlar ve uzmanlar vasıtasıyla taşınan gazete, dergi gibi AKİS kaynakları günümüzde tek tıkla erişilir hale gelmiştir. 20'nci yüzyılın sonlarından itibaren günümüze kadar teknolojik gelişmeler istihbaratın merkezine yerleşmiş, devletlerden uluslararası kuruluşlara, suç örgütlerinden terör gruplarına kadar geniş bir yelpazedeki küresel aktörlerce bireylerin bütün faaliyetleri gözetlenir hale gelmiş ve bu küresel aktörler teknolojik istihbaratın yanı sıra, açık kaynak istihbaratı ve büyük veri gibi günümüzün ve geleceğin istihbaratını şekillendirecek önemli faktörleri kullanmaya başlamış veya bu yönde çaba göstermiştir.

2. AKİS'İN ASKERİ İSTİHBARAT ALANINDA KULLANIMI

İstihbarat askerî harekâtların planlama sürecini veya terminolojik adıyla Askeri Karar Verme Sürecini (AKVES) yönlendiren ve destekleyen asıl güçtür. Kaynakların en verimli şekilde kullanılması için askeri istihbarat toplama gayretleri her aşamada gözden geçirilmelidir (MI Publications, 2021, s. 10) Askeri istihbarat elde etmede kullanılan SİNİS, GÖRİS, Ölçüm ve İz İstihbaratı (ÖLİZİS), Jeo-uzamsal İstihbarat (JEOİS) ve belirli seviyede İNİS vasıtalarının kullanımına yönelik teorik ve metodolojik açıdan nispeten oturmuş ve yaygın kullanıma kavuşmuş yazılı uygulamalar mevcutken, AKİS için bu seviyelerde uygulamaların bulunduğunu söylemek güç olacaktır. Söz konusu vasıtalar içerisinden kullanımı en yaygın ve maliyeti en düşük olan AKİS, ne yazık ki en fazla yanlış anlaşılan ve hatalı uygulamalara maruz kalan disiplin olagelmiştir.

Harekât alanlarına yönelik komutanların askeri istihbarat ihtiyaçlarının çoğu AKİS ile sağlanabilmektedir. AKİS toplama araç ve yöntemleri uygun şekilde entegre edilir, bu sürece yerel, kültürel ve dil alanında uzmanların da dahil edilmesiyle AKİS'in etkinliği daha da artırılabilmektedir (MI Publications, 2021, s.71).

Askeri İstihbarat açısından sivil ve coğrafi faktörler ile askeri yetenekler hakkında arama ve istihbarat tahminleri elde etmede kullanılsa da AKİS geniş bir askeri istihbarat analiz modeli geliştirmek maksadıyla kullanıldığında daha etkili olmaktadır. (JMTC, 1996, s.77).

2.1. Farklı Seviyelerde Askeri İstihbarat açısından Açık Kaynak İstihbaratı:

2.1.1. Stratejik Seviye

AKİS, düşman niyet ve maksadı ile askeri yönden avantaj sağlayacak fırsatlar konusunda gösterge ve uyarılar sunabilir. Yerel dilde ve yerel basından elde edilen medya kaynakları çoğu zaman örtülü kaynaklara nazaran daha güvenilir ve daha kapsamlı olabilmektedir. AKİS diğer istihbarat vasıtaları tarafından tam olarak karşılanamayan kültürel ve sosyal istihbarat konusunda oldukça değerli olabilmektedir. AKİS askerî harekâtlara etki eden coğrafi ve sivillere yönelik yerel çalışmalarda faydalı bilgiler sunabilir (Steele, 1997, s. 3). Araç, silah ve teçhizatların hedef bölgenin coğrafi şartlarına ve meskûn mahal durumuna uygun üretilmesi ve

modernize edilmesine yönelik çalışmalarda AKİS önemli bir yol gösterici olabilir.

Askerî harekât düzenlenecek bölgenin tarihi, geçmiş dönemlerde yabancı güçlerin söz konusu bölgedeki etkisi konusunda gerekli olan temel istihbarat AKİS ile sağlanabilir. (Steele, 2004, s.19) Bunun dışında AKİS; askeri istihbarat için gerekli olan politik, kültürel, demografik, coğrafi, askeri bilgiler ve liderlere/komutanlara ait biyografik istihbarat bilgileri, savunma sanayi alanında teknik istihbarat ile milis/isyancı/terörist grupların ideolojileri, finansmanı, sponsor-vesayet bağlantısı, yapılanması, sayısı, etkinlik seviyesi, genel konuş durumu ve halkla irtibat düzeyi gibi konularda önemli bir vasıtadır.

2.1.2. Operasyonel Seviye

AKİS mevcut durum hakkında bir anlayış oluşturmada ve açık kaynak bilgisini muharebe sahası ile ilişkilendirmede önemli bir vasıtadır (Steele, 2004, s.19). AKİS bölgesel kuvvet planlamaları ve birlik konuşlandırma faaliyetleri öncesinde coğrafi ve sivil alanlarda değerli bilgiler sunabilir. Özellikle AKİS, harekât hazırlığındaki komutanın karşılaşabileceği kuvvetlerinin imkân ve kabiliyetleri hakkında teknik askeri bilgiler, hedef bölgede intikal, görüş mesafesi, sıcaklık, su durumu gibi coğrafi etmenler ile limanların durumu, köprüler, internet ve muhabere altyapısı gibi konularda bilgi sağlayabilir. (Steele, 1997, s. 4).

AKİS müşterek ve koalisyon halinde operasyonlar söz konusu olduğunda diğer istihbarat vasıtalarının kullanılamayacağı veya yabancı unsurlar ile paylaşım sorunu olan durumlarda en iyi vasıta olarak ortaya çıkmaktadır. AKİS operasyonel seviyede; hava durumu, su kaynakları, yerleşim yerleri gibi askerî harekâta etki eden hususları, harp araçlarına ait teknik istihbarat ile milis/isyancı/terörist grupların kullandığı silahlar, imkân ve kabiliyetleri, konuş durumu gibi konularda önemli bir vasıtadır.

2.1.3. Taktik Seviye

AKİS silahlanmayı önleme, terörizmle mücadele ve barışı koruma operasyonları gibi muharebe alanlarında yeni ortaya çıkan durumlarda oldukça etkili ve uygun bir araç olarak kullanılabilir. AKİS hem konvansiyonel hem de örtülü ve özel harekât operasyonlar için faydalı bir vasıtadır. AKİS komutanların yeni bir harekât alanına karşı hazırlıklarında

resmi ve kurumsal haritaların yetersiz olması durumunda açık kaynak haritaları ve diğer açık dijital görsel uygulamalar oldukça kritik ve hayat kurtarıcı kaynaklar olabilirler (Steele, 1997, s. 5).

AKİS taktik seviyede; bölge halkının, ailelerin ve aşiretlerin yapısı, kanaat önderleri ve etki alanları, konuşulan yerel dil ve lehçeler, harekât bölgesine yönelik dijital haritalar, milis/isyancı/terörist grupların moral seviyesi, halk desteği alma durumu hakkında bilgi verebilir. Yerel halkın olayları ve kavramları algılama şekli (terörist-gerilla, dost asker-işgalci asker, radikalizm-dine bağlılık gibi farklı uç noktalarda algılanabilir.) göz önünde bulundurulması gereken hassas bir konudur. Örneğin Irak'ın Sincar bölgesindeki terör örgütlerine yönelik icra edilecek bir harekât öncesinde bölge halkı Yezidilerin etnik ve dini özelliklerine, kanaat önderlerine, farklı bağlantılı Yezidi milis gruplarına ve Yezidilerin bölgelerindeki yabancı unsurlara yönelik bakış açılarına yönelik AKİS çalışması yürütülmesi oldukça faydalı olabilecektir.

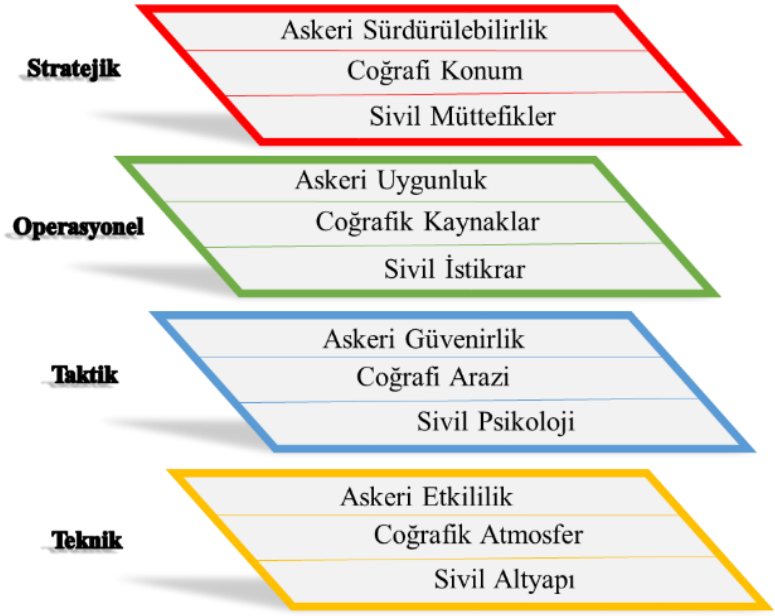
2.1.4. Teknik Seviye

Askeri etkililik (silahların isabet ve imha etkisi, teknik kapasitesi v.b.), coğrafya ve meteorolojik analiz, askeri amaçla kullanılabilecek sivil teknolojik kapasiteler harbin başarısında oldukça önemlidir. Bu konularla ilgili istihbarat elde etmede AKİS en önemli kaynaklardan biridir (JMTC, 1996, s.81).

Savunma sanayi, ülkenin milli üretim kapasiteleri, nükleer kapasite geliştirme çabaları (İran örneği) ve askeri alandaki bilimsel çalışmalarının ortaya koyulmasında AKİS iyi bir konuma sahiptir. AKİS aynı zamanda havaalanları, demiryolları, limanlar, tali ve ana yollar hakkında istihbarat sağlaması hasebiyle lojistik ve mobil sistemlerin planlamalarının omurgasını oluşturur.

Bahse konu seviyelerin hepsini kapsayacak şekilde AKİS, Askeri İstihbaratın planlamaya yönelik unsurları olan; Bilgi Harekâtı, Psikolojik Harekât ve Hedef İstihbaratı elde etmede de kullanılabilmektedir.

Şekil 1. Farklı Seviyelerde Harekâta Yönelik Açık Kaynak İstihbaratı
(Kaynak: NATO OSINT Handbook, 2001, s.15)



2.2. AKİS'in Diğer İstihbarat Vasıtaları ile İlişkisi

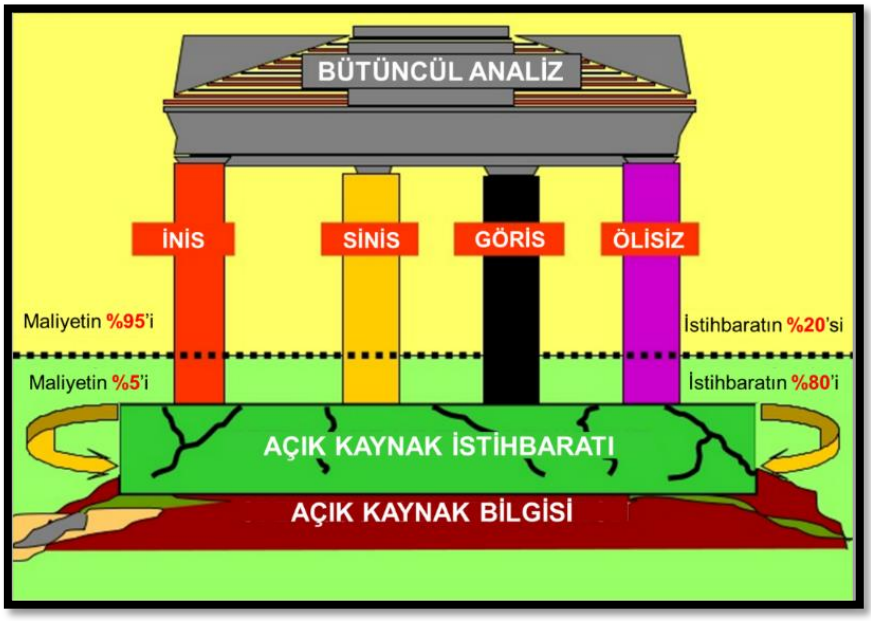
Askeri unsurlar yeni görev aldıklarında, bu vazife özellikle de aşina olunmayan bir harekât ortamında icra edilecek ise içgüdüsel olarak ilk yaptıkları eylem temel bilgileri almak maksadıyla internet ortamına yönelmektir. Bu anlamda AKİS farkındalık ve istihbarat elde etmede başlangıç noktası ve ipucu olma özelliği taşımaktadır. İstihbarat üretim ve analiz sürecinde ilk adım olarak öncelikli istihbarat ihtiyaçları ve emareler oluşturulduktan sonra, AKİS'in bunlardan hangilerine katkı sunabileceğine, münferit disiplin olarak mı yoksa bütüncül yaklaşım çerçevesinde mi kullanılacağına karar verilmelidir (MI Publications, 2021, s. 74). AKİS'in etkili bir şekilde SİNİS, İNİS, GÖRİS, JEOİS ve ÖLİZİS ile irtibatlandırılabileceği rahatlıkla söylenebilir (Williams ve Blum, 2020, s. 9).

AKİS'in de diğer istihbarat vasıtalarında olduğu gibi bir takım istihbarat açıkları/boşlukları ve zaafiyetleri bulunmaktadır. Bu açık ve zaafiyetler diğer istihbarat vasıtaları ile kapatılmaya çalışılmaktadır.

ABD Ordusunun "FM 2-0 Intelligence" isimli talimnamesinde AKİS tek başına veya diğer istihbarat disiplinleri ile entegre şekilde kullanılabildiği için ayrı bir istihbarat disiplini olarak değil, yani "Bütüncül İstihbarat

Disiplini" *("All-Source Intelligence")* olarak da ele alınmıştır. "Bütüncül İstihbarat" ise; açık kaynaklar dâhil bütün her türlü bilginin ve istihbaratın, istihbarat üretim sürecinde kullanılması olarak tanımlanmıştır (US Army FM 2-0 Intelligence, 2004, s. 37). Bu bakış açısı aslında AKİS'in diğer disiplinlerle ne denli bütünleşik olduğunun farklı bir göstergesidir. AKİS'e yönelik söz konusu bütüncül yaklaşım sadece istihbarat topluluklarında benimsenmemektedir. Gelişen teknoloji çağıyla birlikte istihbarat toplulukları dışındaki diğer aktörler (devlet dışı aktörden ve şirketlerden sivil toplum kuruluşlarına) de AKİS'i "Bütüncül İstihbarat Disiplini" olarak entegre etme çabası içerisindedir (Hobbs ve Salisbury, 2014, s. 2).

Şekil 2. Bütüncül İstihbarat Kavramı Çerçevesinde AKİS
(Kaynak: https://www.intelligence101.com/what-is-all-source-intelligence-how-does-it-work)



Eski bir CIA görevlisi olan Arthur HULNICK, AKİS'in genel istihbaratın %80'ini oluşturduğunu belirmiş ve AKİS'in önemini "ne çekici ne de maceracı, açık kaynaklar yine de gizli istihbarat için temel yapı taşıdır." şeklinde vurgulamıştır (Mercado, 2010, s.3).

AKİS'in diğer istihbarat disiplinlerine katkısı; GÖRİS talep etmek için yeterli zaman olmadığında açık kaynak harita uygulamalarından faydalanılabilir veya farklı tarihlerdeki harita alıntıları kıyaslanarak görüntü

kıymetlendirmesi sonucu yeni tesis ve tünel gibi yapılar ortaya çıkarılabilir (örneğin İran'ın gizli nükleer ve füze tesislerine yönelik açık kaynak tespitleri). AKİS, haritalar, grafikler, iletişim bilgileri, yazılı ve görsel materyaller sağlayarak İNİS faaliyetlerine katkı sağlayabilir. Harekât planlanan bölgede yerel halk ile iletişim kurulabilecek medya kanalları, sosyal medya ve internet araçlarının tespiti kapsamında SİNİS'e katkı sağlayabilir.

AKİS'in diğer istihbarat disiplinleri ile ilişkisi şu örneklerle de çeşitlendirilebilir. Sosyal medya paylaşımları terörist ve milis unsurların aktiviteleri veya coğrafi konumları hakkında bilgi verebilir ve bu bilgi GÖRİS vasıtaları ile teyit edilmeye çalışılabilir veya GÖRİS vasıtalarının rastgele veya nispeten geniş bir alanda tarama yapması yerine belirli bir hedefte yoğunlaşması sağlanabilir. Ayrıca AKİS ile sağlanan ticari uydu haritalarıyla GÖRİS elde edilebilir. AKİS, İNİS toplayıcılarına harekât alanının insan dokusu hakkında bilgi verebilir, kaynağın daha iyi tanınmasına yardım edebilir ve böylece kaynak ile ortamın daha iyi ilişkilendirilmesini sağlayabilir. Örneğin, günümüzde bir milis/terör örgütü mensubunun sosyal paylaşımları veya askeri vasıta/teçhizatları ile ilgili medya kanallarıyla elde edilen görüntülerinin AKİS icra edilerek incelenmesi ve analiz edilmesiyle konum tespiti konusunda bazı örnekler görülmektedir. Ayrıca, AKİS ile sosyal medya verilerinin toplanması ile SİNİS disiplini gibi hedef kişilerin ilişki ve irtibatları elde edilebilir.

Modern teknoloji sayesinde AKİS analizleri geçmişte olduğu gibi diğer toplama vasıtalarını destekleme misyonundan çıkarak, daha çok diğer toplama vasıtalarının erişemeyeceği olayların, faaliyetlerin ve yöntemlerin tespit edilmesini ve tanımlanması alanında kullanılabilir hale gelmiştir (Minas, 2010, s. 5).

Askeri istihbarat genelde düzensiz savaş ortamlarında karar alıcılara ve politika üreticilere harekât ortamının anlaşılmasını sağlama konusunda başarısız kalmaktadır (Connable, 2012, s. 5). Özellikle de SİNİS, GÖRİS, ÖLİZİS ve hatta İNİS gibi konvansiyonel alanda daha başarılı olan disiplinlerin düzensiz savaşta istihbarat sağlama konusundaki yetenekleri sorgulanmaktadır. Bu durum istihbarat topluluklarını farklı çözümler bulmaya itmektedir. Diğer taraftan, AKİS'in düzensiz savaşlarda gidişatı değiştirme potansiyelindeki rolü de henüz tam olarak fark edilebilmiş değildir.

Askeri istihbaratı sadece düzenli orduların elde ettiği istihbarattan ziyade, devlet veya devlet dışı silahlı örgütlerin muharebeye yönelik istihbarat elde etmesi şeklinde ele alınırsa iki kenarı keskin bir bıçak gibidir. Devlete ait resmi istihbarat örgütleri nasıl terör örgütleri ve milis gruplar hakkında istihbarat elde etmede AKİS'ten faydalanıyorsa; söz konusu gruplar da aynı şekilde ve hatta daha yüksek seviyede hasım gördükleri orduların görevleri, miktarları, moral durumları ve konumları hakkında istihbarat elde etmede AKİS'ten faydalanmaktadırlar. Yani, yeterli finanse edilmeyen veya iyi organize olamamış devlet dışı aktörler dahi basit veya ileri düzey açık kaynak uygulamalarına erişebilmektedir. Örneğin, DEAŞ Terör Örgütünün illegal para transfer mekanizması olan ve "Havala" olarak adlandırılan sistemin tespiti veya suç örgütlerinin kripto para sistemi kullanmasının takibi maksadıyla aktif AKİS yöntemleri kullanılabilmektedir.

Birçok devlet strateji, planlama ve taktik konularda halka açık bilgi sağlamaz, fakat bu bilgileri elde edebileceğimiz sınırsız açık kaynak verisi bulunmaktadır. Subaylar veya diğer askeri personel kendi sistemlerinin birer ürünü ve yansımasıdır. Bunun doğal bir sonucu olarak; bu grubun yazdığı kitap, makale v.b. ürünler ve verdikleri demeç, açıklama veya paylaşımlar ordularının askeri kültürleri, imkân ve kabiliyetleri, moral seviyesi ve iç sorunları hakkında ipuçları verebilir.

2.3. AKİS'in Askeri İstihbaratta Kullanıma Yönelik Temel Esaslar

AKİS bazı temel esaslar dikkate alındığında askeri istihbarat kullanımında daha faydalı olabilecektir. Bunlar; AKİS'in kaynak ve metotların kombinasyonuyla meydana gelmesi, açık kaynakların keşif, ayırt etme, ayrıştırma ve yayım sürecine tabi tutulmazsa sadece bilgiden ibaret olması, örtülü istihbarat vasıtaları üzerindeki yükü azaltarak komutan ile lojistik ve diğer personelin acil ihtiyaçlarını gidermesi, UA örgütler, koalisyon ve gayri resmi kurumlarla müşterek çalışmalarda ideal bir kaynak olması, elektronik kaynakların yanı sıra matbu doküman ve insan kaynaklarının da AKİS kabul edilmesi, komutanın niyetini ve ilgi alanını gizli tutmak maksadıyla AKİS'in İstihbarata Karşı Koyma faaliyetleri ile birlikte kullanılabilmesi, bunun yanı sıra uydu, casuslar ve diğer istihbarat yeteneklerinin muadili veya tek başına bir disiplin olarak görülmemesi, diğer taraftan bütünleyici yaklaşım ile kullanıldığında önemli faydalar getirmesi, internet ve uzmanlar tarafından sağlanan gri literatür de dahil olmak üzere çevrimiçi ticari harita uygulamaları ile birlikte kullanılabilmesi, diğer

istihbarat vasıtalarında olduğu gibi istihbarat çarkı uygulanmadan AKİS elde edilemeyeceği ve doğru sorular sorulmadan gereken cevapların alınamayacağının dikkate alınması, AKİS'in bir atom ve roket bilimi gibi zor bir iş olarak görülmemesi gerektiği, gerekli eğitim ile personel AKİS uygulayıcısı haline getirilebilmesi, bu konuda yeterli olan personelin: doğruluğunu kanıtlama, değerlendirme, uygun kaynak taraması, mantıki analiz ve uygun sunum gibi temel noktaları unutmaması gerektiği, uygun sitelerin takip edilmesi maksadıyla kayıt altına alınmasını ve yeni bulguların paylaşımını sağlayan yapılandırılmış vasıtalara sahip olunduğunda AKİS'in daha kolay hale gelebilmesi, harekâtın parçası olan psikolojik harekât ve sivil işler konularında faydalanılabilecek yeni bir kaynak olarak görülebilmesi (Steele, 2004, s.43) şeklinde sıralanabilir.

3. AKİS SÜRECİ, YÖNTEMLERİ VE UYGULAMALARI

AKİS uygulaması söz konusu olduğunda "en iyi 10 AKİS aracı" veya "en gelişmiş AKİS araçları" adı altında bazı *(Maltego, Rcon-ng, theHarvester, Shodan, Metagoofil, Searchcode, SpiderFoot vb.)* uygulamalardan bahsedildiği görülmektedir. Elbette bu ve benzeri araçlar oldukça faydalıdır. Burada maksat bu araçların faydalı olup olmadığını tartışmaktan ziyade AKİS uygulamalarının her geçen gün spektrumunun genişlediği göz önüne alındığında, bu alanı belli başlı uygulamalara sınırlamanın sakıncalar yaratabileceğidir. Ulusal güvenlikte (asker, kolluk kuvveti, istihbarat teşkilatı v.b.) görevli profesyonel olarak medya takibi, siber güvenlik, sosyal medya analizi, kriz yönetimi gibi farklı alanlarda AKİS uygulayanlar açısından, uygulaması kolay farklı toplama/işleme araç ve yöntemleriyle çalışılması daha düzenli, sistemli ve esnek bir görev alanı yaratacaktır (Bielska, 2020, s.3). Bu kapsamda Bielska (2020) hazırlamış olduğu el kitabında genel ve sosyal medya arama araçlarından askeri ve terörizmle ilgili arama araçlarına kadar birçok kaynağa yer vermiştir (ss. 17-510).

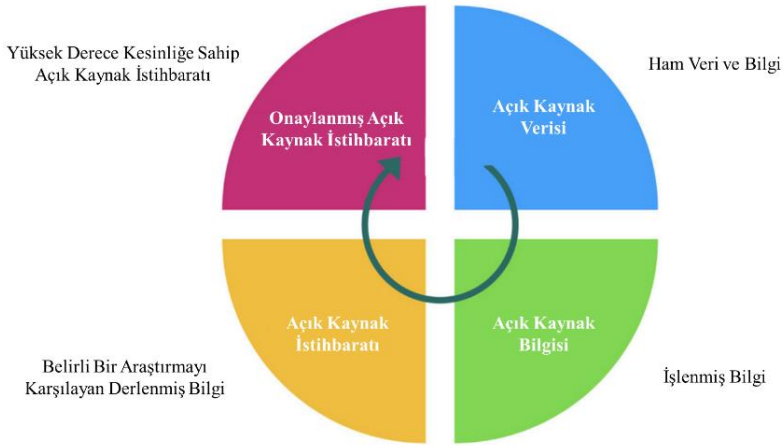
Yukarıda da bahsedildiği üzere AKİS toplama, işleme ve analiz sürecinde kullanmak üzere birçok manuel ve otomatik araç bulunmaktadır. AKİS metodolojisi veri bilimi, istatistik, makine öğrenimi, programlama, veri tabanları, bilgisayar bilimi gibi birçok alanın sentezlenmiş halidir. Veri toplama ve veri tabanı yaratma konusunda her gün yeni yöntemler ortaya çıkmaktadır. AKİS için genel geçer bir teoriden söz etmek mümkün değildir (Layton ve Watters, 2016, s. 4). Ancak, bu bölümde AKİS elde etmenin

teknik boyutuna fazla girmeden bütün AKİS elde etme ve işleme süreçlerinin temelini oluşturabilecek yöntemlerden teorik olarak bahsedilecektir.

3.1. Açık Kaynak İstihbaratını Oluşturan Terimler

Belirli bir hiyerarşi doğrultusunda; Açık Kaynak, Açık Kaynak Verisi, Açık Kaynak Bilgisi, Açık Kaynak İstihbaratı ve nihayet Onaylanmış Açık Kaynak İstihbaratı en ham halinden tekâmül etmiş haline doğru AKİS'i teşkil eden terimlerdir. Bu terimler aşağıdaki şekilde açıklanabilir.

Şekil 2. AKİS Çalışmalarında Veri İşleme Süreci (Kaynak: Böhm ve Lolagar, 2021, s. 3)



Açık kaynak; gizlilik kaygısı olmadan bilgi sağlayan herhangi bir kişi veya gruptur. Açık Kaynak kamuya açık olabilir ancak her kamuya açık bilgi açık kaynak değildir. Açık Kaynak ile kamuya açık bilgi ortamı/vasıtaları kastedilir ve sadece kişilerle sınırlı değildir (ATP 2-22.9 Open-Source Intelligence, ABD Ordusu, 2012, s. 1-1).

Açık kaynak verisi; birincil kaynaktan elde edilen ham formda basım, yayım, sözlü brifing ve diğer bilgilerdir. Fotoğraf, görüntü, ses kaydı ve mektup da Açık Kaynak Verisi olabilir (ATP 2-22.9 Open-Source Intelligence, ABD Ordusu, 2012, ss.2-5).

Açık kaynak bilgisi; belirli bir süzgeçten ve değerlendirmeden geçirilerek verilerin bir araya toplanmış halidir. Gazeteler, kitaplar, medya ve günlük raporlar gibi yayımlanan kapsamlı bilgiler örnek olarak verilebilir (NATO OSINT Handbook, 2001, s.2).

Açık kaynak istihbaratı; belirli bir topluluğun (karar alıcılar, komutanlar) belirli sorularına cevap bulmak maksadıyla kasıtlı olarak ve çaba göstererek ortaya çıkarılan, ayrıştırılan ve yayımlanan açık kaynak bilgisidir (NATO OSINT Handbook, 2001, s.3).

Onaylanmış açık kaynak istihbaratı; yüksek derecede kesinliğe sahip bilgidir. Geçerliliği ve güvenirliği konusunda şüphe olmayan açık kaynaktan veya bir profesyonel tarafından gizlilik derecesine sahip istihbarat kaynaklarına ulaşılarak elde edilen istihbarattır (NATO OSINT Handbook, 2001, s.3).

3.2. AKİS Kaynakları

AKİS kaynakları; internet (forumlar, bloglar, sosyal ağ siteleri, video paylaşım siteleri, meta veri, dijital dosyalar, dark web, coğrafi-konumsal verileri, arama motorları gibi online bulunabilen her şey), geleneksel medya (televizyon, radyo, gazete, kitap, dergi v.b.), uzmanlaşmış yayımlar, akademik çalışmalar, konferanslar, şirket profilleri, yıllık raporlar, çalışan profilleri ve biyografi/resume, meta veri dahil fotoğraf ve videolar ile coğrafi-konumsal bilgiler (haritalar, görüntü ürünleri) gibi oldukça geniş yelpazede karşımıza çıkmaktadır (Hassan ve Hijazi, 2018, s.5).

3.2.1. Medya Kaynakları

İnternet ortaya çıkmadan önce uzun yıllar AKİS basın, radyo ve televizyon gibi görsel, duyusal ve basılı medya ile elde edilmiştir. Medya halen en etkili AKİS kaynağıdır (NATO OSINT Handbook, 2001, s.5).

3.2.2. İnternet

İnternet ile birlikte AKİS'de evrim geçirmiştir. İnternet ile birlikte AKİS'in toplanması, işlenmesi ve yayımı konusunda önemli derecede hız ve veri zenginliği kazanılmıştır. İnternet ile "World Wide Web" (www) terimleri birbiri içerisinde kullanılmaktadır, ancak bu yanlıştır. İnternet temel teknoloji iken WWW onun üzerine kurulan bir servistir. WWW arama motorlarından herkes tarafından indekslenmiş içeriklere ulaşılabilen "surface web" ve sadece "Unique Resource Lovator" (URL) veya IP adresine doğrudan bağlantı kurulması vasıtasıyla erişilen ve çoğu zaman kayıt veya ödeme talep edilen "deep web" olarak ikiye ayrılır. İnternetin diğer bölümü ise küçük karşılıklı ağlardan oluşan ve belirli donanım, konfigürasyon ve giriş yetkisi talep eden "darknet"tir. "Darknet"in en üstüne "dark web" inşa edilmiştir (Böhm ve Lolagar, 2021, s.2). AKİS elde etmede mevcut arama motorları

esas kaynak olmakla birlikte, bu dağının görünmeyen kısmını oluşturan "deep web" ve "dark web" göz ardı edilmemesi gereken alanlardır. İnternet içerikleri aşağıdaki alt başlıklarda incelenebilir.

3.2.3. Gri Literatür

Gri literatür, yasal ve etik olarak elde edilebilir olan, ancak sadece özel kanallarla veya doğrudan yerel erişim ile bilgidir. Üniversiteler, sivil toplum örgütleri ve özellikle düşünce kuruluşları istihbarat kuruluşlarının olağanüstü faydalı açık kaynak bilgileri devşirdiği merkezlerdir. Özellikle stratejik araştırma merkezleri/düşünce kuruluşları devlet ile sivil toplum arasında gri bir alanda konumlanmakta ve çoğu zaman kaliteli stratejik bilgi üretmektedirler (Özdağ, 2018, s. 296).

3.2.4. Uzmanlar ve Gözlemciler

Dünyanın farklı bölgelerinde sahada doğrudan gözlemlerde ve temaslarda bulunabilen, söz konusu bölgenin dili, tarihi, insan dokusu v.b. konularında uzman olan insan kaynakları tam teşekküllü açık kaynaklardır. Bunların elde ettiği açık kaynak verisi, bilgisi veya istihbaratı diğer basılı veya farklı medya kanallarıyla sağlanan bilginin daha üzerindedir.

3.3. AKİS Kullanan Gruplar

AKİS birçok farklı aktör için faydalı olabilir. Bu bölümde belli başlı AKİS kullanan gruplar ve bu grupların AKİS kullanma amaçları açıklanmaya çalışılacaktır.

3.3.1. Devletler

Devlet organları, özellikle de istihbarat teşkilatları ve askeri kurumların altında görev yapan birimler ve organizasyonlar, AKİS kaynaklarından en fazla faydalanan kullanıcılardandır. Devasa teknolojik gelişmeler ve internet kullanımının giderek yaygınlaşması devletlerin AKİS kullanımına daha fazla yoğunlaşmasına sebep olmuştur.

3.3.2. Devlet Destekli Kurumlar

Devlet tarafından desteklenen, fon sağlanan veya ortak proje yürütülen yarı resmi kurum olarak görev yapan organizasyonlar AKİS'ten önemli derecede faydalanan, hatta kapalı kaynakların ötesinde istihbarat analizleri ve ürünleri sağlayan organizasyonlardır. ABD tarafından desteklenen ve yönlendirilen "Open Source Center"

(https://fas.org/irp/dni/osc/index.html) ve Birleşik Krallık tarafından desteklenen ve yönlendirilen BBC Monitoring (https://monitoring.bbc.co.uk/) örnek olarak verilebilir.

3.3.3. Uluslararası Organizasyonlar

Devlet ve devlet destekli kurumların AKİS kullanmaya yönelik çabalarına paralel şekilde Birleşmiş Milletler, NATO ve Avrupa Birliği kurumları da AKİS'i farklı amaçlarla kullanmaktadırlar. BM tarafından küresel düzeyde barışı koruma operasyonlarına yönelik istihbarat ihtiyacını üye devletlerden sağlamak yerine AKİS'i tercih etmektedir. NATO uluslararası organizasyonlar içerisinde AKİS'ten en yoğun şekilde faydalanan kullanıcıdır. NATO bu yönde kitaplar ve broşürler hazırlamaktadır.

3.3.4. Kolluk Kuvvetleri

Kolluk Kuvvetleri AKİS'i vatandaşları taciz, cinsel şiddet, kimlik hırsızlığı benzeri suçlardan korumak maksadıyla kullanmaktadır (Hassan ve Hijazi, 2018, 11). Ayrıca sosyal medya takibi ile terör ve suç örgütü mensupları ve bunların destekçileri de AKİS vasıtasıyla tespit edilmektedir. Ayrıca, Kolluk Kuvvetleri suç örgütlerinin dijital izlerini ve delilleri takip etmek, suç örgütlerinin farklı bölgeler ve ülkeler üzerinden bağlantı ve ağlarını takip etmek amacıyla AKİS kullanmaktadır (Gibson, 2017, s. 15).

3.3.5. Şirketler

Askeri gelişmeler, terörizm, ülke profilleri, suç ağları, savunma teknolojisi gibi alanlarda çalışma yürüten bağımsız şirketler AKİS'ten oldukça geniş bir alanda faydalanmaktadır. Jane's Information Group (https://www.janes.com/), RAND Corporation (https://www.rand.org/about.html) ve Oxford Analytica (https://www.oxan.com/) kurumları örnek olarak verilebilir. Diğer taraftan yeni pazar araştırmaları, rakip firmaların faaliyetleri ve ekonomik verileri veya gelecek yatırımlarla ilgili AKİS kullanan şirketler de giderek artmaktadır.

3.3.6. Penetrasyon Kontrolü Yapanlar, Bilgisayar Korsanları ve İllegal Örgütler

Penetrasyon kontrolü yapan operatörler, Bilgisayar Korsanları (*Hackers*) herhangi bir hedef hakkında istihbarat toplamak maksadıyla açık

kaynakları kullanmaktadırlar. Sosyal mühendislik saldırılarını düzenlemek maksadıyla da AKİS önemli bir araçtır.

3.3.7. Güvenlik Algısı Yüksek Kişiler

Kullandıkları bilgisayar ve akıllı telefon gibi cihazlara yapılabilecek dış müdahalelere karşı algısı açık sıradan vatandaşlar, kişisel güvenlik açıklarını tespit etmek ve kapatmak maksadıyla AKİS kullanırlar. Vatandaşlar ayrıca dijital kimlik görünümlerini takip etmek ve kimlik hırsızlığını önlemek maksadıyla açık kaynaklardan faydalanırlar (Hassan ve Hijazi, 2018, s.11).

3.3.8. Terör Örgütleri

Terör örgütleri veya radikal milis gruplar hedefleri hakkında bilgi toplamak (özellikle Google Maps gibi araçları kullanarak hedeflerin konumu hakkında bilgi elde edebilirler), sosyal medya ile propaganda yapmak ve eleman temin etmek, bomba yapımı gibi askeri konularda bilgi temin etmek maksadıyla AKİS kullanırlar (Hassan ve Hijazi, 2018, s.11).

3.4. AKİS'in Avantaj ve Dezavantajları

3.4.1. Avantajları

AKİS'in birçok avantajı bulunmakla birlikte, öne çıkan avantajları aşağıdaki maddelerde sıralanmıştır.

- Bilgiyi elde etmek kolaydır: Teknolojik gelişmeler ve internet açık kaynak bilgisine kolay erişimin yollarını açmıştır. Bir bilgisayar ve internet bağlantısıyla sınırsız açık kaynak bilgisine ulaşılabilir. (Mercado, 2004, s.47)

- Çok miktarda bilgi kısa zamanda elde edilebilir: Dijital veri büyük miktarda bilgi üretmek için uygundur. Dijital veri sayesinde kısa zamanda birçok açık kaynak verisi taramak mümkündür.

- Geniş spektrumda ve çeşitte içeriği kapsayabilir: Açık kaynak çalışmalarına has olan ve diğer kapalı istihbarat disiplinlerinde olmayan bir özellik de ulusal güvenlik ile ilgili birçok konuyu kapsamasıdır (Dokman, 2020, s. 5).

- Geçmişe dönük bilgiler de aranabilir: Geçmişte olan olayların araştırılmasında ve geniş bir veri havuzu içerisinden eski tarihli bir olayın ortaya çıkarılması konusunda AKİS disiplini diğerlerinden üstündür.

- Düşük seviyede risk barındırır (güvenlidir): AKİS kullanımı daha

tehlikeli ve risk içeren yöntemlerin elimine edilmesini sağlar. İstihbarat çabasının veya faaliyetinin açığa çıkmaması açısından en güvenilir vasıta olduğu söylenebilir.

- Açık kaynak bilgisi düşük maliyetlidir: Medya araçlarına, düşünce kuruluşlarının ürünlerine, çoğu aplikasyona veya arama motorlarına erişim ücretsizdir. Bazı açık kaynak ürünleri ücretli olsa dahi ödenen bedelin misliyle karşılığını verir.

- Gerçek zamanlı bilgiye ulaşılabilir: AKİS denilen veri toplama disiplini belirli olayların anlık tespit ve takip edilmesini sağlar (Dokman, 2020, s. 6).

- Farklı dillerden bilgilere erişilebilir: Yabancı dil ile istihbarat elde etme avantajını en iyi sağlayan istihbarat disiplinidir.

- Bilgi tek noktadan toplanabilir: Bilgi toplanmak istenen bölgeye, topluma ve ortama gitmeden sabit bir ofisten istihbarat elde edilebilir (Dokman, 2020, s.7).

- Bilgi paylaşımı kolaydır: Elde edilen istihbaratın (istihbaratın hassasiyeti göz önüne alınarak) hızlı bir şekilde yatay ve dikey kullanıcılara dağıtılması gerektiği söz konusu olduğunda AKİS önemli bir araçtır.

- Gizli bilgiye ulaşılabilir: Gizlilik disiplini zayıf bazı ülkelerde gizlilik derecesine sahip yazışmaların bir şekilde açık kaynaklara düşmesi veya farklı motivasyondaki kişilerin gizli bilgileri ifşa etmesi sonucu ortaya çıkan istihbarat oldukça kıymetli olabilir.

- Yasal konularda ve soruşturmalarda faydalıdır: Mali soruşturmalarda, hileli ürün/hizmet satışlarında veya telif hakkı davalarında AKİS iyi bir vasıta olmaktadır (Hassan ve Hijazi, 2018, s.16).

3.4.2 Dezavantajları

Her istihbarat disiplininde olduğu gibi AKİS'in de avantajları olduğu kadar aşağıdaki maddelerde sıralandığı üzere bazı dezavantajları da bulunmaktadır.

- Devasa boyutta erişilebilir bilgi bulunmaktadır: Açık kaynak ile devasa boyutlarda elde edilebilir bilgiden bahsedilmektedir. Verinin oldukça ham şekilde olması, kafa karıştırıcı veya istenen şekilde olmayan bilgilerin mevcudiyeti sıklıkla rastlanan durumlardır (Dokman, 2020, s.8).

- Birbirini çürüten bilgiler olabilir: Geniş yelpazede bilginin demokratik bir ortam olan internet ağında var olması, bireylerin istediği bilgiyi kolaylıkla yayabilmesiyle de katlanınca önümüze çelişkili bilgilerin çıkması olağandır (Dokman, 2020, s.8).

- Halka açık bilgi manipüle edilebilir: Kamuya açık olan internet dünyası dezenformasyon, yalan haber ve propaganda faaliyetleri için mükemmel alanlar sunmaktadır. Bundan dolayı açık kaynak bilgilerinin sürekli kontrol edilmesi önem arz etmektedir.

- Kaynakların güvenirliği değişkendir: AKİS elde etme söz konusu olduğunda diğer açık kaynaklarla veya kapalı kaynaklarla teyit edilmesi zorunludur.

3.5. Açık Kaynak İstihbaratında Sınıflandırma

3.5.1. Açık Kaynak Güvenirliği

Birincil Kaynak ve İkincil Kaynak olmak üzere iki çeşit Açık Kaynak bulunmaktadır. Öznel doğaları gereği birincil ve ikincil kaynakları ayırt etmek oldukça güçtür. Birincil kaynaklar ikincil kaynaklara nazaran daha güvenilir olarak görülebilir, ancak bu birincil kaynakların salt otorite sayılacağı anlamına gelmez. Birincil veya ikincil her kaynak aldatma ve önyargılara karşı dikkatli olunarak AKİS üretiminde sıkı bir şekilde değerlendirilmelidir. Açık kaynak güvenirliği A ile F arasında değer alır. A'dan D'ye kadar kaynağın güvenirlik seviyesine göre derece verilirken, ilk defa karşılaşılan kaynak için F değeri verilir, ancak F değeri kaynağın güvenilmez olduğu anlamına gelmez (ATP 2-22.9, 2012, ss. 2-7).

AKİS personeli bilgiyi güvenirlik ve tutarlılık kapsamında değerlendirirken, gerçek bilgi, yanıltma ve önyargı arasındaki farklılıkları ortaya koymaya çalışır. Derecelendirme ve değerlendirmeyi yapan AKİS personeli kişisel yargılarına ve aynı kaynağın daha önceden sağladığı bilgilerin isabetliliğine dayanır. AKİS personeli birbirinden veya karar vericilerden etkilenmeden bağımsız olarak güvenirlik ve tutarlılık derecelendirmesi yapmalıdır (ATP 2-22.9, 2012, ss.2-8).

3.5.2. Birincil kaynak

Çalışma anında yazılan veya üretilen doküman veya nesnedir. Bu kaynaklar bir olay veya süreç esnasında var olan ve derinlemesine bakış açısı sunarlar. Birincil kaynaktan kasıt genellikle orijinal kaynak veya kanıt kastedilmektedir. Orijinal dokümanlar (veya bunların tercümesi), anayasalar,

konuşmalar, röportajlar, videolar veya resmi kayıtlar örnek olarak verilebilir.

Açık kaynakta tarama veya toplama yapan birçok kişi sürat kaygısıyla konuyu gözden geçirmeden, dikkatlice sorgulamadan veya birincil kaynağı bulmaya çalışmadan bilgi elde etmektedir. Bu durum AKİS'in en önemli toplayıcı kaynaklı zafiyetidir (Appel, 2011, s.199). Örneğin, A ülkesinin dışişleri bakanlığından B konusunda açıklama yapıldığı ile ilgili bütün medya kanalları ve sosyal medya hesaplarınca haber paylaşılması, ancak birincil kaynak olan A ülkesi dışişleri bakanlığında konu ile ilgili hiçbir açıklama olmaması oldukça sık rastlanan bir durumdur. Birincil kaynak dikkate alınmadan AKİS üretilmesi konusunda yapılan masumane hataların ciddi sonuçları olabilmektedir.

3.5.3. İkincil kaynak

Birincil kaynakları esas alan yorumlar, analizler ve alıntılar ikincil kaynaktır. Resimler, aktarılan sözler veya grafikler ikincil kaynak olabilir. Örneğin, kaynak olarak sıkça başvurulan ve birincil kaynak gibi görülen Wikipedia veya Liveumap gibi uygulamalar aslında ikincil kaynaktır (Appel, 2011, s. 199).

Tablo 1: Açık Kaynak İstihbaratında Sınıflandırma (Kaynak: ATP 2-22.9, 2012, s. 2-8)

Açık Kaynak Güvenilirlik Derecesi		
A	Güvenilir	Doğruluk, güvenirlik ve uygunluk açısından hiç şüphe yoktur; tam güvenirlik siciline sahiptir.
B	Genellikle Güvenilir	Doğruluk, güvenirlik ve uygunluk açısından az şüphe vardır; tam güvenirlik siciline sahiptir.
C	Oldukça Güvenilir	Doğruluk, güvenirlik ve uygunluk açısından şüphelidir; tam güvenirlik siciline sahiptir.
D	Genellikle Güvenilmez	Doğruluk, güvenirlik ve uygunluk açısından hiç şüphe yoktur; ancak geçmişte geçerli bilgi sağlamıştır.
E	Güvenilmez	Doğruluk, güvenirlik ve uygunluk açısından yoksundur; ancak geçmişte geçerli bilgi sağlamıştır.
F	Hüküm Verilemez	Kaynağın güvenirliği ile ilgili herhangi bir temel/esas yoktur.
Açık Kaynak İçeriğinin Tutarlılık Derecesi		
1	Teyitli/Doğrulanmış	Diğer bağımsız kaynaklarla doğrulanmış; kendi içinde tutarlı; konu ile ilgili diğer bilgilere uygun.
2	Muhtemelen Doğru	Doğrulanmamış; kendi içinde tutarlı; konu ile ilgili diğer bilgilere uygun.
3	Doğruluğu Mümkün	Doğrulanmamış; kendi içinde mantıklı; konu ile ilgili diğer bilgilerin bazılarına uyum sağlar.

4	Doğruluğu Şüpheli	Doğrulanmamış; mümkün ama mantıklı değil; konu ile ilgili başka bilgi yok.
5	Mümkün Değil	Doğrulanmamış; kendi içinde mantıklı değil; konu ile ilgili diğer bilgilerle çelişmektedir.
6	Aldatma	Kasıtlı olarak yanlış; konu ile ilgili diğer bilgilerle çelişmekte; diğer bağımsız kaynaklarla doğrulanmış.
7	Hüküm Verilemez	Kaynağın güvenirliği ile ilgili herhangi bir temel/esas yoktur.

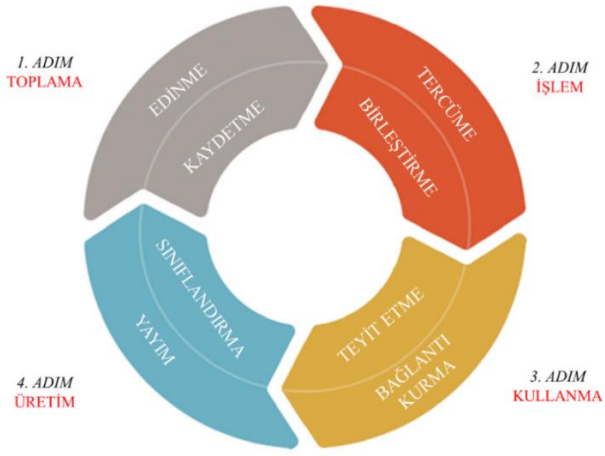
3.5.4. Açık Kaynak İçeriğinin Tutarlılığı

Açık kaynak güvenirliğinde olduğu gibi açık kaynak içeriğinin tutarlılığı da 1 ile 7 arasında değer alır. 1'den 6'ya kadar bilginin güvenirlik seviyesine göre derece verilirken, ilk defa karşılaşılan bilgi için 7 değeri verilir (ATP 2-22.9, 2012, ss.2-8). Bilgi içeriğine 7 değeri verilmesi bilginin güvenilmez olduğunu değil, AKİS personelinin alınan bilgi önceki veya mevcut verilerle teyit/tekzip edemediği anlamına gelir.

3.6. Açık Kaynak İstihbaratı İstihbarat Çarkı

AKİS Çarkı, bilinen istihbarat çarklarına benzemekle birlikte bazı yapısal farklılıklar içermektedir. AKİS Çarkında toplama aşaması açık kaynak bilgisinin elde edilmesi; işleme aşaması bilgiyi değerlendirmek için kullanılacak metodun seçilmesi; kullanma aşaması bilginin istihbarat açısından değerini belirleme; üretim aşaması ise istihbarat ürününü istihbarat topluluklarındaki yetkililere iletme şeklinde özetlenebilir. (Williams ve Blum, 2020, s.13).

Şekil 5. AKİS Çarkı (Kaynak: Williams ve Blum, 2020, s. 13)



3.6.1. Toplama

Toplama safhası özetle kullanılabilir ve potansiyel bilginin tanımlanması ve bu bilginin kaydedilmesidir. Toplama safhasında AKİS personeli anlamlandırır (yabancı dilde ise metnin kaba çevirisini yapar) ve faydalı olduğuna kanaat getirdiği bilgiyi kaydeder. Kayıt aşamasında dikkat edilmesi gereken; bilgi dijital ortamda ise yine aynı şekilde dijital ortama şekilsel düzenlemelerle kaydedilmesi, dijital değilse bilginin taranarak/fotoğraflanarak dijitalleştirilmesi, video ve ses kayıtlarının indirilmesi, internet sayfalarının linklerinin kaydedilmesidir. AKİS'in en önemli safhası olduğu söylenebilir. Çünkü çarkın ihtiyacı olan uygun veri/bilgilerin açık kaynak denizi içerisinden bularak elde etmek özveri isteyen bir süreçtir.

Açık kaynak istihbaratında toplama; bilgi ve istihbarat ihtiyaçlarının tespiti, istihbarat ihtiyaçlarının kategorize edilmesi, toplama yapılacak kaynağın belirlenmesi ve toplama tekniğinin belirlenmesi şeklinde tezahür eder (ATP 2-22.9, 2012, ss.3-1). Elbette AKİS'in en büyük avantajı maliyetsiz ve hızlı olmasıdır, ancak insan kaynağı ve zaman sınırsız değildir. Bu yüzden toplama safhası planlı bir şekilde icra edilmelidir.

3.6.2. İşlem

İşlem safhasında amaç bir değer kazandırılmış ve eyleme dönüştürülebilir istihbarat ürününün belirli kullanıcıya sunulması için hazırlanmasıdır. Bu safha kapalı ve açık istihbarat verilerinin birleştirilmesini de kapsamaktadır (NATO OSINT Handbook, 2001, s.41). İşlem safhasında açık kaynakların orijinal dilinden ana dile çevirisinin yapılması, fotoğraf veya video materyallerinin incelenerek kullanışlı hale getirilmesi gibi farklı şekillerde faaliyetler yürütülür.

AKİS dil uzmanları elde edilen verinin tercümesini yaparken, tercüme yapılan dilin konuşulduğu ülkenin kültürel yapısını ve ince nüansları bilmeli, tercüme yaparken aynı zamanda analitik değer de kazandırmalıdır (Williams ve Blum, 2020, s.17). İşlem aşamasında AKİS personelinin yabancı dil ve farklı açılardan yeterliliği süreci doğrudan etkileyebilmektedir.

Tercüme, transkript olarak birebir tercüme şeklinde veya orijinal metnin özetinin veya ima ettiği hususun çıkarılması şeklinde yapılabilir. AKİS'te mevcut olan bilgi ve veri yoğunluğu dikkate alındığında 5N 1K

sorularına cevap verecek şekilde özet tercüme yapılmasının daha makbul olduğu söylenebilir.

Birleştirme aşamasından kastedilen, farklı cinste ve miktarda veri ve bilgileri tek bir grupta veya başlıkta bir araya getirmektir. Birleştirme aşamasında tercüme bilginin veya farklı sosyal medya içeriklerinin kullanılabilir forma dönüştürülmesi faaliyeti yürütülür.

3.6.3. Kullanma

Kullanma safhasında bilginin kastedilen manada olup olmadığı ve istihbarat toplulukları için herhangi bir değeri olup olmadığı gözden geçirilmektedir. Kullanma aynı zamanda analiz anlamına gelmektedir.

Halka açık bilginin ve açık kaynakların AKİS sürecine uygun şekilde dâhil edilmeden önce gerçekler, göstergeler, eğilimler ve bağlantılar açısından analiz edilmesi bu safhada gerçekleştirilmektedir (ATP 2-22.9, 2012, ss.4-6). Kullanma aşamasında ortaya çıkan istihbarat ürününün bazı analitik çıkarımlar içermesi beklenir.

Kullanma safhası; teyit etme, güvenirlik kontrolü ve bağlantı kurma olmak üzere üç aşamaya ayrılabilir (Williams ve Blum, 2020, s.18).

Teyit etme, bilginin kastedildiği şekilde olup olmadığının anlaşılmasıdır. Medya kaynakları veya gri literatür olarak adlandırılan resmi makamlarca yayımlanan bilginin teyit edilmesi kolayken, sosyal medya için aynısı söylenemez.

Güvenirlik kontrolü, bilginin itimat edilebilir olup olmadığının kesin şekilde test edildiği aşamadır. Bu aşamada bilginin kaynağının şüpheli olduğu, yalan ve aldatma olduğu hususlarında net yargıya varılır. Bağlantı kurma aşamasında, AKİS analizcisi kullanıcıya nesnel tecrübelerini aktarır, konuyla alakalı ilave bilgiler sunarak geçmiş ve mevcut diğer bilgilerle irtibatlandırır ve genel bir tablo oluşturur.

3.6.4. Üretim

Üretim safhasında AKİS ürününe bir sınıflandırma derecesi verilir. Açık kaynak bilgisi elde edilirken toplama, işlem ve kullanma safhalarının nasıl ve hangi seviyede yürütüldüğü sınıflandırmanın seviyesini de belirlemede önem arz etmektedir.

Son olarak, üretim safhasında elde edilen bilginin uygun formda kullanıcılara yayımı yapılır. Yayımlanan AKİS, kullanıcılar tarafından diğer istihbarat disiplinleri ile birleştirilerek "Bütüncül İstihbarat Disiplini" (All-Source Intelligence) ürünü olarak veya münferit olarak karar vericilere veya politika yapıcılara iletilir.

Tamamlanan AKİS belirli bir formda sürat, kesinlik ve uygunluk prensiplerine göre kullanıcılara ve karar alıcılara yayımlanmadan amacını yerine getirmemiş sayılır (ATP 2-22.9, 2012, ss.4-10). AKİS'in yayımında, hedef istihbarat ihtiyacı ve hassasiyet göz önünde bulundurularak olabildiğince geniş kullanıcı kitlesine ulaşılabilmektir.

3.7. AKİS Toplama Çeşitleri

AKİS toplama faaliyeti temel olarak pasif toplama, yarı-pasif toplama ve aktif toplama olmak üzere üç ana yöntem kullanılarak yürütülür. Bir yöntemin diğerine tercih edilmesi, ilgilenilen veri çeşidine ilaveten, istihbarat türüne ve olaya göre farklılık gösterebilir (Hassan ve Hijazi, 2018, s.14).

3.7.1. Pasif Toplama

Pasif toplama veri bildirimi veya tarama gibi manuel istihbarat toplama yöntemleri ile AKİS elde etme yöntemidir. Bu yöntemde veri yığınları arasında kalma riski yüksektir. Ancak bu sorun gerekli bilgiyi gereksiz bilgiden ayırmaya yarayan, aranan kelimeler ve ilgi alanı üzerinden tarama yapabilen yapay zekâ, makine öğrenimi veya doğal dil işleme gibi süreçlerle aşılabilmektedir. Diğer taraftan, her ne kadar bahse konu araçlar kulağa hoş gelse de bunlarında bazı dezavantajları olduğu unutulmamalıdır.

AKİS elde edilirken en çok uygulanan yöntemdir. Aslında, AKİS'in doğası gereği hedef hakkında toplanacak bilginin kamuya açık kaynaklardan derlendiği dikkate alındığında, bütün AKİS toplama yöntemlerinde pasif toplama kullanılmalıdır.

Pasif toplamada kaynak, istihbarat toplama faaliyetinden haberdar olmaz. Teknik açıdan açıklanmak gerekirse, bu yöntemde hedef sunucuya *(server)* doğrudan veya dolaylı olarak herhangi bir veri trafiği/paketi gönderilmez, veri toplanan kaynaklar arşivleme kabiliyetinden yoksundur, dosyalar ve içerik hedef sunucularda korumasız şekilde bırakılmıştır (Hassan ve Hijazi, 2018, s.14).

3.7.2. Yarı Pasif Toplama

Bu yöntem teknik açıdan, hedef hakkında genel bilgiler elde edilirken, hedef sunucuya limitli sayıda veri trafiği gönderilmesi şeklinde açıklanabilir. Bu trafik, keşif faaliyetlerine dikkat çekmekten kaçınmak maksadıyla tipik İnternet trafiğine benzemeye çalışmaktadır. Bu yöntemle, hedefin çevrimiçi kaynaklarının derinlemesine incelemesi yapılmadan ve sadece hedef tarafına herhangi bir alarm vermeden yüzeysel araştırma yapılmaktadır (Hassan ve Hijazi, 2018, s.14).

Ayrıca, bu tür arama isimsiz olarak görülmekte, hedef ancak herhangi bir soruşturma yürütürse *(server ve log ağları kontrol edilerek)* araştırma/keşif faaliyeti olduğuna kanaat getirebilmektedir. Ancak yine de AKİS icra edenin cihazı tespit edilememektedir.

3.7.3. Aktif Toplama

Aktif toplama genellikle profesyoneller tarafından belirli bir içerik veya bilginin elde edilmesi maksadıyla veya potansiyel tehdit ve penetrasyon testlerini denemede uygulanmaktadır.

Bu yöntemde istihbarat toplamak için sistemle doğrudan etkileşim içerisine girilmektedir. Bilgi toplayan kişi veya grup açık portlara erişim, güvenlik açıklarını tarama (yamalı Windows sistemleri), web sunucusu uygulamalarını tarama gibi hedef bilgisayar ve ağ altyapısı hakkında teknik veriler toplamak için gelişmiş teknikler kullanacağından, hedef keşif sürecinin farkında olabilir (Hassan ve Hijazi, 2018, s.15).

Daha önce de vurgulandığı üzere, AKİS'in özü ve doğası gereği aktif ve yarı-pasif toplama yöntemleri AKİS faaliyetlerinde genellikle tercih edilmemektedir.

3.8. AKİS Analiz Yöntemleri:

AKİS analizleri genellikle ticari olarak satılan hazır ürün/hizmetleri veya ücretsiz aplikasyonları kullanarak geniş verileri işleme ve istihbarata dönüştürerek belirli ihtiyaçları gidermeyi amaçlamaktadır. AKİS toplama araçları her gün gelişmesine rağmen, bahse konu araçların kullandığı yöntemler fazla değişmemektedir. Veriyi analiz etmek, tanımlamak ve izole etmek için kullanılabilen AKİS araçları temel olarak; Sözlüksel Analiz, Ağ Analizi, Coğrafi-Konumsal Analiz ve bunların kombinasyonu şeklinde

gruplandırılmaktadır.

3.8.1. Sözcüksel Analiz

Sözcüksel analiz, basit bir tabirle, arama motorlarında herhangi bir gün ve zamanda en çok aranan kelimeleri gösterebilir veya hangi anahtar kelimelerin sıklıkla ortaya çıktığını tespit edebilir. Daha gelişmiş seviyede sözcüksel analiz, dilin altında yatan manayı ortaya çıkarabilir ve sosyal medya kullanan insanların yaş, sosyal sınıf, ekonomik ve eğitim yapısı hakkında bilgi elde edebilir. Williams ve Blum (2020) sözcüksel analizin çeşitlerini aşağıdaki şekilde sıralamıştır:

- *Kelime sıklığı (keyness) analizi;* belirli bir cümlede veya yazıda bir kelimenin hangi sıklıkta geçtiğini tespit eden ölçüdür. Bu analiz ile konuşmacının veya yazarın kullandığı kelimeler üzerinden bir resmi ortaya çıkarılır.

- *Yoğunluk profili oluşturma;* kelime sıklığı analizi aynı zamanda yoğunluk profili çıkarmak için de kullanılır. Bu yöntemle her bir bölümdeki anahtar kelimelerin kullanımı esas alınarak örnek yapının daha geniş bir yapı ile kıyaslanması sağlanır.

- *Kümeleme;* bir küme kendi başına gramer açısından veya anlam açısından anlamsız olan ancak anahtar kelime analizine dahil edilebilen iki veya daha fazla kelime dizisidir

- *Eşdizimleme;* kelime sıklığı analizinde tanımlanan herhangi iki kelimenin birlikte belirli yoğunlukta kendini gösterme olasılığıdır. Eşdizimleme sadece aramanın fonksiyonunu genişletmek için değil bir metindeki ana temaları tanımlamak için kullanılır.

- *Duygu analizi;* toplumun veya terimlerin bir kişi hakkında başkalarıyla paylaşılmayan genel düşünce ve yargısını tanımlamak için kullanılır. (Örneğin bu ayrımcı olarak görülen bir politikacı olabilir.)

- *Duruş analizi;* duygu analizi bir dilin kişiler veya gruplar hakkında nasıl farklılık yarattığını ortaya çıkarıyorsa, duruş analizi de dil tercihlerini bireylerin bilinçaltında yatan değerlerini ve bir konuya karşı davranışsal ifadelerini ortaya çıkarır.

- *Doğal dil işleme;* önceki dönemlerde araştırmacılar ve istihbarat analizcileri farklı bir dilden tercüme yapmak için tercümanlara ihtiyaç duymaktaydı. Doğal dil işleme ve teknolojik gelişmeler bu yükü nispeten

azalttı. *"Google Translate"* gibi ücretsiz uygulamalar hızlı tercüme konusunda oldukça yol kat etmiş durumdadır. Ancak halen bir insanın yaptığı tercüme kadar sıhhatli olamayabilmektedir.

- *Makine Öğrenimi;* sözcüksel analiz ve diğer yöntemlerle ilgili anlatılan her şey makine öğrenimi ile daha etkin hale gelmiştir. Makine öğrenimi, basit bir tabirle, bir programa bir insandan bağımsız olarak belirli karar verme sürecini işleterek bağımsız olarak karar vermesinin öğretilmesidir. Makine öğrenimi hem bilgisayar uzmanı dilbilimci ve hem de makine öğrenimi uzmanlarına ihtiyaç duymaktadır (ss. 23-25).

3.8.2. Sosyal Ağ Analizi

Sosyal ağ analizi; temeli eskilere dayanan sosyoloji, psikoloji, matematik, antropoloji ve ağ bilimi alanları kesişimidir. Son nesil ağ bazlı uygulamalar olmadan önce dahi yıllardır var olan sosyal ağ analizi, bireylerin karşılıklı etkileşimlerinin haritalanması veya krokileştirilmesi ile geçmiş ve gelecek etkileşimler tahmin edilmeye çalışılmıştır. Sosyal ağ analizinde iki temel element bulunur; bireyleri ve varlıkları temsil eden düğümler ile ilişkiler ve bağlantıları temsil eden çizgiler (Layton ve Waters, 2016, s.106).

Sosyal ağ analizi bireyler arası irtibatları analiz ederken içeriği değil geniş ağlar içerisinde bağlantı kurulan aktörlerin ilişkisini anlamaya çalışır. Sosyal ağ analizinin temelini, düğüm noktaları ve bağlantıların analiz edilmesi oluşturur. Düğüm noktasından kasıt ağ içerisindeki veya dışındaki bireylerdir. Sosyal ağ analizi ikili, üçlü veya daha geniş ağların içerisinde yer alan düğüm noktalarının analizine yoğunlaşır.

Sosyal ağ analizinin ölçütleri aşağıdaki şekilde sıralanabilir.

- *Derece;* bir düğümün bağlantı sayısıdır. Derece yükseldikçe düğümün sahip olduğu bağlantı sayısı artar, dolayısıyla bu aynı zamanda düğümün diğerlerini etkileme kapasitesini belirler (Williams ve Blum, 2020, s.23).

- *Klik*; Düğümleri birbiri ile bağlantılı olan topluluk (toplulukta her bireyin birbirini tanıması) örneklemlerine klik denilmektedir. (Layton ve Waters, 2016, s.120).

- *Yoğunluk*; Herhangi bir grafik birçok düğüm ve çizgiden oluşur. Yoğunluk oranının artması demek grup içerisinde etkileşimin arttığı

anlamına gelmektedir. Bu da grubun etkinliğinin ve iletişim hızının yüksek olduğu manası yaratır (Layton ve Waters, 2016, s.114).

- *Arasındalık*; hangi düğümün ne oranda iletişimi kontrol ettiğini gösterir. Diğer bir ifadeyle iletişimin kesişim noktasındaki düğüm ya da bireyin bütün iletişimi aktarma veya nüfuz etme imkânı olduğundan gruba etkisi de yüksektir.

- *Arasındalık merkezliği*; bir düğümün ne kadar diğer düğümler arasında olduğunun ölçütüdür. Diğer düğümler arasındaki en kısa yolun ne kadar bir düğümden geçtiği onun hedef düğüm olduğunu gösterir. (Layton ve Waters, 2016, s.118).

- *Yakınlık merkezliği*; Düğümler arasındaki mesafe iki düğüm arasındaki en yakın ve an uzak mesafe kavramlarıyla açıklanır. Bir düğümün diğer düğümlere mesafesini gösterir. Arasındalık grupta hangi düğümün/bireyin mesajı kontrol ettiğini belirlerken, yakınlık bir gruptaki bireylerin ne derece bağımlı veya bağımsız olduğunu belirler. (Layton ve Waters, 2016, s.118).

- *Merkezilik ölçütü*; Merkeziliğin ölçütü bir düğümün veya bireyin geniş ağ içerisindeki önemini belirler. Yüksek merkeziliğe sahip bireylerin mesaj almaya/vermeye ve yönlendirmeye, faaliyet yoğunluğunu etkileri ve etkileşimi de daha yüksek olur.

- *Yönlülük*; Yönlülük "giden bilgi" ve "gelen bilgi" olarak ölçülür. Aktörlerin yüksek gelen bilgiye sahip olması ağ içerisinde prestij ve önemlerinin yüksek olduğu anlamına gelir. (Williams ve Blum, 2020, s.30).

3.8.3. Coğrafi-Konumsal (geospatial) Analiz

Sözcüksel analiz ve ağ analizine benzer şekilde, coğrafi-konumsal analiz istihbarat personeli için gerekli olan askeri, politik ve sosyal dinamiklerin resmini daha iyi ortaya koyabilmek maksadıyla diğer metotlarla birlikte çalışır (Williams ve Blum, 2020, s.31).

Yeryüzünde konumu bulunan nesne, olay veya olgu jeo-uzamsal veriyi oluşturur. Bu konum statik veya dinamik olabilir. Jeo-uzamsal veri konumsal bilgileri (genellikle koordinatları), karakteristik bilgileri (nesne, olay veya ilgili olgunun özellikleri) ve sıklıkla zamansal bilgileri (zaman veya konum ve özelliklerin bulunduğu süre) birleştirir (Layton ve Waters, 2016, s.171).

Coğrafi-konumsal analiz, istihbarat raporlarının haritalanması ve görsele dönüştürülmesi suretiyle kullanılması bağlamında güçlü bir araç olarak karşımıza çıkmaktadır. Gelişen teknoloji ile ortaya çıkan makine öğrenimi ve doğal dil işleme imkânları AKİS toplama konusunda önemli kazanımlar sağlamıştır. Toplanan bu verileri anlamlandırmak ve ilişkilendirmek istihbarat analizcisini kritik ve önemli bir konuma koymaktadır. Makine öğrenimi ve bazı programlar uzun zaman alan toplama ve işleme görevlerinin yerini alırken, bahse konu verilerden ilgi uyandıran anlatılar ve anlamlı çıkarımlar elde etmek maksadıyla, kendi alanlarının dışında dilbilim, bilgisayar, sosyoloji gibi farklı alanlarda bilgi sahibi ve kabiliyetli istihbarat analizcilerine duyulan ihtiyaç daha da artacaktır.

Coğrafi-konumsal analiz yöntemleri aşağıdaki şekilde sıralanabilir:

- *Coğrafi etiketleme:* Verilen bir paylaşımın veya fotoğrafın enlem ve boylam olarak işaretlenmesini giderek artan doğruluk seviyeleriyle işaretleyen işlenmiş verilerdir. Örneğin; birçok kullanıcı akıllı telefon paylaşımları ile birlikte birçok coğrafi etiket bırakır. Twitter, Facebook ve Instagram gibi sosyal medya programları ile kullanıcılar bilinçli veya bilinçsiz olarak bulundukları mevkiyi ve icra ettikleri faaliyetleri paylaşmaktadırlar.

- *Coğrafi konumlama:* Google Earth ve Google Maps gibi açık kaynak programları kullanılarak analizciler (cami, okul gibi) belirli yapıtların yerini tespit ederek ve yine farklı açık kaynak programları ile fotoğrafları birleştirerek etiketleme yapabilirler (Higgins, 2014, s.1). Coğrafi konumlama ile çatışma alanlarında meydana gelen tank, askeri araç ve silahlı unsurlara ait hareketler, belirli bölgelere yönelik hava taarruzları veya roket atış videoları izlenerek ve bahse konu videolardaki arazi arızaları izlenerek, söz konusu arazi arızalarının açık kaynak programları kullanılarak konumlarının tespit edilmesi suretiyle coğrafi konumlama yapılmaktadır.

- *Coğrafi çıkarım*: Açıkça coğrafi etiketleme yapılmamış bilginin coğrafi konumlamasının yapılmasıdır. Coğrafi çıkarım birçok yöntemle yapılabilir. Bazı web sayfaları *(örneğin, Google ve Craigslist),* kullanıcı deneyimini şekillendirmek maksadıyla kullanıcının yerini kaydeder, bunun için "konuma duyarlı içeriği" kullanıcının tarayıcısının önbelleğinde bırakır. İlgili taraflar, kullanıcının konumunu etrafındakiler düzeyine kadar tüm ayrıntılarıyla görecek şekilde belirlemek için, "yan kanalları" kullanarak

önbellekte kalan konumlara erişebilirler (Yaoqi, Xinshu, Zhenkai ve Prateek, 2014, s. 1)

- *Coğrafi referanslama*: Konumu belirli olan nesneyi fiziki ortamla ilişkilendirir. Bu yöntem genellikle coğrafi bilgi sistemi kullanılarak fiziki veya raster haritayı jeo-uzamsal konumlarla ilişkilendirme yoluyla uygulanır (Williams ve Blum, 2020, s.33). Haritaların üzerinde gösterilen konumlarla ilgili açık bir coğrafi koordinat sistemi olmadığı durumlarda jeo-uzamsal koordinatlar haritanın üzerinde gösterilen bir şekil veya simgeye atanabilir (Murayama, 2012, s.43). Bu haritalar daha sonra araştırma, istihbarat, askeri veya hedef çalışmaları kapsamında kullanılabilir

- *Coğrafi-Konumsal muhakeme*: Hem nesnelerin yeryüzündeki konumları hakkında hem de coğrafi konumsal veriler hakkında eşzamanlı akıl yürütme faaliyetidir (Layton ve Waters, 2016, ss. 173-178).

SONUÇ

AKİS uygulamada en önemli husus basit görünse de öncelikle çerçevesi ve basamakları net şekilde belirlemiş bir metodun benimsenmiş olmasıdır. AKİS işimize yarayacağı düşünülen veya ilginç olan bütün veri ve bilginin toplanması, tasnif edilmesi ve kullanıcılara sunulması değildir. AKİS'te uygun metodun benimsenmemesi hem önemli zannedilen ancak önemsiz olan verinin gereksiz yere toplanmasını, hem de önemsiz görülen ancak hayati öneme sahip verinin gözden kaçırılmasına sebep olacaktır. Dolayısıyla bu durum istihbarat toplayıcısı ve analistinin gerekli ve gereksiz bilgi yığınları altında ezilmesine sebep olacaktır. Diğer önemli husus ise AKİS çarkı/sürecinin basamaklarının belirlenen sıra ve hassasiyetle uygulanmasıdır.

Bütün bunların çerçevesinde AKİS elde etme faaliyetinin yetenek, uzmanlık, kültürel farkındalık ve dil yetenekleri gibi önemli yetiler gerektirdiği unutulmamalıdır (MI Publications, 2020, s.73). AKİS yerine bilinçsiz ve eğitimsiz şekilde yürütülen açık kaynak bilgisi elde etme faaliyeti hem güvenlik hem de güvenirlik zafiyeti yaratabilecektir.

AKİS; İNİS ve SİNİS gibi örtülü istihbarat vasıtalarının yerini alacak bir disiplin değildir. AKİS onların yerini almak yerine bahse konu disiplinlerin gelişmesini sağlamakta ve onlar üzerinde önemli etkiler bırakmaktadır (Mercado, 2010, s.3). Birçok gerekli bilginin açık kaynaklarda yer aldığı doğrudur ancak bunların hepsi kolayca erişilebilir şekilde değildir.

Askeri istihbaratın mevcut yapısı kapsamında olmayan bazı yaklaşımlarla ancak açık kaynakların gizli kapıları açılabilecektir (Briggs ve Matejova, 2019, s. 193).

AKİS'in, başta stratejik seviye olmak üzere farklı seviyelerde askeri istihbarat ihtiyaçlarını karşılayabilecek önemli vasıtalardan biri olduğu söylenebilir. Ancak, tabi ki AKİS istihbarat topluluğu için her derde deva bir ilaç değildir. AKİS diğer toplama vasıtalarının imkân ve kabiliyetlerinde olan bazı seviyelerde doğal olarak yetersiz kalabilmektedir. AKİS en iyi şekilde bütüncül bir yaklaşımla diğer istihbarat disiplinleri ile irtibatlandırılarak ve harekât planlama/icra safhalarına entegre edilerek etkili olabilir.

Askerî harekâtın planlamasına ve karar verme sürecine yönelik olarak istihbarat toplamak maksadıyla birçok yöntem kullanılır. Bunlardan İNİS oldukça değerli, bir o kadar da elde edilmesi zor, iyi eğitilmiş ve tecrübeli istihbarat personeli gerektiren, bazen de zamanlılık konusunda aksamalar yaşanabilen bir disiplindir. GÖRİS ise daha güvenilir ve hızlı bir seçenek olmakla beraber, istenen hedefleri tamamen kapsayabilecek sayısız İHA platformları ve elde edilen verileri kıymetlendirecek analizciler gerektirir. Diğer taraftan SİNİS hedefin tespit edilmesi veya niyetinin ortaya çıkarılmasında oldukça etkili olmakla birlikte, hedef grubun teknolojik cihazları (telsiz, cep telefonu v.b.) kullanmaması veya kısıtlı kullanması gibi bazı kısıtları bulunmaktadır. AKİS'e gelince; basit metotlardan karmaşık programlara ve makine öğrenimine kadar birçok yöntemle birlikte açık kaynakların sınırsız ve engellenemez veri hazinesinden faydalanmanın önemli getiriler sağlayacağı söylenebilecektir.

Geçmişte insan kaynaklarından (İNİS) ve teknik yeteneklerle (GÖRİS, SİNİS) elde edilen istihbarat en değerli bilgi olarak kabul edilse de günümüzde bu algı radikal şekilde değişmeye başlamıştır. Son zamanlarda birçok kurum açık kaynaklardan toplanan istihbaratın kullanışlılığını ve değerini takdir etmektedir (Ziolkowska, 2018, s.8). AKİS'in bu değeri; günümüzde (hibrit savaş kavramının yarattığı etkinin yansıması olarak) askeri operasyonların icrasında özellikle devlet dışı aktörlerin tespit ve analiz edilmesinin önem arz ettiği asimetrik savaşlarda ön plana çıkmaktadır. Nasıl askeri doktrinler ve taktikler sürekli olarak gelişiyorsa, askeri istihbarat temininde bilginin toplanması ve analiz edilmesi konusunda da günümüzde oluşan ivmenin yakalanması bir gereklilik halini almaya başlamaktadır.

Açık kaynak devriminin arkasındaki güçlü teknoloji ve sosyal momentum nedeniyle, geleceğin istihbarat talepleri, açık kaynağı geleneksel ikincil sınıf disiplinden, temel kategoriye alınması hususunu yeniden değerlendirilmesi gerektiğini ortaya çıkaracaktır (Wilhelm, 2012, s.7).

AKİS'in günümüzde olduğu gibi gelecekte de yararlı istihbaratın çoğunluğunu oluşturacağı göz önüne alındığında, büyük veri analizi, sosyal medya ve siber istihbarat gibi açık istihbaratın yönetimi tarzlarına doğru bir geçişin görülmesi muhtemel olacaktır. Günümüz savaşlarında olduğu gibi gelecek savaşlarda da daha akıllı yaklaşım belirlenmesi zorunluluğu ortaya çıkacaktır. Bu durum açık kaynaklardan oluşan "büyük veri" analizini zorunlu kılacaktır (Berman, Felter ve Shapiro, 2018, s.40).

Dijital bilgi ortamı harekât alanına yönelik yeni sorunlar ve olgular getirmektedir. Siber alan ve teknolojiye paralel olarak sürekli gelişmekte olan bir disiplin olan AKİS'in teknik, taktik ve prosedürleri sıklıkla değişmektedir (MI Publications, 2021, s.71). Ancak maalesef devletlerin ve istihbarat örgütlerinin uyguladıkları politikalar genellikle aynı esnekliği ve reaksiyonu gösterememektedir.

Barış zamanında açık kaynak istihbaratı ağırlıklı askeri istihbarat faaliyetlerini rutin bürokratik işler olmaktan çıkarabilen silahlı kuvvetler, kendilerini hızlı ve bir o kadar planlı tepki verebilen hale getirebilir. Aksi takdirde dış askeri istihbarat sisteminden merkeze doğru sürekli haber ve bilgi akışı olsa dahi, muhtemel bir savaş/seferberlik halinde operasyonel etkinliğin, barış zamanlarında ise caydırıcılık oranının düşük seviyelerde kalması muhtemeldir (Yıldız, 2019, s.20).

Türkiye'de AKİS'in teknolojik gereksinimlerinin yerine getirilebilmesi için, özel sektörün desteğinden de yararlanılması gerekebilecektir. Önümüzdeki süreçte, açık kaynakların ortaya koyduğu yoğun ve idaresi güç büyük veri kaynaklarını tespit, tasnif, analiz ve yayınlama yükünü, özel istihbarat şirketi olarak profesyonelleşmiş kurumlarla belirli çerçevede devretmenin istihbarat topluluklarına getireceği faydaların kıymetlendirilmesi gerekecektir.

AKİS ve veri biliminin mevcut durumu, analizciler ve kullanıcılardaki değişiklikler ile veri analizi, otomatik veri toplama, aplikasyon ve araçlar, makine öğrenimi kapsamında geliştirilen algoritmalar, coğrafi konumsal yöntemler gelecekte bu alanı daha karmaşık hale getirecek gibi gözükmektedir (Layton ve Watters, 2016, s.17).

AKİS'te yaşanan gelişmelerin yanı sıra, siber istihbarat veya sosyal medya istihbaratı gibi yeni disiplinlerin ortaya çıkması istihbarat topluluklarının örgütlenmelerinde değişimlere gitmesine yol açacağı, diğer taraftan gelecekte istihbarat ve istihbarata karşı koyma alanında görev yapacak bütün sivil ve askeri personelde, siber ve sosyal medya çalışmalarında uzman, farklı bilgisayar yetenekleri ve dil kabiliyetlerine sahip personelin tercih edilmesine sebep olacağı, dolayısıyla personel yetiştirme politikalarının da bu yönde evrileceği söylenebilecektir.

KAYNAKÇA

Andrew C. (2018). *The secret world: A history of intelligence*. Yale Univercity Press.

Akad M.T. (2018). *Tarihten günümüze istihbarat (1.basım)*. Kastaş Yayınları.

Appel E. (2011) *Internet searches for vetting, Investigations and open-source intelligence*. CRC Press.

ATP 2-22.9 *Open-Source intelligence*. (2012). US Army Headquarters Department of the Army.

ATP 2-01.3 *Intelligence preparation of the battlefield* (2019). US Army Headquarters Department of the Army.

Bazzell M. (2018). *Open source intelligence techniques resources for searching and analyzing online information (6.basım)*

Berman E., Felter J. ve Shapıro J. (2018). *Small wars big data,* Princeton University Press.

Bielska A. (2020). *Open source intelligence tools and resources handbook*, I-Intelligence Press/ABD

Böhm I. ve Lolagar S. (2021). *Open source ıntelligence: Introduction, legal an ethical considerations*. Springer https://doi.org/10.1365/s43439-021-00042-7

Briggs C.M. ve Matejova M. (2019). *Using intelligence and military planning for energy and environmental risks*, Cambridge University Press.

Connable B. (2012) *Military intelligence fusion for complex operations*. RAND Corporation.

Dokman T. (2020). *Open source intelligence (OSINT): Issues and trends*. Zagreb Üniversitesi.

Hanley W. (2005). *The genesis of napoleonic propaganda*. Columbia

University Press.

Gıbson H. (2017) *OSINT from a UK perspective: Considerations from the law enforcement and military domains.* Sheffield Hallam University.

Gill P. ve Phythian M. (2018). *Intelligence in an ınsecure world* (3. Baskı).

Gudgin P. (2000). *Military intelligence.* Phonex Mill: Sutton Pub Ltd.

Hassan N.A. ve Hıjazı R. (2018). *Open source intelligence methods and tools*. Apress.

Infelise M. (2002). *Roman avvisi: information and politics in the seventeenth century*. DOI:10.1017/CBO9780511496929.010

Joint Military Intelligence Training Center (1996). *Open source intelligence professional handbook*, DOD Press Oakton.

Layton R. ve Watters Paul A. (2016) *Automating open source intelligence.* Elsevier.

Mercado S.C. (2005). *Reexamining the distinction between open ınformation and secrets, Studies in Intelligence.* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies.

Mercado S.C. (2010). *Sailing the sea of OSINT in the information age*, CIA Website Studies in Intelligence Vol. 48, No. 3.

Minas H. (2010). Can *the open source intelligence emerge as an indispensable discipline for the intelligence community in the 21st century*? RIEAS.

NATO. (2001). *Open source ıntelligence handbook*

Özdağ Ü. (2018) *İstihbarat teorisi* (13. Baskı).

Steele R. (1997). *Open source ıntelligence: What is it? Why is it important to the military?* Virginia/ABD: Open Source Solutions, Inc.International Public Information Clearinghouse

Steele R. (2004). *Special operations forces open source intelligence handbook*, OSS Press.

The unrealized value of open source intelligence for irregular warfare (https://thestrategybridge.org/the-bridge/2018/7/25/the-unrealized-value-of-open-source-intelligence-for-irregular-warfare)

US Director of National Intelligence. (2019). *National Intelligence Strategy* 2019

US Deparment of the Army (Temmuz-Eylül 2020) *Open source intelligence:*

now more and ever.

US Deparment of the Army (Temmuz-Eylül 2021) *Theater intelligence operations in competition.*

Wilhelm A. (2012). *The next 100 years? Reflections on the future of intelligence*. Routledge

Williams H.J. ve BLUM I. (2020). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. RAND Rapor No:RR1964.

Yıldız G. (2019). *Osmanlı Devletinde askeri istihbarat (1. basım)*. Yeditepe Yayınevi.

Zıółkowska A. (2018). *Open source ıntelligence (OSINT) as an element of military recon*. War Studies University.