İstihbarat Çalışmaları ve Araştırmaları Dergisi

Journal of Intelligence Research and Studies

Ocak 2023, Cilt: 2, Sayı: 1, ss.39-67

January 2023, Volume: 2, Issue: 1, pp.39-67

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

Makaleye ait Bilgiler / Article Information

Araştırma Makalesi / Research Article

Makale Başvuru Tarihi / Application Date : 30 Kasım 2022 / 30 November 2022

Makale Kabul Tarihi / Acceptance Date : 19 Aralık 2022 / 19 December 2022

Makalenin Başlığı / Article Title

Dijital Çağda İstihbarat Analizi

Intelligence Analysis in The Digital Era

Yazar(lar) / Writer(s)

M. Hayati TABAN ve Emre AYDİLEK

Atıf Bilgisi / Citation:

Taban, M.H. ve Aydilek, E. (2023). Dijital Çağda İstihbarat Analizi. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 2(1), ss.39-67, DOI: http://dx.doi.org/10.29228/icad.10

Taban, M.H. ve Aydilek, E. (2023). Intelligence Analysis in The Digital Era. *Journal of Intelligence Research and Studies*, 2(1), pp.39-67, DOI: http://dx.doi.org/10.29228/icad.10

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.10

DİJİTAL ÇAĞDA İSTİHBARAT ANALİZİ

M. Hayati TABAN [*] ve Emre AYDİLEK[**]

ÖZET

Değişen ve çeşitlenen tehdit iklimi, her alanda yaşanan teknolojik gelişmeler ve önemi gittikçe artan big data-algoritmalar-yapay zekâ vb. yeni analiz yöntemleri, günümüzde istihbarat alanının doğasının ve dönüşümünün dinamiklerindendir. Temel amacı devletlerin güvenliğine yönelik tehditlerin bertaraf edilmesine katkı sağlamak olan istihbarat toplulukları/kurumları, değişen koşullarda yeni risklerle/tehditlerle başa çıkmaya çalışmaktadır. İstihbarat döngüsünün en önemli aşamalarında olan istihbarat analizi de bu yeni konjonktüre göre yeniden şekillenmekte ve bu yeni ortama adapte olmaktadır. Bu noktadan hareketle çalışma, dijital çağ olarak adlandırabileceğimiz içinde bulunduğumuz dönemde istihbarat analizine odaklanmaktadır. İstihbarat analizinin dönüşümünde etkili olan dinamiklere ve tartışmalara ağırlıklı olarak yer verilen çalışmada, istihbarat analizinde mevcut ve gelecek perspektifler; veri madenciliğinde uzmanlaşma, algoritmalar geliştirme, insan unsurunun dijital yeniliklerle desteklenmesi gibi spesifik konular incelenmiştir.

Anahtar Kelimeler: *İstihbarat, İstihbarat Analizi, Açık Kaynak İstihbaratı, Dijitalleşme, İstihbaratın Değişimi.*

INTELLIGENCE ANALYSIS IN THE DIGITAL ERA

ABSTRACT

Today, the world has its own global characteristics due to the threat climate, the size of the data, the variety of actors and the speed of change. Intelligence communities/institutions, whose main purpose is to contribute to the elimination of threats to the security of states and to eliminate uncertainties, are trying to cope with the effects of these factors. As one of the most important stages of the intelligence cycle, intelligence analysis is also reshaped according to these factors. From this point of view, this study focuses on intelligence analysis in the digital age. In this age the importance of open-source intelligence has increased cyber space has created new threats. These factors are considered to be effective in the transformation of intelligence analysis. Thus, intelligence analysis has included algorithms by considering these factors and needs to adapt itself to this period by supporting the human element with digital innovations.

Keywords: *Intelligence, Intelligence Analysis, Open-Source Intelligence, Transformation of Intelligence, Digitization.*

[*] Dr. Öğr. Üyesi, Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü, mhtaban@kho.msu.edu.tr, ORCİD: 0000-0003-1785-9965.
[**] Dr., Kastamonu Üniversitesi, BAP Koordinatörlüğü, eaydilek@kastamonu.edu.tr, ORCİD: 0000-0002-4767-2424.
Makale Başvuru Tarihi / Application Date: 30 Kasım 2022 / 30 November 2022
Makale Kabul Tarihi / Acceptance Date: 19 Aralık 2022 / 19 December 2022

GİRİŞ

Dijitalleşmenin doruk noktasına ulaştığı çağımızda ekonomik, politik, sosyal ve kültürel birçok alanda hem fırsatlar hem de zorluklar ve tehditler aynı anda bir arada bulunmaktadır. Güvenlik ve istihbarat açısından düşünüldüğünde küreselleşmenin artan hızı, uluslararası aktörlerin giderek çeşitlenmesi, gelişen teknoloji gibi olgular, küresel belirsizlikler, sistemik riskler ve daha az öngörülebilir bir gelecek yaratmakta. Bu ortamda istihbarat alanında kalıcı stratejik avantaj elde etmenin anahtarı, karmaşık zorlukları hızlı ve doğru bir şekilde tahmin etme ve bunlara uyum sağlama yeteneği olarak öne çıkmaktadır (Director of National Intelligence, 2015, s.4).

Özellikle siber alandaki gelişmeler, istihbari hedef belirlemeden devşirmeye, istihbarat toplamadan işlemeye ve gizli operasyonların yürütülmesine uzanan bir çerçevede istihbaratın her alanına etki etmiştir. Örneğin Soğuk Savaş döneminde ABD'nin ihtiyaç duyduğu istihbari bilgilerin %80'i gizli, %20'si açık kaynaklardan elde edilirken Soğuk Savaş sonrası dünyada bu durum tersine dönmüştür. Açık kaynak istihbaratının (AKİS veya OSINT) daha fazla kullanılabilirliği nedeniyle "sırları elde etmek" için oluşturulmuş istihbarat kurumları, bu yeni bilgi/veri toplama sürecinde (açık kaynaklı bilgileri kendi toplama sürecine entegre etmekte) güçlük çekmiştir (Lowenthal, 2020, s.140). Bu güçlükleri aşmak amacıyla çeşitli çalışmalar yürütülmektedir. Örneğin Birleşik Krallıktaki en eski düşünce kuruluşlarından olan Royal United Services Institute (RUSI) tarafından "Birleşik Krallık Ulusal Güvenliği için Açık Kaynak İstihbaratının Geleceği" başlıklı raporda söz konusu alanda daha geniş ve belirli standartları olan destek altyapısı oluşturulması önerilmektedir (Janjeva, Harris ve Byrne, 2022, s.44).

İstihbarat toplulukları, Soğuk Savaş döneminden çok farklı olan 21. yüzyılın konjönktürüne adapte olmaya çalışmaktadır. Bu öyle bir değişimdir ki; istihbaratın her alanında hissedilmiş ve ivme tek bir temel hedeften (düşman devlet gibi) çok çeşitli hedeflere; varoluşsal tehditlerden belirgin hedeflere yönelik saldırı tehditlerine; herhangi bir A ülkesinin B aktörüne sağladığı silah bilgisinden belirli bir gemi, uçak veya birey hakkında harekete geçirilebilir istihbarat taleplerine doğru gerçekleşmiştir. Sovyetler Birliği'nin nükleer silah ve tehdit kapasitesinin keşfedilmesi için gereken istihbarat kabiliyetiyle, bir terörist grubun bir şehirde, alışveriş merkezinde

veya okulda doğaçlama bombalı eylem planladığını keşfetmek için gerekenler çok farklıdır. Bu iki konu hakkında veri toplama, analiz etme kabiliyeti oldukça asimetriktir. Dünyadaki bu değişikliklerin her biri istihbarat analistlerinden neyi bilmesi beklendiği ve işlerini nasıl yaptıkları üzerinde kayda değer etkiye sahiptir (National Research Council, 2011, s.10).

20. yüzyılın ikinci yarısına hâkim olan Soğuk Savaş sırasında istihbarata ilişkin en önemli sıkıntı, genellikle çok az veriye sahip olmaktı. Fakat 21. yüzyıldaki en temel sorunlardan biri mevcut bilginin hacminin büyüklüğüdür. Ayrıca bilgi teknolojisindeki gelişmeler istihbarat analizinde çalışanlara hem yardımcı olmuş hem de yeni sorunlar ortaya çıkarmıştır. Haber servislerinden ve World Wide Web'den gelen açık kaynaklı bilgilerde yaşanan patlama, istihbarat analizinin hızını ve hacmini gözden geçirmeyi daha da zorlaştırmıştır. Veri baş döndürücü bir hızla çoğalırken analistler ayıklamaları, analiz etmeleri ve yorumlamaları gereken bilgi yığınıyla karşı karşıyadır (Hedley, 2007, s.128). Yukarıda belirtildiği üzere istihbarat alanındaki değişimlerin bir kolu da istihbarat analizinde yaşanmaktadır. Analistlerin çalışma biçiminin son dönemde önemli ölçüde değiştiği açıktır.

ABD Ulusal İstihbarat Konseyi (National Intelligence Council) tarafından 2021 yılında hazırlanan 'Küresel Eğilimler 2040' raporunda istihbarat alanındaki bu yapısal değişimlere dikkat çekilmektedir. Gelecek perspektiflerinin ele alındığı raporda, bilgi teknolojilerindeki gelişmeler vurgulanmaktadır. Devlet ya da devlet dışı aktörlerin bilgiyi nasıl elde ettikleri, yorumladıkları ve kullandıkları konusunda öngörülere yer verilen analizlerde; yapay zekâ, nesnelerin interneti ve diğer araçlardan yararlanma oranının artacağı paylaşımı yapılmaktadır. Bu öngörüler istihbarat toplama ve analizindeki değişimlere işaret etmektedir (National Intelligence Council, 2021, s.97).

Açık kaynaklı bilgilerin hacminin artması, hedeflerin çeşitlenmesi (devlet dışı aktörlerin çoğalması) ve özellikle siber alandaki tehditler günümüz istihbarat alanını zorlayan faktörlerdir. Son dönemlerde istihbarat analizi, insan veya diğer geleneksel bilgi toplama kaynaklı çizgisinden uzaklaşarak; insan ve algoritmaların birleşiminden oluşan yeni ve hibrit bir temelde gelişmektedir. Buradan hareketle bu çalışmada, dijital çağda istihbarat analizi konusu incelenmektedir. Bu çalışmanın iddiası; veri madenciliğini, yapay zekâları ve algoritmaları bir yandan aktif-etkin olarak

kullanmayı başararak çağa ayak uyduran, diğer yandan insan unsurunu dışlamadan en doğru biçimde dijital tabanlı analizle entegre bir model oluşturabilen ülkelerin, geleceğin istihbaratına yön vereceğidir.

Üç bölümden oluşan çalışma, öncelikle istihbaratın dönüşümü ve değişimine tarihsel olarak yaklaşmaktadır. İkinci olarak istihbarat analizi hakkında kısa ama öz bir bilgilendirme yapılmakta ardından üçüncü bölümde günümüzde istihbarat analizinin karşılaştığı sorunlar ve dönüşümü ele alınmaktadır. Çalışma dijitalleşmenin istihbarat analizindeki dönüşümlere etkisine odaklandığından, istihbarata ilişkin bazı temel konuları inceleme dışında bırakmaktadır.

1. İSTİHBARATIN DEĞİŞİMİ VE DÖNÜŞÜMÜ

Klasik tanımıyla istihbarat, bilgilerin karar vericilere belirsizlikleri azaltmak veya kaldırmak amacıyla sağlanmasıdır (Johnson, 2010, s.5). Bu bağlamda bakıldığında istihbaratın amacı başka güçlerin bir devletin ulusal çıkarlarına zarar vermek üzere kurmakta oldukları kumpas plânlarına karşı devleti önceden ikaz etmesi bakımından koruma ya da savunma yararına ve o devletin dış politikası doğrultusunu ve yolunu hazırlaması anlamında da olumlu ve dışa yönelik bir faydaya hizmet eder (Kent, 2003, s.134). Bu nedenle stratejik sürprizlerden kaçınmak, uzun vadeli uzmanlık sağlamak, politika sürecini desteklemek ve bilgi, ihtiyaç ve yöntemlerin gizliliğini korumak, istihbarat kurumlarının var olma sebeplerini oluşturur (Lowenthal, 2020, s.3).

Öteden beri istihbaratın amacı, düşman veya rakiplerin ve bazen ortakların/müttefiklerin istekleri, niyetleri, yetenekleri ve eylemleri hakkındaki belirsizliği azaltmak olmuştur (Fingar, 2011, s.6). Bir toplumun güvenli bir biçimde yaşamını sürdürebilmesi için ilgili devletin dış ilişkiler, milli savunma ve diğer ulusal güvenlik politikalarının geliştirilmesi, koordine edilmesi ve icra edilmesi süreci hayati önem taşımaktadır (Biçer, 2017, s.435). Dolayısıyla istihbaratın amacı yalnızca bilgi toplamak değil karar vericilerin kendi kontrolleri dışındaki güçlerle başa çıkmada daha iyi seçimler yapmalarını sağlamaktır. Böylelikle istihbarat, kritik seçimler anında belirsizlik ve risk derecesinin azaltılmasına yardımcı olmaktadır (Director of National Intelligence, 2015, s.8).

Daha kapsamlı bakıldığında istihbarat bilgi, faaliyet/süreç ve kurum olarak farklı boyutları olan bir kavramdır. Bilgi anlamında istihbarat, bütün verileri kapsamasa dahi oldukça geniş anlamda ve çeşitlilikte bir yığın

oluşturan enformasyondur. Burada dikkat edilmesi gereken nokta, bu bilginin güvenlik kapsamına giren bir araştırma sürecinin sonunda üretildiğidir. Bilgi, nasıl keşfedildiğine bakılmaksızın bilinebilen her şeydir. Bu açıdan istihbarat politika yapıcıların belirtilen ihtiyaçlarını karşılayan ve bu ihtiyaçları karşılamak için toplanmış, işlenmiş ve daraltılmış bilgileri ifade eder. Daha net ifade edilirse, istihbarat bilgiyi içerir ama her bilgi istihbarat değildir. İstihbarat ve onun tanımlandığı, elde edildiği ve analiz edildiği tüm süreç, politika yapıcıların ihtiyaçlarına cevap veren bir niteliktedir (Lowenthal, 2020, s.2). Kurum olarak istihbarat ulusal güvenlik ile ilgili olarak bilgi peşinde koşan kişilerden ve düzenlemelerden oluşan bir organizasyondur. Bu organizasyonun yerine getirdiği faaliyetler de istihbarat kavramına içkindir (Kent, 2003). Bir faaliyet olarak istihbarat ise ulusal güvenlik için önemli olan belirli bilgi türlerinin talep edildiği, toplandığı, analiz edildiği ve politika yapıcılara sağlandığı sürecini; bu sürecin sonunda ortaya çıkan ürünleri, bu süreçlerin ve bilgilerin karşı istihbarat faaliyetleriyle korunması ve yasal makamlar tarafından talep edilen işlemlerin gerçekleştirilmesi işlevlerini kapsar (Lowenthal, 2020, s.4). İstihbarat süreci, istihbarat çarkını oluşturan bir dizi prosedür veya adım sonucunda gerçekleşir. Süreç, bir soru soran veya tavsiye isteyen bir karar verici tarafından başlatılır. Buna istihbarat gereksinimi denir. İstihbarat gereksinimleri ilgili istihbarat birimine iletilir ve döngü başlar. İstihbarat çarkı (ilk beşi ham verileri tamamlanmış, odaklanmış istihbarata dönüştüren, son ikisi elde edilen bu istihbaratı işleyen) yedi adımdan oluşur: 1. problem formülasyonu ve planlama; 2. bilgi toplama; 3. veri harmanlama; 4. veri işleme; 5. veri analizi; 6. rapor yazma; 7. karar vericilere dağıtma ve geri dönüt (Prunckun, 2010, s.5, Lowenthal, 2020, s.160). McGlynn ve Garner benzer ama daha sade bir formülasyonla istihbarat çarkını birbiriyle ilişkili altı aşamaya ayırmıştır: Gereksinimler; planlama ve yönlendirme, toplama, işleme ve kullanım, analiz, üretim, yayma, istihbarat çarkının aşamalarıdır (McGlynn ve Garner, 2019, s.22).

İstihbarat kavramı birçok farklı türde tasnife konu olmuştur. Alanlarına, bilgiyi toplama çeşitlerine, coğrafi-görev alanı ve faaliyet biçimine göre kategorize edilen istihbarat kavramı bu tasniflerin en yaygın tezahürleridir. En geniş sınıflandırmalardan birini yapan Özdağ istihbaratı, alanlarına göre dokuz kategoride incelemiştir. Bunları; siyasi istihbarat, askeri istihbarat, ekonomik istihbarat, sosyal istihbarat, coğrafi istihbarat,

biyografik istihbarat, ulaşım ve iletişim istihbaratı, bilimsel ve teknik istihbarat, siber istihbarat olarak sıralamıştır (Özdağ, 2014, s.8).

Bir başka tasnife göre ise istihbarat bilgiyi toplama çeşitleri açısından üç türlüdür: Teknik istihbarat, insan istihbaratı ve açık kaynak istihbaratı. Teknik istihbarat kendi içinde; muhabere istihbaratı, haberleşme istihbaratı, telemetrik istihbarat, elektronik istihbarat, ölçüm ve işaret istihbaratı, radar istihbaratı, görüntü istihbaratı, fotografik istihbarat gibi alt uzmanlık alanlarından oluşmaktadır (Yılmaz, 2015, s.185). İnsan istihbaratı sahadaki eğitimli uzmanlardan elde edilen bilgilerden oluşmaktadır (Urhal, 2008, s.222). Açık kaynak istihbaratı ise kamuya açık tüm kaynakların sunduğu verilerin toplanması olarak ifade edilebilir. Bu bakımdan hükümetin resmi evrakları, yazılı, görsel ve işitsel medya kaynakları, bilimsel ve süreli yayınlar ile uluslararası kuruluşların raporları açık kaynak istihbaratın bilgi edinme yolları olabilmektedir. Günümüzde istihbaratın yüzde 80'inin açık kaynaklardan temin edildiği tahmin edilmektedir. Açık kaynaklardan istihbarat toplama yöntemi, özellikle internetin yaygınlaşmaya başlaması ve sosyal paylaşım sitelerinin artış göstermesi ile birlikte oldukça önem kazanmıştır. Her gün milyonlarca insanın katrilyonlarca bit veriyi ağ sistemine eklemesi ciddi miktarda ham bir bilgi yığını meydana getirmiştir. Sosyal paylaşım sitelerinin popülerlik kazanması ile birlikte insanlar birçok alanda her türlü bilgiyi gönüllü olarak paylaşmaktadır. Günümüzde istihbarat servislerinin özellikle "Facebook, Twitter, Instagram" gibi sosyal paylaşım sitelerinden faydalanarak hedeflerine yönelik çalışmalar yürüttükleri bilinmektedir (Yılmaz, 2015, ss.184-186). Bunların yanında, literatürde, coğrafi açıdan; iç ve dış istihbarat (Johnson, 2007, s.1), faaliyet açısından operasyonel, taktik ve stratejik istihbarat (Gül, 2014, s.88) gibi farklı terminolojik tasniflerine de rastlanmaktadır. Çalışma kapsam olarak istihbarat analizine odaklandığından, istihbaratın sınıflandırılmasına yönelik bu bilgilerle yetinmektedir.

Akademik açıdan henüz çok yeni (yaklaşık yarım asırdır) bir disiplin olan istihbarat (Kahn, 2008, s.4), profesyonel bir alan olarak, Birinci Dünya Savaşı'nın hemen öncesinde, ilk olarak Britanya'da ve kısa bir süre sonra diğer savaşan ülkelerde ortaya çıkmıştır (Warner, 2007, s.23-24). Uygulamada kurumsal olarak 17. yüzyılın başlarından İkinci Dünya Savaşı'nın hemen sonrasına kadar, Avrupa ülkeleri kapsamlı istihbarat sistemleri geliştirmeye başladılarsa da bugüne kıyasla büyük bir başarı elde edememiş, İkinci Dünya Savaşı'yla birlikte, askeri istihbarat servisleri

kapsam ve gelişmişlik açısından büyük ölçüde genişlemiş ve günümüzdeki çok yönlü ve uzmanlık temelli bir niteliğe bürünmüştür (Prunckun, 2010, s.15).

İlkel düzeyde istihbarat uygulamaların tarihi ise binlerce yıllık bir geçmişe sahiptir. Yeryüzündeki ilk savaşlardan Birinci Dünya Savaşı'nın başlangıcına kadar, neredeyse tüm istihbarı bilgiler fiziksel kaynaklardan elde edilmiştir. Ancak bu yetersiz fiziksel istihbarat süreci, komutanların savaşları kazanmasına çoğu zaman yardımcı olacak düzeye erişememiştir. Modern dönemde ise daha önce önemsiz görülen faktörler değerli hale gelmiştir. Örneğin bir orta çağ kralı için düşmanının ne kadar kömür ve demir üretebileceği pek önemli değildi; oysa böyle bir bilgi modern devletlerin güvenlik kurumları için hayati önem taşımaktadır. Çünkü demiryolları büyük birliklerin hızlı seferber edilmesini, yoğunlaşmasını ve tedarik edilmesini mümkün kılmıştır. Dolayısıyla istihbarat artık, savaşlarda ilk göz önünde bulunması gereken önemli parametrelerden birine dönüşmüştür (Kahn, 2008, ss.5-6).

Son yüzyılda istihbaratın öneminin gittikçe arttığı, yalnızca savaşların kazanılmasında değil, devletlerin politika oluşturma sürecinde de göz önünde bulundurulan önemli bir faktöre dönüştüğünün tekrar vurgulanması yerinde olur. Özellikle İkinci Dünya Savaşı'nda ve takip eden Soğuk Savaş yıllarında istihbarat olgusunun modern devletler için önemini giderek artırmıştır. Bu da istihbarat örgütlenmesinin insan, araç-gereç ve mali kaynaklar açıdan genişlemesi sonucu doğurmuştur.

Soğuk Savaş boyunca, ABD başta olmak üzere birçok Batılı devlet esas olarak Sovyetler Birliği ve komünist bloğa karşı istihbarat toplamaya odaklanmış, dünyanın geri kalan bölgelerine ve sorunlarına daha az ilgi göstermiştir. Terör gibi meseleler ilgilenecek istihbarat konuları listesinde yer alsa da ancak 11 Eylül 2001'den itibaren istihbarat kurumlarının önceliği haline gelmiştir (Johnson, 2007, s.9).

Günümüzle kıyaslandığında Soğuk Savaş sırasında istihbarat toplama yöntemleri önceki dönemlere oranla giderek gelişmeye başladıysa da yine de yeterince kompleks değildi. Baskın uygulama biçimi, uydu keşifleri ve benzeri yöntemlerle elde edilen pahalı teknik istihbarattı (Walsh, 2011, s.11). Uyduların ve keşif uçaklarının (U-2'ler, SR-21'ler, İHA'lar) teknolojik yeteneklerine hayranlık duyan yetkililer, istihbarat bütçesinin çoğunu Sovyet tanklarını ve füze silolarını fotoğraflayabilen ve komünist başkentlerdeki

telefon konuşmalarını dinleyebilen gözetleme araçlarına kanalize etmişti (Johnson, 2007, s.8). Bunun yanında istihbarat toplulukları nükleer silahlar ile ilgili teknoloji transferi ve ticari istihbarata da yer yer önem vermişti. Ancak istihbarat alanında bu dönemde yüksek teknolojiye büyük paralar harcanırken zaman zaman verileri bir araya getirecek insanları (analistleri) unutmuş (Yılmaz, 2015, s.79) beşerî casus ağları ihmal edilmiştir (Johnson, 2007, s.8).

ABD ve Sovyetler Birliği'nin iki kutuplu güvenlik yapısının çöküşü, ulusal güvenlik istihbarat teşkilatlarının her zaman izlediği (ancak Soğuk Savaş'ın zirvesinde devlete varoluşsal tehdit olarak görülmeyen) uluslararası terörizm ve uyuşturucu kaçakçılığı gibi daha büyük bir tehdit çeşitliliği ortaya çıkarmıştır. Amerikan Merkezî Haberalma Teşkilatı (CIA) gibi kurumlar, varlıklarını tek bir büyük ve kalıcı hedeften (Sovyetler Birliği) çok sayıda daha küçük ve spesifik hedeflere ayarlamaya mecbur kalmıştır (Walsh, 2011, ss.14-15).

Takip eden yıllarda -özellikle 11 Eylül 2001'den sonra-, küresel bazda istihbarat örgütlerinin çalışmalarının çoğunun odağı, benzer biçimde ulus devletlerden devlet dışı aktörlere, özellikle de El Kaide gibi terör örgütlerine kaymaya başlamıştır. Ancak devlet dışı aktörleri izlemek, büyük ülkelerin konvansiyonel ve stratejik güçlerini izlemekten çok daha zor olmuştur (Fingar, 2011, s.8). Krizlerin ve çatışmaların doğası değişmiş ve bu kaçınılmaz olarak istihbarat alanına da yansımıştır.

Eski Amerikan Ulusal İstihbarat Direktörü Michael McConnell, konvansiyonel bir askeri tehditle başa çıkmanın, düşmanın kabiliyetini belirlemede nispeten daha kolay olduğunu kabul etmektedir. McConnell'a göre konvansiyonel bir düşman söz konusu olduğunda, düşmanın niyeti bir ölçüde bellidir ancak terörizm söz konusu olduğunda tehdidin doğası gereği muğlaklık ve belirsizlik baskın gelir. Bir başka ifadeyle, düşmanın zarar verme niyeti açıktır ama bu noktada istihbarat tarafından karşılaşılan zorluk düşmanın zarar verme kapasitesini öğrenmektir (McConnell, 2007). Dönemin CIA Direktörü Michael Hayden de istihbarat topluluğunun Soğuk Savaş'ta karşılaştığı sorunlarla bugün karşılaştığı sorunlar arasında bir başka farklılığa dikkat çekmektedir. Hayden'e göre Soğuk Savaş sırasında birlik oluşumları, tanklar ve balistik füze siloları gibi düşman kuvvetlerini bulmak görece kolaydı ama imhası zordu. Bugün ise durum tersine dönmüş ve artık

birincil düşmanın imhası kolay, bulunması ve fark edilmesi zordur (Hayden, 2007).

İstihbaratın dönüşümünü etkileyen en önemli bir diğer faktör teknolojik gelişmelerdir. Son yarım yüzyılda insan ve bilgisayar arasında gelişen bir ilişki olmuştur. Başlangıçta bilgisayarlar, insan problemlerini çözmede ek veya yardımcı araçlar olarak hizmet etmişlerdir. İnternet/Web alanındaki yeni gelişmeler, bilgi-veri alanlarında insan-bilgisayar simbiyozu için yeni roller yaratmış, aslında dinamik problem çözmede kurumsal kabiliyetleri artırmıştır. Web'in icadı ve en sıradan insan görevlerini bile etkilemeye başladığı olağanüstü hız kapasitesi hem dramatik hem de kafa karıştırıcı bir şekilde gerçekleşmiştir (Glassmann ve Kang, 2012, s.674). Bu da istihbarat kaynaklarının tamamıyla başka bir boyut almasına neden olmuştur. Açık kaynak istihbaratının, kamuya açık bilgilerden üretilen ve belirli bir istihbarat ihtiyacını karşılamak amacıyla toplanan, kullanılan ve zamanında uygun bir alıcıya dağıtılan niteliği göz önüne alındığında, internetin getirmiş olduğu değişim daha iyi anlaşılacaktır.

21. yüzyılından başından itibaren istihbarat örgütlerinden tüm nükleer silahlı füzelerin yerini saptamak yerine bireysel teröristlerin, bireysel el yapımı patlayıcı cihazların ve bireysel nakliye konteynırlarının yerini tam olarak belirleyebilmesi beklenmektedir. Odak bir avuç büyük ülkeden, neredeyse 200 ulus-devlette bulunan milyarlarca bireye genişlemiştir. Beklentilerin ve hassasiyet taleplerinin buna bağlı olarak artması, odağı değiştirmekten veya örgütsel birimlere birkaç analist eklemekten fazlasını gerektirmektedir. Küresel iklim değişikliği, bulaşıcı hastalıklar, siber güvenlik, insan kaçakçılığı, sahte ilaçlar ve uluslararası suç ağları gibi yeni sorunlara yönelen istihbarat örgütleri bu odak kaymasına ayak uydurmaya çalışmaktadır (Fingar, 2011, s.9). Bu süreçte istihbarat analizi ne oranda etkilenmektedir sorusunun cevabı için öncelikle istihbarat analizinin ne olduğundan bahsetmek gerekmektedir.

2. İSTİHBARAT ANALİZİ

Analiz, istihbarat döngüsünün en temel aşamalarından biridir (McGlynn ve Garner, 2019, s.22). Toplanan ham istihbaratın işlenmesini ve bu işlenmiş materyalin anlamını deşifre ederek karar vericilere iletilmesini, analistler sağlar (Marrin, 2008, s.131). Bir bakıma raporlama aşaması biter bitmez istihbarat analizi başlar denilebilir. Dolayısıyla istihbarat analizi, bir karar vericiye güvenlik ortamı hakkında bir yorum üretmek amacıyla, bilgiyi

işlemeye ve değerlendirmeye yönelik hem bilişsel hem de metodolojik bir yaklaşımdır (Walsh, 2011, s.237). Özünde istihbarat analizinin amacı uyarı sağlamak, belirsizliği azaltmak ve fırsatları belirlemektir (Fingar, 2011, s.35).

İstihbarat analizi bir gizemi ya da jeopolitik bir bulmacayı çözmeye benzer. Ulusun güvenliğini etkileme potansiyeli olan durumların önceden bilinmeyen boyutlarını keşfetme zorluğu, titizlik gerektirmektedir (Fingar, 2011, s.5). Analiz bir olayı bildirmekten ötesidir; "bu ne anlama geliyor?" sorusuna odaklanmaktır. Analiz sonucunda ortaya çıkan ürün, hızlı bir yorum, bir olayın yakın vadedeki olası sonuçlarının bir değerlendirmesi, uzun vadeli eğilimler ya da onların potansiyel sonuçları formunda olabilir. Her durumda istihbarat analistleri genellikle belirsiz, tutarsız, eksik ve bazen çelişkili verilerden anlam çıkarmaya çalışır (Hedley, 2007, s.123). Bunun da ötesinde analistler savunulabilir sonuçlara dayalı olarak karar vericilere çözümler veya seçenekler sunarlar. Bu noktada bu tür sonuçların mutlak olmadığı ve istihbarat bulgularını sunarken her zaman bir miktar olasılık veya belirsizlik olacağı kabul edilir (Prunckun, 2010, s.2).

İstihbarat analizi bir bakıma ihtiyaç duyulan problemin araştırılmasından nihai istihbarat ürünlerinin sağlanmasına kadar (örneğin, değerlendirmeler, görüntüler, sinyal raporlama) tüm faaliyetleri içeren bir süreçtir. Analizin en önemli ayaklarından biri olan problemi analiz ederken şu sorular sorulur: Problemin geçmişi nedir? Problemin nedenleri nelerdir? Problemin belirtileri nelerdir? Problemle başa çıkmak için mevcut hangi yöntemler var? Bu yöntemlerin sınırlamaları nelerdir? Böylece analiz alt birimler ve dış kuruluşlar tarafından sağlanan rafine, derlenmiş ve işlenmiş bilgi ve verileri kullanarak nihai istihbarat ürünlerini oluşturur (McGlynn ve Garner, 2019, ss.4-28).

Analiz süreci aslında istihbaratın toplanma safhasında başlar. Bir başka ifadeyle analiz açısından ayırt edici durum, istihbaratın toplanmasının analitik ihtiyaçlar için gereken yanıt çerçevesinde olmasıdır. Bu durum veri toplama ve analizi (ve karşı istihbaratı) stratejik bir düzeyde bir araya getiren ve daha sonra istihbarat topluluğuna nüfuz edecek olan 'istihbarat entegrasyonunun' da temelidir (Lowenthal, 2020, s.220).

Günümüzde istihbarat analizinin temeli, dijitalleşmenin doğurduğu bilgi yığınından uygun gerçekleri ayırt etmek ve küresel ölçekteki gelişmeleri ele almak için karar vermesi ve doğrudan eyleme geçmesi

gerekenleri bilgilendirebilecek yargıları ve içgörüleri belirlemeye evrilmiştir. Kararları ve eylemleri olumlu bir fark yaratabilecek şekillerde etkilemek, yaklaşmakta olan krizler konusunda uyarıda bulunmak, tehditleri tanımlamak, sorunları aydınlatmak, bunlara örnek olarak verilebilir (Hedley, 2007, s.124).

Farklı gereksinimler için genellikle (tanımlama, açıklama ve tahmin olmak üzere) üç düzeyde istihbarat analiz yapılır. Tanımlama, mümkün olduğu kadar çok ilgili değişkeni hesaba katarak incelenen olgunun netleştirilmesidir. Açıklama, fenomenin içerdiği unsurların bütün üzerindeki öneminin ve etkilerinin yorumlanmasıdır. Tahmin ise durum hakkında sentez ve sonuç çıkarımıdır (Krizan, 1999, s.29).

Analistler taktik (kısa vadeli veya sınırlı bir alanda), operasyonel (belirli bir eyleme göre uyarlanmış) veya stratejik (uzun vadeli veya daha kapsamlı alanda) istihbarat üretirler (Gill ve Phythian, 2018, s.174). İyi istihbaratın zamanında üretilmiş olması, hedefe yönelik düzenlenmiş olması, anlaşılır olması ve bilinen ile bilinmeyeni net bir şekilde gösterebiliyor olması gerekir. İstihbarat analizi yapılırken tüm bu kriterler göz önüne alınmalıdır (Lowenthal, 2020, s.260). Amerikan istihbarat topluluğu Rusya'nın 2016 ABD seçimlerine müdahale etmesine yönelik hazırladığı raporda istihbarat analizinin amacını, karar vericilere titiz, nesnel, zamanında, faydalı ve istihbarat standartlarına uygun değerlendirmeler sağlamak olarak belirtmiştir (U.S. Office of the Director of National Intelligence, 2017, s.1).

3. İSTİHBARAT ANALİZİNİN DEĞİŞİMİ VE KARŞILAŞAN SORUNLAR

İstihbarat analizinin, sivil politika yapıcılara ve askeri uygulayıcılara, karşılaştıkları sorunlar ve almaları gereken kararlarla doğrudan ilgili bilgiler sağladığı (Lowenthal, 2020, s.220), çözüm önerileri ve tahminler sunduğu daha önce ifade edilmişti. Şu ana kadar oluştan literatür ve kavramsal altyapı sayesinde, çalışmanın kapsamıyla ilişkili yeni ve son bir tartışmaya ihtiyaç vardır: İstihbarat olgusunun niteliğinde, sürecinde, teorik yazınında ve pratik uygulamalarında yaşanan dönüşüm, istihbarat analizinde nasıl tezahür etmiştir?

İstihbarat faaliyetinin başarısı, analistlerin doğrudan değişimin faydasını görmelerini, yeni süreçlere ve uygulamalara uyum sağlamalarını, benimsemelerini ve değişimi içeriden yönlendiren bir dijital kültür geliştirip

benimsemelerine bağlıdır. Dijital dönüşüm, istihbarat faaliyetinin tüm yelpazesine avantaj sağlamaktadır. Analistlerin, tehditleri algılama sürecinde hızlı hareket edebilmesi ve içgörülerini karar vericilere iletebilmesi için, dijital dönüşümleri mümkün olduğunca erken benimsenmesi bir zorunluluktur (Ashwell, 2017, s.408).

Gittikçe dijitalleşen çağımızda -istihbaratla ilgili ya da değil- hem her konuda ciddi sayıda veri/data mevcuttur ve bu hem günden güne artmakta hem de bunlara ulaşmak kolaylaşmaktadır. Dolayısıyla istihbarat açısından incelenecek, değerlendirilecek çok sayıda materyal mevcuttur. Yine de salt bilgi toplamak, hızla değişen ve giderek daha fazla birbirine bağlı olan dünyamızı anlamak için gerekli ancak yeterli olmayan bir koşuldur. Terabaytlarca veri tek başına olayların gidişatını, onları neyin yönlendirdiğini, nereye doğru gittiklerini, neyin raydan çıkıp yönünü değiştirebileceğini veya onları nasıl saptırabileceğini ortaya çıkarmaya yetmez. Verileri anlamlandırmak ve karar vericilere yardımcı olacak bilgileri damıtmak (verileri içgörüye dönüştürmek) için analiz etmek ön koşuldur (Fingar, 2011, s.10).

Günümüzde istihbarat analizini gerçekleştiren ekibin, geniş ulusal güvenlik tehditleri yelpazesini anlaması, bunlara ilişkin yargılar geliştirmesi ve benzeri görülmemiş miktarda ve türde bilgiye erişimle başa çıkması beklenmektedir. Aşırı bilgi yüklemesi bu alanda büyük bir zorluk teşkil etmektedir. Bu zorluklar göz önüne alındığında, analiz topluluğunun kapasitelerini artırmak bir gereklilik olarak ortaya çıkmaktadır (Director of National Intelligence, 2015, s.13).

Son dönemlerde istihbarat analizi, iş birliği içinde çalışan bir ekip tarafından yapılan bir etkinliğe doğru sürekli olarak gelişmektedir. Bu değişimin, uluslararası sorunların gittikçe karmaşıklaşması; daha fazla bilgiyi daha hızlı paylaşmaya verilen önemin artması; analistler, toplayıcılar, operatörler ve karar vericiler arasındaki sınırların bulanıklaşması gibi nedenleri bulunmaktadır (Pherson ve Heuer, 2015, s.25).

Soğuk savaş sonrası istihbarat analizinin ayırt edici özelliklerinden biri açık kaynak istihbaratının (Open Source Intelligence, OSINT) artan kullanılabilirliğidir. Dijital OSINT patlaması, 2000 yıllarda üç şeyin bir araya gelmesiyle gerçekleşmiştir: 3G bağlantılı akıllı telefonların kullanımının artması; vatandaşların, ülkelerindeki olaylarla ilgili büyük miktarda içeriği paylaşmak için az sayıda uygulamaya yönelmesi; bu

verilerin ücretsiz ve dünyanın geri kalanının erişmesi ve analiz etmesi için açık olması (Colquhoun, 2016). Dijitalleşmeyle birlikte kapalı toplulukların ve erişilemez alanların sayısı önemli ölçüde azalmıştır. OSINT'in en büyük avantajı erişilebilirliğidir ancak yine de bu kaynakların analiz edilmesi gerekir. Örneğin, güvenilir olarak bilinen bir gazeteyi haber kaynağı olarak kullanan analistin, bu açık kaynak bilgisini karar alıcılara iletirken şüphe ve sorgulama içerisinde olması gerekir. Sahte haber, aldatıcı bilgi, taraflılık, ön yargı ya da manipülasyon riski her zaman mevcuttur. Analist bu ihtimallere karşı uyanık olmalıdır. Aynı risk sosyal medya istihbaratı için de geçerlidir. Sosyal medya içerik açısından görece manipülasyona ve dezenformasyona açıktır. Sosyal medyadan toplanan istihbaratın analizinde doğru/yararlı bilgiler ve kasıtlı/yanlış gönderilerin ayırt edilmesi önemlidir (Lowenthal, 2020, ss.165-174). Benzer bir risk olarak internetten veya kamuya açık raporlardan elde edilen açık kaynaklı istihbarat, rakipler/düşmanlar tarafından kasıtlı olarak yayınlanan yanlış ve yanıltıcı bilgiler içerebilir. Analistleri yanıltmak ve istihbarat başarısızlığına yol açmak gibi amaçları içeren bu dezenformatik durumlara karşı, sorgulayıcı bir temelde yaklaşmak gerekir (Wu vd, 2022, s.452).

OSINT'in sağladığı verilerin büyüklüğü ve çeşitliliği bu yöntemle toplanan istihbaratın analizinde bilgisayar temelli farklı tekniklerin kullanılmasına yol açmıştır. Metinlerin analiz edilmesinde dilbilimel/metin tabanlı yöntemler, konum bilgileri ve kartografik bilgilerin analiz edilmesinde coğrafi bilgi sistemleri (GIS) ve uzaktan algılama, ilişkilerin, grupların ve ağların analizi için ağ bilimi ve son olarak da medya tabanlı verilerin analizinde görsel adli bilimler, OSINT ile elde edilen verilen analizinde kullanılan tekniklerin başlıcalarıdır (Ünver, 2018, s.8). İnsan destekli olarak gerçekleştirilen bu analizlerin yönü artık makine öğrenmesinin de bu alanda uygulanması ile birlikte, artık sonuç odaklı çıkarım yapmanın otomasyona bağlanacağı bir sürece doğru evrilmektedir (Williams ve Blum, 2018, s.40). OSINT sayesinde bireyler, gruplar (şirketler, kurumlar, örgütler, ülkeler gibi), olaylar, coğrafi bilgiler, IT ile ilgili veriler (alan adları, yazılımlar gibi) ve nesneler (resim ve video gibi) hakkında bilgiler daha kolay ve yoğun biçimde edilinilebilmektedir (Böhm ve Lolagar, 2021, s.325).

Bu şartlar altında istihbarat analizinde bilgisayar tabanlı ağ analizi, profil oluşturma ve veri madenciliği gibi yeni yöntemlerin önemi artmıştır. Örneğin ağ analizi, bireylerden kurumlara çeşitli hedefleri hakkında veri

toplamak için hem suç hem de güvenlik istihbaratında yaygın olarak kullanılmaktadır. Ağdaki düğümler arasındaki temas miktarlarını ölçmek (örneğin, e-posta ve telefon görüşmelerinin meta verilerini kaydederek) görece basittir, ancak bu temaslar içinde yararlı istihbaratı ayıklamak çok daha zordur. Bir diğer örnek olan profil oluşturma ise, hedefleme kararları için temel olarak kullanılan olağandışı veya şüpheli davranış kalıpları için büyük veri kümelerinin incelenmesine dayanan tekniklerdendir. Bu amaçla potansiyel tehditler hakkında veriler yığın halde biriktirilir ancak veri yığınlarının işlenmesinin aynı zamanda pek çok gereksiz bilgi içerdiği (profile uyan ancak hedef faaliyete dâhil olmayan insanlar gibi) unutulmamalıdır (Gill ve Phythian, 2018, s.175).

Büyük veri terimi, mobil İnternet, bulut depolama, sosyal ağlar ve 'nesnelerin interneti' gibi yeni bilgi teknolojileri (IT) tarafından yaratılan katlanarak artan miktarda dijital bilgi anlamına gelmektedir. Büyük veri, bilgide yalnızca niceliksel bir artışı değil aynı zamanda yeni bilgi yaratma ve dünyayı anlama biçimimizde niteliksel bir değişikliğe işaret etmektedir. Büyük verideki patlamanın çoğu, bilginin giderek daha fazla sosyal (birkaç büyük üretici yerine birçok kullanıcı tarafından üretilip iletilen), mobil (her yerde bulunan, internete bağlı mobil cihazlardaki sensörler tarafından toplanan) ve yerel (coğrafi olarak etiketlenen) olmasından kaynaklanmaktadır. Bu patlama sadece istihbaratın toplama alanını değil aynı zamanda işleme, analiz ve dağıtım süreçlerini de doğal olarak etkilemiştir. İstihbarat alanında büyük verinin en büyük vaadi, bilgileri bütünleştirme ve organize etme potansiyelidir. Verileri toplamak, taşımak, depolamak ve organize etmek için kullanılan yeni teknolojiler, tüm kaynaklardan analistlere daha fazla otomasyon ve üretkenlik ile çok daha fazla bilgiye erişim sağlayabilmekte ve böylece sınırlı bilişsel kapasitelerini en zor, en yüksek öncelikli sorunlara yoğunlaştırmalarına imkân vermektedir. Herhangi bir analist tarafından henüz işlenmemiş çok büyük miktarda veri depolanıp daha sonra gelecekteki veriler veya gereksinimler bağlamında işlemek veya ilişkilendirmeleri veya eğilimleri keşfetmek veya tanımak için kullanılabilir. Makine öğrenimi, tüm bu sürecin zamanla gelişmesini sağlar. Verilerin toplanması ve algoritmaların iyileştirilmesi, dinamik ve kademeli olarak daha doğru modellere veya daha sağlam ve uyarlanabilir modellerine imkân verir ve buna göre daha spesifik veya daha anlamlı anormalliklerin tespit edilmesini sağlar (Symon ve Tarapore, 2015, ss.4-6).

Her ne kadar internet ve sosyal medya büyük verinin varlığını mümkün kılan açık kaynaklar olsa da büyük veri internetten de iletişimden de daha fazlasıdır. Büyük veri kullanımı ile amaç normal şartlarda anlamlandıramadığımız veri kümesinden yeni çıkarımlar yapabilmektir. Böylece analistler araştırma konuları hakkında büyük miktarda bilgi toplayıp analiz ederek riskleri ve tehditleri tahmin etmeye yardımcı olabilecek trendler ararlar (Cukier ve Mayer-Schoenberger, 2013, ss.28-29).

Veri madenciliği büyük veri yığınındaki belirli örüntülerin ortaya çıkarılmasını sağlar. Veri madenciliği yoluyla tespit edilen modeller, bu süreçte farklı değişkenlerin bazılarının ilişkili olduğunu göstermekle birlikte nedenselliğe ulaşmakta yeterli değildir. Örneğin analistler, veriler arasındaki korelasyonlarla yalnızca bir kişi tarafından sergilenen belirli bir modelin bir teröristi işaret ettiğine ulaşabilir ancak tek başına bu çıkarım, bireyin tahmin edildiği gibi bir terörist olduğunu göstermez (Lahneman, 2016, s.710). Bunun yanında büyük veri analizi sınırlı soruları ele almak için tek veya çoklu toplama platformu şeklinde yapılandırılmış verileri kullanılarak kim, ne, nerede ve ne zaman sorularının analizinde işe yararken neden ve nasıl sorularının analizinde daha küçük bir rol oynar. Bu nedenle analiz sürecinde, istihbarat döngüsünü yönlendirilmesi ve verilerin kölesi olmak yerine, bu verilerin alıcının/karar vericinin gereksinimlerine hizmet ettiğinden (doğru soruları sorarak ve toplama ve analizi buna göre yönlendirerek) emin olunmalıdır (Symon ve Tarapore, 2015, s.8).

OSINT ürünlerini kullanmayla ilgili en önemli zorluklardan biri, halka açık olan bilgilerin hacmi ve bu bilgilerin doğasında bulunan güvenilirlik dereceleridir. Analiz alanında, verilerin artan hacmi, hızı ve çeşitliliği, 'gürültü ile sinyali' veya yığın verilerden yararlı bilgileri ayırt etmeyi zorlaştırmaktadır. Geleneksel beceriler, sistemler ve süreçler, çok fazla 'sinyalin' olduğu bir ortamda mücadele ettiğinden potansiyel 'istihbarat başarısızlıklarının' oluşmasına neden olabilmektedir. Modern bilgi işlem ve veri altyapısının geliştirilmesi ve sürdürülmesi, ticari sağlayıcıların, kullanıcılarının ihtiyaçlarına uyum sağlamak için önemli kaynaklara ve esnek bir yaklaşıma sahip olmasını gerektirmektedir (Janjeva, Harris ve Byrne, 2022, s.8).

Bu nedenle, güvenilir, 'iyi' istihbaratı 'kötü' istihbarattan ayırmak için, OSINT' analizlerine adapte olacak yeni modellere ihtiyaç vardır. Analiz sürecinde bilginin toplanması, anlaşılması, sınıflandırılması ve aynı zamanda

farklı kullanıcılar, ihtiyaçlar, görevler, organizasyonlar, kurumlar ve yasaların göz önünde bulundurulması gerekmektedir. Ancak böylelikle nihai ürün, mevcut kaynakların rehberliğinde analitik ve iyi sonuçlar sağlayabilecektir (Williams ve Blum, 2018, s.17). Açık kaynak verilerinin 'açık ve var' olması erişimin mutlaka kolay olduğu anlamına gelmez. Araştırmayı ilerletmek için gerekli verilerin belirlenmesi, bu tür verileri elde etmek için en iyi kaynağın ve yöntemin hangisi olduğunu belirlemenin ilk adımıdır. Ayrıca, doğru verilere erişilmesi yetmez. Bu verilerin kullanılabilir bir formatta olması da gerekir. Bu gereklilik analiz sürecini önemli ölçüde yavaşlatma riski barındırdığından, verilerin dönüştürüleceği formatlar da analiz ve üretim sürecinde dikkate alınması gereken bir konudur (Gibson, 2016, s.73).

OSINT altında da sınıflandırılabilen ama sunduğu imkânlardan dolayı farklı bir istihbarat toplama disiplini olarak da kabul edilen dijital çağdaki bir diğer kaynak, sosyal medya istihbaratıdır. Literatüre SOCMINT olarak geçen (Omand, Barlett ve Miller, 2012) sosyal medya istihbaratı, sosyal medyanın çok geniş kitleler tarafından aktif olarak kullanılmasından ötürü, istihbarat açısından değerli bir kaynaktır. Dijital ortamda tartışan, konuşan, şakalaşan, kınayan ve alkışlayan milyonlarca insanın tutumunu ölçmek ve anlamak istihbarat açısından değerli bilgi potansiyeli taşımaktadır. Örneğin şüphelileri hakkında konum vb. bilgiler arayan istihbarat görevlileri için sosyal medya, günümüzde hayati bir kaynak haline gelmiştir. Diğer taraftan kendi amaçları için kamuoyunu ve duyarlılığını anlamaya ve gizlice etkilemeye çalışanlar için de sosyal medya giderek daha da önem kazanmaktadır[1]. Sosyal medyayı izleyerek toplanan istihbaratı ifade eden SOCMINT, dijital çağın önemli bir parametresine dönüşmüştür (Omand, 2017, s.369). SOCMINT kullanılarak olayların 'ne zaman' meydana geldiği, şu anda 'ne' olduğu, 'nerede' ve 'kim' ile ilgili olduğu anlaşılarak gerçek zamanlı durumsal farkındalık sağlanabilir. Terörizmden sokak suçlarına kadar söz konusu faaliyetlerin 'neden' ve 'nasıl' olduğu gibi, gözlemlendikleri şekliyle olayların olası en iyi nedensel açıklamasını oluşturularak bu tür suç örgütlerine dair içgörüler elde edilebilir. Olaylara ve katılımcıların motivasyonlarına ilişkin yeterli açıklamalar elde edildiğinde, olayların nasıl gelişeceğine dair bir tahmin yürütülebilir. Sosyal medyadan

[1] Rusya'nın 2016 ABD başkanlık seçimlerindeki sosyal medya üzerinden yaptıkları için bkz. Robert S. Mueller Report On The Investigation Into Russian Interference In The 2016 Presidential Election, https://www.justice.gov/archives/sco/file/1373816/download

elde edilenler sayesinde politik ve operasyonel otoritelerin 'sırada ne var' ve 'nerede' gibi kaçınılmaz sorularını yanıtlamak kolaylaşabilmektedir (Omand, Barlett ve Miller, 2012, s.804; Omand, Barlett ve Miller, 2014, s.25).

Sosyal medyadan üretilen istihbaratın analizinde dikkat edilmesi gereken hususları örneklendirmek için bazı temel sorular sormak faydalı olabilir: Araştırılan istihbarata ilişkin sosyal medyada en etkili kişiler kimlerdir ve neden bu kadar etkililerdir? Cevap arama sürecinde, takipçi sayısı ve mesajlarının içeriğine bakılabilir. Ancak bu bizi bir başka soruya götürür: Diğer tüm veri toplama kaynakları gibi sosyal medya da aldatıcı içerikler barındırır. Araştırılan sosyal medya hesapları gerçek olmayan bir isimle açılmış olabilir ya da bireyler birden fazla hesaba sahip olabilir. Twitter gibi sosyal ağlarda, sahte takipçi satın alınabilmektedir (399 dolara 100.000 takipçi gibi). Ayrıca bu veriler belirli teknolojiler aracılığıyla elde edilebilmekle birlikte, örneğin Twitter akışlarının coğrafi konumu yanıltıcı olabilir. Bu gibi nedenlerden dolayı analistler büyük belirsizliklerle uğraşırlar. Dolayısıyla çoğu sosyal medya verisi ilk aşamada ham/güvenilmez istihbarattır ve önemli bir raporun temeli haline gelmeden önce -tıpkı diğer tüm istihbarat kaynakları gibi- analizi dikkatli yapılmalıdır (Lowenthal, 2020, s.184).

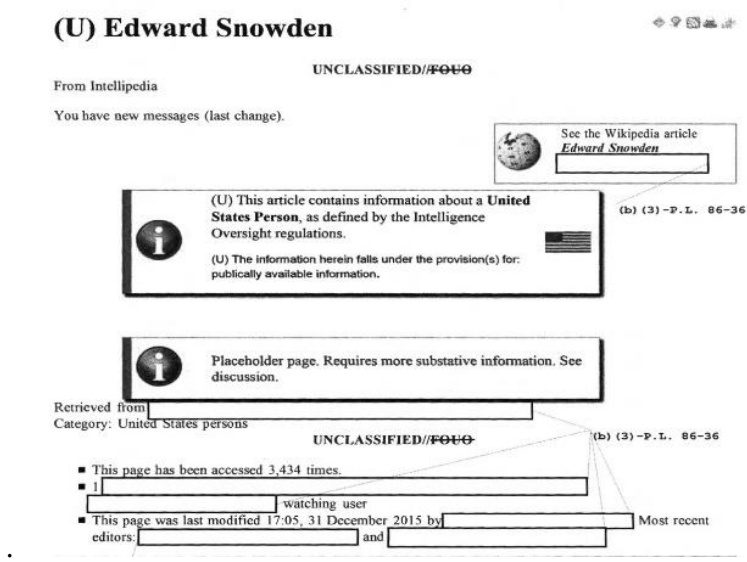
Analiz edilecek bilgi yığını her an arttığından analistlerin bu bilgi kaosunda anlamlı yorumlar getirme yeteneği, hizmet ettikleri topluluklarda kamu güvenliği ve yaşam kalitesi üzerinde büyük bir değere sahiptir. Öte yandan, analitik ve tahmine dayalı verilerden doğrudan operasyonel bir model oluşturma fırsatı, kamu güvenliği ve istihbarat uzmanlarına, rakiplerinin karar ve uygulama döngüleri içinde manevra yapma yeteneği verebilmektedir. Terörizme, uyuşturucuya veya diğer suçlara karşı savaşta, gelişmiş bilgi ve gelecekteki eylemleri tahmin etme yeteneği, ülkeler için hayati önemdedir (McCue, 2015, s.xxiv).

Ancak yığınlar halindeki âtıl/anlamsız veriler, istihbarat açısından bir anlam ifade etmez. Bu nedenle verilerin kullanılabilir olmaları için üzerinde çalışılması gerekir. Bu noktada algoritmalar önem kazanır. Algoritma seçimi, verilerin anlamlandırılmasını etkileyebilir. Farklı veri türlerini (salgın verileri, finansal veriler, sosyal medya verileri vb.) yorumlamak ve anlamlandırmak için farklı algoritmalar ve farklı uzmanlık türleri gereklidir. Ayrıca birbirleriyle uyumlu olmayan veri türlerini (heterojen veriler)

birleştirme ve anlamlı bir bütüne dönüştürme sorunu ile karşı karşıya kalabilme riski mevcuttur. Tıpkı diğer istihbarat kaynaklarının analistlere aktarılmadan önce işlenmesi ve ayıklanması gerektiği gibi, verileri anlam ifade edecek bir biçime veya içeriğe çevirmek, istihbarat analizi için zorunludur (Lowenthal, 2020, s.186).

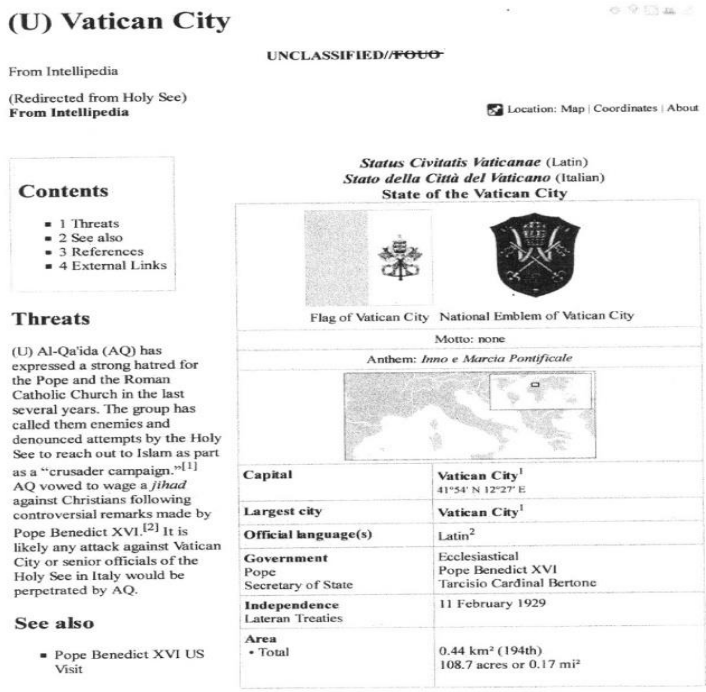
İstihbarat topluluklarının sözü edilen zorluklara ayak uydurma çabaları biz dizi yeniliği beraberinde getirmiştir. Özellikle analiz sürecine yönelik gelişmeler bu açıdan dikkat çekicidir. Bunlardan biri CIA analistleri tarafından geliştirilen ve Wikipedia ile aynı yazılımı kullanan, kimin neyi eklediğine dair bir denetim izi sağlayan Intellipedia[1] platformudur. Bu platform, bilgileri mümkün olan en geniş kitleye ulaştırırken, üç sınıflandırma seviyesine (tasnif dışı, gizli ve çok gizli) göre bilgiyi kategorize eder. Resim 1 ve Resim 2'de örnekleri gösterilen Intellipedia platformu kullanılabilir istihbari verilerin yanı sıra çok sayıda yararlı makale ile analistlerin bakış açılarını genişletmelerine katkıda bulunmaktadır (Gill ve Phythian, 2018, s.178).

Resim 1. Edward Snowden'e ait Intellepedia Ekranı (Kaynak: The Black Vault, http://documents.theblackvault.com/documents/intellipedia/Intellipedia-Snowden.pdf)



[1] İntellipedia hakkında daha fazla bilgi için bkz. Emily Dreyfuss,"The Wikipedia for Spies—And Where It Goes From Here", https://www.wired.com/2017/03/intellipedia-wikipedia-spies-much/

Resim 2. Vatikan'a ait Intellepedia Ekranı (Kaynak: Muckrock,(https://www.muckrock.com/news/archives/2014/feb/17/needs-edit-intellipedia-nsas-own-wikipedia/)



(U) Vatican City

UNCLASSIFIED//~~FOUO~~

From Intellipedia

(Redirected from Holy See)
From Intellipedia

Location: Map | Coordinates | About

Contents

- 1 Threats
- 2 See also
- 3 References
- 4 External Links

Threats

(U) Al-Qa'ida (AQ) has expressed a strong hatred for the Pope and the Roman Catholic Church in the last several years. The group has called them enemies and denounced attempts by the Holy See to reach out to Islam as part as a "crusader campaign."[1] AQ vowed to wage a *jihad* against Christians following controversial remarks made by Pope Benedict XVI.[2] It is likely any attack against Vatican City or senior officials of the Holy See in Italy would be perpetrated by AQ.

See also

- Pope Benedict XVI US Visit

Status Civitatis Vaticanae (Latin)
Stato della Città del Vaticano (Italian)
State of the Vatican City

Flag of Vatican City | National Emblem of Vatican City

Motto: none

Anthem: *Inno e Marcia Pontificale*

Capital	**Vatican City**[1] 41°54′ N 12°27′ E
Largest city	**Vatican City**[1]
Official language(s)	Latin[2]
Government Pope Secretary of State	Ecclesiastical Pope Benedict XVI Tarcisio Cardinal Bertone
Independence Lateran Treaties	11 February 1929
Area • Total	0.44 km² (194th) 108.7 acres or 0.17 mi²

Bunun yanında Amerikan istihbarat topluluğundaki tüm analistler için ortak bir çalışma alanı olan A-Space; iletişim bilgileri ve becerileri, uzmanlıkları ve deneyimleri hakkında ayrıntılar da dâhil olmak üzere Amerikan istihbarat topluluğundaki analistler hakkında bilgiler içeren bir veri tabanı olan Analitik Kaynaklar Kataloğu; dağıtılmış tüm istihbarat ürünlerinin entegre aramalarını, çapraz referanslarını sunan, tüm analistlerin belirli konulardaki raporları bulmasına olanak tanıyan Ulusal İstihbarat Kütüphanesi gibi bazı yeni platformlar, yeni dönemdeki zorluklarla daha kolay baş edebilmek için atılmış adımlara örnektir (National Research Council, 2011, s.11). İstihbarat analizinin platformlaştırılmasında bir diğer somut uygulama, zaman baskısı olan istihbarat değerlendirmelerinin üretiminde insanların, algoritmaların, yazılımların, araçların ve manuel çalışmanın entegrasyonunu geliştirerek istihbarat analistlerini güçlendirmek için tasarlanan Analitik Bileşen Sistemi (ACS) adı verilen bir hesaplama platformudur (Schmidt ve Vogel, 2020). Benzer şekilde hızla artan veri hacimlerini etkin bir şekilde yönetmek için gerekli araçları, analistleri ve

karar vericileri desteklemek için gerçekleştirilen çalışmalar, diğer ülkelerde de devam etmektedir. Örneğin Birleşik Krallık, analistlerin hem kamuya açık kaynaklar hem de dâhili hükümet raporları aracılığıyla bilgileri işlemesine yardımcı olacak (kullanıcıların açık kaynak materyali bulması, bağlaması ve tanıtması için ortak bir alan sunan) bir platform olan Bilgi ve Veri Alışverişi (INDEX) platformunu geliştirmiştir (Janjeva, Harris ve Byrne, 2022, s.10).

Dijital çağda istihbarat analistleri, artık geleneksel yöntemler yerine, otomatik arama, indeksleme, kategorilere ayırma ve yapılandırma süreçlerini takip ederek sürekli olarak bilgiyi (veya indekslerini) kurumsal bilgi tabanına aktarmaktadır. En alt seviyelerde, bu yapılanma söz dizimsel bir seviyede gerçekleştirilse de yakın gelecekte insanların, yerlerin, duyguların, hareketlerin, çağrışımların otomatik olarak tanımlanması gibi semantik veri yapılanmasının sunacağı fırsatlarla önemli ilerlemeler gerçekleşeceği öngörülmektedir. Bu alanda yapılacak çalışmalarla geleceğin analistinin bilgiyle etkileşiminin daha kolay ve işlevsel olacağı tahmin edilmektedir (Hare ve Coghill, 2016, s.9).

Günümüzde üretilen istihbarat, çok farklı formatlarda, bağlantısız veya erişilemeyen çok sayıda sistemde, standartlaştırılmış yapılar olmadan ve üzerinde anlaşmaya varılan kapsayıcı bir ontoloji olmadan üretilmektedir. Bu durum, bilgi toplama çabasının boşa gitmesi, zamanında istihbarat üretilememesi, işaretlerin ve uyarıların gözden kaçırılması ve üretilen istihbaratın karar almayla ilgili olmaması risklerini taşımaktadır. Bu faktörler, istihbarat döngüsünün erken safhalarında ve toplama noktasına mümkün olduğunca yakın çok kaynaklı istihbarat oluşturmak için verilerin birleştirilememesine neden olabilir. Dolayısıyla, istihbarat analizi politika yapıcılara ve uygulayıcılara zamanında, ilgili analitik yargılar ve eyleme geçirilebilir istihbarat sağlamak için zor, külfetli ve üstesinden gelinmesi gereken engeller içeren bir faaliyet haline gelmiştir (Weinbaum ve Shanahan, 2018, s.5).

Veri ve dijital teknolojiler, insan faaliyetinin her sektörü üzerinde belirgin bir etkiye sahip olan hızlı ve devam eden bir dijital dönüşümün temelini oluşturmaktadır. Bu dönüşüme ayak uydurabilenler, rakipleri karşısında kritik bir karar alma avantajına sahip olabilecektir. Geleneksel istihbarat döngüsüne (yönlendirme, toplama, işleme ve dağıtım) dayanan istihbarat analistlerinin artık dijital dönüşümün etkisiyle veri, korelasyon, tahmin ve karar vermeden oluşan yeni bir modelden yararlanması

gerekmektedir. Büyük veri, yapay zekâ ve algoritma kültüründen, paylaşım ve füzyondan yararlanan, nedenlere değil korelasyonlara odaklanan ve geleneksel sınıflandırılmış metodolojilerin yanı sıra bulut, kitlesel ve sosyal medya kaynaklarını kullanan bir modelin, istihbarat analizinin geleceği olması muhtemeldir (Ashwell, 2017, s.405).

SONUÇ

21. yüzyılda özellikle iletişim ve internet alanında yaşanan gelişmeler, bu çağın dijital/bilgi çağı gibi terminolojik ifadelerle adlandırılmasına neden olmuştur. Dijital çağdaki gelişmeler kaçınılmaz olarak istihbarat alanını etkilemiştir. Açık kaynak verilerindeki patlama, sosyal medya platformlarının yaygınlaşması ve veri analizinde yaşanan gelişmeler, istihbarat analizinin dönüşmesini gerektirmiştir.

İstihbarat analiz sürecinde, analistler uzun süre yeterli veri kaynağının olmamasının zorluklarını yaşamış ve yalnızca az miktarda veri yoluyla çıkarım yapabilmişlerdir. Bu da zaman zaman istihbarat başarısızlığının meydana gelmesine yol açmıştır. Sensör, internet ve diğer teknolojilerin hızla gelişmesiyle birlikte, açık kaynaklı istihbarat verileri, sinyal istihbarat verileri, uzaktan algılama görüntüleri gibi istihbarat veri kaynakları bugün bu zorlukları aşmak için ciddi fırsatlar sunmaktadır (Wu vd, 2022, s.451).

Birçok alan için geçerli olduğu gibi istihbarat analizi görevi de dönüşmektedir. Yeni teknikler ve teknolojiyle birleşen yeni bir dizi zorluk, istihbarat faaliyetinin doğasında yapısal bir değişime neden olmaktadır. İstihbarat analizindeki ilk büyük değişiklik, faaliyet alanının hacminin ve kapsamının artmasıdır. İstihbarat analizi artık her zamankinden daha fazla alanda gerçekleşmektedir. 10 yıl önce öyle önemsiz görünen sağlık, siber güvenlik ve iklim değişikliği gibi bağlamlar artık istihbarat analizi için büyük önem taşımaktadır. Bir diğer dönüşüm parametresi, istihbarat analistlerinin her zamankinden daha fazla bilgiyle uğraşmak, her zamankinden daha fazla bilgiyi sentezlemek ve anlamlandırmak zorunda kalmasıdır. Ayrıca istihbarat analizi, artık daha fazla iş birliği gerektirmektedir. Geleneksel istihbarat analizi bireyler tarafından yapılan tekil bir faaliyetken, bu alandaki ekip çalışmasının önemi ve faydası, problem alanının karmaşıklığı arttıkça anlaşılmaktadır (Cooke, 2015, s.132).

Dijital bir dönüşümün içinde bilgi çağı teknolojileri beklenmedik ve durmaksızın bir hızla gelişmeye devam etmektedir. Nesnelerin interneti ve büyük veri analitiği kavramları günlük yaşamın her alanına nüfuz etmiş

durumda. Dijital teknolojilerin etkisi ve internetin gelişimi kitlesel birbirine bağlılığı güçlendirerek tüm faaliyet alanlarındaki hızlı değişimin temelini oluşturmaktadır. Bu değişim istihbarat analizi kuruluşlarının ve kolluk kuvvetlerinin karşı karşıya kaldığı organize suç ve terörizm gibi meseleleri daha iyi anlama ve bunlarla mücadele etmek için süregelen dijital dönüşümden tam olarak yararlanma fırsatı sunmaktadır. Diğer taraftan tehditlere karşı koymak için veri ve bilgi teknolojilerinden yararlanacak analistlerin yetiştirilmesi büyük önem arz etmektedir. World Wide Web, sosyal medya ve artan küreselleşme gibi devlet-örgüt-insan faaliyetinin tüm yönlerini etkileyen olaylar veriye, bilgi teknolojilerine ve insana odaklanan etkin dijital dönüşüm, çağa ayak uydurabileceklere önemli bir rekabet avantajı sağlama potansiyeline sahiptir. Dijitalleşme, daha önce karmaşık olan süreçleri ve görevleri, analistlerin anlamasını ve kullanmasını kolaylaştırmaktadır. Giderek daha fazla otomatikleştirilen veri madenciliği ve analizi yeni ve heyecan verici içgörüler ve modeller sağlamaktadır. Verilerdeki algoritmalar ve korelasyonlar fırsatları ortaya çıkarmakta ve çeşitli faaliyetlerde potansiyel rekabet avantajı sağlayan karar verme sürecini iyileştirmektedir (Ashwell, 2017, ss.393-394).

Dijital dünyada istihbarat üretim sürecinin dönüşmesi kaçınılmazdır. Bu sürecin özü, daha fazla veri aramak ve bir analistin yapabileceğinden çok daha fazla hipotezi inşa etmek için algoritmalar ve istatistikler kullanan makinelere yön vermeye dayanmaktadır. Beşerî analitik beceri ve deneyim makinelerin oluşturduğu korelasyon modellerini ve bilgileri elemek için hala çok fazla gerekli olsa da algoritmalar ve bilgisayar modelleri, analistleri, arama ve işleme yükünün çoğundan kurtarabilir ve analitik görevin kritik unsuruna, yani problem çözmeye odaklanması için daha fazla zaman sunar. Uygulamalar bilgiyi özümseme, anlamlandırma ve karar verme şeklimizi değiştirmektedir. Doğal olarak bilgi yığınlarına, karmaşık fikirlere ve teknolojilere uygun maliyetli erişime izin verir ve bunların kullanımını basitleştirirler (Ashwell, 2017, ss.399-400). Veri işleme teknolojileri, verilerden tam olarak yararlanma, tamamlayıcı entegrasyon ve kapsamlı araştırma/muhakeme gibi dijital yenilikler, istihbarat analizini iyileştirmenin anahtarlarıdır. Derin öğrenme gibi akıllı algoritmalar, istihbarat analistlerinin doğal dil anlama, konuşma tanıma, görüntü sınıflandırma, hedef tanıma gibi işlemleri hızlı bir şekilde gerçekleştirmesine, işleme verimliliğini artırmasına, dolayısıyla analistlerin yükünün azalmasına ve gizli korelasyon bilgilerinin keşfedilmesine yardımcı olan araçlardır. Büyük veri yığınlarının

işlenmesi için fayda sağlayan akıllı algoritmalar ve büyük verileri verimli bir şekilde depolayabilen bulut teknolojileri analiz sürecinde ek yükü azaltan gelişmelerdir (Wu vd, 2022, ss.451-454).

Özetle, dijitalleşme, algoritmalar, yapay zekâ gibi yeni istihbarat analizi modellerinin önemi yadsınamaz bir gerçeğe dönüşmüştür. Ancak sadece bu dijital yöntemler üzerinden istihbarat analizini gerçekleştirmek mümkün değildir. İnsan unsuru analiz sürecinin halen oldukça önemli bir parçasıdır. İstihbarat gizemleri salt bilgi toplanarak çözülemez. Bir gizemin derinlerine inmek, analiz ve muhakeme gerektirir. Veri tufanı çağında bu noktada istihbarat topluluklarının özellikle ekonomistlerden veri bilimcilere kadar uzmanların niceliksel ve niteliksel analitik yeteneklerinden daha fazla yararlanmaları gerekmektedir (Coyne, 2017).

Dijital olarak dönüşen istihbarat organizasyonlarında, insan sezgisinin eşsiz gücüne hâlâ ihtiyaç var. Makineler devasa verileri toplayıp işleyebilir ve birden çok hipotezi dikkate alarak ilgi alanları, modelleri ve aykırı değerleri üretebilirken, insanlar da arama sürecini yönlendiren üst akıl olarak konumlandırılmalı, makinelerin sunacağı pek çok seçenek arasından en değerli bilgi ve bilgi külçelerini hızla elemek ve seçmek için deneyim ve sezgilerini uygulamaya devam etmelidir. Özetle gerekli olan şey makinelerin giderek daha fazla veri işleme sürecini üstlendiği ve analistlere en zor sorun çözme görevine odaklanmaları için giderek daha fazla zaman tanıyan doğru koşullardır. Aynı şekilde analistlerin dijital çağ süreçlerini ve davranışlarını benimsemelerini teşvik eden veri ve teknolojilerle etkileşime girmelerine olanak sağlamak sürecin anahtarı olmaya devam edecektir (Ashwell, 2017, ss.394-407).

Son olarak, istihbarat analizinde dijitalleşmeye yönelik birtakım varoluşsal eleştirilerden bahsetmek gerekir. Wu ve arkadaşlarına (2022) göre akıllı algoritmaların uygulamalarında belirli sınırlamaları olduğu ve istihbarat analizlerinde tamamen insanın yerini alabilmeleri için daha kat edilmesi gereken çok yol var (Wu vd, 2022, s.452). Gilchrist'e (2017) göre ise veri kaynaklarındaki olağanüstü artış bunları işlemek için insan kaynaklarındaki artışla paralel olmamıştır. Doğası gereği insani ve belirsiz bir sorun olan savaşlar için makine çözümlerine ve kesinliğe sahip olacaklarına dair vaatler ve bilgi üstünlüğünün kutsallaştırılması orduları, savunmasız bırakmaktadır. Mevcut yazılımlar-algoritmalar karmaşık insan etkileşimlerini, iyi eğitimli bir analistin yapabileceği veya yapması gerektiği

şekilde veya aynı zaman duyarlılığıyla anlamlandıramaz. Öte yandan askeri analistler geleneksel olarak nicel becerilerden çok nitel becerilere güvenirler. Başarıları büyük ölçüde zor kazanılmış deneyimlerden gelen sezgilere dayanmaktadır. Gelişmiş analitiği çalıştırmak için gereken beceri ve yetenek ise büyük ölçüde bunun tersidir. Analistler sosyal medya gönderilerinden, görüntü kayıtlarına ve tonla kâğıt parçasına kadar her şeyle ilgilenir. Veri standartlarını kontrol etmek hem inanılmaz derecede zordur hem de zaman alıcıdır. 'Veri girişi' zayıf olduğunda, 'veri çıkışı' yanlış olacaktır. Orduya pazarlanan analiz platformlarının birçoğu finans ve endüstri için geliştirildiğinden savaşın doğasında var olan kaosa düzen getirebilecek bir algoritma yazmak büyük ölçüde imkânsızdır (Gilchrist, 2017).

İstihbaratın tarihsel ve konjonktürel anlamda değişimi, güvenlik tehditlerinin bertaraf edilmesinde sürekli yeni zorluklar inşa eden bir diyalektiği doğurmaktadır. Bu durum, istihbarat çarkında en önemli aşamalardan biri olan istihbarat analizinin önemini artırmaktadır. İstihbarat toplulukları teknolojinin, ulaşımın ve iletişimin sürekli gelişiminin yanında artan küreselleşmenin yarattığı yeni koşullara ayak uydurma sorunuyla baş etmek zorundadır. Bu kapsamda istihbarat analizinde yeni yöntemlerin geliştirilmesine ek olarak mobilite ve hibritleşmeyi zorunlu kılan bir anlayışın analistlere yön vermesi gerekliliği ortaya çıkmaktadır.

İnternet ve dijitalleşmenin giderek yaygınlaşacağı aşikârdır. Bunun doğal bir sonucu olarak algoritmalar istihbarat analizindeki süreçlerde ilk sıralarda olmaya devam edecektir. İlerleyen dönemlerde kapsamı ve içeriği artması muhtemel bilgi yığınlarından anlamlı analizler gerçekleştirebilecek analistlerin yetiştirilmesi, eğitilmesi ve uzmanlaştırılması[1], ülkeler ve istihbarat toplulukları için hayati öneme sahip olacaktır. Bilgi güç demektir. Gelecekte bilgiyi yorumlamak, güvenliği sağlamak için temel kıstas olma potansiyeline sahiptir.

[1] 2008 yılında Amerikan Ulusal İstihbarat Direktörü, Ulusal Araştırma Konseyi'nden, analitik yöntemlerle ve bunların istihbarat alanındaki potansiyel uygulamalarıyla ilgili davranışsal ve sosyal bilimlerden elde edilen yöntemleri değerlendirmelerini talep etmiştir. Bu talebin ardından Konsey istihbarat alanında davranışsal ve sosyal bilimlerin özellikle analiz alanında kullanılmasını, bilimsel analitik yöntemlerinin analistlere öğretilmesini, bilimsel iş birliği yöntemlerinin uygulanmasını ve bilimsel iletişim yöntemlerine başvurulmasını önermiştir (National Researh Council, 2011, s.xiii).

KAYNAKÇA

Ashwell, M.L. (2017). The digital transformation of intelligence analysis, *Journal of Financial Crime,* 24(3), ss. 393-411, doi: 10.1108/JFC-03-2017-0020

Biçer, S. (2017). Ulusal güvenlik ve istihbarat sisteminde geleneksel anlayıştan modern ve değişen ihtiyaçlar dönemine geçiş. *Karadeniz Sosyal Bilimler Dergisi*, *9(2)*, ss. 435-464

Böhm, I. ve Lolagar, S. 2021. "Open Source Intelligence: Introduction, Legal, and Ethical Considerations". *International Cybersecurity Law Review, 2(2)*, 317-37. doi: 10.1365/s43439-021-00042-7.

Clark, R. M. (2016). *Intelligence analysis: a target-centric approach*. CQ Press.

Colquhoun, C. (2016). A Brief History of Open Source Intelligence, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

Cooke, N. J. (2015). The Changıng Context And Dynamıcs Of Intellıgence Analysıs, *The Human Factors of Intelligence Analysis* içinde, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 59 (1), ss,130-134

John Coyne, J. (2017). The future of intelligence analysis: computers versus the human brain? *The Strategist,* https://www.aspistrategist.org.au/future-intelligence-analysis-computers-versus-human-brain/

Cukier, K. ve Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs, 92 (3)*, ss. 28-40

Director of National Intelligence (2015). *Vision 2015: A globally networked and integrated intelligence enterprise*. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision_2015.pdf

Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford University Press.

Gibson, Helen. 2016. "Acquisition and Preparation of Data for OSINT Investigations", ss. 69-93 içinde *Open source intelligence investigation: From Strategy to Implementation*, editör B. Akhgar, P. S. Bayerl, ve F. Sampson. New York, NY: Springer Berlin Heidelberg

Mark Gilchrist, M. (2017). You can't write an algorithm for uncertainty: why advanced analytics may not be the solution to the military 'big data' challenge, *The Strategist*, https://www.aspistrategist.org.au/cant-write-algorithm-uncertainty-advanced-analytics-may-not-solution-military-big-data-challenge/

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

Glassman, M., and Kang M.J. (2012). Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)." *Computers in Human Behavior 28(2)*. 673–82. https://doi.org/10.1016/j.chb.2011.11.014.

Global Trends 2040: A More Contested World, Mart 2021, National Intelligence Council https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

Gül, Z. (2014). İstihbarat çeşitleri ve stratejik istihbarat. Harmancı, F.M. v.d. (Ed.). *Güvenlik Sektöründe Temel Stratejiler* içinde. (ss.83-98). Nobel Yayınları.

Hare, N. ve Coghill, P. (2016). The future of the intelligence analysis task, *Intelligence and National Security*, 31 (6), ss. 858-870

Hayden, M. V. (2007). Remarks of central intelligence agency director at the council on foreign relations. New York. https://irp.fas.org/cia/product/dcia090707.html

Hedley, J.H. (2007). The challenges of intelligence analysis. Johnson, L. K. (Ed.). *Strategic Intelligence: Understanding the hidden side of government* içinde. (ss.123-138). Praeger Security International.

Janjeva, A., Harris, A., & Byrne, J. (2022). The Future of Open Source Intelligence for UK National Security. RUSI Occasional Paper, 7

https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf

Johnson, L.K (2007). Introduction. Johnson, L.K. (Ed.) *Handbook of Intelligence Studies* içinde. Routledge.

Johnson, L.K (2010). National Security Intelligence. Johnson, L.K. (Ed.) *The Oxford Handbook of National Security Intelligence* içinde. Routledge, ss.3-32

Kahn, D. (2008). An historical theory of intelligence. Gill, P., Marrin, S. ve Phythian, M. (Ed.). *Intelligence Theory Key Questions and Debates* içinde. Routledge.

Kent, S. (2003). *Stratejik istihbarat* (Y. Özbek ve N. Şüküroğlu, Çev.) ASAM Yayınları.

Krizan, L. (1999). *Intelligence essentials for everyone. occasional paper #6*, Joint Military Intelligence College. https://apps.dtic.mil/sti/pdfs/ADA476726.pdf

Lahneman W. J. (2016). IC data mining in the post-Snowden era, *International Journal of Intelligence and Counter Intelligence.* 29 (4), ss.700-723.

Lowenthal, M. M. (2020). *Intelligence: From secrets to policy*. CQ Press.

Mangır, D. Ş. ve Küçükkırlı, S. N. (2019). Gelenekselden dijitale siber istihbarat ve Rus dış politikası. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. Özel Sayı, ssss. 296-308

Marrin, S. (2008). Intelligence analysis and decisionmaking, Gill, P., Marrin, S. ve Phythian, M. (Ed.). *Intelligence Theory Key Questions and Debates* içinde. Routledge.

McConnell, J. M. (2007). Remarks and Q&A by the director of national intelligence. Project on National Security Reform Conference (July 26), Washington, DC. https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070726_speech.pdf

McCue, C. (2015). *Data mining and predictive analysis: Intelligence gathering and crime analysis*. Butterworth-Heinemann.

McGlynn, P. ve Garner, G. (2019). *Intelligence analysis fundamentals*, CRC Press

Millî İstihbarat Teşkilâtı (2002). *İstihbaratın Tanımı ve İstihbarat Çarkı*, Erişim Tarihi: 10.11.2022. https://www.mit.gov.tr/tarihce/giris.html

Mueller R. S. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election, https://www.justice.gov/archives/sco/file/1373816/download

National Research Council (2011). *Intelligence analysis for tomorrow: Advances from the behavioral and social sciences*. National Academies Press.

Omand, D., Miller, C ve Bartlett, J. (2014). "Towards the Discipline of Social Media Intelligence", ss.24-43 içinde *Open Source Intelligence*

in the Twenty-First Century New Approaches and Opportunities, editör C. Hobbs, M. Moran, ve D. Salisbury

Omand, D. (2017). "Social media intelligence (SOCMINT)". R. Dover, H. Dylan, ve M. S. Goodman (Eds.) Ss. 355-71 içinde *The Palgrave handbook of security, risk and intelligence* içinde, ss. 355-71, editör. London: Palgrave Macmillan

Omand, David., Jamie Bartlett, J. ve Miller, C. (2012). "Introducing social media intelligence (SOCMINT)". *Intelligence and National Security*, 27 (6), ss.: 801-23. doi: 10.1080/02684527.2012.716965 ss. 24-43

Özdağ, Ü. (2014). *İstihbarat teorisi*, Kripto Kitaplar

Pherson, R. H. ve Heuer, R. (2015). *Structured analytic techniques for intelligence analysis*. CQ Press

Prunckun, H. (2010). *Handbook of scientific methods of inquiry for intelligence analysis*, The Scarecrow Press.

Schmidt, M. ve Kathleen, M. V. (2020). "Algorithms that Empower? Platformization in U.S. Intelligence Analysis," *2020 IEEE International Symposium on Technology and Society (ISTAS)* (12-15 November 2020), doi:10.1109/ISTAS50296.2020.

Symon, P. B., ve Tarapore, A. (2015). Defense intelligence analysis in the age of big data. *Joint Force Quarterly,* 79 (4), ss.04-11.

U.S. Office of the Director of National Intelligence (2017). Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution [and] Assessing Russian Activities and Intentions in Recent U.S. Elections. Intelligence Community Assessment. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Urhal, Ö. (2008). *Kamu güvenliği açısından istihbarat ve örgütlü suçlar*. Adalet Yayınları.

Ünver, A. (2018). *Dijital Açık Kaynaklı İstihbarat ve Uluslararası Güvenlik*, EDAM. https://edam.org.tr/dijital-acik-kaynakli-istihbarat-ve-uluslararasi-guvenlik/

Walsh, P. F. (2011). *Intelligence and intelligence analysis*. Routledge

Warner, M. (2007). Sources and methods for the study of intelligence. Johnson, L.L. (Ed.) *Handbook of Intelligence Studies* içinde, Routledge

Weinbaum, C. ve Shanahan, J.N.T. (2018). Intelligence in a data-driven age, *Joint Force Quarterly, 90(3)*, ss. 4-9

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise.* Rand Corporation.

Xu Wu, Daguo Qin, Yang Li (2022) Challenges and Inspirations of AI and Related Technologies in Intelligence Analysis, *IEEE ITAIC*, ss. 451-455

Yılmaz, S. (2015). *İstihbarat bilimi.* Kripto Kitaplar.