DUMLUPINAR ÜNİVERSİTESİ SOSYAL BİLİMLER DERGİSİ
DUMLUPINAR UNIVERSITY JOURNAL OF SOCIAL SCIENCES
E-ISSN: 2587-005X https://dergipark.org.tr/tr/pub/dpusbe
Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 89, 56-71; 2026.
DOI: 10.51290/dpusbe.1814955

Araştırma Makalesi / Research Article

BIG DATANIN İSTİHBARAT ÜZERİNDEKİ ETKİSİ: AÇIK KAYNAK İSTİHBARATININ ARTAN ÖNEMİ, FIRSATLAR VE TEHDİTLER*

Hatice KOÇ [1]
Batuhan Yaşar GÖKSEL[2*]

Öz
Rekabetçi doğası gereği kendisini çağın gereksinimleri doğrultusunda sürekli geliştirme ihtiyacı içerisinde bulan istihbarat disiplini devletler için vazgeçilmez bir veri işleme bilimidir. Günümüz dünyasında yaşanan büyük ölçekli gelişimler ve değişimler sonucunda etkilenen ve kendi dinamikleri içerisinde önemli reformist dönüşümler geçiren istihbarat toplama yöntemleri içerisinde 'Açık Kaynak İstihbaratı (OSINT)' çalışmalarının sürekli ve dur durak bilmeyen bir dönüşüm geçirdiği gözlemlenmiştir. Bu dönüşümü diğer istihbarat toplama yöntemlerinden ayıran en önemli karakteristik özelliğin, imkânları ve kapsamı ilerleyen zaman içerisinde kümülatif ve kesintisiz biçimde artan 'Big Data' tekniklerinde yaşanan gelişimler olduğu saptanmıştır. Enformasyon toplumunun ürettiği yüksek ölçekte veri yığınlarının tabiri caizse 'süzülmüş' analizlerinin, devletlerin güvenlik ihtiyaçlarını karşılama ve istihbarat faaliyetleri gerçekleştirebilme noktalarında vazgeçilmez bir alana dönüştüğü gözlemlenmektedir. Bu bağlamda OSINT ve Big Data mefhumlarının birbirleriyle olan ilişkilerinin doğru biçimde tespit edilebilmesi, bu ilişki perspektifinde ortaya çıkacak potansiyel kullanım araç ve yöntemlerinin devletlerin istihbarat teşkilatlarına ne gibi potansiyel kazanımlar vaat ettiğinin sağlıklı şekilde belirlenebilmesi ve bu kavramların birbirleri ile olan etkileşimleri içerisinde ne gibi tehditler taşıdığının sistematik olarak algılanabilmesi, çağımız devletleri adına bir zorunluluk haline gelmiştir. Bütün bu aktarılanlar dolayısıyla bu çalışma ana odağında Big Data ve OSINT kavramlarını çözümleyerek birbirleri ile kaçınılmaz ilişki içerisinde olan bu kavramların ortaya çıkarttıkları potansiyel fırsatlar ve tehditleri; genel bir literatür taraması kapsamında kavramsal açıklamalar, örnek olaylar ve değerlendirmeler aracılığıyla analiz edecektir.
Anahtar Kelimeler: İstihbarat, Açık kaynak istihbaratı, Big data
JEL Kodları: H56, O33, Z18

THE IMPACT OF BIG DATA ON INTELLIGENCE: THE INCREASING IMPORTANCE OF OPEN SOURCE INTELLIGENCE, OPPORTUNITIES AND THREATS

Abstract
Due to its competitive nature, the discipline of intelligence finds itself in a constant need to evolve in line with the demands of the era, making it an indispensable data processing science for states. As a result of the large-scale developments and changes experienced in today's world, intelligence gathering methods, which have been affected and undergone significant reformist transformations within their own dynamics, have undergone a continuous and relentless transformation in 'Open Source Intelligence (OSINT)' studies. It has been determined that the most important characteristic distinguishing this transformation from other intelligence gathering methods is the developments in 'Big Data' techniques, whose capabilities and scope have increased cumulatively and continuously over time. It has been observed that the filtered analysis of the large amounts of data produced by the information society has become an indispensable area in meeting the security needs of states and carrying out intelligence activities. In this context, it has become imperative for modern states to accurately identify the relationship between the concepts of OSINT and Big Data, to properly determine the potential benefits that the tools and methods arising from this relationship could offer to state intelligence agencies, and to systematically understand the threats inherent in the interaction between these concepts. Therefore, this study will focus on analyzing the concepts of Big Data and OSINT, examining the potential opportunities and threats that these inevitably interrelated concepts present. This analysis will be conducted through conceptual explanations, case studies, and evaluations within the scope of a general literature review.
Keywords: Intelligence, Open source ıntelligence, Big data
JEL Codes: H56, O33, Z18

---

* Bu çalışma; 12-15 Eylül 2024 tarihleri arasında Üsküp'te düzenlenen "Kayfor Balkanlar: 25. Uluslararası Kamu Yönetimi Forumu" kapsamında bildirisi 'Bıg Datanın İstihbarat Üzerindeki Etkisi: Açık Kaynak İstihbaratının Artan Önemi, Fırsatlar Ve Tehditler' başlığıyla yapılan sunumun genişletilmiş halidir.

[1] Doç. Dr., Ankara Hacı Bayram Veli Üni. İktisadi ve İdari Bilimler Fak., ORCID: 0000-0003-0190-512X
[2] Doktora Öğrencisi, Ankara Hacı Bayram Veli Üni. İktisadi ve İdari Bilimler Fak., ORCID: 0009-0001-6103-4576
* **Sorumlu Yazar** (Corresponding Author): goksel.batuhanyasar@hbv.edu.tr
Başvuru Tarihi (Received): 01.11.2025 **Kabul Tarihi** (Accepted): 29.04.2026

Giriş

İstihbarat kavramının İngilizce karşılığı olan "Intelligence" Türkçe olarak akıl, zekâ, bilgi ve istihbarat anlamlarına denk düşmektedir. İstihbari faaliyet olarak nitelendirilebilecek ilk faaliyetlerin medeniyet öncesi dönemlerde insanların avcılık amacıyla iz sürme veya insan faktörüne karşı düşman olarak algılanabilecek her türlü 'şey'e karşın yapılan gözlem ve takiplerden ibaret olduğu söylenebilmektedir. İstihbarat disiplininin özellikle II. Dünya Savaşı'nın ardından hızla gelişen teknolojik araç ve imkânlar sayesinde önemli değişimler içerisine girdiği gözlemlenmektedir. II. Dünya Savaşı esnasında istihbarat toplama yöntemlerinin temelini oluşturan insan istihbaratının yanı sıra sinyal ve görüntü istihbaratlarının çağın teknolojik imkânları uyarınca kullanıldığının bilinmesi, savaş sonrası dönemde teknoloji tabanlı gelişimin önünü bir hayli açmıştır. Günümüz reel politiği, küresel anlamda ülkelerin güç savaşlarının zirveye çıktığı bir dönemdir. Önceden bilebilme yeteneği olarak nitelendirebileceğimiz istihbari bilgilerin ve bu bilgileri yönlendirebilme yeteneği olan istihbarat çalışmalarının önemleri, devletler arası güç uygulayabilme iddiaları açısından temel yapı taşları haline dönüşmüştür.

Açık Kaynak İstihbaratı, belirli istihbari amaçları gerçekleştirebilmek için kamu kullanımına açık bilgi veya verilerin; elde etme, işlemden geçirme, analiz etme ve sonuçlandırma gibi süreçlerden geçirilmesi sonucunda elde edilen istihbari nitelikte araştırma ve çıktılardan oluşmaktadır. Açık kaynak bilgisi ise oluşturucu kaynağı tarafından herhangi bir gizleme veya karartma yapılmayan, gizlenmek istenilse dahi gizlenemeyen türde bilgileri tarif etmektedir. Bu kapsamda açık kaynak bilgisi, kitle iletişim araçları aracılığıyla kolay bir biçimde elde edilebilecek türde bilgilerden oluşmaktadır. Elde edilen bu bilgilerin istihbarat disiplini kapsamında kullanılabilecek değerli bilgiler olabilmesi yalnızca bu bilgilerin elde edilmesine bağlı değildir. İstihbari bilgiye dönüştürülmesi kapsamında açık kaynaklı bilgilerin gerekli uzmanlaşmış ilgililer aracılığıyla işlenmesi ve amacına uygun kullanılması bakımından analiz edilmesi gerekmektedir. Enformasyon çağı içerisinde yüksek teknolojik imkânlara sahip olduğumuz günümüzde veri ve bilgilerin hacminin hatırı sayılır büyüklükte olduğu ve asıl önemli noktanın bilginin niteliksel ve niceliksel ayrımının yapılabilmesinde yattığı söylenebilmektedir.

Bu doğrultuda Türkçe karşılığı Büyük Veri olarak ifade edilen "Big Data" kavramını bilmek, çağın gereklilikleri doğrultusunda kritik düzeyde bir önemdedir. Ham ve işlenmemiş; kaydedilmiş, depolanmış ve sınıflandırılmış fakat organize edilmemiş ve kişisel kullanımlar için kullandığımız bilgisayarlar aracılığıyla analiz edemeyeceğimiz türden verileri tanımlamayan Big Data kavramı, kullanıcısını doğrudan etkilemeyen bilgilerin karşılığı olarak tanımlanmaktadır. Büyük hacimli ve çeşitli veri sınıflarının analiz edilmesine olanak tanıyan Big Data, karar verme süreçleri esnasında önemli bir role bürünen kıymetli bir araç olarak göze çarpmaktadır. Kullanıldığı alanda iş süreçlerini maksimize edebilmeyi, hedeflenen stratejilere yönelik planlar oluşturabilmeyi ve diğer yandan riskleri henüz yaklaşmadan tespit edebilmeyi ve ileriye dönük yenilikçi keşifler gerçekleştirebilmeyi mümkün kılan Big Data, istihbarat teşkilatlarına geniş perspektifte veri toplayabilme ve bu verileri analiz edebilme imkânları sunmaktadır. İstihbarat teşkilatlarına önemli kazanımlar sağlayabilme potansiyelinin aksine Big Data, bir tehdit unsuru olarak da ön plana çıkmaktadır. Dezenformasyona uğratılmış kasti bilgiler, sahte haberler ve manipüle edilmiş bilgiler; 'yanlış girdi sonucu yanlış çıktı' bağlamında istihbarat analiz süreçlerini olumsuz doğrultuda etkileyebilme potansiyeli olan ciddi meselelerdir.

Bu çalışmada; Big Data ve Açık Kaynak İstihbaratı alanlarının kesişim noktaları ve birbirleriyle olan veya olması muhtemel ilişkileri ve bu ilişkilerin önemi, ortaya çıkan ilişkiden ötürü istihbarat teşkilatlarının elde ettiği faydalar incelenecektir. Ayrıca, teknolojinin ortaya çıkarttığı bu kavramların güvenlik sektörüne ve sosyal hayata etkileri üzerinde durulacaktır. Son olarak, mevcut zorluklar ve gelecekteki yönelimler hakkında bir değerlendirme sunulacaktır.

1. Big Data

Big data kavramı klasik veri işleme yöntemleriyle yönetilemeyen ve işlenemeyen kompleks ve çok büyük miktarda verinin ifade edilmesi için kullanılmaktadır. Büyük veri kavramı, bir tek sunucu kaynağına yerleştirilemeyecek ölçekte büyük, klasik sınıflandırma biçimindeki veri tabanlarına göre yapılandırılmamış veya bilinen veri ambarlarına uygun olmayan sürekli akan veriler olarak tanımlanabilmektedir (Kızmaz, 2021, s. 19). Büyük veri kavramı; bilginin tespit edilmesini, tutulmasını, ilgili işlemler doğrultusunda yönetilmesini ve kapsamına dahil ettiği bilginin analizini gelişmiş teknik ve teknolojiler kullanarak sağlamasının yanı sıra bu işlemleri yüksek hacimli ve karmaşık verileri anlamlandırmak üzere yürütülen sürecin de adlandırılmasında kullanılmaktadır (Gandomi ve Haider, 2015, s. 138). Sosyal medya gönderileri, web sitesi çerezleri, GSM operatörlerinin tuttuğu internet erişim, konuşma, mesajlaşma ve konum verileri ile bloglar, sensörler ve akıllı cihaz verileri gibi birçok farklı kaynaktan gelen verilerin anlamlı hale getirilmesine ve işlenmesine olanak sağlayan teknolojileri içermektedir (Doğan ve Aslantekin, 2016, s. 15-36).

Big Data muğlak bir kavram olduğu için tanımlamalarda genelde bileşenleri yani karakteristik özellikleri kullanılmaktadır. "5V" olarak da ifade edilen bu bileşenler; Hız (Velocity), Hacim (Volume), Doğruluk (Veracity), Değer (Value) ve Çeşitlilik (Variety) olarak tanımlanmaktadır (Gandomi ve Haider, 2015, s. 138).

Şekil 1: *Büyük Verinin Bileşenleri*

Kaynak: (Marr, 2014)

Büyük veri, ölçülemeyecek derecede büyük olmasıyla karakterize edilmektedir. Klasik veri sistemleri sınırlı bir kapasitede veriyi işleyebilirken, büyük veri sistemleri petabayt[3] (PB) hatta zettabayt[4] (ZB) ölçeğinde veri işleyebilmektedir. IP (Internet Protocol) temelli cihazlar kaynaklı verilerle beslenen büyük verinin artış hızı için ise en çarpıcı örneklerden biri insanlık tarihinden 2003 yılına dek üretilmiş olan toplam veri miktarının, günümüz bilgi üretimi içerisinde yalnızca iki gün içerisinde üretiliyor olmasıdır (Aktan, 2018, s. 5). İkinci bileşen olan doğruluk, büyük veriyi oluşturan kaynakların güvenilirliği ile ilgilidir. Dijital ortamda veri hacminin çok yüksek olması, bu verilerin kontrolünü zorlaştırmaktadır. Kontrol edilemeyen veri, bilgiye dönüştürülemeyecek ve veri raporları içerisinde yer alan güvenlik problemleri de ekonomi, bilimsel araştırmalar ve stratejik planlamalar kapsamında pek çok probleme neden olabilmektedir. Bu sorunların ortaya çıkmaması için verilerin ulaşılması planlanan hedefler perspektifinde ilişkisel veri tabanlarında (Relational Databases) sınıflandırılması ve yapılandırılmış verilerden yola

[3] 1 PB = 1.048.576 Gigabayt (GB) (Komprise, 2025).
[4] 1 ZB = 1.099.511.627.776 Gigabayt (GB) (Seolog, 2025).

çıkarak çeşitli araştırmalar ve analizler yürütülmektedir (Debattista vd., 2015, s. 92).

Büyük verinin en önemli bileşenlerinden biri olan değer kavramı, verinin analize tabi tutularak anlam kazanmasını belirtmek için kullanılmaktadır. Çünkü verinin hacmi ve doğruluğu önemli olsa da işlenip bilgiye dönmesi önemlidir. Kullanıcıların arama motorlarında yaptığı sorgular, alışveriş alışkanlıkları ve sosyal medya etkileşimleri analiz edilerek kişiselleştirilmiş önerilerle geliştirilen stratejilerle büyük veri analitiği, yalnızca verileri toplamakla kalmayıp, doğru değerlendirme ve uygulamalarla katma değer yaratmayı amaçlamaktadır (Suvay Eker, 2022, s. 118).

Big Datanın diğer bir bileşeni olan çeşitlilik (Variety), verinin heterojen yapısı ile ilgilidir ve analizinde zorluklarla karşılaşılmaktadır (Gandomi ve Haider, 2015, s. 138). Sensörler, IP temelli cihazlar, sosyal medya gibi pek çok kaynaktan elde edilen metin, ses, verinin heterojenliği gibi farklı türlerden oluşmasından kaynaklanabileceği gibi verinin ham ya da yapılandırılmış olma derecesinden de kaynaklanabilmektedir. Video ve resim gibi farklı veri türlerinin işlenmesi zaman alırken, standart bir veri formatına dönüştürülmesi de güçlük yaratmaktadır (Jin vd., 2015, s. 59).

Hız (Velocity), büyük verinin üretim, analiz ve karar süreçlerine dahil edilmesi işlemlerinin gerçek zamanlı olmasını ifade etmektedir (Gandomi ve Haider, 2015, s. 138). Hız, özellikle kritik karar süreçlerinde önem taşırken, çeşitlilik bilginin işleme sürecini zorlaştırabilmektedir. Bu nedenle, büyük veri analizlerinde hem hız hem de çeşitliliğin dengeli yönetilmesi gerekmektedir.

Büyük Veri, kurumların çeşitli kaynaklardan veri toplamasını, depolamasını ve analiz etmesine olanak tanımış, bu özelliğiyle istihbarat departmanlarında da kullanılmaya başlanmıştır. Buradan elde edilen verilerle eksik bilgilerin tamamlanması, olası risklerin tespiti ve öngörüler oluşturmak mümkün olmuştur (Kaisler vd., 2013, s. 999). Bu durum, istihbarat toplama ve karar alma süreçlerinde köklü değişimlere yol açmıştır.

2. Açık Kaynak İstihbaratı (OSINT)

OSINT, belirli istihbarat ihtiyaçlarını karşılamak maksadıyla açık kaynak bilgilerinin toplanması ve toplanan bu bilgilerin istihbarat üretimi maksadıyla istihbarat analizcisine doğru ve etkin bir biçimde sağlanabilmesi süreçlerini içeren istihbarat biçimi olarak tanımlanmaktadır (MİT, 2024). OSINT faaliyetleri için taranacak olan açık kaynak bilgileri ise halkın erişimine açık, potansiyel istihbarat değerine sahip, güvenilir ve elde edilmesi için fazla gayret gerektirmeyecek bilgi çeşidi olarak sınıflandırılmaktadır (CIA FOIA, 2000).

OSINT çeşitli koşul farklılıklarından ötürü diğer istihbarat toplama biçimlerinden farklılıklar göstermektedir (Bukatyi vd., 2023, s. 2):

- OSINT kamuya açık ve yasal olarak elde edilebilen bilgilere odaklanırken diğer istihbarat toplama biçimleri çoğunlukla gizli veya sınıflandırılmış kaynakları içermektedir.
- OSINT sosyal medya, haber makaleleri, kamu kayıtları ve hükümet raporları dahil olmak üzere çeşitli kaynakları kullanır. Buna karşılık diğer istihbarat toplama biçimleri belirli bir kaynak türüne odaklanmaktadır.
- OSINT genellikle büyük hacimli verilerden içgörü ve istihbarat elde etmek için makine öğrenimi ve doğal dil işleme gibi gelişmiş analitik tekniklerin kullanılmasını içerir. Diğer istihbarat toplama biçimleri daha çok insan analizine ve yorumuna dayanmaktadır.

OSINT oluşturma süreci ise öncelikle açık kaynakların niteliğine ve çeşitliliğine daha sonra kaynakların bulunduğu ortamın güvenirliğine ve son olarak da açık kaynaklı veri/bilgiyi istihbarata dönüştürme konusundaki son teknoloji ürünün teknik kabiliyetine ve bu ürünü kullanacak olan istihbarat analistinin kazanımlarına bağlıdır. Bu üç faktör kaynakların doğrulanması ve güvenilirliğinin değerlendirilme şeklini doğrudan etkiler ve aynı zamanda

içeriğin doğruluğunun analiz şeklini de biçimlendirmektedir. Doğrulama, güvenilirlik ve gerçeklik değerlendirmeleri OSINT ürününün daha sonraki analizinde önemli bir rol oynamakta ve sonuç olarak karar alma mekanizmasını birinci dereceden etkilemektedir. Bu nedenle, kaynak doğrulama, güvenilirlik ve doğruluğa ilişkin mevcut zorlukların analizi aynı zamanda nihai OSINT ürünleri ve bunların çıktılarına ilişkin mevcut zorlukların da analizi olarak değerlendirilmelidir (Bordes Perez, 2023, s. 9). Temel OSINT faaliyet süreci beş adımla açıklanabilmektedir (Pastor-Galindo vd., 2020, s. 6):

1. Kaynağın tanımlanması; bilgi kaynağının nerede olduğunun saptanması.
2. Bilginin toplanması; bilgi kaynaklarından ihtiyacı duyulan doğru bilginin alınması.
3. Verilerin işlenmesi; toplanan verilerden hangilerinin işe yarar ve kesin bilgiler olduğunun saptanması.
4. Analiz; işlenen verilerin başka kaynaklardan alınan diğer veri parçaları ile birleştirilip anlamlı bir bütün haline getirilmesi.
5. Rapor; tüm bulguların kaydedildiği nihai bir raporun oluşturulması ve rapor aracılığıyla gerekli yerlere bilgi aktarımının yapılması.

2.1. Açık Kaynak İstihbaratının Tarihçesi

OSINT, insanın tarihte var olduğu günden bugüne değin devletlerin birbirleriyle olan rekabetleri içerisinde kendisine bir yer bulmuştur. Öyle ki Antik Çağ'da üretilen Mısır hiyeroglifleri ve papirüs örnekleri, içeriği ile bizlere o dönemde yaşanan köle ticareti faaliyetleri içerisindeki sadakatsiz ve eylemleri sekteye uğratan unsurları raporlayan ajanların var olduğunu göstermektedir. Aynı zamanda Mezopotamya'da yazılan Asurilere ait metinler de yabancı ülkelere yönelik işgal ve fetih girişimlerinin, herhangi bir eyleme geçilmeden, keşif amacı içerisinde, fethedilmesi düşünülen topraklara ajanlar gönderildiğini ve bunların raporlar halinde dönemin krallarına sunulduğunu kanıtlamaktadır (Kahana ve Suawed, 2020, s. 33).

OSINT kavramının literatürde kendisine aktif bir biçimde yer bulması ise alanın araştırmacıları tarafından 'William Donovan' ismine dayandırılmaktadır. Donovan, II. Dünya Savaşı sırasında, daha sonra ABD Dış İstihbarat Servisi olan Merkezi İstihbarat Teşkilatı'nın (CIA) selefi haline gelecek olan 'Stratejik Hizmetler Ofisi'ni kurmuştur. Bu yapılanma, dönemi içerisinde sadece halka açık bilgilerin analizi ile uğraşmak üzere görevlendirilmiştir. Bu birim savaş dönemi içerisinde sadece dünyanın dört bir yanında farklı dillerde yayın yapan gazeteler, dergiler ve radyo yayınlarını toplayıp analiz etmekle uğraşmıştır (Böhm ve Lolagar, 2021, s. 318).

Lakin yukarıda da ifade edildiği üzere OSINT faaliyetlerini bir isim ve bir dönemle kısıtlamak mümkün değildir. Açık kaynakların herkes tarafından kullanılabilir ve değerlendirilebilir bir halde olması, insanın elinde bulundurduğu imkânlarla paralel olarak fiziki kanıtları değerlendirerek bilgi sahibi olma isteğini gerçekleştirmiştir. Bu durum 20. yüzyıl ve öncesinde fiziki imkânlarla kısıtlanmışken ilerleyen yıllarda işin içerisine kümülatif bir yığılma ile teknoloji meselesi girmiştir.

Fiziki açık kaynak bilgilerinin elde edilmesi ve yorumlanmasının başka disiplinlerin de analiz süreçlerine katılmasıyla gerçekleştiği görülebilmektedir. Örneğin; II. Dünya Savaşı yıllarında Rus istatistikçiler matematik bilimi ile istihbarat bilimini harmanlayarak, Nazi savunma sanayisi unsurlarının bir ay içerisinde kaç adet tank üretebildiklerini tespit edebilecek bir analiz yöntemi geliştirmişlerdir. İstatistikçiler ellerinde var olan bilgilerle birlikte sahadan bizzat raporlanan bilgileri derleyerek çok işlevsel ve hata payı sıfıra yakın olan bir formül oluşturmuşlardır. Bu formül sayesinde ortaya çıkarttıkları sonuçlar gerçek tank sayılarına çok yakın sayılar elde etmiş ve Rus tarafının, Nazi kısmının askeri hareketlerine önlem alabilmesine yönelik farklı hamleler oluşturabilmesine olanak tanımıştır. Bahsedilen formül şu akışta işlemektedir:

"N = M + M/K – 1"

('N' tank sayısı, 'M' elde edilen en büyük seri numarası, 'K' elde edilen toplam seri numarası sayısı)

Nazi kuvvetlerinin 'Panther' ismini verdikleri tanklara açık erişim dolayısıyla tespit edilebilecek biçimde seri numaraları eklemesi, literatüre "Alman Tank Sorunu" olarak geçmiştir. Bu durum savunma sanayisi üretiminin açık ve erişilebilir bir veri haline gelmesine sebep olması dolayısıyla önem arz etmektedir (Clark vd., 2021, s. 20). Bu oluşan açık kaynak bilgisini Rus istatistikçilerin geliştirdiği formül ile analiz eden Rus istihbaratçılar, OSINT kavramının literatürde yaygınlaşmadığı zamanlarda bu faaliyetin tanımına birebir uygun bir istihbari operasyon imkânı bulmuşlardır.

2.2. Açık Kaynak İstihbaratının Artan Önemi

OSINT, 21. yüzyıl bilgi operasyonlarında başlıca yeni bir güç olarak görülmektedir. OSINT ülkeler için 'yeni' bir mefhum değildir çünkü uluslar ve kuruluşlar doğrudan gözlemin, yapılandırılmış okumanın ve bilgi hizmetlerinin yasal bir biçimde analiz edilebilmesinin değerini her zaman anlamışlardır. OSINT ile ilgili 21. yüzyılın başlarında yeni olan gelişme, dünyanın geçirdiği değişim olmuştur. Bu değişim üç farklı eğilim ile açıklanabilmektedir; bunlardan ilki, açık bilginin yayılması ve paylaşılması için bir araç olarak internetin önemli bir derecede yaygınlaşması; ikincisi, yayınlanmış bilginin kümülatif biçimde birikerek dur durak bilmeden oluşturduğu 'bilgi patlaması' ve sonuncusu da istihbarat alanında bu birikim sebebiyle bazı tekniklerin ve alanların değişimi yakalayamamış olmasıdır (NATO, 2001, s. 3).

Enformatik çağın gelişiminin son 'modern' araçlarını kullanabilmemize olanak sağlayan günümüz gelişim süreci içerisinde politik, sosyal, ekonomik ve kültürel alanlar başta olmak üzere hemen her alanda önemli fırsatlar ve tehditler bir arada bulunmaktadır. Bu doğrultuda devletler, güvenlik ve istihbarat disiplini açısından değerlendirildiğinde, küreselleşmenin kontrol edilmesinin imkânının olmadığı ve enformatik gelişimin hızı ve hacmi göz önünde bulundurulduğunda; uluslararası aktörlerin çeşitlerinin giderek artması ve küresel belirsizlik ikliminin yoğunlaşması gibi ana çıktılardan dolayı görece daha az öngörülebilir bir geleceğe adım atmaktadırlar. Bu karışık global ortamda istihbarat alanında istikrarlı ve kalıcı stratejik avantaj kazanabilmenin ana unsuru, karmaşık ve birbiriyle bağıntılı zorlukları hızlı ve kesinliğinden emin bir şekilde analiz etme ve analiz çıktılarına yönelik katma değer ortaya koyabilme yeteneği olarak öne çıkmaktadır. Özellikle siber alandaki gelişmeler, istihbarat toplama yöntemlerinden bu yöntemler aracılığıyla toplanan bilgileri işlemeye ve işlenen bilgiler doğrultusunda yapılacak olan gizli operasyonların yürütülmesine uzanan geniş bir perspektifte istihbaratın çoğu iş alanında önemli bir değişim gerçekleştirmiştir. Örneğin Soğuk Savaş yıllarında ABD'nin istihbari faaliyetlerini gerçekleştirebilmek üzere elde etmek zorunda olduğu istihbari bilgilerin %80'i gizli, %20'si açık kaynaklardan elde edilebilecek durumdaki bilgilerden oluşurken, Soğuk Savaş sonrası dünyada bu durum tam tersine bir dönüşüm geçirmiştir (Taban ve Aydilek, 2022, s. 40).

Bu dönüşüm dolayısıyla istihbarat teşkilatları da kendilerini yenileme ve değişen küresel gerekliliklere ayak uydurabilme yolunda girişimlere başvurmuşlardır. Öyle ki istihbarat teşkilatları, 21. yüzyılın başlarında daha fazla OSINT çalışması yürütebilmek ve yürütülen çalışmaların niteliklerini arttırabilmek amaçlarıyla örgütlenmeleri içerisinde 'Açık Kaynak İstihbaratı Daireleri' kurmuştur. Bu doğrultuda CIA, 2005 yılında 'Open Source Center[5]'ı faaliyete geçirmiştir (Erol, 2022, s. 28). Rusya ve Çin gibi ülkeler ise OSINT faaliyetleri yürütme amacıyla istihbarat teşkilatlarında halihazırda birer birim olarak bulunan 'Askeri İstihbarat' kanatlarını kullanmaktadır. Rusya'da askeri istihbarat alanında faaliyet gösteren 'GRU[6]' (Pringle, 2015, s.

[5] Bu birimin günümüzdeki adı 'National Open Source-Intelligence Agency' olarak geçmektedir.

[6] "GRU"; 'Glavnoye Razvedyvatel'noye Upravleniye', Rusya Silahlı Kuvvetler Genelkurmayı'na bağlı askeri

364) ve Çin'de yine aynı alanda faaliyet gösteren 'PLA[7]'; 2007 yılında kendi iç dinamiklerini değiştirme ve faaliyet alanlarını genişletme açısından bir yenilenmeye gitmiş; OSINT odaklı istihbarat toplama faaliyetlerine başlamıştır.

OSINT eğilimlerine verilen önem kapalı toplumları araştırmada da kendisini gösterebilme potansiyeline sahiptir. Kapalı sınırlara nüfuz etmek, açık toplumların bilgi kaynaklarına erişmekten daha zor durumdadır. OSINT açık kaynaklardan elde edilen istihbarat olduğundan, daha az sayıda kaynak, sınırlı sayıda gözlemciyle daha geniş bir kapsama alanının mümkün olduğu anlamına gelmektedir. Örneğin dünyanın en otoriter hükümetlerinden birisine sahip olan 'Kore Demokratik Halk Cumhuriyeti (KDHC)' düşünüldüğünün aksine nispeten kolay bir OSINT hedefidir. Kuzey Kore sınırları içerisinde yayın yapan sadece iki günlük gazete vardır: "Nodong Sin-mun" ve "Minju Choson". Bu gazeteler sırasıyla iktidar partisi ve hükümetin gazeteleridir. Başkentte 'hiçbir muhalif düşünce gazetesi' ve 'rakip görüş sunacak veya yanlışları ifşa edecek canlı bir taşra medyası' yoktur (Mercado, 2004, s. 49). Bu durum, 'hükümetin kendi eliyle bilgi akışını bozmadığı ihtimali ele alındığında' doğru ve değişmemiş bilginin doğrudan birinci kaynaktan elde edileceğinin işaretini vermektedir.

Açık Kaynak İstihbaratı Dairelerinin ilgili istihbarat teşkilatları içerisinde sabırlı ve zamanını bekleyen, etkili operasyonlara imza attığı bilinmektedir. Örneğin, Mayıs 2015'te bir IŞİD üyesi bir sosyal medya platformunda kendi görselini içeren 'selfie' yayınlamıştır. Fotoğraf içeriği ve açısında da IŞİD'in karargah binası gibi özel bilgi içerecek detayları göstermemeye dikkat etmiştir. Fotoğraf içeriği, fotoğrafın çekildiği yerdeki binanın yükseklik ve boylam bilgisini doğrudan ortaya çıkarmasa da, fotoğrafın meta verilerinin CIA tarafından önceden elde edilmiş olan büyük verilerle birlikte analizine göre, binanın yeri hızlı bir biçimde belirlenmiş ve hava kuvvetleri tespit edilen lokasyonu yok etmek üzere üç füze ateşlemiştir. Sosyal ağda bir paylaşımın yayınlanmasından 3 füzenin hedefi vurmasına kadar olan tüm süreç 24 saatten daha az bir vakit almıştır (Wang, 2020, s. 8). Bu örnekte aktardığımız OSINT temelli operasyonların sayısının yüksek rakamlarda olduğu açık kaynakların gelişimine odaklandığımızda ortaya çıkacaktır. Öyle ki 1995 yılında açık kaynak olarak sınıflandırılabilecek yayınlar (televizyon haberleri, radyo yayınları, gazeteler, akademik materyaller) günde ortalama bir sayıyla 20.000 kelimeyi içerisinde barındırmaktaydı. Fakat günümüzde bu sayı sosyal medya ve diğer tüm basılı olan/olmayan kaynaklarla birleştiğinde sınırsız bir veri olarak önümüzde "yığılmaktadır". 2020 yılında "IoT[8]" aygıtlarının sayısı küresel bağlamda 20,1 milyarı bulmuştur (Şen ve Yurtoğlu, 2020, s. 41). Bu sayının güncel nüfus artışı ve teknolojik gelişmelerin ilerleyişi göz önünde bulundurulduğunda 2030 yılı itibariyle 32,1 milyarı aşacağı tahmin edilmektedir (Statista, 2024). Elimizde bulunan ve gelecekte olması ön görülen rakamlar, OSINT faaliyeti yürütebilmek adına ilgili istihbarat teşkilatına sınırsız bir kaynak anlamına gelmektedir. Açık kaynak bilgisinin önlenemez bir biçimde artacağının habercisi bu rakamlar, bu artış içerisinde etkili ve yerinde olarak değerlendirilebilecek OSINT faaliyetlerinin gelecek yıllar içerisinde öneminin daha da fazla olacağının habercisi niteliğindedir.

3. Big Data ve Açık Kaynak İstihbaratı İlişkisi

Veri günümüzde, anlamlı veya anlamsız bilgiler yığınıdır. Veri, hiçbir işleme tabi tutulmadan, çeşitli fiziki veya sanal yöntemler aracılığıyla ortamdan elde edilen her türlü değer olarak tanımlanmaktadır. Bu bağlamda, istihbarat üretimi amacıyla elde edilen verilerin her vakit anlamlı bir bütünlük veya tamamlayıcı ve açıklayıcı bir bilgiye sahip olmak zorunda olmadığı

istihbarat teşkilatı.

[7] "PLA"; 'People's Liberation Army', Çin Komünist Partisi ve Çin Halk Cumhuriyeti'nin resmi ordusu. Çin istihbarat yapılanması 'Çin Halk Kurtuluş Ordusu' olarak isimlendirilen bu ordu teşkilatlanmasının içerisinde faaliyet göstermektedir.

[8] "IoT"; 'Internet of Things', Nesnelerin İnterneti.

anlaşılmaktadır. Dağınık biçimde elde edilen veya toparlanan verilerin anlamlandırılmış bir forma dönüştürülerek, işe yararlılıklarının artırılması ve anlamlı bu biçimin doğru bir şekilde yorumlanması gerekmektedir (Kuzucuoğlu ve Şeşen, 2021, s. 94).

Yeni nesil internet teknolojilerindeki gelişim aracılığıyla insanlar, yaklaşık "500 Mbits/sn" ve daha da üzerinde hızları kullanabilmeye imkân tanıyacak teknik bir altyapıya sahiptir[9]. Bu hız günümüzde bulunan bilgisayar ağlarındaki hızın çok daha fazla süratle, taşıma kapasitesinin arttığını açıklamaktadır. Sürekli gelişen bir bilgisayar ağı ortamının varlığı, dağınık verileri analiz etmek ve daha gelişmiş çeşitli analiz algoritmalarının oluşturulabileceği anlamına gelmektedir (Arıkan, 2019, s. 28).

Bu bağlamda 'Big Data' olgusu, istihbarat alanı gibi bilgi odaklı faaliyetler için önemli fırsatlar ve zorluklar sunmaktadır. Örneğin, tartışmasız en çok bilinen ve kullanılan 'Büyük Veri' sınıfı, kesinlikle 'insanlar ve toplum hakkında şimdiye kadar sahip olduğumuz en büyük bilgi bütünü' olan sosyal medyadır (Eldridge vd., 2018, s. 394). Birinci dereceden ve en basitinden etki alanı olarak sosyal medya; toplum içerisinde ulusal veya uluslararası bir olay ile alakalı kendi 'ekolojisi' içerisindeki kullanıcıların yorumlarının hacmindeki önemli artışlar, kamuoyundaki önemli değişimlere işaret etmektedir. O dönemde değer ölçütlerinin daha yakından incelenmesi, bu değişimin toplumsal bakış bağlamında olumlu veya olumsuz bir sonuç ortaya çıkaracağı kapsamında değerlendirilip, karar alıcılara hareket alanlarının neler olduğunun ışığını tutabilme potansiyeli taşımaktadır (Moe ve Schweidel, 2014, s. 15). Lakin sosyal medya doğal yapısı açısından görece manipülasyona ve dezenformasyona çok açık bir alan olarak değerlendirilmektedir. Sosyal medyadan toplanan açık kaynak bilgisinin analiz edilmesinde doğru ve yararlı bilgilerin yanlış ve kasıtlı gönderilerden ayırt edilebilmesi çok önemlidir. Bir risk kapsamında değerlendirildiğinde; kamuya açık erişime sahip olan devlet raporlarından ve internetin sunduğu açık kaynaklardan elde edilen bir bilginin, ana kaynağı olan ve 'rakip' olarak sınıflandırılabilecek kimseler -devletler, şahıslar, gizli servisler vb.- tarafından kasıtlı olarak yayınlanan yanıltıcı ve yanlış bilgiler içerebilme ihtimali bulunmaktadır. Bu bilgiler üzerinde incelemeler gerçekleştiren istihbarat analistlerini yanıltmak ve istihbari bilgi üretim sürecini başarısızlığa uğratmak gibi amaçları edinen bu dezenformasyon operasyonlarına kapsamlı ve analitik perspektifte ve sorgulayıcı bir şüphe temelinde yaklaşmak gerekmektedir.

3.1. Açık Kaynak İstihbaratı Faaliyetlerinde Kullanılan Big Data Analiz Araçları

OSINT çalışmalarına kaynak olarak çağımızda hatırı sayılır büyüklükte yer kaplayan sosyal medya ve çevrimiçi sanal platformların 'doğru' okunabildiğinde ne kadar stratejik olabileceğine örnek bir analiz süreci olarak "Olay Çıkarma" kavramı ön plana çıkmaktadır. Olay çıkarma kavramının amacı; "Kimin kime, nerede, ne zaman ve hangi sonuçlarla ne yaptığını" açıklamak için metinsel açıklamalardan meta verileri tanımlamaktır. Olay çıkarmanın içeriğini oluşturan metinsel verilerden kastımız da 'dünya üzerinde üstüne haber yapılmaya konu olmuş' her olaydır. Bu bağlamda yapılan ilk çalışma, "Europe Media Monitor (EMM)[10]", derlenen haber makalelerinden otomatik olarak kaydedilen şiddet içeren olayları tasniflemek için kurgulanmıştır. Bu çalışmayı bir örnekle açıklamak, aslında neyin başarılmaya çalışıldığını en iyi şekilde ifade edecektir:

[9] Dünyada şu zamana kadar ulaşılabilen en yüksek internet hızı "1.02 Petabit/sn"dir. Dünya rekoru olarak nitelenen bu hız, 'Japonya Ulusal Bilgi ve İletişim Teknolojileri Enstitüsü'ndeki araştırmacılar tarafından elde edilmiştir. Bu hız sayesinde saniyede '127.500 GB' veri aktarılabilmektedir.

[10] "Europe Media Monitor (EMM)", dünya çapındaki çevrimiçi medyanın aktardığı güncel haberlerin kolayca görülmesini, keşfedilmesini, anlaşılmasını ve analiz edilebilmesini sağlamak üzere geliştirilmiş bir sistemdir. 70'in üzerinde dilde binlerce haber kaynağını izleyen sistem; haberlerde nelerin aktarıldığını, olayların nerede gerçekleştiğini, kimlerin olaya karıştığını ve ne söylediklerini otomatik olarak belirlemek için gelişmiş bilgi sınıflandırma ve çıkarma tekniklerini kullanmaktadır. Şu anda dünyada rapor edilenler hakkında benzersiz ve bağımsız bir bakış açısını kolay bir biçimde kullanıcılarına sağlamaktadır.

"İntihar patlaması güvenlik firması Kandahar'ı vurdu, Afganistan, 11 Eylül 2007." Başlıklı haberdeki içerik; "Bir intihar bombacısı ABD güvenlik firmasının konvoyunu vurarak 3 kişiyi öldürdü" olarak medyada yer almıştır. EMM sistemi, bu metinden aşağıdaki öğeleri otomatik bir biçimde çıkartmaktadır:

- Saldırgan: Bir İntihar Bombacısı
- Enstrüman: Bomba
- Yöntem: İntihar Bombası
- Hedef: ABD Güvenlik Firması
- Zaman: 11.09.2007
- Yer: Kandahar, Afganistan
- Hasar: 3 Ölü

EMM bu işlemi 'Nexus' adı verilen olay çıkarma sistemini uygulayarak tamamlamıştır. Buradaki temel fikir, her kümenin tek bir olayı temsil etmesidir. Nexus bu işlemi yaparken, makine öğreniminden türetilen sığ bir ayrıştırıcı ve desen eşleştirmeyi kullanmaktadır. Kümedeki her adım, olay hakkında mümkün olduğunca fazla ayrıntı çıkarmak için analiz edilmektedir. Aynı prosedür şu anda 'Gerçek Zamanlı' kümelere uygulanmakta ve böylece canlı bir durum haritası arayüzü oluşturulmaktadır. Bu arayüz günün her saati güncellenmekte ve yeni şiddet olayları meydana geldikçe bu olayları otomatik olarak tespit etmektedir. Her olay, bir olay açıklamasıyla sınıflandırılmakta ve ek bir mekânsal hiyerarşi mantığı uygulanarak makalelerde en çok bahsedilen yere coğrafi olarak konumlandırılmaktadır. Etkinlik açıklamasında kullanılan unsurların formülü ise şu akışta işlemektedir:

- *Olay {Tarih, Yer (Enlem, Boylam), Olay Türü, Öldürülen Sayı, Yaralı Sayısı, Kaçırılan Sayı, Failler, Kurbanlar, Silahlar}.*

Bu sistem sayesinde şiddet olaylarının uzun süreler boyunca kaydedilmesi, bir krizin sistematik bir şekilde izlenebilmesine ve karar vericilerin, durumun kötüleşip kötüleşmediğini ölçmesine yardımcı olabilme potansiyeline sahiptir (Best, 2008, s. 323).

OSINT çalışmalarında Big Data anlamlandırılma çabalarında 'makine öğrenmesi metotları' da kullanılabilmektedir. Şöyle ki, "Intelligence Advanced Research Projects Activity (IARPA)[11]" tarafından üretilen "TrojAI" projesinde makine öğrenmesi teknikleri işlenerek siber istihbarat üzerine analizler yapılmıştır. Açık kaynak istihbaratında makine öğrenmesi metotları kullanılarak yapılacak projelerin bir nevi öncüsü durumundadır. Sistemin işleyişi, siber saldırılara neden olan 'Truva Atları'nın erken tespit edilmesi için makine öğrenmesi türlerinden pekiştirmeli öğrenme tekniğinin uygulanarak bir çıktı üretmesiyle gerçekleşmektedir (Yurtsever, 2024, s. 113).

Diğer sistemleri maddeler halinde sıralayacak olursak:

- "OwlSight"; belirlenen çeşitli istihbarat kaynaklarından büyük hacimlerde veri çekip bunların analizini otomatik bir biçimde gerçekleştiren bir sistemdir. Bu sistem günlük olarak 107'den fazla kötü amaçlı yazılımın ortaya çıkış zamanını, bu yazılımların yayılma hızını ve kapsamında olduğu aile sınıfını belirleyen ve belirlediği bu verileri görselleştirerek düşük yanlış alarm oranına sahip gerçek zamanlı bir uyarı sistemi geliştirmektedir.
- "CyberTwitter"; siber güvenlik alanını ilgilendirebilecek tweet paylaşımlarını saklayan, bu paylaşımların analizini gerçekleştiren ve risk potansiyeline sahip olan analiz sonuçları

[11] "IARPA"; 'Ulusal İstihbarat Direktörlüğü Ofisi' bünyesinde yer alan ve 'Amerika Birleşik Devletleri İstihbarat Topluluğu' ile ilgili çeşitli zorlukların üstesinden gelmek için araştırmalara liderlik etmekten sorumlu bir kuruluştur.

bağlamında ilgili analiste uyarı veren bir sistem olarak tanımlanmaktadır. Bu sistem; "Common Vulnerabilities and Exposures (CVE)[12]", "Adobe" ve "Microsoft" sistemlerinin resmi güvenlik uyarılarından elde edilen ve güvenlik ile ilişkilendirilebilecek kelimeler aracılığıyla geliştirilmiştir. Ana yazılımı doğrultusunda 'X Platformu' üzerinden siber güvenlik ile alakalı bir neden/sonuç oluşturma potansiyeline sahip paylaşımları tespit eden ve ilgilisine uyarı gönderen bir donanım ile donatılmıştır.

- "Tehlike Göstergeleri (Indicator of Compromise, IOC)"; çeşitli sosyal medya platformlarında yapılan paylaşımların içeriklerinden kendisine kaynak elde ederken, araştırma içerisinde ilgili kelimelerin yönlendirmesi aracılığıyla bu sitelerden işlemek üzere veriler çekmektedir. Sistemsel donanımı sayesinde çektiği ham verilere çeşitli 'Doğal Dil İşleme (Natural Language Processing, NLP)' metotları uygulayarak ortaya çıktı sunmaktadır. Bu teknik sayesinde belirlediği verilerde bulunan kötü amaçlı yazılım imzası, "Botnet[13]" IP'leri gibi bilgilerin çıkarımını yaparak potansiyel bir saldırının önlemesi için sistemlerine otomatik girdi oluşturmaktadır (Ekşim ve Civelek, 2019, s. 830).
- "Pajek"; sosyal medya analizlerinde kullanılabilecek ve ücretsiz erişilebilen bir yazılımdır. Dijital olarak birden fazla ve çeşitli program ile uyumlu bir biçimde çalışabilmekte, aynı zamanda analiz sonuçlarını görsel olarak ifade edebilmektedir.
- "R"; açık kaynak kodlu, veri analizi ve görselleştirme programıdır. R'nin programlanma şekli, büyük hacimli veri kaynaklarını az süre içerisinde işleme yeteneği sayesinde diğer programlardan ayrılmaktadır. Aynı zamanda sistem içerisine, açık kaynak kodlu bir biçimde tasarlandığından ötürü yeni ve sınırsız sayıda kullanıcı tarafından eklenti eklenebilmektedir. Bu durum da sistemin kendi kendisini sürekli biriktirmesi anlamına gelmektedir.
- "Hadoop (Hadoop Distributed File System, HDFS)"; sıradan sunucularda oluşan kümeler üzerindeki büyük veri birikimlerini işlemek için ilgili uygulamaları çalıştıran ve dağıtık dosya sistemi ile birlikte 'Hadoop MapReduce' özelliklerini harmanlayan bir veri işleme sistemidir. Aynı zamanda 'Java' katkısıyla geliştirilmiş açık kaynaklı bir kütüphane olarak da değerlendirilebilmektedir. Hadoop, HDFS ve MapReduce[14] gibi üç bileşen ile birlikte hayata geçirilen bir yazılımdır (Savaş ve Topaloğlu, 2016, s. 6).

3.2. Big Data Verilerinin Güvenirliliği ve Taşıdığı Riskler

Big Data'nın OSINT faaliyetlerinde sistemsel olarak bir önceki başlıkta yer alan metotlar ve yazılımlar aracılığıyla gerçek birer sonuç ortaya koyması mümkündür. Lakin diğer taraftan bu çalışmalarda işlenecek olan verinin güvenilirliği her zaman bir risk olarak kalacaktır. Bu riskten ötürü istihbarat analistleri, işlenecek olan verileri çok dikkatli bir biçimde güvenilir ve doğrulanabilir kaynaklardan çekmeli; çekilen verilere de 'Bulanık Mantık' düsturuyla yaklaşmalıdır. Bulanık mantığın kullanımı; kesin olmayan, eksik veya tamamen güvenilir olmayan bilgiye dayalı olarak bir soruya yaklaşık cevap çıkarma yeteneği olarak tanımlanabilmektedir. Bulanık mantıkta her şeye bir derece meselesi[15] olarak yaklaşılmaktadır (Hribar vd., 2014, s. 535). Bu mantık kapsamında yaklaşılması gereken açık erişimli bir kaynak olarak 'Dark Web (Karanlık Ağ)' örnek olarak gösterilebilmektedir. Dark Web, açık kaynağın doğruluğunun kontrol edilmesi en güç ve yanıltıcı olma payı yüksek alanlarından birisini oluşturmaktadır. Aynı açık kaynaklar

[12] "CVE"; 'Ortak Güvenlik Açıkları ve Etkilenmeler Sistemi'.

[13] "Botnetler", çeşitli dolandırıcılık ve siber saldırıları gerçekleştirmek için kullanılan ve ele geçirilmiş bilgisayar cihazlarından oluşan ağlardır. 'Botnet' terimi 'robot' ve 'ağ' kelimelerinden üretilmiştir. Bir botnet'in kurulması genellikle çok katmanlı bir planın sızma aşamasıdır. Botlar; veri hırsızlığı, sunucu çökertme ve kötü amaçlı yazılım dağıtımı gibi kitlesel saldırıları otomatikleştirmek için bir araç görevi görür.

[14] "MapReduce"; filtreleme ve sıralama işlemleri gerçekleştiren, harita prosedürü aracılığıyla özet işlemi gerçekleştiren bir azaltma yöntemidir.

[15] "Bulanık Mantık" kavramı içerisinde 'Doğruluk' mefhumu bile bir derece meselesi olarak değerlendirilmektedir.

gibi son yıllarda uygun yöntem ve araçlar kullanıldığı takdirde araştırılabilecek ve içeriği dolayısıyla istihbari bilgi üretilebilecek kıymetli siber güvenlik bilgilerinin zengin birer kaynağı olarak görülen Dark Web sitelerinin (Sezgin ve Boyacı, 2023, s. 285) sıradan web sitelerinin aksine, kolayca tanımlanabilen bir IP adresi yoktur ve örneğin bir 'Tor Web[16]' sitesinin önce bir 'ISP[17]'ye, sonra da bir bireye çözümlenmesi, 'Tor' üzerinde birden fazla düğüm arasında veri aktarımının karmaşık yapısı nedeniyle katlanarak doğrulanabilmeyi daha zor hale getirmektedir. Dark Web'de coğrafi etiketleme kullanan sosyal medyanın olmayışı ve site kullanıcılarının 'yüzeye çıkma' kaygılarından ötürü nerede bulunduklarının reklamını açık bir biçimde yapmayışları, durumun tespitini daha zor bir hale getirmektedir. Bu platformda yer alan kişilerin coğrafi konumlarını tespit etmek için tek yöntem paylaşımlarının, biyografilerinin ya da reklamlarının üslubunu incelemek olabilir. Dark Web'deki suçlular bu tür bilgileri verme eğiliminde olmadıklarından ve bir araştırmacı tarafından daha fazla bilgi için yapılacak herhangi bir araştırma bu kişilerin "ifşa" edilmesiyle sonuçlanabileceğinden, bu yöntemin bugüne kadar sınırlı ve 'nadir' bir başarısı olmuştur (Kalpakis, 2016, s. 122).

Bu noktadaki başarısızlıkların temel sebebi, Dark Web'in özel bilgi ve teknik yeterlilik gerektiren bir alan olmasından kaynaklanmaktadır. Bu ağın inceliklerine aşina olmayan kişiler veya kuruluşlar, potansiyel olarak zararlı veya yasa dışı içeriğe maruz kalma riskiyle karşı karşıya kalmaktadır (Szymoniak ve Foks, 2024, s. 131). Dark Web üzerindeki risklerin kökeni bu ağın, bir site üzerinden birden fazla yazılım diliyle çalışmasından ötürü üzerinde tam otomatik bir incelemeye izin vermemesi durumundan kaynaklanmaktadır. Aynı doğrultuda, bir bireyin direkt aramasının yapılmasına izin vermeyen site yazılımı; veri alma ve analizini otomatikleştirme noktasında kendi korunmasına sahiptir. Bu korunma noktası tam anlamıyla aşılabilecek bir durumda olmasa dahi 'Katana', 'DarkSearch' ve 'Ahmia Search Engine' gibi bazı arama motorları sayesinde daha sağlıklı sonuçlar verebilecek araştırmalar yapılabilmektedir (Rajamäki vd., 2022, s. 26). Dark Web üzerinden elde edilmesi zorunlu bir hale gelen bilgiye istihbarat teşkilatları çalışanlarının şüphe ile yaklaşması ve elde edilen bu bilgiyi defalarca sorgulamaları, eğer yapabiliyorlarsa bu bilgiyi başka kaynaklar aracılığıyla doğrulamaları; ardından göz önünde tutup, bu bilgi doğrultusunda bir aksiyon almaları gerekmektedir.

Açık kaynaktan veri elde etme süreci ile alakalı başlıca bir başka risk bu sürecin yalnızca devletler, istihbarat teşkilatları, bu kurumların yararlandıkları özel kuruluşlar ve şirketler tarafından gerçekleştirilebilir olmayışından kaynaklanmaktadır. Terör örgütleri ve bağımsız teröristler tarafından da açık kaynaklardan elde edilen veriler doğrultusunda faaliyet alanları noktasında bir genişleme yaşanma ihtimali bulunmaktadır. Örneğin; '07.07.2005' tarihinde İngiltere'nin başkentinde gerçekleştirilen "Londra Saldırıları" ortaya çıkarttığı etkiler dolayısıyla 'İngiltere'nin 11 Eylül'ü' olarak sınıflandırılmıştır. Terör eylemleri sonucu 56 insan yaşamını kaybederken 700'den fazla kişi de olaylar sonucu yaralanmıştır. Bu saldırının ulaşım sistemlerine bir dizi intihar saldırısı şeklinde vuku bulmasında birçok anlam ve neden vardır. Saldırganlar ulaşım sisteminde gerçekleştirmeyi planladıkları bu eylemin sonucunda büyük bir problem ve 'güvenlik bunalımı' oluşturacaklarını iyi ön görmüşler; saldırı planını yaparken de 3'ü eş zamanlı olmak üzere, sık bir biçimde kullanılan farklı metro duraklarında patlatacakları bombaların lokasyonlarını belirlerken de işlerini şansa ya da rastlantıya bırakmamışlardır. Öyle ki saldırganlar "Transport For London" adlı Londra'nın ulaşım verilerinin paylaşıldığı resmi sitede yayınlanan açık kaynak verilerini göz önünde bulundurarak öncelikle metronun en yoğun olduğu saatlerden birisi olan 08:50'de ilk üç bombayı; yine bu sitede kamuya açık bir biçimde istatistiki verileri herkes ile paylaşılan bilgiler doğrultusunda da 09:47'de 'Tavistock Meydanı'ndan geçtiği esnada da bir bombayı otobüste infilak ettirmişlerdir. Saldırganlar bombalama gerçekleştirdikleri 3 metro istasyonundan yaklaşık 57 dakika sonra bu meydanda bir otobüste patlattıkları bombayı da insanların bombalanan bu

[16] "Tor Web"; internet üzerinde kişisel gizliliği koruyan ve güvenliği önemli derecede arttıran bir sanal tüneller ağıdır.
[17] "ISP"; internet servis sağlayıcısı.

istasyonlardan ortak nokta olarak o meydana doğru bir kaçış şeması izleyecekleri tespitinde bulunmuşlar, analiz ettikleri bu çıkarımda da haklı çıkmışlardır (Doğan, 2023, s. 81). Bu örnekten de anlaşılacağı üzere denebilir ki teröristler "başarılı" bir açık kaynak taraması aracılığıyla konjonktürel durum saptaması gerçekleştirmiş; faaliyetlerini görece diğer insanların gözünde aslında 'basit istatistiki veriler' olarak görünen rakamları analiz ederek gerçekleştirmişlerdir. Teröristler hayata geçirdikleri terör eylemine açık kaynak verilerini iyi bir düşünsel planla entegre edebilme başarısı göstermişlerdir.

OSINT faaliyetleri çağımızdaki teknolojik değişimler doğrultusunda dönüşen 'teknoloji toplumu' içerisinde istihbarat teşkilatlarının çalışma alanlarından "vazgeçilmesi en zor" alanı oluşturmaktadır. İşleyişi ve eyleme geçilmesi doğrultusunda ilgilisine hızlı bir sonuç vermesi, kaynak açısından büyük imkânlar tanıması gibi olumlu özelliklerinin yanı sıra belirli bazı dezavantajları mümkün olan OSINT çalışmalarında; bu olumsuzlukların önüne geçebilmek üzere ilerleyen dönemlerde bilginin kapsam ve içeriklerinin artmasının durmayacağı ön görüldüğünde, bilgi birikimleri hakkında nitelikli analizler gerçekleştirebilecek analistlerin yetiştirilmesi ve uzmanlaştırılması; ülkeler ve istihbarat teşkilatlanmaları için kritik düzeyde öneme sahip olacaktır.

3.3. Big Data Analizlerinin Geleceği

Enformasyon teknolojilerini merkezine alan teknolojik ilerleme, toplumun maddi temelinin anlamı üzerine bir devrim yapmıştır. İnteraktif iletişim ağlarının küresel düzlemde yaygınlaşması, yeni iletişim biçimleri ve kanalları oluşturarak hayat tarafından şekillenmesinin yanında hayatı da dönüştürmüştür. Toplum bu dönüşüm ışığında barındırdığı rolleri 'sanal dünyaya' uyarlama gayesi içerisine girişmiştir. Bu doğrultuda bireyin aradığı anlamın kökleri, sınırları ortadan kaldıran ve küresel bir kültür oluşturan teknolojik araçların sınırlarında kalmıştır (Castells, 2008, s. 3-4). Bu sınırların içerisinde kurulan dünyanın meşruiyetini kolektif kullanım eğilimi göstererek sağlayan insanlar, bütün disiplinler gelişimlerde önemli değişikliklere yol açmıştır. Zuboff'un 'Gözetleme Kapitalizmi' olarak kavramsallaştırdığı ve insan deneyiminin davranışsal veriye dönüştürülmesi yoluyla işlenecek bir ham madde olarak tanımladığı kavram (Zuboff, 2021, s. 20-21) bir nevi OSINT çalışmalarında kullanılacak verinin kökeninin öncelikle insanda, insan davranışlarında ve kullanımlarında aranması gerekliliğini ortaya koymaktadır.

Toplumun temasından kaçınamadığı çevrimiçi bilgi ortamındaki son gelişmeler, yazılım tabanlı yaklaşımların OSINT çalışmalarının temel bir unsuru haline geleceğinin işaretçisidir. Teknolojik donanımlar sayesinde otomatikleştirilmiş süreçler, OSINT çalışmaları gerçekleştiren analistlerin vazgeçilmez araçları haline dönüşmüştür (Eldridge vd., 2018, s. 401). Bu durumdan çıkartılabilir ki, OSINT çalışmalarında kullanılacak teknolojik araçların gelişimi ve geleceğe entegrasyonu için ilgili ülkenin istihbarat kimliği iyi okunabilmeli ve analiz edilebilmelidir. İstihbarat teşkilatlarının amaçları doğrultusunda izlemek istediği yolu doğru ve kesin bir biçimde oluşturması, izlenecek yolda kullanılacak olan araçların tespitini de dolaylı yoldan öne çıkartacağı için teknolojik araçlar bağlamında doğru bir gelişme planı doğal bir biçimde göz önüne çıkacaktır. Gelişen teknolojiler bu doğal akış içerisinde, analistlerin sürekli büyüyen verileri anlamlandırma ve karar vericilere zamanında öngörüler sunmak için makinelerle birlikte çalışma yöntemlerini de dönüştürmektedir. 'CIA'nın eski 'Öğrenme Direktörü Joseph Gartin', "Analizin geleceği, yapay zekânın, büyük verinin ve makine öğreniminin uzun zamandır yakından ölçeklendirilmiş bir insan çabası olan her şey üzerindeki güçlü ve potansiyel olarak yıkıcı etkileriyle şekillenecek" sözleriyle bu durumun önemini belirtmektedir (Katz, 2020, s. 3). İstihbarat analistleri günümüzde; kanıtları daha verimli bir şekilde bulmak ve filtrelemek, yargılarını makine tarafından türetilmiş olanlarla keskinleştirmek ve test etmek, basit ve gerekli ancak zaman alıcı görevleri otomatikleştirmek için geliştirilecek yapay zekâ sistemlerinden yararlanabilme imkânına sahiptirler. Bu gereklilikler ülkeler tarafından fark edilmekle birlikte harekete geçmeyi perçinleyecek kadar elzem meseleler haline gelmiştir. Öyle ki 'Bloomberg'in 2023 yılının Eylül ayında yaptığı habere göre CIA,

analistlerin açık kaynaklı bilgiye erişimini optimal düzeyde sağlayabilmek amacıyla 'OpenAI Inc.[18]'in ürettiği ve gelişimine devam ettiği yapay zekâ programına benzer bir programın, istihbarat teşkilatı yapılanması içerisinde kullanımına başlanacağını kamuoyu ile paylaşmıştır. Departmanın direktörü 'Randy Nixon' verdiği röportajda, "Ne kadar veri topladığımızın ve ne hakkında veri topladığımızın ölçeği son 80 küsur yılda astronomik bir şekilde büyüdü. Öyle ki bu durum tüketicilerimiz için göz korkutucu ve zaman zaman kullanılamaz hale gelebilir (Bloomberg, 2023)" sözleriyle yapay zekâ programlarının analizleri doğrultusunda "şeylerin bir araya kolayca getirilebildiği" bir sürece geçilmesine izin vereceğini ve bu durumun da OSINT faaliyetleri kapsamında teşkilatının işlerini daha az riskli ve hata payı daha düşük bir biçimde gerçekleştirebileceğini açıklamıştır. Bu açıklamaların ifade ettiği anlam; yapay zekâ çalışmalarının OSINT faaliyetlerine entegrasyonunun, alanın geleceğini şekillendirecek yeni ve çeşitli yazılımları ortaya çıkartacağının bir göstergesi olarak değerlendirilmektedir.

4. Sonuç

Çağımızda yaşanan teknolojik gelişmelerin hızla ve revizyonist bir şekilde artması, toplumsal yaşamın sanal alanlarda daha etkin bir biçimde yaşanmasına olanak tanımıştır. Bu dönüşüm olgusu geleneksel yöntemlerin ötesinde bilginin üretim ve tüketimi noktasında istihbarat paradigmasında ontolojik bir değişmeye yol açmıştır. Bu değişim bağlamında veri kaynaklarında yaşanan geometrik artış ve veri işleme hızı OSINT faaliyetlerini tali bir destek mekanizması olmaktan çıkararak modern istihbarat mimarisinin merkezine yerleştirmiştir. İstihbarat teşkilatlarına hem fırsatlar hem de tehditler sunan bu 'dönüşmüş' istihbarat toplama yöntemi; istihbarat toplama süreçlerini hızlandırırken, bilgi doğrulama ve analiz yetkinliklerinin ön plana çıktığı bir alan haline gelmiş durumdadır.

Bu bağlamda, Big Data verileri aracılığıyla çalışan istihbarat birimlerinin doğru araçları ve teknikleri kullanarak ellerindeki verileri etkili bir şekilde analiz etmeleri; analiz sonuçlarının doğruluklarını yine teyit etmeleri ve daha sonrasında ilgili istihbarat elemanına 'kesin' bir çıktı olarak analiz edilen veriyi iletmeleri, hayati bir öneme sahiptir. Bu süreç içerisinde fırsatlardan en iyi şekilde faydalanmak ve tehditleri minimize edebilmek için sürekli gelişen teknolojilere uyum sağlamanın yanı sıra uzmanlık standartların küresel rekabet yeterliliği doğrultusunda yükseltilebilmesi, istihbarat teşkilatlarının başarısında belirleyici etkenler olacaktır. Bu kapsamda istihbaratın temel sorunsalının bilgi eksikliğinden değil, devasa veri kümelerinin içerisindeki anlamlı sinyalleri ayıklayabilme yeteneğine -analitik kapasitenin yeterliliği- sahip olamama olduğu gözlemlenmiştir. Buna karşın, söz konusu dijital bolluğun beraberinde getirdiği tehditler, istihbarat disiplininin etik ve operasyonel sınırlarını yeniden tanımlamayı zorunlu kılmaktadır. Verinin silah haline getirilmesi -weaponization of data-, dezenformasyon kampanyalarının hızı ve algoritmik manipülasyonlar; karar vericilerin 'doğru bilgiye' ulaşma sürecini her zamankinden daha kırılgan hale getirmiştir. OSINT'in sunduğu demokratikleşmiş istihbarat sahası bir yandan kolektif güvenliğe katkı sunarken, diğer yandan mahremiyet ihlalleri ve devlet sırlarının ifşası noktasında ciddi bir güvenlik açığı teşkil etmektedir. Bu bağlamda, teknik kapasitenin artırılması tek başına yeterli bir çözüm sunmamakta; beşerî zekânın eleştirel süzgeci ile teknolojik imkânların sentezlendiği yeni bir metodolojik yaklaşıma ihtiyaç duyulduğu tespit edilmiştir.

Enformasyon çağı içerisinde teknolojik gelişmelerin ilerlemesinin durmayacağı göz önünde bir gerçekliktir. Bu gerçekliğin kaçınılmaz bir çıkarımı olarak Big Data'yı işlemi altına alan algoritmalar, istihbarat analizi süreci içerisinde kritik düzeyde öneme sahip olmaya devam edecektir. Doğru bilginin elde edilebilmesinin tam anlamıyla 'güç' elde etmek olduğu unutulmamalıdır. Basit bir bilgiyi komplike bir forma dönüştürecek şekilde yorumlayabilme yeteneği günümüzde devlet güvenliğini sağlamak ve stratejik faydalar elde etmek açısından oldukça önemli bir nitelik haline dönüşmüştür. Diğer yandan açık kaynak taraması sonucunda

[18] "OpenAl Inc."; ABD merkezli yapay zekâ araştırma şirketi.

stratejik faydalar elde edebilecek olan tarafın sadece devletler olmadığı göz önünde bulundurulmalı; kamu iletişim araçları aracılığıyla toplumu bilgilendirmek için paylaşılacak olan bilgilerin içeriklerinin neler olması gerektiği ve ne kadarının açıklanması gerektiği yine kamu güvenliği için detaylıca analiz edilmelidir.

Günün teknolojik gereksinimlerini takip etmek ve rekabet içerisinde bulunulan ülkelerin ellerinde bulundurdukları teknolojilerden geri kalmamak, gelecekte trend olabilecek teknolojik yatırımları öngörebilmek ve bu doğrultuda adımlar atabilmek; söz konusu ülkenin istihbarat teşkilatlanmasının elini güçlendirecek çalışmalar olmaya adaydır. Şekillenen yeni dönem içerisinde değişimin araçsal ve donanımsal yenilenmesi önem açısından yeterli görünse de yaşanması gereken asıl gelişim, zihniyet üzerinde olmalıdır. Bilginin hızı ve hacmi karşısında statik kalan yapıların tasfiyesi kaçınılmaz görünürken, bu dinamik süreci yönetebilen ve normlar çerçevesinde teknolojik üstünlüğü stratejik akılla birleştirebilen aktörler, geleceğin küresel güvenlik mimarisinde belirleyici rol oynayacaklardır. Çalışmada tartışılan fırsat ve tehditlerin dengelenmesi ancak teknik yetkinlik ile derinlemesine analitik perspektifin eşgüdümlü bir şekilde sahaya yansıtılmasıyla mümkün olacaktır.

Yazar Katkı Oranı (Authorship Contributions): Yazarlar çalışmaya eşit oranda katkı sağlamıştır.

Kaynakça

Aktan, E. (2018). Büyük veri: Uygulama alanları, analitiği ve güvenlik boyutu. *Bilgi Yönetimi Dergisi, 1*(1), 1-22.

Arıkan, S. M. (2019). *Veri madenciliği temelli siber tehdit istihbaratı*. [Yayımlanmamış Yüksek Lisans Tezi], Gazi Üniversitesi Bilişim Fakültesi, Ankara.

Best, C. (2008). Web mining for open source Intelligence. *IEEE Computer Society, 12th International Conference Information Visualisation, 1550*(6037), 321-325.

Bloomberg. (2024, Mayıs 10). *CIA Builds ıts own artificial ıntelligence tool in rivalry with China*. https://www.bloomberg.com/news/articles/2023-09-26/cia-builds-its-own-artificial-intelligence-tool-in-rivalry-with-china

Bordes Perez, A. (2023). Open source ıntellıgence: an overvıew of today's operatıonal challenges and human rıghts affected as a consequence. *RISR, 2*(30), 6-33.

Böhm, I. ve Lolagar, S. (2021). Open source ıntelligence ıntroduction, legal and ethical consideration. *International Cybersecurity Law Review, 2*(2021), 317–337.

Bukatyi, Y. I., Bukatyi, D. I., Zhovtiak, N. O. ve Storchak, A. S. (2023). Algorıthm of usıng the Osınt technology ın modern servıces. *Автоматизація Технологічних І Бізнес-Процесів, 15*(1), 1-10.

Castells, M. (2008). *Enformasyon çağı: Ekonomi, toplum ve kültür/ağ toplumunun yükselişi*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

CIA FOIA. (2024, Ağustos 26). *Glossary Of Intellıgence Termınalogy*. https://www.cia.gov/readingroom/docs/CIA-RDP55-00166A000100060001-7.pdf

Clark, G., Gonye, A. ve Miller, S. J. (2021). Lessons from the German tank problem. *Springer Nature, 43*(4), 19-28.

Debattista, J., Lange, C., Scerri, S., ve Auer, S. (2015). Linked 'Big' data: Towards a manifold ıncrease in big data value and veracity. *IEEE/ACM 2nd International Symposium on Big Data Computing (BDC), 2*(2015), 92-98.

Doğan, R. F. (2023). İstanbul, Madrid ve Londra saldırıları sonrasında uluslararası arenada terör algısı. *Hakkari Review*, 7(1), 74-89.

Ekşim, A. ve Civelek, İ. (2019). Twitter tweetleri üzerinden açık kaynak istihbaratı tabanlı yarı-Otomatik siber güvenlik modeli. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *7*(1), 827-836.

Eldridge, C., Hobbs, C. ve Moran, M. (2018). Fusing algorithms and analysts: open-source intelligence in theage of 'Big Data'. *Intelligence and National Security, 33*(3), 391-406.

Erol, K. M. (2022). Açık Kaynak İstihbaratı ve askeri istihbarat. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, *1*(1), 23-59.

Gandomi, A. ve Haider, M. (2015). Beyond the hype: big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137-144.

Hribar G., Podbregar I. ve Ivanus T. (2014). OSINT: A ''Grey Zone''?. *International Journal of Intelligence and CounterIntelligence, 27*(2014), 529-549.

Jin, X., Wah, B. W., Cheng, X., ve Wang, Y. (2015). Significance and Challenges of big data research. *Big Data Research, 2*(2), 59-64.

Kahana, E. ve Suawed, M. (2020). *Ortadoğu istihbarat sözlüğü* (1. Baskı). İyi Düşün Yayınları, İstanbul.

Kaisler, S., Armour, F., Espinosa, J. A. ve Money, W. (2013). Big Data: Issues and Challenges Moving Forward. 2013*, 46th Hawaii International Conference on System Sciences*, Wailea, HI, 995-1004, doi: 10.1109/HICSS.2013.645.

Kalpakis, G. (2016). OSINT and the Dark Web. *Advanced Sciences and Technologies for Security Applications*, 4(8), 111-132.

Katz, B. (2020). The Intelligence edge: Opportunities and challenges from emerging technologies for U.S. intelligence. *Center for Strategic and International Studies, 1*(2020), 1-10.

Kızmaz, M. H. ve Küçükçolak, R. A. (2021). Büyük veri teriminin kökeni ve büyük verinin V'leri, *Working Paper Series, 2*(4), 19-31.

Komprise. (2025). Petabyte. Erişim Tarihi: 23.12.2025. https://www.komprise.com/glossary_terms/petabyte/#:~:text=1%20PB%20%3D%201.048.576%20gigabayt,511.627.776%20kilobayt%20(KB)

Kuzucuoğlu, A. H. ve Şeşen, Y. (2021). Veri ve bilgi güvenliği bağlamında istihbarat faaliyetleri. *Lamre Journal, 2*(2), 93-110.

Marr, B. (2024, Aralık 6). *Big Data: The 5 Vs Everyone Must Know*. https://www.linkedin.com/pulse/20140306073407-64875646-big-data-the-5-vs-everyone-must-know

Mercado, S. C. (2004). Sailing the sea of OSINT in the ınformation age. *Studies in Intelligence*, 48(3), 45-55.

Milli İstihbarat Teşkilatı İstihbarat Sözlüğü. (2024, Ağustos 26). *A.* https://www.mit.gov.tr/sozluk.html#A

Moe, W. W. ve Schweidel, D. A. (2014). *Social media ıntelligence*. Cambridge University Press, New York.

NATO. (2001). *NATO open source ıntelligence handbook*. North Atlantic Treaty Organisation, Brussells.

Pastor-Galindo, J., Nespoli, P., Marmol, F. G. ve Perez, G. M. (2020). The Not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, *2*(8),

1-23.

Pringle, R. W. (2015). *Historical dictionary of russian and soviet ıntelligence*. Rowman & Littlefield, New York.

Rajamäki, J., Lahti, I. ve Parviainen, J. (2022). OSINT on the Dark Web: Child abuse material ınvestigations. *Information & Security,* 1(53), 21-32.

Savaş, S. ve Topaloğlu, N. (2016). Siber güvenlikte yeni bir boyut: sosyal medya istihbaratı. *XVIII. Akademik Bilişim Konferansı* içinde (ss. 4-11). Aydın: Aydın Adnan Menderes Üniversitesi Yayınları.

Seolog. (2025). Petabayt, Exabyte, Zettabyte, Yottabyte. Erişim Tarihi: 23.12.2025. https://www.seolog.com.tr/petabyte-exabyte-zettabyte-yottabyte/

Sezgin, A. ve Boyacı, A. (2023). Açık kaynaklardan test otomasyon araçlarıyla siber tehdit istihbaratı çıkarılması. *Fırat Üniversitesi Mühendislik Bilgisi Dergisi, 35*(1), 283-290.

Statista. (2024, Ağustos 31). Number of Internet of Things (IoT) Connections Worldwide from 2022 to 2023, with Forecasts from 2024 to 2034. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Suvay Eker, H. (2022). Sosyal ağlar büyük veriden nasıl yararlanır: Facebook ve Twitter. *Bilgi Yönetimi Dergisi*, *5*(1), 118-130.

Szymoniak, S. ve Foks, K. (2024). Open source ıntelligence opportunities adn challenges- a review. *Advances in Science and Technology Research Journal, 18*(3), 123-139.

Şen, Y. F. ve Yurtoğlu, D. (2020). Teknoloji ve güvenlik ilişkisi bağlamında yapay zekânın istihbarat analizinde önemi. *Güvenlik Çalışmaları Dergisi*, *1*(22), 24-48.

Taban, M. H. ve Aydilek, E. (2022). Dijital çağda istihbarat analizi. *İstihbarat Çalışmaları ve Araştırmaları Dergisi, 2*(1), 38-67.

Wang, Z. H. (2020). Study on application of open source intelligence from social media in the military. *Journal of Physics: Conference Series*, *5*(1507), 1-11.

Yurtsever, S. B. (2024). Sosyal medya istihbaratının makine öğrenmesi çerçevesinde incelenmesi: terörizm çalışmaları. *Savunma ve Güvenlik Araştırmaları Dergisi, 1*(1), 97-119.

Zuboff, S. (2021). *Gözetleme kapitalizmi çağı: Gücün yeni sınırında insan geleceği için savaş*, Okuyan Us Yayınevi, İstanbul.