ANALİZ

MODERN SAVUNMA İSTİHBARATI VE AÇIK KAYNAKLI İSTİHBARAT (OSINT) YAKLAŞIMI

Dr. Can Kasapoğlu

HAZİRAN 2025

Milli İstihbarat Akademisi

MODERN SAVUNMA İSTİHBARATI VE AÇIK KAYNAKLI İSTİHBARAT (OSINT) YAKLAŞIMI

Dr. Can Kasapoğlu

ANALİZ / HAZİRAN 2025

Milli İstihbarat Akademisi

Milli İstihbarat Akademisi

Telif

Yayın Tarihi: Haziran 2025

Millî İstihbarat Akademisi
E-Posta: bilgi@mia.edu.tr

"Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5'inci maddesinin 2'nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir."

ANALİZ / Haziran 2025

MODERN SAVUNMA İSTİHBARATI VE AÇIK KAYNAKLI İSTİHBARAT (OSINT) YAKLAŞIMI

İÇİNDEKİLER

GRAFİK

FOTOĞRAF

GÖRSEL

HARİTA

TABLO

ŞEKİL

YÖNETİCİ ÖZETİ

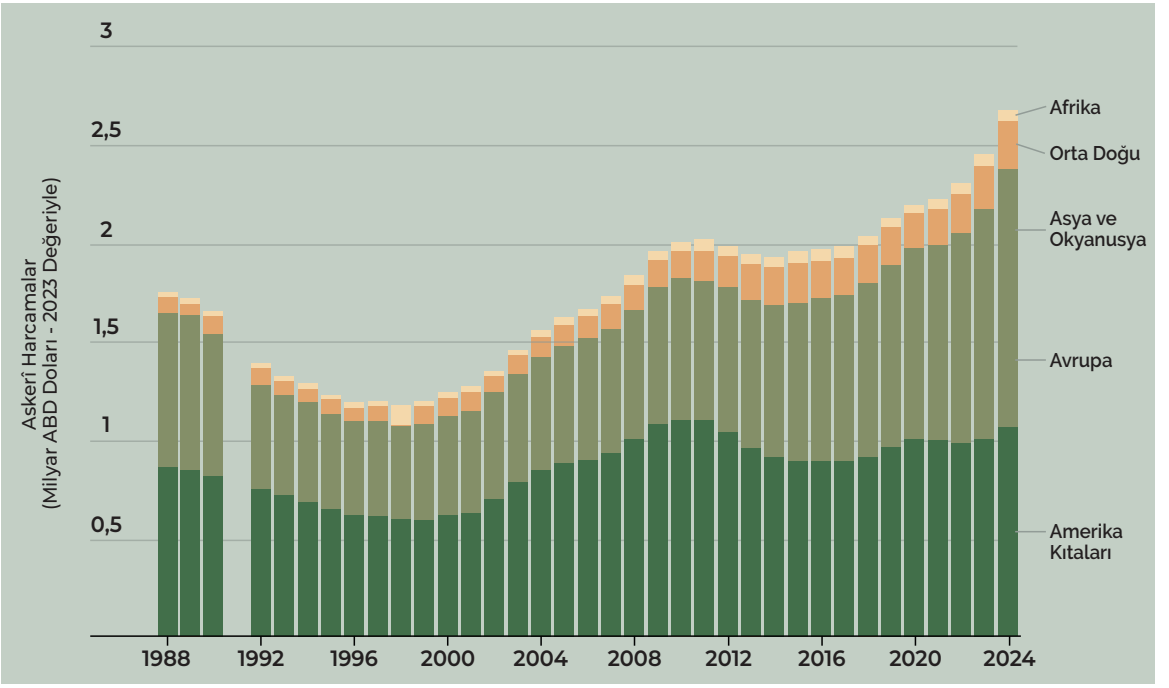
- Soğuk Savaş ve 11 Eylül sonrası yayımlanan siyasa kâğıtları ve yapılan jeopolitik analizlerin büyük bir bölümü, devletler arası harp tehdidini asgari seviyede görmekteydi. Ancak söz konusu öngörüler hatalı çıkmıştır. Zira 21. yüzyıl dominasyon mücadelesinde yüksek yoğunluklu konvansiyonel harp tehdidi ve kitle imha silahlarının kullanımına kadar gidebilecek tırmanma trendleri müşahede edilmektedir. Rusya-Ukrayna Savaşı, Pakistan-Hindistan ve İran-İsrail çatışmaları (2025), konjonktürel askerî gerçekliğin yansıması olmuştur.
- Konjonktürel koşullara ve silahlanma trendlerine paralel olarak savunma istihbaratı ve askerî konularda geliştirilecek istihbarat yetenekleri kritik önem taşımaktadır.
- Enformasyon ortamında yaşanan değişimler özellikle Web 2.0 olarak adlandırılan dönemle birlikte Açık Kaynak İstihbaratı (OSINT) kabiliyetinde ciddi bir yükselişe neden olmuştur. Gerek veri hacmi gerekse nesnelerin interneti (IoT) kapasitesi, geometrik olarak artmaktadır.
- Yapay zekânın gelişmesiyle birlikte analiz kapasitesinde yeniden ciddi bir artış beklenmektedir. Bahse konu yeni imkânların, savunma istihbaratında OSINT 3.0 olarak adlandırılan bir dönemin kapılarını açması muhtemeldir. OSINT 3.0 döneminde yapay zekâ tabanlı sistemler, istihbarat analistinin geleneksel birçok görevini üstlenebilecektir. Diğer yandan insan faktörü, birçok veçhede önemini korumayı sürdürecektir.
- Amerika Birleşik Devletleri (ABD) istihbarat çevreleri başta olmak üzere çeşitli ülkeler, OSINT özelinde yeni istihbarat kuruluşlarının teşkil edilmesi fikri üzerinde değerlendirmeler yapmaktadır.
- Önümüzdeki dönemde analiz kapasitesi ve savunma istihbaratında OSINT kabiliyeti; ülkelerin servisleri dışında düşünce kuruluşu çevreleri, savunma sanayisi kurumları, teknoloji alanında çalışan start-up girişimleri ve özel sektör-kamu iş birliğiyle şekillenecektir. Ön plana çıkacak ülkelerde, kurumların ötesinde strateji ve istihbarat topluluğu kabiliyetinin belirleyici olacağı mütalaa edilmektedir.

GİRİŞ

Rusya-Ukrayna Savaşı başta olmak üzere Orta Doğu'da yaşanan İran-İsrail çatışması ve yansımaları, Pakistan ve Hindistan arasında askerî gerilimin mahdut bir konvansiyonel harp eşiğine tırmanması; 11 Eylül 2001 sonrasında yayımlanan[1] devletler arası harp tehdidinin minimum olduğunu vurgulayan siyasi-askerî değerlendirmeleri büyük ölçüde boşa çıkarmıştır. Rusya Federasyonu'nu transatlantik ittifakın potansiyel bir güvenlik ortağı olarak değerlendiren NATO 2010 Stratejik Konsepti de analitik olarak sert bir duvara çarpan dokümanlar arasında bulunmaktadır. Nitekim 10 yıldan biraz daha uzun bir dönemde NATO, 2022 Stratejik Konsepti ile Rusya Federasyonu'nu doğrudan ve ciddi tehdit olarak tanımlamıştır.[2] Esasen 10 yıllık dönemde konjonktürden çok naif beklentilerin ve isabetsiz analizlerin değiştiğini belirtmek gerekir. Zira NATO 2010 Stratejik Konsepti, 2008 yılında Gürcistan'ın Rus işgaline uğramasından 2 yıl sonra hazırlanmış ve deklare edilmiştir.[3]

Eldeki veriler, devletler arası geniş çaplı konvansiyonel harp ihtimalinin, önceki yüzyıllardan farksız olarak 21. yüzyılda da güçlü bir tehdit olmaya devam edeceğini göstermektedir. Uluslararası silahlı çatışmaların mahiyeti, gayrinizami harp ve düşük yoğunluklu çatışmalar çerçeveleriyle sınırlı ya da ağırlıklı kalmamıştır. Uluslararası siyasal ilişkilerin ayrılmaz bir parçası olan harp kavramı, kuvvet kullanma tehdidi ve caydırıcılıkla birlikte önümüzdeki dönemde de ihtilafların çözümünde belirleyiciliğini sürdürecektir. Savunma ekonomisi trendleri de benzer bir tablo ortaya koymaktadır. 2024 yılı itibarıyla küresel savunma harcamaları 2,7 trilyon doların üzerinde olmuştur.[4] Birçok ülke hızla silahlanmaya devam etmektedir. Eski Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) coğrafyası ve Orta Doğu/Kuzey Afrika coğrafyalarının ötesinde, Tayvan eksenli bir Hint-Pasifik çatışmasının küresel mahiyeti, ABD-Çin harp tehdidini de kapsayacağından çok daha yıkıcı etkiler oluşturacaktır.

Grafik 1: Küresel Savunma Harcamaları (1988-2024)



Kaynak: Stockholm International Peace Research Institute (SIPRI).

Özellikle uluslararası ihtilafların çözümünde harp ve harp tehdidinin ön plana çıktığı bir konjonktürde, müttefik ya da hasım fark etmeksizin devletlerin ve devlet dışı silahlı grupların askerî kapasitelerinin isabetle değerlendirilmesi büyük önem arz etmektedir. Zira tüm aktörlerin harekât tasarılarının, silah sistem kapasitelerinin ya da silahlı kuvvetlerin harp hazırlıklarının ve emir komuta birliğinin yanlış değerlendirildiği hâllerde, Şubat 2022'de Moskova'nın birkaç hafta içinde Kiev'in siyasi-askerî teslimini hesaplaması ya da 2025 tırmanmasında Hindistan'ın Pakistan karşısında kısa sürede kesin bir cezalandırıcı sonuç beklemesi gibi bir stratejik hesap hatasıyla karşılaşılması mukadderdir. Muharebe Sahası İstihbarat Hazırlığı (Intelligence Preparation of the Battlefield, IPB) performansı belirleyici bir faktördür.

BÜYÜK SATRANÇ TAHTASI: AÇIK KAYNAKLI SAVUNMA İSTİHBARATININ ALGORİTMİK DÖKÜMÜ

Zbigniev Brezezinski'nin *Büyük Satranç Tahtası* eserinde de belirttiği üzere satranç analojileri kullanılarak açıklanan uluslararası stratejik meseleler, belki de hiç olmadığı kadar satranç enformasyon ve istihbarat evrenine yaklaşmış; bahse konu klasik oyunun algoritmasına uyumlu bir noktaya gelmiştir. Zira 64 kareden oluşan harp meydanında satranç, rakibin imkân ve kabiliyetine ilişkin neredeyse tam bir istihbarat şeffaflığına dayanmaktadır. Satranç tahtası üzerinde rakibin tüm kuvvetlerini, kuvvetlerinin konuşlandırılma paternlerini ve intikallerini müşahede etmek mümkündür. Aynı şekilde gerçek savaş alanındaki unsurların muharip yeteneklerinin ve tahkimatının da tamamıyla örtülmesi mümkün değildir. Kararlar ancak sınırlılıklar kapsamında verilebilir ve stratejik yaklaşımlar da kombinasyonlara dayanır.

64 kareden oluşan harp meydanında satranç, rakibin imkân ve kabiliyetine ilişkin neredeyse tam bir istihbarat şeffaflığına dayanmaktadır. Satranç tahtası üzerinde rakibin tüm kuvvetlerini, kuvvetlerinin konuşlandırılma paternlerini ve intikallerini müşahede etmek mümkündür.

Taktik düzeyde askerî meselelerin bire bir satranç tahtasıyla örtüştüğünü iddia etmek ve modern savunma istihbaratında espiyonaj faaliyetinin ya da insan istihbaratının (HUMINT) yerinin olmadığını söylemek son derece yanlış bir düşünce olacaktır. Siyasi-askerî meselelerin olduğu oyun tahtasında hâlâ tam olarak bilinmeyen yetenekler, anlaşılamamış konuşlandırma ve intikaller gibi hususlar bulunacaktır. Öte yandan stratejik seviyede, açık kaynaklı savunma istihbaratından gizli tutulabilen olguların sayısı giderek azalmaktadır. Kamuya açık kaynakların kullanabildiği teknolojiler ve veri tabanları her geçen gün arttığı için mezkûr azalma eğilimi devam edecektir. İncelemeye konu hedef bir ülkeye ait bir taburun hareketini izlemek, bir OSINT analisti tarafından gözden kaçırılabilir veya gerçek zamanlı olarak takip edilmesi düşünce kuruluşları ve özel istihbarat şirketleri için her zaman mümkün olmayabilir. Diğer yandan ilgili sınırlılık ve bahsi geçen farazi aktörler, OSINT görevleri açısından çoğu zaman bir anlam ifade etmeyecektir. Bir diğer yandan, aynı hedef ülkenin bir amfibi görev grubu oluşturmak için milyarlarca dolarlık alımlar yapması, tersanelerinde uçak gemisi programı yürütmesi, beşinci nesil savaş uçağı konsorsiyumuna katılması, balistik füzelerini veya stratejik SAM sistemlerini belirli üslerde konuşlandırması ve nükleer caydırıcılık kapasitesinin esasları gibi konuların, siyasi ve askerî boyutlarıyla açık kaynaklı savunma istihbaratından gizlenmesi neredeyse mümkün değildir.

Fotoğraf 1: Su-57 Filosu'nu ve Olası Hasarı Gösteren Açık Kaynaklı Uydu Görüntüsü[5]

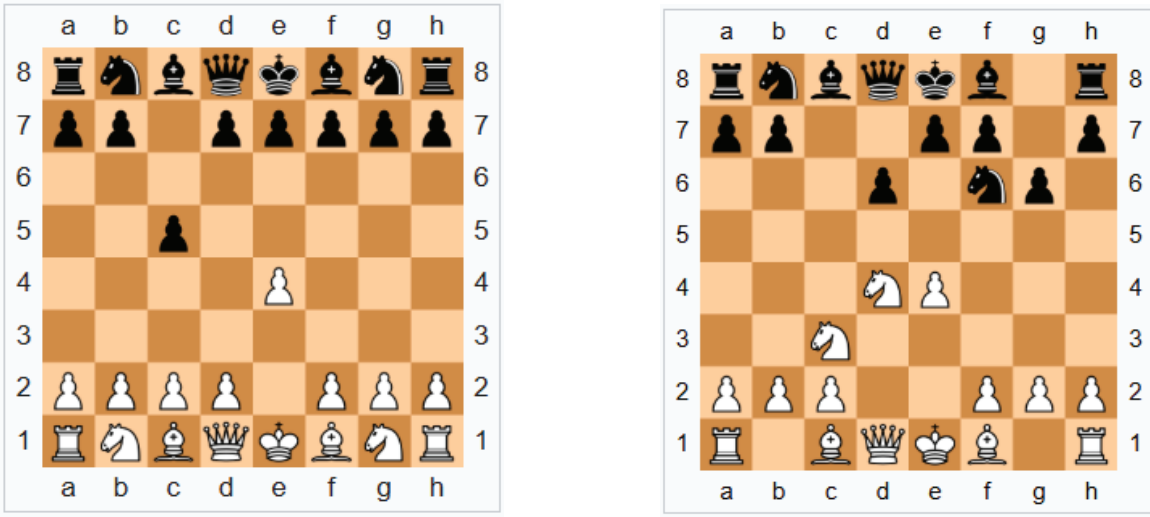
2024 yılında Ukrayna'nın, Rusya'nın Astrahan Oblastı'nda bir hava üssünü vurmasının ardından, üste konuşlu Su-57 Filosu'nu ve olası hasarı gösteren açık kaynaklı uydu görüntüsü Fotoğraf 1'de gösterilmiştir.

Fotoğraf 2: Nur Han Hava Üssü Muharebe Hasarı[6]

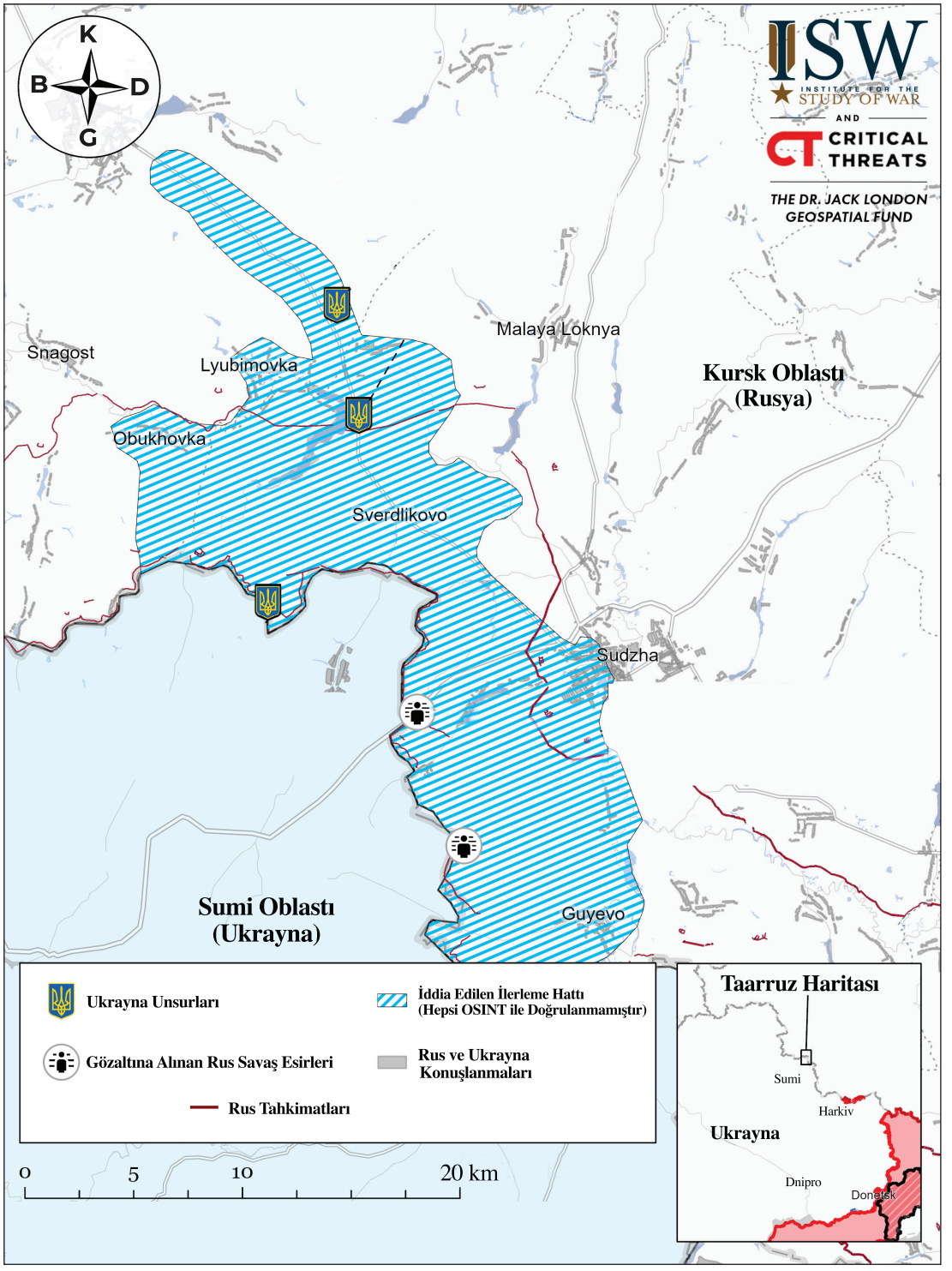
2025 yılı Pakistan-Hindistan çatışmalarında, Hindistan Silahlı Kuvvetleri tarafından vurulan Pakistan Silahlı Kuvvetlerine ait Nur Han Hava Üssü ve açık kaynaklı uydu verisi yoluyla muharebe hasarı Fotoğraf 2'de gösterilmiştir.

Bu noktada kritik bir soru sorarak olası analitik kuşkuların giderilmesi gerekir: "Askerî meselelerin giderek açık kaynaklı savunma istihbaratı kapsamında daha şeffaf ve anlaşılabilir hâle gelmesi, harekât esaslarından biri olan baskın faktörünü tamamen ortadan kaldırır mı?" Bu hususa, satranç analojisini sürdürerek cevap vermek mümkündür. Düşmanın imkân ve kabiliyetine dair eksiksiz bir istihbarata dayanan satranç oyununda, doğrudan sonuç alan ve baskın niteliği yüksek taarruzlar icra etmek mümkündür. Ancak açık kaynak savunma istihbaratının harp sahasındaki artan dominasyonu, savaş alanını giderek daha şeffaf hâle getirse de baskın faktörün etkinliğini ortadan kaldırmayacaktır. Ukrayna Silahlı Kuvvetlerinin 2022 Harkiv ve Herson taarruzları ve 2024 yılında Rusya'nın Kursk bölgesine yapılan taarruz; uydular ve insansız hava araçlarıyla (İHA) neredeyse 24 saat esasına göre izlenen, temas hattının sürekli tahkimatlarla yüzlerce kilometre uzadığı bir harp coğrafyasında dahi mümkün olabilmiştir. Satrançta olduğu gibi istihbarat ortamındaki şeffaflaşma eğilimi, düşman ya da hedef tarafın niyetlerinin aynı ölçüde tahmin edilebilir olması anlamına gelmeyecektir. Dolayısıyla gelişen teknolojik imkânlara ve veri işlemenin yaygınlaşmasına karşın hedef ülkelerin karar verme algoritmalarının ve stratejik kültürlerinin anlaşılması elzemdir. Ayrıca ülke elitine dair biyografik istihbarat analizi ve nöropsikiyatrik profillerinin ve muhakeme yeteneklerinin değerlendirilmesi amacıyla icra edilecek medikal istihbarat çalışmaları da etkili olacaktır. Sözü edilen tüm faktörlere bağlı olarak sonraki adımların isabetli tahmin edilmesinde, istihbaratçılığın yüzyıllara dayanan birikimi önemini sürdürmektedir.

Görsel 1: Sicilya Savunması Açılışı (Solda) ve Sicilya Savunması Ejderha Varyasyonu



Harita 1: Kursk'a Yönelik Baskın Tarzındaki Ukrayna Taarruzu, Açık Kaynaklı İstihbarat Haritalandırması (Ağustos 2024)

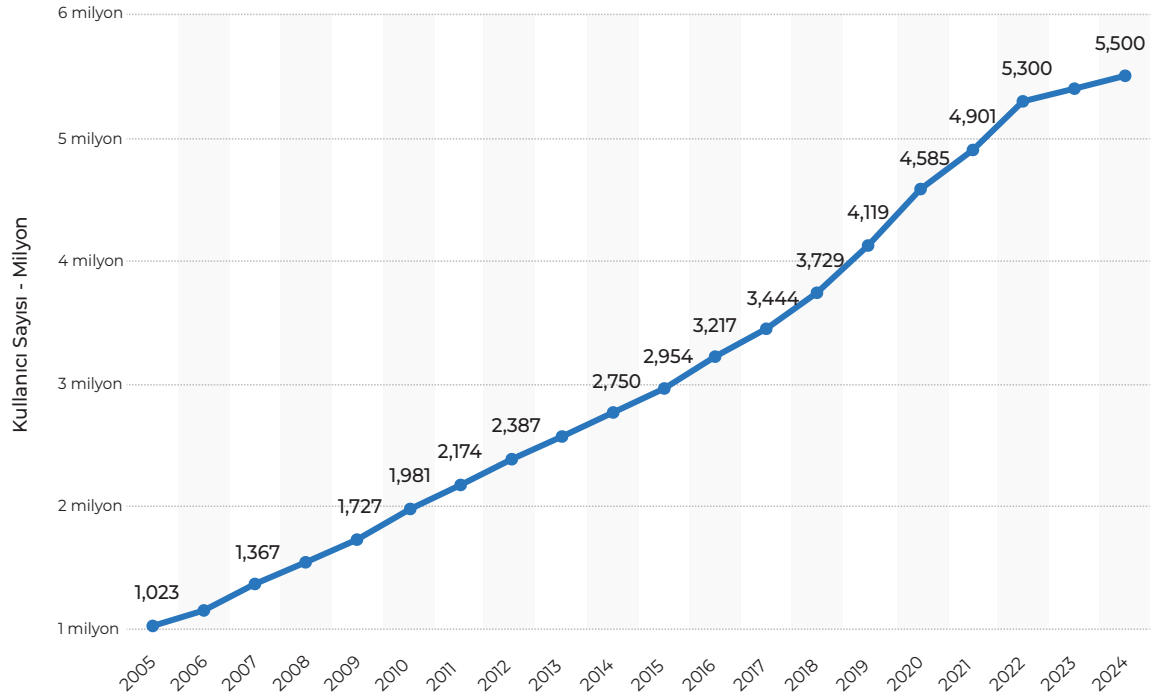


Kaynak: ISW.

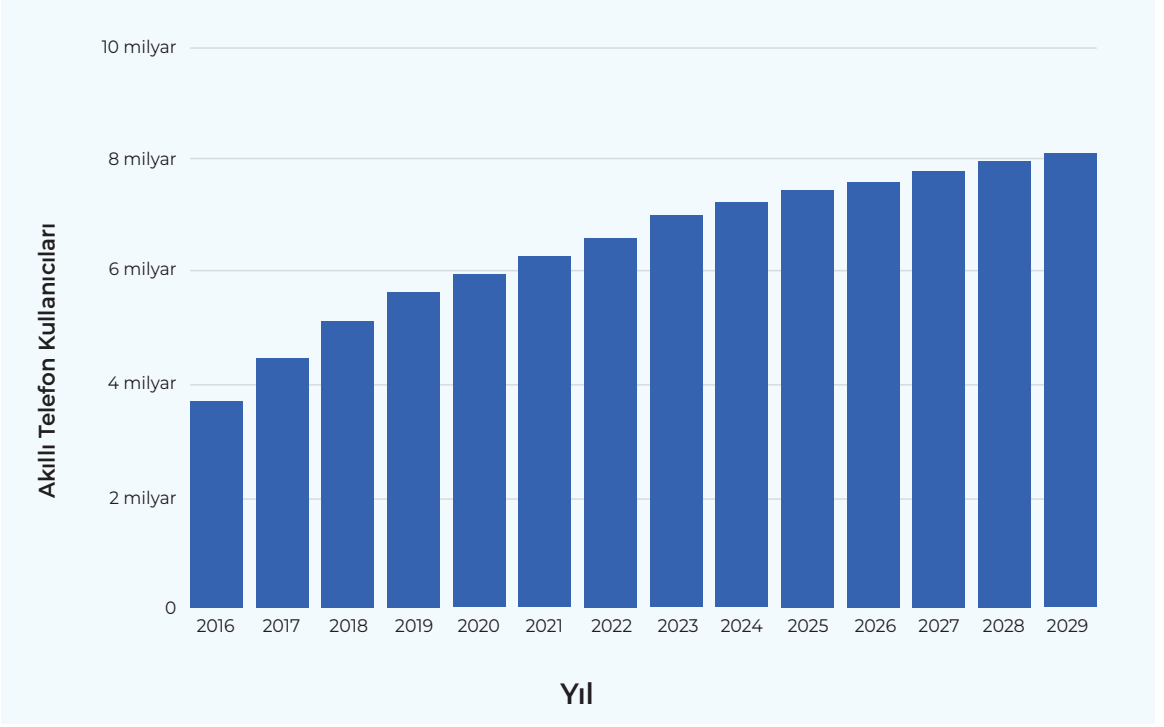
SAVUNMA İSTİHBARATI VE OSINT'İN YENİ YÜZYILI

Günümüzde internetin tüm bireyler tarafından kullanılan bir kaynak hâline gelmesi, dijital okuryazarlığın küresel ölçekte artması ve sosyal medya kullanımının küreselleşmesi, 21. yüzyılın dijital enformasyon ortamını giderek daha erişilebilir hâle getirmiştir. Bazı değerlendirmeler, 2025 Şubat itibarıyla dünya genelinde yaklaşık 5,24 milyar kişinin sosyal medya kullanıcısı olduğunu belirtmektedir. İnternet kullanıcıları, küresel nüfusun yaklaşık %63,9'una denk gelmektedir.[7] Ayrıca akıllı telefonlar ve sosyal medya uygulamaları, harp sahalarına bir ölçüde girmiştir. Dahası 2020'li yıllarla birlikte dünyadaki cep telefonu sayısı, insan nüfusunu geride bırakmıştır. 2022 yılında 7,95 milyar insanın yaşadığı dünyada 8,58 milyar[8] cep telefonu kaydı bulunmaktadır. OSINT açısından en önemli araç olan Web 2.0 parametrelerine uygun (internet bağlantısı ve uygulama kullanımları, kamera, jeolokasyon belirleme yetenekleri olan) akıllı telefonlar da aynı şekilde artış göstermektedir. Günümüzde 7,21 milyar akıllı telefon kullanılmaktadır. Dünyada akıllı telefon, en çok Çin'de bulunurken oransal olarak akıllı telefon pazar penetrasyonu Almanya'da en yüksek seviyededir. 10 milyarın[9] üzerinde cihaz da nesnelerin internetine bağlıdır. Daha açık bir anlatımla dünya, OSINT için bir inkübasyon merkezi hâlindedir.

Grafik 2: 2005-2024 Tarihleri Arasında Dünyadaki İnternet Kullanıcıları[10]

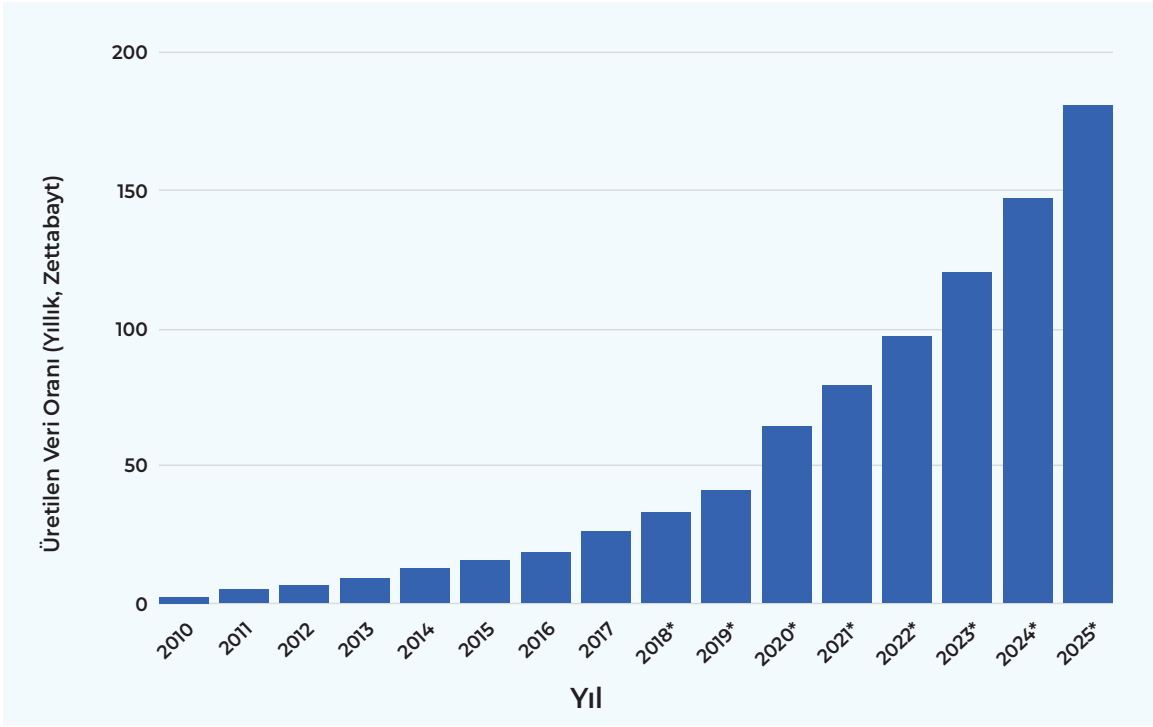


Grafik 3: Küresel Akıllı Telefon Kullanım İstatistiği ve Projeksiyonları[11]



Yapay zekâ destekli ve internet tabanlı teknolojinin geometrik olarak artmakta olduğu; harp ortamında giderek yaygınlaştığı gözlemlenmektedir. Söz konusu yayılma harekât sahasını, neredeyse her adımın izlenebildiği/takip edilebildiği şeffaf bir alana dönüştürmüştür. Bahse konu trend, akıllı telefon devrimi ile hız kazanmıştır. Nitekim 2012 yılında piyasaya çıkan en yeni akıllı telefon 64 GB veri depolayabilme kapasitesine sahip olmuştur. Ancak 2023 yılında, bir kişinin bir günde ürettiği veriyi depolamak için 234 adet aynı telefona ihtiyaç duyulmaktadır. Bu veriler, dünyadaki enformasyon ve veri akışının artış hızını gözler önüne sermektedir.[12] Ayrıca 2013 yılında global ölçekte 4,4 zettabayt data üretilmiştir. Söz konusu üretim, insanlık tarihinin genel veri üretiminden fazladır. Data üretimi, geometrik olarak[13] büyümektedir. Nitekim 2025 yılında global data üretimi 181 zettabayta çıkmıştır.[14] Dolayısıyla bahse konu çerçevede, sivil ve akademik amaçlı kullanılan bilgilerin yanı sıra, askerî enformasyonun da önüne geçilmesi zor bir hızla yayıldığı müşahede edilmektedir. Söz konusu trend, tüm karar alıcılar tarafından yakından takip edilmelidir. Bahsedilen çerçevede askerî bilimler ve veri analizi yeteneklerinin tahkim edilmesi kritiktir.

Grafik 4: Son 15 Yıllık Kısa Bir Dönemde Data Üretimi ve Geometrik Büyüme Eğilimlerinin Analizi[15]



Fotoğraf 3: Rus Ka-52 Taarruz Helikopteri ve 9M39 Füzesi[16]

Savunma İstihbaratında Aktör Çeşitliliği

Savunma istihbaratının OSINT'le birlikte 21. yüzyılda önem kazanmasının birkaç kritik boyutu bulunmaktadır. Bunlardan ilki, uluslararası meselelerin giderek askerîleşen gündemidir. Soğuk Savaş Dönemi'ni müteakip özellikle 11 Eylül terör saldırılarının ardından yayımlanan millî güvenlik siyasa dokümanları ve millî strateji dokümanları; devletler arası savaş riskinin minimuma indiğini[17] belirtirken yükselen güvenlik trendinin düşük yoğunluklu çatışmalar etrafında şekillendiğini öngörmüştür. Bahse konu öngörü; 2014 yılında Kırım'ın işgali, 2022 yılında Rusya-Ukrayna Savaşı ve 2025 yılında İslamabad-Yeni Delhi çatışmasıyla anlamsız hâle gelmiştir. Savunma ekonomisi trendlerinde görüldüğü üzere uluslararası silah pazarı hiç olmadığı kadar hareketlenirken savunma endüstrileri yeniden büyüme trendine girmiştir.

Savunma istihbaratının OSINT ile giderek daha fazla entegre olması; savunma bakanlıkları, istihbarat teşkilatları, gizli servisler, genelkurmay başkanlıkları ve kuvvet karargâhları gibi geleneksel istihbarat aktörlerinin yanı sıra düşünce kuruluşları, jeopolitik risk analizi yapan uzmanlar ve özel istihbarat şirketlerinin de bu alana dâhil olmasına yol açmıştır. OSINT analizi, modern çatışmaların izlenmesi ve jeopolitik gelişmelerin takip edilmesi açısından düşünce kuruluşları için de oldukça kritik bir kabiliyet hâline gelmiştir.

Örneğin Institute for the Study of War (ISW), her hafta yayımladığı Rusya-Ukrayna Savaşı değerlendirmelerinde tamamen ticari kullanımlı uydu görüntülerini, sahadan görsel ve taktik veriler içeren Facebook, Telegram ve X (eski adıyla Twitter) kaynakları ile açık kaynaklı medya platformları (TASS, Kyiv Independent vb.) kullanmakta; değerlendirmelerini kapsamlı bir OSINT portföyü üzerine inşa etmektedir. Söz konusu çalışmalar, açık kaynaklardan elde edilen verilerin anlamlı ve sistematik bir şekilde sentezlendiğinde, harp sahasının güncel dinamiklerine ilişkin kritik bulgular sunduğunu ortaya koymaktadır. ISW'nin bahse konu çalışması, modern askerî OSINT yöntemleriyle elde edilen verilerin nasıl stratejik analizlere dönüştürülebileceğini göstermektedir. Rusya-Ukrayna Savaşı'na dair bir diğer OSINT tracker çalışması, bu satırların yazarı tarafından yayımlanan Hudson Institute Ukraine Military Situation Report (UMSR) adlı çalışmadır. Benzer şekilde Web 2.0 yeteneklerinin kullanımı, haftalık bir askerî durum raporunu mümkün kılmaktadır.

Bu kapsamda OSINT çalışmalarıyla ilgili bir diğer önemli örnek, yine ABD menşeli düşünce kuruluşu Center for Strategic and International Studies (CSIS) tarafından yürütülen Hidden Reach projesidir. Hidden Reach, Çin'in küresel etkisini ve stratejik faaliyetlerini daha iyi anlamak amacıyla OSINT ve uydu görüntülerini kullanarak askerî stratejik analizler[18] sunmaktadır.

Hidden Reach'in son yayınlarında; Çin'in Küba'daki sinyal istihbarat tesisleri, çift kullanımlı tersaneleri ve kutup bölgelerindeki araştırma istasyonları gibi çeşitli kritik sahalardaki faaliyetleri incelenmiştir. Söz konusu çalışmalarda, OSINT aracılığıyla öne çıkan bulgular oldukça çarpıcıdır. Örneğin Küba'da 4 aktif sinyal istihbaratı tesisinin Çin'in ABD'ye yönelik casusluk faaliyetlerine destek sağladığına ilişkin emareler tespit edilmiştir. Pekin hükûmetinin sivil/ticari gemi inşa endüstrisinin askerî amaçlarla nasıl kullanıldığı ve yabancı şirketlerin söz konusu ekosistemdeki rolü de yine Hidden Reach'in

askerî OSINT çalışmalarının katma değerini ortaya koyan örneklerdendir. Bahse konu bulguların önemli siyasi yansımaları da bulunmaktadır. Örneğin söz konusu proje, elde ettiği bulguları interaktif dijital raporlar ve multimedya içerikleri aracılığıyla sunarak politika yapıcıların, strateji çevrelerinin ve Batı kamuoyunun Çin'in küresel yükselişini (ve bu trendin siyasi anlamını) daha derinlemesine anlamasına katkıda bulunmaktadır.

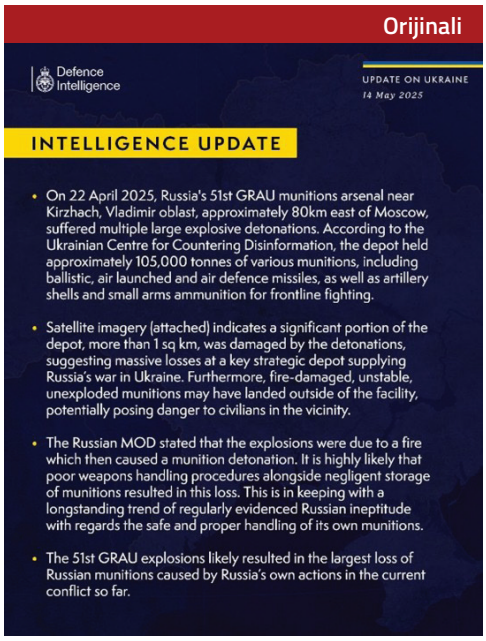
İstihbarat dünyasında, kamu alanı dışında kalan aktörler skalasının gri sahasında, Rus Wagner örneğinde bir dönem gözlemlendiği üzere özel orduların da istihbarat toplama/analiziyle uğraştığı bilinmektedir. Örneğin, ABD Eğitim ve Doktrin Komutanlığı (U.S. Army Training and Doctrine Command, TRADOC) tarafından yayımlanan bir çalışma, Mart 2022'de çok sayıda Ukrayna personelinin hayatını kaybettiği Yavoriv Üssü'ne yönelik füze taarruzunun temel nedeninin, Rus Wagner özel askerî şirketinin +44 koduyla çok sayıda İngiliz GSM hattının bölgede tespit edilmesi ve Kiev yanlısı yabancı savaşçıların hedef alınarak caydırılması olduğunu aktarmıştır.[19]

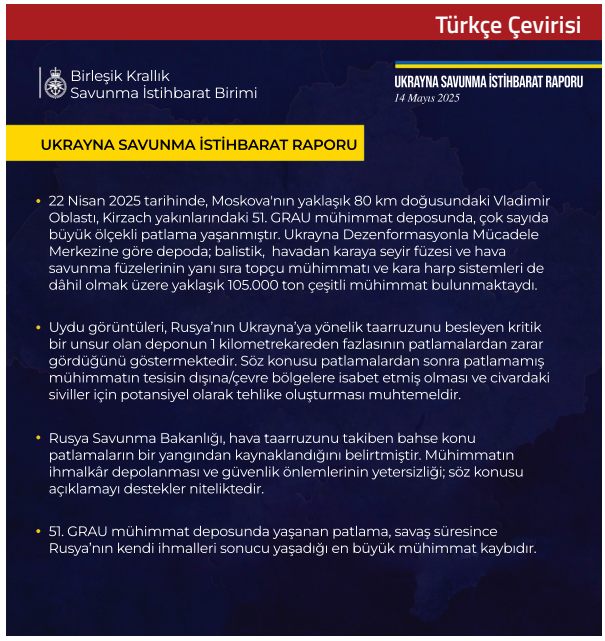
Savunma istihbaratında yaşanan değişim yalnızca teknolojik imkânlar ve OSINT yükselişiyle sınırlı değildir; yeni aktörler de uluslararası zemini daha karmaşık hâle getirmektedir. Zira düşünce kuruluşları kimi zaman yalnızca stratejik meseleler üzerine çalışan bir analist gibi değil, bir siyasanın savunucusu gibi de davranabilmektedir. Söz konusu tabloya savunma dünyasının bir diğer paydaşı olan savunma sanayisi kuruluşlarını da eklemek gerekmektedir. Kamu ya da özel menşeli savunma sanayisi kuruluşları; kendi bünyelerinde istihbarat ve değerlendirme birimleri teşkil etmek[20] ve düşünce kuruluşlarıyla iş birliğine gitmek yoluyla istihbarat analizi üretmektedir.

OSINT strateji topluluğu ve gizlilik parametreleri analizi kapsamında üç husus öne çıkmaktadır. Bunlardan ilki, OSINT'in teknolojik olduğu kadar aynı zamanda jenerasyonel bir nitelik yansıtmasıdır. Daha genç istihbarat analistlerinin özellikle teknolojiyle olan etkileşimleri nedeniyle ön plana çıktığı müşahede edilmektedir. 2020'li yıllarda yaşanan Web 2.0 bağlantılı OSINT devriminin, ilerleyen yıllarda, istihbarat servislerinde de bir stratejik kültürel dönüşümü yönlendirme potansiyeli mevcuttur.

İkinci olarak OSINT kültürü, istihbarat çarkının son veçhelerinde de müşahede edilmektedir. Örneğin Birleşik Krallık Savunma Bakanlığı, Rusya-Ukrayna Savaşı'nın başından beri düzenli olarak askerî[21] istihbarat cari değerlendirmelerini kamuya açık olarak sosyal medya hesabı X üzerinden resmen açıklamaktadır. Benzer şekilde ABD Afrika Komutanlığı, birkaç yıl önce[22] Rus askerî aktörü Wagner'in Libya'da konuşlandırdığı silah sistemlerini resmî internet sitesi üzerinden uydu görüntüleriyle açıklamıştır. Yine Ukrayna Savunma İstihbarat Kurumu (Defence Intelligence of Ukraine, GUR) resmî sosyal medya hesaplarından[23] doğrudan icra edilen harekâtlara dair, Rus cephe gerisinden dahi içerik paylaşmaktadır. Ukrayna askerî istihbaratı, tüm paydaşlara açık bir küresel OSINT yarışması dahi icra etmiştir.[24] Ukrayna Silahlı Kuvvetlerinin sosyal medya kullanımının, tugay ve tabur düzeyinde taktik birliklere kadar indiği gözlemlenmektedir. Söz konusu birliklerin her biri, daha çok sponsor bulmak ve yardım toplamak amacıyla muharebe sahasında içerik paylaşmaktadır.

Görsel 2: Birleşik Krallık Savunma Bakanlığı Ukrayna Cari Askerî İstihbarat Raporu[25]





Fotoğraf 4: Rus 51. GRAU Mühimmat Deposunun Ukrayna Hava Taarruzu Sonrası Aldığı Hasar[26]

Görsel 3: Ukrayna Savaş Yaptırımları Hackathon Yarışması[27]

Fotoğraf 5: ABD Afrika Komutanlığının Yayımladığı Wagner Libya İleri-Konuşlu Unsurlarına Ait Uydu Görüntüleri[28]

AÇIK KAYNAKLI SAVUNMA İSTİHBARATI TEKNOLOJİLERİ VE YÖNTEMLERİ

Savunma istihbaratının 21. yüzyılda uğradığı değişiklik, askerî sistemlerdeki gelişmelerden çok enformasyon ortamındaki değişimlerden neşet etmektedir. RAND Corporation tarafından 2018 yılında kaleme alınan "İkinci Nesil Açık Kaynaklı İstihbarat" başlıklı rapor, dijitalleşme ve sosyal medya platformlarının yükselişiyle beraber gelen Web 2.0 enformasyon teknolojileri devriminin, savunma konularında OSINT icrası açısından kritik bir faktör olduğunu ortaya koymaktadır. Bağlantılı olarak RAND tarafından "ikinci nesil askerî OSINT" olarak tanımlanan paradigmaya göre "X, Facebook, YouTube, Telegram ve Signal" gibi kullanıcı içeriğine dayanan uygulamaların yaygınlaşması OSINT'in dinamik, gerçek zamanlı ve teknik analiz gerektiren bir istihbarat disiplinine evrilmesini sağlamıştır. 2005 sonrası dönemde ivme kazanan bu yaklaşımda, sosyal medyaya yansıyan görüntüler, konum verileri (geolocation) ve referansları gibi enformasyon kaynakları, istihbarat için önemli hâle gelmiştir.[29]

Bir diğer ifadeyle Soğuk Savaş Dönemi'nde ve hemen sonrasındaki geçiş aşamasında, çok gizli olarak tanımlanan ve teknolojik olarak yalnızca devletlere -hatta bir grup elit devlet kulübüne- ait olan uzay teknolojileri tabanlı izleme gibi imkânlar, 21. yüzyılın ilerleyen aşamalarında ticari seçeneklere dönüşmüştür. Bugün ABD ve Birleşik Krallık gibi siyasa yapımının ön plana çıktığı ülkelerde, önde gelen hemen her düşünce kuruluşu, çok yüksek çözünürlüklü ticari uydu görüntülerini tamamen yasal bir zeminde ve açık kaynağa dayanarak satın alabilmektedir. Söz konusu faaliyet; ilgili düşünce kuruluşlarının büyük birlik intikallerini ve konuşlanmalarını, silah sistemlerini, hava/deniz üslerini izlemesini ve istihbarat analizi hazırlamasını mümkün kılmıştır. Dalış anında denizaltılar ya da hava harekâtı icrasında anlık durum gibi istisnaların haricinde, neredeyse tüm askerî unsurların takibi, OSINT kullanılarak mümkündür.

Savunma istihbaratını mümkün kılan bir diğer husus, envanterlerin giderek şeffaflaşması ve uluslararası yayınlara konu olmasıdır. Londra merkezli düşünce kuruluşu The International Institute for Strategic Studies'in (IISS) Military Balance yıllık güncellenen savunma veri tabanı ve İsveç merkezli düşünce kuruluşu Stockholm International Peace Research Institute (SIPRI) tarafından yapılan savunma alımları ve savunma ekonomisi değerlendirmeleri, söz konusu alanda birincil örnekleri teşkil etmektedir. Düşünce kuruluşlarının dışında savunma konularına özel Defense News gibi uluslararası mecralar[30] da ortaya çıkmıştır. Söz konusu neşriyat gerek endüstri liderlerini gerekse de son kullanıcıları bir araya getirmektedir.

Teknolojik olarak Web 2.0 ve akıllı telefonların harp sahasına girmesi ayrıca uydu görüntülerinin ticarileşmesi ve jeouzamsal araçların ortaya çıkması, savunma istihbaratında OSINT döneminin en önemli hususlarındandır. Ayrıca silah sistemlerinin analizleri ve dizayn hususlarının da açık kaynaklı olarak değerlendirilmesinde ciddi bir artış müşahede edilmektedir. Böyle bir ortamda, harekât güvenliği ve personelin dikkati, kritik bir mahiyet kazanmaktadır.

Fotoğraf 6'da, Suriye'de Baas rejimi tarafından icra edilen, savaş suçları kapsamındaki kimyasal harp taarruzlarında kullanılan mühimmat gösterilmektedir. Soldaki fotoğrafta genellikle ülkenin güneyinde rastlanan ve ağırlıklı olarak dönemin Suriye Arap Silahlı Kuvvetleri 4. Zırhlı Tümeni envanterinde

bulunan (Mahir Esed komutasındaki birlik), kimileri İran tarafından imal edilen 107 mm çapındaki topçu roketleri müşahede edilmektedir. Sağdaki fotoğrafta ise ülkenin kuzeyindeki döner-kanatlı platformlar tarafından düzenlenen klor-varil bombası taarruzlarında kullanılan hava-kara güdümsüz mühimmatı bulunmaktadır. Savunma istihbaratı ve OSINT açısından önemli olan husus, bahse konu görsellerin harp sahasında akıllı telefonlar aracılığıyla siviller tarafından çekilmiş ve sosyal medya platformlarına yüklenmiş olmasıdır. Konuya dair ilk ve en kapsamlı değerlendirmenin[31] bir OSINT ağı olan Bellingcat tarafından yayımlanması dikkat çekicidir.

Fotoğraf 6: Baas Rejimi Suriye Arap Silahlı Kuvvetlerine Ait Kimyasal Harp Atış Vasıtaları

Kaynak: Bellingcat.

Sosyal medya içeriklerini analiz etmek için yararlanılan ve ticari kullanıma açık enformasyon araçlar (commercial off the shelf/COTS tools), bu dönüşümde etkili olan başlıca teknolojilerdendir. Çift kullanımlı (dual use) teknolojilerin en sık karşılaşılan örneklerinden biri olan bu araçlar, kelime temelli analiz (lexical analysis), sosyal ağ analizleri (social network analysis) ve coğrafi konumlama (geospatial analysis) gibi tekniklerle ham verileri anlamlı istihbarat çıktısına dönüştürmek için kullanılmaktadır.[32] Örneğin bir çatışma bölgesinden paylaşılan Tweet'ler ile paylaşım zamanı ve konumunun eşleştirilmesi (bir nevi veri üçlemesi[33] çerçevesinde) özellikle bir çatışmanın erken aşamalarında kritik değerlendirmeler sunabilmektedir.

Jeouzamsal (geospatial) analiz kapsamında ele alınan metodolojiler, içlerinde "geolocation, geoinference ve georeferencing" gibi alt teknikler bulundurmaktadır. Birbirlerini tamamlayan bu tekniklerin kullanımı ve metodolojileri, Tablo 1'de detaylandırılmıştır.

Tablo 1: Konuma Bağlı (Location-Based) OSINT Metodolojileri

Yöntem	Tanım	Metodoloji	Kullanım Alanları
Geolocating	Bir görseldeki nesneleri haritalarla eşleştirerek konum tespiti yapılması.	1. İlgili fotoğraf ya da video seçilir. 2. Referans noktası olarak tanınabilir yapılar (örneğin, bir kilise) tespit edilir. 3. Google Earth ve Panoramio gibi araçlarla harita üzerinde bu yapılar bulunur ve konum belirlenir.	Sosyal medya analizleri, hedef tespiti, açık kaynaklı istihbarat.
Geoinference	Konum bilgisi verilmeyen durumlarda, çevresel ipuçlarından yola çıkarak konum tahmin edilmesi.	1. Kullanıcıların sosyal medya paylaşımları ve diğer dijital izleri analiz edilir. 2. Paylaşımlardaki yerel unsurlar/ipuçları tespit edilir. 3. Algoritmalar ve dil analizi ile bu unsurlardan konum tahmin edilir.	Dijital izleme, sosyal medya takibi, kullanıcı konum tahmini.
Georeferencing	Eski haritalara gerçek dünya koordinatlarının eklenmesi.	1. Eski harita veya görsel seçilir. 2. Harita üzerindeki noktalar belirlenir (örneğin bir bina veya yol). 3. Modern verilerle bu noktalar örtüştürülür ve gerçek dünya koordinatları atanır.	Harita güncellemeleri, askerî hedefleme, altyapı analizi.

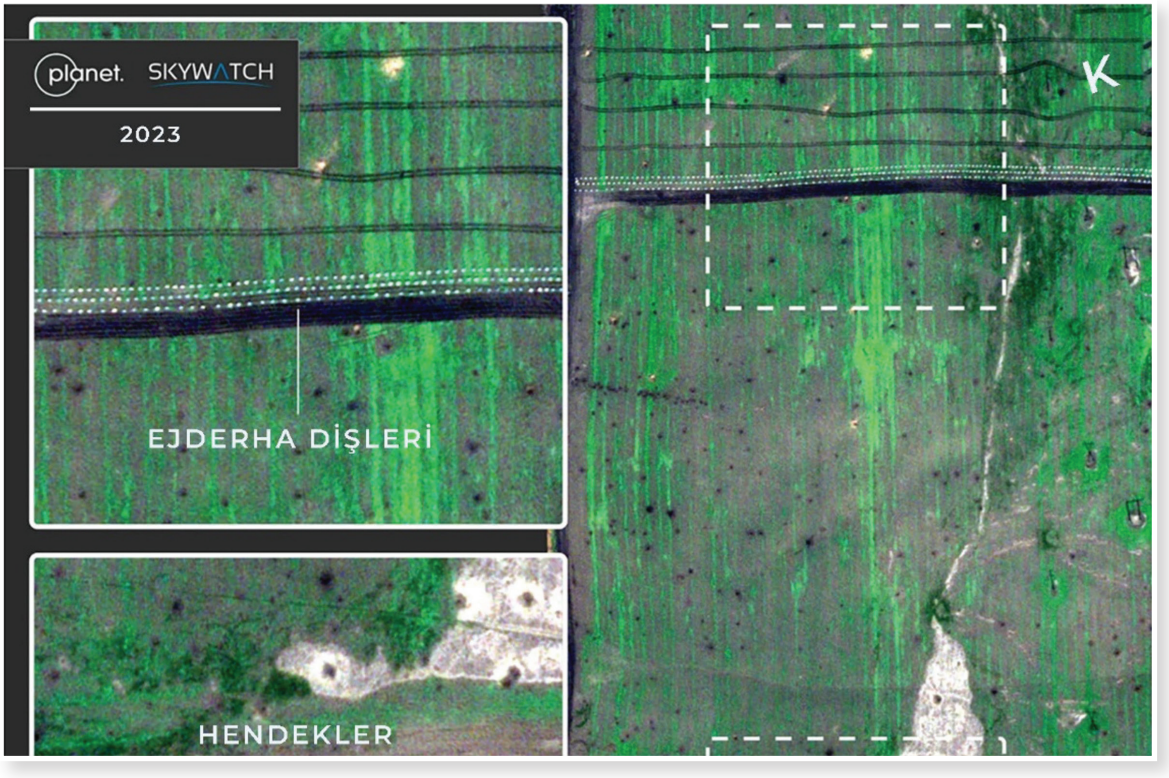
Tabiatıyla sivil ve ticari ihtiyaçlar için geliştirilen bu araçlar, istihbarat topluluğunun teknik gereksinimlerini karşılamada yetersiz kalabilmektedir. Söz konusu çerçevede, bahsi geçen sivil kullanımlı teknolojilerin askerî amaçlara hizmet edebilmek üzere uyarlanması, askerî istihbarat çevrelerinde gerekli yatırımlarla desteklenerek önceliklendirilmelidir.

RAND Corporation'a göre söz konusu teknolojik dönüşüm OSINT'i yalnızca geleneksel istihbarat kaynaklarını tamamlayan değil, onları bazen doğrudan ikame eden bir disipline de dönüştürmüştür. Gelişmiş yapay zekâ algoritmaları ve büyük veri analitiği sayesinde, daha önce yalnızca gizli operasyonlarla elde edilebilecek bilgilerin artık açık kaynaklardan kolaylıkla türetilebilmesi, enformasyon ortamının giderek "demokratikleştiğine" işaret etmektedir. Bu çerçevede istihbarat birimlerinin sosyal medya, kullanıcı kaynaklı içerik ve otomasyon teknolojilerine yönelik kapasite geliştirmesi bir ihtiyaç, hatta kritik zorunluluk hâline gelmiştir.

Konuma bağlı OSINT'in yapısını derinden değiştiren diğer önemli faktörlerden biri ise uydu teknolojileridir. Örneğin süregelen Rusya-Ukrayna Savaşı'nda, çoğunlukla Planet ve Maxar gibi özel uydu görüntüleme şirketleri tarafından paylaşılan uydu görüntüleri, kamuoyuna "savaşın ilk aylarında Rus yığınaklarına, taarruz istikametlerine ve birliklerinin muharebe kuruluşuna" dair önemli bilgiler sunmuştur.[34]

Söz konusu eğilim, beraberinde önemli bağımlılıklar da getirmektedir. OSINT verilerine yansıyan bilgilere göre geçtiğimiz aylarda ABD hükûmeti, Maxar'in Ukrayna'ya sağladığı uydu bazlı enformasyon paylaşımının engellenmesine karar vermiştir. Söz konusu durum, Ukrayna askerî/siyasi karar alıcıları ve özellikle dron pilotları için "paralize edici" olarak adlandırılabilecek negatif etkilere sebep olmuştur.[35] Starlink'in uydu tabanlı iletişim ve internet hizmeti, Ukraynalı birlikler için muhabere altyapısının vazgeçilmez bir unsuru hâline gelmiştir. Bazı kaynaklar, Ukrayna'nın söz konusu sisteme bir alternatif bulana kadar Starlink'e bağımlı olduğunu dahi öne sürmüştür. Bir başka deyişle Ukrayna'daki savaşın akıbeti, hâlihazırda ağırlıklı olarak özel-ticari bir firma tarafından sağlanan hizmetlere bağımlıdır.[36] Dolayısıyla enformasyon paylaşımı ve OSINT çerçevesinde, kamu/savunma çevreleri ve sivil/ticari sektör ile ortak faydaya dayalı bir bağ geliştirilmesi önem arz etmektedir.

Fotoğraf 7: Rus Yığınakları, Ejderha Dişleri ve Siperleri[37]



Kaynak: Skywatch, Planet, 2023 (Son güncelleme 11 Mart 2025).

Fotoğraf 8: Mykhailivka Bölgesindeki Rus Yığınaklarının Uydu Görüntüsü[38]

Kaynak: Skywatch, Planet, 2023.

SAVUNMA İSTİHBARATINDA OSINT YAKLAŞIMININ GELECEĞİ VE OLASILIKLAR

Yapay zekânın gelişmesi, askerî OSINT'in hâlihazırdaki dijital yapısında önemli değişimlere sebep olmaktadır. Bahse konu dönemde, makine öğrenimi (machine learning), otomatik mantık yürütme (automated reasoning) ve semantik web (semantic web) gibi yeni teknolojilerin askerî veri analizine entegrasyonu öne çıkmaktadır.

İkinci nesil OSINT, yukarıda bahsedilen sosyal medya kaynaklı kanalların sunduğu dinamik web sayfaları ve kullanıcıların paylaşımına dayanan "insan merkezli" (human-centric) içeriklerle beslenmektedir. Üçüncü nesil OSINT ise yapay zekâ destekli teknolojilerin verileri doğrudan ve dolaylı bir şekilde işleyebilmesiyle farklılaşmaktadır. İlerleyen yıllarda yapay zekâ destekli teknolojilerin, askerî OSINT'i yeni bir boyuta taşıyacağı değerlendirilmektedir.

Mezkûr gelişmeler, verinin hacmini ve hızını artırmakta olup özellikle canlı video yayıncılığının (live video broadcasting) artışı, gerçek zamanlı olay farkındalığı sağlamaktadır. Ancak bu tür büyük veri setlerinin işlenebilmesi için bilgisayar destekli analizlere (machine learning algorithms, automated systems) ihtiyaç duyulmaktadır. Hâlihazırda internet tabanlı bazı kullanımların veya açık kaynaklı web sitelerinin hassas güvenlik bilgilerini içeren faaliyetleri işlemek için kullanılması bile önemli güvenlik zafiyetlerine sebebiyet vermektedir. 2021 yılında önde gelen açık kaynaklı savunma istihbarat analizi kurumu Bellingcat'in, ABD askerlerinin gizli nükleer bilgileri çevrim içi platformlarda çalışma notlarına döktüğünü açığa çıkarması, söz konusu çerçevede en kritik örneklerden biridir.[39]

Üçüncü nesil OSINT yalnızca istihbarat analizine değil, aynı zamanda istihbarat operasyonlarına (intelligence operations) yönelik yeni fırsatlar da sunmaktadır. Örneğin artırılmış gerçeklik (augmented reality, AR) ve giyilebilir teknolojiler (wearable devices) gibi yenilikler, hedefleme (targeting) ve HUMINT operasyonlarında devrim yaratma potansiyeline sahiptir. Google Glass gibi giyilebilir cihazlar ve dijital verilerin fiziksel dünya üzerine yerleştirilmesini sağlayan artırılmış gerçeklik teknolojilerinin, istihbarat operasyonlarını önemli ölçüde geliştirebileceği değerlendirilmektedir. Ayrıca psikometrik analizler (psychometrics), bireysel davranışları tahmin etmek için kullanılan veriye dayalı psikoloji, OSINT ve psikolojik savaş (psychological operations) arasındaki sınırları daha da bulanıklaştırmaktadır. 2018 yılında Cambridge Analytica'nın kamuya açık verilerden bireylerin siyasi davranışlarını tahmin edebilme yeteneğini geliştirmesi, istihbarat operasyonlarının yeni sınırlarına dair önemli bulgular sunmakta ayrıca yeni dönem OSINT'in etik ve hukuki boyutlarını da gündeme getirmektedir.[40]

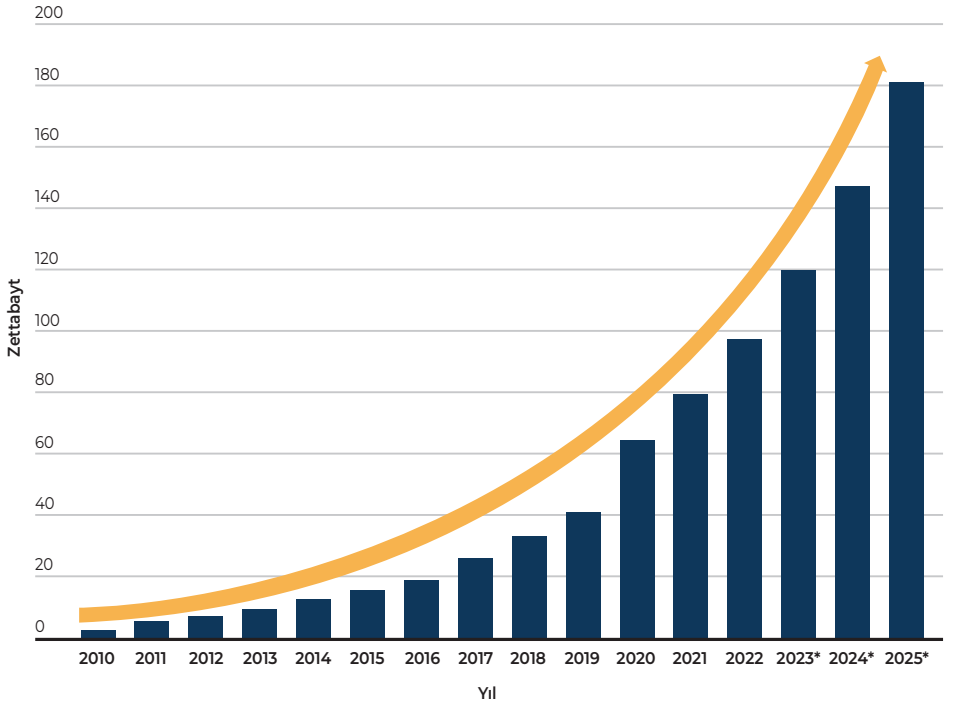
Şifreleme (encryption), üçüncü nesil OSINT'in bir diğer belirleyici özelliğidir. Uçtan uca şifreleme (end to end encryption) kullanımı giderek yaygınlaşırken OSINT'e erişim ve analiz etme kabiliyeti büyük bir zorlukla karşı karşıya kalmaktadır. Ancak şifreleme teknolojilerinin daha yaygın hâle gelmesi, sınırların bulanıklaşmasına yol açmaktadır. Söz konusu durumun önümüzdeki yıllarda ilgili birimler içerisinde askerî kripto analizi için yeni yöntemlerin geliştirilmesini zorunlu kılması muhtemeldir.

ABD Dışişleri Bakanlığının Mayıs 2024'te yayımlanan OSINT stratejisine göre devletlerin modern ve geleceğe dönük askerî OSINT planlamaları "teknoloji/veri yönetimi, uzman personel ve etik sorumluluk ve iş birliği ile operasyonel entegrasyon" olmak üzere üç temel sütun üzerine inşa edilmelidir.[41]

İlk olarak yukarıda bahsedilen hızlı ve yüksek miktarlı kamuya açık ve ticari verilerin sistematik şekilde toplanması, merkezî veri havuzlarında sınıflandırılması ve analiz edilebilir hâle getirilmesi gerekmektedir. Bu çerçevede bahse konu altyapının geliştirilmesi kritiktir. Modern harp ve askerî planlama ortamında, sosyal medya ve açık kaynaklardan gelen bilgilerin gerçek zamanlı izlenmesi ve aksiyon merkezli bir şekilde işlenebilmesinin, askerî karar süreçlerine çeviklik kazandıracağı öngörülmektedir. Mezkûr teknoloji destekli OSINT analizi yapısı, siber güvenlik sistemleriyle entegre edildiğinde hem bilgi güvenliği hem de operasyonel istikrar sağlanacaktır.

Üçüncü nesil askerî OSINT kapsamında detaylandırıldığı üzere yapay zekâ ve makine öğrenimi, bu büyük veri setlerinin hızlı ve isabetli şekilde işlenmesi konusunda en önemli faktörlerden biridir. Nitekim 2019 yılından sonra küresel ölçekte toplanan, işlenen ve tüketilen veri oranı büyük bir hızla artmaktadır. Söz konusu eğilim, bu verilerin karar mekanizmalarına destek olabilmesi için anlamlı ve verimli bir veri işleme sisteminin önemini vurgulamaktadır. Bazı değerlendirmelere göre 2025 yılı itibarıyla dünya genelinde erişilebilir veri miktarının 180 zettabaytı aşması önemlidir. Bu düzey, 2020 yılında 64,2 zettabayt olarak kaydedilen veri miktarının neredeyse üç katına tekabül etmektedir.[42]

Grafik 5: Dünya Genelinde Oluşturulan, Toplanan, Kopyalanan ve Tüketilen Veri Hacmi[43]



Modern savunma istihbaratı ve bu kapsamda askerî OSINT'in etkinliği, bahse konu alanda çalışacak uzman personelin kalitesine ve farkındalığına bağlıdır. Askerî OSINT alanında çalışan analistlerin yalnızca teknik becerilere değil; kaynak doğrulama, dezenformasyon analizi, dijital gizlilik, kişisel verilerin korunması ve uluslararası hukuk bilgisine de sahip olması gerekmektedir. Bu sebeple devletler, gerekli veri işleme altyapısının yanı sıra OSINT personeli için zorunlu eğitim programları oluşturmalı; sahaya özgü vaka analizleriyle uygulamalı yetkinlik geliştirmeli ve etik kodlar çerçevesinde hareket etmelerini sağlamalıdır. Senaryo bazlı eğitimler ve veri doğrulamaya dair kriz yönetimleri, söz konusu çerçevede ayrıca önemlidir.

Son olarak bir ülkedeki OSINT kapasitesinin güçlenmesi "özel sektör, üniversiteler, düşünce kuruluşları, teknoloji şirketleri, start-up'lar ve müttefik ülkelerle" yapılacak çok yönlü iş birlikleriyle mümkündür. Kamu ve özel sektör arasında bir teknoloji ve inovasyon köprüsü görevi görebilecek olan bu iş birliklerinin, savunma gibi özel sektöre kıyasla daha yavaş değişen alanlarda inovasyonu hızlandırması muhtemeldir.

Nitekim kamu sektörüne göre çok daha yenilikçi ve uyarlanabilir fikirlere sahip olan start-up/özel sektör zemini; mobil uygulamalar, interaktif veri paylaşım teknolojileri ve kullanıcı dostu analiz platformları sayesinde OSINT'i sadece siyasi/askerî karar alıcıların değil, sahada görev yapan operasyonel ve taktik seviyede personelin de aktif olarak kullanabileceği bir araca dönüştürmektedir. ABD'nin değerlendirmelerine göre günümüzde askerî analizler çerçevesinde OSINT yalnızca destekleyici bir unsur olarak kalmamakta, aynı zamanda modern askerî stratejilerin temel bileşenlerinden biri hâline gelmektedir.

Ukrayna askerî istihbaratının ve kritik askerî birliklerinden 414. Taarruzi SİHA Tugayının en temel kamuoyu paylaşımlarını X, Telegram, Signal ve Facebook gibi kanallardan sağladıkları müşahede edilmektedir.

Öte yandan özel sektörün modern askerî OSINT ekosistemindeki rolü, Birleşik Krallık'ın önde gelen düşünce kuruluşu Royal United Services Institute (RUSI) tarafından da incelenmiştir. Bellingcat gibi kuruluşlar, 2014'ten bu yana OSINT'in somut sonuç alabilme zeminini gözler önüne sermiştir.[44] Bahse konu kurumlar, Ukrayna yakınlarındaki Rus askerî hareketliliğini izlemekten Kuzey Kore'nin yaptırımları atlatmasına kadar çeşitli olaylarda da yenilikçi veri analiz yöntemleriyle sahada devlet dışı OSINT'in etkili bir örneğini sunmuştur. Modern enformasyon ortamındaki en önemli tehditlerden biri olan dezenformasyon ile mücadelede de önemli roller oynamışlardır. Dolayısıyla önümüzdeki dönemde özel sektör ekosistemi ve kamu sektörü arasında OSINT ve veri paylaşımı konusundaki iş birliği, giderek daha kritik olacaktır.

NATO'nun en önemli stratejik birimlerinden biri olan Allied Command Transformation'in (ACT) değerlendirmelerine göre OSINT planlaması, bugünün küresel enformasyon ortamını daha iyi anlamak ve karar alma süreçlerini iyileştirmek amacıyla yeniden yapılandırılmalıdır.[45] Bahse konu yeni değerlendirmelere göre NATO'nun ihtiyacı olan sistem; kullanıcı dostu arayüzü, entegre veri yönetimi, öngörücü analiz yetenekleri, görsel raporlama araçları ve operasyonel OSINT'i tek bir platformda birleştiren kapsamlı bir yapıdır. Bu sistem çerçevesinde; nitelikli insan kaynağı, standartlaşmış süreçler ve uyarlanabilir teknolojik araçlar olarak özetlenebilen üç temel bileşen öne çıkmaktadır.

Bu kapsamda OSINT analistlerinin; veriyi okumakla birlikte anlamlandırma, modelleme ve operasyonel bağlama oturtma yetkinliğine sahip olması gerekmektedir. NATO ACT'nin değerlendirmelerine göre bu çerçevede gerekli niteliklere ve becerilere sahip uzmanlar, teknolojik araçları kullanmakla kalmayıp aynı zamanda bilgi güvenliği, kaynak güvenilirliği ve etik sınırlar konusunda da yetkin olmalıdır. Askerî/stratejik karar alıcılar ile aynı yapılar içerisinde çalışabilen bahse konu analistler, farklı kaynaklardan gelen verileri anlamlı bütünlere dönüştürerek karar vericilere zamanında ve etkili destek sağlamalıdır.[46] Sonuç olarak NATO'nun gelecekteki OSINT yapılanması "insan, süreç ve araçların" senkronize bir şekilde çalıştığı, bilgi ortamını anlama ve yönlendirme kabiliyetini artıran bütüncül bir yapıda kurgulanmalıdır. Bu yapı sadece istihbarat üretimini değil, aynı zamanda stratejik kararları destekleyen canlı bir analiz kapasitesini de beraberinde getirmelidir.

Merkezî İstihbarat Teşkilatı (CIA) gibi bazı stratejik kurumlar, önümüzdeki dönemde "OSINT Analizi Birimi" kurulmasına dair çalışmalar yapmaktadır. CIA'in "A Case for an Open Source Agency" başlıklı raporunda önerilen OSINT birimi; yalnızca istihbarat toplamakla sınırlı olmayan, aynı zamanda stratejik analiz ve politika yapımını doğrudan destekleyen bağımsız bir kurum modeli üzerine inşa edilmelidir.[47]

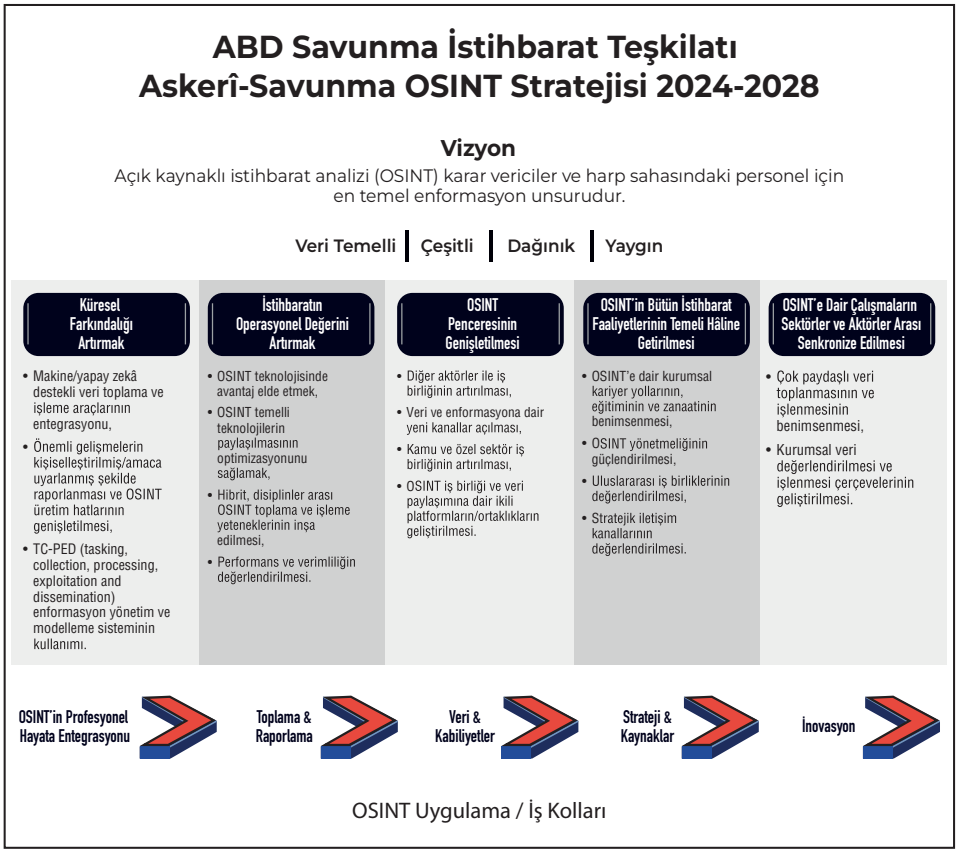
Rapora göre söz konusu yapı devletin tüm kurumlarına, farklı alanlarda hizmet verebilecek şekilde organize edilmeli; akademi, özel sektör ve medya gibi dış kaynak ekosistemi ile sürekli etkileşim içinde olmalıdır. Bu kurumun amacı, açık kaynaklardan elde edilen bilgileri hızlı, şeffaf ve doğru analiz ederek karar alıcıların kullanımına anlaşılabilir bir biçimde sunmak olmalıdır.

Önerilen OSINT teşkilatı, mevcut istihbarat kurumlarının tamamlayıcısı olarak değil, onları destekleyen ve açık kaynakları kurumsal bir yetkinlikle işleyen bağımsız bir otorite olarak konumlanmalıdır. Teknolojik altyapısı güçlü olmalı; büyük veri, yapay zekâ ve bilgi görselleştirme gibi modern araçlarla donatılmalıdır. Bahse konu kurumun en önemli özelliklerinden biri ise kamu kullanımına açık kaynaklar ile çalışmasıdır. Kapalı/gizli kaynaklara dayanmayan çalışmalarıyla demokratik denetime daha açık ve hesap verebilir bir yapıya sahip olacak bu kurumun, enformasyon merkezli askerî/stratejik karar alma süreçlerinde merkezî bir rol oynayacağı öngörülmektedir.

ABD'nin 2024-2028 OSINT stratejisinde, modern askerî savunma istihbaratının temel taşlarına dair önemli ipuçları sunulmaktadır. Buna göre bir devletin OSINT stratejisi beş temel hedeften oluşmalıdır:

1. Karar alıcılar ve sahadaki askerlere durumsal farkındalığı artıracak, kişiselleştirilmiş OSINT verilerini sunmak,
2. OSINT'in (aksiyonel) enformasyon değerini en üst seviyeye çıkarmak,
3. Kamunun stratejik birimlerindeki OSINT kapasitesini artırmak,
4. OSINT'i bütün ilgili disiplinlerin temelinde konumlandırmak ve
5. OSINT'i diğer kamu ve sivil enformasyon kaynaklarıyla senkronize hâle getirmek.[48]

Şekil 1: Askerî-Savunma OSINT Stratejisi 2024-2028



SONUÇ

SONUÇ

OSINT'in gizlilik derecesi konusunda diğer istihbarat türlerine kıyasla çok daha geniş bir zemine yayılan doğası, istihbarat servisleri kadar düşünce kuruluşlarının ve özel istihbarat kurumlarının da siyasa yapımında ve istihbarat analizinde etkin rol oynamasına neden olmuştur. Dolayısıyla gelecek on yıllarda ülkelerin veri işleme kapasitelerinin, siyasalarının etkinliğinde önemli rol oynayacağı değerlendirilmektedir.

Analizde detaylı olarak değerlendirildiği üzere hâlihazırdaki enformasyon ortamında yaşanan hızlı dijitalleşme, istihbarat teknolojilerinin ticari imkânlarla yaygınlaşması ve yükselen veri hacmi gibi temel analitik enformasyon imkânları birleştiğinde, Soğuk Savaş yıllarında çok yüksek gizlilik derecesine sahip askerî bilgilerin günümüzde kamuya açık kaynaklarla analiz edilebildiği ve yayımlanabildiği bir denklem ortaya çıkmaktadır. Başka bir ifadeyle herhangi bir ülkeye dair uydu görüntüleri verilerinin, askerî envanterinin niteliklerinin, dış ve güvenlik siyasasına dair siyasi/askerî değerlendirmelerin yasal sınırlılıklar içinde kalarak ve nispi olarak düşük bütçelerle elde edilmesi mümkündür. Söz konusu denklem, bir yandan hedef ülke ve grupların askerî kapasitelerinin, envanterlerinin ve doktrin esaslarının kapalı bir espiyonaj çalışmasına gerek kalmaksızın izlenmesini, stratejik ve operasyonel seviyelerde mümkün kılmaktadır. Diğer yandan ülkenin savunma alımlarını, tatbikatlarını, geliştirdiği konseptleri, silahlı kuvvetlerinin harbe hazırlık seviyesini giderek dış dünyaya daha çok açmaktadır. Taktik seviyede somut bulgular ve belgeler elde edebilmek için HUMINT'in öneminin yadsınması da mümkün değildir.

Enformasyon ortamındaki dönüşümün beraberinde getirdiği Web 2.0, günümüz OSINT imkânlarını savunma istihbaratında mümkün kılmıştır. Diğer yandan yapay zekânın denkleme dâhil olması, analist havuzuna insan dışında başka bir varlık ekleyerek askerî OSINT 3.0'a gidecek bir yönelim çizmektedir.

Dünyada stratejik ajandanın hızla askerîleşmesiyle birlikte savunma konularının kazandığı önem açıktır. Önümüzdeki dönemde gerek istihbarat servisleri gerekse de ülkelerin entelektüel kapitalini oluşturan strateji ve iş çevrelerinin savunma istihbaratı alanında OSINT kabiliyeti, ülke siyasasının doğru belirlenmesi ve gerekli etkinlikle uygulanmasında kritik bir rol oynayacaktır.

KAYNAKÇA VE NOTLAR

KAYNAKÇA VE NOTLAR

[1] United Kingdom Government, The Strategic Defence and Security Review: Securing Britain in an Age of Uncertainty (London: United Kingdom Government, 2010) Erişim Adresi: https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty [Erişim Tarihi: 25 Mayıs 2025].

[2] North Atlantic Treaty Organization, NATO 2022 Strategic Concept (Brüksel: NATO, 2022), Erişim Adresi: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf [Erişim Tarihi: 25 Mayıs 2025].

[3] North Atlantic Treaty Organization, "NATO Adopts New Strategic Concept," NATO, 19 Kasım 2010 Erişim Adresi: https://www.nato.int/cps/en/natohq/news_68172.htm [Erişim Tarihi: 25 Mayıs 2025].

[4] Stockholm International Peace Research Institute (SIPRI), "Unprecedented Rise in Global Military Expenditure as European and Middle East Spending Surges," SIPRI, 28 Nisan 2025 Erişim Adresi: https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges [Erişim Tarihi: 25 Mayıs 2025].

[5] Brady Africk, "Russian forces in Ukraine continue to expand defenses along the front line. This updated map shows many of Russia's new fortifications and links to the full interactive version," X (eski adıyla Twitter), 10 Haziran 2024 Erişim Adresi: https://x.com/bradyafr/status/1800244923603542038 [Erişim Tarihi: 25 Mayıs 2025].

[6] Africk, Brady. "Russian forces in Ukraine continue to expand defenses along the front line. This updated map shows many of Russia's new fortifications and links to the full interactive version." X, 10 Haziran 2024. Erişim Adresi: https://x.com/bradyafr/status/1800244923603542038 [Erişim Tarihi: 25 Mayıs 2025].

[7] Statista. *Worldwide Digital Population 2025*. Erişim Adresi: https://www.statista.com/statistics/617136/digital-population-worldwide/ [Erişim Tarihi: 17 Mayıs 2025].

[8] Felix Richter, "Charted: There Are More Mobile Phones Than People in the World," *World Economic Forum*, 11 Nisan 2023, Erişim Adresi: https://www.weforum.org/stories/2023/04/charted-there-are-more-phones-than-people-in-the-world/ [Erişim Tarihi: 25 Mayıs 2025].

[9] Howarth, Josh. "How Many People Own Smartphones? (2024–2029)." *Exploding Topics*, 24 Nisan 2025. Erişim Adresi: https://explodingtopics.com/blog/smartphone-stats [Erişim Tarihi: 25 Mayıs 2025].

[10] Statista, "2005'ten 2023'e Dünya Genelinde İnternet Kullanıcısı Sayısı," son güncelleme 2024, Erişim Adresi: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[11] Howarth, Josh. "How Many People Own Smartphones? (2024–2029)." *Exploding Topics*, 24 Nisan 2025. Erişim Adresi: https://explodingtopics.com/blog/smartphone-stats [Erişim Tarihi: 25 Mayıs 2025].

[12] Defense Intelligence Agency, *Open Source Intelligence (OSINT) Strategy 2024–2028* (Washington, D.C.: Department of Defense, October 23, 2023), Erişim Adresi: https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf

[13] Peter Layton, *Algorithmic Warfare: Applying Artificial Intelligence to Warfighting* (Canberra: Air Power Development Centre, 2018), Erişim Adresi: https://airpower.airforce.gov.au/sites/default/files/2021-03/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf [Erişim Tarihi: 25 Mayıs 2025].

[14] Fabio Duarte, "Amount of Data Created Daily (2025)," *Exploding Topics*, 24 Nisan 2025, Erişim Adresi: https://explodingtopics.com/blog/data-generated-per-day [Erişim Tarihi: 25 Mayıs 2025].

[15] Fabio Duarte, "Amount of Data Created Daily (2025)," *Exploding Topics*, 24 Nisan 2025, Erişim Adresi: https://explodingtopics.com/blog/data-generated-per-day [Erişim Tarihi: 25 Mayıs 2025].

[16] Guy Plopsky, "A photo recently posted on the 'warhistoryalconafter' Telegram channel showing a VKS Ka-52M armed with a pair of infrared-guided 9M39 missiles," X, 19 Mayıs 2025, Erişim Adresi: https://x.com/GuyPlopsky/status/1924525498224513165 [Erişim Tarihi: 25 Mayıs 2025].

[17] Birleşik Krallık Hükûmeti, Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, Cm 7948 (Ekim 2010) Erişim Adresi: https://assets.publishing.service.gov.uk/media/5a78da-21ed915d0422065d95/strategic-defence-security-review.pdf [Erişim Tarihi: 25 Mayıs 2025].

[18] Matthew P. Funaiole, Brian Hart ve Aidan Powers-Riggs, "Murky Waters: Navigating the Risks of China's Dual-Use Shipyards," *Center for Strategic and International Studies (CSIS)*, 25 Mart 2025, Erişim Adresi: https://features.csis.org/hiddenreach/china-shipyard-tiers/ [Erişim Tarihi: 25 Mayıs 2025].

[19] TRADOC G-2, "Smart Phones Playing Prominent Role in Russia-Ukraine War," *U.S. Army Training and Doctrine Command G-2 Operational Environment Enterprise*, 2025, Erişim Adresi: https://oe.tradoc.army.mil/product/smart-phones-playing-prominent-role-in-russia-ukraine-war/ [Erişim Tarihi: 25 Mayıs 2025].

[20] Lockheed Martin, "Search Results for 'Intelligence Analysis'," Lockheed Martin Careers, Erişim Adresi: https://www.lockheedmartinjobs.com/search-jobs?acm=ALL&alrpm=6252001,4566966&ascf=%5b%7B%22key%22:%22is_manager%22,%22value%22:%22Intelligence+Analysis%22%7D%5d [Erişim Tarihi: 25 Mayıs 2025].

[21] Birleşik Krallık Savunma Bakanlığı [@DefenceHQ], "Latest Defence Intelligence update on the situation in Ukraine – 19 May 2025," *X*, 19 Mayıs 2025, Erişim Adresi: https://x.com/DefenceHQ/status/1924397803838607778 [Erişim Tarihi: 25 Mayıs 2025].

[22] U.S. Africa Command, "Russia and the Wagner Group Continue to Be Involved in Ground, Air Operations in Libya," *U.S. Africa Command*, 24 Temmuz 2020 Erişim Adresi: https://www.africom.mil/pressrelease/33034/russia-and-the-wagner-group-continue-to-be-in [Erişim Tarihi: 25 Mayıs 2025].

[23] Defence Intelligence of Ukraine [@DI_Ukraine], *X*, Erişim Adresi: https://x.com/DI_Ukraine [Erişim Tarihi: 25 Mayıs 2025].

[24] Defence Intelligence of Ukraine, "WAR&SANCTIONS: Registration for the International OSINT Hackathon Closes Tomorrow," Defence Intelligence of Ukraine, 20 Mayıs 2025, Erişim Adresi: https://gur.gov.ua/en/content/warsanctions-reiestratsiia-na-mizhnarodnyi-khakaton-dlia-osintrozsliduvachiv-zavershuietsia-zavtra [Erişim Tarihi: 25 Mayıs 2025].

[25] Birleşik Krallık Savunma Bakanlığı [@DefenceHQ], "Latest Defence Intelligence update on the situation in Ukraine – 14 May 2025," *X*, 14 Mayıs 2025, Erişim Adresi: https://x.com/DefenceHQ/status/1922585910610133147 [Erişim Tarihi: 25 Mayıs 2025].

[26] A.g.e.

[27] Defence Intelligence of Ukraine [@DI_Ukraine], "Registration for the international OSINT hackathon is closing soon," *X*, 20 Mayıs 2025 Erişim Adresi: https://x.com/DI_Ukraine/status/1924755159717994559 [Erişim Tarihi: 25 Mayıs 2025].

---

[28] U.S. Africa Command, "Russia and the Wagner Group Continue to Be Involved in Ground, Air Operations in Libya," *U.S. Africa Command*, 24 Temmuz 2020, Erişim Adresi: https://www.africom.mil/pressrelease/33034/russia-and-the-wagner-group-continue-to-be-in [Erişim Tarihi: 25 Mayıs 2025].

[29] Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise, RAND, 17 Mayıs 2025, Erişim Adresi: https://www.rand.org/pubs/research_reports/RR1964.html

[30] Defense News, *Defense News*, erişim 25 Mayıs 2025, Erişim Adresi: https://www.defensenews.com/

[31] Higgins, Eliot. "The Chemical Munitions Used By the Syrian Government 2012–2018." Bellingcat, 14 Haziran 2018. Erişim Adresi: https://www.bellingcat.com/news/mena/2018/06/14/chemical-munitions-used-syrian-government-2012-2018/ [Erişim Tarihi: 25 Mayıs 2025].

[32] Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise, RAND, 17 Mayıs 2025, Erişim Adresi: https://www.rand.org/pubs/research_reports/RR1964.html

[33] Data triangulation (veri üçlemesi ya da veri üçgenlemesi); bir konuyu, durumu ya da olguyu daha güvenilir kılmak için birden fazla veri kaynağının bir arada kullanılmasıdır. Veri üçlemesi özellikle sosyal bilimlerde, eğitim araştırmalarında, kalite araştırmalarında ve analizlerde; veri doğrulama ve görüşleri çeşitlendirme amacıyla kullanılmaktadır.

[34] Suchomimus, *High Quality Satellite Imagery Russian Defensive Position in Novotroitske, Near Crimea*, YouTube video, 2023, Erişim Adresi: https://www.youtube.com/watch?v=KB-n79HKcU8

[35] Sinéad Baker ve Mia Jankowicz, "US Block on Maxar Satellite Images Effectively Blinds Ukraine's Drone Pilots," *Business Insider*, 7 Mart 2025, Erişim Adresi: https://www.businessinsider.com/maxar-pulling-satellite-imagery-will-hurt-ukraines-drone-abilities-pilot-2025-3

[36] Mathieu Pollet, "Ukraine is stuck with Musk's Starlink for now," *Politico.eu*, 7 Nisan 2025, Erişim Adresi: https://www.politico.eu/article/ukraine-stuck-with-elon-musk-starlink-satellite-internet/

[37] Brady Africk, "Russian Field Fortifications in Ukraine," *Brady Africk* (Substack), 19 Mayıs 2024, Erişim Adresi: https://read.bradyafrick.com/p/russian-field-fortifications-in-ukraine

[38] Seth G. Jones, Alexander Palmer ve Joseph Bermudez Jr., "Ukraine's Offensive Operations: Shifting the Offense-Defense Balance," *Center for Strategic and International Studies*, Haziran 2023, Erişim Adresi: https://www.csis.org/analysis/ukraines-offensive-operations-shifting-offense-defense-balance

[39] Foeke Postma, "ABD Askerleri, Nükleer Silah Sırlarını Flashcard Uygulamalarıyla Ortaya Çıkardı," *Bellingcat*, 28 Mayıs 2021, Erişim Adresi: https://www.bellingcat.com/news/2021/05/28/us-soldiers-expose-nuclear-weapons-secrets-via-flashcard-apps/

[40] Cambridge Analytica: how did it turn clicks into votes?, The Guardian, 6 Mayıs 2018, Erişim Adresi: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

[41] Açık Kaynaklı İstihbarat Stratejisi, ABD Disisleri Bakanlığı, Mayıs 2024, Erişim Adresi: https://www.state.gov/wp-content/uploads/2024/05/INR-Open-Source-Intelligence-Strategy.pdf

[42] Statista, *Worldwide Data Created, Captured, Copied, and Consumed 2010–2025*, Erişim Adresi: https://www.statista.com/statistics/871513/worldwide-data-created/ [Erişim Tarihi: 17 Mayıs 2025].

[43] Jack Stubbs ve Jamie Collier, *The Future of Open Source Intelligence: Insights for the Defence and Security Community* (Londra: Royal United Services Institute, 2022), Erişim Adresi: https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf [Erişim Tarihi: 17 Mayıs 2025].

[44] A.g.e.

[45] NATO Allied Command Transformation. Request for Information: OSINT Exploitation Capability. Norfolk, VA: NATO ACT, Mayıs 2023. Erişim Adresi: https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059_qa1a.pdf

[46] A.g.e.

[47] Gregory F. Treverton, *A Case for an Open Source Agency* (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence), Erişim Adresi: https://www.cia.gov/resources/csi/static/582de039146e-9d5636f6ca3a5b48a656/Article-A-Case-for-an-Open-Source-Agency.pdf [Erişim Tarihi: 17 Mayıs 2025].

[48] Defense Intelligence Agency, *Open Source Intelligence (OSINT) Strategy 2024–2028* (Washington, D.C.: Department of Defense, October 23, 2023), Erişim Adresi: https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf

NOTLAR

MODERN SAVUNMA İSTİHBARATI VE AÇIK KAYNAKLI İSTİHBARAT (OSINT) YAKLAŞIMI

HAZİRAN 2025