DEPARTMENT OF DEFENSE

OSINT STRATEGY 2024–2028

OSINT is the premier source of intelligence information for decisionmakers and warfighters.

October 23, 2023

This page intentionally left blank.

DEPARTMENT OF DEFENSE

OSINT STRATEGY 2024–2028

OSINT is the premier source of intelligence information for decisionmakers and warfighters.

This page intentionally left blank.

Table of Contents

Foreword 5

Administration 7

Executive Summary 11

Strategic Goals and Objectives Overview 13

Open Source Challenges and Opportunities 15

Strategic Goals and Enabling Objectives 21

Strategic Goal 1: Enhance decisionmaker and warfighter situational awareness through timely delivery of customized, serialized OSINT products and data 21

Strategic Goal 2: Maximize the intelligence value of open source information 21

Strategic Goal 3: Expand the open source aperture internally and externally 22

Strategic Goal 4: Establish OSINT as a premier intelligence capability and the foundation for all other disciplines 24

Strategic Goal 5: Synchronize OSINT with all other Publicly and Commercially Available Information (PAI/CAI) activities 25

References 26

LTG Scott D. Berrier
22nd Director
Defense Intelligence Agency

Alan S. MacDougall, PhD
Director, Science & Technology, DIA/ST
DIEM for OSINT (delegated)

Brad H. Ahlskog
Chief, OSINT Integration Center, DIA/ST
Chair, Defense Open Source Council

Foreword

In 3 decades since the creation of the first website, the Internet has grown to well over one billion sites. Four and a half billion users access 200 million active websites every day. The global digital data environment doubles in size every 2 years. Technology-enabled devices track and monetize all aspects of the human experience. Within the U.S. Government, Open Source Intelligence (OSINT) has evolved substantially since the establishment of the Open Source Center (OSC) in 2005. The fast pace of the ongoing technology revolution poses significant challenges for a growing community of collection activities across the Defense Intelligence Enterprise (DIE).

In 2012, the Defense Intelligence Agency (DIA) published the first U.S. DoD OSINT strategy. Since then, DoD OSINT has proven its unique value as a primary source of intelligence during multiple crisis situations.

This strategy will strengthen the DoD OSINT community and enable a true enterprise approach oriented squarely on the intelligence challenges posed by strategic competition. The central idea is to drive up the intelligence value of OSINT by unifying collection and reporting, integrating advanced technologies, and professionalizing the workforce.

Operating on behalf of the Director, DIA, as the Defense Intelligence Enterprise Manager (DIEM) for OSINT, the Defense Open Source Council (DOSC) will collaborate to set standards, track progress, and synchronize activities. We call on all Defense Intelligence Enterprise components to rise to the challenges ahead to fulfill our vision of OSINT as the "first resort" source of intelligence for decision makers and warfighters.

Administration

This strategy updates and replaces the 2012–2017 DoD OSINT Strategy. It applies to Department of Defense components at all echelons or organizational levels that have OSINT programs and activities.

The goals, objectives, and underlying methodologies for strengthening OSINT are widely applicable to all foreign partner engagements.

The requirement for a DoD OSINT strategy is established in Department of Defense Instruction 3115.12, Open Source Intelligence, which also establishes the Defense Intelligence Agency (DIA) as the lead component for OSINT. In December 2021, the Under Secretary of Defense for Intelligence & Security further designated the Director, DIA as the Defense Intelligence Enterprise Manager (DIEM) for OSINT. The DIEM-OSINT designation was codified as department policy in DoD Directive 5105.21 by the Deputy Secretary of Defense on January 25, 2023.

DIA is also tasked to lead the Defense Open Source Council (DOSC), defined in policy as the primary governance mechanism for DoD OSINT. Among the list of DOSC responsibilities is the task to establish an OSINT strategy.

The Director, DIA, tasked the Open Source Intelligence Integration Center (OSIC) to lead execution of the Agency's DOSC and DIEM responsibilities. The Chief, OSIC also serves Chair of the DOSC, and provides primary staff secretariat support that drives the DOSC agenda.
.

The Defense Open Source Council (DOSC)

Is the primary governance body for Defense OSINT and serves as a forum for the coordination and facilitation of Defense OSINT activities and programs.

Advises and reports to the DIEM for OSINT and the DIE OSINT Board of Governors on Defense issues and recommends initiatives to improve the effectiveness and efficiency of Defense OSINT programs, activities, and systems.

Coordinates activities and resolves Defense OSINT issues programs and activities including Tradecraft, Training, Policy, Tools, and Data.

Coordinates Defense OSINT recom-mendations and activities with the National Open Source Committee (NOSC).

Establishes and maintains a Defense OSINT strategy to guide the full range of Defense OSINT efforts.

Reports to the DIEM for OSINT and the DIE OSINT BoG on issues, performance metrics, and resource recommendations, and identifies matters for BoG decision and direction.

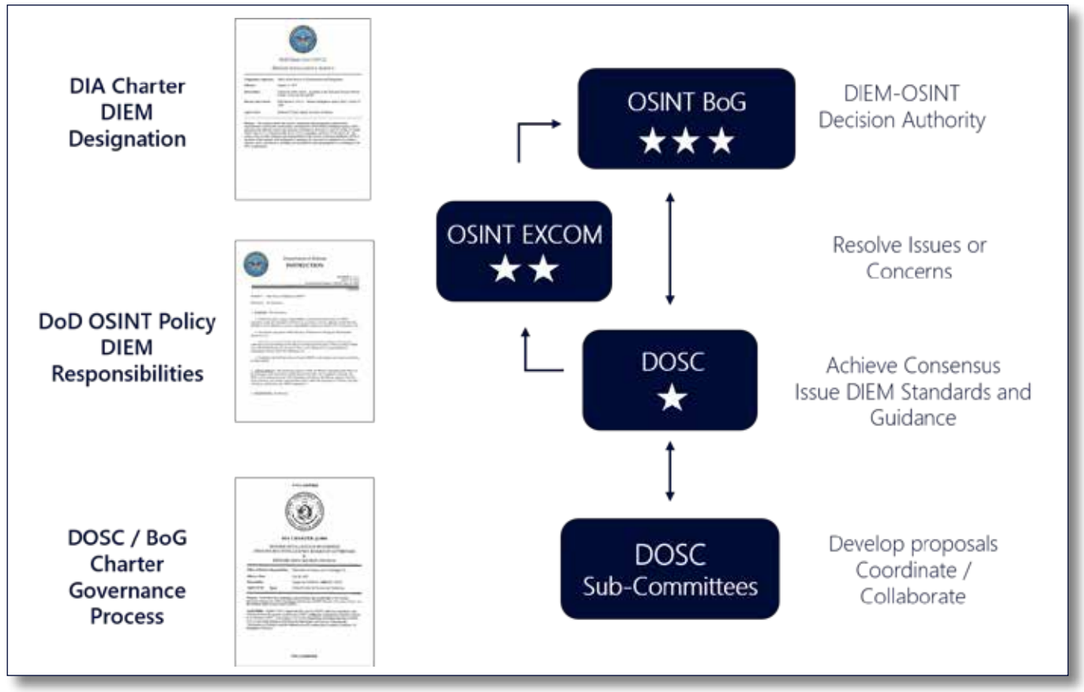
—DIA Charter 22-004

All DoD components with OSINT programs provide representation to the DOSC. DOSC members represent their components and serve as a two-way conduit of information for developing and disseminating OSINT guidelines, standards, and procedures.

The DOSC is the primary governance body for Defense OSINT, and serves as a forum for coordination and facilitation of Defense OSINT activities and programs at the working and action officer levels.

The DOSC advises and reports to the DIEM-OSINT and the DIE OSINT Board of Governors (BoG) on issues, performance metrics, and resource recommendations; and identifies matters for BoG decision and direction.

The OSINT BoG assesses and prioritizes Defense OSINT activities and capabilities, integrates OSINT Community perspectives, and promotes a unified approach to Defense OSINT. The DIEM for OSINT may convene a Defense OSINT Executive Committee (EXCOM) to address specific issues that do not require the attention of the BoG.



OSINT Governance Overview

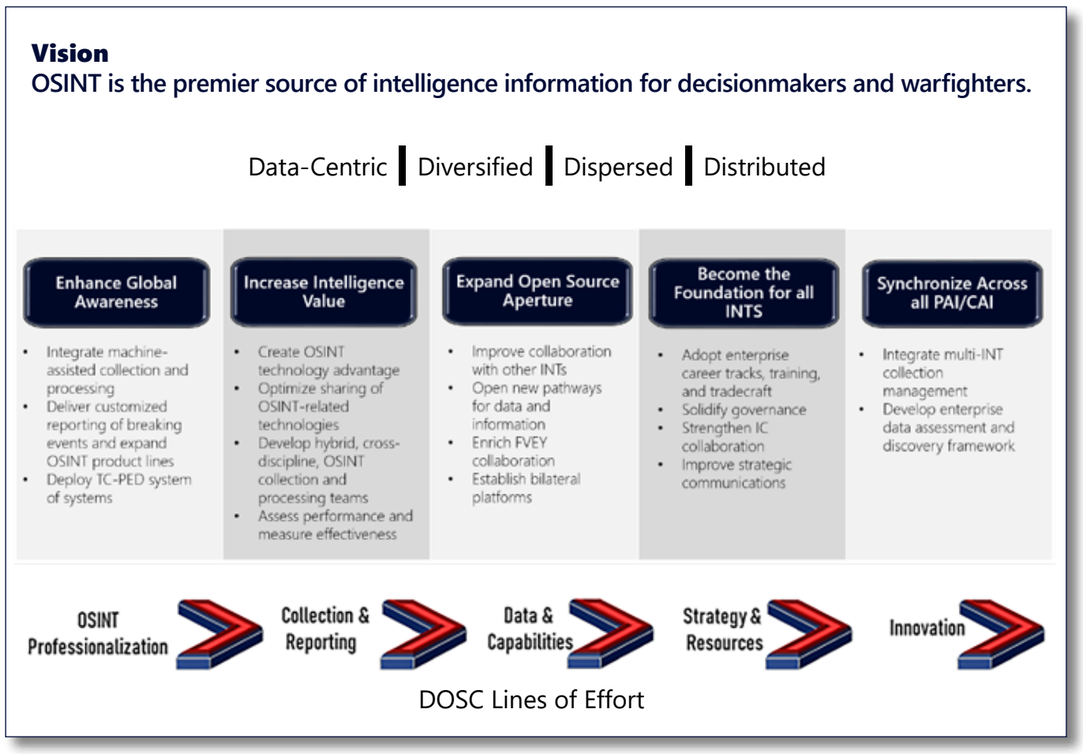
◀ USSOUTHCOM leverages OSINT to expand multilateral partner nation collaboration. Captain Nickalious Beaumont (Jamaica Defence Force, left) and members of the Caribbean Task Force simulate the employment of military resources for military operations during Exercise TRADEWINDS 2022 in Belize City, Belize, on May 11, 2022. Photo by Corporal Mitchell Paquette, 12 Wing Imaging Services.

This page intentionally left blank.

Executive Summary

Much has changed since publication of the last OSINT strategy in 2012, which coincided with a surge in mobile device sales and social media platform users that reshaped the open source landscape. The conditions were set for the digital revolution that continues today. In 2012, the newest smart phone could store 64GB of data — it would take 234 of these to store the data produced by a single person each day in 2023, and this number will double in 2 years.

Against this backdrop, the challenges ahead for Defense OSINT are daunting. The good news is the Defense Intelligence Enterprise has spent the past 10 years ramping up Open Source capabilities. The Defense Intelligence Agency, designated in 2021 as the Defense Intelligence Enterprise Manager for OSINT, through the Open Source Intelligence Integration Center (OSIC), leads a robust Defense Open Source Council (DOSC) to coordinate and synchronize OSINT across the Department.



Defense OSINT Strategy 2024–2028.

▲ Matthew D. Skilling (center), poses with his Army Europe Open Source Center team members. The OSINT Foundation announced Skilling as the inaugural winner of the OSINT Practitioner of the Year award, Nov. 10, 2022. Also pictured are team members, from left to right: Sgt. Taras Demyanyk, Brian Couzelis, David Papava, Eugene Shilman, 1st Lt. Chelsea Michta, Michael Camprise, Matthew Skilling, Samuel Bankester, Spc. Marvin Lopez, Sgt. Skyler Barsten, Mirjana Bourke, Spc. Curtis Maxwell, and Capt. Kristy Bland. Photo by Staff Sgt. Michael A Parker.

This strategy establishes a vision, goals, and objectives to elevate OSINT as a core intelligence discipline that provides high-value unclassified reporting, while simultaneously serving as a catalyst for enriched all source analysis and a valuable cueing mechanism for the other intelligence arts. To do this, the DOSC will lead enterprise-level initiatives designed to increase the intelligence value of OSINT reporting, integrate new technologies, improve data management, and maximize sharing of collected data and information. Through a fully-federated, system for synchronizing tasking, collection, processing, exploitation, and dissemination, DOSC member organizations will collaborate to optimize their OSINT activities from end to end, eliminating redundancy and duplication of effort. Adherence to four Guiding Principles — Data Centricity, Diversified Collection, Dispersed Operations, Distributed Enterprise — will serve as anchor points as the enterprise drives towards this vision.

The operating environment will continue to evolve into a common competitive space for discovery, posing new challenges and opportunities for Defense OSINT.

Artificial intelligence will provide unprecedented capability to sift through vast quantities of data extract concepts in their entirety. It will simultaneously enable rapid creation of false information that will call into question the validity of all data collected from open sources. Social media platforms will continue to serve as hubs for people with shared interests, but the proliferation of spam accounts could push many web platforms towards invitation-only policies. Changes in privacy laws and digital security procedures will also limit access to information that is readily available today.

Although technology advancements are a key feature of this strategy, people will continue to be our greatest asset. Investing in a highly trained workforce is the key to long-term success and securing the future of Defense OSINT. External engagements are an equally important force multiplier. The DOSC will expand collaboration with the commercial sector, government think tanks, and academic experts to anticipate open source challenges and opportunities. Internationally, the DOSC will forge new collaboration pathways with foreign allies and partners to establish a globally-postured OSINT collection and reporting platform.

Strategic Goals and Objectives Overview

Goal 1	Goal 2	Goal 3	Goal 4	Goal 5
Enhance decisionmaker/warfighter situational awareness.	**Maximize the intelligence value of open source information.**	**Expand the Open Source aperture internally and externally.**	**Establish OSINT as the premier intelligence capability and the foundation for all other disciplines.**	**Synchronize OSINT with all other PAI/CAI activities.**
Obj 1.1. Integrate AI/ML capabilities for collecting, processing, and reporting OSINT.	**Obj 2.1.** Attain and maintain OSINT technology advantage; expand engagements across research and development organizations.	**Obj 3.1.** Improve collaboration with other Intelligence disciplines.	**Obj 4.1.** Create and institutionalize OSINT Training, tradecraft, and Civilian/Military career tracks.	**Obj 5.1.** Integrate Multi-Int Collection Management.
Obj 1.2. Expand and enrich OSINT reporting, adopt new product lines, and implement feedback loop for assessing effectiveness	**Obj 2.2.** Optimize sharing of OSINT technologies, support joint tool development, and establish collaboration venues.	**Obj 3.2.** Open new pathways and develop novel procedures for acquiring Open Source data and information.	**Obj 4.2.** Strengthen OSINT policy and governance.	**Obj 5.2.** Develop an Industry-focused commercial data & tool assessment, acquisition, and discovery framework.
Obj 1.3. Develop and Deploy an Open Source, Cross-Domain TCPED system; integrate OSINT with all source analyst workflows.	**Obj 2.3.** Develop hybrid, cross-discipline, OSINT collection and processing teams armed with latest tools/capabilities.	**Obj 3.3.** Optimize OSINT collaboration with FVEY partners.	**Obj 4.3.** Expand and enrich OSINT engagement within national-level intelligence Communities.	
	Obj 2.4. Establish assessment and evaluation criteria and standards to measure performance and effectiveness of OSINT collection.	**Obj 3.4.** Establish bilateral OSINT partnerships in priority geographic regions; expand intelligence collaboration with foreign partners.	**Obj 4.4.** Improve awareness and understanding of OSINT across all government, private sector, and public audiences.	

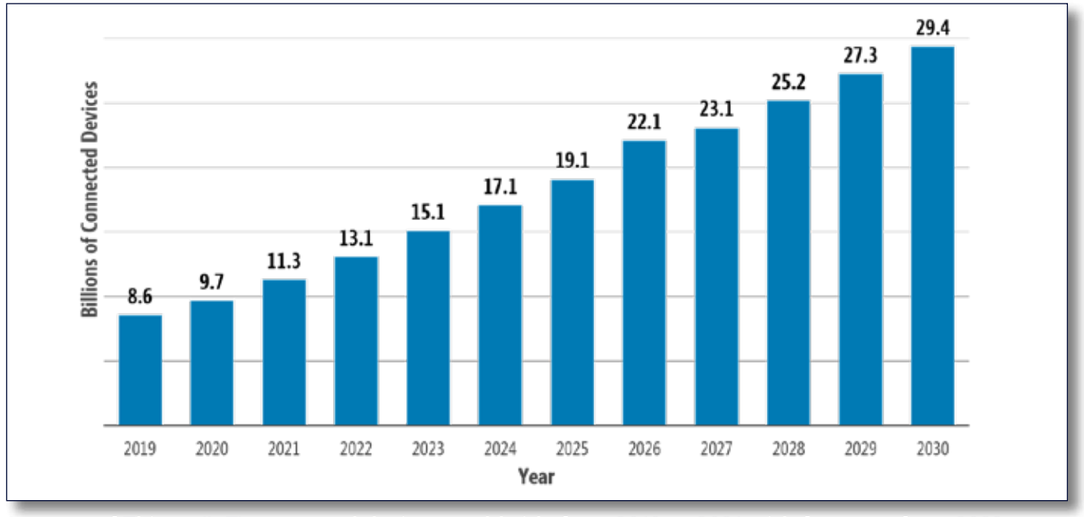
Open Source Challenges and Opportunities

In an era of Strategic Competition, Open Source Intelligence (OSINT) derives insights, produces actionable intelligence, enables timely and effective public messaging and international engagements, and provides leaders with timely options for developing strategic communications.

In the open source operating environment, change is the only constant. A prime example is the emergence of large quantities of data as an open-market commodity, which has created new opportunities for OSINT collection and exploitation. Since 2018, the total value of data bought and sold on the global economy surpassed that of crude oil.

Technological advances, changing societal norms, and revised data privacy regulations will continue to create challenges, and the OSINT community must adapt to gain and maintain information dominance. The Internet of Things will track every aspect of personal information including health, fitness, entertainment, temperature control, lighting, and home security systems. Smart cities will integrate traffic management, intelligent connected vehicles, public safety, intelligent shopping, and energy efficiency technologies.

Social media messaging platforms, online collaboration sites, and mobile applications will continue to serve as hubs for people with shared interests. The proliferation of spam accounts, offensive content, and false information could push many web platforms towards invitation-only, rendering these services inaccessible under current OSINT policies and authorities. Changes in international privacy laws, expanded government regulation of digital platforms, data governance, and digital security will limit access to and use of information that is readily available today.



Internet of Things (IoT) connected devices worldwide from 2019 to 2021 with forecasts from 2022 to 2030 (in billions).

Artificial Intelligence (AI)

Leveraging the power of AI to sharp-en our intelligence insights and illumi-nate opportunities is critical to our future success. Our adversaries understand the significance of mastering advanced tech-nologies to undercut our strategic and tactical dominance.

—DIA AI Strategy

Artificial intelligence tools and capabilities represent a double-edged sword for the OSINT community. They provide unprecedented capability to sift through vast quantities of data, while simultaneously enabling rapid creation of false information. However, artificial intelligence (AI) fundamentally changes the impact of OSINT. Building algorithms to associate disparate data points will enable the extraction of entire concepts from the open source environment. Generative AI, in the hands of nefarious actors, has potential to create digital media content that will call into question the validity of all data collected in in the global open source environment, requiring trained OSINT professionals and robust analysis to validate collected information.

OSINT must evolve to establish and maintain a competitive advantage in the volatile open source operating environment of the future. OSINT is an intelligence collection discipline infused with technical skills, enhanced digital literacy, and advanced tradecraft.

It requires heavy investment in data science, stewardship and continued human-machine integration throughout the intelligence cycle. Adopting an enterprise-wide, data-centric approach to OSINT places increased emphasis on the importance of life-cycle management principles. Discovery of existing data collections at the front end avoids duplication of collection efforts or repeat acquisitions of costly commercially available information, tools, and services. Through a modernized OSINT requirements management system, DOSC members will have automated access to centralized data storage repositories with secure, cross domain accessibility.

The OSINT center of gravity resides in human operators, and not in any machine or tool. Machine-based collection and processing will augment highly skilled human operators orchestrating compilation of multiple streams of open source information to create high-value intelligence reports, cross-cue other collection platforms, and feed the all source analysis process. Simple, single-source OSINT reporting will increasingly be addressed by machines at scale freeing open source teams to focus on more complex collection methods. Likewise, the teaming of machine translation and native-speaker human collectors will remain an essential ingredient of OSINT success, especially pertaining to real-time understanding of social media content and sentiment heavily laced with local dialect, cultural nuances, and idiomatic expressions unique to online digital life. Trained and empowered open source officers will lead integration of requirements managers, online collectors, data scientists, librarians, acquisition and contracts specialists, and privacy/civil liberties officers operating as a multi-discipline team. Together they will unlock global information and harvest the intelligence value of open source data.

Novel sources of information stemming from the commercial data marketplace will present new opportunities for the OSINT community to diversify collection and acquisition and hedge against over-dependency on a limited number of social media and data providers.

Competition for relevance in the crowded digital data ecosystem — the pursuit of being the "next-big thing" — necessitates an agile OSINT collection posture that is not overly-dependent on a specific social media outlet or data provider.

Third-party data brokers, industry partners, and academia with persistent global reach can provide expertise, access, and agility far outpacing what the government can create, scale, and sustain. OSINT will provide secure and efficient pathways for locating, assessing, collecting, and accessing these data sources, while adhering to the highest standards for protecting sensitive and personal information that is increasingly available on the commercial data market.

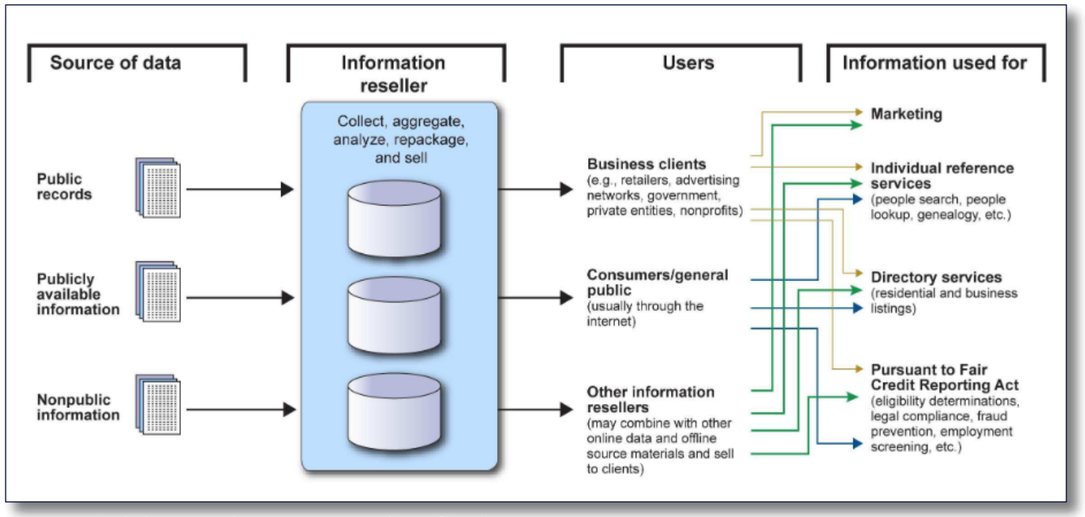
Effective ties and unity of effort between OSINT and the other intelligence disciplines will increase in importance as the scale and scope of open source

▲ The U.S. Air Force Intermediate OSINT course empowers Intel analysts. U.S. Air Force Senior Airman Erin K. Stephens, geospatial imagery analyst with the 123rd Intelligence Squadron, works in the 188th Wing Innovation Lab in Fort Smith, Arkansas, December 21, 2022. Photo by Maj Jennifer Gerhardt, U.S. Air Force.

increases. OSINT informs a wide range of classified intelligence and intelligence-related planning and operational activities. Focused collection of open source data and information will facilitate operations security (OPSEC) and protect sensitive intelligence operations. Technical exploitation of the expanding universe of Internet-connected devices will require greater collaboration between the technical collection disciplines. Persistent global positioning technologies will provide endless possibilities for expanded collaboration between OSINT and other intelligence disciplines.

The demands on OSINT will inevitably continue to outpace the growth of capabilities within the individual DIE components. The path to success is a fully integrated enterprise approach to all open source activities and programs across the DIE, whether conducted for OSINT, or to support a wide range of intelligence requirements.

The DOSC, under direction of the DIEM-OSINT, will adapt and evolve to lead these efforts and serve as the central point of collaboration in the highly complex and always-evolving open source operating environment of the future.



Commercial data market sources and applications.

U.S. Army LTG James B. Jarrard, U.S. Army Pacific deputy commanding general, provides opening remarks to commence USARPAC's third annual Artificial Intelligence/Machine Learning Summit in Fort Shafter, Hawaii, Oct. 25, 2023. USARPAC aims to unify the AI/ML Community of Interest under a shared purpose to address USARPAC challenges where AI/ML capabilities can be integrated. U.S. Army photo by SPC Taylor Gray. ▶

VISION

Make OSINT the "first resort" source of intelligence for decisionmakers and warfighters.

Strategic Goals And Enabling Objectives

Strategic Goal 1: Enhance decision-maker and warfighter situational awareness through timely delivery of customized, serialized OSINT products and data.

Enabling Objective 1.1— Integrate advanced technologies for collecting, processing, and reporting OSINT. Maintaining an accurate understanding of global events, especially in the early stages of emerging crisis situations, is increasingly difficult for warfighters and decision-makers. Rapid assimilation of open source information across multiple data streams requires effective use of artificial intelligence and machine learning (AI/ML) capabilities to enhance, expand, and accelerate OSINT collection activities across the DIE. Prioritization of associative sensemaking will enable the extraction of concepts from the open source environment.

Enabling Objective 1.2 — Expand and enrich OSINT reporting and adopt new product lines tailored to unique requirements for unclassified decision aids and strategic messaging. Communicating to global audiences in the information environment is an essential element of integrated deterrence, which is a centerpiece of our National Defense Strategies. Timely, precise, and in-depth OSINT reporting enables leaders to outpace adversarial narratives, and is essential to the formulation of strategic messaging and pro-active engagement with partners, allies, and the public at large.

Enabling Objective 1.3 — Develop and Deploy an Open Source, Cross-Domain, Tasking, Collection, Processing, Exploitation, and Dissemination (TC-PED) system accessible to the Defense Intelligence Enterprise, FVEYs and IC partners. OSINT is unique as an intelligence discipline in that it supports all other forms of intelligence. OSINT provides broad insights for shaping collection plans, tips, and cues other collection capabilities, and fills gaps to round out all source analysis. To fulfill the role as the DIE's first stop on any new intelligence endeavor, the DOSC must work together to develop and adopt a fully functioning TC-PED architecture for OSINT, accessible to authorized US and Coalition users at all classification levels across multiple networks, that orchestrates collection, ensures full access to all open source data and reporting, provides data enrichment microservices, integrates seamlessly with all source analysis, and populates catalogs and repositories.

Strategic Goal 2: Maximize the intel-ligence value of open source information.

Enabling Objective 2.1 — Attain and maintain an OSINT technology advantage. The open source information space is a highly dynamic operating environment fueled by novel, technology-based approaches to support a wide range of government and private-sector business requirements. Beyond their commercial value, these capabilities have game-changing potential for transforming vast quantities of open source information into valuable Defense intelligence, at the speed and scale required to keep pace with warfighter and decision-maker demands for OSINT.

Enabling Objective 2.2 — Optimize sharing of OSINT-related technologies across the DIE. Developing, acquiring, and gaining approval to deploy new technologies on DoD networks is a complex, time consuming process. Sharing technology solutions across the enterprise mitigates opportunity costs and promotes increased collaboration; all resulting in greater efficiency, preservation or resources, and enhanced mission focus.

Enabling Objective 2.3 — Develop hybrid, multi-discipline solutions for scalable OSINT collection and processing teams. The open source data environment will become increasingly challenging for OSINT collectors, necessitating novel approaches for collection of open source information, and processing it into high value intelligence products.

Enabling Objective 2.4 — Establish assessment and evaluation criteria and standards to measure performance and effectiveness of OSINT collection and reporting. It is critical for the DIE to measure the performance and effectiveness of OSINT collection and reporting.

Strategic Goal 3: Expand the open source aperture internally and externally.

Enabling Objective 3.1 — Improve collaboration with other Intelligence disciplines. OSINT provides situational awareness and foundational collection that enables other intelligence disciplines to focus their capabilities on the hardest targets and requirements that can be answered by no other means. A sudden increase in social media postings can be the first indicator of an emerging crisis, and a starting point for other focused collection. Publicly shared images can provide location data or other relevant information that can be used to inform other collection efforts.

Enabling Objective 3.2 — Open new pathways and develop novel procedures for acquiring Open Source data and information. The online open source environment is constantly evolving. Sustaining access, locating unique data sources, and extracting information with intelligence value from a network of more than 200 million nodes hosting 4 billion users every day is a complex set of activities. Machine association of disparate data points will enable analysts and leaders to identify the ontology of threats, make sense of the information environment, and extract whole concepts from the open source domain. To succeed, the DOSC must identify and execute a diversified collection posture that mitigates dependency on single sources of data or information. Across the DIE, open source data governance will apply the core principles for ensuring data is visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS) in accordance with the DoD Data Strategy.

▲ Sailors from 30th Naval Construction Regiment conduct training in the Expeditionary Maritime Operations Center during a Command Post Exercise (CPX) onboard Naval Base Guam. 30th NCR is assigned to Commander, Task Force 75, which executes command and control of assigned Navy Expeditionary Combat Forces in the 7th Fleet area of operations. Photo by Chief Petty Officer Chad Butler.

Defense OSINT Strategy 2024–2028

Enabling Objective 3.3 — Close the gaps that impede full OSINT collaboration. Global strategic competition, particularly in the Indo-Pacific region, requires the utmost degree of collaboration. To accelerate expanded OSINT collaboration, DOSC components will develop options to improve partnership and interoperability, such as forward-based OSINT platforms, and leverage these opportunities to promote more effective international partnerships among all DOSC members.

Enabling Objective 3.4 — Establish bilateral and multilateral OSINT partnerships in priority geographic regions to open new collection pathways and expand intelligence collaboration with foreign partners. OSINT is less encumbered than other intelligence disciplines by limitations in sharing classified information. For these and other reasons, OSINT provides unique opportunities to engage more freely and openly with our foreign security partners. Many of these partners have unique insights, access, and understanding of regional issues, and in some cases a high density of native language expertise.

Strategic Goal 4: Establish OSINT as a premier intelligence capability and the foundation for all other disciplines.

Enabling Objective 4.1 — Create and institutionalize OSINT Training, Tradecraft, and Civilian / Military career pathways. The complex open source environment requires unique skills and abilities that are not resident in existing civilian and military career tracks. To professionalize the OSINT workforce, the DOSC will identify training and certification standards, determine core and essential tasks, and facilitate development, implementation, and sustainment of common training courses. Where possible, these will include options for in-person or online attendance through DIE training portals, not only for OSINT practitioners but also leaders and managers across the DIE.

Enabling Objective 4.2 — Strengthen OSINT governance. The decentralized nature of OSINT collection activity across the DIE has enabled highly impressive development of capabilities, programs, tools, and procedures at the component level.

Enabling Objective 4.3 — Expand and enrich engagement within respective US and FVEY policy and oversight regimes. Ongoing and recent deliberations on the ideal OSINT governance model highlight the fact that no single department or agency is ideally positioned to lead OSINT at the national level. New organizational constructs, international agreements, and changing public sensitivities regarding data privacy will have profound effects on Defense OSINT organizations.

Enabling Objective 4.4 — Improve awareness and understanding of OSINT across all Defense, federal government, private sector, and public audiences. OSINT needs to take a more deliberate approach to educating and informing all audiences on its capabilities and limitations, and be forthright regarding successes and failures.

Strategic Goal 5: Synchronize OSINT with all other Publicly and Commercially Available Information (PAI/CAI) activities.

Enabling Objective 5.1 — Integrate Multi-Int Collection Management. In the open source domain, data-centricity encompasses all collection of PAI/CAI, not just for OSINT purposes, regardless of its end use by other intelligence disciplines.

Enabling Objective 5.2 — Develop an Enterprise Data and Tool Assessment, Acquisition, and Discovery Framework. Diverse procedures for acquiring commercial data and tools increases the risks of poor data quality, malicious code, and low return on investment across the DIE.

References

Department of Defense Directive 5143.01, Under Secretary of Defense for Intelligence and Security, October 24, 2014, as amended.

Department of Defense Directive 5105.21, Defense Intelligence Agency, January 25, 2023.

Department of Defense Directive 3115.18, DoD Access to and Use of Publicly Available Information (PAI), June 11, 2019, as amended.

Department of Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities, August 8, 2016.

(U) Department of Defense Instruction 3115.12, Open Source Intelligence (OSINT), August 24, 2010, as amended.

Notes

DEFENSE INTELLIGENCE AGENCY

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION