OSINT Policy Landscape

June 13, 2024

Table of Contents:

Executive Summary

Open Source Intelligence (OSINT) is an evolving discipline that is now receiving more attention and resources from intelligence and national security agencies. The conflict in Ukraine and widespread access to social media has highlighted the benefits of OSINT to the intelligence community. In order to better harness this intelligence discipline, the IC has recently published a number of policies to govern the use and acquisition of OSINT technologies.

Intelligence Community OSINT Strategy

The Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA) released their Intelligence Community (IC) Open Source Intelligence (OSINT) Strategy in March 2024. The IC is leaning on industry to help make their OSINT mission a success.

To advance the OSINT discipline, the IC will streamline data acquisition, develop innovative technologies to collect and derive insight from open source data, strengthen the coordination of open source collection activities across the community, update and standardize OSINT tradecraft, and develop a highly skilled OSINT workforce.

The strategy establishes the Director of the Central Intelligence Agency (D/CIA) serves as the OSINT Functional Manager (OSFM) for the IC. Day-to-day functions for the implementation of the strategy is vested in the Director of the Open Source Enterprise (D/OSE). D/OSE will work closely with the ***Defense Intelligence Enterprise Manager for OSINT at the Defense Intelligence Agency (DIA) and the IC OSINT Executive at the Office of the Director of National Intelligence (ODNI)*** to build out policy for this strategy.

The Four Strategic Focus Areas:

1. Coordinate Open Source Data Acquisition and Expand Sharing

The strategy seeks to expand the availability of Publicly Available Information (PAI) and Commercially Available Information (CAI) within the IC. To do this, OSINT leaders within the IC will coordinate with the IC Data Officers to acquire PAI and CAI for distribution across the IC based on mission needs.

CAI and PAI usage and metrics will be tracked in a “centralized, multi-domain data catalog.” The IC also plans to build common OSINT platforms and “implement a pathway to deliver IC OSINT products to the broader U.S. Government.”

2. Establish Integrated Open Source Collection Management

The IC will work to better “deconflict” its capabilities so that they are not wasting their “sensitive collection capabilities to obtain intelligence that can be derived from open source information.” The IC will also begin constructing a “new and improved community-wide collection orchestration system.”

3. Drive OSINT Innovation To Deliver New Capabilities

The IC will work to accelerate efforts around artificial intelligence, machine learning, and human language technologies to improve the value derived from OSINT. The IC is looking to test new

capabilities on unclassified systems to acquire capabilities faster. They are also looking to industry and academia to "develop, test, and deploy OSINT tools and tradecraft."

4. Develop the Next-Generation OSINT Workforce and Tradecraft

The strategy calls for the "OSINT community [to] be at the forefront of the IC in testing the use of [Generative AI]." To do this, the workforce will need skills training to properly use the technology and develop frameworks for its use. Training on both Generative AI and OSINT in general must be conducted for "both OSINT professionals and all-source analysts who conduct OSINT activities."

State Department OSINT Strategy

The Bureau of Intelligence and Research (INR) released there Open Source Intelligence Strategy in May 2024.

This strategy outlines the INR's efforts on developing and modernizing OSINT practices. These goals are meant to complement to broad IC OSINT Strategy 2024-2026 and the INR's 2025 Strategic Plan. Four strategic goals are outlined within this report in order to achieve the State Department's vision of effectively and efficiently utilizing OSINT.

The Four Strategic Focus Areas:

1. Establish Governance and Policy for OSINT Use:

The INR will establish standards and policies in order to align with guidelines established in Executive Order 12333. The key efforts by the INR consist of establishing SOPs and guidances to align with legal and policy requirements, promoting equities within policy and guidance, and monitoring and evaluating OSINT production by the INR.

2. Invest in OSINT Capabilities:

The INR will acquire and develop OSINT tools and data, and utilize and manage these tools and data to advance the INRs capabilities to of delivering proper data to INR analysts. A few lines of effort are engaging with industry aprtners, identifying core datasets, funding OSINT programs, oversight of OSINT data and tools, and creating guides for OSINT information.

3. Strengthen OSINT Training and Tradecraft:

Technical and methodological skills are critical to OSINT, and the INR is seeking to enhance these skills through straining programs for its workforce. The INR will facilitate in-house education and develop a training curriculum, establish differences between OSINT and open source research, provide trainings on un-classified products and assessments, and posting products on their online distribution platform Tempo.

4. Deepen Collaboration with Allies, Partners, Industry, Academia, and Other Nongovernmental Entities:

The INR wishes to foster a deeper connection with current partnerships in the IC and other government agencies, as well as non-governmental entities. The INR is looking to increase these partnerships

through maintained contact, as well as establishing best practices and processes on collaborationand coordination with other IC agencies.

U.S. Space Force Commercial Space Strategy

The U.S. Space Force released their commercial space strategy in April 2024. It states that the USSF's "priority missions for new commercial integration are Tactical, Surveillance, Reconnaissance, and Tracking (TacSRT); Spacebased Environmental Monitoring (SBEM); Positioning, Navigation, and Timing (PNT); and Space Access, Mobility, and Logistics (SAML); as well as the continued integration of commercial space solutions into mature missions like SATCOM, Launch, and Space Domain Awareness (SDA)."

OSINT tools have the opportunity to play a large role in TacSRT, SDA, and others in the listed priorities.

The strategy focuses on expanding resourcing for commercial offerings and integrate them into a hybrid architecture. Program Executive Officers (PEOs) and the the Commercial Space Office (COMSO) will work to identify and test new commercial solutions.

NGA Commercial GEOINT Strategy

NGA released their commercial GEOINT strategy in 2015 and updated it in 2018. NGA has established their Commercial GEOINT Activity (CGA) to serve as a "front door" for commercial GEOINT vendors. NGA has previously entered into contracts with Planet Feed and Subscription Contracts to gain open source coverage of the globe. Their Janus Contracts allowed them to transition to some open source services.

The strategy lays out three goals:

- Expand data and service access through partnerships to feed analysis and production
- Fortify GEOINT Assurance through diversity of commercial suppliers
- Drive analytic and production capability by integrating commercial GEOINT, automation, and artificial intelligence

The strategy also calls upon industry to provide more training as a service around unclassified open source methods.

National Security Space: Actions Needed to Better Use Commercial Satellite Imagery and Analytics

In 2022 the GAO had released recommendations to the DOD and ODNI. The GAO states that the IC and DOD are slow in incorporating commercial capabilities, which can create a technological disadvantage to competitors. The IC and DOD have requirements for commercial acquisitions but are unable to incorporate commercial satellite imagery effectively .As a result, the GAO has release four recommendations to address these issues. All recommendations from the GAO are still listed as "Open".

1. Definition of clear roles and responsibilities between the DOD and IC

The Secretary of Defense and Director of National intelligence should ensure clear roles and responsibilities on the acquisition of commercial satellite imagery. In January 2024, the DOD provided an update on these roles in order to provide interim guidance. In September 2022, the DOD would "address the recommendation by revising DoDD 5105.23 National Reconnaissance Office (NRO) and DoDD 5105.60, National Geospatial-Intelligence Agency (NGA)" related to roles and responsibilities.

2. Incorporation and Scaling of Commercial Satellite Capabilities into Operational support contracts

The Secretary of Defense and Director of National Intelligence should ensure the NRO, in coordination with NGA, IC, and DOD stakeholders, assess approaches to incorporating commercial satellite capabilities into operation support contracts. In January 2024, the DOD provided an update stating they were using quarterly performance reviews and designated officials to ensure contract flexibility and efficient acquisition processes. The GAO notes this update does not meet their recommendations.

3. Creation of Goals and Measures towards Maximizing Commercial Satellite Imagery

The Director of National intelligence, in conjunction with the Secreatary of Defense, should ensure the NRO and NGA develop goals and measurements to track and enhance the progress of adopting and maximizing the use of commercial satellite imagery. On January 19, 2024, the ODNI provided an update stating that "formal response to this recommendation is being coordinated as part of a larger response to all open ODNI recommendations itemized in the GAO letter of 9/29/23 to Congress."

4. Roles and Responsibilities for Commercial Analytics Services that use Remote Sensing Data

The Director of National Intelligence, in coordination with the Secretary of Defense, should ensure the NGA develop roles and responsibilities related to how remote sensing data is used in commercial analytic services. A specific note for thsis guidance is provided stating "The guidance should note the components responsible for addressing resourcing visibility and for identifying performance goals and measures related to commercial analytic services that use remote sensing data."

On January 19, 2024, the ODNI provided an update stating that "formal response to this recommendation is being coordinated as part of a larger response to all open ODNI recommendations itemized in the GAO letter of 9/29/23 to Congress."

Intelligence Community Policy Framework for Commercially Available Information

The IC publushes a Framework for Commercially Available Information in May 2024. The framework lays out general principles for the access and collection of commercially available information (CAI) and how the IC deals with sensitive CAI.

The IC will be required to determine the original source of CAI datasets, determine if the data is biased, and ensure that data is not collected for the purpose of discrimination.

Sensitive CAI is classified as data that is either purchased from a commercial entity or given access for no cost through a commercial entity and contains substantial personally identifiable information (PII) of U.S. persons.

Access to CAI should be governed by the following requirements:

- Participation in the procurement process
- Consideration of mission need, legal authority, data sensitivity, privacy/civil liberties risk, privacy-enhancing techniques, data sourcing/integrity/quality, and security risks.
- IC agencies can use prior assessments of these products by other IC agencies
- Approval from element heads or delegated authority

Sensitive CAI is subject to requirements such as Authority to Operate (ATO), Privacy Overlays, and appropriate access restrictions on vendor systems.

IC agencies should have enhanced safeguards in place to protect sensitive CAI, procedures such as:

- Attribute-based access controls
- Procedures for auditing queries
- Written justification from senior executives for queries
- Approval from senior executives for any searches that constitute “data mining”
- Dissemination restriction
- Privacy-enhancing techniques
- Procedures for deleting U.S. person information

Intelligence Authorization Act Provisions

Both the House and Senate versions of the FY24 Intelligence Authorization Act include provisions to expand the use of OSINT in the IC. The FY24 Intelligence Authorization Act was included in the FY24 NDAA and signed into law by President Biden in December 2023.

Section 432 “Development of Plan to Make Open-Source Intelligence Products Available to Certain Federal Employees” covers new policies for OSINT. The section requires policies and procedures to be developed to:

- Make available OSINT tools to federal employees with a need for the technology
- Increase the accessibility of publicly available foreign language material that is translated within the IC
- Make unclassified products derived from OSINT available to State and local government officials

It also requires the Director of National Intelligence (DNI) to update “Intelligence Community Directive 209: Maximizing the Utility of Analytic Products” to better cover the production and dissemination of unclassified intelligence products dervived entirely from OSINT.

Section 6311 of the FY23 Intelligence Authorization Act established a pilot program to "assess open source support for export controls and foreign investment screening." ODNI would work in conjunction with the Department of Commerce and Department of Homeland Security to carry out these functions. It specifically states that these authorities may "modernize analytic systems, including through the acquisition, development, or application of automated tools."

DoD 3115.12 Open Source Intelligence (OSINT)

The Under Secretary of Defense for Intelligence & Security (USD I&S) released DoDI 3115.12 "Open Source Intelligence" in August 2010, and was updated in July 2020.

The policy "establishes policy, assigns responsibilities, and prescribes procedures for OSINT operations within the DoD." It also establishes the DoD Open Source Council (DOSC). This policy identifies the Director of the Defense Intelligence Agency (DIA) as the DoD Lead Component for OSINT.

Ethical Frameworks in Open-Source Intelligence

The Ethical Frameworks in Open-Source Intelligence was created by the Public-Private Analytic Exchange Program in 2022, Shani Spivak of the FBI being the champion agency. Definitions and history of OSINT are provided in the beginning of the document, which leads to outlining the changes that OSINT has undergone with the creation of the internet. The definitions of OSINT end with a breakdown of its usage in the public and private sectors.

For OSINT, there are different ethics for both public and private sectors as there are no "nationally or internationally accepted guidelines for how social media intelligence is collected, analyzed, and obtained." But, it is accepted that this information must be used "in a way that does not violate existing privacy laws, must not be used in a malicious manner, and must be done only when necessary."

Certain legal standards provide a basis on ethics in OSINT with the fourth amendment and local, jurisdictional differences being of note. Some states such as Michigan an Missouri have amended their constitution and privacy rights to explicitly include electronic data and communications. For now, there are not current ethical standards that the public and private sector must follow, as long as the information obtained is found so legally and its usage is legal.