



---

by First Lieutenant Moriamo O. Sulaiman-Ifelodun and Colonel Robert M. Wilkinson (Retired)

---

## Introduction

How can S-2s and collection managers more effectively integrate open-source intelligence (OSINT) into planning and requirements to improve intelligence for a changing and challenging world? This article provides a proposal to meet this objective by better integrating OSINT collection requirements into information collection planning as part of multi-domain operations.

## Why Now?

The digital information environment continues to evolve, bringing far-reaching and dynamic challenges for the operational environment. To address the challenges, commanders must understand all relevant aspects of the digital information environment, including identifying and responding to our adversaries' influence operations. OSINT can address many of the commander's intelligence requirements related to the operational environment, if G-2/S-2s and collection managers devote sufficient time and effort to developing and designing collection requirements up front and continue refining them throughout multi-domain operations. G-2/S-2s and collection managers can leverage OSINT as part of a fully coordinated planning effort so that requirements are developed appropriately using OSINT tools and capabilities joined with regional, cultural, and language expertise.

Our suggestion to G-2/S-2s and collection managers, especially those who have not considered OSINT recently, is to revisit OSINT doctrine. ATP 2-22.9, *Open-Source Intelligence* (and its classified companion *Volume II*), issued in 2019, improves understanding of OSINT as a collection discipline. Intelligence staffs should already be familiar with ATP 2-01,

*Plan Requirements and Assess Collection*, issued in 2014. Unfortunately, ATP 2-01 does not discuss the specifics of information collection planning for each intelligence discipline. Therefore, we suggest ATP 2-22.9, chapter 3, as a starting point to increase understanding of collection management for OSINT.<sup>1</sup> To address any remaining questions, we offer this article to help Army intelligence professionals and organizations achieve increased understanding in breadth and depth of intelligence operations through OSINT.

## OSINT 101

For those unfamiliar with OSINT, here is a quick overview. Congress defined OSINT as "intelligence that is produced from publicly available information [PAI] and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."<sup>2</sup> OSINT results from collecting and analyzing information obtained from the publicly accessible portion of the global information pool.<sup>3</sup> Therefore, the term *OSINT* refers to the specialized intelligence discipline, single-source products created, and the collection activity itself.

OSINT is often referred to as open-source information, which is a misnomer. PAI is raw material that can be processed, exploited, and disseminated as an OSINT product or as inputs to all-source production. OSINT is an integral part of the intelligence warfighting function through the collection of PAI to answer intelligence requirements. Ignoring PAI as a source of intelligence reduces collection effectiveness. PAI collection for other purposes, such as information collection for operations, is not an OSINT activity. However, commanders should consider how much operations

security (OPSEC) risk their operations create when collecting PAI without using the G-2/S-2s trained and equipped OSINT practitioners to answer requirements.

OSINT traces its roots to foreign broadcast monitoring services during World War II. Understandably, 21<sup>st</sup> century OSINT is far more complex. The ever-growing multitude of modes generating data and content are changing the ways PAI is published and consumed, creating perpetual challenges for OSINT as a discipline. Therefore, the OSINT discipline evolves in real time as the proliferation of new media platforms and “Internet of Things” devices generating PAI continues to mature. Unfortunately, policy generally lags behind technology. OSINT is an evolving discipline; its tactics, techniques, and procedures frequently change as technologies stack, creating exponential change in the cyberspace domain.

In 2016, OSINT was revitalized through new Department of Defense (DoD) and Army policies designed to address explosive growth in traditional and social media digital content as well as the advent of new, rich PAI data sources that new technologies were generating. To address a growing demand signal from commanders, the Army OSINT Office (AOO), at the U.S. Army Intelligence and Security Command, was established and became the man-train-equip proponent for OSINT. An acknowledged leader in the DoD for its ability to field OSINT capabilities, AOO raised the DoD standard through training courses, requirements and capabilities management, and auditing/compliance functions. For the Army, AOO is the primary linkage for developing an OSINT capability. G-2/S-2s and collection managers can become familiar with AOO offerings by visiting their web portals and attending the monthly community of interest video teleconferences.

### **So Why Do Military Intelligence Organizations Need to Improve Their OSINT Capability?**

Upon receipt of a new mission, we instinctively turn to the internet and smart devices to develop foundational information and knowledge for mission analysis and intelligence preparation of the battlefield. OSINT can be the starting point to tip and cue intelligence disciplines when generating intelligence knowledge, developing awareness, and tracking events and atmospherics as they develop. It helps further refine situational awareness and enrich understanding of the operational environment to better inform the commander and staff. OSINT also provides indicators for warning to direct deeper research. OSINT can be agile when configured to support situational development and warning missions.



Photo by Joseph Eddins

Publicly available information is becoming increasingly important in the fields of intelligence analysis, cybersecurity, and criminal investigations, among others.

OSINT is comparatively cost-effective. It is quite often the only persistent information collection capability available when exquisite systems and capabilities are unavailable or deployed elsewhere. With training, tradecraft, and tools, a multitude of PAI data points can be collected, processed, and exploited as a single-source production effort or can support vitally important all-source production. OSINT enhances the intelligence process, particularly by tipping and cueing other intelligence disciplines for tasking and collection—making more effective use of a system of systems. Moreover, OSINT can support targeting with insights that enrich the target picture and inform assessments of non-lethal effects or post-strike battle damage. Finally, when it comes to shaping strategic engagements with our partners and allies, we often look to OSINT as the entry-level sharing opportunity to build or strengthen trust with these partners.

A solid understanding of intelligence oversight and Army OSINT guidance is essential to the proper planning and conduct of OSINT activities. DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, directs us to start collection with the least intrusive collection methods first. Specifically, procedure 2, “Collection of [U.S. person information] USPI,” specifies PAI as the least intrusive.<sup>4</sup> Army Directive 2016-37 (U.S. Army Open-Source Intelligence Activities) states that when an intelligence professional “copies, stores or otherwise preserves” something into an intelligence component database, they have conducted an OSINT collection activity.<sup>5</sup> For most all-source analysts, suddenly becoming a collector is a radical change!

### **What G-2/S-2s and Collection Managers Need to Know about OSINT to Improve Collection Management**

For all the reasons described above, OSINT is a remarkably effective discipline for developing a holistic picture.

But are we properly and effectively planning for, executing, integrating, and streamlining a deliberate PAI collection effort in support of our everyday intelligence missions? Do we have the appropriate capability in place (defined as properly trained and equipped personnel) to effectively address information and intelligence gaps in a timely manner? Do G-2/S-2s and collection managers understand how to leverage that capability appropriately? How does one identify, describe, and nominate an OSINT collection requirement to an external OSINT activity? How do we consider the OSINT discipline's prime directive of "collect once, share broadly" to minimize redundancy and collection fratricide? In this area, doctrine and practice need to be updated. Here is a suggested path.

Going back to basics, the intelligence process, shown in Figure 1, begins with plan and direct. More time and effort must be devoted to this step in order to properly focus and leverage PAI collection and OSINT processing, exploitation, and dissemination (PED) to support all-source or single-source production. Let's begin the process of planning and directing by appreciating the discipline's unique challenges.

- ◆ A foreign intelligence or counterintelligence mission.
- ◆ An OSINT authority granted by a commander at the proper echelon.
- ◆ A validated intelligence requirement.
- ◆ An approved collection plan (including a risk assessment).

Time is another limiting factor. G-2/S-2s should understand that the time necessary for OSINT planning, initial research, collection, and PED is proportional to the complexity of the requirement and the scope of the question. Deliberately crafted, precise, and time-bounded questions are best suited for OSINT activities.

The digital information environment is dynamic, and its constant changes present a variety of challenges. The sheer volume of content and data generated each day is daunting. It requires skill, technical expertise, cultural knowledge, language capabilities, and technological aids, all of which are constantly evolving. Our experience in the U.S. Army Pacific area of responsibility shows we must be efficient and effective. Collection managers should understand each OSINT

activity with a stake in their area of responsibility. Coordination and collaboration are critical to achieving success and avoiding redundant collection.

Geographical and operational boundaries are normal collection planning considerations; however, OSINT practitioners operate in cyberspace. Proximity to the target matters, but more important is the question, Which OSINT activity has the best capability and domain expertise to address this requirement?

Information control mechanisms vary across the operational environment. Nation states where censorship is high and freedom of the press is correspondingly low are often the highest risk targets. Therefore, risk versus reward is always a consideration. Hard targets require more precision, creativity, and tradecraft. Collection managers across the intelligence community should protect access to certain open sources for only the

most advanced OSINT activities.

With continuing advances in technology and telecommunications, it is possible to address existing requirements in new ways and to develop new intelligence questions that were not considered in the past. Collection

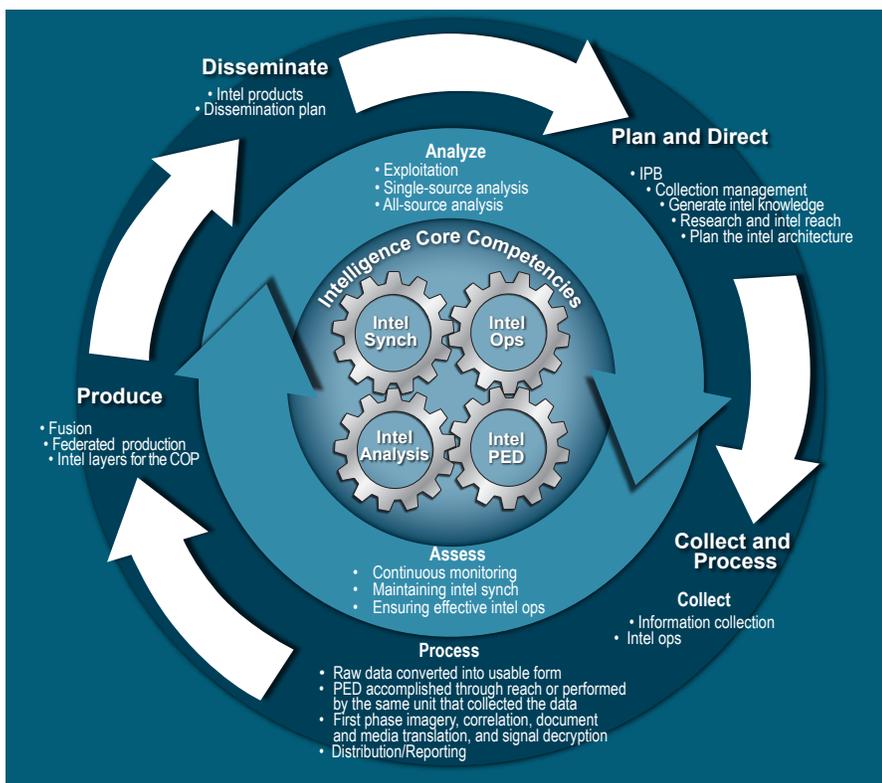


Figure 1. The Intelligence Process<sup>6</sup>

Collection managers must understand the supporting OSINT activities' capabilities, limitations, and constraints. OSINT-specific constraints include obtaining proper authorities and developing a plan to address all OPSEC and cybersecurity risks. The OSINT activity must have—

managers should frequently consult with their supporting OSINT activity on emerging requirements to understand and appreciate what novel capabilities may be available and then update collection strategies and the staff accordingly during integrated planning sessions.

Collection managers must coordinate with joint, inter-agency, and multinational partners to avoid duplicate collection and ensure widest dissemination. Creating “swimlanes” for each partner’s OSINT capability is a good way to organize a theater-wide OSINT effort, whether by topic, country, region, warfighting domain, or combat capability. Keep in mind that the goal is to avoid duplicative visits to the same resources in order to minimize risk. By collecting once and sharing broadly, we make the best use of resources and domain expertise, ultimately paying off in both effectiveness and efficiency.<sup>7</sup>

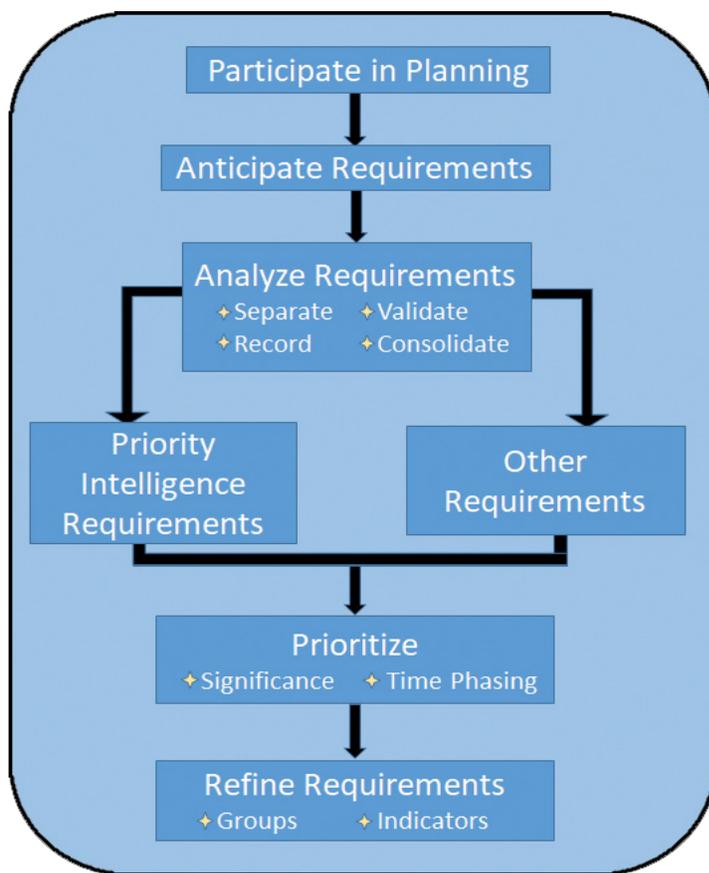
### Design and Architecture Considerations

ATP 2-01 says requirements are constantly developed, consolidated, and refined throughout the planning process. Maximum efficiency in information collection is achieved when all the collection tasks are carefully synchronized with an appropriate mix of collection assets to satisfy as many distinct requirements as possible.<sup>8</sup> OSINT can answer initial requests for information (RFIs) that shape the mission, commanders’ decision making, and time-phasing requirements management. Once multi-domain operations are underway, OSINT supports and informs information requirements and intelligence gaps, providing insights that might not be found on higher classification systems and are sometimes overlooked.

Effective requirements development depends on establishing the intelligence architecture and having effective network connectivity that provides situational understanding and input from the entire staff.<sup>9</sup> Design considerations include an important choice for commanders, specifically whether to—

- ◆ Organize an OSINT activity within an all-source team by integrating and embedding OSINT practitioners.
- ◆ Organize as a single-intelligence discipline team.
- ◆ Train and equip all-source analysts to collect PAI as part of their mission.

The all-source effort is directly supported, and OSINT is integrated into production. Disadvantages to the blended approach include burdening all-source analysts with OSINT training requirements, collection policy compliance, sustainment of technical proficiency, and record keeping. Embedding OSINT practitioners into an all-source team may be more effective but requires borrowed manpower (or



Staff elements that develop requirements follow a development process that includes subordinate tasks and products.<sup>10</sup>

contracted labor) and their efforts may get lost as merely a source citation at the end of a classified product.

In the Indo-Pacific Theater, the single-intelligence discipline team design is preferred. Just like other intelligence disciplines, the OSINT activities respond to tasking through priority intelligence requirements, intelligence requirements, RFIs, directed requirements, and emphasis messages. Thinking broadly, production of OSINT reports is the best way to put points on the intelligence community scoreboard for the Army OSINT program. And when properly disseminated, OSINT reports support the “collect once and share broadly” mandate.

In terms of architecture, PAI collection requires seamless network connectivity. The DoD Non-classified Internet Protocol Router Network (NIPRNET), primarily an administrative and logistical network, is now an essential collection platform. Coordination with G-6/S-6 is required to ensure the dedication of sufficient connectivity, system flexibility, and bandwidth to OSINT activity.

### Techniques for OSINT Collection Planning

In our experience, OSINT is an afterthought. When creating indicators and specific information requirements (see Figure 2 on the next page), consider where OSINT can contribute. Done properly, OSINT takes time. Planning and

coordination of emerging requirements provide a sufficient lead time essential to effective OSINT activities. The required risk management procedures and developed best practices require time to plan, prepare, and execute.

To use a human intelligence (HUMINT) analogy, OSINT practitioners must plan and prepare before collection, including the digital equivalent to planning routes and site selection. During collection, OSINT must follow specific procedures using tradecraft and technologies to manage risk. Like HUMINT collectors, they have plenty of production and administrative work to do after a source meeting in order to process, exploit, and disseminate what is collected. For example, OSINT practitioners are required to keep collection logs for audits.

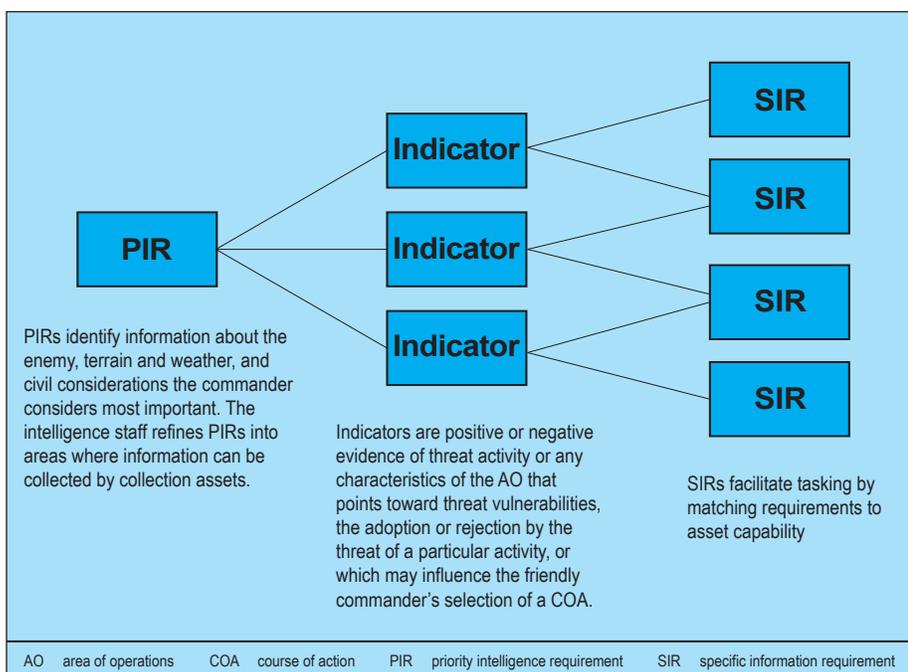


Figure 2. Relationship between Priority Intelligence Requirement, Indicators, and Specific Information Requirements<sup>11</sup>

Proper PAI collection and exploitation involve considering the validity of the source as well as the veracity of the information. Independent PAI sources with the same information give more credibility than a single item from an unverified source or suspicious social media account. In the age of fake news, misinformation and disinformation are ubiquitous. OSINT practitioners are trained to expose potentially false information and recognize fake social media accounts.

Well-prepared OSINT reports include a characterization of the sources and all relevant context about where information was found. This can include any translation capabilities applied to the original content. As everyone should know, machine translation services are imperfect with varying degrees of accuracy, depending on the language, context, and

content. Sarcasm, emojis, shortcuts, local slang, and internet lingo add layers of complexity.

## OSINT Enterprise Collection Management

Advice to G-2/S-2s and collection managers should include advocacy for the use of two systems of record in unison to achieve optimal OSINT integration and synchronization: the open-source collection acquisition requirement–management system (OSCAR–MS) and the community on-line intelligence system for end-users and managers (COLISEUM).

**OSCAR–MS (The Asking System).** The intelligence community's system of record for managing open-source requirements is called OSCAR–MS. Consumers input their requirements and request support from OSINT producers who advertise in the National Open Source Enterprise

Capabilities Manual; it is not a formal tasking system.

OSCAR–MS lacks a mechanism to enforce an obligation to support. The OSCAR–MS portal resides only on the SECRET Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (the SIPRNET portal is far less popular). The default procedure for many consumers is to tag all the OSINT producers with the same requests (the shotgun approach). Producing organizations can then opt in, partially or completely, to accept the requirement. Generally, Army consumers at tactical and operational echelons lack consistent access to OSCAR–MS. Therefore, awareness of existing requirements, as well as knowing which producer accepted those requirements and where to find existing

products, continues to challenge the force. We should all use OSCAR–MS because Army Directive 2016-37 requires it. A new and much improved OSCAR–MS is in development. The developers should consider a tactical to national hierarchy for collection requirements and collection operations, such as those that exist in geospatial intelligence, HUMINT, signals intelligence, and COLISEUM.

**COLISEUM (The Tasking System).** COLISEUM is a web-based application to provide for online RFI and production requirement registration. Collection managers can use COLISEUM to task OSINT resources, either organic assets or external, through requests for support to answer requirements. However, the requirements must be moved manually to OSCAR–MS at operational and strategic echelons in order to reach all potential producers.

## Streamlining the Collection Management Processes for OSINT.

The connection between collection requirements management and intelligence operations is fragmented because the two preferred systems do not talk to each other. OSCAR–MS should be updated to restructure and allow organizational validation down to the lowest levels and to streamline the hierarchy of support within theaters, not just at strategic and national levels. A shared data path between the two systems would streamline collection and mitigate collection fratricide.

## Conclusion

Strategic competition means increased complexity in all warfighting domains. Hybrid warfare, including information warfare and other ambiguous actions in cyberspace, is the new normal. Therefore, we must make better use of the abundance of PAI to provide persistent information collection across our areas of interest. OSINT should be optimized in a dynamic fashion to increase the production of relevant intelligence while minimizing redundancies. Furthermore, we should harness technologies to decrease OPSEC and cybersecurity risks while increasing PAI collection and PED.

We challenge G-2/S-2s and collection managers to plan, integrate, and synchronize OSINT into all collection requirements and intelligence operations. We recommend echelons at brigade and above integrate OSINT into all plans and orders, so that requirements can be developed to leverage OSINT appropriately. OSINT requires a multifaceted joint, interagency, and multinational approach, coordinated by G-2/S-2s and collection managers at multiple echelons, to maximize the use of domain expertise, language capability, cultural understanding, proximity to the target, and sophistication of OSINT capability. Every OSINT organization in the DoD and intelligence community should collaborate and coordinate to achieve the “collect once and share broadly” objective. 

## Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-22.9, *Open-Source Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 15 August 2019) (common access card [CAC] login required).
2. National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163, 119 Stat. 3411 (2006).
3. Department of the Army, ATP 2-22.9, *Open-Source Intelligence*.
4. Department of Defense (DoD), DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC: U.S. GPO, August 8, 2016), 14.
5. Department of the Army, Army Directive 2016-37 (U.S. Army Open-Source Intelligence Activities) (Washington, DC, 22 November 2016) (CAC login required).
6. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019), 3-2.
7. “INTEllIGENCE: Open Source Intelligence,” Central Intelligence Agency website, posted July 23, 2010, last updated August 6, 2018, <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html>.
8. Department of the Army, ATP 2-01, *Plan Requirements and Assess Collection* (Washington, DC: U.S. GPO, 19 August 2014), 3-1.
9. *Ibid.*, 3-2.
10. *Ibid.*, 3-3
11. *Ibid.*, 2-3.

## References

- DoD. DoD Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*. Washington, DC: U.S. GPO, June 11, 2019.
- Department of the Army. ATP 2-33.4, *Intelligence Analysis*. Washington, DC: U.S. GPO, 10 January 2020.
- Department of the Army. Field Manual 2-0, *Intelligence*. Washington, DC: U.S. GPO, 6 July 2018.
- Department of the Army. *U.S. Army OSINT Handbook*. Fort Belvoir, VA: U.S. Army OSINT Office, 2016.
- Office of the Secretary of Defense. *Summary of the 2018 National Defense Strategy of The United States of America*. n.d. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

1LT Moriamo Sulaiman-Ifelodun is the executive officer to the U.S. Army Pacific (USARPAC) G-2, and she has served more than 5 years in the U.S. Indo-Pacific Command area of responsibility. Before commissioning in 2017, she served and deployed with 1<sup>st</sup> Special Forces Group (Airborne) as an imagery sergeant and collection manager in Operation Inherent Resolve. She holds a bachelor of science degree in toxicology and is working on her master of professional studies in public relations and communications to better promote military intelligence in the information domain and its effect on the battlefield. She has completed Basic Open-Source Intelligence (OSINT) Courses 301 and 302 and is the presumptive candidate to lead the USARPAC OSINT team.

COL Robert Wilkinson (retired) is a contractor with Northrop Grumman, supporting the Army OSINT Office from Fort Shafter, HI. Bob served for 33 years in the U.S. Army Reserve and Army National Guard in a variety of operational and intelligence billets, including multiple deployments and two tours in combat. He holds a bachelor of arts degree in history and a master of arts degree in intelligence studies. Supporting the Army OSINT program since 2014, Bob's OSINT experiences include capability developer at the U.S. Army Intelligence Center of Excellence, OSINT practitioner for USARPAC G-2, and senior trainer for the Army OSINT Office.