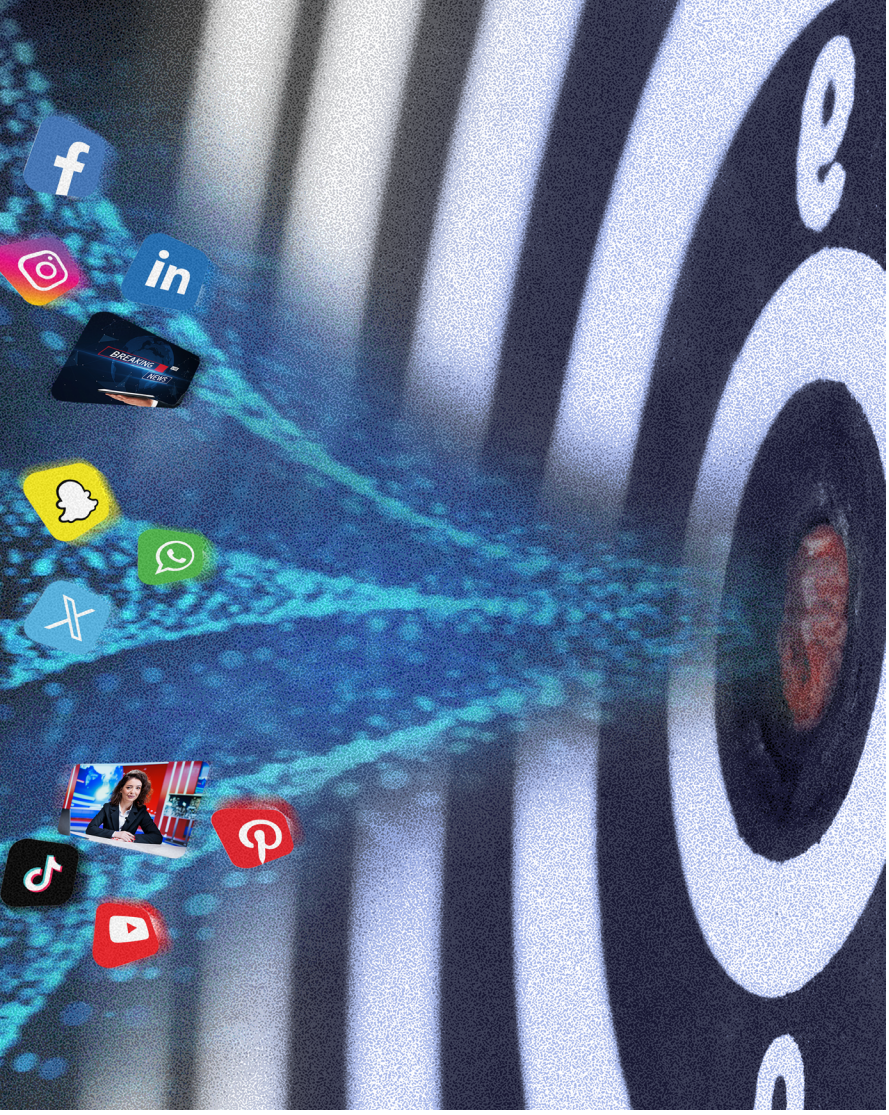

REDEFINING OPEN-SOURCE INTELLIGENCE: BUILDING A PROFESSIONALIZED, INDEPENDENT DISCIPLINE

BY DR. JEFFREY A. MADER

The views and opinions expressed in this article are those of the author and do not necessarily reflect an official policy or position of the U.S. Army Intelligence Center of Excellence or the Department of the Army.

The Case for Integration and Professionalization

The modern intelligence landscape stands at a critical juncture. The exponential growth of publicly available information (PAI), from social media to commercial satellite imagery, has fundamentally transformed how national security threats are identified and monitored. Yet institutional structures for integrating PAI remain trapped in legacy paradigms. The Army and the broader intelligence community (IC) continue to treat open-source intelligence (OSINT) as a passive supplement rather than recognizing it as a distinct, professionalized discipline worthy of equal standing.

The imperative to professionalize OSINT is not new. As early as 2005, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction sharply criticized the IC's failure to integrate OSINT into analytic workflows, labeling it underutilized and structurally marginalized.[1] Two decades later, these deficiencies persist. While the IC touts OSINT as the "INT [intelligence discipline] of First Resort,"[2] it remains conceptually and doctrinally adrift, with ambiguous definitions and unclear authorities preventing its coherent integration into broader intelligence structures.

To meet modern demands and avoid a future intelligence failure, the Army must pursue a dual transformation. First, it should institutionalize PAI research and collection as foundational skills across all intelligence disciplines. Second, it must redefine and elevate OSINT as a distinct discipline, modeled after the human intelligence (HUMINT) framework, complete with trained collectors, formal authorities, and doctrinal clarity.

The Dilemma: Accessibility Versus Professionalism

The use of PAI in intelligence has deep historical roots, from Renaissance gazettes to Cold War radio intercepts.[3] What distinguishes the modern era is the velocity, volume, and granularity of available information. Over the last decade, civilian-led efforts like Bellingcat's small army of citizen journalists have demonstrated the power of open-source methods, earning OSINT the moniker "the people's panopticon—a welcome threat to malefactors and governments with something to hide."[4]

Russia's 2022 invasion of Ukraine validated OSINT's operational relevance in unprecedented ways. As the invasion began, public messaging channels and commercial satellite imagery were the primary sources of actionable information for battlefield awareness and civilian evacuations. A federated

network of independent collectors, digital volunteers, and private-sector experts tracked troop movements, monitored refugee flows, and debunked disinformation in real time, relying exclusively on open sources. In many cases, these non-state actors outpaced state institutions in both speed and reach.[5]

Their success, however, blurred critical distinctions between amateur open-source sleuthing and professional OSINT. The visibility of these efforts fostered the mistaken belief that anyone using PAI is conducting OSINT, deepening conceptual confusion about what constitutes OSINT and who is qualified to produce it. Left unresolved, this confusion dilutes the discipline's meaning and obscures the professional standards it requires.

Publicly Available Information or Professional Open-Source Intelligence?

The democratization of information has empowered a broad pool of actors to analyze PAI, yet that accessibility has led to the conflation of general research with professional intelligence production. It is essential to distinguish between the general use of PAI and the formal practice of OSINT. U.S. Code defines OSINT as "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[6] The problem with this definition is that it frames OSINT as a product or activity, not a discipline with structural requirements like collection methodologies, validated tradecraft, certified training, and formal authorities. By this definition, anyone who reviews a website or uses Google Maps could call themselves an OSINT practitioner. This unbounded identity weakens institutional legitimacy and increases operational risk. If any PAI-based product is labeled OSINT, the term becomes professionally meaningless.

In contrast, trained OSINT collectors systematically identify and exploit sources that are not obvious or readily accessible, such as deep-web repositories and unindexed foreign-language platforms. They use custom tradecraft (e.g., Python scrapers, API queries, cross-lingual correlation) to extract what ordinary searches won't reveal. Just as HUMINT is distinguished from tactical questioning, the answer is not to restrict access to PAI but to professionalize OSINT operations as a specialized function.

Following a Proven Model

Army HUMINT provides a compelling model for professionalizing OSINT. Not all human-derived information is treated equally; a structured approach governs intelligence gathering from human sources, ranging from broad awareness to focused, legally constrained collection by trained professionals.

Congress authorizes the collection of intelligence "through human sources,"[7] and the IC defines HUMINT as "a category of intelligence derived from information collected and provided by human sources."[8] Recognizing the flaw in equating all human-derived information with HUMINT, in 2025, the Department of Defense refined this definition to "intelligence derived from information collected and provided by human sources by trained and certified HUMINT collectors holding the mission and authority to collect such information using approved HUMINT collection methodology and Defense HUMINT authorities."[9] This distinction is crucial. While many interpersonal engagements can yield information of intelligence value, not all such activity constitutes HUMINT. What distinguishes it is the combination of training, authority, and sophisticated tradecraft.

With this boundary established, the Department of Defense codified a tiered spectrum of human-source activities. At the lowest level, the "Every Soldier is a Sensor" (ES2) program draws on observations of all personnel during routine duties.[10] While ES2 may feed intelligence products, it is not considered HUMINT. At higher levels, liaison activities, debriefing, and clandestine source operations constitute formal HUMINT and are conducted solely by trained and authorized collectors. Each tier entails greater operational risk, is bound by stricter legal authorities, and demands progressively more advanced training, specialized tradecraft, and deliberate oversight.[11] This graduated structure offers a compelling precedent for professionalizing OSINT.

Defining Open-Source Intelligence as a Discipline

To professionalize OSINT, the Army should anchor it in a HUMINT-style definition that treats it as a discipline, not merely a source. This paper proposes the following Army definition: Open Source Intelligence[12] (OSINT) is a category of intelligence derived from information collected by trained and certified OSINT collectors who are assigned to organizations with the mission and authority to collect information from publicly and commercially available sources in response to validated requirements.

Unlike the definition in public law, this is an affirmative, function-based definition that mirrors HUMINT by focusing on trained collectors operating under defined authorities. Adopting it elevates OSINT from simply a product of PAI to a distinct collection discipline that transforms the vast array of public data into reliable intelligence through proven methodology and rigorous validation that surpasses non-specialist capabilities. This structured reporting distinguishes professional OSINT from PAI research and collection activities, which provide information support but not finished intelligence products like intelligence information reports. Just as HUMINT produces intelligence information reports through doctrinally governed processes, professional OSINT operations generate formal open-source intelligence reports.[13]

Legal Flexibility

Some institutional reluctance to redefine OSINT stems from perceived legal constraints. The oft-cited definition of OSINT is drawn from a congressional finding in the 2006 National Defense Authorization Act, now codified at *50 U.S.C. § 3038*. However, as administrative law makes clear, findings and prefatory text do not carry the weight of statutory mandates.[14] Courts have consistently held that such language does not limit agency discretion.[15]

The Army, and by extension the Department of Defense, retains full discretion to adopt a more nuanced definition of OSINT tailored to its operational and doctrinal needs. This discretion will continue should future legislation codify a new IC definition of OSINT. This flexibility invites innovation. Rather than clinging to a minimalist definition from two decades ago, the Army should articulate a doctrine that reflects the modern information environment, anchored in professionalization, accountability, and specialization.

A Necessary Foundation

Intelligence professionals emphasize that OSINT should be defined by the intent, process, and policy underpinning its use.[16] Only trained practitioners in validated collection activities can convert the noise of PAI into clear, dependable intelligence. However, the broader use of PAI remains essential to all intelligence activities.[17]

The Army has taken meaningful steps in this regard with the publication of Army Directive 2025-15, which frames the safe, ethical, and technically sound use of PAI.[18] This directive establishes PAI research and collection as foundational skills for all intelligence professionals and provides access to low-risk U.S. Government-owned or controlled websites. This enables Soldiers to quickly access tactically relevant information without incurring the risk of interacting with the broader internet, something for which OSINT collectors are specifically trained and equipped.

From advanced individual training forward, analysts are introduced to browser safety, metadata awareness, and structured search strategies.[19] Yet without doctrinal clarity, this initial training generates ambiguity.[20] If a junior analyst finds a key insight in public information and includes it in an all-source product, is that OSINT? Disciplined conceptual separation can resolve this ambiguity. PAI research and collection must be seen as universal capabilities applied within risk-informed boundaries. OSINT, however, should be treated as a formal discipline executed by trained specialists operating under unique legal, procedural, and technical authorities to exploit hidden, unindexed sources and generate insights beyond the reach of casual PAI collection.

Next Steps

The Army began building an OSINT training pipeline before the Ukraine conflict, and practitioners have since provided timely intelligence that demonstrates the discipline's tactical value in real-world operations.[21] Yet these practitioners have often succeeded despite institutional structures, not because of them. Working in doctrinal vacuums with little authoritative guidance, they effectively built the OSINT discipline on the fly. While the initiative displayed is commendable, this improvisational success is not sustainable. Without formal recognition and professionalization, the Army risks allowing this hard-won capability to stagnate.

A key reason for this potential regression is the lack of professional indicators. OSINT must transition from a catch-all practice to a defined profession that shares core features with other intelligence specialties: labor specialization, recognized tradecraft, credentialing mechanisms, and authoritative outputs.[22] While geospatial intelligence (GEOINT) and signals intelligence meet this standard, HUMINT offers a particularly instructive model for establishing these professional foundations.

Toward a Professionalized Future

To formally institutionalize OSINT as a distinct profession, this article proposes a hierarchical practitioner model, conceptually akin to HUMINT's graduated authorities. This framework acknowledges varying degrees of training, access, and operational responsibility:

- **PAI Research and Collection User:** Baseline fluency in open-source environments for all intelligence personnel. This category requires no specific OSINT funding and is limited to low-risk PAI sources. It enables general intelligence personnel to use PAI in support of their mission.
- **Advanced PAI Research and Collection User:** Engages in medium-risk PAI collection. Funded by individual commands as needed, this role requires specific training and technology but lacks formal OSINT mission authorities and is not considered formal OSINT.
- **Tier 1 OSINT Collector:** Operates with programmatic funding and an authorized OSINT mission, engaging in high-risk collection. Requires completion of an OSINT Basic Course covering advanced tradecraft, technology, and legal authorities. Produces formal open-source intelligence reports and operates under structured oversight.
- **Tier 2 OSINT Collector:** Represents the highest tier, with programmatic funding and an authorized mission for sensitive collection. Requires an OSINT Advanced Course covering sophisticated attribution management and advanced techniques.

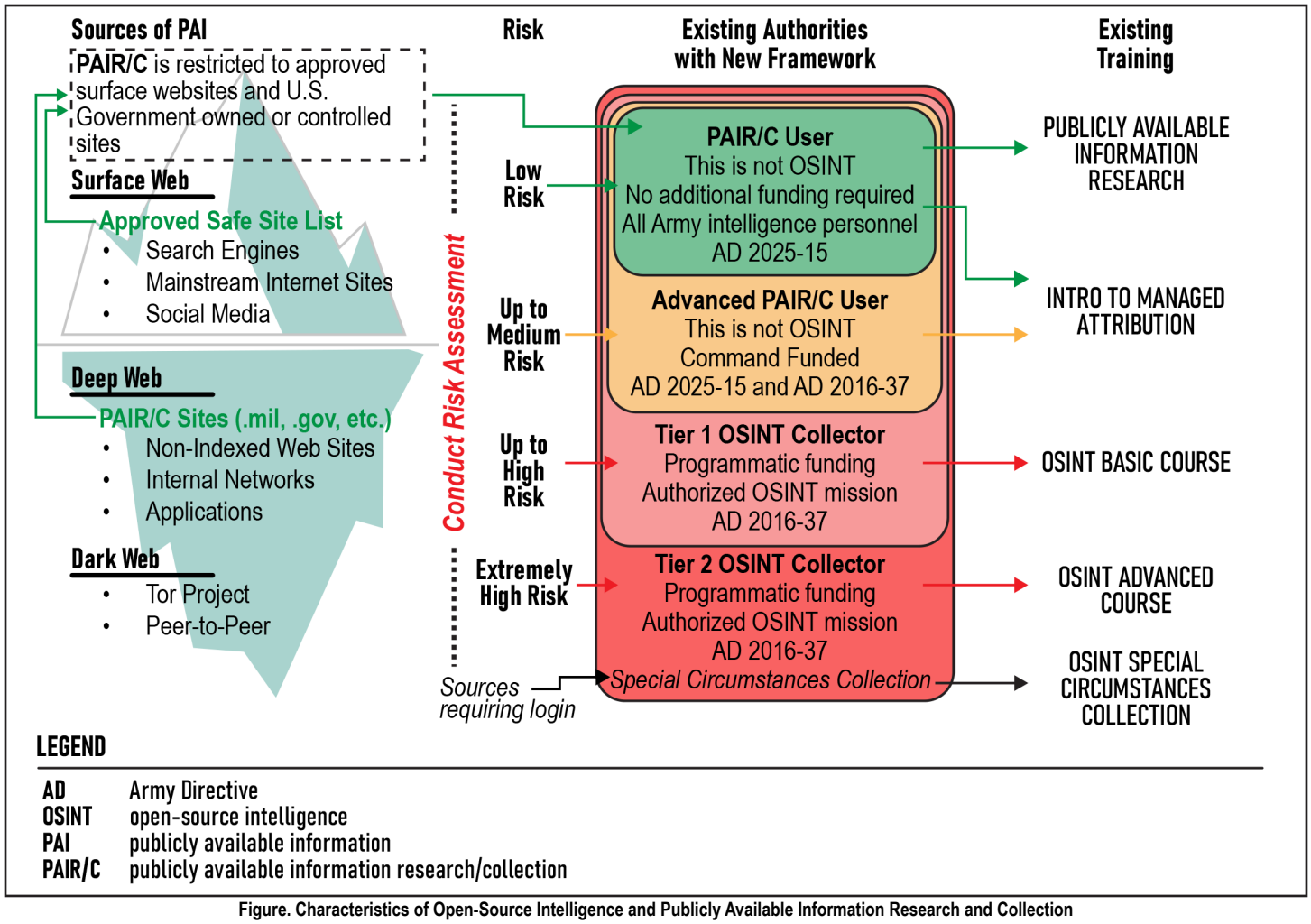

Figure. Characteristics of Open-Source Intelligence and Publicly Available Information Research and Collection

The Army has already established many essential components of this model. From an authority perspective, Army Directive 2025-15 created the PAI research and collection user roles, while Army Directive 2016-37 formally recognized OSINT as a distinct discipline.[23] The Army has also established programmatic funding to support its OSINT Enterprise.[24]

Training already exists to support this model. The PAI Research Course ensures that all intelligence personnel possess baseline proficiency in PAI use.[25] For advanced PAI research and collection activities, managed attribution training provides the technical skills needed. The OSINT Basic Course is an additional skill identifier training program whose graduates are certified OSINT collectors.[26] Finally, the OSINT Advanced Course and Special Circumstances Collection Course provide the technology and tradecraft required for extremely high-risk, special circumstances collection.

Key Implementation Considerations

Integration remains a critical gap. Among the missteps identified by the Weapons of Mass Destruction Commission report, the underutilization of OSINT remains prescient.[27] At the time, agencies lacked formal processes to collect, analyze, and disseminate PAI effectively. As a result, OSINT is often viewed as a secondary source or used merely to support traditional collection disciplines rather than being treated as a stand-alone discipline.[28]

Two decades after the Commission's report, OSINT is still not fully integrated into the intelligence process; it lacks formal tasking, collection, processing, exploitation, and dissemination; and it remains undervalued. Integrating PAI research and collection, and OSINT, into the Army's intelligence process is crucial to maximizing their value. This integration starts with clearly defining intelligence objectives, with PAI research and collection as the initial action for all intelligence personnel. Once PAI research and collection resources are exhausted, soldiers can request OSINT support to gather information from hard-to-identify sources.

OSINT collection plans should leverage diverse sources across tiers to ensure comprehensive coverage. Standardized processing and AI-enabled tools will enhance analysis, while integrating insights from all OSINT tiers into final assessments is essential. Tailored intelligence products should reflect findings from all tiers to meet commanders' needs, and feedback mechanisms will support continuous improvement, ultimately enhancing the Army's overall intelligence capabilities.

Institutionalizing Open-Source Intelligence Before the Next Crisis

Open information is abundant; intelligence is scarce. What distinguishes the two is disciplined collection, validated

tradecraft, and alignment to mission requirements. If the Army conflates simple PAI use with formal OSINT, it will lack the coherence required for the next conflict. Institutionalizing PAI research and collection ensures that every intelligence professional can safely exploit public information—but codifying OSINT as a distinct discipline, anchored in training, authorities, and outputs, will transform access into advantage.

This article advocates for doctrinal changes to make PAI research and collection fundamental components for all intelligence professionals and to incorporate OSINT into the intelligence process to guarantee its proper use. Without properly employing OSINT specialists, commanders risk blind spots, misinterpretation, and legal exposure. With it, they gain access to unique data, faster insights, validated intelligence, and assurance of compliance. This transformation is essential for the Army to avoid potential failures and ensure that information is processed and employed rigorously.

The Army stands at a pivotal moment, analogous to the birth of GEOINT during World War II or the formalization of HUMINT in the Cold War.[29] OSINT can either remain an undefined supplement or be deliberately shaped into a profession. The proposed framework captures OSINT's potential while establishing the professional boundaries necessary for institutional legitimacy and operational effectiveness.

The path forward is clear: establish PAI research and collection as the foundation for universal PAI literacy while simultaneously building OSINT as a specialized discipline with its own training pipeline and authoritative outputs. This dual approach acknowledges the democratization of information while maintaining the professional standards essential for intelligence operations. Without professionalization, OSINT will remain a fragmented supplement. With it, the Army gains a disciplined capability essential for decision dominance in an increasingly transparent and contested information environment.

Endnotes

In memory of Colonel (retired) Eric Heist, whose mentorship and support through countless conversations and draft reviews made this article possible.

1. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Government Publishing Office [GPO], 2005), https://govinfo.library.unt.edu/wmd/report/wmd_report.pdf.

2. Office of the Director of National Intelligence, *The IC OSINT Strategy*, 2024–2026 (GPO, 2024), front cover, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

3. Ludo Block, "The Long History of OSINT," *Journal of Intelligence History* 23, no. 2: 95–109, https://doi.org/10.1080/16161262.2023.2224091; and Joseph E. Roop, *Foreign Broadcast Information Service: History, Part I, 1941–1947* (Central Intelligence Agency, April 1969), https://www.cia.gov/readingroom/sites/default/files/FBIS_history_part1_0.pdf. Declassified August 10, 2009.

4. "The Promise of Open-Source Intelligence," *The Economist*, August 7, 2021, https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence.

5. Gabriel Geiger and Sebastian Skov Andersen, "Inside the OSINT Operation to Get Foreign Students Out of Ukraine," *VICE*, March 18, 2022, https://www.vice.com/en/article/inside-the-osint-operation-to-get-foreign-students-out-of-ukraine/.

6. National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109–163, 119 Stat. 3136, https://www.congress.gov/109/plaws/publ163/PLAW-109publ163.pdf.

7. Director of the Central Intelligence Agency, *50 USC §3036*, https://uscode.house.gov/view.xhtml?req=(title:50%20section:3036%20edition:prelim).

8. Office of the Director of National Intelligence, Intelligence Community Directive 304: Human intelligence (GPO, 2008), https://www.odni.gov/files/documents/ICD/ICD-304.pdf. Amended in July 2009.

9. Office of the Under Secretary of Defense for Intelligence and Security, *DoD Directive 5200.37: Defense Human Intelligence* (Department of Defense, 2025), 13, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520037p.PDF?ver=6bUKd1-XwoCriO_O6ADQ7A%3D%3D.

10. Stew Magnuson, "Army Wants to Make 'Every Soldier a Sensor'," *National Defense*, May 1, 2007, https://www.nationaldefensemagazine.org/articles/2007/5/1/2007may-army-wants-to-make-every-soldier-a-sensor.

11. Department of the Army, Field Manual 2-22.3, *Human Intelligence Collector Operations* (GPO, 2006), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43392-FM_2-22.3-001-WEB-4.pdf.

12. Open source intelligence should not be hyphenated. Where "open-source" is an adjectival phrase describing "intelligence," placing a hyphen between "open" and "source" is grammatically correct according to most style guides (i.e., APA, MLA); however, "open source intelligence" is a noun phrase as the three words collectively describe a single thing (i.e., OSINT). In a noun phrase, the adjectives "open" and "source" do not simply modify the noun "intelligence;" rather, all three words become a single noun and do not require hyphenation between the adjectives.

13. Matthew D. Skilling, "Mapping the Information Environment with Open-Source Intelligence and Allies," *Military Intelligence Professional Bulletin* 48, no. 1 (April 2022): 27–29, https://mipb.ikn.army.mil/issues/pai-for-int-purposes/.

14. United States v. Morrison, 529 U.S. 598 (2000), https://supreme.justia.com/cases/federal/us/529/598/.

15. Reeves v. Astrue, 526 F.3d 732 (11th Cir. 2008), https://www.justice.gov/sites/default/files/osg/briefs/2009/01/01/2008-1322.pet.rep.pdf.

16. Corrinne Geiger, "The Reawakening of Open-Source Intelligence," *Military Intelligence Professional Bulletin* 48, no. 1 (April 2022): 9–12, https://mipb.ikn.army.mil/issues/pai-for-int-purposes/.

17. Laura Potter and Christina Bembenek, "The Risk of Not Knowing: Enabling Intelligence Professionals to Leverage Publicly Available Information," *Military Intelligence Professional Bulletin* 48, no. 1 (April 2022): 5–8 https://mipb.ikn.army.mil/issues/pai-for-int-purposes/.

18. Department of the Army, Army Directive 2025-15, *Use of Publicly Available Information for Intelligence Activities* (GPO, 2025), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN44787-ARMY_DIR_2025-15-000-WEB-1.pdf.

19. Anthony R. Hale, "Always Out Front," *Military Intelligence Professional Bulletin* 48, no. 1 (April 2022): 3–4. https://mipb.ikn.army.mil/issues/pai-for-int-purposes/.

20. Jarrod R. Gack, "The Open-Source Intelligence Conundrum: Creating the Discipline or Integrating the Data?" *Military Intelligence Professional Bulletin* 48, no. 1 (April 2022): 17–22. https://mipb.ikn.army.mil/issues/pai-for-int-purposes/.

21. Skilling, "Mapping the Information Environment"; and Christina Bembenek and Chels Michta, "Allies and Open Sources: Lessons from Northern Raven, the Largest OSINT Collection Operation in NATO's History," Modern War Institute, June 28, 2024, https://mwi.westpoint.edu/allies-and-open-sources-lessons-from-northern-raven-the-largest-osint-collection-operation-in-natos-history/.

22. Chris Rasmussen, "How the Intelligence Community Has Held Back Open-Source Intelligence, and How It Needs to Change," Center for the Study of Intelligence, *Studies in Intelligence* 68, no. 2 (June 2024): 47–51, https://www.cia.gov/resources/csi/static/Commentary-How-Open-Source-Limitations-Must-Be-Overcome.pdf.

23. Department of the Army, Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities* (GPO, 2016).

24. Nathaniel Rushing (Department of the Army, Office of the Deputy Chief of Staff for Intelligence, Open-Source Intelligence Lead), interview with the author, March 15, 2025.

25. Hale, "Always Out Front."

26. Department of the Army, Pamphlet 611-1, *Military Occupational Classification and Structure* (GPO, 2022), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36922-PAM_611-21-000-WEB-2.pdf.

27. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*.

28. J. Kelly, personal communication about remarks on OSINT collection and analysis integration presented at the Guidehouse Federal Open-Source Intelligence Community of Practice seminar, October 17, 2024.

29. Cooper-Morgan Bryant, "Out in the Open: U.S. GEOINT and OSINT in the Cold War 1946-1986" (master's thesis, Harvard University Division of Continuing Education, 2024), https://dash.harvard.edu/entities/publication/85ef3997-ee70-4d51-86d1-da8294a9e776.

Dr. Jeffrey Mader serves as a contract consultant for the Headquarters, Department of the Army, Deputy Chief of Staff for Intelligence, where he is responsible for developing open-source intelligence policy. Before his current role at the Pentagon, he built a multimillion-dollar business unit that provides threat intelligence and privacy protection support to ultra-high-net-worth individuals and corporations. His previous experience includes providing signature reduction and due diligence support to a special mission unit and the Defense Intelligence Agency. Dr. Mader is also the founder and director of the Penrose Institute, a non-profit dedicated to the formalization and expanded application of identity management. Dr. Mader earned a PhD from Oklahoma State University, a Master of Business Administration from George Washington University, and a bachelor's degree from Georgetown University.