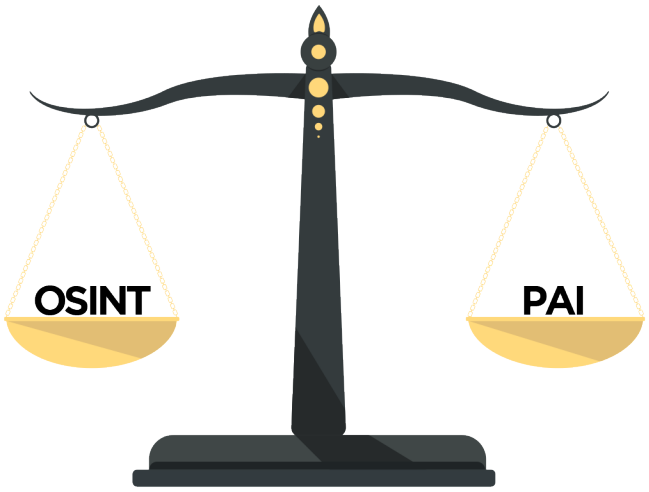


By Chief Warrant Officer 4 Jarrod R. Gack (Retired)

THE OPEN-SOURCE INTELLIGENCE CONUNDRUM: CREATING THE DISCIPLINE OR INTEGRATING THE DATA?

The views expressed in this article are the author's alone and do not necessarily reflect the opinion of Science Applications International Corporation (SAIC) or any U.S. Army organization.

Introduction

In 1992, ADM William Studeman, then Director of the National Security Agency (NSA) and former Acting Director of the Central Intelligence Agency (CIA), gave a presentation on the history of the Foreign Broadcast Information Service (FBIS), the predecessor to today's CIA Open Source Enterprise. Reflecting on the end of the Cold War, ADM Studeman opined that throughout the intelligence community "no area is full of more promise for intelligence than open source access and exploitation."[1]

ADM Studeman's comments may have shocked some in the audience given his leadership in America's human intelligence (HUMINT) and signals intelligence (SIGINT) disciplines, but his comments were hardly novel. In 1947, U.S. intelligence pioneer Sherman Kent estimated that 80 percent of the information policymakers require could be found in open sources.[2] Former Director of the Defense Intelligence Agency LTG Samuel Wilson went further, estimating that open sources account for 90 percent of relevant intelligence.[3]

Despite its apparent popularity, open-source intelligence (OSINT) made little progress through the early 21st century. In 1997, CIA budget cuts nearly dissolved FBIS. A decade later, a congressional report found that intelligence professionals "disagree over [open source information's] value relative to that of clandestinely-collected secret information."[4] Demonstrating the point, a 2005 article in *The Washington Times* quoted an unnamed Director of Central Intelligence, claiming "I only have money to pay for secrets" when confronted with an OSINT-related proposal.[5]

Congress was more confident in OSINT. In 2004, it passed the Intelligence Reform and Terrorism Prevention Act, which identified OSINT as "a valuable source that must be integrated into the intelligence cycle [process]."[6] A few months later, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* indicated that "the need for exploiting open source material is greater now than ever before" but also that "the Intelligence Community's open source programs have not expanded commensurate with either the increase in available information or with the growing importance of open source data."[7] By 2006, OSINT had entered federal law through the National Defense Authorization Act. The act included a number of OSINT-related provisions, including a mandate for the Defense Intelligence Enterprise to establish plans for an OSINT specialty in the Services.[8]

The advent of social media was likely the driver for Congress's interest. In mid-2004, Myspace became the first social media platform to record one million active users. Within 3 years, YouTube had achieved nearly 150 million subscribers.[9] Over the next decade, social media—applications and platforms enabling users to create and share content about their lives—would expand to reach nearly one in three people on Earth.[10]

Nearly two decades since the Intelligence Reform and Terrorism Prevention Act was signed into law, little OSINT integration has occurred. The Office of the Director of National Intelligence identifies OSINT as a separate discipline, but the Department of Defense (DoD) has failed to truly integrate it into the intelligence process or to establish OSINT specialties in the Services. OSINT operations remain ad hoc, budgetary support remains limited, and even regulatory guidance is practically nonexistent. As global public data continues to increase, questions abound. What is OSINT? How is it different from publicly available information (PAI), and why do we care? Why, despite endorsement from the Director of National Intelligence and countless intelligence community leaders, does it remain a virtual afterthought in most intelligence organizations?[11] Is OSINT a discipline, or should PAI be just another data source?

The OSINT Conundrum

Disagreements continue over the distinction between OSINT and PAI. Army policy requires special authorities and additional

training to collect, exploit, or produce OSINT-derived products.[12] PAI requires no additional training or authority. The permissiveness offered by avoiding "OSINT" creates a natural incentive for intelligence professionals to forgo "OSINT activities" in favor of "PAI exploitation." The question is, can they?

Neither federal law nor executive order defines PAI, but DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, defines PAI as—

> ***Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.[13]***

PAI is information accessible to the public, including information the public can purchase. Unlike PAI, federal law does define OSINT in the 2006 National Defense Authorization Act:

> ***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.[14]***

OSINT is produced using PAI that addresses an intelligence requirement. In other words, any intelligence-related PAI collection, exploitation, or production—whether conducted by a trained "OSINTer" or another single-source intelligence element—qualifies as OSINT.

The implications are significant. Despite training mandates, the Service provides no force structure and few program resources to sustain an OSINT capability. As a result, most organizations have the choice of either gutting other intelligence capabilities to pursue OSINT or accepting a prohibition on the use of PAI. Given its widespread availability, low acquisition cost, and increasing relevance to national security, excluding PAI from intelligence activity is unproductive.

Fortunately, it is also unnecessary—at least from a practical perspective. While Army and joint publications recognize OSINT as a separate discipline, they fail to define what makes OSINT unique; therefore, they also fail to define what activities require additional training and authorization.[15] Moreover, many conventional disciplines already collect PAI in some form, often as part of their mission. For example—

- Internet Relay Chat (IRC) chats and message boards certainly are "communications systems," a component of SIGINT.[16]
- Instagram photos, Google Street View imagery, and commercial satellite photography all fit into definitions of imagery intelligence.[17]
- Ship and aircraft transponder signatures, reported over publicly available Automatic Identification System and Automatic Dependent Surveillance-Broadcast systems, fit well into the NSA's definition of electronic intelligence.[18]

Presumably, the OSINT discipline must involve some discrete characteristics that other disciplines do not have. By defining these, Army intelligence can better determine which PAI-related activities require OSINT-specific training and authorities and which may be pursued by other disciplines. In an attempt to better characterize the difference between "OSINT the discipline" and other intelligence applications for PAI, let's examine OSINT's unique characteristics.

Defining the Discipline

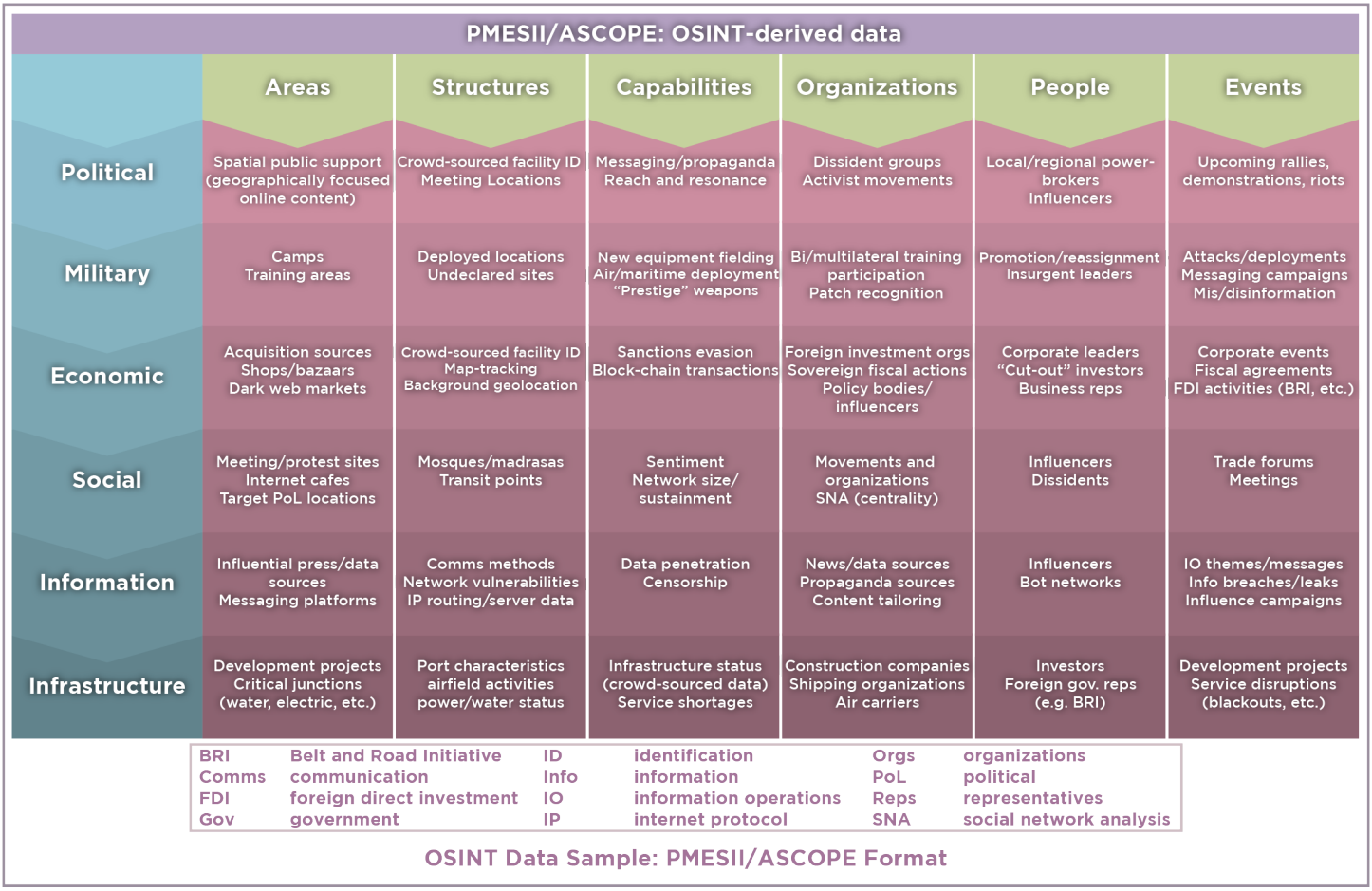
JP 2-0, *Joint Intelligence*, defines intelligence disciplines as "well-defined areas that involve specific categories, collections, and analysis with emphasis on technical or human resources capabilities."[19] This is not universally true of OSINT, at least not the legal definition. That definition—which effectively says that OSINT is any PAI used for intelligence purposes—includes commercial imagery, communications systems, electronic emissions, and a host of other data that are already germane to other disciplines.

While the legal definition of OSINT is too broad to align neatly with the characteristics of a discipline, recent experiences in the public and private sector demonstrate a number of unique features that can identify influence activities and drive kinetic operations. Recent publications also indicate that certain data categories and collections are unique to OSINT. These include—

- Collection of bulk volume and content data across public platforms.
- Collection of location indicators, including textual clues and background features.
- Collection of social network information, based on user content and online interaction.
- Exploitation of metadata embedded in digital files, including images and videos.
- Exploitation of transaction data, including block-chain and foreign currency transfers.
- Detection of bots, using transmission volume and online transmission patterns.
- Exploitation of dark web content, including the use of commercial indexing tools.[20]

The operational variables (political, military, economic, social, information, infrastructure [PMESII]) and civil considerations (areas, structures, capabilities, organizations, people, and events [ASCOPE]) provide a way to structure OSINT collections and data. The table, on the next page, provides an example for grouping OSINT data using these analytic frameworks.

In many cases, information pertinent to other single-source elements is also online. Often, PAI offers a less intrusive, cheaper mechanism for acquisition without relying on the intelligence community's more traditional collection systems.



OSINT Data Sample: PMESII/ASCOPE Format

Managing OSINT as a distinct discipline does not prevent its use by other intelligence activities, nor does it mean that any intelligence activity using PAI should be bound by OSINT-specific training and authority requirements. PAI offers value to every intelligence discipline; the challenge is how to shed the bureaucratic burden without undermining effectiveness.[21]

Single-Source OSINT Integration

Social media purportedly offers something for everyone. It turns out that "everyone" includes the Army's other single-source disciplines. Social media is not alone in this regard: PAI, which now comprises nearly two billion active websites, five billion social media profiles, and billions of daily users, offers a treasure trove of single-source data.

HUMINT

Over the past few years, academics have written volumes on the threat that technology poses to HUMINT activities, including statements contending digital integration creates an environment prohibitive to spy work. As the argument goes, on one hand, adversaries can access online personal data, preventing would-be agents from assuming new identities, and on the other hand, a limited online footprint invites scrutiny because it is anomalous.[22]

Although the internet is responsible for many of these challenges, it may also be the solution. Ubiquitous data platforms, such as social media, present a virtually unlimited pool of potential sources, many of whom volunteer details of their placement and access online. Chat programs, job forums, dating sites, and other networking platforms offer easy opportunities to establish contact and build rapport. America's adversaries have certainly made use of the online environment. For example, from 2014 through 2018, the Islamic State of Iraq and Syria (ISIS) choreographed a spectacularly successful online recruitment campaign, attracting up to 40,000 foreign nationals from 110 different countries.[23] Some studies indicate that recruits so deeply immersed themselves in ISIS's ideology that they were willing to kill for the group without ever having met an actual ISIS member.[24]

Virtual HUMINT may offer options to maintain source networks while reducing scrutiny from adversaries. A 2015 study from the Naval Postgraduate School assessed available online platforms, the source acquisition cycle, and source maintenance in a virtual environment. The study's author found that—

> ***The online environments of social networking, dating, and gaming can serve as effective mechanisms for the virtual recruitment of human sources. Furthermore, most of the countries and territories that are of interest for intelligence collectors can be accessed through these environments—making virtual HUMINT not only a possibility but also a realistic option.***[25]

GEOINT

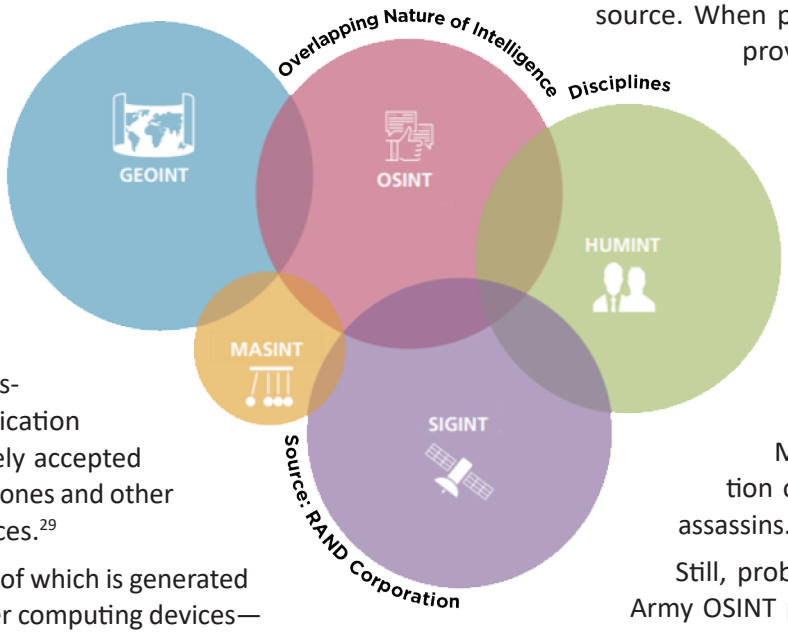
Unlike HUMINT, geospatial intelligence (GEOINT) has integrated open-source data for years. Beginning in the 1990s, America's GEOINT organizations began purchasing commercial imagery to fill coverage gaps and acquire releasable content for partners. In late 2008, the National Geospatial-Intelligence Agency expanded the intelligence community's commercial imagery acquisitions, awarding the $7 billion commercial imagery contract to private sector companies.[26]

The National Reconnaissance Office has since assumed management of the contract and plans to expand its commercial partnerships significantly.

This trend will likely accelerate. Over the past two decades, the commercial imagery market has exploded worldwide, with top satellite manufacturers fielding more than 300 imaging platforms in the past decade. Commercial platforms now deliver better image quality than spy satellites did just two decades ago. Furthermore, ground-based imagery from social media users, bloggers, activists, and other sources continue to expand at a breakneck pace, offering a low-cost source of high-resolution, multi-angle imagery for exploitation.[27]

SIGINT

The NSA defines SIGINT as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems."[28] While NSA rarely discusses the exact communication systems targeted, it is widely accepted that this includes cellular phones and other connected computing devices.[29]



The growth of PAI—much of which is generated on cellular phones and other computing devices—offers a glut of SIGINT-relevant data. Social media "friends," "likes," and "shares" offer insight into network structures and relations. Website posts and IRC chats offer context and the ability to monitor target interaction. In many instances, traditional SIGINT and emerging OSINT functions overlap:[30]

- Both disciplines define networks based on communication activities (cellular metadata versus Facebook friends).
- Both disciplines glean understanding from message content (telephone conversations versus chat features).
- Both disciplines collect from the target's perspective, making both vulnerable to bias and inaccuracy but also useful for sentiment sampling.

Integrating OSINT and SIGINT is not only logical, but the defining characteristics of each discipline incorporate similar concepts. A recent survey found that nearly three quarters of respondents used social media as a primary communication system, making social media an explicit target for SIGINT collection.[31] Conversely, much of the content on social media is publicly available, making it an explicit OSINT target as well. The same goes for nearly every social media platform, chat server, and content hosting site on the web.

The challenge is policy. Army directives layer additional authority, training, and oversight requirements on intelligence professionals planning to exploit PAI with no exception for information that is already germane to other disciplines. This creates an incentive either to ignore Army mandates or to ignore the troves of information awaiting discovery online.

Recommendations

OSINT—whether a separate discipline or a contributor to other single-source activities—represents the world's largest, cheapest, most accessible intelligence source. When pursued aggressively, it has proven invaluable to national security operations. Though Army OSINT successes remain classified, widely publicized OSINT vignettes demonstrate the utility of focused PAI exploitation. Examples of these are Russia's role in the downing of Malaysian Airlines flight MH17 and the identification of Sergei Skripal's would-be assassins.[32]

Still, problems are everywhere. The Army OSINT program is lacking in scope and resourcing, training is not institutionalized, and policy is limited and outdated. Additionally, few dedicated OSINT personnel remain on modified tables of organization and equipment or tables of distribution and allowances across the force. Today's challenges are not insurmountable, but they will require a dedicated effort and real prioritization from Army intelligence leaders. The following recommendations may constitute a good starting point: (1) formalize the Army OSINT discipline and (2) resolve OSINT policy conflicts.

Formalize the Army OSINT Discipline. The Army has made some incremental progress toward formalizing OSINT over the past 6 years. This includes publishing an Army techniques publication (ATP 2-22.9, *Open-Source Intelligence*); a Service-level OSINT strategy, Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities*; and a DOTMLPF–P assessment.[33] Yet, OSINT remains largely an ad hoc operation with incomplete policy and almost no program support.

With PAI growth continuing to outpace exploitation capability, incremental progress is no longer adequate. Army intelligence leaders must decide how to treat OSINT and PAI and determine what capabilities are required to effectively

integrate public data into Army intelligence activities. A good place to start is by clearly delineating discipline-specific OSINT tasks and functions from other single-source applications. Next, the Army G-2 should work with Army major commands and Army Service component commands to formulate a Service-wide OSINT requirement. This requirement should include specific short-term, mid-range, and long-term objectives, with accompanying resource and personnel requirements, and should receive the Army G-2's endorsement before submission to the appropriate program evaluation group.

Resolve OSINT Policy Conflicts. Army OSINT policy is not only outdated and incomplete, but it is also inconsistent with joint doctrine. For instance, JP 2-03, *Geospatial Intelligence in Joint Operations*, mentions GEOINT applications for commercial imagery and open-source data nine times,[34] but the Army directive prohibits collection of either without separate written authority, a separate collection plan, and additional training. In many cases, single-source elements are not even aware of these requirements. One reason is the absence of an Army regulation clarifying OSINT- and PAI-related requirements. That document remains in draft, despite an Army directive calling for its publication by late 2019.

Army G-2 leaders must prioritize publication of the OSINT Army regulation. In addition to clarifying authority processes, the Army regulation should differentiate between discipline-specific requirements and other single-source OSINT applications and clarify OSINT-related responsibilities at the Department of the Army G-2, U.S. Army Intelligence and Security Command, and U.S. Army Intelligence Center of Excellence. Finally, the regulation should prescribe a governance process that includes all Army major commands.

Conclusion

As ADM Studeman observed nearly three decades ago, public information holds staggering potential for Army intelligence. The Army has yet to realize that potential, or aggressively pursue OSINT integration, as directed by law. Opportunities remain, but time is fleeting. As technology continues to evolve, making up for lost time will become more challenging and demand even greater investment. We can only hope that we have moved past "only paying for secrets."

Endnotes

1. William O. Studeman, "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information," *Competitive Intelligence Review* 4, no. 1 (Spring 1993): 25, https://onlinelibrary.wiley.com/doi/abs/10.1002/cir.3880040106. This article was based on a presentation ADM Studeman gave at the 1992 symposium on "National Security and National Competitiveness: Open Source Solutions," in McLean, VA.

2. Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for a National Defense Establishment, Submitted by Allen W. Dulles, April 25, 1947, reprinted in U.S. Congress, 80th Congress, 1st Session, Senate, Committee on Armed Services, *National Defense Establishment (Unification of the Armed Services)*, Hearings, Part 1, 525.

3. Donna O'Harren, "Opportunity Knocking: Open Source Intelligence for the War on Terrorism" (thesis, Naval Postgraduate School, Monterey, CA, December 2006), 9.

4. Richard A. Best Jr. and Alfred Cumming, *Open Source Intelligence (OSINT): Issues for Congress* (Washington, DC: Congressional Research Service, Library of Congress, 2007, updated 2008), 2.

5. Ronald A. Marks, "Spying and the Internet," *Washington Times*, April 24, 2005, https://www.washingtontimes.com/news/2005/apr/24/20050424-101721-8924r/.

6. Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 1052 (2004).

7. Laurence H. Silberman and Charles S. Robb, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, DC, 31 March 2005), 378.

8. National Defense Authorization Act for Fiscal Year 2006, H.R. 1815, 109th Cong., § 931 (2006).

9. Esteban Ortiz-Ospina, "The rise of social media," Our World in Data, 18 September 2019, https://ourworldindata.org/rise-of-social-media.

10. Ibid.

11. Avril Haines and Stephanie O'Sullivan, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation* (Washington, DC: Center for Strategic and International Studies, 2021), xi, 20. Avril Haines currently serves as the Director of National Intelligence.

12. For more, see Exec. Order No. 12333, 3 C.F.R. 200 (1981); Department of Defense (DoD), DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC, August 8, 2016); Department of the Army, Army Regulation 381-10, *U.S. Army Intelligence Activities* (Washington, DC: U.S. Government Publishing Office [GPO], May 3, 2007); and Army Techniques Publication (ATP) 2-22.9, *Open Source Intelligence* (Washington, DC: U.S. GPO, August 2019).

13. DoD, DoD Manual 5240.01, *Procedures Governing the Conduct*, 53.

14. National Defense Authorization Act.

15. Department of the Army, ATP 2-22.9, *Open-Source Intelligence*, v; and Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 22 October 2013), B-1.

16. "Signals Intelligence," National Security Agency/Central Security Service, accessed 19 August 2021, https://www.nsa.gov/Signals-Intelligence/.

17. "What is Intelligence?" Office of the Director of National Intelligence, accessed 19 August 2021, https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

18. Richard L. Bernard, *Electronic Intelligence (ELINT) at NSA* (Fort Meade, MD: Center for Cryptologic History, 2009), 1.

19. Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, B-1.

20. Meysam Alizadeh, Jacob N. Shapiro, Cody Buntain, and Joshua A. Tucker, "Content-based features predict social media influence operations," *Science Advances* 6, no. 30 (22 July 2020); Youri van der Weide, "Using the Sun and the Shadows for Geolocation," Bellingcat, December 3, 2020; and "US Air Force Targets and Destroys ISIS HQ Building Using Social Media," Military.com, 3 June 2015.

21. For more on OSINT as a discipline and data source, see Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), ix.

22. Hundreds of articles and publications discuss this topic, including Kyle S. Cunliffe, "Hard target espionage in the information era: new challenges for the second oldest profession," *Intelligence and National Security* 36, no. 7 (2021): 1018–1034, https://doi.org/10.1080/02684527.2021.1947555; Edward Lucas, *Spycraft Rebooted: How Technology is Changing Espionage* (Seattle: Amazon Publishing, 2018); David V. Gioe, " 'The More Things Change': HUMINT in the Cyber Age," in *The Palgrave Handbook of Security, Risk and Intelligence*, ed. Robert Dover, Huw Dylan, and Michael S. Goodman (London: Palgrave Macmillan, 2017), 213–227; Robert M. Clark, *Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2014); and Devin Streeter, "Biometrics and Intelligence Asset Protection: Biometric Technology and its Impact on Counterintelligence and Intelligence" (unpublished paper, Liberty University Helms School of Government, Lynchburg, VA, 2013).

23. Antonia Ward, "ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa," *The RAND Blog*, RAND Corporation, December 11, 2018, https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html.

24. Makenzi Taylor, "ISIS Recruitment of Youth via Social Media," *Global Affairs Review* (February 2, 2020); and Ata AlSarayreh, "How ISIS uses social media for recruitment" (thesis, Canadian Forces College, Ottawa, 2020).

25. Dori Koren, "Virtual HUMINT: conducting human intelligence operations in the virtual environment" (thesis, Naval Postgraduate School, Monterey, CA, 15 September 2015).

26. Kelsey Atherton, "The commercial imagery that will benefit national security challenges," C4ISRNET, 5 September 2018, https://www.c4isrnet.com/c2-comms/satellites/2018/09/05/nro-to-take-over-major-contract-from-nga/.

27. "Disruptive microsatellite imager captures images of less than a metre resolution," Community Research and Development Information Service, accessed November 8, 2021, https://cordis.europa.eu/article/id/413233-disruptive-microsatellite-imager-captures-images-of-less-than-a-metre-resolution.

28. "Signals Intelligence," National Security Agency/Central Security Service, accessed November 8, 2021, https://www.nsa.gov/Signals-Intelligence/Overview/.

29. Ryan Goodman and Derek Jinks, "Military Targeting Based on Cellphone Location," Just Security, February 18, 2014, https://www.justsecurity.org/7200/military-targeting-based-cellphone-location/; Faye Bowers, "Via eavesdropping, terror suspects nabbed," *Christian Science Monitor*, June 2, 2004, https://www.csmonitor.com/2004/0602/p02s01-usmi.html; and National Security Agency, *NSA Scientific Advisory Board Panel on Digital Network Intelligence (DNI) (Née "C2C") Report to Director* (Washington, DC, 28 June 1999). The report was declassified on 17 May 2004.

30. Robert K. Ackerman, "A New -INT Looms for Social Media," *Signal*, October 1, 2013.

31. "Top Communication Channels Most Used by Customers in 2020," CommBox, accessed November 8, 2021, https://www.commbox.io/top-communication-channels-most-used-by-customers-in-2020/.

32. "The promise of open-source intelligence," *Economist*, 7 August 2021.

33. DOTMLPF–P: doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

34. Office of the Chairman of the Joint Chiefs of Staff, JP 2-03, *Geospatial Intelligence in Joint Operations* (Washington, DC: The Joint Staff, 5 July 2017).

CW4 Jay Gack recently retired from the Army after 23 years of service. From 2016 to 2020, he managed the Army's main open-source intelligence (OSINT) pilot at the 513th Military Intelligence Brigade–Theater. He has also contributed to various studies on technology and intelligence, including a 2019 study by RAND Corporation on the military application of OSINT. He holds a master's degree in strategic intelligence from the National Intelligence University and is currently a senior open-source advisor for Science Applications International Corporation (SAIC).