

# MI PROFESSIONAL BULLETIN

April 2022  
PB 34-22-1

**PUBLICLY  
AVAILABLE  
INFORMATION  
FOR INTELLIGENCE  
PURPOSES**  
SPECIAL EDITION



### **Commanding General**

MG Anthony R. Hale

### **Command Sergeant Major, MI Corps**

CSM Tammy M. Everette

### **Chief Warrant Officer, MI Corps**

CW5 Aaron H. Anderson

### **Chief of Staff**

COL Jarrod P. Moreland

### **Commandant, Intelligence School**

COL Crayton E. Simmons

### **Director of Training and Doctrine**

Beth A. Leeder

### **Managing Editor**

Tracey A. Remus

### **Associate Editor**

Maria T. Eichmann

### **Design and Layout**

Jonathan S. Dinger

### **Cover Design**

Jonathan S. Dinger

### **Military Staff**

SFC Lee A. Schaper

SFC Andrew J. Gunn

### **Manuscripts**

Please send your manuscripts, including supporting documents, and any inquiries by email to—[usarmy.huachuca.icoe.mbx.mipb@army.mil](mailto:usarmy.huachuca.icoe.mbx.mipb@army.mil); visit our webpage for full article submission guidelines at <https://mipb.army.mil>.

### **Mailing Address**

MIPB (ATZS-DST-B), DOTD, USAICoE, 550 Cibique St., Fort Huachuca, AZ 85613-7017.

### **Reprints**

Material in this bulletin is not copyrighted (except where indicated). Content may be re-printed if the MI Professional Bulletin and the authors are credited.

*The views expressed in the articles are those of the authors and do not necessarily reflect the official policy or position of the Departments of the Army or Defense, or the U.S. Government. Article content is not authenticated Army information and does not supercede information in any other Army publications.*

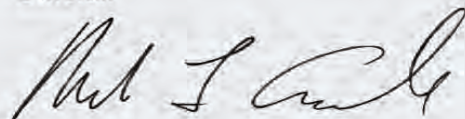
The U.S. Army Intelligence Center of Excellence publishes the Military Intelligence Professional Bulletin (MIPB) under the provisions of AR 25-30. MIPB presents information designed to keep intelligence professionals informed of current and emerging developments within military intelligence. MIPB provides an open forum for the exchange and discussion of ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, and other topics for purposes of professional development.

By Order of the Secretary of the Army:

**JAMES C. MCCONVILLE**

*General, United States Army  
Chief of Staff*

Official:



**MARK F. AVERILL**

*Administrative Assistant  
to the Secretary of the Army*

**2220013**

# MI PROFESSIONAL BULLETIN

April 2022  
PB 34-22-1  
Volume 48 Number 1

## PUBLICLY AVAILABLE INFORMATION FOR INTELLIGENCE PURPOSES

03

**Always Out Front**

by MG Anthony R. Hale

05

**The Risk of Not Knowing:  
Enabling Intelligence  
Professionals to Leverage Publicly  
Available Information**

by LTG Laura Potter and COL Christina Bembenek

09

**The Reawakening of Open-Source  
Intelligence**

by Ms. Corrine Geiger

13

**Open-Source Intelligence in the  
Canadian Intelligence Community**

by LCol David Holtz, Canadian Army, and  
Ms. Angela Maxwell, Canadian Forces  
Intelligence Command

17

**The Open-Source Intelligence  
Conundrum: Creating the  
Discipline or Integrating the  
Data?**

by CW4 Jarrod R. Gack (Retired)

23

**Open-Source Intelligence:  
Developing Analytical Capability  
for the Australian Army**

by WO1 Greg Hopper, Australian Army

27

**Mapping the Information  
Environment with Open-Source  
Intelligence and Allies**

by Mr. Matthew D. Skilling

30

**Open-Source Intelligence in the  
82<sup>nd</sup> Airborne Division G-2**

by SGT Christian Torres

35

**Publicly Available Information's  
Importance to the Intelligence  
Disciplines**

by CW2 Christopher D. Hurtig

**Bonus -**

**39 Modular J2X Staff Officer Course (Distance Learning)**  
by Mr. David Summers

**40 Army Intelligence Talent Management**  
by Mr. Sergio Sanchez



# MODERNIZING MIPB

## Up and Running!

MIPB continues to make great strides as we leverage 21<sup>st</sup> century technology to facilitate professional development for the Military Intelligence (MI) Corps. We now have—

- A customized website on LandWarNet at <https://mipb.army.mil>.
- A social media advertising campaign.
- A program to analyze usage metrics to support future changes.

### This First Special Edition Is Also Available Online!

A must-read edition: Publicly Available Information for Intelligence Purposes is posted and individual articles can be downloaded from the new MIPB website at <https://mipb.army.mil>.

### Social Media

We are partnering with other Army and Department of Defense organizations on an article-by-article basis to amplify our social media messaging and inform a broader audience.

### “Voice of the Frontier” Podcasts

The MIPB website is hosting podcasts relevant to the MI Corps.

- **Questions from the Field**—The first MI podcast from Fort Huachuca featuring a conversation between the leadership from U.S. Army Intelligence Center of Excellence (USAICoE), Army G-2, and U.S. Army Intelligence and Security Command (INSCOM).
- **Breaking Doctrine: Intelligence Driving Operations**—A U.S. Army Combined Arms Center podcast featuring a discussion between leadership from USAICoE and the Combined Arms Doctrine Directorate.
- **Questions on the Minds of the NCO Corps**—Hosted by the Commandant of the MI NCO Academy in conversation with the Army G-2 Sergeant Major, the INSCOM Command Sergeant Major, and the Office of the Chief of MI.
- **Coffee with the Command**—A fireside chat with the USAICoE leadership hosted by the Commander's Action Group Chief in conversation with the Commander and Command Sergeant Major USAICoE.

### We want your feedback!

If you have comments or suggestions on how we can improve MIPB, please let us know!

### Contact MIPB

[usarmy.huachuca.lcoe.mbx.mipb@army.mil](mailto:usarmy.huachuca.lcoe.mbx.mipb@army.mil)





# ALWAYS OUT FRONT

by Major General Anthony R. Hale  
Commanding General  
U.S. Army Intelligence Center of Excellence



As the Army modernizes, with military intelligence (MI) often in the forefront, we must carefully focus our efforts in several areas. The latest drafts of key Army operational doctrine have an elevated emphasis on understanding the operational environment. This understanding must occur not only across all domains but also across all dimensions. The new FM 3-0, *Operations*, which likely will be published in October, will discuss the three dimensions affecting operations: physical, human, and information. Answering intelligence requirements across all domains and dimensions is not new but the scope and volume of operational requirements associated with these doctrinal changes are increasing at a time when MI cannot grow the force.

Meeting the requirements associated with the Army's new conceptualization of information advantage alone is significant. I say alone because of the growth in demands on our branch based on other operational capabilities, like extended long-range targeting. Therefore, MI must optimize the use of all personnel and capabilities across all intelligence disciplines, complementary intelligence capabilities, and all-source intelligence. Three areas of great potential for optimizing intelligence support across the Army are better exploiting publicly available information (PAI) for intelligence purposes, open-source intelligence (OSINT), and commercially available information (CAI). Optimizing intelligence, in this case, is as much mindset and creativity as it is improving systems and building future capabilities. That is why this special edition of *Military Intelligence Professional Belletín* is so important.



## Intelligence Support to Information Advantage

While only draft Army doctrine, the Army is already moving out on implementing Army information advantage capabilities through a series of tasks driven by an OPT led by DA G-3/5/7. Information advantage replaces older Army doctrine on information operations and other doctrinal concepts to better grapple with the information dimension during operations. Five lines of effort are currently associated with information advantage:

- ◆ Enable decision making.
- ◆ Protect friendly information.
- ◆ Inform and educate domestic audiences.
- ◆ Inform and influence foreign audiences.
- ◆ Conduct information warfare.

As part of the DA G-3/5/7 OPT phase II operations, the USAICoE and DA G-2 co-hosted an Intelligence Doctrine Forum at Fort Huachuca, 24–26 May 2022. The forum included partners from academia, CENTCOM, SOCOM, INSCOM, ACO, NGIC, Australian Army, TRADOC, USAREUR-AF, USARPAC, ARCYBER, Cyber/Fires/Mission Command/Special Operations COEs, an MDTF (JBLM), I Corps, III Corps, XVIII ABN Corps, USMA Cyber Institute, and DAMO-SO. The forum was highly successful in jump-starting the development of an MI publication on intelligence support to IA at the theater army and corps. The MI publication will serve as a doctrinal bridge until Army IA doctrine and IA implementation discussions are mature enough for inclusion across other MI publications.

**Way ahead:** Doctrine Division, USAICoE, is engaging with forum participants and other units and organizations to develop the writer's draft of the MI publication. Soon we will complete revision of a detailed outline, timeline, and project plan. We project worldwide staffing of the publication this fall and completion of the publication in January 2023.

**ABN** airborne  
**ACO** Army Cryptologic Operations  
**ARCYBER** U.S. Army Cyber Command  
**CENTCOM** U. S. Central Command  
**COE** Center of Excellence  
**DA** Department of the Army  
**DAMO-SO** Department of the Army Management Office-Strategic Operations  
**G-2** assistant chief of staff, intelligence  
**G-3/5/7** assistant chief of staff, operations, plans, and training  
**IA** information advantage  
**INSCOM** U.S. Army Intelligence and Security Command  
**JBLM** Joint Base Lewis-McChord  
**MDTF** Multi-Domain Task Force  
**MI** military intelligence  
**NGIC** National Ground Intelligence Center  
**OPT** operational planning team  
**SOCOM** U.S. Special Operations Command  
**TRADOC** U. S. Army Training and Doctrine Command  
**USAICoE** U.S. Army Intelligence Center of Excellence  
**USAREUR-AF** U.S. Army Europe and Africa  
**USARPAC** U.S. Army Pacific  
**USMA** U.S. Military Academy

This edition of MIPB, our first special edition, does a great job providing a broad and comprehensive look at PAI for intelligence purposes now and into the future. The first article, “The Risk of Not Knowing: Enabling Intelligence Professionals to Leverage Publicly Available Information” by LTG Laura Potter and COL Christina Bembeneck, sets the stage and provides an overarching context to the other seven excellent articles. These articles address many aspects of PAI, including—

- ◆ Policy, doctrine, and training.
- ◆ Efforts with our multinational partners.
- ◆ Use of PAI across other intelligence disciplines.
- ◆ Collection management challenges.
- ◆ Use of commercial software.
- ◆ Use of OSINT in U.S. Army Europe and Africa.
- ◆ The OSINT cell at division level.
- ◆ PAI strategic implications.

These articles discuss the advantages of optimizing PAI and OSINT within our existing fundamental intelligence processes. I would highlight two of the advantages paraphrasing from the various articles:

- ◆ With the continued growth of social media and other PAI sources, PAI is often timely. PAI can capture “now” events that inform “now” operational and targeting decisions as well as focusing other information collection capabilities. We have seen this recently demonstrated in the myriad daily news reports on Russian operations in Ukraine. Intelligence professionals should understand how to routinely use PAI to enrich their intelligence discipline, provide overall context, provide threat warnings, and answer intelligence requirements.
- ◆ The public availability of the information speeds sharing between nations, helps build and consolidate foundational intelligence, and builds the trust between partners necessary to expand sharing across all intelligence disciplines. For these reasons, performing PAI for intelligence purposes is critical in today’s environment.

The U.S. Army Intelligence Center of Excellence (USAICoE) has multiple efforts, some complete and some ongoing, to improve the effectiveness of exploiting PAI and OSINT. We are aggressively undertaking these measures. Even though

both are discussed in the MIPB articles, I want to highlight two of those efforts:

- ◆ USAICoE is revising OSINT doctrine. The draft ATP 2-22.9 (Volume 1), *Open-Source Intelligence*, describes the difference between accessing PAI and OSINT activities. It emphasizes the value of PAI and describes systematic approaches to plan, prepare, collect, and produce intelligence from PAI. The initial draft staffing is complete, and we anticipate staffing the final draft at the end of July 2022.
- ◆ In February 2022, USAICoE began integrating publicly available information research (PAIR) into all 35-series courses. We are also working with the broader OSINT community to create the OSINT Basic Course, which will be ready for instruction in the first quarter of fiscal year 2023. This course will replace the current OSINT 301 and OSINT 302 courses and will build on the foundation established within the PAIR curriculum.

So, what now? I challenge all of you to help with the effort to optimize PAI, OSINT, and CAI and to periodically send USAICoE feedback on what you are doing in these areas. We will make many changes to our intelligence doctrine in FM 2-0, *Intelligence*, based on the changes to FM 3-0, *Operations*, but our fundamental processes will not really change. Therefore, you have the doctrine and training in place now to meet this challenge if you apply sound and legally sufficient creativity. Discussing the risks associated with PAI should not deter us from applying common sense guidance to our intelligence operations.

While the Army strategic contexts are competition, crisis, and conflict, make no mistake, the intelligence warfighting function is always engaged in collecting against and providing intelligence about our peer threats and other foreign actors. Meeting my challenge includes operating across our MI formations in the manner discussed in LTG Potter and COL Bembeneck’s article. As LTG Potter and COL Bembeneck state, “Leveraging PAI as a source of information allows insight into our adversaries’ actions almost at the speed of thought, which is critical to obtaining systemic advantage. Soldiers in S-2 sections at every echelon need to analyze the threat in the information dimension of the operational environment.” Go and meet the challenge and optimize your use of PAI, OSINT, and CAI to ensure we win. — Desert 6. 🌟

**Always Out Front!**



# THE RISK OF NOT KNOWING:


## Enabling Intelligence Professionals to Leverage Publicly Available Information

*War is evolving in form toward informationized warfare, and intelligent warfare is on the horizon.*

*—2019 Chinese Defense White Paper*

### **We start with a fictional story...**

The first indicator was the surge in false tweets about unsafe and discriminatory work conditions for Chinese workers at the Port of Seattle. Then, a human intelligence (HUMINT) analyst building a profile on a prominent Chinese officer in the People's Liberation Army sustainment force noticed a new photo album on the Chinese officer's WeChat profile that featured barren tundra with few roads and structures. She passed the images to a geospatial intelligence (GEOINT) analyst who examined the shadows and angles of the sun, which indicated a point in the Arctic. A signals intelligence (SIGINT) analyst copied phone numbers listed in the officer's WeChat profile and noticed the list included several numbers with the area code for Banks Island, Canada. Tipped by this uncommon activity in social media, all-source analysts dug further into both publicly available information (PAI) and classified databases, leading to a startling discovery—the Chinese were preparing to seize land on Banks Island in order to control a portion of the Northwest Passage. By fomenting unrest at the Port of Seattle, the Chinese were ensuring that any American effort to reinforce troops in Alaska, as well as any support to the United States from its Canadian ally, would be bogged down. The U.S. Army team collaborated with their Canadian partners by quickly sharing the unclassified PAI while they worked through classification guidance on the more sensitive details, and a combined operation began to take shape.



by  
Lieutenant  
General Laura Potter  
and Colonel  
Christina Bembenek

## Introduction

Vignettes like this are possible when all intelligence professionals understand how to routinely use PAI to enrich their particular intelligence discipline and to identify indications and warnings of hostile activities. Leveraging PAI as a source of information allows insight into our adversaries' actions almost at the speed of thought, which is critical to obtaining systemic advantage. Soldiers in S-2 sections at every echelon need to analyze the threat in the information dimension of the operational environment.

As the intelligence community works toward more clearly defined regulations and governance for open-source intelligence (OSINT), the U.S. Army Intelligence Center of Excellence (USAICoE), supported by the Army OSINT Office, is training our Soldiers on safe and effective ways to use PAI to fulfill commanders' intelligence requirements, which include understanding and articulating the risks.

Distinguishing between PAI and OSINT is a key concern among intelligence professionals, and admittedly, the multiple regulations and directives have left some gray areas, as outlined in Ms. Corrine Geiger's article "The Reawakening of Open-Source Intelligence."<sup>1</sup> Department of Defense (DoD) Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*, allows for the use of PAI to "plan, inform, enable, execute, and support the full spectrum of DoD missions."<sup>2</sup> As with any intelligence activity, analysts must adhere to proper intelligence oversight procedures, as specified in DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, which ensures any collection occurs "in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons."<sup>3</sup> Both the intelligence community and the DoD are working on updating policies to more clearly outline authorities for working in the information dimension of today's dynamic and technologically evolving operational environment.

Understanding the evolving policy and regulations is important, but at the end of the day, intelligence is for commanders, and intelligence professionals must properly advise commanders on the risks inherent to using PAI for intelligence purposes. To clarify the guidance for maneuver commanders, analysts can reference ATP 2-22.9, *Open-Source Intelligence*, which outlines specific risk levels for OSINT collection. These risk levels clarify what levels of operational security risk the OSINT activity could pose to military operations. By coordinating

“ Understanding the evolving policy and regulations is important, but at the end of the day, intelligence is for commanders ”

closely with the operations teams, S-2s and G-2s can ensure their teams are prudently leveraging PAI without putting planned or ongoing operations at risk—the same assessment they would make when planning unmanned aircraft system or SIGINT collection.

### Publicly Available Information Training

To assist in understanding how to leverage PAI effectively, USAICoE has developed six training modules for all intelligence series analysts on open-source research methodologies, basic workings of the internet (to understand the "tracks" analysts leave when they conduct research online), and ways to create OSINT requests for information. This training will enable analysts to understand how to think through operational security considerations and take measures to mask or safeguard their searches. They will also learn how to distinguish between general research that increases commanders' overall understanding of the operational environment and intelligence preparation for an upcoming mission. Three of the training modules are available on LandWarNet as of March 2022 via interactive multimedia instruction to all intelligence professionals, ensuring we can train the entire military intelligence force now.<sup>4</sup> USAICoE also began integrating the six modules into all courses at Fort Huachuca, starting with the 35F, Intelligence Analyst, and 35M, Human Intelligence Collector, Advanced Individual Training courses in February 2022.

The USAICoE instruction will emphasize that PAI is a source of information that, like any other, must be corroborated by other sources and methods. All-source analysts can validate the authenticity and credibility of a particular source of PAI through coordination with other intelligence disciplines. For example, they can leverage GEOINT or SIGINT to verify if a particular source on social media is physically located in the area the reporting is from or whether other people or journalists in the area reported on the events. Organizations like Bellingcat have developed several techniques to verify the authenticity of PAI and build detailed analytical products. Bellingcat's most famous success was the report they provided to the United Nations that definitively linked Russian forces to the shooting down of Malaysian Airlines Flight 17 over Ukraine. "In the frenzy to determine who—and what—shot down Malaysian Airlines Flight 17, a group of citizen journalists armed with simple intuition and an internet connection has been collecting information more nimbly than American spies."<sup>5</sup>



National capabilities are a finite resource. Intelligence professionals must train on how to use every source available and to use traditional analytical tradecraft to assess validity and turn information into actual intelligence. GEOINT analysts have multiple tools to analyze images and videos on the web and in social media to verify location, time of day, and image authenticity. This includes analyzing an image's digital fingerprint, using web map services to map track, or an open-source investigative tool, like the kind developed by Bellingcat, to associate a particular geographic location using Python scripts and Application Programming Interfaces.<sup>6</sup> HUMINT is another area that can benefit greatly from the vast quantities of data available in digital media. During World War II, Allied analysts with the Office of Strategic Services estimated Nazi casualties by reading the obituary sections of German newspapers available in Switzerland.<sup>7</sup> Today, HUMINT analysts can conduct similar research through digital means and then cross-reference with classified information.

In addition, PAI opens an avenue to share unclassified information with our foreign partners and collaborate on adversary assessments. Many intelligence-sharing agreements, particularly in the U.S. Indo-Pacific Command, allow only limited sharing of classified information between intelligence entities. PAI offers a means to share information quickly without compromising sources or methods. Foreign partners will also be more adept at analyzing social media and cultural nuances within their own countries as compared to most U.S. military analysts. An excellent example of this is the work done by European analysts who provide open-source information on pro-Kremlin disinformation trends, trending disinformation topics, and analytical reports on the top sources of Russian disinformation within the EU vs DISINFORMATION database.<sup>8</sup> Establishing routine information exchanges using PAI will help ensure U.S. intelligence professionals receive the high-quality products our foreign partners create and enable a more comprehensive and accurate understanding of the operational environment.

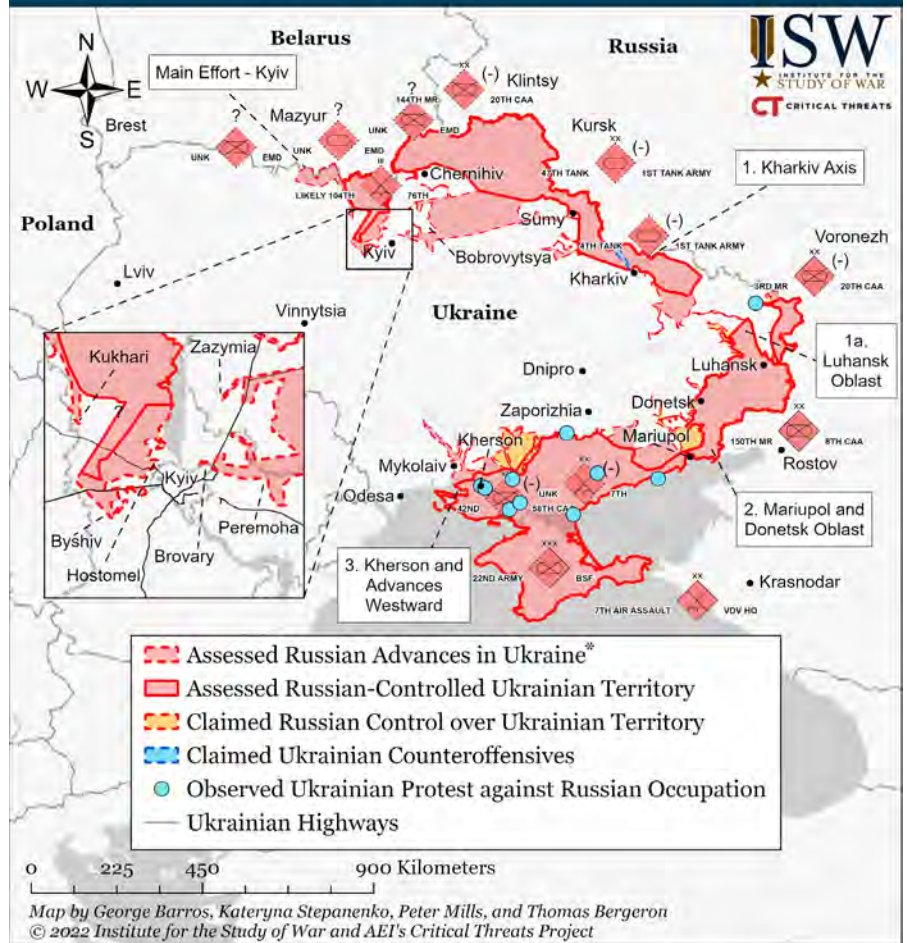
### Assessing and Managing Risk

Accessing PAI on the internet opens up an infinite amount of information and data for analysis but also exposes individuals and units to varying levels of risk. This includes the risk that once our adversaries identify the websites where analysts are conducting research, they will begin to add false information to those sites or create a redirect to false sites. This is a valid concern because deception figures largely in both Russian and

Chinese doctrine, and our adversaries are actively working to deceive many of our sensors. Like any information, analysts must use other sources and methods to determine the veracity of information.

Another potential risk is that website owners and foreign governments will identify that a U.S. military person or specific unit has accessed their information. Proper use of virtual private networks or managed attribution can lower this risk. However, even if the search is traced, foreign entities still have to analyze the information, determine their own risk calculation, and then take action. For example, if a Russian army officer is communicating on VKontakte and discovers that a United States person is accessing his information, the Russian army officer could stop using that platform—which inhibits his ability to communicate with family, friends, and fellow soldiers—or he could accept the risk.

## Assessed Control of Terrain in Ukraine and Main Russian Maneuver Axes as of March 17, 2022, 3:00 PM ET



\* Assessed Russian advances are areas where ISW assesses Russian forces have operated in or launched attacks against but do not control.

A map of the situation in Ukraine created from publicly available information by the Institute for the Study of War and AEI's Critical Threats Project. (Reprinted by permission of the Institute for the Study of War and AEI's Critical Threats Project)

Our military leaders increasingly use social media to communicate to the lowest levels, and our adversaries are collecting this information. The risk of not informing our Soldiers generally outweighs the risk of an adversary agency building a source profile. Moreover, we accept as fact that Russia and China are collecting every bit of PAI they can find about United States forces; undoubtedly, they also expect United States intelligence agencies are doing the same. By training intelligence professionals to clearly identify the risks inherent to online research and the ways to mitigate them, they can better assist commanders in deciding whether accessing PAI—or posting unit and individual information—is worth the risk of adversary collection.

## Conclusion

In the current operational environment, U.S. forces will rarely be unobserved both at home and overseas. In addition to ubiquitous satellite and unmanned sensors, social media provides near real-time reporting on human activity. Russian and Chinese doctrine is explicit about the importance of gathering information, particularly in cyberspace, to track adversaries. If we are to actively campaign in competition, we must train our intelligence professionals to leverage every source of information available to understand our enemy's activities and intentions. Army intelligence has the benefit of truly exquisite, classified collection capabilities, but PAI is a valuable starting point for all intelligence disciplines, as well as a means to answer commander's information requirements. There will always be a risk to using open-source information, but training all intelligence professionals to safely and effectively leverage PAI provides us an advantage in this exceptionally competitive space that outweighs the risk of not knowing. ✨

## Acknowledgment

The map on page 5 titled “Assessed Control of Terrain in Ukraine and Main Russian Maneuver Axes as of March 17, 2022, 3:00 PM ET” is reprinted by permission of the copyright holder, the Institute for the Study of War and AEI's Critical Threats Project, <https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-march-17>.

## Epigraph

The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing, July 2019), 7, [http://www.andrewerickson.com/wp-content/uploads/2019/07/China-Defense-White-Paper\\_2019\\_English.doc](http://www.andrewerickson.com/wp-content/uploads/2019/07/China-Defense-White-Paper_2019_English.doc).

## Endnotes

1. Corrine Geiger, “The Reawakening of Open-Source Intelligence,” *Military Intelligence Professional Bulletin* 48, no. 1, n.d. This article provides a full discussion on the differences between publicly available information and open-source intelligence.
2. Department of Defense Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)* (Washington, DC, June 11, 2019, incorporating Change 1, August 20, 2020), 3.
3. Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC, August 8, 2016), 1.
4. “Publicly Available Information,” Learning Innovation Branch, LandWarNet eUniversity, last updated 20 February 2022, <https://libicoe.army.mil/products/pai> (common access card login required).
5. Lorenzo Franceschi-Bicchieri, “The Group of Bloggers Unearthing MH17 Intel Quicker Than U.S. Spies,” *Mashable*, July 23, 2014, <https://mashable.com/archive/citizen-journalists-mh17-spies>.
6. “Help Bellingcat Build Tools For Open Source Investigators!” *Bellingcat*, July 6, 2021, <https://www.bellingcat.com/resources/2021/07/06/help-bellingcat-build-tools-for-open-source-investigators/>.
7. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2018).
8. EU vs DISINFORMATION, accessed 16 March 2022, <https://euvsdisinfo.eu>.

*LTG Laura Potter is the Deputy Chief of Staff for Intelligence (G-2) of the U.S. Army. Previously, she was the commanding general of the U.S. Army Intelligence Center of Excellence and Fort Huachuca. LTG Potter has served in multiple intelligence positions at the tactical, operational, and strategic levels. She is a Distinguished Military Graduate of Dickinson College, Carlisle, PA, where she received a bachelor's degree in Russian and Spanish. She holds a master's degree from Georgetown University's School of Foreign Service, Center for Eurasian, Russian, and East European Studies, and a master's degree in national security and strategic studies from the Naval War College.*

*COL Christina Bembenek is the Commandant for the U.S. Army Intelligence School at Fort Huachuca, AZ. She previously served as the 82<sup>nd</sup> Airborne Division G-2 and in multiple intelligence positions at the tactical, operational, and strategic levels.*





---

# THE REAWAKENING OF OPEN-SOURCE INTELLIGENCE

*By Ms. Corrine Geiger*

---



*Sometimes the critical key to unlock the whole conundrum is right there under your nose....You have to know what to look for and how to recognize it when you see it.*

—LTG (Retired) Samuel V. Wilson  
Former Director, Defense Intelligence Agency

## Introduction

Throughout history, people have made predictions that have proven to be wrong. For example, in the 1990s, they said that the internet was a passing fad, and 100 years earlier, that everything that could be invented had already been invented.<sup>1</sup> And more recently, many said that open-source intelligence (OSINT) was just gray literature.<sup>2</sup> However, these three areas are now an ever-present part of modern life, driven by mobile communications, portable electronic devices, social media, virtual workspaces, and various other technologies in the field of data. These technologies have modernized technical capabilities able to respond to oceans of data, transforming a new OSINT for modern warfare.

As of March 2020, approximately 2.5 exabytes of data were generated on the internet daily.<sup>3</sup> This adds up to volumes of valuable data and publicly available information (PAI) in the cyberspace domain. It comes in near real time, and an experienced professional with the right skillset can navigate through the overcrowded terrain within the cyberspace domain to track down tailored information to a specific problem set, fill intelligence gaps, and tip and cue other intelligence disciplines and collection efforts.

Perhaps most importantly, PAI gathered from the cyberspace domain can provide indications and warnings to more sensitive intelligence collection methods and warfighters. However, the swift resurgence of OSINT and the mass influx of information caused a great deal of confusion among consumers of the discipline. As a result, OSINT is often misunderstood and underutilized. This article defines and differentiates PAI and OSINT. It also discusses the use of PAI for all intelligence disciplines disparate to OSINT and OSINT's reemergence as a paramount intelligence discipline.

## What Is the Difference between OSINT and PAI?

A common question adding to the perplexity of OSINT is, "What's the difference between OSINT and PAI?" There remains much bewilderment on this topic across the Department of Defense and intelligence community. OSINT and PAI are not synonymous. While OSINT cannot exist without PAI, PAI very much exists without OSINT.

PAI is broadly defined 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

### Terms Analogous to OSINT

There is a lack of understanding of various terms analogous to OSINT, such as open-source information, open-source research, and open-source collection. Open-source information and PAI are interchangeable, while open-source research and open-source collection are quite divergent. Open-source research consists of any use of PAI for a non-intelligence purpose, whereas open-source collection (or collection of PAI) falls within the confines of collection; "Information is collected when it is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence or other purposes."<sup>4</sup>

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. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public."<sup>5</sup> PAI has wide use outside of intelligence activities, and much of the operations community relies heavily upon it. Additionally, all intelligence disciplines use information to create either foreign intelligence or counterintelligence, the least intrusively collected of which is PAI.

Only when information is collected against an intelligence requirement does the information formally become intelligence. Yet, finished intelligence products are not manufactured until the information goes through a process of collection, processing, exploitation, and dissemination. This process does not exclude OSINT. By definition, OSINT is "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."<sup>6</sup> Furthermore, in accordance with the Army's policy on OSINT, the conduct of OSINT activities is authorized for "Army intelligence personnel (military, civilians, and contractors) assigned, attached, detailed to, or supporting Army intelligence organizations, units, or elements with an [authorized] OSINT mission."<sup>7</sup>

## The Role of PAI in Intelligence

PAI presents a fundamental component of all intelligence collection and is applicable to all intelligence disciplines. "Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."<sup>8</sup> Since PAI is generally the least intrusive means of collection, the majority of collection activities will often begin with PAI collection (see Figure 1, on the next page, for examples of PAI data sources). However, Army intelligence personnel using PAI

while operating under non-OSINT intelligence collection disciplines' authorities, rules, and regulations are not conducting OSINT activities and must refer to their respective policies. For example, a geospatial intelligence (GEOINT) professional who collects and analyzes an image from a commercial mapping site available to the public is using PAI as part of the GEOINT mission. Likewise, a counterintelligence (CI) special agent who identifies a threat from a social media platform as part of a national security investigation is conducting a CI activity. OSINT activities are unlike other intelligence disciplines' use of PAI in that PAI can be used at the tactical, operational, and strategic levels of war while producing a product that is inherently shareable with our allies and partners to drive combined joint multidomain operations. However, all OSINT collection activities must remain passive.

Other disciplines, such as human intelligence (HUMINT) and signals intelligence (SIGINT), are inherently more intrusive, can conduct active collection activities, and are intrinsically classified. OSINT does not involve messaging or personal interaction; in fact, unlike other intelligence disciplines, "OSINT collectors neither own nor control the means of collection; they must rely on others to collect, edit, and publish information, which is then subsequently acquired."<sup>9</sup> Unlike HUMINT, SIGINT, and GEOINT, OSINT relies exclusively on others to publish information to the public on their own accord. It is not requested, elicited, or tasked.

## OSINT as a Discipline

A lack of control over the inordinate amount of information is precisely what makes OSINT distinct from other intelligence disciplines. OSINT collection activities extend well beyond a simple internet search. OSINT professionals must know how to triage and validate massive amounts of information. They must weed through misinformation and disinformation, propaganda, foreign malign influence, external biases, and circular reporting at levels unimaginable, without any personal interaction, while trying to determine the value of the information. OSINT professionals must also understand all the nuances of the deep and dark web, know how to navigate through them passively without standing out, and garner the most applicable information to their problem set or mission.

Approximately 10 percent of all data on the internet lies on the surface web; the rest is in the deep and dark web.<sup>10</sup> Yet most users are unfamiliar with these portions of the internet and lack the ability to navigate them and discover useful results. Therefore, personnel conducting OSINT activities require training on the right tactics, techniques, and procedures (TTPs). Training must be agile and constantly revised to keep up with all the social and technological changes that occur within the cyberspace domain.

## OSINT Transformation

OSINT provides commanders access to large amounts of data worldwide. It is impossible to view, sort through, and verify or validate all information at that scale. As a result, the OSINT community is constantly seeking and reviewing new tools and technologies to aid with collection and prioritization. The Army focuses on building a fully integrated and unified OSINT enterprise to expand data sharing, expedite decision making at echelon, and enhance the use of cloud capabilities to include evolving artificial intelligence, semantic analysis, and machine learning services and tools. Future OSINT professionals must use technology, such as artificial intelligence and machine learning, to create and use algorithms that can shift mountains of data to answer specific intelligence requirements. Future OSINT professionals must also maintain vast familiarity of both the cyberspace domain and the information environment, have an understanding of data governance and the inner workings of the unabridged internet, and be resourced with capabilities designed to quickly sift through exabytes' worth of data.

The Army is constantly reviewing and evolving training, tools, and capabilities to meet the demands of emerging technologies so that OSINT will be "a fully operationalized intelligence discipline in support of [multidomain operations] MDO."<sup>11</sup> For example, as distributed ledger technologies, cryptocurrency, and metadata steganography become more prevalent, OSINT professionals will require diverse backgrounds and niche skillsets that feed OSINT's role as a single-source intelligence discipline. This is something the Army cannot accomplish on its own. The Army continues to explore partnerships with

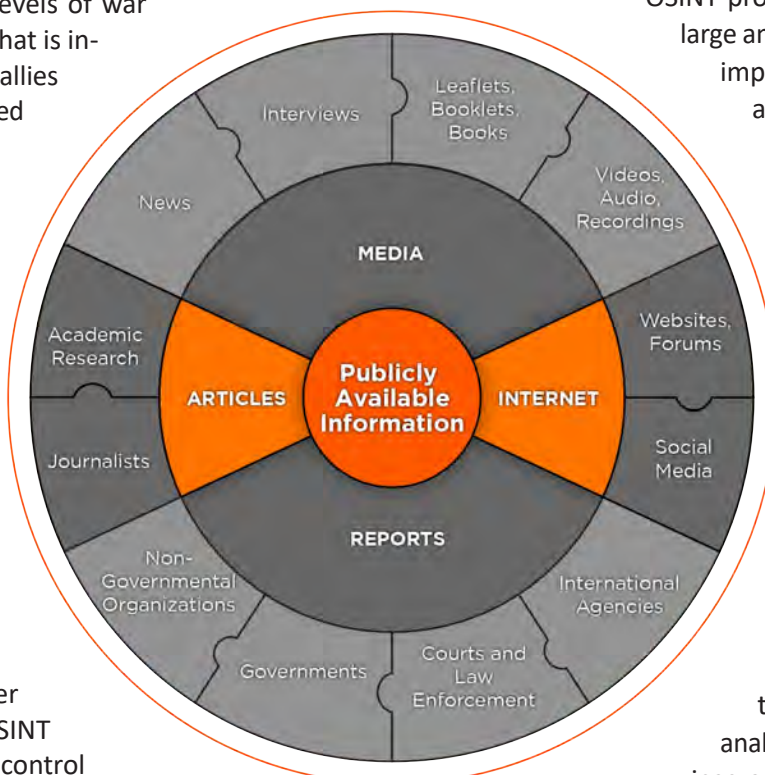



Figure 1. Publicly Available Information Data Sources

academia and industry. It also continues to collaborate with joint and foreign partners and allies to mature the OSINT enterprise and expand OSINT's capacity.

## Conclusion

Despite the fact that OSINT is derived of PAI, it is appreciably more than PAI. The magnitude of OSINT emanates well beyond that of simple information. OSINT requires a specialized skillset for safe and adequate collection, and OSINT collection activities entail tailored TTPs, processes, technologies, governance, tools, and dissemination. The internet changed the paradigm of how the world shares information. The internet is ubiquitous and will continue to drive the evolution of capabilities and ingest information at levels we cannot begin to fathom. Along with the internet, OSINT has evolved past the days of newspaper clippings, radio broadcasts, and gray literature.

The evolution of the cyberspace domain and artificial intelligence capabilities will place OSINT at the forefront of a commander's capabilities for situational awareness. It will strengthen relationships and intelligence sharing with foreign partners and allies while providing near-real-time intelligence updates and atmospheric to warfighters. OSINT is nuanced and dynamic, and is inherently tied to the cyberspace domain, which requires both a breadth and depth of information automation and data science knowledge from OSINT professionals. OSINT will never replace other intelligence disciplines, but it will enhance, broaden, and tip and cue their efforts. OSINT is often the corner and edge pieces of the puzzle that help indicate which pieces are needed to fill the center and complete the picture—it is the “source of first resort.”<sup>12</sup> After all, “ninety percent of Intelligence comes from open sources. The other 10 percent, the clandestine work, is just the more dramatic.”<sup>13</sup> 

## Epigraph

Steven Pressfield, “General Sam V. Wilson,” *The Creative Process* (blog), July 2010, <https://stevenpressfield.com/2010/07/general-sam-v-wilson/>. This quote is from an in-depth interview Pressfield conducted with LTG Wilson.

## Endnotes

1. Clifford Stoll, “The Internet? Bah! Hype Alert. Why cyberspace isn't, and will never be, nirvana,” *Newsweek*, February 26, 1995, <https://www.newsweek.com/clifford-stoll-said-internet-would-die-1995-566797>; and Dennis Crouch, “Tracing the Quote: Everything that can be invented has been invented,” *Patently-O*, January 6, 2011, <https://patentlyo.com/patent/2011/01/tracing-the-quote-everything-that-can-be-invented-has-been-invented.html>.

2. Gray literature is information produced by government agencies, academic institutions, and the for-profit sector that is not typically made available by commercial publishers. Examples of gray literature include reports, proceedings, dissertations and theses, white papers, and newsletters. “What is gray literature? How do I search for it?” Johns Hopkins University & Medicine, accessed

October 19, 2021, <https://welch.jhmi.edu/get-help/what-gray-literature-how-do-i-search-it>.

3. “What is an Exabyte?” Wasabi, accessed October 18, 2021, <https://wasabi.com/help/glossary-of-terms/exabyte-definition/>. An exabyte is a multiple of a byte, which is the unit of file size for storing digital information. Since *exa* indicates multiplication by the sixth power of 1,000, an exabyte is equal to one quintillion (1,000,000,000,000,000,000) bytes or 1,000 petabytes (or 1,000,000 terabytes).

4. Department of Defense (DoD), DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC, August 8, 2016), 45.

5. *Ibid.*, 53.

6. Office of the Director of National Intelligence, *U.S. National Intelligence: An Overview 2011* (Washington, DC, 2011), 54, [https://www.dni.gov/files/documents/IC\\_Consumers\\_Guide\\_2011.pdf](https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf).

7. Secretary of the Army, Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities* (Washington, DC, 22 November 2016), 1.

8. Executive Order 12333, *United States Intelligence Activities*, as amended (December 4, 1981).

9. Mark M. Lowenthal and Robert M. Clark, *The Five Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016).

10. Subhendu Kumar Pani, Sanjay Kumar Singh, Lalit Garg, Ram Bilas Pachori, and Xiaobo Zhang, eds., *Intelligent Data Analytics for Terror Threat Prediction* (Hoboken, NJ: John Wiley & Sons, 2021), 309.

11. Dennis A. Eger (Defense Intelligence Senior Level, Senior Army Open-Source Intelligence Advisor), during Army Open-Source Intelligence strategy working group.

12. Former ambassador John D. Negroponte, first Director of National Intelligence, quoted in Pani et al., *Intelligent Data Analytics*, 14.

13. Pressfield, “General Sam V. Wilson.”

## References

DoD. DoD Instruction 3115.12. *Open Source Intelligence (OSINT)*. Washington, DC, August 24, 2010, incorporating change 2, July 16, 2020.

DoD. DoD Directive 3115.18. *DoD Access to and Use of Publicly Available Information (PAI)*. Washington, DC, June 11, 2019, incorporating change 1, August 20, 2020.

Ms. Corrine Geiger is the open-source intelligence policy advisor for the Headquarters, Department of the Army, Deputy Chief of Staff, G-2. She has more than 19 years in the Department of Defense and more than 11 years in the intelligence community. She serves in the U.S. Army Reserve as an intelligence professional, previously served as a defense contractor for both the Army and the Under Secretary of Defense for Intelligence and Security, and recently joined the ranks of Civil Service as a Department of the Army Civilian. Ms. Geiger deployed multiple times to Iraq and Afghanistan in her military capacity, and she continues to support ongoing missions as an Army Reservist. She holds a bachelor's degree in social sciences from Ashford University and is currently pursuing a master's of applied intelligence at Georgetown University.



products that offer critical inputs to decision makers. CFINTCOM's regional OSINT daily updates are one way our

community is leveraging the open-source domain to enable tactical to strategic effects. OSINT analysts are responsible for converting and refining the collected information; they process, exploit, and disseminate (PED) the initial information for further analysis or report it directly as single-source intelligence. The use of the PED process in OSINT is a relevant technique and procedure ensuring commanders and staffs receive critical information that will enable decision making.

Within the Intelligence Command, OSINT analysts have access to articles from various media sources, academic publications, reports from organizations such as the United Nations and the Organization of Security and Co-operation in Europe, official reports from governments and military sources, and other local language reporting. In some cases, OSINT analysts leverage machine translation to enhance the quality of the OSINT daily product, but subscription services, such as BBC Monitoring, typically translate foreign language material.

Language can be a barrier to valuable sources; for this reason, the OSINT capability has engaged contracted support services to use when neither machine translation nor government translation services will suffice. Although production of the OSINT daily updates does not generally employ these advanced services, they are available for responding to follow-on questions cued by the daily products.

The selection of articles to include in the daily products is an analytical process. Daily, the analysts select from hundreds of available data sources, which requires analytical skill and experience to ensure the reporting of correct information and use of the most relevant sources. The end user depends on the OSINT analyst's knowledge of the information landscape to determine which OSINT sources will be pertinent to inform the assigned IRs. The analysts must first evaluate the sources against the IRs and then further refine the selection based on the sources' credibility.

## Introduction

Open-source intelligence (OSINT) is a powerful tool that can provide valuable information and insights to better inform the decision maker. The importance of OSINT has not escaped the Canadian intelligence community; however, today, even defining OSINT can be difficult as we struggle to differentiate some aspects of traditional signals intelligence (SIGINT) and human intelligence (HUMINT) activities within virtual space. The OSINT activity spectrum includes the passive collection of information from social media. Although it does not include actively engaging with persons of interest in online fora, OSINT in part informs the results of "social warfare" as a weapons system.

This article will focus on the Canadian Forces Intelligence Command's (CFINTCOM) OSINT daily summaries as one way the Canadian intelligence community leverages OSINT to enable both intelligence professionals and generalists in the military community. It will also discuss how we share these same OSINT products to enhance relationships with allies and partner nations.

## OSINT Requirements and Sources

The CFINTCOM OSINT Operational Support Team produces a series of regionally or thematically focused unclassified products collected from publicly available information based on direction in the form of priority information requirements (PIRs) and supporting information requirements (IRs). The products offer a short synopsis of the day's headlines as well as full-text reporting of articles organized by geography or theme.

These unclassified OSINT daily regional updates enable intelligence professionals and operators to maintain general regional situational awareness and, in some cases, to inform all-source classified intelligence product development. With some additional processing, the OSINT daily product can enable further all-source production in the form of high-quality stand-alone

## Dissemination of the OSINT Daily Product

The power of these OSINT daily products is that they are shared widely by email on any unclassified system. This distribution method ensures that users can access the product on a mobile device anywhere in the world at any time. In the intelligence function, we know that one of the challenges is enabling access to information when needed. As Cynthia Grabo wrote in *Anticipating Surprise*, “warning does not exist until it has been conveyed to the policymaker, and [they] must know that [they have] been warned.”<sup>1</sup> A high-value product with wide distribution and easy access can be disseminated, shared, and integrated into the intelligence cycle. By contrast, the exploitation of classified products is restricted by limited access to classified systems.

Dissemination of the OSINT daily product is primarily to intelligence organizations and professionals, but distribution lists include others, such as regional staff desk officers at strategic- and operational-level headquarters, liaison officers, and embassy staff. Of note, the intent is not to create a finished intelligence product for general officers and flag officers; however, the OSINT daily update can be a valuable tool for general officers’ and flag officers’ staff particularly when traveling.

warning  
does not exist until it has been  
conveyed to the policymaker,  
and [they] must know that [they  
have] been warned.

—Cynthia Grabo

The CFINTCOM’s OSINT daily product is a valuable tool for our worldwide liaison staff and for the intelligence and operations staff at our embassies. Generalist staffs use this tool to maintain situational awareness within the region where they are operating, particularly when they have limited access to classified materials. Intelligence and operations staffs can, on a limited basis, share these products with allied and partner nations to demonstrate a commitment to sharing information. This is particularly useful for dealing with countries that tend to be transactional in their information-sharing approach. The OSINT daily is successful primarily because the PED process makes it a high-quality, relevant product. The quality of these OSINT dailies is driven by the focus on IRs and feedback to the analysis as part of the intelligence cycle.

The OSINT daily product is also helpful as a catalyst for “breaking the ice” in awkward situations when intelligence professionals want to discuss an area of intelligence interest but the classified products are not yet available for dissemination outside of the national production chain.

Analyst-to-analyst discussions with allies and partners are easier if an open-source product is available as the centerpiece for discussion. The sharing of ideas can be framed on open-source information while waiting until the classified material is available to be shared in the form of a releasable product.

Another use for these focused OSINT daily updates is to reduce the burden on deployed analysts and J-2/G-2 staff and enable the country and regional analysts at the operational- and strategic-level headquarters. High-quality OSINT products are of value to the all-source analyst and the all-source analytical element within our intelligence centers and to analysts at operational and strategic levels. The effect of IR-driven general OSINT products that are being delivered on a regular basis is that all-source analysts are enabled with information that provides both broad knowledge about the environment in their area of intelligence interest and information that could be used to support sourcing.

The OSINT dailies are saved on a local SharePoint platform that is accessible to anyone with a Department of National Defence account. External partners and agencies can and do save copies of the OSINT daily update to create their own local database of OSINT products. An OSINT database can be a powerful tool for all-source analysts to draw on, creating an effective way to quickly discover and retrieve information for classified product development. This approach cues the all-source analyst to first review the relevant information available and then either develop a request for information, ask the OSINT analyst for a refinement in the IR, or directly collaborate with the OSINT analyst as part of an all-source process. In this way, the daily development and use of the OSINT products can be a crucial enabler for all-source cueing.

## Challenges of Online Intelligence Collection

Every intelligence analyst is familiar with the frustration of trying to obtain relevant information from internet search engines, which are limited by the bias of previous search history, region, and prioritization of popular search results over relevant ones. This frustration increases when attempting to exploit machine learning to deliver tailored search results on a periodic basis based on predefined parameters. It is quickly apparent that many results are not relevant, despite

Canadian Forces  
Intelligence Command

Commandement  
du renseignement des  
Forces canadiennes





containing keywords of interest. Comparing automated results to the products created by a trained, experienced OSINT analyst has shown that the benefits of human insight are irrefutable. A machine learning solution that can provide a daily push notification in response to our PIRs and IRs has yet to be fully realized.

Intelligence analysts are also often impeded in their online intelligence collection because they do not have access to sources behind subscription-only firewalls or their searches are being blocked by our own network protocols as part of our cyber defense. The CFINTCOM OSINT capability has tools, software, and subscriptions that can assist analysts in overcoming these limitations.

A more complex and challenging problem for our community is ensuring adherence to the policies related to collecting and using OSINT data as they pertain to the privacy of Canadian citizens and intellectual property. It is not always easy to ascertain if a Canadian citizen is the author or originator of the information we would like to collect, particularly in the social media environment. In a media landscape where anyone can post information without attribution, it becomes a legal imperative to investigate the source of online information in order to respect both privacy and intellectual property.

## OSINT Analysis

Unknown authorship is only one of the reasons that it can be difficult to assess the quality of the information available in the open-source domain. Foreign actors, right-wing extremists, and pranksters use misinformation and disinformation to purposefully manipulate and distort online information to the adversary's advantage. Most often, only the highest quality and most relevant sources are used to inform the OSINT daily products and the responses to requests for information; however, the product may still include misinformation/disinformation if doing so will add to the end user's understanding of a particular issue or problem. In these instances, the OSINT daily product will include a source comment to alert the reader and, if possible, additional references to present a balanced understanding of the facts pertaining to the situation.

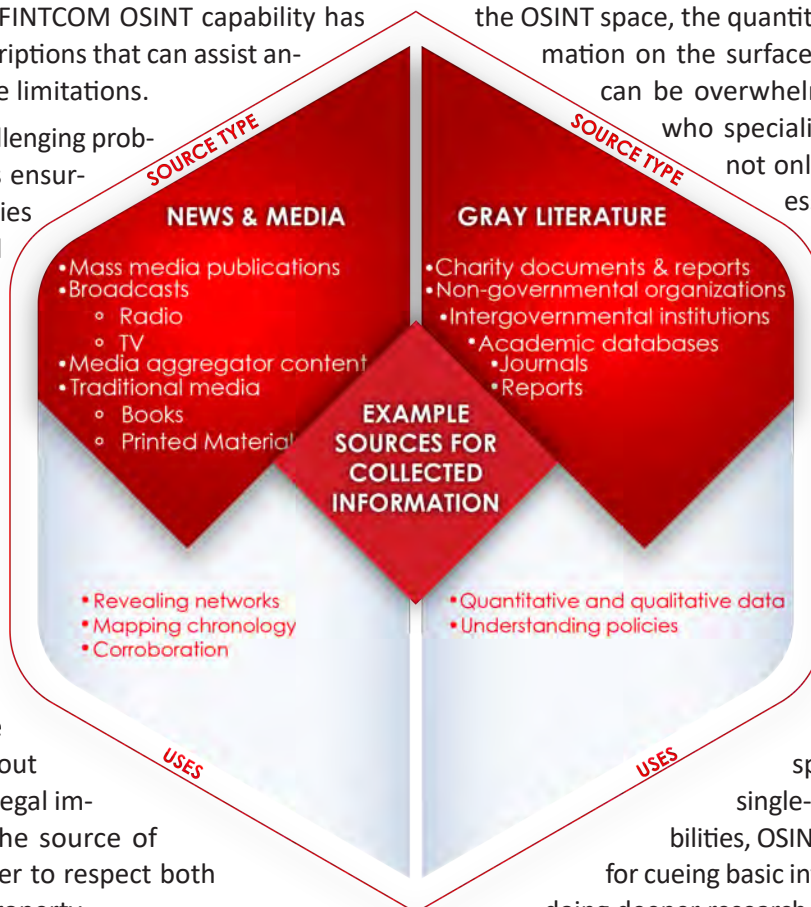
Comments on the source are the primary, but not the only, type of analysis that is added to the OSINT daily product. Other types of analysis include the creation of infographics to visualize patterns and trends, comments drawing attention to the way in which a situation has changed since the previous report, or a timeline of upcoming events and activity to watch for.

Staying current with all classified sources can already overwhelm analysts who are charged with becoming experts in an area and providing high-quality, relevant intelligence. In the OSINT space, the quantity of publicly available information on the surface, deep web, and dark web can be overwhelming. Engaging colleagues who specialize in the OSINT domain is not only appropriate but also necessary in order to be effective as an organization. OSINT, as a domain, is significant in scope and requires specialist training and equipment to be effective. The OSINT analyst has the requisite tools and training to work in the open-source realm.

Specialists in OSINT are just as crucial to the all-source fusion concept as are the HUMINT, SIGINT, or imagery intelligence specialist. Like these other single-discipline intelligence capabilities, OSINT requires a tactical element for cueing basic information and a backend for doing deeper research with specialists and experts who can leverage the power of the available sources. Conducting internet searches without the use of specialized tools and advanced tradecraft can reveal more information about the institution than it is advisable to permit. Thus, policies exist to prohibit the negligent use of the internet for intelligence gathering. OSINT specialists are proficient in collecting information in a manner that protects the institution's PIRs from foreign actors.

## Conclusion

OSINT is a critical element to the development of intelligence. As a stand-alone capability, products like the CFINTCOM daily regional update enable general situational data and information on relevant intelligence questions as defined through an intelligence business process that is tested and proven. As an element of the all-source intelligence production process,





tailored OSINT products are critical to intelligence production because of the value that OSINT analysts provide through their expert knowledge of the regional OSINT landscape, access to specialized tools and datasets, and the business processes they follow as a part of the intelligence cycle. The result of this intelligence-driven process is that all-source analysts, as well as generalists, receive a high-quality product that enables them to answer their ongoing IRs. ✨

#### Endnote

1. Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Lanham, MD: University Press of America, 2004), 14.

LCol David Holtz is an intelligence professional in the Canadian Army. With 36 years of service, he has operational experience as a G-2, J-2, and G-3 and experience leading an intelligence unit on operations. LCol Holtz holds a master of arts with distinction in intelligence collection. He currently serves as the senior Intelligence Directing Staff at the Canadian Army Command and Staff College.

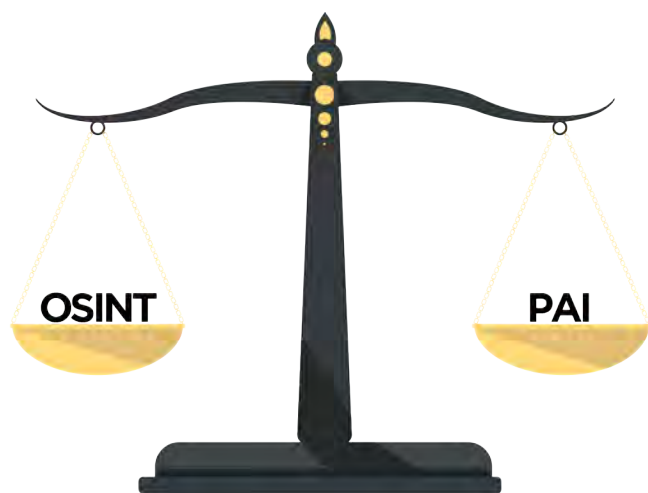
Ms. Angela Maxwell is the interim director of the Open-Source Intelligence Operational Support Team at Canadian Forces Intelligence Command, where she has worked for the past 15 years. She is also an intelligence professional in the Canadian Navy and has operational experience serving in Afghanistan and the Middle East.



### Publicly Available Information

To assist in understanding how to leverage publicly available information (PAI) effectively, the U.S. Army Intelligence Center of Excellence has developed three interactive multimedia instruction modules—Digital Literacy, Operating in the Cyber Domain, and Threat Capabilities in the Information Environment and Cyber Domain. These modules are available to all Army intelligence professionals at <https://libicoe.army.mil/products/pai> (common access card login required).

PAI is becoming more crucial in intelligence analysis, cybersecurity, and criminal investigations. Researching PAI brings with it an increasing need to protect oneself from threats while operating in the cyber domain. As our activities in this domain grow, so too must our actions in security. In this training, Service members will learn the ground rules of operating and protecting themselves in the cyber domain.



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."<sup>1</sup>

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.<sup>2</sup> Former Director of the Defense Intelligence Agency LTG Samuel Wilson went further, estimating that open sources account for 90 percent of relevant intelligence.<sup>3</sup>

Despite its apparent popularity, open-source intelligence (OSINT) made little progress through the early 21<sup>st</sup> 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."<sup>4</sup> 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.<sup>5</sup>

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]."<sup>6</sup> 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."<sup>7</sup> 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.<sup>8</sup>

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.<sup>9</sup> 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.<sup>10</sup>

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?<sup>11</sup> 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.<sup>12</sup> 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.*<sup>13</sup>

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.*<sup>14</sup>

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.<sup>15</sup> 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.<sup>16</sup>
- ◆ Instagram photos, Google Street View imagery, and commercial satellite photography all fit into definitions of imagery intelligence.<sup>17</sup>
- ◆ 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.<sup>18</sup>

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.”<sup>19</sup> 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 on-line transmission patterns.
- ◆ Exploitation of dark web content, including the use of commercial indexing tools.<sup>20</sup>

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.



PMESII/ASCOPE: OSINT-derived data																																		
	Areas	Structures	Capabilities	Organizations	People	Events																												
Political	Spatial public support (geographically focused online content)	Crowd-sourced facility ID Meeting Locations	Messaging/propaganda Reach and resonance	Dissident groups Activist movements	Local/regional power-brokers Influencers	Upcoming rallies, demonstrations, riots																												
Military	Camps Training areas	Deployed locations Undeclared sites	New equipment fielding Air/maritime deployment "Prestige" weapons	Bi/multilateral training participation Patch recognition	Promotion/reassignment Insurgent leaders	Attacks/deployments Messaging campaigns Mis/disinformation																												
Economic	Acquisition sources Shops/bazaars Dark web markets	Crowd-sourced facility ID Map-tracking Background geolocation	Sanctions evasion Block-chain transactions	Foreign investment orgs Sovereign fiscal actions Policy bodies/influencers	Corporate leaders "Cut-out" investors Business reps	Corporate events Fiscal agreements FDI activities (BRI, etc.)																												
Social	Meeting/protest sites Internet cafes Target PoL locations	Mosques/madrasas Transit points	Sentiment Network size/sustainment	Movements and organizations SNA (centrality)	Influencers Dissidents	Trade forums Meetings																												
Information	Influential press/data sources Messaging platforms	Comms methods Network vulnerabilities IP routing/server data	Data penetration Censorship	News/data sources Propaganda sources Content tailoring	Influencers Bot networks	IO themes/messages Info breaches/leaks Influence campaigns																												
Infrastructure	Development projects Critical junctions (water, electric, etc.)	Port characteristics airfield activities power/water status	Infrastructure status (crowd-sourced data) Service shortages	Construction companies Shipping organizations Air carriers	Investors Foreign gov. reps (e.g. BRI)	Development projects Service disruptions (blackouts, etc.)																												
<table> <tr> <td>BRI</td><td>Belt and Road Initiative</td><td>ID</td><td>identification</td><td>Orgs</td><td>organizations</td><td></td></tr> <tr> <td>Comms</td><td>communication</td><td>Info</td><td>information</td><td>PoL</td><td>political</td><td></td></tr> <tr> <td>FDI</td><td>foreign direct investment</td><td>IO</td><td>information operations</td><td>Reps</td><td>representatives</td><td></td></tr> <tr> <td>Gov</td><td>government</td><td>IP</td><td>internet protocol</td><td>SNA</td><td>social network analysis</td><td></td></tr> </table>							BRI	Belt and Road Initiative	ID	identification	Orgs	organizations		Comms	communication	Info	information	PoL	political		FDI	foreign direct investment	IO	information operations	Reps	representatives		Gov	government	IP	internet protocol	SNA	social network analysis	
BRI	Belt and Road Initiative	ID	identification	Orgs	organizations																													
Comms	communication	Info	information	PoL	political																													
FDI	foreign direct investment	IO	information operations	Reps	representatives																													
Gov	government	IP	internet protocol	SNA	social network analysis																													
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.<sup>21</sup>

## 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.<sup>22</sup>

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.<sup>23</sup> 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.<sup>24</sup>

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.*<sup>25</sup>

## 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.<sup>26</sup>

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.<sup>27</sup>

## 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.”<sup>28</sup> While NSA rarely discusses the exact communication systems targeted, it is widely accepted that this includes cellular phones and other connected computing devices.<sup>29</sup>

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:<sup>30</sup>

- ◆ 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.<sup>31</sup> 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.

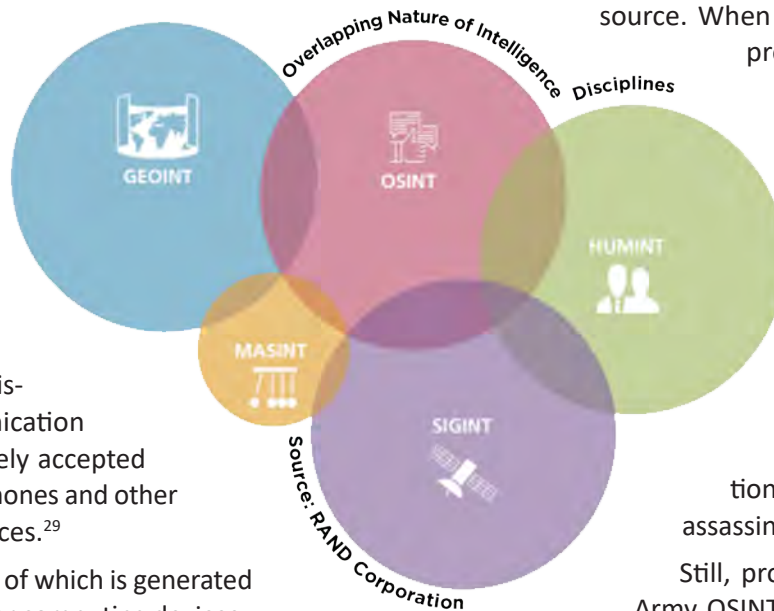
## Recommendations

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.<sup>32</sup>

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.<sup>33</sup> 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,<sup>34</sup> 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, 80<sup>th</sup> Congress, 1<sup>st</sup> 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, 109<sup>th</sup> 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.

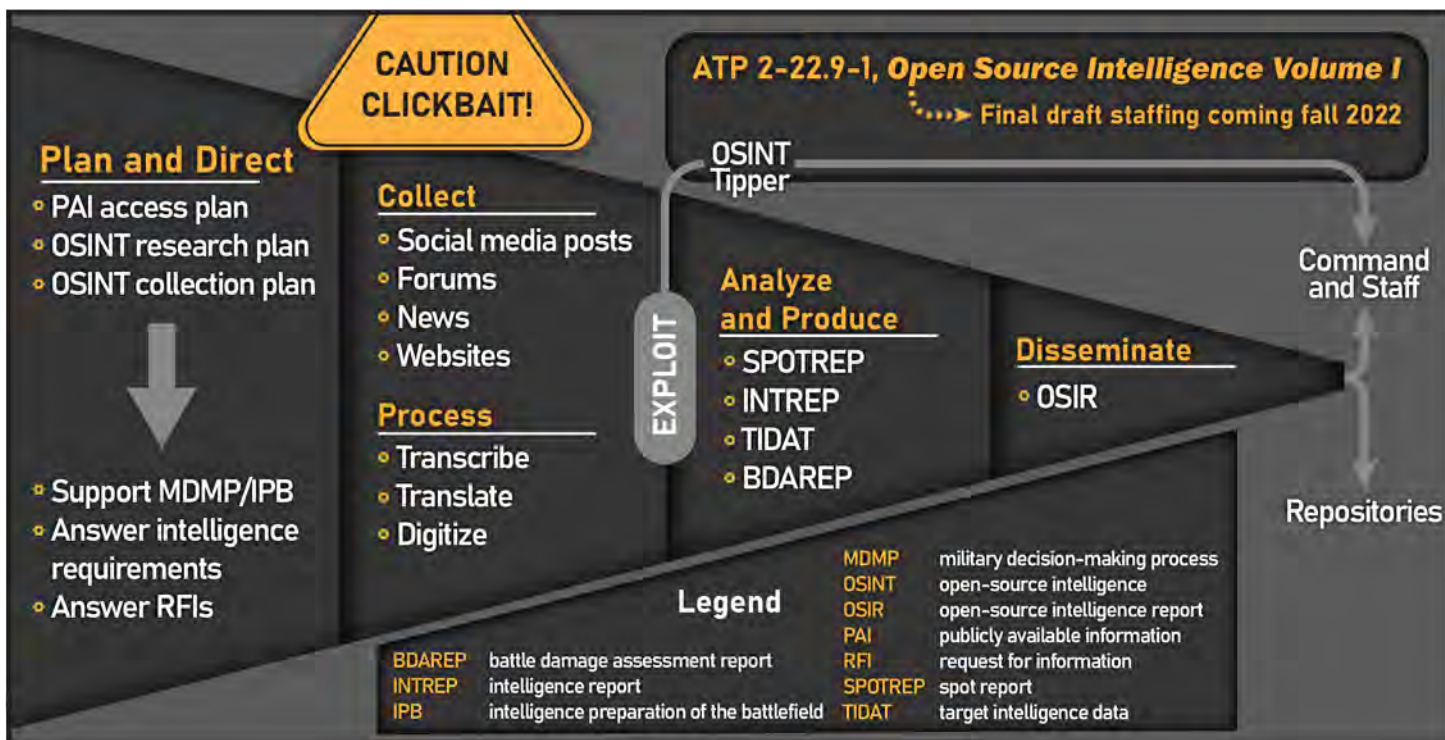
19. Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, B-1.

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.commbio.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 513<sup>th</sup> 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).





# OPEN-SOURCE INTELLIGENCE: DEVELOPING ANALYTICAL CAPABILITY FOR THE AUSTRALIAN ARMY

By Warrant Officer Class 1 Greg Hopper, Australian Army

*Army is responding to Accelerated Warfare as an Army in Motion—our teams are ready now and future ready for cooperation, competition and conflict.*

—Lieutenant General Rick Burr, AO, DSC, MVO  
Chief of Army, Australian Army

## Introduction

The Australian Army is renewing its focus to meet the challenges of the current and future operating environments when working with joint, interagency, coalition, and whole of government task forces. It is also reviewing the impact and role of open-source intelligence (OSINT) in supplementing and supporting traditional military intelligence. The Australian Army, through the Land Intelligence, Surveillance, Reconnaissance, and Electronic Warfare (LISREW) program in the Land Capability Division, Army Headquarters, has started the process to develop tactical and operational OSINT. The LISREW program aims to support commanders' decision making by improving situational awareness, which it achieves through a layered, multispectral network of sensors enabled by specialist intelligence.

The Australian Army is focusing on being future ready, and OSINT forms a key part of that requirement. LISREW has the authority to conduct OSINT analysis across the Army to inform the joint force. We are currently in discovery and undertaking trials to understand the workforce requirements, available systems, and software. The key challenges are individual intelligence analysis, collection management, and software support. This article will describe these challenges and will explain how we are identifying common problems and solutions.

As the Army OSINT workforce has grown, systems and commercially available software have been deconflicted with the Australian Defence Force, Joint Capability Group. This has allowed an economy of effort, increasing the capacity for the development of a Service OSINT capability while supporting joint needs. Until this point, some work had been done to meet specific capability requirements for supported commanders and units; however, this was by necessity rather

than by design. This is now being addressed through significant engagement to develop baseline OSINT skills for analysts across the Army and the broader Australian Defence Force writ large.

The **Army Objective Force** seeks to optimize the Army for Accelerated Warfare. The Army Objective Force represents the next steps in the future design of the joint force—with an Army in Motion that will work more effectively across all domains and environments.

The **Joint Capability Group** was formed in July 2017 and has continued to evolve since its inception. The group provides a wide range of enabling capabilities to the Australian Defence Force services, including logistics support and services, health services, professional military education and training, and military legal services. The Joint Capability Group is also responsible for progressing leading-edge capabilities, such as cyberspace, data link, and satellite communications.

**Forces Command's** role is to prepare land forces in order to enable the joint force.

**Special Operations Command's** role is to provide ready and relevant forces to conduct special operations across the operational domain in a joint, combined, or interagency environment in support of Australia's national interests.

**Joint Operations Command's** role is to plan, control, and conduct operations, activities, and actions as directed to meet Australia's strategic objectives. Joint Operations Command is the critical node in applying defense capability at the operational level and conducts operations and exercises to meet government aims, deepen Australia's alliances and partnerships, and prepare the joint force for future contingencies.

## Developing Open-Source Intelligence Analysts

The Australian Army has developed its OSINT training continuum through attendance at a range of military-partnered OSINT courses and commercial vendor training.<sup>1</sup> Feedback from the training indicated that commercial vendor training depended mostly on licensed software that was part of the vendor package, creating a reliance on the commercial software for OSINT research and analysis activities.

Although these types of applications are important in the context of OSINT capability development, intelligence analysts require the ability to conduct OSINT in a commercially agnostic environment in order to develop their critical thinking skills and generate comprehension of the operating environment's

magnitude and scope. Like learning to drive a car, once people are competent in basic skills, they can readily transfer those skills to larger, more complex vehicles without having to cover the fundamentals again.

This lesson has shaped the Australian Army's development of a customized OSINT training package for intelligence analysts, drawn from the breadth of training we attended. Focusing on individual analyst tradecraft skills was critical for the development of a generalist OSINT analyst. Regardless of an analyst's level of employment (tactical to strategic) within the Australian Army or the Australian Defence Force, the OSINT training package focuses more on individual appreciation of a range of tools and the process of OSINT rather than specific training and reliance on individual tools. This means that as the Australian Army develops its OSINT workforce for Service, partnered, or joint operations, capability development across the wider Australian Defence Force for the joint force integrator can occur using commercially available software for the breadth of OSINT activity required for information fusion and intelligence support.

Select Australian Army OSINT analysts now have the flexibility to apply their skills within the scope of a capability rather than training on individual tools. For example, this can be supporting tactical units for threat warning or situational awareness using limited tooling and online access, or operating in an intelligence fusion environment with significant commercial tooling support and defined reporting requirements.

In order to develop the breadth of skills for general OSINT analysts, we applied the following core fundamental OSINT skills to our training:

- ◆ **Australian and Australian Defence Force policy and legislation, including data management.** Describes the details required for a clear legal understanding of individual requirements and collective OSINT activities.
- ◆ **Operating in the open-source environment and the internet.** Teaches the pillars of open-source intelligence, digital domains, and key terms and concepts related to the internet and the web (surface web, deep web, and dark web).

#### Three Layers of the Web<sup>2</sup>

##### Surface Web

- Accessible.
- Indexed for search engines.
- Little illegal activity.
- Relatively small.

##### Deep Web

- Accessible by password, encryption, or through gateway software.
- Not indexed for search engines.
- Little illegal activity outside of dark web.
- Huge in size and growing exponentially.

- ◆ **Search engines and web browsers.** Describes how to exploit search engines to conduct safe and secure initial website reconnaissance.
- ◆ **Open-source research opportunities and limitations.** Describes open-source intelligence, associated drivers, and risk management, including identifying and collecting information from news aggregators, multimedia, and other open resources.
- ◆ **Threats to open-source research and mitigation.** Focuses on operational security and communications security in an open-source context. Delivers practical security tradecraft relevant to open-source research and provides insight into adversary tradecraft implemented to mitigate compromise.
- ◆ **Online web resources and data extraction software.** Teaches how to use online tools to discover data from deep web sources and exploit online maps and tracking tools.
- ◆ **Source evaluation.** Teaches how to understand and explain source evaluation and content assessment techniques, including information corroboration, image and video verification, and the currency, relevance, authority, accuracy, and purpose method.

#### The Currency, Relevance, Authority, Accuracy, and Purpose Method<sup>3</sup>

**Currency:** The timeliness of the information.

**Relevance:** The importance of the information for your needs.

**Authority:** The source of the information.

**Accuracy:** The reliability, truthfulness, and correctness of the content.

**Purpose:** The reason the information exists.

- ◆ **Planning of open-source collection.** Describes the use of online tools to discover data from deep web sources and exploit online maps and tracking tools.
- ◆ **Open-source research and evaluation.** Introduces analysts to the ontology of various data, information, and resources that assist participants in managing open-source information collection tasks.
- ◆ **Research plans.** Highlights the importance of creating a research plan in the initial stage to produce better quality OSINT reports and briefings. Teaches analysts the value of using a research plan to navigate their OSINT process, as the plan will help them to understand the

##### Dark Web

- Restricted to special browsers.
- Not indexed for search engines.
- Large-scale illegal activity.
- Unmeasurable due to nature.



information they are trying to produce, the audience they are producing it for, and ways to manage the information they require. Analysts learn how to identify resources and apply advanced use of search engines. They also learn how to track search trends and exploit search engines using Boolean functions before commencing their task.

- ◆ **Use of social media.** Describes and outlines the social media landscape. Categorizes social media landscapes by theme, platform, and location to improve participant understanding and research tradecraft. Reviews social networking sites in depth, discussing platform history and evolution, usage by different threat actors, trends in activity and relation to real-world threats, and security incidents.

## Collection Management Challenges

The key elements of the training provide analysts an understanding of the OSINT environment and introduce the capabilities and limitations that are imposed before, during, and after online activities. Moreover, the importance of planning and deconfliction is reinforced throughout the training, with an emphasis on attribution management to account for the environment and hostile threat manipulations.

These elements include a focus on the requirements and collection management process within the OSINT team environment. This process is manageable when individuals and teams are conducting activities; however, the complexity of deconfliction across the enterprise has yet to be addressed. This is compounded again within the joint or partnered environments with increased numbers of analysts conducting online activities. The ability to coordinate collection and conduct research is paramount within the OSINT environment when there are potentially hundreds of analysts pursuing information requirements online. Key challenges for requirements and collection management in an OSINT environment include—

- ◆ **Deconfliction of source information being applied to assessments.** This becomes more difficult when dozens of commercial software platforms are used or analysts are conducting individual tradecraft research across the organization. How do we mitigate single-source reporting from multiple analyst assessments?

- ◆ **Increase in OSINT analysts' online activities.** As the number of OSINT analysts' online activities increases, a single analyst's innocuous search may no longer be innocuous. The digital footprint to websites and data sources resulting from increased analyst research may provide hostile entities an understanding of our requirements and tactics, techniques, and procedures. This could give our adversary an opportunity to manipulate the environment or conduct targeted misinformation.

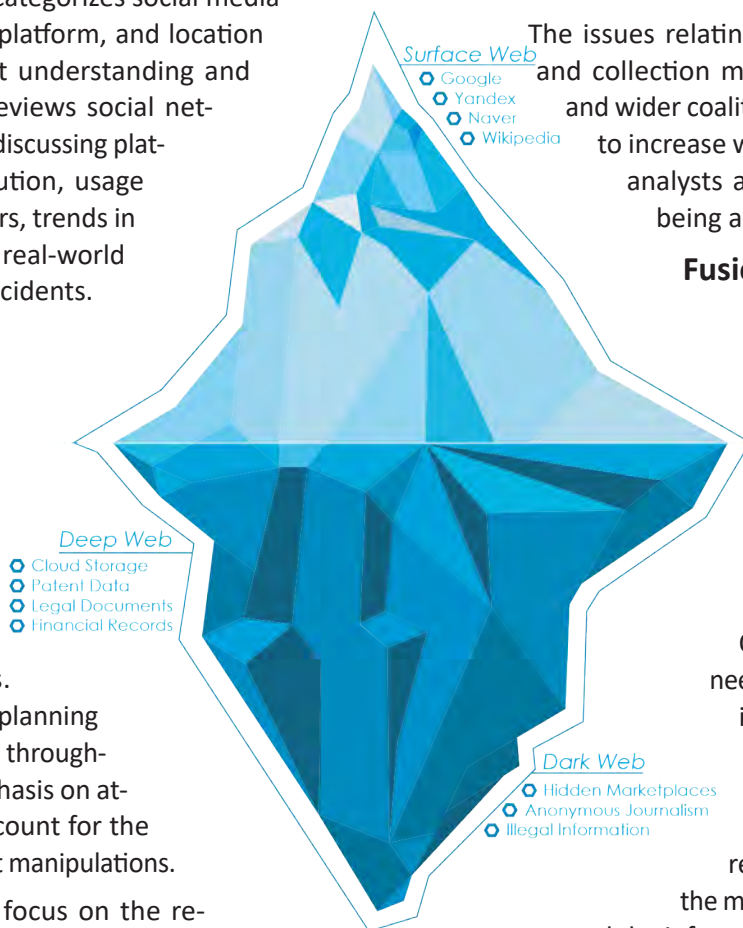
The issues relating to OSINT source validation and collection management across the Army and wider coalition environment will continue to increase with the expansion of qualified analysts and the varied software tools being applied.

## Fusion and the Use of Commercial OSINT Software

As the Australian Army continues to develop its capability across the organization (Forces Command, Special Operations Command, and in support of Joint Operations Command), OSINT needs remain varied and challenging. Although individual skills are critical for intelligence analysts conducting research and for indicators and warning, the reality is that we must protect the members of our OSINT workforce and the information they are analyzing when operating online. We can achieve this protection with tools and systems that reduce their attribution, thereby retaining personal and organizational anonymity and protections.

The development of software and applications for the conduct of OSINT within the Australian Defence Force environment remains limited, with commercial sources being the most economical approach. As the Australian Army continues to develop the individual OSINT skills and knowledge of its people, we are pursuing systems and commercial software for the OSINT capability across the Australian Defence Force, alongside other Services. In doing so, the Army can support commercial software application trials and provide recommendations for differing levels of command and operational focus.

The breadth of capabilities from OSINT is extensive, with many commercial platforms for niche collection requirements;



however, when looking at commercial software, we need to consider more than just functionality. When selecting vendors, the Army, and more broadly the Australian Defence Force, should ask the following questions:

- ◆ Where did the software originate?
- ◆ What security measures are in place to support online user activities?
- ◆ Who can access the searches and research being conducted?
- ◆ Can the gathered information be easily packaged and transferred?
- ◆ What are the information export formats?
- ◆ Can search parameters be exported and integrated with competing OSINT software?

The selection of OSINT software remains a challenge to ensure applications provide the security and reduced attribution required for the conduct of intelligence operations research. The Army's ability to leverage multiple OSINT software applications in this area creates greater scope to develop and steer the support to end users within the Army and its commands.

## Conclusion

The challenges that the Australian Army faces in developing its OSINT analytical capability require us to remain squarely focused on developing individual skills and knowledge across

the workforce. The application and employment of the skills are the cornerstone to empowering a flexible resource for OSINT across the spectrum of operations at all levels of command. Through the development of the basics, a variety of commercial software, implemented via the Joint Capability Group as the joint force integrator, will ensure OSINT analysts have the ability to apply relevant and timely assessments. These assessments will support tactical units' threat warning and situational awareness as well as operations in an operational or strategic setting. ✨

## Epigraph

Australian Army, *Army in Motion Accelerated Warfare Statement by Lieutenant General Rick Burr, AO, DSC, MVO* (22 October 2020), 1, <https://www.army.gov.au/our-work/army-motion/accelerated-warfare>.

## Endnotes

1. U.S. Department of the Army's Basic Open-Source Intelligence Courses 301 and 302; and commercial vendors such as SANS Institute, BlackHorse Solutions, Cyberspace Open Source Methods and Operations (COSMO), Janes, and OSINT Combine.
2. Andrew Quinney, "Surface web vs deep web vs dark web," Service Care Solutions, 27 June 2016, <https://www.servicecare.org.uk/news/surface-web-vs-deep-web-vs-dark-web-61792715468>.
3. "Evaluating Sources: The CRAAP Test," Benedictine University, accessed October 29, 2021, <https://researchguides.ben.edu/source-evaluation>.

*WO1 Greg Hopper is a career intelligence professional with over 30 years' experience in a range of intelligence disciplines, including combat intelligence, special operations, psychological operations, and human intelligence. WO1 Hopper has operational experience from multiple deployments to the Middle East and the South West Pacific. He works in the Australian Army's Land Intelligence, Surveillance, Reconnaissance, and Electronic Warfare directorate at Army Headquarters, responsible for developing future intelligence capabilities.*



## BE ON THE LOOKOUT...

### ATP 2-01.4, Intelligence Support to Army Targeting

- Currently under development.
- Provides foundational guidance for executing Army intelligence support to targeting at echelons theater and below.
- Focuses on conducting support to targeting across all intelligence disciplines.
- Complements and expands on the discussions of intelligence support to targeting in FM 3-60, *Targeting*.



**Final draft staffing in late summer 2022**







# MAPPING THE INFORMATION ENVIRONMENT WITH OPEN-SOURCE INTELLIGENCE AND ALLIES

By Mr. Matthew D. Skilling

## Introduction

In 1946, Argentine author Jorge Luis Borges wrote “On Exactitude in Science,” a short story in which he tells the tale of a great Empire, skilled in cartography, that wished to create an intricately detailed map of its territory. The Empire’s cartographers started with a map at 1:1000 scale. Finding the detail lacking, they moved to 1:100 scale, then 1:10, and finally created a map at 1:1 scale. The map contained every possible detail and covered the entirety of the Empire’s lands. As the Empire expanded, so did the map. Centuries later, the Empire fell, but remnants of the unwieldy map remained.<sup>1</sup>

With the advent of the internet, Borges’ fabled 1:1 map became reality. Today, this map finds a parallel in the doctrinal term *information environment*. The information environment touches every operational domain and acts as the embodiment of a nation’s combined knowledge. Exploiting the information environment can lead to understanding the battlespace, and controlling the information environment provides a level of control over the battlespace.

In the last decade, several nations leveraged operations within the information environment for military purposes to impose their will against a neighboring territory and to expand their map. Notable examples include China in the South China Sea and Russia in Georgia and Ukraine.

## Understanding the Information Environment

U.S. Army Europe and Africa (USAREUR–AF) identified an increased need to understand the information environment following Russia’s 2014 annexation of Ukrainian territory in Crimea and Donbas. Upon review, indicators and warnings before the offensive were present in messaging campaigns on regional and local media outlets and in social media posts citing troops and equipment participating in short-notice exercises.

It is crucial to improve the U.S. Army’s understanding of the information environment as part of multidomain operations and information advantage activities. Open-source intelligence (OSINT)—the exploitation of publicly available information for intelligence purposes—uniquely fills this requirement. It provides information environment intelligence that is timely, tailored, and inherently sharable. OSINT supports validation and the tipping and cueing of other intelligence functions, and it monitors for indicators and warnings. Most importantly, it provides context to intelligence by expanding traditional reports from stand-alone pieces of information to part of the theater’s information environment 1:1 battlespace map.

## Northern Raven

The Army Europe Open Source Center leads this effort and includes a dedicated OSINT collection and technical control division for European federated collection with assigned military, civilian, and contract staff. Despite organic growth in the last few years, the need for a multinational response is necessary to collect the theater at a 1:1 scale. USAREUR–AF established Northern Raven (NRV), an OSINT combined collection operation in 2019.

NRV is an OSINT community of nearly 20 North Atlantic Treaty Organization (NATO) allies and European partner nations built on the professionalism and personal connections of the participants to provide a cultural and numerical advantage in the information environment. It mitigates shortfalls, expands capacity, and develops joint understanding and techniques. This community cannot be replicated by our adversaries and solidifies the bonds across theater to improve U.S., allied, and partner posture and competitiveness in the information environment.

In a combination of episodic deployments and standing exchanges, the multinational OSINT team conducts OSINT tasking, collection, processing, exploitation, and dissemination (also known as TC-PED) across NATO allies and European partners to increase, improve, and synchronize collection capacity within Europe. NRV addresses four key challenges observed in theater:

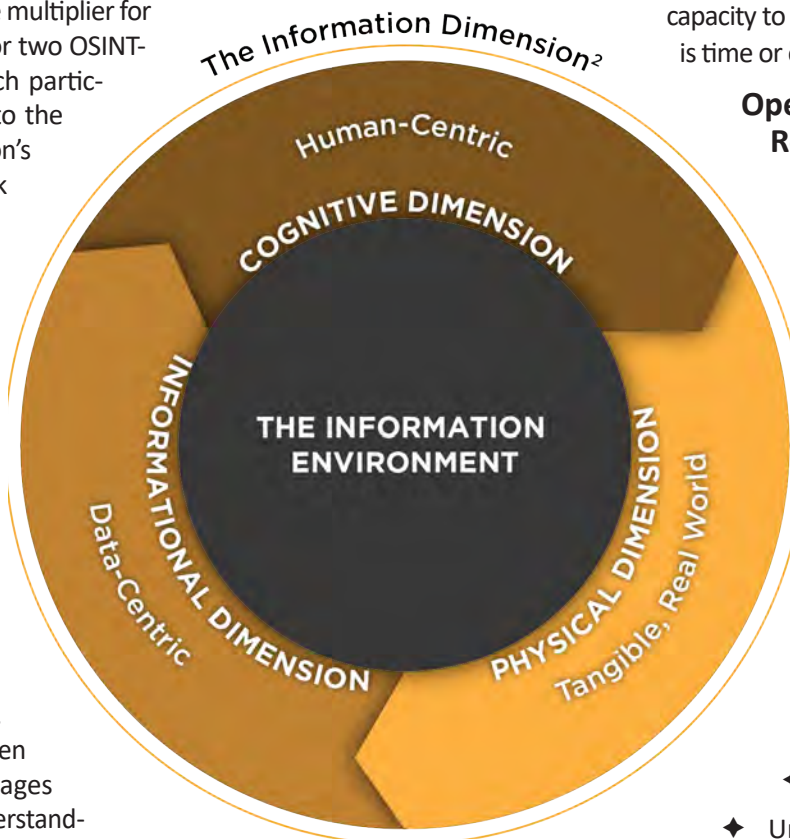
- ◆ Personnel.
- ◆ Cultural knowledge.
- ◆ Training.
- ◆ Tools.

**Personnel.** Personnel shortfalls in emerging disciplines like OSINT are not unique to our nation. Across Europe, militaries are struggling to develop and maintain collectors and analysts to meet the demands of the information environment. NRV acts as a force multiplier for participating nations. One or two OSINT-trained personnel from each participating nation gain access to the combined collection operation's shared resources and network of nearly 100 intelligence professionals with unique skillsets and expertise.

**Cultural Knowledge.** NRV identifies and fills information shortfalls through knowledge sharing and cross-communication. For the United States, these shortfalls commonly relate to language skills, cultural understanding, and subject matter expertise. Soldiers from Europe are often proficient in multiple languages and maintain a detailed understanding of the information environment through daily contact. Additionally, many European militaries are not bound to regular troop rotations. This allows additional time for partner "OSINTers" to build extensive subject matter expertise in advisory unit composition, training, tactics, and procedures. With regard to time and cost, it is not feasible to train U.S. Soldiers to match this skillset and level of understanding. However, a cornerstone of the U.S. Army is the ability to develop doctrine and training.

**Training.** The U.S. Army's OSINT training pipeline is robust; it starts from the basics of publicly available information and builds toward advanced collection tradecraft. A vast majority of allies and partners use on-the-job training to develop collection skills and lack a formal training curriculum. As part of NRV, the U.S. Army provides the first two courses in the OSINT training program, creating a baseline set of collection tactics, techniques, and procedures to establish common terms and mitigate associated risks. During the training, NRV members actively share and update tradecraft as approaches to collection evolve. At the conclusion of training, NRV members gain limited access to U.S. OSINT capabilities.

**Tools.** While allies and partners excel at knowledge depth, the U.S. Army provides innovation, technical capability, and capacity. NRV participants have the ability to conduct live environment training using U.S. OSINT tools. The commercial-off-the-shelf tools focus on signature reduction and machine-assisted bulk data collection and reduce the time-cost associated with collection across multiple sources. For many nations, these tools are inaccessible because of cost, procurement timeline, and foreign sale constraints. Using the tools in a live environment provides additional capacity to the partners, even if the usage is time or event bound.



## Open-Source Intelligence Reports

NRV captures individual pieces of information in reports similar to traditional intelligence functions. Open-source intelligence reports (OSIRs) are published on several domains and platforms for widest dissemination. The reports are a reflection of how the participating nations view information environment activities and typically fall into three categories:

- ◆ Inform.
- ◆ Understand.
- ◆ Defend

**Inform.** Nations using OSINT to inform prioritize speed. Information OSIRs are short with a high publication rate. They typically have few collector comments and leave assessments of truthfulness to the end user. This is a passive type of collection; it relies on tools to bulk-gather data and puts the OSINT collector in a processing, exploitation, and dissemination role for broad topics or general information. The analytical element has the burden of bundling these reports generated at near real time.

**Understand.** Nations using OSINT to build understanding prioritize context and consolidation. Understand-style OSIRs are in long form with operational details, and they focus heavily on collector comments for context. These reports typically publish based on events or quarterly review timelines. Often, the collector and analyst are the same Soldier, allowing for source assessment and real-world context. Analytical elements rely on these OSIRs to drive long-term analysis. This collection typically requires an active collector



## Open-Source Intelligence Reports

### Inform

- Prioritize speed.
  - Contain few analyst comments.
  - Leave assessment to the end user.

### Understand

- Prioritize context and consolidation.
- Contain source assessments.
- Provide real-world context.

### Defend

- Present unique approach.
- Focus on “how” not “what.”
- Assess effects of adversary operations on populace.

to better understand, inform, and defend the information environment and influence the battlespace. Gathering OSINT is more than browsing social media. The public availability of the information speeds sharing between nations, helps consolidate foundational intelligence, and builds the trust necessary to expand sharing across all intelligence functions. As the United States, allies, and partners in Europe continue to share, the context of intelligence reports expands and empowers our leaders to make faster and more informed decisions to maintain the critical advantage of time. ✨

role. The collector leverages language, cultural knowledge, and subject matter expertise to search for answers to specific intelligence requirements.

**Defend.** The use of OSIRs for defense is a unique approach. The reports vary in length, with a focus on “how” instead of the traditional 5Ws (who, what, where, when, and why). Using the borders on their own map as defensive lines, collectors search for adversary operations within the information environment and assess the effect within their own population. Unlike the other two report types, defensive OSIRs do not directly support multidomain operations. Instead, they support information advantage activities. These reports require a deep understanding of the nation’s own information environment, and in some cases, legal hurdles can prevent intelligence collection against a nation’s own population.

## Conclusion

USAREUR–AF’s development of multinational OSINT is an innovative space leading the U.S. Army’s transition to multidomain operations and operations in the information environment. Every NRV participant nation draws a unique version of the 1:1 map. NRV attempts to merge these versions

### Endnotes

1. Translated into English by Andrew Hurley, the original Spanish title is *Del rigor en la ciencia*. Some English translations prefer “On Rigor in Science.” The story was first published in March 1946, in the journal *Los Anales de Buenos Aires*, año 1, no. 3, where it formed part of a piece called “Museo.” “On Exactitude in Science,” Genius Media Online, accessed November 18, 2021, <https://genius.com/Jorge-luis-borges-on-exactitude-in-science-annotated>.
2. Graphic adaptation from Office of the Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)* (Washington, DC: The Joint Staff, 25 July 2018), 2.

*Mr. Matthew Skilling is assigned to the 24<sup>th</sup> Military Intelligence Battalion, 66<sup>th</sup> Military Intelligence Brigade–Theater, U.S. Army Europe and Africa, as Chief of Open-Source Intelligence Operations. He is a former intelligence noncommissioned officer in the U.S. Army and holds a juris doctorate from Valparaiso University School of Law.*



**Sergeant Christian Torres**

### Creating an OSINT Cell at the Division Level

In February 2021, the 82<sup>nd</sup> Airborne Division's G-2 began operating its first open-source intelligence (OSINT) cell. In establishing the cell, the 82<sup>nd</sup> G-2 fulfilled all the crucial requirements of the Army OSINT Office and U.S. Army Forces Command (FORSCOM). Specifically, it—

- ◆ Staffed positions with analysts who had completed the basic OSINT courses (OS 301 and 302).
- ◆ Obtained authority to conduct OSINT research.
- ◆ Established risk assessments.
- ◆ Created collection plans.

Instead of using all-source analysts, the 82<sup>nd</sup> Airborne Division chose a signals intelligence (SIGINT) analyst and a geospatial intelligence (GEOINT) imagery analyst as the first members of the team. Having Soldiers with diverse technical backgrounds enables the analysis of different types of publicly available information (PAI) and allows for better-informed tipping of other intelligence capabilities. As a GEOINT analyst, I have analyzed publicly available geospatial data, tipped our GEOINT cell, and structured a request for information to best capitalize on this type of PAI. The OSINT cell also receives weekly assistance from a contracted FORSCOM OSINT analyst whose subject matter expertise provides the G-2 staff with the ability to identify information about OSINT best practices, understand the legal space of OSINT, and help ensure proper legal procedure.

Over the past 11 months, the 82<sup>nd</sup> Airborne Division G-2 OSINT cell has expanded by adding two Soldiers. In addition

to certifying the training our new OSINT analysts received in OS 301 and 302, we also began providing additional training that reflects some of our lessons learned. OS 301 and 302 provide a solid basis for Soldiers and teach that creativity is one of the best tools an OSINT analyst can have because they broaden the type of information analysts think about collecting. What we learned over time is that creativity in OSINT is critically dependent on the quantity and quality of knowledge that analysts possess. The OSINT cell can easily facilitate an increase in knowledge by providing experience and reading material. Unlike any other intelligence discipline, OSINT has many learning resources. The real challenge is teaching analysts how to differentiate between what is important and what is not.

### Lessons from *Lawrence of Arabia*

For junior military intelligence Soldiers, too much focus is often on surface-level matters. A GEOINT analyst may fixate on the arrival or departure of a specific piece of equipment, a SIGINT analyst may look at an individual frequency or selector, and an all-source analyst may try to find and accumulate reports to support a single theory. These may lack a deeper analysis—asking the “so what?” For OSINT, this can be an even greater pitfall because of the vast amount of publicly available data. Reading hundreds of news articles in a week may cause information overload that makes finding what is important impossible because PAI is, by itself, often unremarkable. It is only through the aggregation, contextualization, and interpretation of PAI that our minds can process it into information of value. The OSINT analyst must go a step further and take a wide breadth of historical knowledge to fuse the rendered PAI and make it into information of intelligence value.



The movie *Lawrence of Arabia*, a historical drama based on the life of T. E. Lawrence, demonstrates relating PAI with context. Lawrence was a British archaeological scholar, military strategist, and author best known for his legendary war activities in the Middle East during World War I. Early in the movie, he receives an Egyptian newspaper to read the local headlines. As he expected, he reads that Arab tribes were attacking Turkish strongholds, to which he remarks, “I bet that no one in this headquarters even knows it happened. Or would care if it did.”<sup>1</sup> Lawrence, using his background as a Middle East scholar and having a desire to find information, was able to identify key PAI that was important for decision makers. In the case of Lawrence, he went deeper in his analysis by identifying the Arab tribes’ attacks as an indicator of escalation. This inherently made Arabia a crucial factor in the battlespace, which others had not fully realized. He did not just look at what had happened (in this case, an Arab tribe attacked Turkish forces), but he also looked at what the event meant. He saw there was an additional element, a new player, in the fight against the Ottoman Empire. It was in his later missions that he was able to find a way to capitalize on those indicators because he personally understood the motivations of the Arab tribes. Lawrence was able to do this because he applied strategic thinking—the act of taking background knowledge and weighing it against desired outcomes for an overarching purpose—to the knowledge he already had.



National Library of Norway. Public domain, via Wikimedia Commons

T.E. Lawrence in traditional Arab robes during the World War I and the period of the Arab Revolt.

## Applying Game Theory Concepts to OSINT

For our OSINT cell, the way we teach strategic thinking is by teaching and discussing game theory. Simply put, game theory is a theoretical framework of decision making that divides people into “players” as part of a “game.” The games can range from economics and evolutionary biology to warfare. Regardless of the player, game theory considers all players as “rational agents.” Being rational means players will always seek to make a decision to optimize the yields of their actions. In other words, people will do whatever they think is in their best interest. Examples of this are the prisoner’s dilemma and the dictator game.

### Game Theory

Game theory is a branch of applied mathematics that provides tools for analyzing situations in which parties, called players, make decisions that are interdependent. This interdependence causes each player to consider the other player’s possible decisions, or strategies, in formulating strategy. A solution to a game describes the optimal decisions of the players, who may have similar, opposed, or mixed interests, and the outcomes that may result from these decisions.<sup>2</sup>

### Prisoner’s Dilemma

American mathematician Albert W. Tucker originally formulated the prisoner’s dilemma. Two prisoners, A and B, suspected of committing a robbery together, are isolated and urged to confess. Each is concerned only with getting the shortest possible prison sentence for himself; each must decide whether to confess without knowing his partner’s decision. Both prisoners, however, know the consequences of their decisions: (1) if both confess, both go to jail for five years; (2) if neither confesses, both go to jail for one year (for carrying concealed weapons); and (3) if one confesses while the other does not, the confessor goes free (for turning state’s evidence) and the silent one goes to jail for 20 years.<sup>3</sup>

### The Dictator Game

In the dictator game, the first player, “the proposer,” determines an allocation (split) of some endowment (such as a cash prize). The second player, the “responder,” simply receives the remainder of the endowment not allocated by the proposer to himself. The responder’s role is entirely passive (he has no strategic input into the outcome of the game). As a result, the dictator game is not formally a game at all (as the term is used in game theory). To be a game, every player’s outcome must depend on the actions of at least some others. Since the proposer’s outcome depends only on his own actions, this situation is one of decision theory and not game theory. Despite this formal point, the name persists in the game theory literature because of the result’s usefulness to game theory at large.<sup>4</sup>

Game theory provides the OSINT analyst a structuralized analytical tool to enable finding the “so-what.” In our OSINT section, we do this by making a key part of research to investigate the motivations of the actors, identifying factors the “rational agents” will consider. OSINT is particularly well suited for this. With military intelligence naturally focusing through a military lens, an OSINT analyst can step away from this to investigate PAI and examine what an adversary might

be doing in the information environment. Instead of trying to see what kind of capabilities or maneuvers adversaries are concerned with, which is the subject matter other intelligence disciplines focus on, the OSINT analyst is more easily able to see what the adversary's grand strategy might be.

For example, if Country Y begins to withdraw from Country X, this may signal to other intelligence disciplines the end of further escalations, but the OSINT analyst might be able to find economic or political factors indicating inevitable further escalation from Country Y. The OSINT analyst may be able to provide critical awareness that, while immediate concerns have diminished, the threat picture from Country Y has only slightly changed. In another scenario, the amassing of Country Y's forces onto Country X's border may indicate imminent war, but the OSINT analyst might find that Country Y's current dictator is amassing forces to bolster votes in an upcoming election, and that while still possible, Country X is not truly seeking all-out war. In both cases, a grasp of game theory coupled with an OSINT analyst's knowledge facilitates deeper analysis. It is by teaching game theory that we can reliably achieve deeper analysis.

In the G-2 OSINT cell, when looking at a piece of information, we routinely ask our Soldiers, "What does game theory say?" We do this to ensure we are consistently applying analysis to our collection. It forces us to apply a structuralized method of reasoning that makes us collect as much information as possible, analyze the likely courses of action, and assess the data we have. By identifying what an adversary thinks is in their best interest, i.e., how they would best win their "game," we can identify likely courses of action. Since the 82<sup>nd</sup> Airborne Division serves as America's immediate response force, it is crucial that our research drive our intelligence assessments. Game theory helps our OSINT team digest the data we collect, determine its importance, and make quality OSINT products while we monitor for emergent threats.

## OSINT Products

In the year since our OSINT cell's inception, we have been able to provide a wide range of OSINT products. Typically, we provide a biweekly summary of major events in the world that could have an impact on the immediate response force. The OSINT cell disseminates this to leadership throughout the 82<sup>nd</sup> Airborne Division. When major events occur with the potential to trigger an immediate response force deployment, we often provide sentiment analysis to give decision makers an understanding of not only the events but also foreign nationals' reactions.

The OSINT cell also created a coronavirus disease 2019 (COVID-19) hotspot tracker to monitor the impacts of COVID-19 and its subsequent variants. We were able to set up a system to identify how serious an increase of infection was for a specific country. By researching different business statics formulas, we have found ways to see how COVID-19 affects a given country in ways that more accurately captures the growth of cases than merely looking at the daily infection increase. We then used other forms of PAI to assess what response we might see from that country. My own background as a GEOINT analyst helped with this because I was able to take publicly available graphic information system data, also known as GIS data, and combine it with our findings to turn it into a map visually depicting what we found. Prevalence of COVID-19 in any given country is a critical limiting factor to decision making strategies, and PAI is well suited for this kind of collection.

## OSINT during Operation Allies Refuge

When the immediate response force was activated to support Operation Allies Refuge, the recent noncombatant evacuation operation in Afghanistan, we had the opportunity to fully test our OSINT capabilities in a real-world scenario. The operation proved to be atypical from most stories one hears about OSINT. The most well-known stories involve an OSINT team that, through creativity and perseverance, found where the "bad guys" were, resulting in clear and decisive action. The reality of Operation Allies Refuge was that our primary mission was to provide the safe evacuation of personnel. The Taliban were providing security around the perimeter of Afghanistan's Hamid Karzai International Airport and throughout Kabul. OSINT collection on the Islamic State-Khorasan Province, also known as ISIS-K, was limited because of the rapid and asymmetric way the group operates. However, the OSINT cell was able to determine how members of the group had attacked in the past and provided situational awareness after major ISIS-K events. The one thing we could do was monitor the information space in Kabul—a wide net to cast. Our primary focus in supporting elements on the ground was monitoring sentiment for potential civil unrest leading to breaches of the perimeter around the airport. Although

When you strip away the genre differences and the technological complexities, all games share four defining traits: a goal, rules, a feedback system, and voluntary participation.<sup>5</sup>

—Jane McGonigal,  
American game designer and author



we looked for indicators and warnings of future attacks, the biggest threat was from an unruly crowd. This consisted of monitoring an array of public feeds from social media and the news.

OSINT was useful in helping limit the effects of selection bias during Operation Allies Refuge. In numerous instances, we had to dispel or qualify sensationalist PAI. The prevalence of people using sensational PAI likely had to do with our reliance on intelligence products. When other intelligence disciplines create reports, a trained analyst vets the reports. When the intelligence community makes an assessment, one generally has confidence in the corresponding report. This in turn creates an odd effect by which some people may treat raw PAI reporting (i.e., news reports and social media posts) with the same confidence as an intelligence report. Compounding this effect is the nature of the internet, which often gives users information comparable to what they have recently seen. A person looking at PAI, whether it is the news or their own social media feed, can easily get a warped perception of people's sentiments, especially in a rapidly developing, emotionally charged event like Operation Allies Refuge. Our OSINT team helped serve as a preventive and corrective measure against biases and echo chambers.



U.S. Air Force photo by ATC Jade Dubiel

U.S. Army Soldiers assigned to the 82<sup>nd</sup> Airborne Division, Pope Army Airfield, NC, receive a brief before heading to board a C-17 Globemaster III at Joint Base Charleston, SC, August 14, 2021. The 82<sup>nd</sup> Soldiers deployed to the Middle East as part of the immediate response force activation to help provide for the safe and secure movement of United States citizens, Special Immigration Visa recipients, and vulnerable Afghan populations from Afghanistan.

## Casting a Wide Net for Collection

While there are instances of finding “that one specific message” indicating a possible threat requiring a decision maker’s action, the reality is most OSINT activities will likely concentrate on monitoring general sentiments to provide general situational awareness. This is in part due to two things: everyone has access to PAI, and large-scale combat operations demand a general approach.

With everyone having access to PAI, people are inclined to do their own “OSINT.” In fact, most people apply OSINT

techniques when they use the internet to learn about a type of product they plan to buy, so it is normal for people to want to go online to find information about current operations. However, as these “non-OSINTers” get information, they naturally want to use it, which can sometimes require an OSINT analyst to do damage control. It is like when a judge tells jurors in a high-profile case not to seek out information about the case while the trial is ongoing, expecting them to avoid the internet and the news, which these days is virtually impossible. Therefore, the OSINT analyst needs to accept that others will unintentionally be doing “OSINT.” OSINT analysts should therefore situate themselves as the vetters of questionable information. Not only does it reduce redundancy, but it also allows the OSINT analyst to become aware of what others within the team are concerned about.

As the Army transitions from counterinsurgency operations to large-scale combat operations, FORSCOM OSINT will do the same. As mentioned earlier, OSINT success stories often involve applying detective work to find specific adversaries. In reality, this sort of occurrence will be rare. We like to think that in large-scale combat operations, enemy troops will commit a vast number of operations security violations that OSINT analysts will find, or that civilians will readily post on social media about those “noisy tank drivers” who just arrived. This is a misguided expectation that comes from applying our experience in counterinsurgency operations to large-scale combat operations.

While instances of a chance post may reveal enemy positions, the reality is that most civilians will be more preoccupied with surviving conflict than using social media to post comments about the arrival of the enemy, and adversaries will not frequently post revealing information. We saw this during Operation Allies Refuge. Initially, there were a substantial number of posts on social media as people amassed to flee the country. The most informative were daytime videos typically posted on social media at night while people rested to prepare for the next day. As the evacuation progressed, social media posts became less frequent. This was presumably because most people tweeting and posting about the operation early on had either evacuated or begun to accept their new conditions in Afghanistan. Additionally, people were reportedly afraid of retaliation if their posts associated them with trying to leave the country.<sup>6</sup>

In large-scale combat operations, we are likely to see a similar pattern. We can mitigate this situation by casting a wide net for collection rather than focusing on finding information about specific individuals. The OSINT analyst can effectively capture new information by monitoring sentiment, reading articles about strategic efforts, and perusing local news to get a picture of what is happening. Elements within an OSINT cell can investigate specifics, but this may not always be fruitful

because information flow can mask relevant PAI. During the 2020 conflict between Armenia and Azerbaijan, government agencies from the two nations restricted internet access. The presence of disinformation campaigns, misinformation, and growing groupthink created an information environment where it was hard for anyone to get an accurate read of the situation.<sup>7</sup> The reliability of any given post on the conflict would thus be suspect.

The reality of large-scale combat operations is that aggregated information from the news and social media will be the most reliable way of driving OSINT collection. Looking at the greater context of streaming information will provide more effective understanding. Much as it was for T.E. Lawrence, OSINT analysts in large-scale combat operations will be doing most of their work analyzing the nature of the reporting rather than the reporting itself.

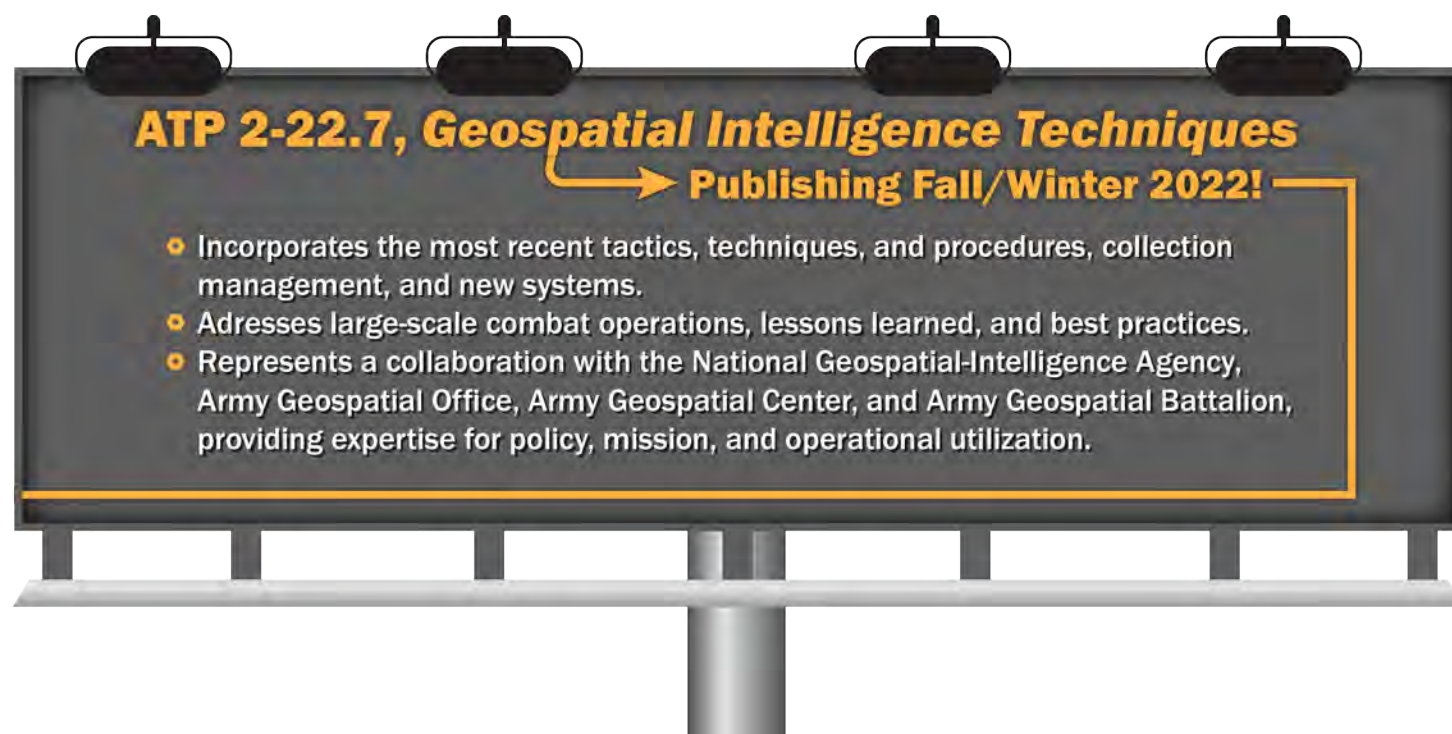
## Conclusion

As the Army shifts from counterinsurgency operations to large-scale combat operations, establishing an OSINT cell at the division level has provided us an opportunity to form an environment that promotes creative research on globally significant matters. Although our team can exploit clear tactical uses of OSINT, we have found that focusing on the big picture first—the strategic-level issues—helps to illuminate what we find in PAI. Coupled with analytic techniques derived from game theory, we have been able to set up a framework for understanding how to conduct OSINT for the immediate response force mission. ✨

## Endnotes

1. *Lawrence of Arabia*, directed by David Lean (1962; London, UK: Horizon Pictures).
2. *Encyclopaedia Britannica Online*, s.v. “game theory,” accessed November 1, 2021, <https://www.britannica.com/science/game-theory>.
3. *Encyclopaedia Britannica Online*, s.v. “The prisoner’s dilemma,” accessed November 1, 2021, <https://www.britannica.com/science/game-theory/The-prisoners-dilemma>.
4. Psychology Wiki, s.v. “Dictator game,” accessed November 3, 2021, [https://psychology.wikia.org/wiki/Dictator\\_game](https://psychology.wikia.org/wiki/Dictator_game).
5. Jane McGonigal, *Reality is Broken: Why Games Make Us Better and How They Can Change the World* (London: Penguin Books, January 20, 2011).
6. Katie Collins, “The Taliban are spinning social media to their advantage, despite sites’ bans,” CNET, August 18, 2021, <https://www.cnet.com/news/the-taliban-thrive-on-social-media-despite-sites-bans/>.
7. Katy Pearce, “While Armenia and Azerbaijan fought over Nagorno-Karabakh, their citizens battled on social media,” *Washington Post*, December 4, 2020, <https://www.washingtonpost.com/politics/2020/12/04/while-armenia-azerbaijan-fought-over-nagorno-karabakh-their-citizens-battled-social-media/>.

SGT Christian Torres joined the Army in 2017 as a geospatial imagery intelligence (GEOINT) analyst. The following year, he was assigned to the 82<sup>nd</sup> Airborne Division G-2 GEOINT cell. In 2021, he moved to the newly formed G-2 open-source intelligence team as part of the indications and warnings cell. He holds a bachelor of arts in philosophy.





By Chief Warrant Officer 2 Christopher D. Hurtig

# PUBLICLY AVAILABLE INFORMATION'S IMPORTANCE TO THE INTELLIGENCE DISCIPLINES

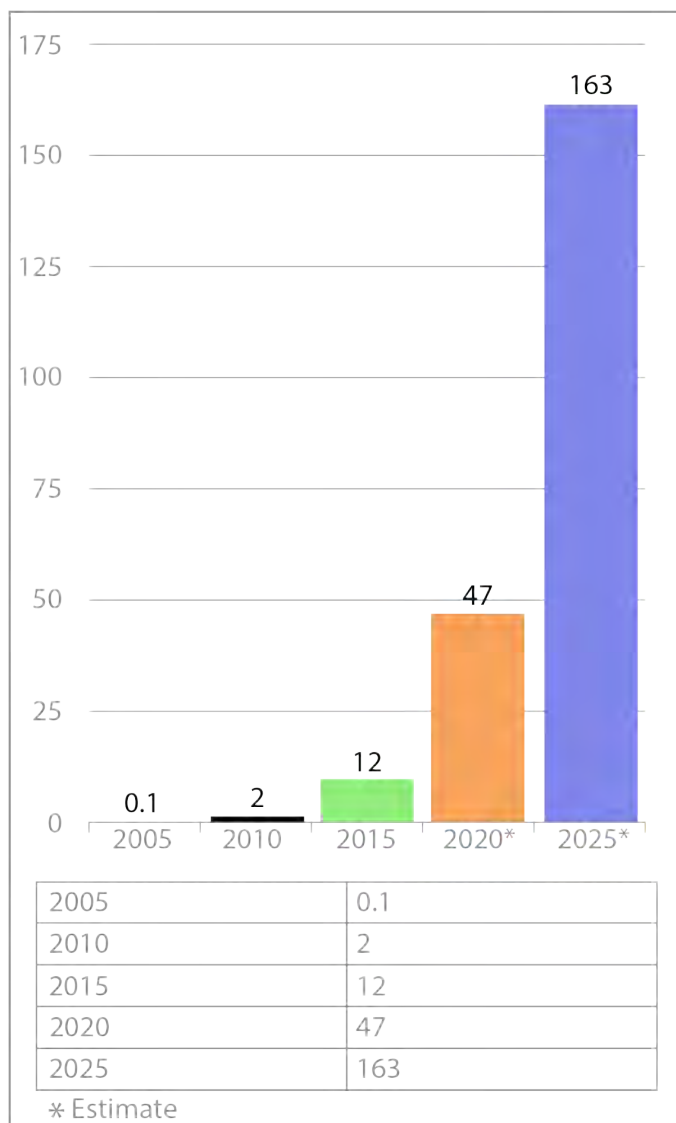
## Introduction

Publicly available information (PAI) is unclassified data that is intelligence-discipline agnostic and plays an increasingly important role in intelligence analysis. The evolution of technology within the last 10 years, the development of the Internet of Things, and advancements in machine learning have led to an explosion of PAI available for analysis by intelligence professionals. Within multidomain operations, incorporating PAI into the intelligence disciplines' products has become crucial. The abundance of PAI and its importance as a source supports the Department of Defense (DoD) intelligence communities' efforts to transition from a manpower-intensive enterprise to one that is automation-intensive, capable of supporting commanders' ability to react quickly to dynamic situations and outmaneuver their enemies.<sup>1</sup>

## PAI's Use in Strategic Competition

Adversaries within strategic competition use a variety of methods below the threshold of war to achieve their objectives. These methods include, but are not limited to, paramilitary activities, military intimidation, economic coercion, and offensive cyberspace operations. In the 21<sup>st</sup> century, data is viewed as a commodity that peer and near-peer adversaries leverage by exporting telecommunication architecture to gain regional and international influence.<sup>2</sup> PAI can provide friendly forces the necessary data points to identify, track, and counter adversarial operations by enriching analysis from traditional sensitive collection. In 2010, 2 zettabytes (1 zettabyte equals a billion terabytes) of data were created and consumed globally; in 2020, that number increased to approximately 47 zettabytes.<sup>3</sup>

PAI is collected and aggregated using methods that provide the greatest level of fidelity required to support multidomain operations. While adversary antiaccess and area denial capabilities may be able to disrupt traditional intelligence, surveillance, and reconnaissance platforms, PAI is pervasive and will continue to be created in areas of interest within all phases of multidomain operations.



Amount of Data Created Worldwide, from 2005 to 2025 in zettabytes<sup>4</sup>

## PAI's Relationship with the Intelligence Disciplines

As society becomes more digitally connected and increasing numbers of data points are collected, aggregated, and stored, tracking the evolving sources and developing new

methods of collection become more important. PAI, either purchased or collected, has overtaken the intelligence collection disciplines.

Should we think of commercial imagery as open-source intelligence (OSINT) or imagery intelligence? Should we view technical data derived from PAI as measurement and signature intelligence or signals intelligence (SIGINT)? Alternatively, should we view a post on social media platforms as human intelligence or SIGINT? The blurring of lines between traditional and emerging collection methods requires intelligence professionals to incorporate PAI and the intelligence collection to extrapolate relevant information for commanders, particularly given unclear lines of the strategic competition’s gray zone.

PAI’s Use in Open-Source Intelligence

The broad nature of OSINT and dependence on PAI can cause confusion between the intelligence discipline and supporting data. DoD 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, etc.”<sup>5</sup> Historically, PAI was the foundation of OSINT in the form of news articles and journals; now, resources are primarily social media and the internet. We view data as a commodity that people produce worldwide because they share information about their location, activities, hobbies, habits, friends, and family. Largely, people have relinquished control of their data, using “free” applications that then sell the aggregated data—meaning it becomes available for public consumption at the unclassified level.

OSINT uses PAI to provide timely diverse data spanning the gamut of social media, federal and nongovernment agencies, and technical resources. PAI spans the diplomatic, information, military, economic, financial, intelligence, and law enforcement spectrum, also known as the DIME–FIL spectrum, and may help satisfy OSINT requirements. Metrics can identify the level of engagement, response rate, and reach of an individual or a topic. This information, layered with demographic data, may identify populations and themes to support

information operations. A more tailored example would be the analysis of an official social media account. PAI can provide exact quotes from an individual or entity regarding specific topics. Over time, changes in rhetoric may indicate changes in stance on a particular topic or a measure of response to specific actions or activities.<sup>6</sup>

PAI’s Use in Geospatial Intelligence

Commercial geospatial imagery allows analysts and commanders the ability to—

- ◆ Share intelligence.
- ◆ Increase the frequency of collection.
- ◆ Enable the National Reconnaissance Office’s (NRO’s) overhead systems collection of more sensitive targets.

Within the Five Eyes (FVEY) community, a cross-domain solution creates passage for commercial imagery through to classified networks supporting information sharing. During operations, partners and allies will likely not have access to the same networks as our FVEY partners, requiring the sharing of imagery and analysis on networks below impact level (IL) 6 (DoD classified information up to SECRET). Depending on which partners the United States is working with, this could be as low as IL4 (DoD-controlled unclassified information) or IL2 (DoD information that has been approved for public release [low confidentiality, moderate integrity]). (Note: The information IL numbers are determined by the combination of the sensitivity of the information to be stored and/or processed in the cloud and the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information.<sup>7</sup>)

Current foreign disclosure processes for sharing overhead systems collection are incompatible with the operational tempo of multidomain operations. Unclassified imagery can support information operations by providing alternative imagery to targets of interest. Commercial imagery, particularly in support of targeting, shared in an automated fashion can enable joint effects by mitigating cross-domain solution and foreign disclosure requirements.

Satellite Operator	Proposed Satellites	Resolution
Planet	~150	0.72m–5m
Spaceflight Industries	60	1m
Satellologic	300	1m
Hera Systems	48	.5m
UrtheCast	16	0.75m–22m
Capella Space	30	1–30m SAR
Canon	>100	1m
DigitalGlobe	6	0.3m

Planned Proliferated Earth Observation Constellations (as of 2018)<sup>8</sup>

The asymmetric nature of strategic competition means that throughout shaping activities and into large-scale combat operations, imagery requirements and the number of named areas of interest to support commanders are immense. Since the mid-1990s, commercial satellite imagery quality and quantity have continued to improve at a swift pace because of the falling cost of space launches and increased demand from both government and private industry.

Commercial imagery resolution has matured to a point where it can support multidiscipline analytical requirements. The regularity of commercial imagery collection now provides temporal data to enable change detection analysis at the unclassified level. This can be taken one step further using object recognition software. Automating change detection and layering object recognition onto unclassified commercial imagery alerts, which can be passed automatically to allies and partners, can provide commanders additional decision space rather than waiting for an NRO overhead system to provide the requisite intelligence.

The proliferation of commercial imagery also eases the burden on NRO systems collection. Not every target requires the level of traditional collection that sensitive assets provide. Deconflicting collection assets will allow national assets to remain focused on priority targets while commercial assets support secondary and tertiary targets.

### PAI's Use in Signals Intelligence and Signature Management

The evolution of the Internet of Things, combined with the implementation of the 5<sup>th</sup> generation mobile network (5G) and development of “smart cities,” provides opportunities for collectors to use PAI to support SIGINT activities and friendly force signature management. Modern societies’ use of electronic wearables, smartphones, and other connected devices means a constant stream of data is collected, stored, aggregated, and processed. Employment of 5G technology increases the ability to collect data through ubiquitous technical surveillance techniques. Given that PAI is created worldwide, PAI can support strategic competition analysis and associated lines of effort by identifying patterns, trends, and indicators of adversary global priorities. While any one data set may not provide salient information, the fusion of data sets provides geolocation, facial recognition, device metadata, and personal data. Government or civilian corporations can use a variety of data mining techniques to support their specific information requirements.

Targets of interest, identified by cross-cueing intelligence and PAI collection capabilities during competition, will provide a more complete picture of a target and the digital footprint for further development as operations transition into crisis and armed conflict in a contested environment. Similarly, peer and near-peer adversaries are collecting the digital footprint of our Service members, sources, allies, and partners for their own targeting priorities.

**First-Party Tracking:** Websites allow data aggregation of the end users and catalog information directly entered by the user.

**Third-Party Tracking:** Uses indirect means to monitor and gather internet user information via an intermediary. Can lead to “massive aggregation of personal information.”

**Cookie-Matching Technology:** Enables aggregators to share cookies or a collection of cookies, allowing for a more holistic look at an end user’s online habits.

**Device Fingerprinting:** Each device’s unique signature, built on a string of data, paired with a user’s IP address can deliver a level of detail equal to cookies or enable the “regeneration” of deleted cookies.

Data Mining Techniques<sup>9</sup>



Where 5G Technology Has Been Deployed<sup>10</sup>

As PAI and its ability to be aggregated with other data sets become more robust, signature management training will become increasingly important. The ability to manage a digital footprint will also become more important because the absence of PAI is just as conspicuous and detrimental to operations security as an unmanaged digital footprint.

### PAI's Use in Human Intelligence and Counterintelligence

Intelligence professionals can use PAI to support source validation operations, particularly in environments where access to more sensitive collection information may be restricted. The pervasive and persistent nature of PAI means




potential sources are providing historical reference data that intelligence professionals can use to identify sources' access and placement and verify relationships. PAI also provides the ability to identify sources' patterns of life and subsequently potentially anomalous activity.

Peer and near-peer adversaries have similar capabilities, potentially requiring sources to learn digital tradecraft to mitigate possible identification. Within China's smart cities, the fusion of online applications and offline data sets and real-world internet services, such as ride-sharing, meal delivery, or peer-to-peer financial transfers, has created an unprecedented level of fidelity regarding a person's pattern of life, associates, and activity.<sup>11</sup> The ability to create a mask for operationally relevant digital signatures among false signatures will be key to validating and ensuring the security of military personnel, sources, and allies.

## Conclusion

As the world becomes more and more digitally connected, PAI will continue to be increasingly important to military operations and the intelligence community. During multidomain operations, PAI from commercial imagery, ubiquitous technical surveillance, and other commercially available information sources will supplement traditional intelligence, surveillance, and reconnaissance collection platforms within antiaccess and area denial environments. Smart cities, at home and abroad, will become sources of PAI, which can present both opportunities and vulnerabilities during all phases of military operations. PAI volume and variety will continue to evolve in the future. Our ability to store, parse, manipulate, and aggregate PAI with traditional intelligence collection must increase.

Projections indicate approximately 163 zettabytes of data will be created annually by 2025.<sup>12</sup> Because of the way PAI is currently incorporated into analysis through OSINT tools, units and commands without the ability to support managed attribution solutions do not have access to the same level of PAI.<sup>13</sup> During multidomain operations, every unit will require the ability to augment its organic collection capabilities with PAI. To support this requirement, policy changes and an expansion of current analytical tools associated with PAI need to occur.

Emerging technologies, the Internet of Things, and processing capacity will provide new and unique ways of merging PAI with traditional collection. Data science and machine learning/artificial intelligence capabilities will be necessary to aggregate and analyze previously nontraditional, previously uncorrelated data sets. Similar to how the advent of photography and electronic signatures ushered in new intelligence disciplines, PAI will require the intelligence community to make a similar evolution. Peer and near-peer adversaries within the strategic competition space have ensured the full incorporation of PAI into intelligence disciplines is essential for maintaining information dominance. 

## Endnotes

1. Nishawn S. Smagh, *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition* (Washington, DC: Congressional Research Service, June 4, 2020).
2. Mason P. Jones and Erica L. McCaslin, "Special Operations in a 5G World: Can We Still Hide in the Shadows?" (master's thesis, Naval Postgraduate School, Monterey, CA, 2020), 21–22, [https://calhoun.nps.edu/bitstream/handle/10945/65560/20Jun\\_Jones\\_McCaslin.pdf?sequence=1&isAllowed=y](https://calhoun.nps.edu/bitstream/handle/10945/65560/20Jun_Jones_McCaslin.pdf?sequence=1&isAllowed=y).
3. "Information created globally 2005–2025," StatInvestor, accessed 30 November 2021, <https://statinvestor.com/data/35219/data-created-worldwide/>.
4. Ibid.
5. Department of Defense (DoD), DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC, August 8, 2016), 53.
6. Jones and McCaslin, "Special Operations in a 5G World."
7. Defense Information Systems Agency, *Cloud Computing Security Requirements Guide* (Washington, DC, May 2018), 9–10.
8. Matthew A. Hallex and Travis S. Cottom, "Proliferated Commercial Satellite Constellations Implications for National Security," *Joint Force Quarterly* 97 (2<sup>nd</sup> Quarter 2020): 22, [https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97\\_20-29\\_Hallex-Cottom.pdf?ver=2020-03-31-130614-940](https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_20-29_Hallex-Cottom.pdf?ver=2020-03-31-130614-940).
9. Jones and McCaslin, "Special Operations in a 5G World," 21–22.
10. "Where 5g Technology Has Been Deployed," Statista, accessed 6 December 2021, <https://www.statista.com/chart/23194/5g-networks-deployment-world-map/>.
11. Jones and McCaslin, "Special Operations in a 5G World."
12. "Information created globally 2005–2025."
13. DoD, DoD Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)* (Washington, DC, June 11, 2019). Change 1 was issued on August 20, 2020.

CW2 Christopher Hurtig is assigned to the SOJ22 as the enabler chief within Special Operations Command, Pacific, Camp H.M. Smith, HI. His past assignments include serving with Task Force [observe, detect, identify, and neutralize] ODIN; the 532<sup>nd</sup> Military Intelligence Brigade, Camp Humphrey, South Korea; and the 1<sup>st</sup> Battalion, 503<sup>rd</sup> Infantry Regiment, 173<sup>rd</sup> Airborne Brigade Combat Team. He then served as the South Asia noncommissioned officer in charge within the Special Operations Command Pacific SOJ2. He was accepted into the Warrant Officer Program, and upon completion of the Warrant Officer Basic Course, he became the fusion chief at 3<sup>rd</sup> Brigade Combat Team, 82<sup>nd</sup> Airborne Division. CW2 Hurtig has deployed to Iraq and to Afghanistan where he assumed the role of senior intelligence analyst for the Train Advise and Assist Command-South mission. CW2 Hurtig holds a bachelor of arts in intelligence studies from American Military University.

# Modular J2X Staff Officer Course

(Distance Learning)  
by Mr. David Summers



During fiscal year (FY) 2021, the Human Intelligence Training–Joint Center of Excellence (HT–JCOE) fielded the J2X Staff Officer Course (Distance Learning [DL]). The course trains senior Department of Defense intelligence professionals to manage and facilitate counterintelligence (CI) and human intelligence (HUMINT) activities. The course prepares graduates to fill staff officer positions in combatant commands, sub-unified commands, and joint task forces. It is an asynchronous, instructor-mediated, college-style, collaborative distance learning course, conducted on the Blackboard Learning Management System (LMS) on the SECRET Internet Protocol Router Network (SIPRNET). The term *asynchronous* means that students and instructors are not online at the same time.

Beginning in January 2022, HT–JCOE transformed the distance learning course into a modular course consisting of five modules. Modules A through D last 2 weeks (10 training days), and module E lasts 1 week (5 training days).

- ◆ Module A—Manage CI Activities.
- ◆ Module B—Manage HUMINT Activities.
- ◆ Module C—Manage Operations Support Activities.
- ◆ Module D—Manage J2X Activities.
- ◆ Module E—Capstone Exercise and Summative Exam.

The modular format provides students with maximum flexibility and many options. A student can enroll in a class and take all modules in sequence. Alternatively, they can opt to do a single relevant module. For example, if a student is going to an assignment at a combatant command J2X HUMINT Operations Branch, they can complete module B only. A student might start a class and get through modules A and B but then discover that their unit’s mission requirements preclude them from continuing to the next module. No problem. After

notifying their primary instructor and Service training executor, the student can re-enroll in the next scheduled class for modules C, D, and E. Students can theoretically spread out their efforts and do one module per class over time. They have 18 months to complete all modules but must finish modules A through D before enrolling in module E. Upon completion of all modules, they graduate and receive an academic evaluation report and a graduation certificate/diploma. In FY 2022, HT–JCOE is offering four modular J2X Staff Officer Course (DL) classes, each with the five modules (A through E).

HT–JCOE has a responsibility to account for all students attending its courses, whether in residence or in distance learning. Students must check in with their assigned instructors on the Blackboard LMS at the beginning of every training day. There is a daily schedule of module activities, and the schedule allocates time for students to accomplish all assignments. Students are expected to commit between 20 and 25 hours per week (4 to 5 hours per training day) to the course. Given the challenges associated with participating in distance learning on the SIPRNET (e.g., accessibility, connectivity, conflicting operational requirements, and student and/or family personal issues), the course cadre are flexible and, if necessary, will work with students on an individual basis to help them meet HT–JCOE’s accountability requirements and accomplish the course within the overall module timeframe. ✨

*Mr. David Summers is the Director of the J2X Staff Officer Course (Distance Learning) at the Human Intelligence Training–Joint Center of Excellence (HT–JCOE), Fort Huachuca, AZ. He has served as an Army civilian for 14 years, working initially as a doctrine writer at the U.S. Army Intelligence Center of Excellence and later as an instructor at HT–JCOE. Mr. Summers retired after a 26-year career as a U.S. Army military intelligence officer. From 2003 to 2004, he served as the CJ2X, Combined Joint Task Force 7, in Iraq.*

After serving with the Army for 3 years, I sought to expand my understanding of how Army senior leaders make decisions. Toward that end, I applied to the Army's Enterprise Talent Management–Temporary Duty program. In November 2021, I was selected to serve as a special project officer supporting an intelligence functional community operational planning team.

The Senior Enterprise Talent Management and the Enterprise Talent Management are civilian leader programs for GS-14/15 and GS-12/13 employees, respectively. These programs prepare participants for positions of greater responsibility in the Department of Army through advanced senior-level educational and experiential learning opportunities. The Civilian Senior Leader Management Office, Assistant Secretary of the Army (Manpower and Reserve Affairs), collaborates with senior executives to ensure applicants and projects are compatible before assignment.

Ms. Katherine Coviello, a Defense Intelligence Senior Level (DISL) executive and the intelligence functional representative for staff management, started the intelligence functional community operational planning team at the direction of the Assistant Deputy Chief of Staff, Intelligence. The goals of the operational planning team are to standardize the functional discipline, identify specific skillsets and training, and establish guidelines for personnel in staff management billets. The Army Civilian Career Management Activity and Enterprise Talent Management program managers selected an intelligence specialist to assist with this operational planning team. This provided the specialized experience necessary to understand the various intelligence disciplines and the way they integrate to support the warfighter as a staff manager.


The intelligence functional community, formerly administratively designated Career Program 35–Intelligence and Security, focuses on intelligence, security, and intelligence support roles. The intelligence functional community concept stemmed from the *The Army People Strategy*<sup>1</sup> and *Army People Strategy: Civilian Implementation Plan*,<sup>2</sup> which directed the expansion of talent management capabilities into all phases of the human capital lifecycle. Intelligence staff managers participate in the planning, integration, and execution of intelligence activities, intelligence-supported activities, and military intelligence operations to enhance decision making for Army and joint staff, from brigade to combatant command to Service component commands.

Unlike other functional specialties (e.g., counterintelligence, human intelligence, and geospatial intelligence), staff

management billets are discipline-agnostic and exist in all intelligence disciplines. Additionally, the staff management functional discipline lacked a career progression map, and unlike more established disciplines, there is no one-stop-shop training source for staff managers. Currently, staff managers learn primarily via on-the-job training.

Selecting the appropriate courses to serve as a solid foundation for all staff managers, regardless of intelligence discipline, while at the same time providing flexibility for nontraditional missions was a challenge for the operational planning team. The solution to this problem was with the operational planning team stakeholders who recommended courses pertaining to functional training, career broadening, and leadership that served as the basis for a career map. This map will assist staff managers from GG-11 through Defense Intelligence Senior Executive Service and DISL.

The Enterprise Talent Management–Temporary Duty program, is not onerous. Senior civilians at the U.S. Army Technical Support Squadron and the 704<sup>th</sup> Military Intelligence Brigade endorsed and facilitated my application. Once “onboard,” I interacted daily with DISL executives, who provided mentorship, guidance, and advice. Moreover, I was able to tap into senior civilians from across the Department of Defense intelligence enterprise. Similarly, biweekly coaching sessions with an Army career coach helped me better understand myself and focus my career goals. The combination of DISL mentorship, insight and clarity about Army personnel management, and coaching sessions ensured the success of the staff management operational planning team and built a solid foundation for my continued professional and personal development. My Enterprise Talent Management–Temporary Duty assignment, coupled with DISL mentorship and guidance, exemplified the objective of the Enterprise Talent Management program as a whole—career development! In 90 days, I learned more about how the Army functions than in previous assignments.

Intelligence staff management personnel will soon have a career map for a more professional functional discipline. Likewise, Army intelligence leaders will have a cadre of trained personnel capable of managing the intelligence workforce. The future of the intelligence functional community looks bright. 

## Endnotes

1. Department of the Army, *The Army People Strategy* (October 2019), [https://www.army.mil/e2/downloads/rv7/the\\_army\\_people\\_strategy\\_2019\\_10\\_11\\_signed\\_final.pdf](https://www.army.mil/e2/downloads/rv7/the_army_people_strategy_2019_10_11_signed_final.pdf).
2. Department of the Army, *Army People Strategy: Civilian Implementation Plan* (2020), [https://home.army.mil/jbmhh/application/files/6115/9112/8485/Army\\_People\\_Strategy\\_Civilian\\_Implementation\\_Plan\\_-\\_14\\_May\\_20.pdf](https://home.army.mil/jbmhh/application/files/6115/9112/8485/Army_People_Strategy_Civilian_Implementation_Plan_-_14_May_20.pdf)

Mr. Sergio Sanchez is the Deputy Human Intelligence Operations Cell Chief, U.S. Army Technical Support Squadron, Fort Meade, MD.





# Contact & Article

## Submission Information



*This is your professional bulletin. We need your support by writing and submitting articles for publication.*

**When writing an article, select a topic relevant to Army MI professionals.**

Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the intelligence community. Articles about current operations, TTPs, and equipment and training are always welcome as are lessons learned, historical perspectives, problems and solutions, and short “quick tips” on better employment of equipment and personnel. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

**When submitting articles to MIPB, please consider the following:**

- ◆ Feature articles, in most cases, should be between 1,000 and 3,000 words, double-spaced with normal margins without embedded graphics.
- ◆ We cannot guarantee we will publish all submitted articles.
- ◆ Please do not send overly large and complicated or small print graphics/PowerPoint slides. What looks good as a PowerPoint presentation doesn't always translate well to an 8 1/2" x 11" article format.
- ◆ Please do not include any personally identifiable information (PII) in your article or biography.
- ◆ Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- ◆ All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

**What we need from you:**

- ◆ Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.
- ◆ A cover letter/email with your work or home email, telephone number, and a comment stating your desire to have your article published.
- ◆ **(Outside of USAICoE)** A release signed by your unit's information security officer stating that your article and any accompanying graphics and photos are unclassified, not sensitive, and releasable in the public domain. A sample security release memorandum is available from the MIPB Staff. Contact us at the email address at the bottom of the page.
- ◆ **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297) for information on how to get a security release approved for your article. A critical part of the process is providing all of the source material for the article to the information security reviewer in order to get approval of the release.
- ◆ Article in Microsoft Word; do not use special document templates.
- ◆ Pictures, graphics, crests, or logos relevant to your topic. Include complete captions (the 5 Ws), and photographer credits. Please do not send copyrighted images. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg.** Photos must be at least 300 dpi. If relevant, note where graphics and photos should appear in the article. PowerPoint (**not in .tif/.jpg format**) is acceptable for graphs, figures, etc.
- ◆ The full name of each author in the byline and a short biography for each. Biographies should include authors' current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications.

We will edit the articles and put them in a style and format appropriate for MIPB. From time to time, we may contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

Submit articles and graphics to [usarmy.huachuca.icoe.mbx](mailto:usarmy.huachuca.icoe.mbx). [mipb@army.mil](mailto:mipb@army.mil). For any questions, email us at the above address or call 520-533-7836/DSN 821-7836.

**MIPB (ATZS-DST-B)**  
**Directorate of Training and Doctrine**  
**USAICoE**  
**550 Cibique St.**  
**Fort Huachuca, AZ 85613-7017**



**Headquarters, Department of the Army.**  
**This publication is approved for public release.**  
**Distribution unlimited.**

**PIN: 212787-000**