By Chief Warrant Officer 2 Christopher D. Hurtig

PUBLICLY AVAILABLE INFORMATION'S IMPORTANCE TO THE INTELLIGENCE DISCIPLINES

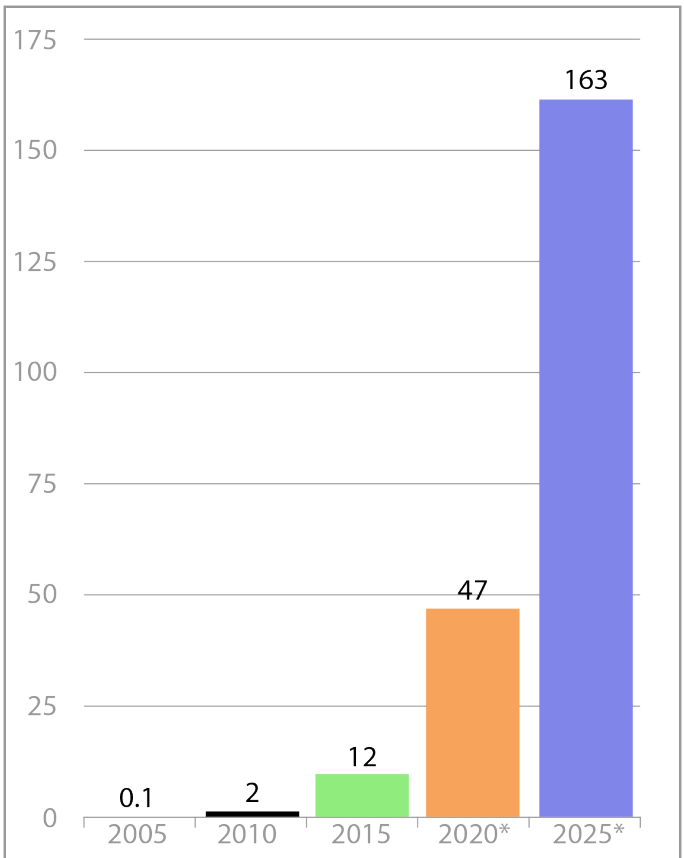
Introduction

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.[1]

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 21st century, data is viewed as a commodity that peer and near-peer adversaries leverage by exporting telecommunication architecture to gain regional and international influence.[2] 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.[3]

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.



2005	0.1
2010	2
2015	12
2020	47
2025	163

* Estimate

Amount of Data Created Worldwide, from 2005 to 2025 in zettabytes[4]

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."[5] 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.[6]

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.[7])

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
Satellogic	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)[8]

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 5th 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.

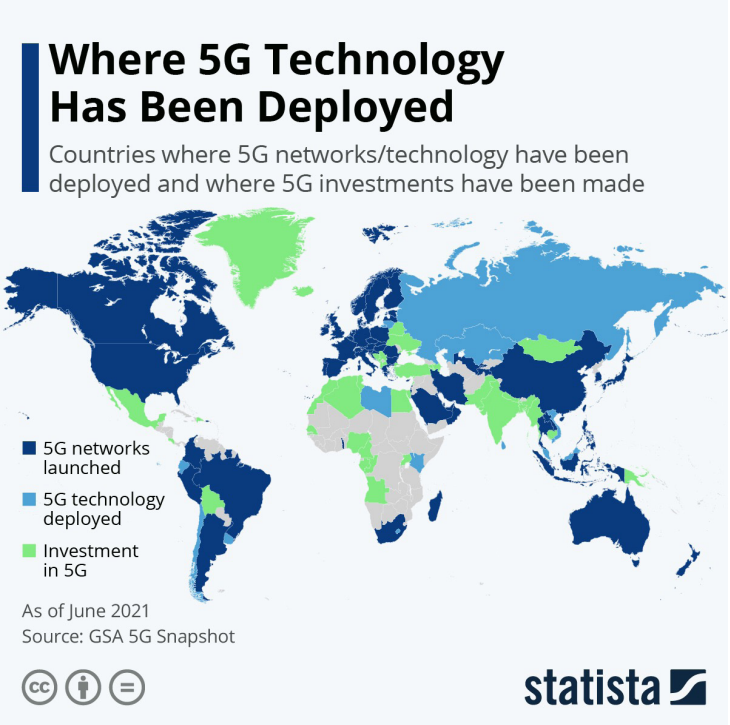
First-Party Tracking: Websites allow data aggregation of the end users and catalog information directly entered by the user.

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[9]



Where 5G Technology Has Been Deployed[10]

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.[11] 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.[12] 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.[13] 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.

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 (2nd 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.

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 532nd Military Intelligence Brigade, Camp Humphrey, South Korea; and the 1st Battalion, 503rd Infantry Regiment, 173rd 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 3rd Brigade Combat Team, 82nd 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.