Issues in Information Systems
Volume 26, Issue 3, pp. 61-74, 2025

DOI: https://doi.org/10.48009/3_iis_2025_2025_105

Rebranding second-generation open-source intelligence: "It's not your father's OSINT"

Fred Hoffman, *Mercyhurst University, fhoffman@mercyhurst.edu*
Brian Fuller, *Mercyhurst University, bfuller@mercyhurst.edu*

Abstract

For decades, first-generation open-source intelligence (OSINT) was exclusively performed by intelligence organizations and largely consisted of the translation and analysis of foreign-language radio, TV broadcasts, newspapers, and other publicly available documents by cleared native language speakers from other countries. Since the 1990s, due to the impact of Information Age technologies, OSINT has steadily increased in importance. The multiple technological advances driving OSINT's ongoing evolution, which led some scholars and intelligence professionals to refer to its current state as "second-generation OSINT," have impacted which skills OSINT practitioners require, what OSINT tradecraft should be employed, what OSINT can and should collect, how that research and collection is best performed, how source and data validation is performed, how technical and topical risk mitigation is conducted, and how OSINT analysis is conducted. The ever-increasing and changing big data environment has also had a significant impact on the changes in OSINT practices. Thanks to these tectonic shifts, second-generation OSINT hardly resembles what it had originally been. Just like most intelligence disciplines, OSINT's rapid, ongoing evolution necessitates rebranding because OSINT practitioners, managers, and customers must all comprehensively understand and appreciate what OSINT can do, how it can be successfully integrated with other intelligence collection disciplines, and what its ethical, legal, and operational limitations are.

Keywords: open-source intelligence, OSINT, intelligence community, Open Source Executive, artificial intelligence

Introduction

In its inaugural OSINT strategy document, the Office of the Director of National Intelligence (ODNI) described open-source intelligence, or OSINT, as "intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps" (IC OSINT Strategy, 2024, p. 5). The purpose of this article was to examine how and why OSINT has expanded, proliferated, and evolved into what is now a recognized intelligence collection discipline that contributes considerably to answering public and private sector client intelligence requirements, yet differs considerably from what it had been during the Cold War (1947-1991). While many different government organizations and private sector firms and individuals now engage in OSINT, there is a lack of consensus on how OSINT can and should be conducted, OSINT security threats, OSINT tradecraft and threat mitigation, and how OSINT should be integrated with intelligence acquired via other security disciplines (Hughes, 2022). In advocating for rebranding OSINT, the authors make the case for public and private sector OSINT practitioners, customers, and other OSINT stakeholders to more comprehensively understand, resource, and manage open-source intelligence collection.

PAI and CAI

Publicly available information, or PAI, is information that is accessible in the public domain (Vogel, 2024). PAI can be gathered from such a wide array of sources as websites, databases, printed documents, public speeches, television broadcasts, and social media (Varzhanskyi, 2024). PAI also encompasses information identified in table 1, below:

Table 1. Types of publicly available information. Source: Author-generated.

Types of Publicly Available Information
Has been published or broadcast for public consumption
Is available upon request to the public
Is accessible to the public online
Is available to the public by subscription or purchase
Can be seen or heard by any casual observer
Is made available at a meeting open to the public
Is obtained by visiting any place or attending any event that is open to the public

Another commonly heard OSINT acronym is CAI, which stands for commercially available information, which can be derived from company web sites, trade shows, industry-specific publications, and a variety of other sources (Usher, 2024). CAI is any information [data] that is of a type made available or obtainable and sold, leased, or licensed to the general public or to non-governmental entities for purposes other than governmental purposes (Data Management, 2022). PAI and CAI become OSINT when they are "processed into actionable intelligence and distributed to the relevant parties" (Browne, 2024). PAI and CAI differ from proprietary information, which "is sold exclusively to the government or access is gained through government regulation" (OSINT Foundation, 2025).

Why does OSINT need rebranding?

OSINT requires rebranding because today's OSINT practitioners, managers, and customers are no longer just government consumers. Intelligence practitioners, managers, and decision-makers within the private sector, law enforcement, and non-governmental organizations (NGO) must all adequately comprehend and appreciate how OSINT can enhance their operations, how it can safely take advantage of the "Big Data" environment, how it can be successfully integrated with other intelligence collection disciplines and resources, what its risks and limitations might be, and how it can influence decision-makers needs. OSINT's rapid, ongoing evolution and expansion beyond the IC (and, indeed, beyond U.S. shores) necessitates serious discussion among intelligence professionals on such topics as how OSINT should be performed, where it should reside within the IC (both government and private sector), what are the ethical and legal uses of OSINT, and how OSINT could be most effectively integrated with other existing collection disciplines or capabilities. In short: Today's OSINT needs rebranding.

The consequences of poor rebranding

As any Marketing 101 student can tell you, how your organization chooses to present something to one or more target audiences really matters. This truism is amply illustrated by the flawed effort to rebrand the U.S. car manufacturer Oldsmobile in the late 1980s. Founded by Ransom E. Olds in 1897, Oldsmobile quickly became very popular, introducing the first mass-production assembly line years before Henry Ford, offering the first mass-produced car with an automatic transmission in 1938, and introducing the first air bags in their cars in 1974 (Meagher, 2024). Unfortunately, starting in the late 1970s, Oldsmobile, which

over decades had built a "reputation for innovation and uniqueness," gradually devolved into a bland, Chevy-powered manufacturer largely indistinguishable from other GM brands (Meagher, 2024). In 1988, concerned Oldsmobile executives attempted to boost sagging sales with an ad campaign meant to "shake the image that it built boring cars for sleepy seniors" by telling prospective buyers, "We're not your father's Oldsmobile" (Hunting, 2022). New Oldsmobile TV commercials depicted celebrities like William Shatner and Ringo Starr being chauffeured around by their adult children (Schreiber, 2021). Unfortunately, the ad campaign that sought to rebrand Oldsmobile by enticing younger drivers not only confused its intended target audience but ultimately proved counterproductive, turning off both younger and older drivers alike: In 1989, Oldsmobile sales proved to be 15 percent lower than the year before (Los Angeles Times, 1990). By 2000, General Motors executives decided they would terminate the brand, and the last Oldsmobile rolled off the assembly line in 2004 (History of Oldsmobile, 2025).

How (and why) has OSINT evolved in recent years

The technology-driven, transformative changes that have taken place in OSINT in the 21st century have been so impactful and profound that the authors of a 2018 RAND report suggested that today's open-source intelligence "should be seen as a second generation of OSINT" (Williams and Blum, 2018, p. ix). The generational distinctions between Cold War-era OSINT and the OSINT of today extend to such things as (1) who is conducting OSINT; (2) what OSINT can target; (3) what tools, techniques, and tradecraft are used in OSINT; and (4) how the acquired public information is aggregated, analyzed, and delivered to clients; and implications of the (5) veracity, volume, variety, velocity of big data (Usher, 2024).

First generation OSINT

Prior to the Information Age, OSINT primarily involved "translations of foreign press or insights from grey literature" (Harding, 2024). First generation OSINT, or, "your father's OSINT," was largely based on the exploitation of documents and other printed media and, later, radio and television broadcasts (Williams and Blum, 2018). Although the first recorded use of the term open-source intelligence, and the acronym OSINT, appeared in a 1990 article by Robert Steele, OSINT's history actually goes back much further (Block, 2024). After examining three case studies (World War I-era Germany and the Netherlands, and the American Civil War), Block (2024) concluded that "methodical and structured practices aimed at the collection and exploitation of information from open sources to fulfil intelligence requirements existed decades before the establishment of the BBC Monitoring Service and the FBMS (Foreign Broadcast Monitoring Service)" (p. 108). Whereas OSINT is frequently said to have begun in the U.S. with the FBMS in 1941, its use in the U.S. actually dates at least as far back as to the American Civil War, where information gleaned from published newspapers "was equally exploited by both sides" (Block, 2024, p. 100). First generation OSINT sources can be properly labelled as "Traditional Media" or the "Pre-social Media" resources and data.

Second generation OSINT

The two Information Age technological innovations that first brought about the "second generation of OSINT" (Williams & Blum, 2018, p. ix) were the internet and social media. Thanks to those two technological developments, OSINT can now "be collected from multiple online sources, including social media, search engines, websites, online forums, company directories and online databases" (Browne et al., 2024, p. 2912). Since then, additional technologies like big data, cloud computing, artificial intelligence, and the proliferation of specialized software applications have further transformed the nature of OSINT (Brown et al., 2024; Ganguly, 2022). In addition to such traditional first generation OSINT targets as radio, newspapers, television, public documents, and publicly-made speeches and statements, second generation OSINT is now able to target government and commercial websites, social media platforms, online databases and datasets, academic repositories, the dark web, the deep web, the domain name system, online fora, and application programming interfaces, or API (Browne, 2024; Kovaci & Iacob, 2024).

Methodology

In researching this paper, the authors used qualitative research methodologies that included: (1) a selective review of the available literature on OSINT, (2) interviews with OSINT subject matter experts, and (3) experience-based observations by the co-authors, who between them have half a century of direct experience with both first- and second-generation OSINT. The review of the literature was focused on identifying the impacts that Information Age technology has had on OSINT collection and analysis, and on the challenges that arose due to that transformation. Some of the most impactful impacts and challenges are identified below:

OSINT's expanded importance within the U.S. intelligence community
Few would contest the assertion that OSINT has significantly grown in importance within the U.S. intelligence community: During the Cold War, only around 20% of U.S. intelligence on the Soviet Union came from open sources; today, that percentage has increased to 80 – 90% (Vogel, 2024). In 1994, CIA established the Community Open Source Program Office, or COSPRO, while recognition of the growing value of OSINT resulted in the Director of National Intelligence designating OSINT as its own intelligence collection discipline in 2006, establishment of the Open Source Center (OSC) in 2005, OSC's redesignation as the Open Source Enterprise (OSE) in 2015, and issuance of the Intelligence Community's (IC) first-ever OSINT Strategy in 2024 (Harding, 2024; Vogel, 2024). As Juliane Gallina, CIA's Deputy Director for Digital Innovation (DDI), observed, "It is important to remember that CIA is not only a HUMINT-focused organization, but we also serve as the functional manager for OSINT for the intelligence community" (Host, 2025). Despite these developments, Usher (2024) concluded, "The amount of CAI/PAI is exploding, and the IC is not keeping pace to make proper use of it" (p. 24). In part, he asserted, this was because IC officers face "financial, security, and bureaucratic obstacles" to obtaining OSINT, and even when they do, they "often lack the data management and OSINT tradecraft skills or access to cutting-edge analytic tools to effectively utilize the data" (Usher, 2024, p. 25). Counterintuitively, and despite the growth of OSINT's importance and current standing as an independent intelligence collection discipline, "intelligence organizations seem reluctant to adopt OSINT" (Rietjens, 2025, p. 30). At the same time, there is a growing awareness within the government for the need for increased OSINT operations, as those "subjects" or "targets of interest" are not operating on classified government networks, but on the open, deep, and dark web (Langrock & Smilyanets, 2024).

Intelligence outsourcing
Usher (2024) noted how "The private sector has found tools and strategies to absorb and analyze new data and to push out products at speed" (p. 24). The proliferation of OSINT practices beyond the IC is evidenced in the manner, and by the extent to which, private sector intelligence providers responded to Russia's 2022 invasion of Ukraine. "When Russia invaded Ukraine in 2022, some of the timeliest intelligence was provided not by intelligence agencies, but by private actors" (Tucker & Robson-Morrow, 2025, p. 1). In addition to using OSINT to accurately predict that Russia was, indeed, going to invade, private OSINT practitioners also made other significant contributions:

Intelligence teams working within Western companies "accurately assessed the possibility of an invasion and helped evacuate employees, draw down business operations, and mitigate risks to supply chains" (Tucker & Robson-Morrow, 2025, p. 1). Today, private sector security firms like Control Risks, Sibylline, Emergent Risk International, Dragonfy, Global Guardian, S-RM, Max Security, and Recorded Future engage in OSINT to "provide intelligence products and services that range from comprehensive geopolitical and security consulting to niche service provision such as kidnap and ransom response training or analysis of offshore maritime piracy in the Gulf of Guinea" (Tucker & Robson-Morrow, 2025, p. 1).

Expanded skills required by OSINT professionals

Forty years ago, drawing upon native language proficiency and intimate familiarity with the political culture of the foreign country in which they had been born, first-generation OSINT practitioners could readily comprehend the policy implications of a newspaper article published in Moscow. Today, OSINT has changed, and so have the necessary skills and capabilities of OSINT practitioners. As Harding (2024) explained, "What once was largely translation work is now deriving unique insights from massive, public datasets, using the power of cloud computing and artificial intelligence (AI) to find all the needles in the haystack, and sharing those insights with a wide range of customers."

Modern OSINT practitioners now have a considerable number of OSINT techniques and specialized tools that they can use to gain publicly available information, increasing the timeliness of responding to their intelligence requirements. These include such things as social media investigation, DNS lookup, reverse image search, scraping, Google dorks, geolocation, exploit database searches, and vulnerability database searches (Browne, 2024). This list can be expanded even further to include such resources as: Meta search engines, foreign search engines, dark web search engines, website analytics tools, translation tools, social media exploitation platforms and databases, geopolitical databases, alerting and monitoring platforms, image search and verification tools, and managed attribution tools. Today's OSINT practitioners need to comprehend the value and utility of such targeted information, know which specialized software applications to use to acquire it, and understand how to correctly employ that software while at the same time engaging in the OSINT collection tradecraft necessary to avoid alerting information owners to outside interest in their information, known as topical risk.

The growing specialization of OSINT

To be truly proficient, modern OSINT collectors and analysts need to know where to look for data, how to collect it legally and ethically, how to use specialized tradecraft and high-end collection tools to acquire it, and must also possess familiarity with specialized analytic tools to make sense of, integrate, and visualize it all (Usher, 2024). Specialized software exists to identify and track sentiment on social media, geolocate photographs, and perform a wide range of other OSINT tasks. In short: Language aptitude and cultural familiarity are no longer sufficient for today's OSINT practitioners. OSINT practitioners must keep up with changes in the big data domain, the tools necessary to properly collect data while mitigating technical and topical risks, and changes to laws and policies (Browne et al., 2024).

Interest in OSINT beyond the IC

Whereas first generation OSINT remained largely within the purview of governments, second generation OSINT has been increasingly used by a wide range of individuals and organizations ranging from OSINT collectors at CIA and in other IC organizations to investigative journalists (Ganguly, 2022). Usher (2024) described a "dynamic ecosystem of national security-focused companies, non-profits, and academia" that "have developed specialized expertise and products" based on their OSINT activities (p. 24). Cybersecurity professionals make use of OSINT for ethical hacking, penetration testing, and identifying external threats (Borges, 2024). Other firms, such as Zero Trafficking, C4ADS, and Public Democracy, "seek to collect, analyze, and share findings from publicly available data to further public interests such as illuminating unsolved mysteries, exposing human trafficking, or combatting misinformation" (Tucker, 2025, p. 1).

The Center for Intelligence Research, Analysis, and Training (CIRAT) at Mercyhurst University has successfully used OSINT as its primary intelligence discipline, providing the private sector, government, law enforcement, and NGOs with such intelligence-driven services as strategic intelligence, competitive business intelligence, tactical intelligence, country threat assessments, vulnerability assessments, supply chain risk and security, geopolitical activities, monitoring of indicators and warnings tied to course of action development, executive protections, and cyber threat assessments.

Open-source investigations

Some private sector firms are remarkably skilled at OSINT; one of the most well-known private sector entities engaging in OSINT is the Netherlands-based investigative journalist group known as Bellingcat, established by British citizen Eliot Higgins in 2014. To differentiate itself "from government and corporate intelligence practices and products," Bellingcat describes its work as open-source investigation (OSINV), rather than as open-source intelligence (OSINT) (Van Puyvelde, 2023, p. 3).

The Hetherington group is another private sector firm that has built itself on providing exact, precise delivery of critical intelligence from its expertise in OSINT investigations and training, with its focus being to keep people, businesses, and assets safe from online threats, while obtaining critical information (Hetherington, 2024). Within the academic sector, the Intelligence Studies Program at Mercyhurst University is leading the way, with a strong focus on the OSINT discipline as a foundational training for students.

Table 2. Comparison of 1st and 2nd generation OSINT. Source: Generated by authors.

Comparing 1st and 2nd Generation OSINT		
Category	**1st Generation OSINT**	**2nd Generation OSINT**
Timeframe	**1940s through early 1990s**	**From the 1990s-current Day**
OSINT practitioner's organizational affiliation	Federal government (national-level intelligence organization)	National intelligence organizations, global security operations centers (GSOC), federal, state, and local law enforcement, competitive intelligence firms, and private investigators
Types of desirable OSINT practitioner skills and experience	Native language proficiency in one or more foreign languages and cultural understanding of the target country, understanding of traditional media sources	Digital research and collection skills (all levels of the web), leveraging open-source tools and platforms, managed attribution, digital translation, social media sources, technical and topical risk mitigation
Types of OSINT source materials	Hard-copy printed materials (newspapers, magazines, manuals, books); radio and TV broadcasts, handwritten materials, and public forums	Traditional, social, or new media information available in the public domain, in a venue where the public has reasonable access, or online databases of PAI (CAI)
Considered to be an independent intelligence collection discipline?	No	Yes, after 2006
Percentage of U.S. intelligence community's collected intelligence derived from OSINT on the former Soviet Union (or, after 1991, the Russian Federation)	~20%	~80-90%

State actor OSINT capabilities

In 1991, years before the proliferation of the internet and the creation of social media, Huo Zhongwen and Wang Zongxiao published a book in China entitled, Sources and Techniques of Obtaining National Defense Science and Technology Intelligence. In this book, described by one CIA analyst as "China's spy manual" (Munoz, 2015, p. 35), the authors urged that OSINT should be systematically used to collect national defense science and technology information (Huo and Wang, 1991). While much has been written about Chinese industrial espionage and hacking as means to illicitly gather intellectual property from foreign governments and firms, less well known is China's longstanding and massive use of OSINT to acquire publicly available information from foreign governments, companies, and various third parties (Hannas et al., 2013). Some of China's best intelligence collection work is OSINT, largely because there is a wealth of publicly available information from US government websites and publications, third-party publications, and newspapers (Hannas et al., 2013). As three respected Western experts on Chinese intelligence operations asserted about China's intelligence acquisition efforts, "There is nothing like it in the world" (Hannas et al., 2013, p. 2-3). In addition to placing high emphasis on OSINT, China and other state actors "are much less complacent than the IC" in exploiting CAI and PAI (Usher, 2024, p. 24).

Non-state actor OSINT capabilities

Not only state actors, but also non-state actors, such as insurgents, terrorists, and criminal organizations, engage in OSINT. In some instances, non-state actors have proven to be even more proficient than state actors in leveraging OSINT: For example, prior to its 7 October 2023 surprise attack, Hamas made more effective use of OSINT than did Israel (Van Puyvelde, 2023). Whereas OSINT lay "at the heart of Hamas' operational plan to simultaneously attack many Israeli targets and cause extensive damage," Israel's "OSINT systems underperformed in the run-up to the 7 October attacks" (Barnea, 2024, p. 1073).

Limitations

This article was narrowly focused on examining why and how open-source intelligence collection evolved from first- to second-generation OSINT, transitioning from being a very limited function solely performed by a handful of government analysts with unique backgrounds and skills to one that is now widely practiced in a variety of ways by both government and private sector analysts. The primary target audiences for this article are senior- and mid-level managers and OSINT practitioners in both the intelligence community and in the private sector who are currently grappling with such varied (but related) issues as the need to understand: (1) what 2nd generation OSINT is, (2) how it should be performed, (3) how OSINT products should be analyzed and integrated with other intelligence, (4) how OSINT efforts should be resourced (skills, tools, training, experience), and (5) how to cope with the growing security challenges associated with certain types of OSINT work. Clearly, this article cannot answer all of these questions; instead, it seeks to identify an appropriate framework within which 2nd generation OSINT can be better understood and discussed.

Results

Following their systematic review of the literature, the authors engaged in content analysis to identify ways that Information Age technologies impacted OSINT, and to identify the implications of those changes for today's OSINT practitioners. OSINT practitioners, supervisors, and beneficiaries, both inside and outside the government, must pay attention to certain identifiable needs that have arisen due to the massive evolution in OSINT that has occurred in the 21st century. At least a dozen of those needs are identified and described below:

The need for a shared understanding of OSINT

Just a couple of quotes from the scholarly literature on OSINT illustrate the extent to which consensus on what OSINT is and how it should be conducted remains lacking. Van Puyvelde (2023) noted that "OSINT often involves using grey data available online, even when its release was unauthorized" (p. 3). Or, as Borges (2024) asserted, "If any specialist skills, tools, or techniques are required to access a piece of information, it cannot reasonably be considered open-source" (para 15). Such divergent opinions on what OSINT is and how it should be conducted lends credence to Borges' (2024) assertion that, "Open-source intelligence is widely misunderstood and misused." Hatfield (2024) goes even further by asserting that OSINT "is a fundamentally incoherent concept that should be abandoned" (p. 397).

The need to determine OSINT's role (and place) in the IC

Vogel (2024) asserted that despite ODNI in 2006 designating OSINT as a separate and distinct intelligence collection discipline, OSINT continues to be "perceived as a lesser intelligence discipline by the IC" (p. 193-194). There does appear to be a lack of unanimity among intelligence professionals as to how OSINT should be most effectively leveraged within the IC. As former DIA Director Patrick Hughes (2022) explained, "We need acknowledgment of (OSINT's) place in the several disciplines of intelligence, and we also need a systematic understanding of what it is, what it is not, and how best to harness its inherent power and value for the work of intelligence on behalf of our nation" (p. 5). While some senior intelligence officers have urged for OSINT to become its own, independent intelligence agency (Usher, 2024), each of the 18 organizational entities in the IC currently seeks to independently integrate OSINT with their other, existing collection disciplines and specialties (Host, 2025). For example, CIA established its DDI to "respond to its growing need to understand, utilize and respond to emerging digital technologies. The DDI combines the agency's missions of cyber collection and security, OSINT, IT, data and others" (Host, 2025). Usher (2024) acknowledged that despite countless discussions for at least a decade, the IC still has not adopted "an all-encompassing solution" to the increasing OSINT challenge (p. 24). There is also a need to determine the role of OSINT in the private and non-governmental sectors. As the IC within the government is regulated, albeit not uniformly, there are regulations or laws governing the use of OSINT in these other sectors of the IC. The question is then posed: Is OSINT a discipline to be uniformly regulated and defined throughout the entire IC, or as sub-sections of the IC? Who should be the governing body in supervising "Second Generation" OSINT within these sub-sections or the entire IC?

The need for specialized skills

Whereas first generation OSINT principally relied upon native or near-native foreign language and cultural experts to translate and explain foreign language radio broadcasts or newspaper articles, second generation OSINT calls for a collaborative effort by a team of practitioners possessing a wide range of specialized, technical skills. Lakshmi Raman, CIA's chief AI officer, asserted that CIA is now incorporating large language models, or LLM, in generative AI to support CIA's OSINT mission (Host, 2025). To use AI and OSINT to support its human intelligence officers requires CIA to have "a cohort of data scientists, analytic methodologies, AI professionals and engineers" (Host, 2025).

The need for specialized tools

Thanks to advances in technology, there is now a large (and growing) variety of specialized, automated tools that can be used to accelerate and enhance the collection, analysis, and visualization of data (Mobili, 2023). For example, Maltego is a data mining tool that helps researchers identify and analyze relationships between people, groups, and websites. Recorded Future provides comprehensive, real-time, and unbiased threat intelligence by connecting the dots across internal telemetry and external sources using the AI-driven Intelligence Graph. The Intelligence Graph indexes, organizes, and analyzes data from over a million sources, including the open web, dark web, technical feeds, and customer telemetry. By integrating

seamlessly with existing security tools and workflows, this intelligence-driven approach enhances your security stack, allowing your team to better prioritize risks, streamline decisions, and respond to threats with greater confidence and efficiency. Shodan is a search engine designed for finding and identifying devices connected to the internet. TweetDeck, Hootsuite, and Babel Street are specialized tools that enable researchers to monitor and analyze social media trends and sentiments. Samdesk is a crisis and monitoring tool utilizing an AI engine that proactively scans the world for anomalies that impact the operational environment and provides an immediate alert so action can be taken expeditiously. Since possessing and using these tools costs money and requires expertise, a cottage industry of OSINT contractors has sprung up in the private sector, supporting both government agencies and competitive intelligence customers in the private sector (Mobili, 2023).

The need for OSINT tradecraft

Within the U.S. intelligence community, the term tradecraft refers to the techniques, methods, and technologies used in a particular intelligence collection discipline (Weinbaum, 2024). Today, there can be times when a collector may wish to acquire open-source information from certain foreign websites, such as those in sensitive countries like Russia, China, Iran, or North Korea. OSINT practitioners must employ tradecraft to gain access to and acquire publicly available, digital information from sensitive sites and/or within sensitive countries in a non-alerting manner (Ragan, 2023). What websites are visited, when, and for how long can tip off a foreign intelligence service (FIS) to the fact that outsiders are collecting information; while managed attribution is necessary to obfuscate an OSINT collector's location, tradecraft is also necessary to avoid drawing FIS attention to the collection activity itself (Ragan, 2023).

The need for managed attribution

Managed Attribution (MA) is a portfolio of capabilities, policies, tradecraft, training, and acquisition that enables the Intelligence Community to conduct research, communications, and operations missions by leveraging open and commercially available Internet technologies and networks. MA is a technological capability that disassociates online activity conducted by an organization, business, or the U.S. Government, thereby not revealing interests, intentions, or collection priorities (Hoffman, 2025). MA uses a technology that has no connections to the applicable Information Network or any official IP space. OSINT practitioners in the national security realm, law enforcement, and academia frequently find it necessary to form a digital identity, especially when conducting OSINT collection on sensitive sites in certain countries (Drecker, 2023). While a virtual private network (VPN) can help mask one's country of origin, IP and geographical location, a managed attribution capability "allows researchers to spoof their true location across different, configurable geo-locations, manipulate their hardware and software fingerprints, and to collect, annotate, and securely store internet-based PAI (Publicly Available Information)" (Fuchs & Lemon, 2019).

The need to validate sources

One of the key components of human intelligence, or HUMINT, is source validation. HUMINTers will routinely ask, "Who provided this information? How reliable is the source of the information? On what do we base our assessment about a source's reliability?" While OSINT may obtain information from a reputable publication, who was the author of the article? And from whom did the author obtain the reported information? In some cases, OSINT may yield information that cannot reveal the source at all. Even Bellingcat's editorial standards and practices (Editorial, 2020) acknowledge that while "the use of anonymous sources is generally avoided," there "may be isolated occasions when this is acceptable" (p. 3). Varzhanskyi (2024) asserted that "most of the risks accompanying the realization of OSINT can be leveled if we responsibly approach the choice of sources and double-check the information" (p. 22).

The need to recognize and obey data protection regulations
Different countries and regions are governed by different policies concerning data privacy: What may be considered legitimately collected PAI in one country may be deemed "protected" in another. For example, the European Union's General Data Protection Regulation (GDPR) and the U.K.'s Data Protection Act both "had the goal of protecting personal data from unauthorised collection, storage, and exploitation" (Sandhu, 2023).

The need to recognize that adversaries also use OSINT
Nation states, substate actors, and criminal organizations have all come to appreciate the value of OSINT. Defending against adversary use of OSINT is a topic of understandably high interest to cybersecurity professionals (Nagendran, 2024). Sometimes, knowing that adversaries are targeting you with OSINT provides opportunities: As Varzhanskyi (2024) explained, the Russians in 2022 were apparently so misled by public statements by senior U.S. and Ukrainian officials about an impending counteroffensive in the Kherson region they transferred troops to Kherson and away from Kharkiv – which Ukraine's armed forces then liberated.

The need to be wary of possible data manipulation
Especially in cases where OSINT leverages AI to collect data, one must remain alert to the possibility of data being intentionally manipulated by an adversary from whom the data is acquired (Varzhanskyi, 2024). As one example, Varzhanskyi (2024) describes how European OSINT collectors were misled by Russian disinformation stories planted in both the news media and Wikipedia about the 2014 downing of Malaysian Airlines flight MH17. Based on his examination of the Russia-Ukraine conflict, Varzhanskyi (2024) warned that OSINT collectors and analysts must be wary of an adversary's attempts to exercise "reflexive control" by providing false data that is then collected by friendly intelligence, a situation he described as "the hunter" getting "into a trap dexterously rigged by an adversary" (p. 1).

On social media platforms, perpetrators can use trolls and bots to spread disinformation (Nagendran, 2024). Nefarious actors can also use generative AI to create convincing deepfakes (Generative AI, 2025). Varzhanskyi (2024) warned how the "rapid development of machine learning technologies and neural networks allows for the creation of increasingly advanced deep fakes…which are already being used for information operations" (p. 18). As disinformation has moved from the political, government, and social spheres to the corporate world, it has grown in both scope and impact. However, there is a lack of a standard solution to counter disinformation. OSINT practitioners are especially vulnerable to this risk. Ensuring proper vetting of data is conducted, and trusted sources are routinely used for collecting PAI, is the responsibility of the practitioner and should be part of a practitioner's tradecraft.

The need to carefully embrace AI
Artificial intelligence, or AI, appeals to OSINT practitioners because it can "help reduce the time and workload of intelligence analysis by grouping data into relevant categories" (Browne, 2024, p. 2912). AI also appeals to OSINT practitioners as a means to reduce the risk of data overload (Nagendran, 2024). Some of the ways AI is currently transforming OSINT is by "AI-driven web scraping, social media monitoring through sentiment analysis, natural language processing, and image/video analysis" (Kovaci & Iacob, 2024, p. 1). "AI is not changing the way information is gathered; it is reshaping the entire process, making it more efficient, accurate, and responsive to the evolving nature of information on the Internet" (Kovaci & Iacob, 2024, p. 1). The IC's high interest in AI also extends to OSINT: One of the ways CIA's DDI intends to leverage both AI and OSINT is to significantly expedite how quickly CIA officers can gain "insights from a mixture of OSINT and clandestine intelligence collection" (Host, 2025). Although AI offers considerable advantages to OSINT practitioners, one must also exercise caution to ensure that privacy concerns, the potential for data biases, and the need for human oversight are both understood and adequately addressed

(Kovaci & Iacob, 2024). GenerativeAI regarding OSINT activities should be embraced, but removing the "human in the loop" is a dangerous and unrecommended practice. Utilizing GenAI to expedite research and collection, and to build products for analysis, is a welcome practice. However, the OSINT practitioners must still ensure the data is accurate and clean.

The need to adequately address AI-related data issues

As part of his argument in favor of establishing a 19th IC agency, the Open Source Agency, "to acquire, curate, develop, employ, and share CAI and PAI data sources for intelligence purposes," Usher (2024) referred to the three challenges of "volume, velocity, and veracity" that the intelligence community already faces when collecting and analyzing OSINT (p. 24, 26). AI-enabled OSINT raises "issues with data quality, data quantity, data integration, analysis and interpretation, privacy, and ethical considerations" (Govardhan et al., 2023, p. 236). Varzhanskyi (2024) asserted that the risk of falling victim to reflexive control has increased as increasingly large amounts of data are automatically ingested and processed (p. 2).

While artificial intelligence, or AI, promises to speed up OSINT collection and analysis, the quality of analysis will be limited by the quality of data accessible to the collection system (Ghioni et al., 2024). Inside the Mercyhurst University's CIRAT, the embracing of GenAI as a capability for conducting OSINT is alive and well. The Center utilizes a software capability called Rover, which is provided by Vizru. Vizru ZEOS, the world's first zero-code application development environment, democratizes innovation within an enterprise. Rover provides a secure Gateway to AI Insights that seamlessly combines public and enterprise data without compromising Data Security. The CIRAT has utilized Rover to support OSINT operations, allowing for the GenAI software to pull from a robust data lake of trusted data, thereby increasing the time from research and collection to analysis, to product development, to decision making. With its interoperability with data visualization tools, analysts are spending more time analyzing and less time collecting. However, the number one focus with using this capability is ensuring the security of the data being exposed to networks and stored on-premises.

Conclusions

Second-generation OSINT is now a far cry from its humble beginnings. Today, not only U.S. intelligence community organizations, but also such varied private sector businesses and entities like Global Security Operations Centers (GSOC), think tanks, journalists, academics, investigators, and others have come to appreciate the value of publicly- and commercially available information acquired to meet their respective intelligence requirements.

One glaring research gap we noticed in our review of the OSINT literature was the lack of research focused on the implications of the diversity of understanding of what "second generation" OSINT is, how it is conducted, what it can (and cannot) target, how OSINT can integrate with other intelligence collection disciplines, and what its strengths, weaknesses, and limitations are. Relevant OSINT stakeholders include government and private sector practitioners and clients, officials involved in intelligence oversight, general counsels, legislators, executive branch actors, and others. Studying this issue, and then properly "rebranding" second generation OSINT, is therefore necessary to ensuring all OSINT stakeholders have a shared, comprehensive understanding of what open-source intelligence is and how best to safely manage, integrate, and exploit it.

References

Barnea, A. (2024). Israeli intelligence was caught off guard: The Hamas attack on 7 October 2023 — A preliminary analysis. *International journal of intelligence and CounterIntelligence*, *37*(3), 1056-1082.

Block, L. (2024). The long history of OSINT. *Journal of Intelligence History*, *23*(2), 95-109.

Borges, E. (24 June 2024). What is open-source intelligence (OSINT)? *Recorded Future*, https://www.recordedfuture.com/blog/open-source-intelligence-definition

Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. *International Journal of Information Security*, *23*(4), 2911-2938.

Data Management Lexicon. (January, 2022). Office of the Director of National Intelligence. Washington, DC.

Dreker, M.R. (2023). Risks, privacy, and harassment. In: Dreker, M.R., Downey, K.J. (eds) *Building Your Academic Research Digital Identity*. Springer, Cham. https://doi.org/10.1007/978-3-031-50317-7_9

Editorial standards & practices. (2020). *Bellingcat*, https://www.bellingcat.com/app/uploads/2020/09/Editorial-Standards-Practices.pdf. Accessed 22 June 2022

Fuchs, M., & Lemon, J. (2019). Sans 2019 threat hunting survey: The differing needs of new and experienced hunters. SANS Institute Information Reading Room.

Ganguly, M. (2022). The future of investigative journalism in the age of automation, *Open-Source Intelligence (OSINT) and Artificial Intelligence (AI)*. PhD dissertation. University of Westminster.

Generative AI is the ultimate disinformation amplifier. (6 March 2024). *DW Akademie*, https://akademie.dw.com/en/generative-ai-is-the-ultimate-disinformation-amplifier/a-68593890

Govardhan, D., Krishna, G. G., Charan, V., Sai, S. V., & Chintala, R. R. (2023, 19-21 July 2023). *Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity*. Paper presented at the 2023 2nd International Conference on Edge Computing and Applications (ICECAA).

Hannas, W. C., A. G., Mulvenon, J., and Puglisi, A. B. (2013). Chinese industrial espionage: Technology acquisition and military modernization. Routledge.

Harding, E. (2024). The IC's new OSINT strategy gets the basics right. *Center for Strategic & International Studies*, https://www.csis.org/analysis/ics-new-osint-strategy-gets-basics-right

Hatfield, J. M. (2024). There is no such thing as open-source intelligence. *International journal of intelligence and CounterIntelligence*, *37*(2), 397-418.

Hetherington, C. Osint: The Authoritative Guide to Due Diligence. Hetherington Group.

Hoffman, F. (2024). Learning by doing: Acquiring the tacit knowledge of how to conduct an open-source intelligence collection and analysis project. *Issues in Information Systems, 25*(3), 81-93.

Host, P. (3 April 2025). CIA leveraging digital transformation tools in HUMINT missions. *Executive.gov*, https://executivegov.com/2025/04/cia-digital-transformation-tools-humint-juliane-gallina/

Hughes, P. M. (2022). Open-source information: The thread of knowledge that ties our societal fabric together – A discipline of intelligence. *American Intelligence Journal 39*(1), p. 5-15.

Hunting, B. (28 November 2022). When the new generation of Olds killed your father's Oldsmobile. *Motor Trend*, https://www.motortrend.com/features/not-your-fathers-oldsmobile-general-motors-history/

IC OSINT Strategy 2024-2026 (2024.) Office of the Director of National Intelligence, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

Langrock, S., and Smilyanets, D. (9 April 2024). Improving dark web investigations with threat intelligence. *Recorded Future*, https://www.recordedfuture.com/blog/improving-dark-web-investigations-with-threat-intelligence

Kovaci, P.-D., and Iacob, N. M. (2024). Artificial intelligence and OSINT: Considerations and challenges. *Romanian Cyber Security Journal, 2*(6), 1-8.

Meagher, D. (8 April 2024). What ever happened to Oldsmobile? *Slashgear*, https://www.slashgear.com/1553417/what-ever-happened-to-oldsmobile/

Mobili, M. (2023). Review OSINT tool for social engineering. *Frontiers in Big Data 6*, p. 1-13.

Munoz, A. G. (2015). Intelligence in public media. *Studies in Intelligence 59*(4), p. 33-35.

Nagendran, P. (2024). Analysing and Reducing Vulnerability to OSINT. Master's thesis. Oslo University.

Olds is NOT 'Not your father's car' anymore. (1990). *Los Angeles Times Archives*, https://www.latimes.com/archives/la-xpm-1990-01-04-fi-527-story.html

Standards. (2025). OSINT Foundation, https://www.osintfoundation.com/osint/Standards.asp

Ragan, S. (23 February 2023). Practical OSINT tips for betting planning and tradecraft. *Authentic8*, https://www.authentic8.com/blog/OSINT-tips-planning-tradecraft

Rietjens, S., Sinterniklaas, R., & Coulthart, S. (2025). How intelligence organisations innovate. *Intelligence and National Security, 40*(1), 22-41.

Sandhu, S. S. (2023). Analysis of role of OSINT in the wars around the World. Master's thesis, Hochschule Offenburg.

Schreiber, R. (26 January 2021). Yes, it really was your father's Oldsmobile. *Hagerty*, https://www.hagerty.com/media/entertainment/yes-it-really-was-your-fathers-oldsmobile/

Tucker, K., & Robson-Morrow, M. (2025). Intelligence outsourcing for non-traditional clients: the rise of private sector intelligence providers. *Intelligence and National Security*, 1-20.

Usher, W. (2024). The case for creating an open-source intelligence agency. *Studies in Intelligence 68*(3), 23-29.

Van Puyvelde, D., & Rienzi, F. T. (2023). The rise of open-source intelligence. *European Journal of International Security*, 1-15.

Varzhanskyi, I. (2024). Reflexive control as a risk factor for using OSINT: Insights from the Russia–Ukraine conflict. *International Journal of Intelligence and CounterIntelligence*, *37*(2), 419-449.

Vogel, K. M. (2024). OSINT and the U.S. Intelligence Community: Is the past prologue? In Open Source Investigations in the Age of Google (pp. 188-203). *World Scientific*.

Weinbaum, C. (29 August 2024). Intelligence officers have an ethical responsibility to use tradecraft. *International Journal of Intelligence and CounterIntelligence*, p. 1-22.

Williams, H. J. and Blum, I. (2018). Defining second generation open-source intelligence (OSINT) for the defense enterprise. RAND: Santa Monica, CA