Issues in Information Systems
Volume 26, Issue 3, pp. 75-85, 2025

DOI: https://doi.org/10.48009/3_iis_2025_2025_106

How Mercyhurst's CIRAT does OSINT – and why

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

Abstract

Mercyhurst University's Intelligence Studies program, the oldest intelligence studies program in academia, was founded in 1992. In 1997, Mercyhurst's Intelligence Studies program established its award-winning Center for Intelligence, Research, Analysis, and Training (CIRAT), which to this day remains the flagship program for conducting open-source intelligence (OSINT). For a generation, CIRAT has successfully performed OSINT projects for a wide range of government, law enforcement, and private sector clients. Due to the impact of multiple Information Age technologies and trends since the end of the Cold War, open-source intelligence collection, or OSINT, has transformed and proliferated to such an extent that some practitioners now refer to it as *second-generation* OSINT. The purpose of this study was to employ qualitative research methodologies to analyse CIRAT procedures and performance to better comprehend the reasons for CIRAT's continued success. We found that CIRAT OSINT projects were successful because student OSINT researchers have been consistently and systematically trained in OSINT principles, procedures, and methodologies and adequately supervised by experienced principal investigators and OSINT subject matter experts. Through participation in CIRAT, students learn through training and experience how OSINT should be properly conducted, what technological tools and tradecraft are necessary to enable its success while mitigating its risks, and how OSINT can be conducted professionally, ethically, and legally. The implications of our findings are that today's second-generation OSINT practitioners benefit considerably from having both the educational foundation and experiential, tacit learning necessary to not only perform OSINT efficiently and effectively, but also safely and ethically.

Keywords: open-source intelligence, OSINT, OSINT tradecraft, managed attribution

Introduction

In 1992, Mercyhurst University in Erie, Pennsylvania, founded the first-ever Intelligence Studies program in the United States, and five years later established its Center for Intelligence Research, Analysis, and Training, or CIRAT (Heibel, 2025). CIRAT was intended to provide its students with the ability to combine classroom "lessons learned" about intelligence collection and analysis with state-of-the-art, specialized software applications to solve open-source intelligence (OSINT) challenges presented to them by real-world government and private sector clients from the United States and overseas (Heibel, 2025). Today, not only students from the Intelligence Studies department, but also graduate and undergraduate students from CIS (Computer and Information Systems) and other Mercyhurst University departments, participate throughout the year in one of the Center's six established program areas, working on CIRAT projects under the supervision of Mercyhurst faculty members, or Principal Investigators (Fuller, 2025). In 2008, six Mercyhurst Intelligence Studies students participated in a competition sponsored by the Office of the

Director of National Intelligence. Their task was to answer the question, “Is Al Qaeda a cohesive organization with strong and centralized control, intent and direction?” “Seven 13-hour workdays later, they discovered their answer had surpassed those of more than 20 other competitors, some veterans of the U.S. intelligence community, to win the first-ever ODNI-sponsored ‘Open Source Challenge’” (*Mercyhurst*, 2008). “The Mercyhurst team was one of two winners among 24 competitors. The other team took top honors by answering the second of two questions posed by ODNI’s challenge. Coincidentally, that team, iJET Intelligent Risk Systems, a private firm working with multinational organizations to monitor, protect against and respond to global threats, had two employees on its team that graduated from Mercyhurst’s master’s program in Applied Intelligence” (*Mercyhurst*, 2008). This helped launch the CIRAT into the IC as being recognized as an OSINT expert program.

The secret to CIRAT’s track record of success to date is not only that its practitioners (students) successfully obtain valuable information that generates actionable intelligence and insights for its various clients, but also that project team members are trained to do so in a professional, safe, and secure manner that mitigates all risks and is conducted discreetly, legally, and ethically (Fuller, 2025).

Although a steadily growing number of organizations currently conduct OSINT, there are a number of factors that continue to set CIRAT apart from the pack. In order to effectively convey what those contributing factors are, this article addresses certain relevant, related topics:

- How, why, and to what extent Digital Age technologies transformed OSINT;
- What types of information are now accessible to OSINT practitioners;
- Who currently conducts OSINT;
- What types of OSINT data sources exist around the world, and the threats associated with them;
- Why managed attribution and OSINT tradecraft are so essential;
- Ethical and legal considerations for OSINT practitioners.

Methodology

The authors employed several qualitative research methodologies in seeking to answer the research question, “How can today’s second-generation OSINT practitioners benefit from examining how Mercyhurst University’s CIRAT program conducts open-source intelligence collection and analysis?” The qualitative research methodologies employed included an examination of CIRAT projects and procedures, interviews of CIRAT principal investigators, supervisors, researchers, and customers, and content analysis of CIRAT project-related documents.

An examination of contributing factors

To properly understand why Mercyhurst’s CIRAT program has been so consistently successful, it is necessary to examine the factors contributing to that success. These include: How OSINT has evolved since the end of the Cold War, the types of information OSINT practitioners can now acquire, the expansion of governmental and non-governmental entities performing OSINT, the risks associated with certain types of OSINT research, how managed attribution and OSINT tradecraft can mitigate those risks, and why it is essential for OSINT practitioners to operate legally and ethically.

First-generation OSINT

In the 20th century, U.S., British, and a handful of foreign intelligence organizations conducted open-source intelligence, or OSINT, to gain intelligence insights from foreign-language radio and television broadcasts, newspapers, and other publicly available documents (Block, 2024). In the middle of the 20th century, the two principal OSINT organizations in the United States were the Foreign Broadcast Information Service (FBIS) and the Joint Publication Research Service (JPRS) (Bryant, 2024). Established in 1941, just before the U.S. entered the World War II, FBIS was the U.S. government's first OSINT organization (Roop, 1969). FBIS was established "to monitor foreign shortwave radio broadcasts from 'belligerent, occupied, and neutral countries' directed at the USA" (Serscikov, 2024, p. 1031). By 1992, FBIS "operated 19 regional bureaus that monitored 'more than 3,500 publications in 55 languages and 790 hours of television a week in 29 languages from 50 countries'" (Serscikov, 2024, p. 1032).

In addition to FBIS, there was also the Joint Publication Research Service, or JPRS. Founded within the department of Commerce in March of 1957, the JPRS provided "translations of foreign documents in areas of science, technology, and the social sciences" (Hassig, 1987, p. 559). At one point, JPRS was the government's largest translation body (Serscikov, 2024). Hulnick (2002) described how the two organizations differed by saying, "if an analyst could alert FBIS to an anticipated speech by a world leader, the translation service would find the appropriate media outlet, capture the speech, translate it, and provide it by cable, usually within 24 hours. For the analyst doing more in-depth work, the Joint Publication Research Service (JPRS) would contract out book or journal translations for those who could not read the book in its original language" (Hulnick, 2002, p. 570). Because acquiring, translating, and analyzing foreign broadcasts and hard copy documents was so labour-intensive, tedious, and sometimes hazardous, analogue-era (or "First Generation") OSINT collection and analysis was basically limited to national intelligence organizations that had been established for that express purpose (Block, 2024).

Second generation OSINT

Since the end of the Cold War (1947-1991), OSINT has undergone a massive transformation due to such significant and rapid technological developments as the digitization of information, the creation of the internet and social media, the proliferation of broadband Internet access, and the popularity of mobile telephony and mobile apps. "The World Wide Web went public in 1991. Google, the world's most popular web-based search engine, dates to 1998. Space Imaging released the world's first high-resolution commercial satellite images in 1999" (Mercado, 2024, p. 51). Such changes led Williams and Blum (2018) to describe today's OSINT as "second generation open-source intelligence" (p. 2).

Not only did the collection of openly available information rapidly expand into and within the private sector, but the introduction of (and synergy between) these and many other new technologies also provided OSINT practitioners with an ever-expanding suite of collection tools. For example: Not only could OSINT practitioners now access the internet and acquire a digital image of a facility, they could also geolocate it, or determine its precise location on a map (Mercado, 2024). They could also chronolocate it, or date a depicted image by "comparing videos from social media against satellite imagery" (Mercado, 2024, p. 52). It is not uncommon for modern parents to sternly warn their children that "Once something is on the internet, it's there forever" (Jennings, 2010). While this statement is not entirely true, there are a number of techniques that OSINT practitioners can use, such as the Wayback Machine, to obtain historical information from websites – even after a website owner has "scrubbed" their current site of the data (Arora et al., 2016). The increasing value and impact of OSINT, and the proliferation of both government and private OSINT practitioners, have become increasingly apparent over the past decade or so, especially in the wake of Russia's invasion of Ukraine on 24 February 2022. As Baffa (2025) explained:

> "Real-time updates from anyone with a cell phone or an internet connection are being posted by amateur analysts, journalists, and ordinary citizens throughout the region on social media channels and blogs, reaching thousands of people and impacting the course of the war. Footage and photos from phones, combined with commercial satellite images and Google traffic alerts, have revealed Russian troop movements and military convoys, with results shared to and from Twitter and TikTok."

Types of information now accessible via OSINT

There are three categories of information that OSINT practitioners may encounter in their research: Publicly available information (PAI), commercially available information (CAI), and proprietary information. Two may be legally and ethically accessed and acquired via OSINT, but one may not.

PAI

Publicly available information, or PAI, is any information that is accessible in the public domain (Vogel, 2024). "Properly handled, PAI is the foundation that useful intelligence reports are built upon" (Monday, 2022, p. 149). Unfortunately, accessible does not necessarily mean readily available; for example, an online researcher performing Google word searches may be surprised to learn that roughly 96% of all the information on the internet is not search engine optimized (SEO) and is therefore inaccessible through Boolean word searches on the so-called "surface web" (Sultana & Jilani, 2021).

Rather, the vast majority of the internet is located on the Deep Web and the Dark Web. "The Deep Web constitutes a vast repository of hidden information, encompassing personal files, academic research, and sensitive databases like email and online banking records. Conversely, the Dark Web represents a minute fraction of this hidden space, notorious for facilitating illegal activities such as trading illicit goods, sharing stolen data, and orchestrating cyberattacks" (Sultana & Jilani, 2021, p. 372).

CAI

CAI is also "available commercially to the general public, and as such, is a subset" of PAI (ODNI, 2022, p. 8). To acquire CAI, OSINT practitioners or their parent organizations purchase it from the company that produces or aggregates it, either as a one-time purchase or as a subscription (ODNI, 2022). While CAI saves OSINT practitioners a considerable amount of time and effort required to conduct targeted collection, scrape the web, and aggregate the information, it becomes an expensive proposition to repeatedly pay for CAI (ODNI, 2022). In 2022, a Senior Advisory Group Panel on Commercially Available Information, or CAI, reported to the Director of National Intelligence, Avril Haines, that while CAI "clearly provides intelligence value", it also "raises significant issues related to privacy and civil liberties" (ODNI, 2022, p. 3).

Proprietary information

Unlike CAI, which a company willingly sells, there is also proprietary information. Proprietary information consists of trade secrets that a company definitely does not want made available to the public, such as the recipe for Coca-Cola (Ganotra, 2018). To protect proprietary information, companies have two primary options: they can either patent it or secure their trade secrets in a manner similar to how government agencies handle classified information. According to patent law, third parties wishing to use the information contained in a patent must pay royalties to the patent owner (Khan, 2021). The problem with a patent, though, is that patenting "means creating a public document available to anyone" (Hulnick, 2002, p. 577). OSINT practitioners who surreptitiously acquire proprietary information from a company – that is, without the knowledge and consent of the information's owner – do so illegally (Dvojmoč, 2019).

Increased interest in OSINT

Whereas first-generation OSINT was predominantly performed in the United States by FBIS and JPRS, modern, second-generation OSINT is not only conducted throughout the entire U.S. intelligence community and by intelligence organizations within all the military services, but also by federal, state, and even municipal law enforcement agencies (Cohen et al., 2025). “The digital age has brought unprecedented challenges to the intelligence community and law enforcement agencies, necessitating a fundamental shift in how analysts operate and how information is processed” (Cohen et al., 2025, p. 1). OSINT has also become extremely popular in the private sector: OSINT has long been embraced by competitive intelligence firms (Fleisher, 2008). “DOD contractors include Fortune 100 companies that can analyze the financial battlefield as expertly as any government agency. Agile firms, like Roger Robinson’s RWR Advisory Group, are already tracking China’s overseas business relationships through open-source methods” (Bernier, 2021, p. 47). Foreign governments and companies have also increasingly turned to OSINT to meet their intelligence requirements (Li et al., 2025). Even non-state actors like terrorists, insurgents, separatists, and organized crime groups have leveraged OSINT – in some cases, even more productively than their state actor adversaries (Barnea, 2024). OSINT has also become recognized in the academic sector, with such programs as Mercyhurst University’s Intelligence Studies program and entities like the Center for Intelligence Research, Analysis, and Training.

OSINT operations and risk

Although OSINT has been eagerly embraced by a steadily growing number of government and commercial practitioners in the United States and overseas, there is no unanimity in the way OSINT operations are conducted (Fuller, 2025). This can present problems because while first-generation OSINT was a comparatively low-risk activity, second-generation OSINT is not low-risk (Fuller, 2025). In today’s Big Data age, the digital sources of OSINT present significant technical and topical risks not seen with first-generation OSINT sources.

OSINT target tiers

Operators of sensitive websites overseas may feel compelled to identify online visitors whose motivation is not simply to access and acquire data, but to attack their website, deny or corrupt its data, and disrupt their organization’s operations (Thummala & Falco, 2024). For example, in March of 2022, just a few weeks after Russia had invaded Ukraine, Network Battalion 65 (NB65), comprised of individuals affiliated with the hacktivist group Anonymous, asserted that they had breached the satellite imaging capabilities of Russia’s State Corporation for Space Activities (ROSCOSMOS), a state organization that managed Russia’s space exploration, manned space flight, satellite operations, and international space cooperation (Thummala & Falco, 2024). Around the same time, NB65 also claimed to have attacked the All-Russia Television and Radio Broadcasting Company, “resulting in the encryption of 786.2 GB of data, comprising 900,000 emails and 4,000 files” (Thummala & Falco, 2024, p. 3). Prior to attacking the ROSCOSMOS web site, NB used “OSINT methods” to “glean information regarding ROSCOSMOS’s network infrastructure, domain names, IP addresses, and subdomains” (Thummala & Falco, 2024, p. 8).
Based on a risk assessment, websites are identified as belong to one of three “tiers,” with each tier presenting a different level of risk to OSINT practitioners. The Mercyhurst University OSINT program defines these tiers as:

Tier 0

When a risk assessment determines that the threat knowledge of the OSINT activity will not pose a risk to imminent or ongoing operations or intelligence priorities, sources, or methods, it is a Tier 0 research or collection activity. An example of a Tier 0 website would be The New York Times website (Fuller, 2025).

Tier 1

When a risk assessment determines a website owner's identification of the envisioned OSINT activity could pose a risk to imminent or ongoing operations, or to intelligence priorities, sources, or methods, that website is designated a Tier 1 research or collection activity. An example of a Tier 1 website would be Russia's Rossiya 24 television station website in the Russian Federation (Fuller, 2025).

Tier 2

When a risk assessment determines that the threat knowledge of the OSINT activity will pose a risk to imminent or ongoing operations or intelligence priorities, sources, or methods, it is a Tier 2 research or collection activity. An example of a Tier 2 website would be a site known to be monitored by a foreign intelligence service or a site offering fake passports, credit cards, and drivers licenses on Dark Web (Fuller, 2025).

OSINT risks

Reducing one's digital signature

Prudent OSINT practitioners employ a combination of managed attribution and OSINT tradecraft when visiting Tier 1 or Tier 2 websites (Fuller, 2025). Failure to engage in these precautions could lead to an OSINT researcher unwittingly downloading malware like viruses, ransomware, or spyware (Yeboah-Ofori & Brimicombe, 2018). Referring to Marine OSINT practitioners, Barrows (2019) wrote, "The OSINT cell knows how to minimize their digital signature, use tools that are specific to OSINT, and optimize collection" (p. 34).

Why Managed Attribution is Necessary

OSINT collection tradecraft refers to the combination of tools, techniques, and procedures that online researchers use to safely and securely copy, store, or otherwise preserve PAI or CAI in any manner (Fuller, 2025). Utilizing Managed Attribution tradecraft and technological capabilities is the key to a successful collection when risk is involved (Fuller, 2025). Four of the reasons Mercyhurst's CIRAT teams use managed attribution are: (1) to gain access to data that may be otherwise denied to U.S. IP/PoPs; (2) to avoid misinformation and obfuscation targeting networks; (3) to mask collectors' true interests, intentions, and mission; (4) to protect the collector's own critical information and infrastructure from malware and other malicious attacks (Fuller, 2025).

The limits of VPNs, incognito mode, and misattribution

One of the primary objectives for online researchers visiting Tier 1 and Tier 2 websites should be to obfuscate their digital footprint and their network information, but there's much more to the story than just that. To prevent website owners from realizing their sites are of intelligence interest, some online researchers use virtual private networks, or VPN, to misattribute who they are and mask their true identities. While using a VPN is better than nothing because it may depict to the visited website that the user is visiting their site from a more benign region or country, it does not prevent browsers, websites and search engines from collecting other data "on many variables that can identify you" (Authentic8, 2025). Also, relying on just a VPN does not mitigate the risk of importing malware from visited websites (Authentic8, 2025).

Managed attribution

The term managed attribution refers to the technical means used to prevent a website operator from identifying the identity, location, organizational affiliation, and collection objectives of a website visitor by disassociating online activity and network information (Fuller, 2025). Managed attribution is more than just software; it refers to a "portfolio of capabilities, policy, tradecraft, training, and acquisition, which enables DoD and the Intelligence Community to conduct research, communications, and operations missions by leveraging open and commercially available Internet technologies and networks" (Fuller, 2025). An excellent example of this would be the managed attribution services that Authentic8 provides through its Silo, Toolbox, and Tor browsers. The risk to Tier 1 and Tier 2 website visitors stems from the fact that websites can collect a great deal of information whenever an online user visits, such as, "internet address and connection (registered owner, subscriber information), browser and device type (OS, software/plugins installed, time zone, audio/video devices, cookies, HTML5 local storage, canvas fingerprinting, audio rendering), unique online behaviors (social media connections, shopping interests, websites visited, account activity) and more" (Authentic8, 2025).

Correctly employing managed attribution not only makes it possible for OSINT practitioners to protect their true identity and intentions but also to craft an unobtrusive online identity that will blend in with those of other visitors to that website (Authentic8, 2025). Managed attribution provides significantly better security than either a VPN or an anonymous web browser. One managed attribution provider is Ntrepid. Aaron Murdock explained, "I teach my law enforcement clients that Nfusion is their Personal Protective Equipment, their PPE. Just like strapping on their boots, their vest, and whatever else they need as their personal protective gear that separates them from the world…That's exactly what Nfusion does as an OSINT platform. It gives people a way to conduct research in a safe environment" (Young, 2023). OSINT operators who do not use a managed attribution platform risk identity exposure, adversarial countermeasures, the acquisition of false information, and disorganized data collection (OSINT Operations, 2025).

Within the intelligence community, to include intelligence activities within each of the armed services, there is recognition that managed attribution is a necessary component of OSINT. In writing about the U.S. Marine Corps' use of OSINT, Barrows (2019) wrote, "The vision is to establish a Marine OSINT program of record that facilitates resourcing to include commercial–Internet service provider, managed attribution, tools, and training" (p. 35).

OSINT tradecraft

Within the intelligence community, the term tradecraft "refers to the methods, processes, tools and skills used for intelligence gathering" (Tradecraft, 2025). Even with a managed attribution capability, an OSINT practitioner must also employ OSINT collection tradecraft to prevent a website operator from becoming alerted to their presence and activities. For example, understanding website analytics is one key component of good OSINT tradecraft. Identifying information such as the time of day most users are active on a website, the countries that most users are visiting from, the types of browsers and operating systems users primarily access the website from, and the websites that users are primarily coming from to reach the website (Fuller, 2025. These are just a handful of the types of information you can glean from a data analytics website, such as Similarweb, that will help in refining your tradecraft for a specific OSINT collection activity. Although using tradecraft to collect OSINT is not a novel concept within the intelligence community, too many other OSINT practitioners are apparently unaware of how to perform it correctly, or of its criticality in certain collection scenarios. An examination of OSINT literature reveals this deficiency.

As Weinbaum (2024) observed, though, tradecraft is "substantively different" for HUMINT, SIGINT, and OSINT (p. 3). Intelligence community and Department of Defense (DoD) publications make scant reference to OSINT collection tradecraft, and do not define what it is. For example, DoD Joint Publication 2-0 (2019), which "provides the doctrinal foundation and fundamental principles that guide joint and national intelligence products, services, and assessments" (Joint Publications, 2025). DoD Joint Publication 2-0 only refers to tradecraft in the context of OSINT by stating that, “OSINT is susceptible to manipulation and deception, and thus requires tradecraft and review during processing” (Weinbaum, 2024, p. 21). The NATO Open Source Intelligence Handbook (2001) is a 57-page guide that “provides preliminary joint and coalition training information on the subject of Open Source Intelligence” (NATO, p. 3). The word tradecraft does not appear once in this document. The Special Operations Forces Open Source Intelligence (OSINT) Handbook, published in 2004, contains 21 references to tradecraft in 125 pages (Steele, 2004). However, all references are to analytic tradecraft, rather than collection tradecraft (Steele, 2004).

Similarly, there is very little written in books and scholarly journals about OSINT collection tradecraft. For example, the Open Source Intelligence Tools and Resources Handbook (2020) is a 510-page-long eBook about OSINT that does not once mention the word tradecraft (Bielska, 2020). Similarly, Open Source Investigations in the Age of Google (2024), a 388 page edited book on OSINT, does not identify OSINT tradecraft as a topic, does not list the word “tradecraft” in its index, and in fact only mentions the word tradecraft four times in the entire book. Not one of the articles in the book define what tradecraft means, how it is used, or provide examples of its use by OSINT practitioners (Wilson, 2024). Mercyhurst faculty train CIRAT team students on why OSINT tradecraft is necessary and how to perform it successfully to mitigate risk; the weight faculty places on tradecraft is evidenced by how CIRAT describes OSINT, which includes the phrase, “Mitigating all technical and topical risk” (Fuller, 2025).

Legal and Ethical OSINT

OSINT practitioners must pay attention to “protecting the privacy of individuals in the course of investigations” (Mercado, 2024). Weinbaum (2024) argued that intelligence officers have an ethical responsibility to use tradecraft that “transcends military or civilian affiliation, rank or seniority, employment status (contractor versus government personnel), intelligence discipline, and intelligence career field” (p. 1). In addition to having the responsibility to use tradecraft themselves, intelligence officers also have an obligation to point out when tradecraft is “being used poorly, or not at all; and to teach and mentor all who ask for help or do not know to ask” (Weinbaum, 2024, p. 1). Ethics are a key component of CIRAT OSINT work: “All CIRAT team members must sign End User Agreements that explain ethical behavior before conducting any OISNT research or collection” (Fuller, 2025).

Results

What makes Mercyhurst’s CIRAT unique in the OSINT world is that its team members are trained in seven essential skills that enable them to acquire open-source intelligence capably, securely, legally, and ethically. Those skills are:

- Knowing what they are supposed to be researching or collecting in answering defined, priority intelligence requirements;
- Knowing where and how to search for the information needed;
- Knowing what tools they can leverage to enable particular types of collection;
- Knowing how to properly and safely employ those tools;
- Knowing when and how to properly use managed attribution;
- Knowing what OSINT and HUMINT tradecraft is, and how to employ tradecraft to mitigate risk while searching for open-source information;
- Knowing what is ethically and legally permissible in OSINT collection based on clients' policies, regulations, and national and international laws (Fuller, 2025).

Not all OSINT practitioners in other environments receive the same level of thorough training and monitoring. As Tucker and Robson-Morrow (2025) concluded, "Open-source intelligence is an increasing focus in intelligence studies; however, little systematic attention has been paid to the vendors that collect, analyze, and operationalize intelligence outside of classified national security environments" (p. 1).

Conclusions

OSINT's technology-driven evolution has created seemingly endless opportunities for open-source intelligence collection while concurrently leading to the proliferation of individual OSINT researchers and organizations both inside the government and in the private sector and overseas. While second-generation OSINT offers many new opportunities for the collection of PAI, CAI, and grey literature, it also presents risks to unwitting OSINT collectors, networks, and their organizations, especially those conducting online research on Tier 1 and Tier 2 websites. For over 25 years now, Mercyhurst's CIRAT program has systematically taught its OSINT practitioners how to correctly and effectively use specialized tools and tradecraft to mitigate those risks and perform their collection tasks safely, ethically, and legally. This qualitative study revealed the value of not only providing students with foundational knowledge about OSINT tools, tactics, techniques, and procedures but also adequately and consistently supervising them to ensure they acquire the tactic knowledge required to perform OSINT effectively, efficiently, safely, and legally.

References

Arora, S. K., Li, Y., Youtie, J., & Shapira, P. (2016). Using the wayback machine to mine websites in the social sciences: A methodological resource. *Journal of the Association for Information Science and Technology*, *67*(8), 1904-1915.

Baffa, R. (2025). The Ukraine-Russia war confirms the value of OSINT. *Babelstreet*, https://www. babelstreet.com/blog/the-ukraine-russia-war-confirms-the-value-of-osint

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.

Barrows, H. A. (2019). OSINT: The need for an open-source intelligence workforce. *Marine Corps Gazette*, 34-36.

Bernier, J. (2021). "The Pentagon's first financial war: How DoD can fight back against China." *PRISM 9*(3), p. 34-49.

Bielska, A. (2020). *Open Source Intelligence Tools and Resources Handbook*. I-Intelligence GmbH.

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

Bryant, C. M. (2024). *Out in the Open: US GEOINT and OSINT in the Cold War 1946-1986*. Harvard University.

Cohen, D., Elalouf, A., & Citrinowicz, D. (2025). Uncovering Salafi jihadist terror activity through advanced technological tools. *Journal of Policing, Intelligence and Counter Terrorism*, 1-17.

Dvojmoč, M. (2019). Corporate intelligence as the new reality: The necessity of corporate security in modern global business. *Journal of Criminal Justice and Security*, (2), 205-223.

Fleisher, C. S. (2008). Using open source data in developing competitive and marketing intelligence. *European journal of marketing*, *42*(7/8), 852-866.

Fuller, B. (11 April 2025). "Safeguarding CIRAT researchers." Face-to-face interview at Mercyhurst University.

Heibel, B. (13 April 2025). Face-to-face interview.

Hassig, D. (1987). U.S. Joint Publications Research Service translations: A user's manual. *Government Publications Review, 14*(5), 559-572. DOI: https://doi.org/10.1016/0277-9390(87)90053-7

Hulnick, A. S. (2002). The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence 15:* p. 565-579

Li, W., Wang, C., Cui, X., Liu, Z., Guo, W., & Cui, L. (2025). COSINT-Agent: A knowledge-driven multimodal agent for Chinese open source intelligence. *arXiv preprint arXiv:2503.03215*.

Jennings, B. (2010). Facebook and the social network phenomenon. *UWIRE Text*, 1-1.

Khan, M. (2021). *The Role of Intermediaries in Shaping Fair Use*. University of California, Berkeley.

Managed Attribution. (2025). *Authentic8*, https://www.authentic8.com/glossary/what-is-managed-attribution

Mercado, S. (September 2024). "Open source investigations in the age of Google." *Studies in Intelligence 68*(3), p. 51-52.

"Mercyhurst Intelligence team presents findings during ODNI Conference in Washington D.C." (18 September 2008). *Mercyhurst College*, http://intel.mercyhurst.edu/content/09192008

Monday, M. (2022). "Can OSINT be saved? Civilians, and a new Open Source Center may resurrect it." *American Intelligence Journal 39*(1), p. 149-156.

NATO Open Source Intelligence Handbook. (November, 2001). NATO

"ODNI Senior Advisory Group Panel Declassified Report on Commercially Available Information." (27 January 2022). *U.S. Office of the Director of National Intelligence*. https://www.dni.gov/files /ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

OSINT Operations: Analyzing the Information Domain. (2025). *Ntrepid*, https://ntrepidcorp.com/missions/osint/

Roop, J. E. (1969). *Foreign Broadcast Information Service History, Part I, 1941-1947*: Central Intelligence Agency Langley, VA.

Serscikov, G. (2024). "Grey literature in the intelligence domain: twilight or revival?" *Intelligence and National Security 39*(6), p. 1028-1050.

Steele, R. D. (2004). *Special Operations Forces Open Source Intelligence Handbook*. OSS International Press.

Sultana, J., & Jilani, A. K. (2021). Exploring and analysing surface, deep, dark web and attacks. *Security Incidents & Response Against Cyber Attacks*, 85-96.

Tradecraft. (2025). *Authentic8*, https://www.authentic8.com/glossary/what-is-tradecraft

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.

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. (2024). "Intelligence officers have an ethical responsibility to use tradecraft." *International journal of intelligence and CounterIntelligence*, p. 1-22. DOI: 10.1080/08850607.2024.2381999

Wilson, H., Samuel, O., & Plesch, D. (2024). *Open Source Investigations in the Age of Google* (p. 388). World Scientific Publishing Company.

Yeboah-Ofori, A., & Brimicombe, A. (2018). Cyber intelligence and OSINT: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *7*(1), 87-98.

Young, J. R. (2023). Working smarter: On a mission to make the complex seem simple. Ntrepidcorp, https://ntrepidcorp.com/uploads/2023/08