National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

AVOIDING THE INCREMENTALIST TRAP: THE CASE FOR INSTITUTIONALISING OPEN SOURCE INTELLIGENCE AS A JOINT CAPABILITY

Lieutenant-Colonel Neil A. McPhedran

JCSP 50

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

AVOIDING THE INCREMENTALIST TRAP: THE CASE FOR INSTITUTIONALISING OPEN SOURCE INTELLIGENCE AS A JOINT CAPABILITY

Lieutenant-Colonel Neil A. McPhedran

AVOIDING THE INCREMENTALIST TRAP:
THE CASE FOR INSTITUTIONALISING OPEN SOURCE INTELLIGENCE AS A JOINT CAPABILITY

AIM

1. The aim of this service paper is to analyse the value of open source intelligence (OSINT) in the contemporary operating environment and consider whether the Canadian Armed Forces (CAF) is taking the appropriate steps to ensure that its use is optimized in support of current and future needs. It will suggest that current approaches remain overly *ad hoc* and recommend that Canadian Forces Intelligence Command (CFINTCOM) seize the opportunity which the present moment represents to develop a strategy which recognises and resources OSINT as a foundational intelligence discipline on par with that of other traditional disciplines. It is posited that this would have the dual benefit of both ensuring the establishment and maintenance of a robust capability postured to enable elements across the joint force, while also reducing the burden on the operational commands and environmental services whose current disaggregated efforts risk detracting from other priorities.

INTRODUCTION

2. Throughout its history the essential task of military intelligence (MI) has remained constant- providing commanders with the required assessments on enemy, weather, terrain and civil considerations needed to achieve a decision advantage over their adversaries.[1] Yet while this fundamental nature remains unchanged, the character of core supporting collection disciplines have evolved over time, often as a result of technological change. And while many such advances have been largely evolutionary, such as that seen with the progress of imagery intelligence (IMINT) from the early aircraft of the First World War to the variety of sensors and geographic information systems that now make up today's broader geospatial intelligence (GEOINT) category,[2] OSINT has experienced truly revolutionary change since the dawning of the information age. In many ways this change continues to befuddle many in the MI and wider Intelligence Community (IC),[3] while at the same time representing a strategic opportunity of critical importance to the future flourishing of the function.

3. The reasons for these difficulties are both numerous and at times complex, and begin with what remains an ongoing struggle to update understandings of OSINT and its component parts. For the purposes of this paper, a combination of definitions will be

[1] Robert R. Glass and Philip B. Davidson, *Intelligence is for Commanders*. (Harrisburg: Military Service Publishing Company, 1948).
[2] Susan Henrico and Dries Putter, "Intelligence Collection Disciplines—A Systematic Review," in *Journal of Applied Security Research* (Jan 2024): 1.
[3] Bowman H. Miller, "Open Source Intelligence (OSINT): An Oxymoron?" in *International Journal of Intelligence and Counter-Intelligence*, 31:4 (2018): 702.

drawn upon with the intent of establishing a common baseline. First is that of OSINT itself, defined succinctly in an early journal article on the subject by Robert Steel as intelligence "based on information which can be obtained legally and ethically from public sources."[4] Second is to consider what such public sources consist of, namely publicly available information (PAI), and noting that this also includes purchased commercially available information (CAI) as well as other recently coined "ints" such as social media intelligence (SOCMINT) and other various new sources of data.[5] Finally, before progressing further it also behooves us to underscore the rapidity of ongoing change in this space, with information and data sources continuing to proliferate at exponential rates and increasingly overlapping with other disciplines which had previously be in the exclusive domain of governments, including signals intelligence (SIGINT).[6] Even at such a cursory level it becomes possible to appreciate why traditional and bureaucratic organisations such as the military have struggled to adapt at the speed and scale needed fully address such change and thus continue to lag behind the private sector.

DISCUSSION

OSINT's Coming of Age

4. As has already been mentioned above, the existence of OSINT is far from new despite the renewed interest and at times associated confusion which has resulted from its increasing prominence (and complexity) since the term was first coined in the early 1990s. Going back to the advent of modern industrialised war in the late 19th and early-20th Centuries, MI has included the use of PAI, such as media and academic publications, to assist in the production of multi-source intelligence, with examples going back as far as the US Civil War if not further.[7] Yet while the intelligence derived from such open sources has always been of value, its relative importance in relation to classified sources has increased markedly as a result of both advances in modern information technology as well as the increasing need to share intelligence with partners and wider populations as a means to compete in the modern pan-domain operational environment.[8] In this respect the ongoing conflict in Ukraine represents a particularly prescient case study and one which is both familiar and often used to bolster arguments in favour of increased investments in OSINT.

---

[4] Robert D. Steele, "The importance of open source intelligence to the military," in *International Journal of Intelligence and Counter-Intelligence*, 8:4 (1995): 457.
[5] Corrine Geiger, "The Reawaking of Open-Source Intelligence," in *Military Intelligence Professional Bulletin, 48:1* (April 2022): 10.
[6] Cortney Weinbaum, Steven Berner and Bruce McClintock, "SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain," *RAND Corporation Perspectives (Online*), 2017: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE273/RAND_PE273.pdf
[7] Ludo Block, "The long history of OSINT," in *Journal of Intelligence History* (June 2023): 5.
[8] Brian Cheng, Scott Fisher and Jason C. Morgan, "Find It, Vet It, Share It: The US Government's Open-Source Intelligence Problem and How to Fix It," in *Modern War Institute (Online),* March 24, 2023: https://mwi.westpoint.edu/find-it-vet-it-share-it-the-us-governments-open-source-intelligence-problem-and-how-to-fix-it/

5. Over approximately the past thirty years this change has been rapid with regard to both the volume of PAI as well as the technological means available for processing and analysis (and of which automated translation and machine learning are but two examples).[9] Unlike during the earlier industrial age, when OSINT tended to be focused on news and media sources that could be accessed either in hardcopy or via local broadcast, such information and data can now be accessed globally either for free or at a cost. In addition, these traditional sources have expanded to include a range of formats previously unknown, such as that coming from social media and other commercial sources of data which challenge conventional understandings of PAI.[10] Furthermore, these sources continue to multiply without any indication of this changing for the foreseeable future, something which our adversaries have already seized on and are leveraging for their advantage at industrial scale.[11]

OSINT in the CAF Today

6. To date the CAF's approach to this change in the open source information environment brought on by the internet has been both incremental and driven by the competing challenges of meeting operational needs while also addressing valid concerns such as those related to personal privacy and operational security (OPSEC). Following what were presumably initial forays into the changing information space by MI staffs at all levels and for which there are limited available historical sources, the first evidence of a centralised joint effort was the establishment of CFINTCOM's now named Open Source Intelligence Operational Support Team in the early-2000s. This team appears to have functioned largely as a service provider of PAI of potential intelligence value, particularly with respect to a variety of media and other subscription services.[12] In time this effort came to be augmented by the addition of departmental policy, including the Chief of Defence Intelligence (CDI) functional directives (FDs) on OSINT Activities on the Internet (OAI) and the Handling and Protection of Canadian Citizen Information, as well as the establishment of associated minimum training standards.[13] While such initiatives have been useful in helping codify requirements and associated authorities for the conduct of OAI, both limited institutional expertise and continued rapid change in technology and available sources of data have seen these efforts struggle to keep pace with operational requirements.

7. Looking beyond CFINTCOM, the CAF's two operational commands, Canadian Joint Operations Command (CJOC) and Canadian Forces Special Operations Command

[9] Geiger, "The Reawaking of Open-Source Intelligence," 11.
[10] United States Government, "Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information," 27 January 2022.
[11] Ron Penninger, "Operationalizing OSINT Full-Spectrum Military Operations," in *Small Wars Journal (Online)* (Jan 2019): https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations
[12] David Holtz and Angela Maxwell, "Open Source Intelligence in the Canadian Intelligence Community," in *Military Intelligence Professional Bulletin*, 48:1 (April 2022):13.
[13] 6th Canadian Combat Support Brigade Standing Orders, "Open Source Intelligence Activities on the Internet," 20 September 2023.

(CANSOFCOM), as well as the three environmental services, appear to have largely been left to their own devices to navigate this now defined policy space. Antidotal evidence, the full discussion of which is beyond the scope of this paper, indicates that this experience has been mixed on account of a variety of factors. Particularly illustrative of the current state of affairs is the approach that the Canadian Army (CA) has taken to OAI in recent years. Largely lacking a clear force employment mandate yet nevertheless increasingly expected to force generate personnel and teams capable of conducting OAI, in 2022 the CA released a dedicated OAI Concept of Operations (CONOP) aimed at codifying the standards, authorities and processes needed to ensure compliance with the previously referenced CFINTCOM FDs.[14] While arguably necessary to hedge in the absence of a wider CAF strategy, challenges with operationalising this direction across intelligence staffs and units, both regular force and reserve, provides a cautionary tale with respect to the difficulties in seeking to add new and complex capabilities in the absence of strategic vision and associated resourcing. At time of writing it appears that 6 Canadian Combat Support Brigade (6 CCSB) and its dedicated MI unit, the Canadian Army Intelligence Regiment (CA Int Regt), are the only elements of the CA that have conducted the necessary staff work to scale this direction down to the tactical level and conduct robust experimentation with the integration of open source data in support of tactical training.[15]

Future Prospects and Potential CAF Way Forward

8. Having considered both the increasing value of OSINT as well as some of the potential challenges in developing associated capability at the operational command and environmental levels, the need appears particularly pressing to consider how this capability might be institutionalised. However daunting, particularly in a resource constrained environment such as the one currently being experienced, it appears inevitable that this will require a dedicated enterprise strategy recognising OSINT as a foundational intelligence discipline worthy of the same level of capability investment currently enjoyed by traditional disciplines. In order to be successful, it is anticipated that this will require dedicated resource allocation to the following focus areas at a minimum:

a. Governance. As both an emergent intelligence discipline and one which poses unique challenges with respect to data and information acquisition, management of both holdings and requirements across the Defence Intelligence Enterprise (DIE) and wider IC, sensitive privacy considerations, collaboration with private industry, and overlap with other intelligence disciplines,[16] centralised oversight of CAF OSINT is increasingly important to both leveraging its potential and avoiding possibly costly mistakes. Meeting

[14] Canadian Army, "Open-Source Intelligence Activities on the Internet (OAI) Concept of Operations (CONOPS)," 7 December 2022.
[15] 14 Military Intelligence Company, "Exercise Order: Hunting Dragon," November 24, 2023.
[16] Robert Ashley, Harry Kemsley and Sean Corbett, "OSINT in support of the Defence Intelligence Enterprise (DIE)- Parts One and Two," in *Janes The World of Intelligence Podcast* (3 and 10 October 2023).

this challenge will require increased investment in governance under the functional authority of CDI in order to both oversee CAF activities and well as pursue alignment with other government departments, allies and partners. In many ways this parallels what is already in place within CFINTCOM's Director General Intelligence Policy and Partnerships with respect to more mature disciplines,[17] indicating that the addition of another staff element dedicated to OSINT may make for a natural organisational fit.

b. Ownership. Maturation of OSINT into a foundational intelligence discipline as is being argued for here will require the ability to force develop, force generate, force manage, force sustain, and force employ in a deliberate manner and again in a way similar to other intelligence disciplines that are already represented by specialised units. Expanding the current Open Source Intelligence Operational Support Team within CFINTCOM to full unit status and with resourcing to also function as the CAF's OSINT Centre of Excellence would be a logical start point for such an effort while also potentially helping establish the CAF as a leader amongst allies in this space. Again, already established units like Joint Task Force X (JTFX) and the Canadian Forces Joint Imagery Centre (CFJIC) represent potential models for emulation, including with respect to the manner in which they are able to manage various functions including fielding and equipping standardised groupings for integration as part of modular and deployable intelligence centres. And while such unit comparisons may in many ways be apt, it would also be a mistake to overlook potential areas for experimentation noting that such a unit many also offer unique opportunities for a leveraging a dispersed workforce.[18]

c. Professional Development. Realisation of the vision being outlined here is likely to require a variety of adaptations to training and education, including increased attention to OSINT as part of both intelligence officer and non-commissioned member (NCM) career courses, specialist qualifications for members posted into OSINT collection and analysis positions, as well as standardised refresher training likely in the form of intelligence specific individual battled task standards (IBTS), primary combat function (PCF) or pre-deployment training (PDT). The potential necessity of establishing a dedicated NCM trade may also be worthy of consideration.

---

[17]Government of Canada. "Canadian Forces Intelligence Command," Accessed February 15, 2024: https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-forces-intelligence-command.html

[18] Chris Rasmussen, "Avoiding the Secrecy Trap in Open Source Intelligence," in *The Cipher Brief (Online),* 21 March 2023: https://www.thecipherbrief.com/column_article/avoiding-the-secrecy-trap-in-open-source-intelligence

Risks of Inaction

9. It is recognised that many if not all of the above recommendations will be seen by some as unwelcome, particularly coming at a time when personnel and financial constraints are already presenting significant challenges for existing elements of the DIE. That said, a brief survey of the current and projected operational environment suggests a growing array of risks associated with inaction, with the following being perhaps the most pressing:

a. Failure to Respond in Support of the Pan-Domain Operating Concept (PFEC). One of the most immediately evident implications of the PFEC for the DIE is that the associated campaigning mindset will require increased intelligence support to information operations at the strategic, operational and tactical levels, as well as growing collaboration with non-traditional partners.[19] This reality will place increased importance on unclassified and rapidly releasable products leveraging OSINT. Doing this effectively will demand robust governance and nuanced capability without which the intelligence function's ability to support institutional requirements can be expected to suffer.

b. Erosion of Core Intelligence Tradecraft Required for Large Scale Combat Operations (LSCO). Unlike in the case of the operations which have defined many the CAF's expeditionary deployments over the past thirty years, it would be unrealistic to believe that in the case of LSCO tactical elements at division and below will benefit from co-location with the sort of fusion centres which were commonplace in Afghanistan and Iraq. With such general intelligence support increasingly vulnerable to disruption by long-range precision fires and a contested electro-magnetic environment, close intelligence support at the tactical level is likely to demand both depth and breadth from a smaller number of highly trained and capable intelligence personnel.[20] Having these personnel and associated staffs, most of whom reside within tactical formations and units, overleveraged against OSINT capability development detracts from this focus at a time when the risks of doing so are increasingly severe.

c. Increased Exposure to Hostile Intelligence, Legal and Reputational Risk. Finally, unlike in the days when conducting OSINT might look like buying a newspaper or signing out a book, OAI involves operating on a

[19] Potter and Bembenek, "The Risks of Not Knowing," 7.
[20] Jack Watling, "Preparing Military Intelligence for Great Power Competition," in *The RUSI Journal*, 166:1 (2021): 70-72.

two-way range in which operators are vulnerable to cyber threats, misinformation and disinformation, and a murky conceptual and ethical environment which is ripe for exploitation by hostile actors.[21] Having MI personnel operating in this space without the necessary training, systems and oversight during an age of great power competition and potential conflict is to court disaster, yet in the absence of deliberate choices the unauthorised assumption of this type of risk may become increasingly inevitable.

CONCLUSION

10. Over the course of this paper it has been argued that the importance of OSINT in relation to other intelligence disciplines critical to the MI function has been increasing for several decades and will almost certainly continue to do so for the foreseeable future. This assessment is borne out by a multitude of historical examples and has been made all the more evident in view of the conduct of ongoing global competition and conflicts. Yet despite these undeniable trends, OSINT remains under resourced in many Western militaries, including the CAF, as they struggle to transition from mechanised to "informationalised" concepts of war while at the same time being disrupted by technological change and personnel pressures. With the risks of the status quo mounting, the current pace of change is no longer acceptable and as such functional leadership from CFINTCOM in needed to ensure course is set towards an enterprise strategy which postures the CAF to seize this opportunity and potentially help scale it across the Government of Canada in support of national security priorities.

[21] Michael J. Rasak, "Event Barraging and the Death of Tactical Open-Source Intelligence," in *Military Review* (Jan-Feb 2021): 48.

BIBLIOGRAPHY

Allen, T.S. "Open-Source Intelligence: A Double-Edged Sword." *Proceedings*, 144:8 (Aug 2018): https://www.usni.org/magazines/proceedings/2018/august/open-source-intelligence-double-edged-sword

Ashley, Robert, Harry Kemsley and Sean Corbett. "OSINT in support of the Defence Intelligence Enterprise (DIE)- Parts One and Two." *Janes The World of Intelligence Podcast* (3 and 10 October 2023).

Block, Ludo. "The long history of OSINT." *Journal of Intelligence History* (June 2023): 1-15.

Canadian Army. "Open-Source Intelligence Activities on the Internet (OAI) Concept of Operations (CONOPS)." 7 December 2022.

Cheng, Brian, Scott Fisher and Jason C. Morgan. "Find It, Vet It, Share It: The US Government's Open-Source Intelligence Problem and How to Fix It." *Modern War Institute*, March 24, 2023. https://mwi.westpoint.edu/find-it-vet-it-share-it-the-us-governments-open-source-intelligence-problem-and-how-to-fix-it/

Colquhoun, Cameron. "A Brief History of Open Source Intelligence." *Bellingcat*, July 14, 2016. https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

14 Military Intelligence Company, Canadian Army Intelligence Regiment. "Exercise Order: Hunting Dragon." November 24, 2023.

Gack, Jarrod R. "The Open-Source Intelligence Conundrum: Creating the Discipline or Integrating the Data?" *Military Intelligence Professional Bulletin*, 48:1 (April 2022): 17-22.

Geiger, Corrine. "The Reawaking of Open-Source Intelligence." *Military Intelligence Professional Bulletin*, 48:1 (April 2022): 10-12.

Glass, Robert R. and Philip B. Davidson. *Intelligence is for Commanders*. Harrisburg: Military Service Publishing Company, 1948.

Government of Canada. "Canadian Forces Intelligence Command." Accessed February 15, 2024. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-forces-intelligence-command.html

Henrico, Susan and Dries Putter. "Intelligence Collection Disciplines—A Systematic Review." *Journal of Applied Security Research* (Jan 2024): 1-25.

Holtz, David and Angela Maxwell. “Open Source Intelligence in the Canadian Intelligence Community.” *Military Intelligence Professional Bulletin*, 48:1 (April 2022):13-16.

Miller, Bowman H. “Open Source Intelligence (OSINT): An Oxymoron?” International Journal of Intelligence and Counter-Intelligence, 31:4 (2018): 702-719.

Penninger, Ron. “Operationalizing OSINT Full-Spectrum Military Operations.” *Small Wars Journal* (Jan 2019): https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations

Potter, Laura and Christina Bembenek. “The Risks of Not Knowing: Enabling Intelligence Professionals to Leverage Publicly Available Information.” *Military Intelligence Professional Bulletin*, 48:1 (April 2022): 5-8.

Rasak, Michael J. “Event Barraging and the Death of Tactical Open-Source Intelligence.” *Military Review* (Jan-Feb 2021): 48-57.

Rasmussen, Chris. “Avoiding the Secrecy Trap in Open Source Intelligence.” *The Cipher Brief* (21 Marcy 2023): https://www.thecipherbrief.com/column_article/avoiding-the-secrecy-trap-in-open-source-intelligence

6th Canadian Combat Support Brigade Standing Orders. “Open Source Intelligence Activities on the Internet.” 20 September 2023.

Skilling, Matthew D. “Mapping the Information Environment with Open-Source Intelligence and Allies.” *Military Intelligence Professional Bulletin*, 48:1 (April 2022): 27-29.

Steele, Robert D. “The importance of open source intelligence to the military.” *International Journal of Intelligence and Counter-Intelligence*, 8:4 (1995): 457-470.

United States Government. “Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information.” 27 January 2022.

Weinbaum, Cortney, Steven Berner and Bruce McClintock. “SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain.” RAND Corporation Perspectives (2017): https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE273/RAND_PE273.pdf

Watling, Jack. “Preparing Military Intelligence for Great Power Competition.” *The RUSI Journal*, 166:1 (2021): 68-80.