# OPEN-SOURCE INTELLIGENCE IN THE CANADIAN INTELLIGENCE COMMUNITY

BY

Lieutenant-Colonel David Holtz,
Canadian Army,
and Ms. Angela Maxwell,
Canadian Forces Intelligence Command

## Introduction

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

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

## OSINT Requirements and Sources

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

These unclassified OSINT daily regional updates enable intelligence professionals and operators to maintain general regional situational awareness and, in some cases, to inform all-source classified intelligence product development. With some additional processing, the OSINT daily product can enable further all-source production in the form of high-quality stand-alone products that offer critical inputs to decision makers. CFINTCOM's regional OSINT daily updates are one way our community is leveraging the open-source domain to enable tactical to strategic effects. OSINT analysts are responsible for converting and refining the collected information; they process, exploit, and disseminate (PED) the initial information for further analysis or report it directly as single-source intelligence. The use of the PED process in OSINT is a relevant technique and procedure ensuring commanders and staffs receive critical information that will enable decision making.

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

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

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

## Dissemination of the OSINT Daily Product

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

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

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

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

The OSINT daily product is also helpful as a catalyst for "breaking the ice" in awkward situations when intelligence professionals want to discuss an area of intelligence interest but the classified products are not yet available for dissemination outside of the national production chain. Analyst-to-analyst discussions with allies and partners are easier if an open-source product is available as the centerpiece for discussion. The sharing of ideas can be framed on open-source information while waiting until the classified material is available to be shared in the form of a releasable product.


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

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

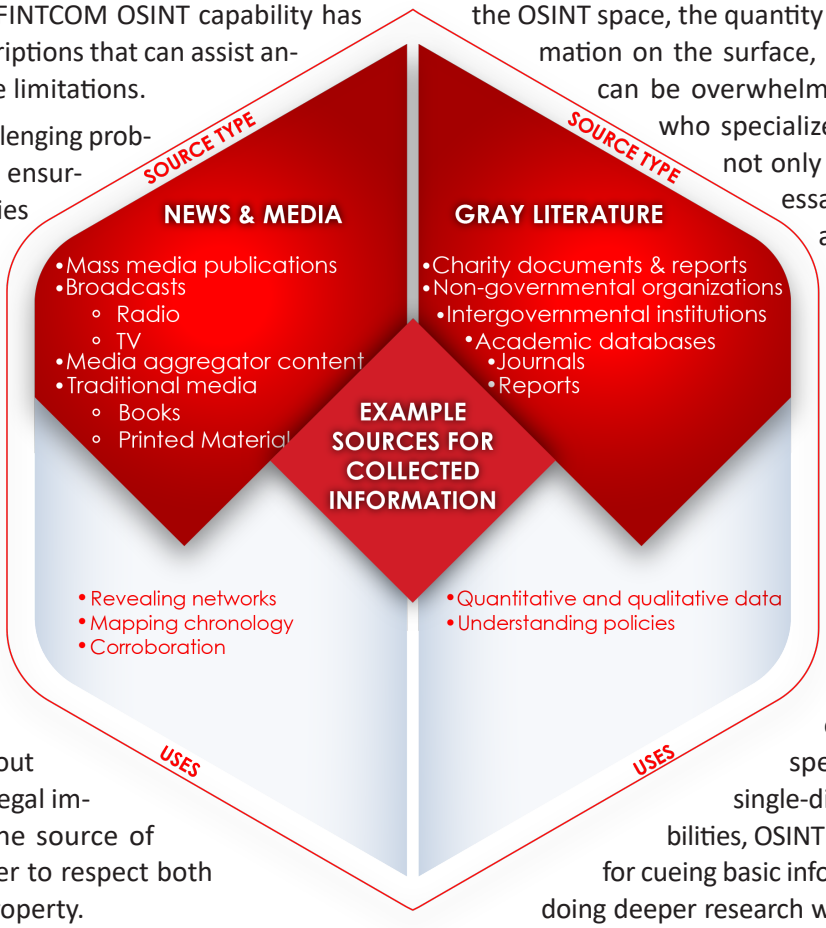
## Challenges of Online Intelligence Collection

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

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

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

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




## OSINT Analysis

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

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

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

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

## Conclusion

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

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

**Endnote**

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

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

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


## Publicly Available Information

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

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