INTELLIGENCE ASSESSMENT SECRETARIAT | SECRÉTARIAT DE L'ÉVALUATION DU RENSEIGNEMENT

THE FUTURE OF OPEN SOURCE INTELLIGENCE (OSINT) IN THE CANADIAN INTELLIGENCE COMMUNITY

PROTECTED B

APRIL 2023

Analyst: / Graphics:

VISION STATEMENT: A MORE COORDINATED AND ENHANCED APPROACH TO OPEN SOURCE INTELLIGENCE CAPACITIES AND CAPABILITIES WITHIN THE CANADIAN INTELLIGENCE COMMUNITY.

CONTEXT

Recent events have revealed gaps, vulnerabilities, and opportunities for the Canadian Intelligence Community (IC) to effectively leverage open source intelligence (OSINT), while also highlighting the significance of publicly available information (PAI) in identifying threats and developing intelligence pictures. The Public Order Emergency Commission report notes that the Government acknowledged concerns related to our ability to properly monitor and collect open-source information, including from social media, as well as the absence of a legislative framework and the lack of necessary tools to engage in this type of collection.

The vast amounts of accessible open source data provides greater opportunity for government and non-governmental entities to **leverage PAI for OSINT efforts that support intelligence operations, assessment, and decision making advantage**.

CONSIDERATIONS

The Canadian IC must ensure it adheres to applicable **legal and policy requirements**, respecting the Canadian Charter of Rights and Freedoms and adhering to the Privacy Act. Intelligence activities, including leveraging PAI for OSINT purposes, must have an appropriate legal authority and be conducted in line with policies and procedures that ensure appropriate use and compliance.

The goals and problems identified within each pillar often **converge**. For example, public-private partnerships cross People, Process, Tools & Technology, and Authorities pillars, depending on its framing.

There are additional considerations depending on the type of intelligence, such as whether OSINT activities are in support of **threat intelligence, strategic intelligence, investigative intelligence, or information warfare.** Enhanced OSINT capabilities will need to address these various types of activities.

Other **Five Eyes countries** have developed OSINT programs that address some of the outlined goals, which the Canadian IC should examine when developing its own approach.

PROCESS

DEFINITIONS

GOAL:
Determine whether a community-wide definition for OSINT and PAI is necessary across the Canadian IC that guides OSINT activities and scope.

PROBLEM STATEMENT:
There is no common definition for OSINT and PAI, which fragments what constitutes OSINT across the IC. For example, research conducted in support of intelligence analysis is sometimes considered OSINT. There are different types of OSINT activities (e.g. social media monitoring versus dark and deep web harvesting). Additionally, there is a difference between the collection and analysis of PAI for OSINT, which complicates the interpretation of OSINT activities. At the same time, a community held definition should not restrict ongoing OSINT efforts within the IC.

COORDINATION & COLLABORATION

GOAL:
Align OSINT efforts and intelligence requirements and priorities across the community and with partners.

PROBLEM STATEMENT:
There is no clear coordination amongst the Canadian IC that supports Canada's OSINT functions as it relates to mapping responsibilities or lines of effort. For example, Canadian representation in some Five Eyes OSINT discussions have not been a community-wide effort.

REQUIREMENTS

GOAL:
Ensure that OSINT activities properly reflect the intelligence requirements and priorities.

PROBLEM STATEMENT:
Intelligence requirements and priorities across mandates demand different responses, and thus different OSINT analytical workflows. For example, intelligence analysts require different OSINT tradecraft depending on respective files and functions (i.e. strategic versus tactical intelligence analysis).

AUTHORITIES

POLICY & LEGISLATION

GOAL:
Map current authorities across the community that could enable OSINT functions. Consider policy or legislative changes that could address OSINT limiters.

PROBLEM STATEMENT:
It is unclear if existing policies and governance structures can address OSINT requirements or gaps, or if additional legislation is required, similar to those put forward by Five Eyes counterparts like Australia.

INFORMATION SHARING

GOAL:
Develop ways to establish greater information sharing and dissemination practices related to OSINT activities—including data, information, and analysis—between and amongst departments, with senior officials and decision makers including Cabinet Ministers, and with foreign partners.

PROBLEM STATEMENT:
There is limited information sharing and dissemination protocols to share OSINT data and/or products with other departments, senior officials, and foreign partners in a timely and efficient way. This is related to varying information and privacy restrictions, access requirements to specific types of data, capacity issues, and unclear parameters regarding what can be shared and/or requested between and amongst relevant stakeholders.

PEOPLE

TRAINING

GOAL:
Standardize and streamline processes for appropriate OSINT training as it relates to specific OSINT activities.

PROBLEM STATEMENT:
Some departments have adequate training for personnel on OSINT activities, including in-house or commercially available courses. However, sometimes these programs are ad hoc and unable to meet demand, depending on the type of training required. For example, there are resource capacity concerns to administrating training for authorized analysts conducting OSINT that requires to access publicly available platforms.

PARTNERSHIPS

GOAL:
Identify whether (inter)department internal branches or groups could bolster OSINT efforts under current policy authorities and departmental mandates, or if further human resources dedicated to OSINT are required.

PROBLEM STATEMENT:
It is not clear if other branches within departments can assist the IC in addressing OSINT concerns under their authorizations. For example, internal services such as Communications Directorates have the authority to monitor social media for trends and sentiments, which could support intelligence efforts under preexisting data governance structures.

GOAL:
Enhance public-private partnerships (3P) that could fulfill OSINT requirements.

PROBLEM STATEMENT:
Industry and nongovernmental partners have greater capacity and capability to provide reflexive and agile solutions to OSINT functions—including but not limited to tools, technology, and training—which the IC has not yet effectively leveraged. Additionally, emerging technologies expand and adapt at rates that Government of Canada systems cannot maintain.

TOOLS & TECHNOLOGY

PROCUREMENT

GOAL:
Develop a strategic approach to services, tools, and technology procurement.

PROBLEM STATEMENT:
It is unclear what tools and databases are most relevant for respective OSINT activities (ranging from strategic to tactical activities) across the IC, either internally or externally available. It is not known between departments which commercial tools have been considered, vetted, adopted, or rejected, depending on their relevance to fulfilling specific OSINT needs. Additionally, it is unclear if terms for the acquisition of tools could be negotiated on behalf of all departments interested in such products.

PROBLEM STATEMENT:
There are barriers to the acquisition and adoption of commercial tools, including vetting and obtaining such products, as well as legal barriers and cost considerations. For example, there are vast amounts of commercial tools available and the process of identifying, vetting, and trialing a commercial product can take several months. The acquisition of such a tool following a trial period may take even longer.

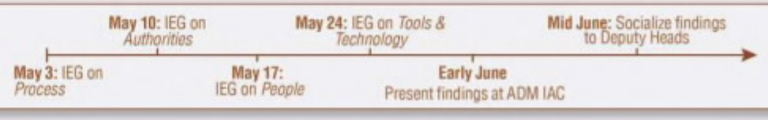
PROCESSING

GOAL:
Identify adequate processing and automation system—including storage and custodianship—that streamline PAI data for OSINT usage (e.g. Big Data and AI analytics).

PROBLEM STATEMENT:
Accessing greater amounts of data for OSINT purposes can hinder analytical workflows when overwhelmed with information if not processed and streamlined appropriately.

CRITICAL PATH

Establish four Interdepartmental Expert Groups (IEGs) addressing each pillar, which will be presented at a future ADM Intelligence Assessment Committee (ADM IAC) meeting and, once approved, socialized to Deputy Heads.



Government of Canada | Gouvernement du Canada
Privy Council Office | Bureau du Conseil privé

Canada