

Canadian OSINT 101: Ethical and Legal Espionage Guide for Independent Canadian Spies and Spymasters

Marie Landry's Spy Shop

March 17, 2025

1 Introduction

Open Source Intelligence (OSINT) is the practice of collecting, analyzing, and interpreting publicly available data from various sources such as news articles, social media, public records, and technical databases. This guide is designed for independent investigators and spymasters who wish to engage in intelligence activities in an ethical and legal manner while adhering to Canadian and international guidelines.

2 Legal and Ethical Considerations

2.1 Canadian Legal Framework

Operating within Canada requires compliance with:

- The **Privacy Act** – Protects personal information from unauthorized collection and use.
- The **Criminal Code of Canada** – Prohibits hacking, unauthorized surveillance, and interception of private communications.
- The **Personal Information Protection and Electronic Documents Act (PIPEDA)** – Regulates the collection, use, and disclosure of personal information by private entities.
- The **Countering Foreign Interference Act** – Strengthens regulations against foreign intelligence operations.

2.2 International Regulations

Intelligence gathering is also governed by:

- The **Universal Declaration of Human Rights** – Protects privacy rights under Article 12.
- The **Budapest Convention on Cybercrime** – Outlines international cybercrime standards.
- The **General Data Protection Regulation (GDPR)** – Governs data protection within the European Union.

2.3 Ethical Guidelines

Ethical OSINT practitioners should:

1. Only collect information from **publicly available sources**.
2. Avoid any form of **hacking** or unauthorized access.
3. Respect **privacy laws** and data protection guidelines.
4. Verify information before using it in decision-making.

3 OSINT Techniques and Tools

3.1 Data Collection

- **Search Engines:** Google Dorking, Bing, Yandex
- **Social Media Intelligence (SOCMINT):** Twitter API, Facebook Graph Search
- **Domain and Network Intelligence:** WHOIS lookup, Shodan, VirusTotal
- **Public Records and Government Databases:** Court records, corporate filings, land registries
- **Deep Web and Dark Web Monitoring:** Tor, Ahmia

3.2 Data Analysis

- **Metadata Analysis:** EXIF tools, FOCA
- **Geospatial Intelligence (GEOINT):** Google Earth, OpenStreetMap, Sentinel Hub
- **Automated OSINT Tools:** Maltego, SpiderFoot, TheHarvester

3.3 Operational Security (OPSEC)

To protect yourself while conducting OSINT investigations:

- Use a **virtual private network (VPN)** to mask your IP.
- Employ **virtual machines** to avoid malware infections.
- Avoid logging in to personal accounts when investigating.
- Utilize **burner emails and phone numbers** for interactions.

4 OSINT in Espionage and Intelligence Work

4.1 Tactical Applications

- **Counterintelligence:** Identifying disinformation and misinformation campaigns.
- **Corporate Espionage:** Monitoring competitors (legally) through open sources.
- **Cyber Threat Intelligence:** Tracking hackers and digital vulnerabilities.
- **Political Intelligence:** Monitoring geopolitical events and actors.

4.2 Case Study: Detecting Disinformation

An OSINT investigation can reveal coordinated disinformation campaigns by:

1. Identifying **bot networks** through unnatural activity patterns.
2. Verifying sources using **fact-checking databases**.
3. Analyzing content metadata for **manipulation indicators**.

5 Best Practices and Resources

5.1 Best Practices

- Maintain **documentation** of all research activities.
- Keep up with **legal changes** regarding OSINT.
- Join professional OSINT communities for collaboration.

5.2 Further Learning

Recommended OSINT courses and resources:

- **The Canadian OSINT Centre** (<https://theosintcentre.ca>)
- **OSINT Framework** (<https://osintframework.com>)
- **I-Intelligence OSINT Training** (<https://i-intelligence.eu>)
- **Government of Canada Open Source Due Diligence Guide** (<https://science.gc.ca>)

6 Conclusion

OSINT is a powerful tool for intelligence gathering when used legally and ethically. Independent spies and spymasters must balance the drive for information with adherence to privacy laws and ethical guidelines. With the right tools, techniques, and operational security measures, one can gather valuable intelligence while maintaining integrity and legality.