Te Pourewa Mātaki
Inspector-General of Intelligence and Security

Open Source Insight New Zealand Conference Keynote Address

18 October 2023

Brendan Horsley – Inspector-General of Intelligence and Security

Note: These are speech notes which informed the speech given and may differ from what was said on the day.

Introduction

Open Source intelligence is generally defined as "the collection, analysis and use of data from openly available sources, for intelligence purposes" and is now largely driven by the development of tools that can simultaneously scan hundreds of sources and platforms. Results can be analysed and displayed quickly and clearly.

Historically OSINT has not been a major focus of intelligence and security agencies. The view that OSINT is of lesser intelligence value compared to classified forms of intelligence such as signals or human intelligence has been institutionally entrenched. More recently, however rapidly increasing data access and processing across a range of technologies and outputs has increased the opportunities of OSINT in both scale and scope. Today information from open sources, compared to classified intelligence, is accessible and less costly to collect. Since the early 2000s it is often estimated that 90 to 95 percent of intelligence comes from open sources.[1]

OSINT continues to evolve and now largely involves the development and use of tools that can simultaneously scan hundreds of sources and platforms. These tools may also include access to datasets obtained through a data broker or from hacked and leaked sources.[2]

---

1 Richard A Best and Alfred Cumming *CRS Report for Congress Open Source Intelligence (OSINT): Issues for Congress* (5 December 2007) https://sgp/fas.org/crs/intel/RL34270.pdf. At 4.

2 Review Committee on the Intelligence and Security Services (CTIVD) *Automated OSINT: tools and sources for open source investigation* (22 December 2021). At 4-5.

Alongside this, the rapid development of Artificial Intelligence and Machine Learning with tools such as Chat GPT may not only further change how people operate online but may greatly increase the capacity of agencies to undertake open source collection and analysis at scale and at speed.

Role of the Inspector-General and open source review

As Inspector-General I provide independent oversight of the activities of the NZSIS and the GCSB. These activities are most often classified in nature, so I have a special role with access to most of the agencies systems. I look at the lawfulness and propriety of the agencies actions. I do this by:

- Conducting Inquiries and reviews into the activities of the agencies
- Receive and investigate complaints
- Review all intelligence warrants and other authorisations that the agencies obtain for activities
- Receive protected disclosures about the agencies and from all other agencies that involve classified information

I do not look at the effectiveness of the agencies activities.

I have a small office, which includes a Deputy IGIS, four investigators and two office support staff.

I publish an annual work programme which sets out the inquiries and reviews that I am conducting in the coming year.

It is timely that I am speaking to you today as my office has been undertaking a review into the NZSIS and GCSB's open source collection activities, which are nearing completion. This is what I call a "baseline review" where we aim to get a current picture of a particular activity that is not well understood and identify potential issues. Those reviews have raised a number of issues about the use of OSINT and I think those issues are not just for the intelligence agencies. I'll come to why I think that in a moment.

OSINT continues to evolve and now largely involves the development and use of tools that can simultaneously scan hundreds of sources and platforms. These tools may also include access to datasets obtained through a data broker or from hacked and leaked sources. Sometimes the tools may automatically create identities or accounts to access sites.

We were interested to understand the legality and propriety of using such tools.

Open source intelligence for the intelligence and security agencies under the ISA

The first thing to understand is the context for the Intelligence agencies activities. What is their mandate, powers and authorising framework? It does differ from other agencies represented here.

I start with function. The core statutory function, although there are others, of an intelligence agency is to collect and analyse intelligence in accordance with the NZ Government's priorities; and to provide that intelligence and analysis to relevant bodies. They can do anything lawful in pursuit of that function. If the activity is unlawful they can apply for an intelligence warrant to carry out any such activities.

In carrying out their functions the agencies are required to comply with any Ministerial Policy Statements that may be relevant and to use the least intrusive means of gathering information. So how does this apply to the intelligence agency's use of OSINT, and does it have broader application to other agencies?

For "lawful' OSINT activities I consider the framework set out in the Ministerial Policy Statement for Publicly Available Information provides a useful set of principles and is a good place to start for all agencies. The principles are:

- **Respect for privacy** – recognising that people may still have privacy interests in publicly available information
- **Necessity** – publicly available information should only be obtained, collected and used for a purpose that is consistent with the NZSIS and GCSB statutory functions
- **Proportionality** – the collection of PAI should be proportionate to the purposes for which it was carried out
- **Least intrusive means** – GCSB and NZSIS should use the least intrusive means available to obtain information
- **Respect for freedom of expression** – the exercise of the right to freedom of expression does not of itself justify the NZSIS or GCSB taking action against an individual (section 19 of the ISA))
- **Legal obligations** – collection must be in accordance with the law
- **Oversight** – all activities must be carried out in a manner that facilitates effective oversight.

The MPS applies to information that is lawful to collect. There are some instances, however, where the collection of apparently publicly available information may be unlawful. These can include:

- Using methods that may breach the terms and conditions of a particular method, such as using web scraping or bots to collect information. This includes doing so through third party tools
- Obtaining (including buying) or accessing datasets that were hacked and leaked online
- Using assumed identities or gaining entry to platforms/groups through unauthorised means

In the above contexts Crown Law, the intelligence agencies and my office consider that the collection of intelligence may involve: crimes of receiving stolen property, accessing a computer system dishonestly or without authorisation, or simply breaching express terms and conditions. All of which would amount to unlawful collect.

The Intelligence and Security Act 2017 provides the NZSIS and GCSB with an ability to obtain an intelligence warrant to undertake otherwise unlawful activities. Other government agencies have a different authorising framework under the Search and Surveillance Act. The obvious issue that arises for agencies is how fit for purpose are the authorising frameworks for agencies engaging in OSINT and collecting publicly available information. I consider all agencies need to have some statutory authority to enable the type of potentially unlawful OSINT collect that I have just discussed.

Key considerations for open source

Informed by international research and my review into the intelligence agency's activities, I wanted to set out some key considerations that I consider agencies should consider when undertaking these activities.

In 2021 the Dutch intelligence oversight body published a report on the intelligence and security services use of automated OSINT tools. The Dutch review examined the lawfulness of the OSINT tools and the datasets and whether the services have a sufficient understanding of how the tools work. The review found that automated OSINT can involve a serious violation of privacy. The report also noted a lack of understanding in the intelligence services on how the OSINT tools worked and the underlying data sources impacted – information that is necessary to:

- carry out necessity and proportionality assessments,
- evaluate the reliability of the data received and
- ensure the services are carrying out lawful data processing.

In a different context, the US Department of Justice has recently issued guidance for gathering online cyber threat intelligence and purchasing data from illicit sources. That guidance notes that

unauthorised access to platforms and purchasing stolen data sets will often be unlawful and could result in DOJ investigation.

So what does this mean for agencies gathering OSINT? Here are some thoughts for best practice.

What is the legal basis for the activities that are being undertaken?

This should be the starting point for any activities. Agencies should fully understand what activities they are proposing to do and:

- Whether the OSINT collection fits within the functions and role of their agency?
- Whether the information is truly publicly available and whether the methods being used may be unlawful?
- If the methods are unlawful, whether there are appropriate authorisations in place to undertake the activities?
- Regardless of the lawfulness, whether any concerns arise under the Privacy Act 2020 or New Zealand Bill of Rights 1990

How should agencies approach the use of third party tools?

There are a vast number of open source tools that are either freely available or that can be purchased which enable agencies to conduct open source collection at speed and at scale. The use of these tools raise unique issues and I consider that there needs to be a cautious assessment process of these tools before they adopted. This might include consideration of:

- How the tool works and whether there use any unlawful methods
- The types of information collected and the expectation of privacy in that information, including considering whether a Privacy Impact Assessment should be completed?
- How will tool data be stored by the company? Will the company have ongoing access to the data? Who owns the data?
- How is artificial intelligence used by the tool and how does the data of searches contribute to machine learning of the tool in general?
- Who is the company providing the tool and are they reputable?

How will the collection impact on freedom of expression?

The GCSB and the NZSIS have specific obligations under the ISA in relation to the freedom of expression, where expression by itself does not justify the agencies taking any action. As much of online content will involve people exercising the right to express themselves, the agencies need to

consider what justification they have in collecting information other than simply that they are expressive views, regardless of how extreme those views are. However, an expression advocating or linking to violence may be sufficient to justify the intelligence and security agencies undertaking further investigation, but they must always be conscious that the collection they are undertaking is necessary for the protection of national security. Freedom of expression should be considered on a case by case basis.

Are there appropriate policies and procedures in place?

Given the potentially intrusive nature of open source intelligence collection, it is important that agencies adopt policies and procedures ensuring that agencies have a clear scope for what activities can and cannot be done, set an appropriate approval process, detail record-keeping expectations, describe how information will be retained and stored, and provide for how collection activities may be audited.

What oversight is there for the activities?

Finally it is vital that agencies activities are amenable to effective oversight, both internally and externally. This might be by:

- Having clear knowledge of the activities at a senior leadership level
- Providing for internal compliance checks on the activities
- Briefing external oversight bodies about the extent of activities (eg Privacy Commissioner, Ombudsman, Independent Police Conduct Authority).

Conclusion

My office will be concluding our review into the agencies open source activities in the coming months and look to publish our findings. While focussed on the intelligence and security context, I hope that my thoughts provide useful for considerations for other agencies who are developing their approach to open source intelligence.