Intelligence Bias – An Open and Closed Case

DAVE MCMAHON, SLG | JUNE 2023

uOttawa
Laboratoire sur l'intégrité de l'information
Information Integrity Lab

Intelligence Bias – An Open and Closed Case

The subject of bias in intelligence analysis has been widely studied, and a great deal of effort has gone into education and quality assurance. Can open-source intelligence (OSINT) further mitigate bias in traditional analysis or does it come with its own challenges?

There has been potential for bias in conventional (closed source) classified intelligence in a number of places. Relying on a single source, however special, is like looking at the world through a straw. The resulting analysis can yield an incomplete picture or narrow perspective.

We may find ourselves looking in the wrong place for the right information, like searching for answers about transnational criminal groups cyber hacking Canadian critical infrastructure from Asia when the only collection available is from high Arctic high-frequency radio sensors monitoring Russian military manoeuvres. Re-tasking and pivoting conventional collection can be a bit of an extreme sport and is not as agile as open-source intelligence (OSINT).

RELYING ON A SINGLE SOURCE, HOWEVER SPECIAL, IS LIKE LOOKING AT THE WORLD THROUGH A STRAW. THE RESULTING ANALYSIS CAN YIELD AN INCOMPLETE PICTURE OR NARROW PERSPECTIVE.

A risk-sensitive organization will always be tempted to collect information that is easy to access rather than information that is necessary. Without strict client-driven requirements and feedback, there is a tendency to push intelligence to potential consumers without checking if it is actionable, relevant, or worth the price. Many public sector consumers are getting intel for free, so they may not provide the same feedback as if they were paying full price for it.

This brings me to my next point. The absence of information is not information of absence. Too often, I have read a report that says, "We have no evidence of threat, therefore the threat level is low." Risk is a product of likelihood, impact and uncertainty. If one is only looking for ABC, it is easy to get blindsided by XYZ. For many years, the intelligence community was focused on the usual Cold War spies, only to miss 9/11. Pivoting to fighting the war on terror blinded us to the Arab Spring, systematic cyber espionage, and deliberate interference in critical infrastructure. Today, how much is the intelligence community focused on powerful non-state actors, existential threats like climate change, population growth, energy shortages, and disruptive science and technology?

Mandates create bias by limiting the types of sources and methods a government agency may use or by restricting the location, jurisdiction, or topic of collection. What if the threat actor were a paramilitary transnational criminal organization operating globally and implicated in state-sponsored espionage disinformation, cyber warfare, crime, terrorism and war crimes? In this instance, the threat actor would cross multiple jurisdictions and mandates but not one lead agency. The fear of violating a mandate often means missed coverage.

Conversely, a mandate may drive an agency to produce intelligence for which there is no current client interest because trends and threats change faster than legislation.

The practice of consolidating or white-labelling[1] intelligence from other producers, especially from partners and commercial, academic, and open sources involves removing references. Classification is a form of branding insomuch as it is a security handling label. This practice of "repackaging" can unduly elevate the veracity of the intelligence by creating feedback loops and making it appear that multiple sources are confirming the same thing. I have seen similar phenomena in the media where major news stories have been build up based on a single tweet by a random person online. We also see this when journalists interview other journalists and build up a story. It is critical that all information in an intelligence report be fact checked and referenced to primary sources.

[1] "Analyst Finds Work Plagiarized in British Dossier." Los Angeles Times, 8 Feb. 2003, www.latimes.com/archives/la-xpm-2003-feb-08-fg-plagiarism8-story.html.

This brings us to foreign bias. The vast quantity of classified intelligence consumed by Canada comes from foreign sources and is ingested without question. The same is true for OSINT and news media. We have seen a trend from secret intelligence that has spilled into OSINT involving political partisanship and even subtle colouring of the analysis based upon cultural and social norms—left or right, liberal or conservative.

It is also important to consider that the foreign intelligence may have been collected under different legal and ethical frameworks inconsistent with Canadian values or law. Conversely, if something is legal in Canada but not in other jurisdictions, your favourite source could be suddenly shut down, but you will still be billed. We are seeing this happen right now.

THE VAST QUANTITY OF CLASSIFIED INTELLIGENCE CONSUMED BY CANADA COMES FROM FOREIGN SOURCES AND IS INGESTED WITHOUT QUESTION.

Subscribing to foreign data sources, tasking providers, and using foreign-managed attribution systems represent unnecessary exposure to your operational security, especially where trusted data brokers and vetted sovereign capability exists. Your supply chain is susceptible to foreign ownership, control, and influence, especially if the adversary gets inside that chain using surreptitious means or through mergers and acquisitions.

Using foreign suppliers establishes critical dependency that may not be reliable when you need it or leaves you with only leftover answers to questions allies have already asked. Foreign providers working in much more lucrative markets may not entertain Canada's unique collection priorities, not to mention ITAR and no-foreign restrictions that come with many high-end commercial and OSINT data products and tools.

Finally, there is the risk of politicizing the reporting either by only reporting what leadership wants to hear or hyping a threat to justify action or fund programs. This occurs less often these days, but speaking truth to power is always a risk.

Political staff still do the majority of politicizing by cherry-picking intelligence to fit an agenda, taking a narrative out of context, compiling DIY intelligence using Google or ChatGPT, making things up, or ignoring good intelligence altogether. We are currently watching a highly politicized debate around foreign interference here in Canada.

Does the emergence of open-source and commercial intelligence help or hinder the process?

There is an unfortunate perception among some that open-source intelligence is less reliable than traditional closed sources. I have heard statements such as, "OSINT is all hearsay" or "Free is worth what you pay for it."

The RAND Corporation wrote about the intelligence community's deadly bias toward classified reporting, stating "government officials, commissions, and think tanks have warned that the U.S. intelligence community has blinded itself to enormous sources of intelligence, simply because the information is publicly available."[2]

The truth is that 90% of classified reporting is already padded with or informed by open-source material. The wide-aperture and diverse nature of OSINT mitigates many of the aforementioned biases because OSINT is all-domain and multi-source. It is not driven by a single collection method, target, or mandate.

Whether using classified or open source data, validation and verification of source reliability are the same. In the world of classified intelligence, analysts often assume data is reliable because it has already been labelled top secret and appears in the system.

The notion that commercial intelligence cannot be trusted and is intentionally biased (because companies are only interested in profits) is generally without substance.

Commercial intelligence companies only produce intel that someone is willing to pay for. Furthermore, clients pay for relevant facts and informed analysis; commercial intelligence must therefore be unique, timely, accurate, and cost-effective. It is subject to verification of the facts, quality assurance and assessment of value by the consumer. If the intel does not meet these criteria, the company will not get repeat business. Market competition and other checks and balances keep the process fair, honest, and frugal.

On the other hand, open raw information obtained directly from social media and news networks must be scrutinized. Social media is ripe with misinformation. Media companies are predisposed to bias, as they are in the business of selling ads and chasing ratings for revenue, which means printing big headlines and adapting content to their audience. This creates a risk of popularized investigative reporting turning into tabloid journalism or misinformation for entertainment, such as a history channel broadcasting shows about ancient aliens and other conspiracy theories.

MEDIA COMPANIES ARE PREDISPOSED TO BIAS, AS THEY ARE IN THE BUSINESS OF SELLING ADS AND CHASING RATINGS FOR REVENUE, WHICH MEANS PRINTING BIG HEADLINES AND ADAPTING CONTENT TO THEIR AUDIENCE.

Finally, monocultures are fertile ground for analytical bias. It is critical that we create diversity in the analytical team to include age, gender, experience, ethnicity, language, culture, education, and open world views. We should look for intelligence, critical thinking, honesty, integrity, empathy, communications skills, and neutrality. We need an internal challenge function within the analytical cell.

My conclusion is that open-source and commercial intelligence have the potential to significantly reduce bias when sound analytical practices are followed.

[2] Weinbaum, Cortney. "The Intelligence Community's Deadly Bias toward Classified Sources." RAND Corporation, 12 Apr. 2021, www.rand.org/blog/2021/04/the-intelligence-communitys-deadly-bias-toward-classified.html.

AUTHOR

Dave McMahon is the Chief Intelligence Officer at Sapper Labs Group (SLG). He has 40 years of experience in intelligence.

Sapper Labs Group (SLG) is an all-source intelligence company providing open-source intelligence (OSINT) technology, training, talent, and finished intelligence analysis for human rights investigations, national security, defence, law enforcement, critical infrastructure protection, privacy, peace, and prosperity.