INTELLIGENCE CHALLENGES OF THE DATA RICH WORLD

Date: November 24th, 2020

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 24, 2020, Phil Gratton presented *Intelligence Challenges of the Data Rich World* at the 2020 CASIS West Coast Security Conference. The presentation was followed by a group panel for questions and answers. Main discussion topics included the abundance of data; non-threat related data-sets; and legislative and operational advancements towards contributing to cutting-edge intelligence processes.

NATURE OF DISCUSSION

Presentation

The speaker focused upon the challenges an analyst may face when dealing with an abundance of data, and the sections of the National Security Act which enable analysts to deal with large-scale data-sets.

Question Period

During the question period, the importance of sharing information with partner intelligence agencies and the benefits of doing so were discussed.

BACKGROUND

Presentation

As an organization that has historically engaged with covert human intelligence (HUMINT) practices, the Canadian Security and Intelligence Service (CSIS) has evolved to incorporate reliable and accurate data into their methods of analysis. Advances in data generation, storage, and analysis have broadened the capacity of intelligence work and have facilitated a new wave of powerful threat

assessment products based on increasingly systematic and sophisticated data collection and analysis techniques.

Yet, one of the first obstacles in dealing with data can be the deluge of data that exists for an analyst to examine. At CSIS, this means a more robust and sophisticated ability to analyze data in support of the operations to corroborate human and technical sources, to further identify individuals of interest and to generate new investigative leads. Although this is a data-rich world, there are tough challenges to address.

The increased volume of data from a technological stand-point is one of the first challenges. To assist analysts in their incorporation of data to their HUMINT expertise, CSIS relies upon a process that speaks to Canadian legislation, structures, and the established practices that are in place to assign authorities to find, decide, deliver, monitor, and report. In the last few years, CSIS has undergone significant legislative changes that have affected the way that they acquire, analyze, and store vast amounts of data.

The National Security Act is a key part of this. It came into force in the summer of 2019 and introduced the most significant changes to the CSIS Act since the organization was created in 1984. These changes add greater transparency and accountability to the work that CSIS does, and modernizes authorities in specific areas, including their data set framework. The CSIS Act provided a clear legal mandate for the organization with regard to the collection and retention of datasets, including laying out the parameters by which CSIS can collect, retain, and query datasets containing personal information that is not directly and immediately related to a specific threat to the security of Canada, but could be useful in helping paint a picture of a threat, or trends toward the threat. In this realm of non-threat related datasets, the Act sets out three types of data sets: Canadian datasets, foreign datasets, and publicly available datasets.

A Canadian dataset is defined in the CSIS Act as a dataset that predominantly relates to an individual within Canada or Canadians who may be abroad, which includes Canadian citizens, permanent residents, or Canadian corporations. While these datasets are of great value, they are also the most laborious to acquire from a process perspective; with CSIS having to apply to the federal court to retain and exploit them.

Canadian foreign datasets must remain segregated and this is done through technology from operational holdings and can be only queried by designated

employees in accordance with the provisions of the CSIS Act. There is also extensive record-keeping in the audit requirements and all of this is subject to review by the National Security and Intelligence Review Agency (NSIRA).

Finally, publicly available datasets or non-threat related data-sets rely upon Section 11 of the CSIS Act. It is highly prescriptive and features its own process orient to safeguards that speak to the complexity of working with data sets. These legislative and operational advancements have resulted in cutting-edge intelligence. Everything CSIS does stems from the CSIS Act and while the organization has a part of the Act that deals with non-threat related data sets, they also have the ability to obtain warrants from the federal court under Section 21 of the CSIS Act; this allows CSIS, to capture data outside the public realm with the permission of the federal court.

In a data-rich environment, it is essential that we have the authority to leverage modern tools to support investigations while ensuring Canadian's privacy is protected. This means engaging in these collaborations with eyes wide open, ensuring due diligence before entering into partnerships or funding arrangements and increasing awareness of all those in the community about the threat.

Question Period

CSIS, in the context of working with agencies that are not evolving as quickly, strives to work extensively with Canada's 5 Eyes partners (New Zealand, Australia, United Kingdom and the United States). While there is no one leader of the 5 Eyes partners, there are a few nations who are ahead of the game, and CSIS relies on working with them to acquire their techniques and/or collection methods. From the larger perspective, each of the 5 Eyes partners all relatively face the same threats, so the best measure is arguably to start sharing techniques. This method is more efficient and sustainable than each nation being expected to develop their own algorithms. Furthermore, Canada has always been seen as a trusted partner within the 5 Eyes community, giving CSIS the opportunity to leverage that reputation to facilitate more exchanges of information.

KEY POINTS OF DISCUSSION

Presentation

- The deluge of data faced by an analyst is one of the primary obstacles faced by modern intelligence agencies; it becomes even more challenging when analysts have to combine HUMINT and technological data together.

- Legislative and operational advancements of the CSIS Act have resulted in cutting-edge intelligence processes.
- It is essential that we have the authority to leverage modern tools to support investigations while ensuring Canadian's privacy is protected.

Question Period

- CSIS relies upon its partnerships with 5 Eyes members to ensure that new intelligence gathering and collection techniques are continuously being shared and upgraded.
- Sharing techniques allows for each nation to work collaboratively against the same threats.
- Canada is a trusted partner within the 5 Eyes community, CSIS should leverage that reputation to facilitate more exchanges of information.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/