LESSONS LEARNED IN INTELLIGENCE ANALYSIS

Date: September 20, 2018

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

KEY EVENTS

On September 20, 2018 the Canadian Association for Security and Intelligence Studies (CASIS) Vancouver hosted its eighth roundtable meeting which covered "Lesson Learned in Intelligence Analysis." The following presentation was hosted by John Pyrik, a former intelligence officer, and the first analytical methodologist for the Canadian Security Intelligence Service (CSIS). The subsequent roundtable discussion focused on examining the notion of whether Canada has been excessively lenient towards individuals who have been convicted of espionage, with particular regards to the selling of classified information.

NATURE OF DISCUSSION

The presentation focused on first defining intelligence and what are the basic requirements of obtaining intelligence. Which continued to an examination of intelligence failures, such as the Cuban missile crisis, the Iranian revolution, and the 9/11 attacks. Moreover, the importance of analysists using structured analytical techniques when producing intelligence products was also discussed. With a particular focus on how these techniques can potentially improve the quality of intelligence analysis. Furthermore, the potentially increased role of AI in intelligence collection and analysis, and the fundamental importance of the human analyst was also covered in the presentation.

BACKGROUND

The presentation began with a general introduction asking, what is intelligence? Despite the term intelligence being widely used, it was explained the police,

military and national intelligence services will have difference uses for intelligence, and thus will define intelligence differently.

Therefore, the term intelligence, is without a universally accepted definition. Further commenting that the term is occasionally used to refer to what could be more accurately described as information or facts. While in other instances the term is used to refer to the analysis of information that has been processed into a final intelligence product. Intelligence was described as being the final derived output, from an initial input of raw data, which is then processed in several stages. Thereby defining intelligence in accordance with the latter understanding of what is meant by the term, to provide the appropriate context of how the term would be used in the presentation.

Several historical instances of intelligence failure were mentioned. In addition to failures of collection and analysis, poor communication was identified between agencies, a lack of client receptivity and failures of policy as key factors which may lead to an intelligence failure. The first example was the failure to predict the 1979 Iranian revolution, described as a failure of intelligence collection. Since a narrow range of sources were used, thus creating an inaccurate perception of the political situation in Iran.

When discussing the Cuban missile crisis, it could be argued that a lack of proper collection in combination with failures of analysis led to the resulting surprise when the missiles were discovered in Cuba. Since inadequate collection efforts were compounded by a biased perception of what actions and risks the Soviet Union would be willing to take.

The September 11th attacks were presented as an example of an intelligence failure resulting from poor communication. Although there was a large amount of pertinent information that was known, this information was not shared. This was described as an “unknown known”, in reference to the former United States Secretary of Defence Donald Rumsfeld. Meaning that since this information was not shared or distributed properly, it could not be used effectively and was thus not accounted, therefore, effectively remained “unknown”.

Distinction was drawn between failures of poor intelligence and of poor response by those acting on the intelligence that has been provided. Noting that even with good intelligence, the risk of an operational failure remains. Therefore, even the best intelligence cannot guarantee operational success.

On the topic of improving intelligence analysis, two categorizations of the methods by which intelligence analysis could be improved were discussed. One set of methods would be through "learning and sharing." Where analysts would engage in seminars and mentoring session, in order to improve their tradecraft. Furthermore, the sharing of information through an internal wiki could also be beneficial to accomplishing this goal.

The second set of methods were of a structural nature, involving the development of a set of standards and best practices as a mean to improve analytical tradecraft. This would involve formalizing what a good assessment should look like and implement institutional mechanisms for reviewing assessments. Moreover, the employment of a structural analytics methodologist, to directly advise and assist analysts with the use of structured analytic techniques.

To conclude, there are limitations to relying on structured analytic techniques to improve the quality of analysis. Noting that there is a limited understanding to the overall effectiveness of these techniques in actually achieving this goal. With the additional problem of convincing analysis to further incorporate structured analytic techniques into their assessments; it should also be noted that an extract cost-benefit analysis of using structured analytic techniques has yet to be determined.

KEY POINTS OF DISCUSSION

- It was argued that the traditional approach of eliminating all bias from an assessment may not be entirely correct. Arguably, the mere presence of bias is not always bad, and thus a distinction can therefore be drawn between good biases and bad biases. A group of individuals that are influenced by their bias by constantly leaning towards the believed correct answer were referred to as "superforecasters." They challenge the notion that the best method for improving intelligence analysis is specifically by removing the analyst's biases from an assessment.
- Since the AI will be able to identify correlations, a human analyst will be required to examine those correlation and determine their validity. The use of AI and machine learning systems will eventually provide analysist with useful tools to generate better intelligence assessments. However, it could be argued that these systems will not replace the analysts themselves as the final assessment will still require a measure of human oversight.
- It was noted that a significant amount of work will need to be done in order to convert the necessary data, in to a machine-readable form. So that this data,

could be at least in principle, be properly analysed by an AI program. The need for more precise database coding requirements to be created, as well as a large volume of none-digital based sources and files were cited as potential challenges to accomplishing this goal. Therefore, it was argued that if it could not be fully determined that an AI would be able to provide an accurate analysis, without human oversight, then the cost may not be justified.

- Intelligence failures may have distinct causes, which may require different solutions to properly address. For example, by potentially solving problems relating to the analysis of intelligence by incorporating the use of structured analytic techniques, problems such as collection, improper communication, or client receptivity may still remain.
- Structured analytic techniques can in principle be used to improve intelligence analysis. However, these techniques have not always been eagerly adopted by analysts, and their effectiveness is not guaranteed.

WEST COAST PERSPECTIVES

- The notion of lenience towards individuals convicted of espionage, with a specific reference to Jeffrey Delisle and whether this could create a security risk was discussed. It was noted that despite the extent of Delisle's crimes, he had been granted parole less than halfway into his sentence. Some in attendance held the opinion that since Delisle would never hold a security clearance again, he was therefore, no longer a security risk. Thus, continued imprisonment would not be necessary since the risk of Delisle reoffending was non-existent.
- Some addressed that a severe punishment as a means of deterrence was not an effective measure in practice. Thus, other than to mitigate the potential risk of reoffending, it is possible that the absolute requirement for an individual to serve an extensive sentence in this context would be unnecessary.
- It was also argued that the nature of the crimes committed by Delisle, were severe enough to warrant further imprisonment. With a comparison being made between Delisle's actions and committing first-degree murder. This comparison was due to the potential harm that may have been caused by revealing classified information to a foreign nation. Therefore, the need for Delisle's continued imprisonment could be view as serving principles of justice, rather than any implications directly pertaining to deterrence.
- It was noted that there may be ethical concerns regarding how the data gathered by focusing on particular identity or ethnic group would in turn be

used. With the practical difficulties of gaining the cooperation of certain groups, and properly accounting for the unique concerns of each group were also discussed.

- A potential alternative approach discussed is the increased recruiting of minority groups, in order to allow for more diverse perspectives to be taken into consideration. However, a counter argument that was raised to the utility of this approach, was that organizations such as CSIS may have prevailing norms, which in practice may prevent these perspectives from being heard. Minority groups may conform to these norms, therefore, limiting the extent that the perspective of minority groups will be properly represented, despite increased recruiting efforts.

KEY TAKEAWAYS

- Structured analytic techniques can in principle be used to improve intelligence analysis. However, these techniques have not always been eagerly adopted by analysts, and their effectiveness is not guaranteed.
- Intelligence failures may have distinct causes, which may require different solutions to properly addresses. For example, by potentially solving problems relating to the proper analysis of intelligence by incorporating the use of structured analytic techniques, the further problems of collection or problems involving a lack of proper communication or client still remain.
- The exact role of AI in furthering the practice of intelligence analysis at this time is unclear. As the concerns involving the need for human oversight, and the work still required for the proper implementation of an AI analysis system still need to be addressed.
- The issue of whether lenience towards those convicted of espionage creates a security risk generated a debate over the utility of deterrence for preventing future crimes of this nature. With strong opinions being presented on both sides of the debate.
- The presence of curtain norms in organizations such as CSIS, may limit the extent that minority opinions can be taken into account, and the extent that bias can be addressed.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/