

Canadian
Forces
College

Collège
des
Forces
Canadiennes



Canadian Army Intelligence at the Brigade Group Level

Major Laurel Williams

JCSP 49

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2023.

PCEMI n° 49

Étude militaire

Avertissement

Les opinions exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté le Roi du Chef du Canada, représenté par le ministre de la Défense nationale, 2023.

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI 49

2022 - 2023

Service Paper – Étude militaire

CANADIAN ARMY INTELLIGENCE AT THE BRIGADE GROUP LEVEL

Major Laurel Williams

“This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

CANADIAN ARMY INTELLIGENCE AT THE BRIGADE GROUP LEVEL

AIM

1. The aim of this service paper is to argue the requirement for a doctrinal Canadian Army (CA) intelligence organization at the formation-level, with a collection capability. Given Canadian Armed Forces (CAF) limitations with regard to division-level operations, this paper will focus on the Brigade Group (Bde Gp) as the formation.

INTRODUCTION

2. In evaluating the Bde Gp's operational intelligence needs, it is necessary to briefly describe the history of the All-Source Intelligence Centre (ASIC), first established in 2003. Its predecessor organization was the 1st Canadian Division's 1 Intelligence Company (1 Int Coy) which was shuttered in 2000.¹ 1 Int Coy provided the basis for the concept of a multi-source analytical unit with a collection operations capability, which evolved during CAF's mission in Afghanistan. As combat operations in Afghanistan ended in 2011, the CAF published a Joint Doctrine Note² to describe the ASIC employed in that mission. Since then, the term ASIC has been used in numerous CA doctrine publications in ways that imply there is confusion on what level of intelligence the ASIC provides, and from where. Notably, intelligence-specific doctrine is lacking in the CA, and a clear concept of the organization's place in CA operations has not been provided. These doctrinal issues will be discussed further.

3. CA operational intelligence needs will be described, along with a review of doctrine to illustrate the relevance of a company-sized intelligence organization within the Bde Gp. The doctrine review will continue with a focus on the current concepts of the ASIC. The paper will end with a recommendation to capture the need for a CA intelligence collection and analysis organization at the Bde Gp level. It will also note recommendations to scope additional doctrinal reviews.

DISCUSSION

4. A keystone CA doctrine publication, *Brigade Tactics*, explains brigade operations in the context of a division.³ Although this publication indicates that the division may be allied, multinational, or Canadian,⁴ there is no CA doctrine specific to division employment and the Bde Gp is explicitly the organizational level with which the CA will prepare to conduct operations.⁵ The likelihood of the deployment of a Canadian division is small enough that CA modernization guidance does not acknowledge the possibility. Instead, *Advancing with Purpose* points out that

¹ Canadian Armed Forces. Joint Doctrine Note 2011/01 The All-Source Intelligence Centre, 2011. p 3

² Joint Doctrine Notes are not doctrine, rather they are intended to generate discussion and capture concepts that may later enter into doctrinal documents.

³ DND. B-GL-321-003/FP-001 *Brigade Tactics*. 2017. p. iii

⁴ *Ibid.* p. 1-6

⁵ Canadian Army. *Advancing with Purpose: The Canadian Army Modernization Strategy*. 2020. p. 17

interoperability with allies will concentrate on Canadian brigade operations in a multinational division, and integrating a multinational battle group into a Canadian brigade.⁶ The primacy of the Bde Gp in CA doctrine is evident.

5. A Bde Gp's intelligence requirements are doctrinally focused on high-value targets and understanding the adversary's organization and disposition within the Bde Gp's area of operations.⁷ A level up, the division is consumed with, among other intelligence requirements: adversary reserves; formations in depth; armoured and airmobile assets; the location of weapons of mass destruction; artillery; water crossing sites; command and control (C2), and communications elements.⁸ A level down, the battalion (or Battle Group (BG)), needs intelligence that enables near-real time engagement of targets. In a conventional setting, it will be concerned with company-sized elements.⁹

6. These divisions of responsibility for intelligence by organizational level come from dated doctrine. They do not reflect the consideration of complex human terrain or the host nation, which are particularly important considerations in modern operations other than conventional conflict. The intelligence doctrine definitions remain useful for simply illustrating that there are differences between the type of information required by each organizational level of the CA in operations. Although the Bde Gp intelligence staffs and/or unit are not seized with the responsibilities of the division, the Bde Gp nonetheless requires the processed intelligence from that level to enable its operations. Intelligence is also a critical aspect of planning fires and effects, and the brigade is "the lowest level of headquarters that can integrate and synchronize joint effects."¹⁰ Therefore, the Bde Gp needs a robust and tailorable intelligence element to support these activities.

7. Given the CA's lack of deployable divisions, and its lack of division-level intelligence organizations, the Bde Gp must be prepared to span the gap in intelligence requirements between the Bde Gp and the theatre/corps level intelligence organizations. This will ensure that it has timely intelligence to support planning and operations. To illustrate, consider the hypothetical example of a Bde Gp deployed under a Joint Task Force (JTF). The JTF is a theatre operational HQ, which may have an ASIC that is responsive to the JTF J2 for intelligence taskings.¹¹ Some of these taskings will naturally provide for the production of intelligence to the level that the Bde Gp requires, however the majority will likely straddle the operational and strategic levels, and may be in support of other services as needed. If the ASIC has been tasked with support to deliberate targeting, then it will have been tailored to that task, not the provision division-level intelligence products to the Bde Gp. It follows from this that the brigade would require a tailorable intelligence organization to provide adequate support to its level of complex planning and operations.

⁶ DND. *Advancing with Purpose: The Canadian Army Modernization Strategy*. 2020. p. 47

⁷ DND. B-GL-357-001/FP-001 *Intelligence*, 2001. p. 23

⁸ *Ibid.* p.23

⁹ *Ibid.* p.23

¹⁰ *Ibid.* p. 17

¹¹ DND. B-GJ-005-200/FP-001 *Canadian Forces Joint Publication 2-0 – Intelligence*. 2011. p. 4-7

8. *Brigade Tactics* includes numerous mentions of the importance of intelligence and alludes to the roles of the battalion and Bde Gp intelligence staffs, which are more fulsomely developed in other doctrine.¹² It indicates specifically that the “brigade will be supported by an allocated brigade military intelligence (MI) company (formerly the [ASIC])....”¹³ It also refers to the work of the Bde G2 (Intelligence) staff that is carried out with the Bde’s intelligence platoon or company.¹⁴ It is not clear from these statements that the basic difference between an MI coy and an ASIC is understood. An ASIC is an intelligence unit which includes an all-source analytical capability and a complement of task-tailored collection assets.¹⁵ It can exist at more than one level at once, but usually there is only one in a JTF, in the Canadian context.¹⁶ An MI coy, in contrast, is an intelligence sub-unit that can include a basic analytical capability, but does not have integral collection assets (sometimes referred to as enablers). Other parts of the doctrine circumvent this issue by simply referring to the G2 and the intelligence element. This is positive in that it does not create undue expectations on the CAF intelligence enterprise to necessarily provide enablers to the Bde Gp’s intelligence element – the flexibility to task-tailor is left untouched by the neutral descriptor ‘element.’

9. Battle Group (BG) doctrine hints at the possible employment of an ASIC-type organization at that level, though this is an interpretation of the doctrine. *Battle Group in Operations* states, for instance, that information from BG Human Intelligence (HUMINT) operations will be processed through the ASIC for input into the BG common operating picture (COP).¹⁷ When discussing engineer intelligence, those tasks are noted to contribute to the intelligence picture “through the ASIC at each level.”¹⁸ It is unclear whether this refers to a BG-, Bde-, or TF-level ASIC. If referring to a TF ASIC, this poses a challenge because it implies that a theatre asset would be tailoring its intelligence production to the needs of a BG, whose intelligence needs require a finer degree of granularity than the TF as a whole. If the implication is that the BG has its own ASIC, there are challenges to making it happen. It is possible to have ASICs at the BG and other levels, and the generation and employment of such an organization would be task-tailored. However, the realities of personnel availability, equipment, and network requirements would severely limit the implementation of ASICs at BG level. Creative solutions and investment could mitigate some of the issues, but not to the degree where multiple ASICs could be generated for several levels during operations.

10. The future operating environment will put more emphasis on pan-domain effects.¹⁹ This means that the CA will be in multiple supporting or supported relationship with forces and elements in the sea, air, cyber, space, and information domains. These operations will still

¹² DND. B-GL-331-002/FP-001 Staff Duties for Land Operations. 2008.

¹³ DND. B-GL-321-003/FP-001 Brigade Tactics. 2017. p. 2-20

¹⁴ *Ibid.* p. 5-10

¹⁵ DND. B-GJ-005-200/FP-001. Canadian Forces Joint Publication 2-0 – Intelligence. 2011. p. 4-7

¹⁶ *Ibid.* p. 4-7

¹⁷ DND. B-GL-321-005/FP-001 Battle Group in Operations. 2012. p. 3B6-1

¹⁸ *Ibid.* p. 4B1-4

¹⁹ DND. Pan-Domain Force Employment Concept (PFEC): Prevailing in an Uncertain World. 2020. p.13

require intelligence to aid commanders' decision-making, but will do so under conditions where the ability to sense is vastly increased by technology and the speed of dissemination. The increased ability to sense, however, poses a challenge to the ability to *make* sense.²⁰ That is, ever-increasing volumes of data must be analyzed to create intelligence. The CAF acknowledges that in addition to increased volume, that the activities and functions required of the intelligence enterprise will also grow.²¹ When all levels are depending on intelligence for sense-making amid the crush of data, a dedicated element to conduct that function between the Bde Gp-BG and Bde Gp-TF levels is crucial.

11. The CA understands that the pan-domain future operating environment will see its forces employed in complex operations “involving a diverse range of conditions and a wide array of multi-faceted, adaptable adversaries.”²² As the CA moves towards developing capabilities to meet those challenges, it aims to achieve near-real time situational awareness at all levels.²³ The CA's capstone concept for operations envisions a force that is able to make decisions quickly by ensuring a shared understanding of the environmental and adversary impacts, pushing intelligence products further down the Chain of Command than ever before.²⁴ This cannot be achieved through stove-piped coordination cells, nor can it be done with simply a team of generalist intelligence personnel.

12. As BG and Bde Gp doctrine both noted, enablers may need to be employed by or with the BG and Bde Gp. These enablers may include Electronic Warfare (EW), HUMINT, psychological operations (psyops), per doctrine.^{25,26} However, there are many other assets that have become useful in providing accurate and/or credible data quickly, such as full-motion video (FMV) analysis, signals intelligence (SIGINT), and social media analysis, among many others. Further reading of *Brigade Tactics* suggests a variety of intelligence support tasks for the Bde Gp G2 staff and the intelligence element, including detailed Intelligence Preparation of the Operating Environment (IPOE), support to psychological operations, ISTAR planning, estimative intelligence captured materiel and personnel exploitation, trend and link analysis. A troops-to-task analysis is outside the scope of this paper. That said, experience would suggest that to carry out that number and variety of tasks at the Bde Gp level would require a significant intelligence capability to provide close support.²⁷ This is not within the capacity of integral staff, even with augmentation by a support team of generalist intelligence personnel. Therefore, current doctrine, practice, and practical limitations challenge the CA's ability to achieve the effects laid out in *Close Engagement* and *PFEC*.

²⁰ *Ibid.* p. 24

²¹ *Ibid.* p. 24

²² DND. *Close Engagement: Land Power in an Age of Uncertainty*. 2019. p. 55

²³ DND. *Pan-Domain Force Employment Concept (PFEC): Prevailing in an Uncertain World*. 2020. p. 4

²⁴ DND. *Close Engagement: Land Power in an Age of Uncertainty*. 2019. p. 20

²⁵ DND. B-GL-321-005/FP-001 *Battle Group in Operations*. 2012.

²⁶ DND. B-GL-321-003/FP-001 *Brigade Tactics*. 2017.

²⁷ DND. Joint Doctrine Note 2011/01 *The All-Source Intelligence Centre*, 2011. p 4-5

13. One of the practical limitations on executing current doctrine regarding intelligence organizations at the Bde Gp level is available personnel. Although the Intelligence Branch's numbers have grown since the Afghanistan era, the expectations of the function have increased, as demonstrated by the capstone and keystone doctrines noted in this paper. This will need to be overcome, or will require creative mitigation through non-traditional career paths, improved quality of life policies to aid recruitment and retention, or emerging technologies such as artificial intelligence (AI).

14. Secure processing is another practical limitation that forms the basis of an argument against a multi-source intelligence capability at the Bde Gp. While it is true that without access to classified networks the processing and dissemination of intelligence can be limited, much of the real-time information that is to be processed to aid decision-makers is available through open sources.²⁸ Given that the intelligence produced at the Bde Gp would primarily be targeted at the Bde HQ and units, the communications systems would be sufficient for passing on the necessary intelligence analysis. Reach-back is another method that could be used to overcome the processing issue. The majority of the processing could be done by a dedicated Bde Gp element, though physically dislocated from that HQ. This would require only an adequate communications network.

CONCLUSION

15. This paper demonstrated that the Bde Gp is considered the key CA unit for conducting operations. It described Bde Gp intelligence requirements as inadequately defined in current doctrine, as well as the conditions of the future operating environment. These conditions include increased public scrutiny of military actions due to the boom in non-traditional media platforms, the requirement for speed of decision-making and action, and pan-domain considerations. The key limiting factors to be analyzed when determining the composition and location of a Bde Gp intelligence organization were identified as the need for secure processing systems and infrastructure, and the scarcity of available general and specialist intelligence personnel for deployment. It is clear that there is a desire in CA doctrine, and a need driven by modernization, to establish a robust, task-tailorable intelligence element at the Bde Gp.

RECOMMENDATION

16. CA intelligence doctrine should be developed to include the requirement for a deployed company-sized, Bde Gp intelligence organization. This organization should be task-tailored and scalable to suit the mission and the Bde Gp construct, as well as complementary to the theatre intelligence architecture. CA doctrine, particularly intelligence doctrine, must be updated to reflect the significant changes to our operating environment and significant changes to the CAF intelligence enterprise. Other CA doctrine should clarify the concept of an ASIC at all levels, instead describing the intelligence functions and effects required, with organizational references

²⁸ Chris Pallaris. "Open Source Intelligence: A Strategic Enabler of National Security." *CSS Analyses in Security Policy*. Vol 3, No 32. Center for Security Studies, ETH Zurich. 2008. p. 1

limited to a generic multi-source, company-sized intelligence element. CA should consider limiting the use of the term ASIC to the JTF-level ASIC described in Canadian Forces Joint Publication (CFJP) 2.0. The physical location of the element should not be tied to a specific echelon, owing to resource limitations and allowing for creative solutions to each expeditionary operation. A fulsome review of relevant doctrine, including a comparative analysis of allied intelligence should also be undertaken to ensure interoperability is maintained in light of any changes that may be made to CA doctrine and practice.

Bibliography

DND. *Pan-Domain Force Employment Concept (PFEC): Prevailing in an Uncertain World*. 2020.

DND. *Close Engagement: Land Power in an Age of Uncertainty*. 2019.

DND. *Advancing with Purpose: The Canadian Army Modernization Strategy*. 2020.

DND. *B-GL-321-005/FP-001 Battle Group in Operations*. 2012.

DND. *B-GL-321-003/FP-001 Brigade Tactics*. 2017.

DND. *B-GL-331-002/FP-001 Staff Duties for Land Operations*. 2008.

DND. *B-GL-357-001/FP-001 Intelligence*. 2001.

DND. *B-GJ-005-200/FP-001 Canadian Forces Joint Publication 2-0: Intelligence*. 2011.

DND. *Joint Doctrine Note 2011/01 The All-Source Intelligence Centre*. 2011.

Chris Pallaris. "Open Source Intelligence: A Strategic Enabler of National Security." *CSS Analyses in Security Policy*. Vol 3, No 32. Center for Security Studies, ETH Zurich. 2008.