National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CAF COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE MODERNIZATION

Major Howard Han

JCSP 47

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.

PCEMI 47

Étude militaire

Avertissement

Les opinons 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.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 47 - PCEMI 47
2020 - 2021

SERVICE PAPER – ÉTUDE MILITAIRE

CAF COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE MODERNIZATION

By Major Howard Han

Word Count: 2,526

Nombre de mots : 2.526

CANADIAN ARMED FORCES (CAF) COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (C4ISR) MODERNIZATION

AIM

1. The aim of this paper is to discuss the existing CAF C4ISR capability deficiencies in order to provide a recommendation on how to immediately improve C4ISR within the CAF and advance future CAF C4ISR capability.

INTRODUCTION

2. Although this paper is written in response to the Royal Canadian Air Force (RCAF) topic of "Military Integrated Information Infrastructure - C4ISR present status",[1] the subject of C4ISR modernization is truly a joint issue. *Strong, Secure, Engaged: Canada's Defence Policy* describes a joint CAF C4ISR capability as a requirement under initiative 62.[2] thus all ISR information must be consumable by the joint community. As such, this paper will discuss this topic from a joint perspective and provide recommendations for the RCAF to champion with the other commands. In this paper, C4ISR capability refers to the people, processes and training and not specific hardware solutions because equipment supports people and C4ISR cannot be solved by equipment alone.

3. This paper argues that the CAF needs to update its joint ISR (JISR) doctrine and create a JISR governance body prior to advancing a new joint C4ISR capability. To that end, the paper will discuss the current capability gaps to frame the argument and then discuss the necessary organizational requirements to justify change. This paper will also outline how this new organization can create doctrine and facilitate joint training to immediately improve the CAF C4ISR capability. Finally, it will present how this new organization can guide C4ISR capability development, as well as, prioritize the integration of legacy systems in a resource constrained environment. It should be noted that the author was a former project director for the Canadian Army's (CA) Land ISR Modernization Project (LISR Mod) so this paper provides a perspective on the common joint issues encountered in advancing the CA's LISR Mod project.

DISCUSSION

JISR Overview

4. Although JISR operations are not new to the CAF, JISR operations have not evolved to operate in a digitally networked environment. Currently, the CAF is utilizing a mixture of liaison officers, limited direct tactical data links (i.e. LINK 16) and traditional

[1] Canadian Forces College. *JCSP 47 DS545 Service Paper Topic Lists*. "Military Integrated Information Infrastructure - C4ISR present status." (Serial 23), dated 18 Nov 19.
[2] Department of National Defence, *Strong, Secure, and Engaged*, (National Printing Bureau, Gatineau, QC), p.41.

military communication systems (i.e. voice radios) to network ISR information across the force. This is a problem because much of the information is being moved inefficiently and requires human input to share across the various independent ISR networks. This creates a situation where ISR assets cannot readily or quickly share information to support JISR related tasks such as: sensor cross-queuing, target confirmation and target tracking. Furthermore, these ISR networks are also not integrated within a common digital Command and Control (C2) system which limits how quickly ISR information can be displayed to the joint command[3] or shared across a coalition network such as Battlefield Information Collection and Exploitation System (BICES) which restricts the speed of the decision-action cycle.[4]

5. The fusion of multiple networks is not a simple matter because each network was not designed to support joint needs. Simply bolting together, a number of networks is problematic because high-bandwidth, long-range, communication systems are costly and integration costs are high. As well, not all information is required to effectively build a comprehensive JISR picture. This creates the issue of determining which ISR systems need to communicate within a larger joint system – essentially a JISR *system of systems*; however, designing such a system, requires a JISR staff that is proficient in all of the CAF ISR capabilities as they can identify how the supporting JISR network should facilitate their work.

6. Currently, the CAF creates ad hoc JISR staff based on each mission's requirements drawing from each element as required. This creates a situation where various ISR operators are drawn together from across the CAF and directed to operate in a joint manner. This usually results in sub-optimal processes as operators struggle to learn the combined capabilities of the CAF and utilize non-standard solutions to move information around the force. Therein lies the main issue with JISR, the absence of JISR doctrine or regular training to build JISR proficiency.

Doctrine and Training

7. The CA describes doctrine as being "built in a hierarchical fashion to include a philosophy, supporting principles, practices and procedures."[5] Doctrine plays an important role in standardizing how the military trains and operates. Although doctrine does not govern military activities, it provides a common starting point for action. Currently, there is no JISR doctrine and the absence of a JISR doctrine also creates a vacuum of responsibility for JISR capability development. This leads to each element

[3] It is important to note that a common Canadian digital C2 tool does not yet exist as Canadian Joint Information Management (CJIM) is still being developed.

[4] The issue of decision-action cycle speed cannot be understated. Future conflicts will be decided by the force that is able to quickly and accurately execute their strategy. Jon R. Lindsay's "Technology Theory of War" describes how smaller, agile, forces with an information edge can overcome larger, slower, forces so integrating information into decision-making needs to be done in an effective manner to give the CAF and its coalition allies the edge in future conflicts. Jon R. Lindsay. *Information Technology and Military Power*. Cornell University Press, 2020. p 13

[5] Department of National Defence, *Land Operations*. B-GL-300-001(Army Publishing Office, Kingston, ON). p 3 -1/30.

developing systems independently which is why current C4ISR capabilities do not communicate with each other, staff processes remain unclear and capability development stove-piped.

8. As well, the absence of doctrine has resulted in Canadian Joint Operations Command (CJOC), arguably the largest stakeholder in JISR, not being able to directly influence how joint elements should collectively train despite commanding these elements on operations. This lack of joint training results in a steep learning curve as staff are required to quickly learn JISR operations within a deployed headquarters.

9. The lack of doctrine and joint training has created practical problems on operations. These are:

a. Variable understanding of how ISR works in a joint environment for ISR operators;

b. Lack of standardization for joint ISR equipment and capabilities[6];

c. A poor understanding of the greater JISR capabilities; and

d. Duplication of effort/capabilities and inefficient use of limited resources.

10. Tied to the absence of doctrine is an issue regarding how JISR experience is captured and institutionalized. Normally, experience is captured institutionally in the form of lessons learned and after-action reports (AAR) leading to periodic updates to doctrine. Currently, there is no single organization that is responsible for capturing these lessons and so JISR experiences are not readily accessible or being lost. This experience is critical to informing processes, training and capability development.

11. This leads into the issue of joint training. While there are episodic JISR training events they are not mandatory and frequently unsupportable by the force generators because these activities are seen as surplus and not core activities such as CJOC's Exercise UNIFIED VISION. From a capability development perspective, this is a major problem because frequent training helps operators refine operational requirements through practice and the AAR process. Frequent training also avoids the issue of procuring short-term fixes using the Urgent Operational Requirements process as the force would be continually training thereby identifying equipment issues through the Unsatisfactory Condition Report process. Following these processes would enable the DND/CAF to procure systems in a more cost effective and transparent manner thereby, decreasing the risk of governmental embarrassment.

---

[6] While all elements are required to procure systems that meeting Standing NATO Agreements (STANAG), information technology is advancing faster than NATO working groups can establish standards. This issue has led to incompatibility issues being created by software updates within the same software. As an example, if one were to look at their MS Windows™ 10 operating systems, they will note that each system has a different build, these various builds can create conflicts within the software operating in the Windows 10™ operating environment. This issue can be typically resolved by all users adopting the same version of the software.

12. Ultimately, many of these issues would be rectified if JISR doctrine was created in the CAF.[7] The new doctrine would harmonize training, establish expectations and standards regarding JISR across the force. As well, a common doctrine would also provide the other elements a framework for capability design when advancing new ISR capabilities.

Organization

13. While doctrine is critical, there also needs to be a responsible authority for joint activities and capability development. Organizationally, there is a vacuum as it lets each element decide how it will interact in the joint realm as well as manage their equipment procurement. Allied nations like the UK have recognized this issue and have adopted a new organizational approach. The British Army has created 1st ISTAR brigade to reorganize their land ISTAR capabilities together before advancing their new equipment projects to ensure that the capability is developed holistically before procuring new equipment.[8] This formation has brought their various land sensors and intelligence assets together under a single command and provides an ISTAR fusion centre to coordinate assets and output information. While this particular organization may not be ideal for Canada, it illustrates the importance of unifying ISR capabilities organizationally prior to investing in new equipment.

Equipment

14. While SSE has made it very clear that the future of CAF ISR capability exists within the joint realm,[9] current ISR capabilities were developed and procured by each separate CAF element to conduct ISR activities for very specific use cases and within each element's C2 system. As such, legacy ISR capabilities excel at the tasks their element's assigned tasks but were never designed with joint operations as the primary capability requirement. This is a major technological hurdle as sensors and ISR data are not intrinsically compatible and can be complex to integrate. This integration work is more than just linking of systems through communication networks, it also includes the rendering of information into common data sets that can be understood by the receiving system. In some cases, the cost of integration exceeds the value of the original system. This situation creates a conundrum of deciding what sensor capabilities should be upgraded or replaced, as well as, software management issues.

15. Currently, new major capital projects advance to Chief Force Development (CFD) with detailed core requirements for their respective elements but present very superficial

---

[7] It is important to note that *Canadian Forces Joint Doctrine 3.0 Operations* and *Intelligence, Surveillance, Target Acquisition and Reconnaissance: The Enduring Doctrine* discuss the requirements for joint operations but do not provide many details on how it should be force generated.

[8] The UK Army is advancing their new land C4ISR systems under three projects SERPENS, ZODIAC and ORION. The CAF should look to leverage the experiences of the UK in advance of its own JISR modernization design.

[9] Department of National Defence, *Strong, Secure, and Engaged*, (National Printing Bureau, Gatineau, QC), p.65

details on joint design. Normally, a list of dependencies is provided with an impact assessment if a particular dependency is not integrated; however, these lists do not have any sort of prioritization. It is left to the sponsoring element to select the most important criterion as projects are implemented. Frequently due to cost overruns, projects remove or lower the joint capabilities as project teams are keen to ensure that core capabilities are delivered first. This approach has created the current situation where newly fielded capabilities are delivered with little joint integration, such as the CA's new Medium Range Radar capability.

16. The management of new systems and legacy capability is a complex problem. Each element has a vested interest in maintaining capabilities but it is not affordable or even optimal to integrate all of the ISR assets into a singular C4ISR backbone. These issues are why a centralized body is required to effectively manage legacy and future ISR equipment. Key decisions such as system management, identification of capability gaps and software upgrade schedules would ensure procurement optimization and maintain operational readiness. As well, such a body could provide the necessary advice on the prioritization of procurement and what systems are to be integrated. Finally, this organization could also ensure that each element is being engaged well in advance of the procurement process on how ISR equipment should be integrated into the future C4ISR design.

Organizational Change

17. Evolving the CAF will require better knowledge of JISR so change management is a challenging proposition; however, if there were a JISR Centre of Excellence (COE) the CAF could better understand JISR before making major organizational changes. The CA currently utilizes such a model to standardize its combat training activities at the Combat Training Centre in CFB Gagetown and the COEs are effective at standardizing training activities and institutionalizing lessons learned from operations. A JISR COE could also assist the capability development process by facilitating experiments, user acceptance trials and informing operational requirements. While such an organization does not have to have formal command and control relationships, it should be enabled to speak authoritatively on JISR issues, coordinate JISR training and advise each element on how their ISR capabilities should fit into the larger JISR capability.

18. While there are a number of organizations that could lead a JISR COE, it would probably be most sensible to have CJOC lead JISR development and C4ISR design. As the force employer, the organization is best equipped to direct how JISR should be executed; however, the COE would need participation from the other elements. Joint participation would be necessary in ensuring that the elements' gateway training and supporting ISR doctrine are aligned. As well, the JISR COE could also ensure that new projects had input from CJOC and guide the other elements in C4ISR design early in the procurement process to ensure compatibility with the new joint C2 tool. This organization could also help prioritize integration or divestment of legacy systems to ensure that the relevant operational capabilities are maintained. Lastly, the JISR COE

would also be able to advise CJOC on CAF ISR capabilities and inform force apportionment planning.

CONCLUSION

19. The issue of C4ISR is a joint problem, the CAF will continue to struggle in fielding integrated JISR capabilities if it does not change both its doctrine and organizational approach to JISR. A new governing body is required to provide oversight on the development of this advanced capability and it must include all of the CAF elements to be effective.

20. Beyond organization and doctrine, the CAF also needs to train JISR to make a C4ISR capability effective and to properly design the supporting processes and equipment to manage ISR information. While organization and doctrine will support joint training, there also needs to be a coordinating agency to facilitate joint training, set standards and provide force employment advice regarding JISR. A joint COE approach would remedy this issue and inform many decisions regarding new and legacy ISR capabilities as well as guiding the development of a unified C4ISR capability.

RECOMMENDATION

21. It is recommended that CAF establish CJOC as the lead organization for JISR and that a JISR COE be created with support from the other elements. The COE should be charged with the responsibility of developing JISR doctrine, joint training and joint capability development.

BIBLIOGRAPHY

Canadian Army Training and Doctrine Centre. (2013). *Intelligence, Surveillance, Target Acquisition and Reconnaissance: The Enduring Doctrine.* Kingston, ON: Her Majesty the Queen, Minister of National Defence.

Canadian Forces College. (2019). *DS 545 - Service Paper Topic Lists.*

Canadian Forces Warfare Centre. (2010). *Canadian Force Joint Publication 3.0 Operations.* Ottawa, ON: Colonel R. Ken Chadder, CD.

Department of National Defence. (2007). *Land Operations.* Kingston, ON: Army Publishing Office.

Department of National Defence. (2017). *Strong, Secure and Engaged: Canada's Defence Policy.* Gatineau: National Printing Bureau.

Lindsay, J. R. (202). *Information Technology and Military Power.* Online: Cornell University Press.

NATO Standardization Office. (2013). *NATO Standardization Agreements.* Brussels, Belgium: NATO Secure.