

Canadian
Forces
College

Collège
des
Forces
Canadiennes



CANADIAN FORCES JOINT SIGNAL REGIMENT – A JOINT COMMAND AND CONTROL ENABLER

Major E.A.S. Gillingham

JCSP 40

Exercise Solo Flight

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.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2014.

PCEMI 40

Exercice Solo Flight

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 la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2014.

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES
JCSP 40 - PCEMI 40
2013 - 2014

SOLO FLIGHT

**CANADIAN FORCES JOINT SIGNAL REGIMENT –
A JOINT COMMAND AND CONTROL ENABLER**

By Major E.A.S. Gillingham

“This paper was written by a student 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.”

Word Count: 5443

“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.”

Compte de mots : 5443

INTRODUCTION

Command and Control: The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2.

- David Alberts - Agility, Focus and Convergence

During the past decade, the Canadian Armed Forces (CAF) has recognized the need and challenges of operating in a joint, interagency, multinational and public (JIMP) environment. The Department has also leaned forward to develop an understanding of the future security environment and its implications across the land, sea, air, and cyberspace domains. Integrated command and control (C2) of combined and joint forces has persistently been raised as a shortcoming by commanders and has been captured in deficiency reports in the recent past. The 1st Canadian Division Headquarters, although an Army organization, remains the sole CAF organization tasked with deploying and employing a Combined Joint Inter-Agency Task Force (CJIATF) headquarters. It identified that requirement to operate in a complex C2 environment as well as the necessity of integrating information to support the joint force commander's decision action cycle.¹ Created in 2000, the Canadian Forces Joint Signal Regiment (CFJSR) was intended to provide joint C2 capabilities to commanders during domestic and international operations. Combining the communications extension and restoral

¹ Comd 1st Cdn Division, *Command and Control Information Systems Statement of Capability Deficiency*. 1st Canadian Division - Canadian Forces Base Kingston: file 3350-1(Comd), 19 June 2012

capabilities from 79 Comm Regt with the headquarters close support and information services delivery capabilities from 1 CDHSR, the CFJSR has continued to fulfill its missions in an increasingly complex environment. Both 79 Comm Regt and 1 CDHSR were units under control of the Canadian Forces Communication Command (CFCC). This was an operational command that spanned the services and handled all communication and signaling requirements. 79 Comm Regt was established in order to pull together the CFCC tasks of communication extension and maintenance tasks to CF operations and 1 CDHSR was manned, equipped and tasked to support the Division Commander and staff with the close signals support necessary to operate in a deployed environment.

This paper will look at the elemental operating environment and C2 challenges that exist. It will demonstrate that the CFJSR's ability to fulfill its mandate is in jeopardy by analyzing the current and future security environment in order to identify the C2 requirements of the CF and its mission partners. This analysis will be followed by a brief examination of the current doctrine, organizational structure, personnel, infrastructure, and readiness, to assess whether the CFJSR has the proper capabilities to meet the C2 challenges of today and tomorrow. Finally, recommendations will be made to address the operational-level C2 requirements of the CF through a revitalized CFJSR.

The foundation for Command, Control, Computers, Communication, Intelligence, Surveillance and Reconnaissance (C4ISR) is Communication Information Systems (CIS)², the critical integrator of the information and decision maker remains effective C2.

The increasing demands for technology to support a joint force commander require that technical obsolescence remain an ever-present consideration, so that C2 systems can fulfill evolving data fusion and information exchange requirements. While this paper will not analyze the technical issues encompassing C2, the relevance of a CAF unit dedicated to providing C2 to joint force commanders anywhere, anytime is increasingly dependent on these technical requirements being addressed.

The military has suffered from an inability to get out in front of a problem space and influence the future environment. This is based on the traditional learning environment, analyzing operations and influencing training by adopting lessons learned which enables the primary training audience to fight the last battle, not the battle yet to come.

As the Force Employer that will suffer the most without joint C2, Canadian Joint Operations Command (CJOC) is the logical, yet not formally appointed, champion for such capabilities. The CJOC J6 has been mired in force generation issues since its infancy. It needs to be more visible in engaging the more pressing problem space - force development³ of joint command and control capabilities.

² Department of National Defence, Vice Chief of Defence Staff. *Command and Control Operating Concept*. National Defence Headquarters. Ottawa. (14 June 2012) p20

³ Force development (FD) is the integration of allocated and projected Army resources into a time-phased program to develop a force that is properly organized, equipped, trained, and supported to carry out the Army missions and functions world-wide. This includes force planning, programming, analysis, structuring, combat, and training developments. Force generation (FG) is the structured progression of increased unit readiness over time to produce trained, ready, and cohesive units prepared on a rotational basis for operational deployment.

SECTION 1 – THE SECURITY ENVIRONMENT

David Alberts states quite clearly in his article *The Future of C2*, that the situations for which C2 is best adapted have been transformed by the realities of the information age.⁴ Documents such as the Future Security Environment produced by the Chief of Force Development⁵ and All Possible Wars authored by Sam Tangredi⁶ aim to define the environment the military will operate in. Predicting the future, however, can only be a forecast or estimation. As such, basing planning efforts on this guess introduces inherent risk. The trends communicated in the previously mentioned documents highlight a theme of globalization, with an increasing likelihood of regional instability as emerging powers test the tenuous balance of power. This clearly indicates a continued requirement for military forces to be prepared to continue to operate in a high threat environment from physical as well as informational domains. This preparation to conduct international engagements and operations other than war, often require a different approach to C2. As recent as Op ATTENTION, situational awareness and the limited time and access to appropriate sources of information were C2 challenges, which re-emphasized the importance of addressing the long standing problem of effective joint C2 capabilities.⁷

⁴ David Alberts. "Agility, Focus, and Convergence: The Future of Command and Control". *The International C2 Journal*, Vol 1, no. 1, (2007): p 2

⁵ Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. 27 January, 2009

⁶ Sam J. Tangredi. *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001-2025*. McNair Paper 63, Institute for National Strategic Studies, National Defense University. Washington, DC. (2000)

⁷ Col Dawe, *Post-Tour Observations from Op ATTENTION R0*, TF DCOMD, March 2012

Across the future security environment, while the military is a strong user of technology as a force multiplier, it does not have a monopoly over this resource. Due to the global availability and affordability of technology, there is a growing attentiveness and cause for concern when operating in an increasingly dynamic environment as to how both state and non-state actors may leverage technology to achieve their goals.⁸ By defining and analyzing the environment, one can appreciate the necessary evolution of C2 and that communications will remain an essential element in enabling C2 into the future.⁹

Whether the environment is defined as JIMP or analyzed with the comprehensive approach¹⁰, advances in technology support the processes and procedures that allow improved synchronization and collaboration with all mission partners. Due to the increasingly complex and unpredictable environment, technology is often seen as a substitute for traditional C2. Emerging technology forces the competition between human ingenuity (smart soldier in a tactical environment) and capability obsolescence throughout the future security environment. Canada has a poor track record in the acquisition of C2 systems. Project delays, inflexible processes and changes in scope to reduce costs have often led to capabilities being delivered based on obsolete requirements. As a result, the CAF has leaned heavily on the resourcefulness of its soldiers to keep pace with its allies and remain interoperable. C2, in the broader context,

⁸ Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. (27 January, 2009). p 8

⁹ *Ibid.*, p. 9

¹⁰ Janine Davidson, Operationalizing the Comprehensive Approach: The Military as “Enabler...”, Small Wars Journal (Feb 18 2009). URL: <http://smallwarsjournal.com/blog/operationalizing-the-comprehensive-approach-the-military-as-enabler>

encompasses the technical pillar however, also succeeds through doctrine, processes and training. It is not surprising that the complexity of the environment determines the level of integration, collaboration and synchronization. As an example, the complexity of the Vancouver 2010 Olympics highlighted a key takeaway which was a requirement for integrated C2.¹¹

In 2008, Chief of Force Development's office led an initiative which resulted in a list of C2 deficiencies¹² based on the operating environment of the time. Integrated C2 capability challenges and constraints remain extant however, stovepipe service [Army, Navy, Air Force] solutions continue to be sought to deliver on current operating requirements. The desire for common C2 processes, information, applications, security environment, user interfaces and networks¹³ remain a target that is continually impacted by competing priorities. The ever-present themes of integration, fusion and adaptability strongly resonate at the strategic level and are interpreted differently depending on perspective at the operational level.

SUBSECTION A: C2 – LAND

The land domain has been aptly defined in USJP 3-31 to be the area of the Earth's surface ending at the high water mark and overlapping with the maritime domain. The current and future security environment reality is that conflict and instability are based on population and resource centres; a land-centric environment. Land operations, whether

¹¹ Department of National Defence, Commander JTF Games. *Report on the Strategic Lessons Observed and Recommendations Derived from Op PODIUM*. Joint Task Force Games: file 6497-333-1(JTFG/RDIMS #93042), (14 June 2010). p 35

¹² Department of National Defence, Chief of Force Development. *Command Domain Capability Alternative Report*. National Defence Headquarters, Ottawa. (August 2008)

¹³ *Ibid*, p 14-15

domestic or international, have become increasingly complex with the multilayered and multifaceted approach that incorporate civilian agencies and other government departments in order to more dynamically seek and render solutions on behalf of the political masters. This not only increases the level of complexity but through demonstration of joint force enablers such as air, maritime and special forces as force multipliers, commanders are required to ensure synchronization of these enablers during adaptive dispersed operations. This synchronization is essential and drives the need for robust C2.

The vision for the Canadian Army (CA) relies on the integrated information environment¹⁴ ensuring it is aligned with joint force development. Regardless of the technical solution supporting this information environment, the reality is that the battlespace is evolving and the amount of information available to stakeholders (not bound by political affiliation or geography) can be overwhelming. This battlespace overlaps with the brown water regions the Royal Canadian Navy (RCN) operate routinely throughout.

SUBSECTION B: C2 – SEA

Given the size and composition of the RCN, discussions pertaining to its future employment continue [blue or brown water navy]. Guidance has been issued from the strategic level (CFDS) which has supported the operational direction that the navy to be a

¹⁴ Department of National Defence, Commander Canadian Army. *The Army: Advancing With Purpose*. 2nd ed. Director Land Strategic Planning. Ottawa (2009).p 39

medium global force.¹⁵ What has remained a constant throughout decades of operations is the supporting and supported role the RCN has taken enabling joint operations. While force projection is a key tenet of the RCN vision, it maintains independent command suites [various ship platforms] capable of exercising a full range of maritime operations anywhere in a marine environment. Based on not only the life-cycle management of the platforms and its many on-board systems, but also the vision of the commander, integrating with the CAF elements, continues to prove challenging. This was exercised during activities as recent as JointEx13¹⁶ in which the Commander of CJOC commented that “we need to refine our understanding of coalition C2 and national C2”.¹⁷ In 2001 the Commander of the RCN pushed out doctrine leading the concept of [amongst other characteristics] interoperability that was to guide the development and employment of the RCN for decades.¹⁸

The current Commander of the RCN has articulated in his executive plan the intent to “implement joint-enabled cyber, space, C2 and intelligence, Surveillance and Reconnaissance capabilities”.¹⁹ What is not clear is how this executive plan considers the vision of the CA or the RCAF during a similar timeframe. The RCN C2 structure is better configured to interface with maritime air and coalition naval forces than with the army.

¹⁵ Department of National Defence, Directorate of Maritime Strategy. *Leadmark The Navy's Strategy for 2020*. National Defence Headquarters, Ottawa, (18 June 2001), p 90

¹⁶ National Defence JointEx 2013 URL <http://www.forces.gc.ca/en/operations-exercises/jointex-2013.page>

¹⁷ Chris Thatcher, JointEx: Exercising National Command and Control. VANGUARD, (Aug, 2013) <http://vanguardcanada.com/jointex-exercising-national-command-and-control/>

¹⁸ Department of National Defence, Directorate of Maritime Strategy. *Leadmark The Navy's Strategy for 2020*. National Defence Headquarters, Ottawa.(18 June 2001)

¹⁹ Department of National Defence, Commander Royal Canadian Navy. *Commander's Guidance and Direction to the Royal Canadian Navy Executive Plan 2013-2017*. National Defence Headquarters, Ottawa. (2013)

This makes brown water challenging in that there is no robust means for land and naval forces to exchange information directly. Instead, they must typically funnel information through Ottawa, which then sends it back to the other Forces.

SUBSECTION C: C2 – AIR

The traditional role of the Royal Canadian Air Force (RCAF) has been to ensure the security of sovereign airspace, conduct search and rescue operations in coordination with other agencies, and support missions of the land and maritime components through the provision of relevant, responsive and effective airpower. The support the RCAF has provided in the realm of joint operations has been invaluable on the battlefield. The lessons learned at the tactical level will continue to ensure that the joint culture remains a key focus of the future leaders in the RCAF. Air Force Vector's provides guidance and focus on achieving integrated effects with the other services. It also outlines the operating concepts of each service in order to outline the RCAF's deductions into the future.²⁰ The tactical successes can overshadow the cultural differences, direction of training and necessary integration in a joint environment.

The need for a joint culture is not strongly supported in the more technical direction of the RCAF C4ISR Strategy that outlines concepts that "optimize the RCAF's

²⁰ Department of National Defence, Director General Air Force Development. *Air Force Vectors*, Canadian Forces Aerospace Warfare Centre, (2014) p 16-22

future S&R effects and flexibility”.²¹ It is clearly articulated that the technical solution will be complex due to the RCAF’s airframes and the architecture currently employed. C2, while identified as a technical problem from the RCAF perspective, only refers to joint operations lessons learned as a requirement for further pilot training with very little about sharing intelligence across services. The RCAF has taken a leading role in Tactical Data Links (TDL). However, fusion, integration and use of information provided to joint force commanders appear to remain very air-centric.

The need to ensure integration across the services is not overtly supported through the RCAF doctrine and is clearly distinct from the land and sea environments. This highlights the independent thought and direction of the RCAF. Whether through daily Air Tasking Order (ATO), scheduled sustainment of short-notice deployment – C2 beyond the walls of the RCAF is not clearly integrated nor is it highlighted as a priority and, while not unanimously shared across the RCAF, does indicate the differences in concept from within a single service. The reliance on technology, information sharing and support to the overall mission situational awareness is not bound by the framework of the RCAF. It needs to be recognized that while the common factor of physically connecting the services is technical, the reason for it has been borne out of necessity of C2 in a joint environment. Failure to do so impacts the effectiveness of the Commander, and creates duplication of effort for his staff who must seek to gather data and serve as the integrators of critical information by seeking to parse through a tremendous amount of information on multiple systems.

²¹ Department of National Defence, Commander Royal Canadian Air Force. *Future Concepts Directive*. National Defence Headquarters. Ottawa. (4 April 2013)

Quickly analyzing the future security environment, predictions have been made that there will be an increased reliance and requirement on surveillance capabilities.²² This does not indicate the necessary level of integration with the other services to ultimately support the operational capability of a joint task force. While C2 is well aligned to achieve success during single service operations, the CAF relies heavily on the technical prowess of soldiers, sailors and airmen and women to resolve complex C2 problems in a joint environment. The ad hoc approach that the land, sea and air elements of the CAF approach joint C2 points to a shortfall in vision, strategy, and coordination of efforts. This issue will become increasingly exacerbated in a progressively complex future security environment. The future of the CAF operating environment sees an increase in joint and combined efforts where unfortunately, an ad hoc approach will not always produce successful results.

SUBSECTION D: C2 – CYBER

The CAF operates within a digital C2 environment making cyber a major factor of consideration. Unfortunately, the cyber environment is not well understood by the majority of the stakeholders who have become so heavily reliant on it. Cyber is still debated over the ideology of whether it is a domain or an enabling capability.²³ This evolution highlights a number of schools of thought that confirm the conceptual status of this framework. What can be anticipated is the irregular tactics of evolving cyber attacks

²² Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. (27 January, 2009). p 38

²³ O. Hathaway, et al. "The Law of Cyber Attack." *California Law Review* 100, no. 4 (2012). p 827

- disruption of electronic means²⁴ as well as exploitation and denial (such as those used to affect C2). The protection and restoration of C2 assets and/or information ensures the joint force commander is not supported with a reliable decision-making process. The broad understanding of computer network attack (CNA) and the resulting effects identifies a critical vulnerability that must be protected.

Describing this environment has been likened to describing the shape of an ever-changing lava lamp²⁵ which amplifies the artificial nature of the domain. The traditional domains of land, sea, air and space are bound by physical geography, equipment and tactics whereas cyber adapts to every situation making it difficult to define. A cyber threat is not limited to conventional military forces. Cold War deterrence models do not apply and the implicit reliance on the adaptation of C2 is heavily favored.

Richard Clarke makes a poignant comment in his book on Cyber War that it is unlikely any nation is effectively deterred today from using its own cyber weapons in a crisis; and the potential of retaliation with cyber weapons probably does not yet deter any nation from pursuing whatever policy it has in mind.²⁶ This openly articulates that in the current cyber environment, we only know what we know, but we also have to understand that there is a lot that we simply do not. Threatened organizations either defend themselves or disappear. The CAF cannot afford to slip passively into an environment that could have such a potentially devastating impact on the global community. C2 in a

²⁴ Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. (27 January, 2009). p 82

²⁵ Dr Mitchell, "Cyberpower, Cyberwar." (slides from lecture, Canadian Forces College, Toronto ON April 30, 2014)

²⁶ Richard Clare, *Cyber War - The Next Threat to National Security and What to Do About It* (HarperCollins: 2010). p. 94

cyber-based environment requires an organization to ensure the confidentiality, integrity and availability of information so joint force commanders can prosecute campaigns.

Given the current C2 challenges faced by JTF commanders, it is troubling to think of how severe these challenges would become in a contested cyber environment.

Global stability is predicated on the agreement and satisfaction of hierarchical needs. This tenuous balance is forever shifting as the geopolitical situation morphs. The plethora of factors that contribute the ever-shifting balance directly impacts the nature and evolution of the security environment.

There are predictions which highlight an increased reliance on multilateral cooperation in order to operate with success in the future security environment whether through governing bodies such as the United Nations (UN) and the North Atlantic Treaty Organization (NATO). This leads the requirement to improve and increase current information sharing and networking protocols with the goal of adapting to the ever-changing environment, not only between the CAF's own services, but also with allied forces and other agencies, both governmental and non-governmental. The CAF is currently not well positioned to do so, and JTF Commanders would be hard pressed to communicate with mission partners in a secure and timely manner, or maintain situational awareness in this setting, given the state of current joint capabilities.

Based on future trends, the military's desire to remain technologically relevant in a rapidly changing environment²⁷ needs to be tempered across the CAF in order to place

²⁷ Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. (27 January, 2009). p. 76-77

joint interoperability above the individual service requirements. As safe assumption is that the CAF will be expected to work in a coalition environment, with other government departments²⁸ as well as other services. The resulting interdependence on joint military and civilian partnerships amplifies the complexity of C2 in this environment.

There does however, remain an existing misinterpreted ideology (culturally fostered) that individual services can conduct operations independently²⁹ in the contemporary environment. The operating environment is not bound by geography or organizational hierarchy. This mindset continues to influence the overall environment as stovepipe solutions continue to be developed in isolation as the elements within the CAF seek a methodology to address current challenges and adopt a readiness posture that will prepare them for future tasks.

The service chiefs have outlined in their respective guidance that their focus, as the CAF postures for the future, is on integration and joint operations. The ideology may be correct, but the culture of focusing on technical solutions³⁰ through the plethora of chaired working groups identifies deep rooted issues on why the CAF needs to become a better learning organization. Integrating capabilities to support joint force commanders does not simply entail providing information but rather supporting the C2 by synthesizing the emerging technology and integrating the systems and information. It means capitalizing on emerging technology to standardize our systems when logical and integrate information in a robust and flexible network of networks. Existing joint C2

²⁸ *Ibid.*, p 87

²⁹ Robert Wilkie. Hybrid Warfare: Something Old, Not Something New. *Air and Space Power Journal* (Winter 2009).

³⁰ Department of National Defence, Chief of Force Development. *Command Domain Capability Alternative Report*. National Defence Headquarters, Ottawa. (August 2008)

capabilities tend to be focused on specific mission silos, such as maritime helicopters and LRP connectivity with ships or tactical helicopters with the army. Since combined joint task force's (CJTFs) are formed in an ad hoc manner based on mission requirements, joint force commanders rely on interoperable C2 systems across all capabilities. Until this becomes a reality, a joint enabler is required which can integrate disparate systems and information into a cohesive whole for the commander, and ensure that the integrated network (and not just the components managed by individual services) is properly defended.

SECTION 2 – CURRENT CAPABILITIES

The Vice Chief of Defence Staff (VCDS) communicated in March 2013, that the development of adaptable communication systems and information systems are needed to support a flexible command and control capability.³¹ With each service planning and executing based on stovepipe solutions, the CAF continues to re-identify shortfalls while operating in a joint, combined and/or coalition environment. The capability shortfalls that have been identified by the Army, Navy, Air Force (and SOF) continue to be addressed in a joint environment. Tangible effects/ solutions are more readily achieved at the lowest level in a more timely fashion. Program/project conception, approval and fielding are not synchronized with the services that have the funding and the desire to achieve success in the shortest window possible. There has been a gap between strategic guidance and the desire to achieve adaptable CIS to support flexible C2 and the delivery on capability by

³¹ VCDS, Communications and Information Systems Operating Concept. National Defence, Ottawa, (March 2013) p i

the individual services. The cyclical problem has been the project timeline versus a commander's desire for effect. The problem with C2 is that it is being boxed in and summarized as a simple problem with a simple technical solution. A joint champion would be required to deliver a joint vision, and set clear objectives to develop an enabling capability for joint C2 on behalf of the strategic leadership. This cycle continues to repeat as the evolution of technology continuously outpaces capability delivery that meets a commander's desired effect for C2.

The backbone of effective command and control is CIS³² and missing, unclear or an overwhelming amount of information impedes the joint force commander's ability to succeed in a complex environment. Situational awareness (Common Operating Picture), Intelligence capability and an insatiable desire for more information, knowledge and understanding are all required to facilitate C2 in a complex environment. This drives the process and the technical usefulness of the support mechanisms which are becoming increasingly specialized.

SUBSECTION A – DOCTRINE

Doctrine: from the Latin “doctrina” which means teaching, learning, is defined as a stated principle of government policy, mainly in foreign or military affairs.³³ Canada has often been humorously touted as difficult to predict given its very lack of adherence to its own doctrine. In recent years the defined operational framework brought about

³² Department of National Defence, Vice Chief of Defence Staff. *Communications and Information Systems Operating Concept*. National Defence Headquarters. Ottawa. (13 March 2013) p 1

³³ Online Oxford Dictionary, Define: Doctrine. Oxford University Press, (copyright 2014), accessed 4 May 2014. URL: <http://www.oxforddictionaries.com/definition/english/doctrine>

through CF Transformation has seen yet another iteration in the C2 force employment model with the stand up of the Canadian Joint Operations Command. Through the structural changes and definition of force employment and force generation, the operational level remains extant providing C2 for sea, land, air and space activities which must be conceived and conducted as a single, concentrated (or joint) effort.³⁴

Canadian doctrine has evolved (in line with our closest allies) to adopt a whole of government (WoG)³⁵ or comprehensive approach to operations. The benefits of establishing a collaborative and synchronized environment with shared understanding of desired outcomes far outweigh the complexity of the C2 structure required to succeed. Whether operating in a joint, combined or coalition environment, interoperability through common tactics, techniques and procedures (TTPs), doctrine and technology is fundamental to the success of any force commander.

Command and control has proven challenging in a national environment yet, NATO has enabled C2 on a more complex level through doctrine, procedures and training. NATO outlines in AJP 01 that common NATO doctrine is essential to enhance interoperability.³⁶ Through principles such as unity of effort and unity of purpose, commanders can concentrate on the tasks (whether at the operational or tactical level) and not on the tools to facilitate C2. Each tool such as a NATO information gateway like the Battlefield Information Collection and Exploitation System (BICES) or some future mission network (FMN), provide independent layers to connect organizations in order to

³⁴ Department of National Defence. B-GJ-005-000/FP-001 *Canadian Forces Joint Publication 01 - Canadian Military Doctrine*. Ottawa: Canadian Forces Experimentation Centre. (2009). p 5-3

³⁵ *Ibid.*, p 6-4

³⁶ NATO, *Allied Joint Doctrine AJP-01(D)*, (December 2010). p 1-1

exercise C2. The ability for an organization to successfully support C2 is more than fusing the multitude of layers together and adapting the system of systems. In order to enable the joint force commander collaboration and synchronization in a JIMP environment outline the necessity for adaptive C2.

A basic comparison of the provision of operational C2 between NATO Joint Force Headquarters and a Canadian Joint Task Force highlight the strengths of training (TTPs), which enable the processes, and balances the international scale of operations. The lack of integrated spirals of technology and doctrinal responsibilities at a national level plague interoperability.

SUBSECTION B – CFJSR

A recognized leader in the provision of rapidly deployable C2 capability for any joint force commander spanning the full range of defence missions is the CFJSR. On 1 June 2000, the Canadian Forces Joint Signal Regiment (CFJSR) was officially stood up as a unit following the amalgamation of the former 1st Canadian Division Headquarters and Signal Regiment (1 CDHSR) and 79 Communication Regiment (79 Comm Regt). Its role is to provide high readiness and sustainment of close signals support to a joint force commander as well as general signals support to CAF operations.

It is designed to provide general support³⁷ to deployed CAF elements for CIS in accordance with operational requirements by maintaining the Information Technology Infrastructure (ITI), and by using the facilities of Information Technology (IT) and the

³⁷ Definition of General Support: The support provided to the force as a whole and not to any particular sub-division thereof, thereby supporting the operational level. General support is usually provided from a centralized location (ref: B-GL-300-004/FP-001, Land Force Sustainment p25).

National Command and Control Information Systems (NCCIS). The CFJSR is also mandated to provide close signal support³⁸ to a joint force commander and staff with rapidly deployable headquarters, CIS and 1st line combat service support³⁹ capabilities.

The CFJSR is a one-of capability in the CAF that is designed with the mandate to satisfy an operational command and control turnkey solution for a Joint Force Commander anywhere in the world.

Through the adaptation of equipment, doctrine and organizational culture, the military evolves. Equipment deficiencies can be solved by money, doctrine deficiencies can be solved by time - the critical link is in the mindset; of not only the soldiers, but also the commanders and the future leaders. Since its establishment in 1914, the lineage of the CFJSR has been involved in every major Canadian military operation ranging from war fighting, to peace support operations, to disaster relief operations, to operations in Canada in support of local and national authorities. It maintains scalable high-readiness capabilities to support future CAF operations.

The CFJSR has been relied upon to support operations anywhere, anytime. The lack of modularity of the CFJSR for a long period of time made it an inflexible giant, not readily adaptable to the ad hoc nature of CJTFs. This has, in turn, made it less appealing

³⁸ Definition of Close Support: The intimate support provided to the formation commander to deal with tasks of immediate concern to his operations. It includes the provision of the command post facility; power generation and distribution; line and cable plan design, installation and maintenance; establishment; operation and maintenance of all network and CIS service including unclassified, protected and classified domains, less specific intelligence and space support systems; provision of local service desk and user support services; local management of cryptographic equipment and key material; provision of rover's and local message courier service; local transportation of personnel and equipment; provision of LOCC to a tactical HQ; tactical voice communications to subordinate task for elements; to support RSOMI, local force protection activities and movement control; headquarters access control;

³⁹ Combat service support includes but is not limited to: supply services, accommodations, power generation and distribution, feeding, transport, maintenance (vehicle, weapons, communications and CIS), medical (UMS) and personnel administrative support (including chaplain services).

to commanders who require an adaptable, capable C2 element. On the other hand, some planners have also insisted in using the CFJSR as a shopping list of equipment and augmentees, compounding the lack of appeal with a fundamental misunderstanding of what the CFJSR could offer and could become if adequately sourced. The lack of ability to seamlessly integrate with service capabilities has further compounded this problem. Through an understanding of the genesis of the CFJSR, a joint force commander [and more importantly the CAF] will recognize that the whole is greater than the sum of all its parts.

Due to the ad hoc nature of tasking and employment of the CFJSR, a unit with unique skills, training, experience and readiness to support a joint force commander with the ability to integrate systems and information is becoming obsolete in an environment where the demand for C2 capability is increasing.

In order to maintain the readiness and capability to support operations, while attempting to remain relevant in a time that does not recognize it as a system of systems, the CFJSR has attempted to effectively become its own force developer. This has been attempted in an effort to mimic the organizational structure of the US Joint Command Support Element (JCSE).⁴⁰ While the incredible ingenuity of the soldiers to provide ad hoc technical solutions, this in no way compensates for the delivery of integrated operational capabilities.

⁴⁰Joint Communication Support Element <http://www.jcse.mil>

Should the evolution of technology guide how commanders exercise C2, as David Alberts predicts with regards to the future of network-centric organizations⁴¹, a single organization will not be relied upon to enable joint C2, as the integration and fusion of information will eventually be executed in a seamless, peer-to-peer environment with decentralized control individually.

Arguably, this is not where the CAF has postured itself for the next decade, but by embracing the speed of technological advances and the ability to self-synchronize⁴², the CAF is poised to lead the evolution of C2 in a more contemporary operating environment.

The history and culture of the CFJSR has been strongly influenced by the land environment and recent history touts the success of the organization on the international platform. The current operating space is focused on the land domain with coincidental ties to the air domain based on common C2 platforms. Without the integration of the air and sea elements to enable the growth of joint C2, along with solutions to better integrate with mission partners, the CAF will continue down the path of stove pipe single-service technical solutions delivered to the individual services thereby further contributing to the dissolution of the CFJSR - an existing enabler requiring intervention and support to surpass joint force commanders C2 expectations.

⁴¹ David Alberts. "Agility, Focus, and Convergence: The Future of Command and Control". *The International C2 Journal*, Vol 1, no. 1, (2007), p 11

⁴² *Ibid*

SECTION 3 – RECOMMENDATIONS

The CFJSR is a vital and dynamic model of capability in the CAF due to its ability to quickly be able to adapt to the needs of a joint operational commander and act as the key enabler for operational C2 in support of CAF missions. Based on the definition of the future security environment and the identified C2 challenges domestic and international, this paper posits a number of recommendations to support the delivery of operational C2 for CAF in the future security environment.

Through CAF Transformation, Commander CJOC is the unofficial Joint Champion. This unofficial title should be formalized as the commander is a peer to the environmental chiefs, VCDS and CFD which will enable the guidance, support and direction that dissolved post-CFCC. It is at the commander-level that the joint organization capable of integrating C2 across the CAF be confirmed by all as the CFJSR. This integration will support the development and fielding of future concepts and capabilities.

Due to the current training and readiness state of the CFJSR, it is relied upon as an invaluable unit because of its ability to quickly be able to adapt to the needs of a joint operation at a moment's notice. The CFJSR needs to be part of the operational framework (higher level) to avoid being lost among the myriad "tactical service providers" and have capability compromised simply due to its ownership.

The requirement for the CFJSR to maintain its own force development capability must be removed and elevated to a level where this can achieve the greatest gains across the services - at the CJOC / CFD level. The establishment of a champion [for force

development] will enable strategic planning for the single entity service provider.

Regardless of the in-garrison ownership of the CFJSR, its sole function must remain dedicated to the provision of joint C2 for CAF operations.

The pillar of technology is a crutch for the delivery of C2 as CIS integration plays a critical function. There are existing technology delivery projects ongoing across the services, and the integration of C2 delivery capability must include the CFJSR as the subject matter expert (SME) for joint operational C2. Even the CFJSR Modernization Project is dedicated to the delivery of what will be equipment edging on obsolete by the time the unit is capable of employing it. A joint enabler is required which can integrate disparate systems / information into a cohesive whole for the commander as well as ensure that the integrated network is properly defended.

CONCLUSION

“The Canadian Armed Forces must continue working to become a joint, interoperable, and integrated force” with view to ensuring all future capability development is integrated, adaptive and networked.⁴³ The future of command and control in this environment at the operational level must be recognized and reinforced as a dedicated mission set for the only CAF organization dedicated to this goal, the CFJSR.

This paper considered and assessed the aspects of the current and future security environment and derived a common theme of joint, interoperable and integrated C2 in the

⁴³ Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. (27 January, 2009). p 89-91

future spanning each of the domains (air/land/sea/cyber). It also looked at the current capabilities through doctrine and organization and showcased the CFJSR as an existing CAF joint C2 enabler. Unlike the services within individual requirements directorates (such as Directorate of Land Requirements - DLR or Directorate of Air Requirements - DAR), the CFJSR has, surprisingly, not been integrated into the operational C2 concept of operations. It has been explained that while technical solutions currently exist to joint interoperability issues, there is a requirement for a shift in the culture of joint operational C2 as the complexity of the environment increases. Given the growing number of stakeholders, the emerging technology and synthesis of information required to ultimately support a joint force commander and his decision making process, C2 cannot be ad hoc and an organization dedicated to this is more relevant now than any other time in history.

Through the analysis of the current and future security environment, this paper demonstrated that the CFJSR's ability to fulfill its mandate is in jeopardy. This was influenced by a brief examination of the current doctrine and organizational structure which raised the issue that the current success the CFJSR has enjoyed has not been due to doctrine, technology or processes, but rather due to the ingenuity of extremely innovative soldiers. This paper also highlighted that if joint ownership of a revitalized CFJSR is not synchronized at the operational level, the CAF will have difficulty meeting the joint C2 challenges of tomorrow.

BIBLIOGRAPHY

- Alberts, David S. “Agility, Focus, and Convergence: The Future of Command and Control”. *The International C2 Journal*, Vol 1, no 1, 2007
- Barry, Charles. *Transforming NATO Command and Control for Future Missions*. *NATO World Security Network*. 15 Oct 2003
 URL: <http://www.worldsecuritynetwork.com/NATO/Barry-Charles/Transforming-NATO-Command-and-Control-for-Future-Missions>
- Canada, Department of National Defence, Director General Air Force Development. *Air Force Vectors*, Canadian Forces Aerospace Warfare Centre, 2014
- Canada, Department of National Defence, Commander Royal Canadian Navy. *Commander’s Guidance and Direction to the Royal Canadian Navy Executive Plan 2013-2017*. National Defence Headquarters, Ottawa, 2013
- Canada, Department of National Defence, Directorate of Maritime Strategy. *Leadmark The Navy’s Strategy for 2020*. National Defence Headquarters, Ottawa, 18 June 2001
- Canada, Department of National Defence, Director JC4ISR. *DJC4ISR Governance Workplan*. National Defence Headquarters: file 2700-1(DJC4ISR), 19 July 2013
- Canada, Department of National Defence. *Land Operations 2021 Adaptive Dispersed Operations. The Force Employment Concept for Canada’s Army of Tomorrow*. Directorate of Land Concepts and Design. Kingston: 2007
- Canada, Department of National Defence, Commander JTF Games. *Report on the Strategic Lessons Observed and Recommendations Derived from Op PODIUM*. Joint Task Force Games: file 6497-333-1(JTFG/RDIMS #93042), 14 June 2010
- Canada, Department of National Defence, Commander Canadian Army. *The Army: Advancing With Purpose*. 2nd ed. Director Land Strategic Planning. Ottawa 2009
- Canada, Department of National Defence, Chief of Force Development. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. National Defence Headquarters, Ottawa. 27 January, 2009
- Canada. Department of National Defence. B-GJ-005-000/FP-001 *Canadian Forces Joint Publication 01 - Canadian Military Doctrine*. Ottawa: Canadian Forces Experimentation Centre. 2009

- Canada. Department of National Defence. Working DRAFT 1: *Canadian Forces Joint Publication 06 - Communication Information Systems Doctrine*. Ottawa: Canadian Forces Experimentation Centre. DRAFT
- Canada. Department of National Defence. B-GL-300-003/FP-001 *Command in Land Operations*. Kingston: Land Force Doctrine and Training. 2007
- Canada. Department of National Defence, Chief of Force Development. *Command Domain Capability Alternative Report*. National Defence Headquarters, Ottawa. August 2008
- Canada, Department of National Defence, *Projecting Power: Canada's Air Force 2035*. Edited by Dr. Andrew Godefroy. The Canadian Forces Aerospace Warfare Centre: 2009.
- Canada, Department of National Defence, Commander Royal Canadian Air Force. *Future Concepts Directive*. National Defence Headquarters. Ottawa. 4 April 2013
- Canada, Department of National Defence, Vice Chief of Defence Staff. *Command and Control Operating Concept*. National Defence Headquarters. Ottawa. 14 June 2012
- Canada, Department of National Defence, Vice Chief of Defence Staff.. *Communications and Information Systems Operating Concept*. National Defence Headquarters. Ottawa. 13 March 2013
- Canada, Department of National Defence, Commander 1st Canadian Division. *1st Canadian Division Headquarters Command and Control Information Systems Statement of Capability Deficiency*. 1st Canadian Division, Canadian Forces Base Kingston: 3350-1(Comd), 19 June 2012
- Canada, Department of National Defence, Vice Chief of Defence Staff. *C4ISR Capability Development Strategy*. National Defence Headquarters, Ottawa. 13 July 2009
- Clare, Richard. "Cyber War - The Next Threat to National Security and What to Do About It" HarperCollins: 2010
- Davidson, Janine. *Operationalizing the Comprehensive Approach: The Military as "Enabler..."*, Small Wars Journal (18 Feb 2009).
URL: <http://smallwarsjournal.com/blog/operationalizing-the-comprehensive-approach-the-military-as-enabler>
- Dawe, P. Colonel. *Post-Tour Observations from Op ATTENTION Roto 0 TF DComd*. 16 March 2012.

Hathaway, Oona A., R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel. "The Law of Cyber Attack." *California Law Review* 100, no. 4 2012

Langland, K.G. Lieutenant-Commander. *Update Report-Canadian Future Mission Network Activities and Plans*. National Defence Headquarters: file 1775-1(DJC4ISR), 18 July 2013

Mitchell, Paul. "Cyberpower, Cyberwar." Lecture, Canadian Forces College, Toronto ON April 30, 2014

NATO, Allied Joint Doctrine *AJP-01(D)*, December 2010

NATO, Director C2CoE. *NNEC Best Practices Handbook, Catalysing the Art of C2*. ver 1.0 July 2009

Tangredi, Sam J. *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001-2025*. McNair Paper 63, Institute for National Strategic Studies, National Defense University. Washington, DC. 2000

United States. Department of Defense. Joint Publication 3-31 *Command and Control for Joint Land Operations*. Washington, DC: 24 February 2014