CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 33 / PCEMI N^{o} 33

MASTER OF DEFENCE STUDIES

THE FUTURE REQUIREMENT FOR AN INTEGRATED COMMAND AND CONTROL SYSTEM – FINDING A PATH TO SUCCESS

By/par Major Lee J. Hammond

Term Three, Syndicate 5

22 April 2007

CONTENTS

ABSTRACT

The establishment of Canada Command and Canadian Expeditionary Forces Command prompted the Chief of Defence Staff to issue supplemental direction to the Canadian Forces in 2006 to redouble its efforts to create an Integrated Command and Control System. This direction was issued almost four years after this capability requirement was first articulated in a comprehensive plan known as the C4ISR Campaign Plan.[1] The enclosed paper has a two part thesis. First, the current approach to field an IC2S into the CF remains inadequate. Second, these inadequacies can be overcome and success is achievable if the recommendations of the paper are followed.

In order to support its thesis, the paper is broken down into two parts matching the double thesis format. Part I, includes Chapters 1 to 3, and is an analysis aimed at identifying the challenges and limits faced by the CF with its existing approach to acquiring an IC2S. Part II of the paper is aimed at educating the reader on how the CF can achieve its goals with an IC2S. This part begins with Chapter 4, where the results from the author's consultation with a broad variety of servicing CF personnel are presented. Subsequent chapters offer examples of allied successes with example technologies, and recommendations on what factors the CF should carefully manage in introducing an IC2S.

Overall, the paper seeks to highlight that despite a clear vision, a good plan, and well articulated orders, success for the IC2S is far from certain. However, the author argues that these challenges can be overcome if new internal processes, and a new way of thinking are applied to acquiring an IC2S.

---

[1] C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

INTRODUCTION

In August 2006, in a letter to top Canadian Forces leaders, the Chief of Defence Staff (CDS), General Rick Hillier, emphasized the importance of the Canadian Forces (CF) acquiring an Integrated Command and Control System (IC2S) as a top priority. In this letter, Hillier envisioned a system that spans strategic, operational and tactical realms in an environment of Command Centricity and Mission Command.[2] The mandate of the system, in General Hillier's view, is to "enable commanders to engage and exercise effective command."[3] Hillier stated clearly that existing systems are falling short in fulfilling this need.

General Hillier's letter reflects efforts by the Canadian Forces (CF) to improve their capabilities in the area of Command and Control (C2). His direction to subordinates was a reflection of two facts. First, existing C2 systems are insufficient for the new organizational structures such as Canada Command (Canada COM) and Canadian Expeditionary Forces Command (CEFCOM). Second, the disbandment of the Deputy Chief of Defence Staff (DCDS) organization has left efforts to improve C2 capabilities, particularly at the Strategic and Operational levels, in some disarray.

The CDS envisions immediate steps to rectify the noted operational shortcomings, particularly the requirements of Canada COM and CEFCOM. In subsequent phases, he has directed that the wide variety of networks currently in use by the CF be converged within two years, and that the new system provide a single integrated capability operating at the Secret level. Longer term goals envision a full operational capability through

---

[2] General R.J. Hillier, *CDS Directive – Command and Control Information System* (NDHQ Ottawa: file 1243-1 (CDS)), 4 August 2006, 1.

[3] *Ibid*., 1.

enhancements over time, including the ability to operate with other government departments and allied classified systems.[4]

With General Hillier, a clear vision is rarely lacking. Indeed, his orders reinforce the objectives of CF experts in the field of C2, and are reflective of long time efforts. While this paper was originally envisioned as an aid to defining the needs of a future IC2S, in fact, a clear understanding of what the CF wants, and how to get there, has already been articulated in the C4ISR Campaign Plan, published in 2003. However, even with a clear CDS vision and a comprehensive plan, there remains much doubt as to whether the Canadian Forces can achieve its goals.

To begin, does the CF possess the institutional wherewithal to achieve its vision in an area that is challenging the most technically advanced nations in the world, including Britain, the United States, and Australia? Second, will the CF commit the necessary personnel and funding resources, virtually in perpetuity, to operate in the digital arena? Third, will the existing project approval processes and doctrine be appropriate for delivering the needed capabilities to the CF – and, will other Government Departments such as Treasury Board accept that the CF may never achieve 'Final Operating Capability' (FOC) in this area? Finally, despite the quality and depth of the briefings offered to the senior levels of the CF, do senior leaders truly understand the technical difficulties and evolutionary nature of the advances taking place today? Hence, the fundamental questions facing the CF in introducing an effective IC2S are related to the means available, human resource challenges, the doctrinal underpinnings of an IC2S, and finally, the necessary leadership that will be required for effective implementation.

---

[4] *Ibid*., 1.

To address these and related questions, this paper will make two principle arguments. First, the current approach to field an IC2S into the CF remains inadequate. Second, these inadequacies can be overcome and success is achievable. There are good news stories in the world of C2, and Canada can leverage these successes to improve its own capabilities. In general terms, the achievement of the goals outlined in the C4ISR Campaign Plan and the CDS vision will not be easy, quick, or inexpensive. Realizing this fact up front is one of the goals of this paper, and planning for the difficulties that the CF will encounter in a realistic way will ensure that the CF continues to get closer to its C2 goals.

This paper is broken down into two Parts. Part I, which includes Chapters 1 to 3, is an analysis aimed at identifying the challenges and limits faced by the CF with the existing approach to acquiring an IC2S. It provides a view of the current situation in the CF, including existing capabilities, the vision for the future and ongoing work. Additionally, the doctrine under which a future C2 system must operate is examined in Chapter 2, while the challenges to a future C2 system are covered in Chapter 3. Part II of the paper is aimed at educating the reader on how the CF can achieve its goals with an IC2S. This part begins with Chapter 4, where the results from the author's consultation with a broad variety of servicing CF personnel are presented. In Chapter 5, the successes of allied nations in various areas related to IC2S will be highlighted. In Chapter 6, recommendations on what factors the CF should carefully manage in introducing an IC2S are offered. While nothing in this Chapter will be revolutionary, it is hoped that the layman will benefit from some of these recommendations. Finally, some conclusions are

offered in Chapter 7.[5] By the end of the paper, the goal is to ensure that the reader understands that success with a future IC2S is achievable, but getting there will not be easy.

[5] The Canadian Forces have not yet definitively selected the acronym that will be used when describing the concepts outlined in this paper. Thus, the very generic term C2, and occasionally terms such as C4ISR and IC2S will be used. Nevertheless, when these or other terms are used, they should be viewed as falling within the same generic category. Other synonymous terms that are in wide use include C2IS, which includes Information Systems; Command, Control, Communications and Computers (C4); C4I, which includes Intelligence; Integrated Command and Control System (IC2S); and C4ISR, which adds Surveillance and Reconnaissance to Intelligence.

PART I

CHAPTER 1 – THE INTEGRATED COMMAND AND CONTROL SYTEM REQUIREMENTS

The aim of this first chapter is to explain the baseline from which the CF can move forward in achieving its IC2S goals. The complexity of both existing capabilities and future plans exceed the understanding of most personnel inside and outside the military. An idea of how complex may be understood from Figure 1. Nevertheless, in order to start with some common ground, this chapter will begin with a macro level description of current capabilities. By necessity, this description will not be holistic; however, it should frame the problem for the purposes of this paper. Then, a basic description of the current CF vision and desired characteristics for a future IC2S will be offered. Again, this description will only tell part of the story, since there are long documents describing the complete capability requirement. Current ongoing work will then be described. The CF is not starting from scratch, and these efforts will show where the CF is today in achieving its goals. Finally, the Chapter will conclude with a very brief discussion on the contemporary operating environment as it relates to C2. Taken together, this chapter will set the scene for where the CF is, where it is going, and for subsequent discussions where some of the shortcomings in the current plans will become apparent.

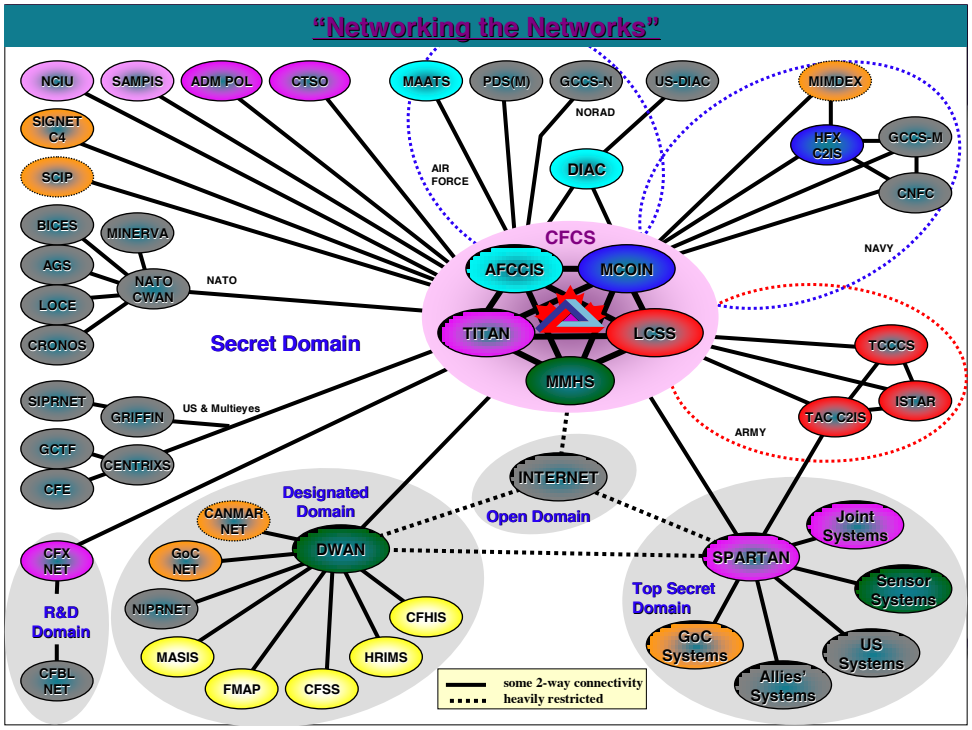

Figure 1 – Complexity of the IC2S Project Requirement
Source: C4ISR Campaign Plan

1.1 CURRENT CAPABILITIES

In this section the Command and Control capabilities currently in use by the CF at the unclassified and classified levels will be described. To begin, an examination of existing C2 capabilities will immediately uncover a perplexing alphabet-soup of different systems with exotic code names or acronyms. To assist the reader, a Glossary of the various acronyms, code words and normal usage of each system is provided at Appendix 1. Therefore, this section of the paper will provide a very macro level understanding of current C2 capabilities and their shortcomings.

The most widely accessible C2 system in the CF is the DWAN. As the default unclassified desk-top system, the DWAN is the primary tool for internal and external communications in the CF. Its capabilities duplicate that of a home-based desk-top

computer that is connected to the Internet, with appropriate firewalls, and with added specialist military software applications. A Defence Intranet, which rather poorly duplicates the capabilities of the Internet, is also a component of this system. In summary then, the DWAN is the system that virtually all CF members use daily for most of their tasks.

The capability deficiencies of the DWAN are at the centre of current CF C2 shortcomings. The most important factor is that the DWAN operates in the unclassified domain, which has "engendered a poor Operational Security (OPSEC) culture as well as believing [sic] that everything that we need to do can be effected [sic] at the Unclassified (UNCLAS) level."[6] Simply expressed, classified systems are so limited in number, most members of the CF work in the unclassified domain, when in all probability, this is often not appropriate. Moreover, because the majority of personnel within the CF have no access to classified material, the advantages that this material could provide to commanders is often unavailable.[7]

There are several other major issues concerning the DWAN. For example, even within the unclassified domain, the information available to users is often difficult, if not impossible to find. The efficiency of *Google* is not replicated on the Defence Intranet, for example. Moreover, keeping the DWAN consistent with the needs of the CF has also been a challenge. Experts describe the DWAN as the most unresponsive and most difficult network to manage. One officer stated that "it seems that there is not a single

---

[6] Name Withheld, Consultation A, Naval Commander, consultations with author, February 2007.

[7] Research and Development Canada, Sandy Babcock, "DND/CF Network Enabled Operations Working Paper," (Toronto: Directorate of Scientific and Technical Policy, January 2006), 44.

organization in the CF that cannot veto some advancement on that network."[8] Thus, the DWAN is clearly deficient in meeting contemporary CF needs in that it is unclassified and unresponsive.

In the classified realm, the CF possesses a wide variety of systems. To start, the CF has limited access to different versions of the American Global Command and Control System (GCCS), and there is a desire to access to the American Secure Internet Protocol Network (SIPRNET). National systems include examples such as TITAN, MCOIN, AFCCIS, LCSS, ADDN, and MMHS, to name but a few. While many of these systems are highly effective in the role for which they were intended, there are two essential problems. First, most often these disparate systems cannot communicate with each other, and more importantly, their distribution is highly restricted. For example, the current CNet, a Canadian/US system, hosts approximately 5000 users across all commands, but it "lacks the reach of a national C2 system and incompatibilities exist within the current [individual] components."[9] Thus, despite their individual usefulness, the wide variety of different secure systems hinders the effectiveness of the CF overall due to compatibility problems and limited distribution.

Compatibility between the various systems at the tactical level is also a major shortcoming of existing C2 systems. Each of these systems "operates a variety of applications and is supported separately."[10] They also typically run on different

---

[8] Name Withheld, Consultation B, Army Signals Lieutenant-Colonel, consultations with author, February 2007.

[9] Lieutenant-General W.J. Natynczyk, *VCDS Direction – CF Integrated Command and Control Information System* (NDHQ Ottawa: file 2700-1 (CFD)), 18 September 2006, 1.

[10] *Ibid*., 2.

operating systems, and…cannot be integrated in the existing C2IS.[11] These capabilities include various versions of the LINK System, radios and other communications means that are not all compatible. Nevertheless, they are important from a Joint perspective, since they provide the raw data needed by national command and control systems. Therefore, it would be accurate to state that current classified capabilities within the CF are a conglomeration of different systems acquired over many years, without much consideration to integration or Joint interoperability. Given these shortcomings, the need for a clear CF vision for a future C2 capability is a necessity, and perhaps not surprisingly, such a vision does exist.

1.2 THE CF VISION

This section will outline the CF vision for a future IC2S as expressed by both the senior military leadership, as well as in the formal CF documents that are currently guiding this capability development. It should be emphasized that the problems outlined above have been well understood for some time. Hence, the CF has painstakingly formulated its vision for the future in the C4ISR Campaign Plan, which is reinforced by a bevy of supporting documents, analysis and studies. The intent of this document "is to provide central coordination for developing C4ISR capabilities in order to place them on an evolutionary path toward an end-state where the boundaries between systems cease to be barriers to C2 progress."[12] Within these documents, the CF has essentially answered the question of 'what' they want, and they have formulated at strategy of 'how' to

---

[11] *Ibid*., 2.

[12] Department of National Defence, *Canadian Forces C4ISR Command Guidance and Campaign Plan* (Ottawa: Deputy Chief of Defence Staff, December 2003), 12.

achieve their vision. The following sections will outline some of the most important aspects of this vision.

1.2.1 Desired Characteristics

The objective is a CF-wide C2 capability that provides operational advantage across the spectrum of military operations, with a goal of trusted and relevant information provided in a timely manner.[13] This vision is based on the tenant that "the act of exercising command and control rests on the interaction of people, whose behavior is shaped by doctrine, structure and information."[14] The C4ISR Campaign Plan and the CDS direction have been designed to address all of these aspects, and thus, it is worth examining what the desired characteristics of the future IC2S will be.

In a letter dated 18 September, 2006 the Vice-Chief of Defence Staff (VCDS) issued direction supplementing the guidance of the CDS in his letter. This comprehensive direction reinforced the most important goals articulated in the four year old C4ISR Campaign Plan. While a great many features were outlined as desirable, the most important goals were to integrate the capabilities of existing systems into a single 'system of systems.' Moreover, the VCDS articulated the requirement to have up to 50,000 users operating in the Secret domain, and that the system be available for domestic and international users. As well, the VCDS emphasized the importance of the system providing seamless operation from the tactical to the operational level.[15]

---

[13] Department of National Defence, *Canadian Forces Command Decision Support Capability: Principles and Goals* (Ottawa: Director General Joint Force Development, September 2003), 6.

[14] *Ibid*., 9.

[15] VCDS Direction, 1.

The most important component of the CF vision, and one on which this paper will expend considerable effort, is the desire to establish an integrated Common Operating Picture (COP). In order to provide this, the intent is to migrate to a common core using the United States Department of Defense Global Command and Control System (GCCS).[16] The COP is envisioned as being user definable, and as having the capability to show a plan and its intent, with the ability to 'drill down' to the level of detail required by users. The COP will actually consist of multiple COPs from each environment, all joined together to provide general situational awareness.[17]

If one considers the vision articulated by the CDS, the VCDS, and in the C4ISR Campaign Plan, it is clear that the CF has a detailed and comprehensive requirement for what it wants. The shear scope of the vision is breathtakingly ambitious when compared to current capabilities. Indeed, one might wonder whether even half of these goals are obtainable in the timeframe envisioned. As this paper will show, it will take more than a clear plan and good vision to obtain these goals.

1.3 CURRENT ONGOING WORK

The current work being undertaken by the CF on IC2S capabilities is based on the direction provided in the now four year old C4ISR Campaign Plan. The recent CDS and VCDS direction is aimed at providing new impetus to this area of endeavor in a climate where successes have been very slow to appear. Indeed, the CF experience over the last four years has shown some of the difficulties that lay ahead. This section will explain some of the details of the Command directives and the C4ISR Campaign Plan, where the

---

[16] Department of National Defence, *Canadian Forces C4ISR Campaign Plan – Interim Report* (Ottawa: Director Joint Force Capabilities, June 2003), 6.

[17] *Ibid*., 11-12.

CF is in achieving its milestones, and more importantly, where some of the impediments are beginning to arise.

In his supplemental guidance, the VCDS emphasized the importance of immediately addressing some of the most immediate governance issues facing IC2S.[18] In response to this guidance, by 30 November 2006, Director Joint Capability Production (DJCP) 6 was able to report that plans for an improved governance structure were ongoing, and that some convergence activities between the Navy's MCOIN System and the Canadian Forces TITAN systems were already underway. Moreover, a migration strategy for the integration of the Air Force AFCCS system and the Army's LCSS into the larger network was being studied.[19] At the same time, the IC2S project staff, following analysis of the CDS vision, reported that in addition to the IC2S project, "other initiatives, and existing projects, [will] provide the solution to the CDS vision."[20] Thus, it is clear that already, some significant progress towards the CF and CDS vision is being achieved. However, some significant challenges remain.

A supporting partner project to the IC2S, is the Joint Intelligence and Information Fusion Capability (JIIFC) Project. This project has resulted in the creation of a JIIFC Detachment in the Ottawa region, which has until now focused on turning concepts and vision into real practical capabilities. The *COMMAND VIEW* System is an example of

---

[18] VCDS Direction, 1-2

[19] Lieutenant-General W.J. Natynczyk, *Quarterly Progress Report on the Implementation of a CF Integrated Command and Control Information System* (NDHQ Ottawa: file 2700-1 (DJCP 6)), 30 November 2006, 2.

[20] Department of National Defence, *Integrated Command and Control System: Interim Findings* (Ottawa: DND Canada, January 2007), 2.

the efforts of this organization. Unfortunately, the JIIFC project is "in recovery,"[21] while it completes necessary project documentation and completes a work break-down-structure.[22] This hiatus in activity is reflective of many CF projects, particularly those involved with C2. It demonstrates the challenges of resource shortages in both personnel and funding, which are perhaps the two biggest threats to the CF vision.

Current work on the IC2S capability is using a system of convergence points first described in the C4ISR Campaign Plan.[23] These convergence points are consolidated into a Target Integration Model (TIM) that features specific milestones. TIM 08 is aimed at delivering capabilities by 2008, and is the current CF focus. Amongst its many goals, TIM 08 specifically aims to achieve a "robust, interconnected, and integrated C4ISR capability in support of decision making."[24] The most important component of this goal is the establishment of the COP.[25]

---

[21] Department of National Defence, *Briefing to CDS/VCDS – Joint Information and Intelligence Fusion Capability Detachment Update: JIIFC Det Strawman to 2010* (Ottawa: DND Canada, 18 December 2006), Slide 8.

[22] *Ibid*., Slide 33.

[23] Department of National Defence, *Canadian Forces C4ISR Command Guidance and Campaign Plan* (Ottawa: Deputy Chief of Defence Staff, December 2003), 6.

[24] *Ibid*., 13.

[25] *Ibid*.,53.

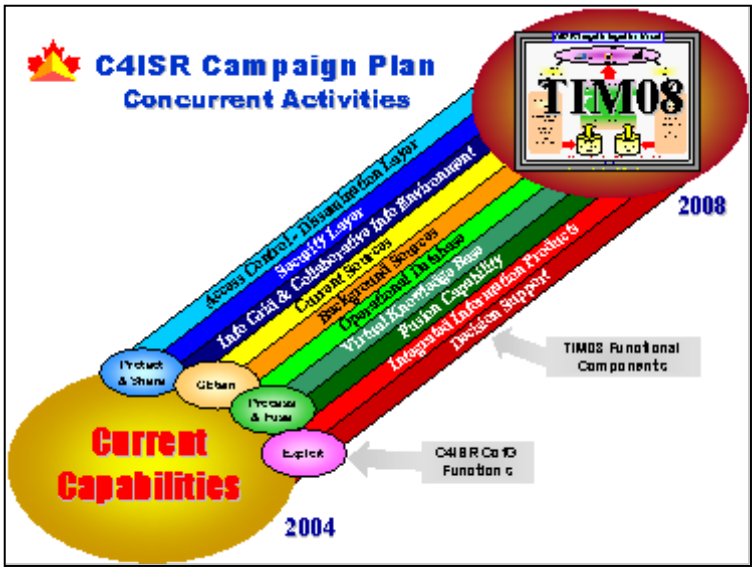

Figure 2. – The Target Integration Model
Source: C4ISR Campaign Plan Operational View 1

Clearly, with the stand-down of the DCDS staff, which necessitated the CDS and VCDS direction of 2006, the goals of TIM 08 are in peril of not being met. This demonstrates the great challenges facing a project as complex as IC2S. Even though the C4ISR Campaign Plan articulated a clear approach that recognized the evolutionary nature of technology, the external distraction of CF wide organizational changes have had a major impact on the progress of the project.

1.4 THE CONTEMPORARY OPERATING ENVIRONMENT

One of the great challenges in delivering a Crown Project is that it must be undertaken in a climate of continuous change, which always presents the danger of recent work becoming quickly obsolete. This reality is especially relevant to C2 projects due to their heavy reliance on fast changing technologies. One of the factors that has rapidly changed over the life of the C4ISR Campaign Plan is the Contemporary Operating Environment (COE). Thus, the aim of this section is to set the scene for the future IC2S by providing a basic overview of those principle factors of the COE that will affect IC2S. Three main areas will be covered, including the changing environment of conflict itself, the changing nature of the threat, and the fact that coalitions will continue to play a

predominant role in Canadian operations. While these three areas are far from being the only aspects of the COE that will affect IC2S, they are especially relevant, and thus will be the focus of this section.

1.4.1 The Changing Nature of Conflict

A significant factor that will influence the requirements for a future IC2S is the changing nature of conflict. This reality is well recognized by Canada and her allies, and has resulted in a plethora of new acronyms such as J.I.M.P, 3D+C, and D.I.M.E to name but a few.[26] Taken together, these widely accepted acronyms recognize that most problems in the world today cannot be solved by military means alone.[27] This, therefore, implies a greater degree of military integration with external actors such as Other Government Departments (OGD's) and Non-Governmental Organizations (NGO's). Indeed, "the CF will seek to operate in unison with Canadian interagency and multinational security partners."[28] Unfortunately, not all of these disparate groups are necessarily happy to integrate with the CF, nevertheless, the ability to pass information between these actors and the CF will be critical to future success.

An additional important requirement of a modern digital C2 system is that it must function in a non-contiguous battlespace. Higher headquarters and component parts "will

---

[26] D.I.M.E = Diplomatic, Information, Military, Economic; J.I.M.P = Joint, Interagency, Multi-National, Public; 3D+C = Defence, Diplomacy, Development and Commerce.

[27] Michael Thomson and Barbara D. Adams, *Network Enabled Operations – DRDC Toronto No. CR-2005-162*. (Toronto: Defence Research and Development Canada, May 2005); available from http://pubs.drdc-rddc.gc.ca/inbasket/CEBsupport.050513_1410.CR%202005-162%20final.pdf; Internet; accessed 19 April 2007, 5.

[28] Babcock, 4.

sometimes [be] continents apart."[29] It is this factor, more than any other, which may cause the CF desire for a COP to be exceedingly difficult to achieve. While Air Force and Navy elements have developed, over a series of decades, the Tactical Data Link Systems to feed the COP, the dispersed areas of operations over which the Army is now operating is a relatively new phenomenon. Moreover, the fact that Land Forces are now routinely operating in a 'three block war' environment, which is often highly urbanized, is also problematic. Radios do not work well in the concrete jungle of modern cities. Until recently, networks have been "optimized for operations in open areas and have difficulty supporting extremely fluid operations in complex and urban terrain, such as the mountains of Afghanistan or the streets of Baghdad."[30] Thus, the physical posture of modern military forces, with their highly dispersed operations in complex terrain will prove to be a major challenge to the future IC2S.

Finally, intelligence will play a key role in building the utility of the COP.[31] Much of this intelligence may not come from CF or allied sensors, but may, for example, be provided by NGOs, foreign nationals, or CSIS. This reality will apply on both international and domestic operations, and will make the job of an IC2S exponentially more difficult.[32] Consequently, the integration challenges of IC2S will be far more difficult than simply digitizing the CF alone.

---

[29] Brigadier-General G.W. Nordick, "Guest Editorial: Command and Control Aspects of Digitization," *The Army Doctrine and Training Bulletin* Volume 6, Number 1 (Spring 2003), 1.

[30] Christopher J. Toomey, "Army Digitization: Making it Ready For Prime Time," *Parameters* 33, Number 4 (Winter 2003-2004) [Journal on-line]; available from http://www.carlisle.army.mil/usawc/Parameters/03winter/toomey.htm; Internet; accessed 18 April 2007, 3.

[31] Department of National Defence, *Capability Development Record – Command* (Kingston: Director Army Doctrine, June 2006), 23.

1.4.2 The Changing Threat

The nature of the military threat will also significantly challenge a future IC2S. For example, in traditional military operations "the enemy is well defined; in operations other than war, changing environments and situations may lead to rapid, radical shifts in the definition of the enemy."[33] Moreover, opponents could include sovereign armies, organized rebels, militias, irregulars, terrorist bands, civilians, rioters and looters.[34] Thus, the demands upon the IC2S will be significantly greater, since the system will have to be protected and usable against opponents spanning the range from simple peasants, to sophisticated governments capable of employing network attack tactics. Thus, not only will the system require extensive security, it will have to be able to integrate with non-traditional information sources. Without these dual, but competing requirements, the IC2S will be of limited utility.

1.4.3 Coalitions and Their Impact

As the CF plans its future requirements, it must be capable of conducting operations in Canadian-only and international environments.[35] If the CF only ever conducted operations on its own, building an IC2S would be fairly straight forward. The reality, however, is that the land, sea and air elements of the CF routinely conduct operations with their counterparts from allied and coalition partners. More than any other

---

[32] *Ibid*., 25.

[33] United States, National Research Council, *Realizing The Potential of C4I* (Washington: National Academy Press, 1999), 54.

[34] David C. Gompert, Hans Pung, Kevin A. O'Brian and Jeffry Peterson, *Stretching the Network – Using Transformed Forces in Demanding Contingencies Other Than War* (Santa Monica, CA: Rand Corporation, 2004), 13.

[35] Australia, Department of Defence, Defence Science and Technology Organization, Leoni Warne, Irena Ali, Derek Bopping, Dennis Hart, and Celina Pascoe, *The Network Centric Warrior: The Human Dimension of Network Centric Warfare* (Edinburgh: DSTO Information Sciences Laboratory, 2004) [On–line]; available from http://www.dsto.defence.gov.au/publications/3430/DSTO-CR-0373.pdf; Internet; accessed 19 April 2007, 10.

factor, this takes the control over IC2S out of the hands of CF leaders, and places it with principle allies such as the United States, and the commercial companies that build the C2 technologies. It is for this reason that the IC2S system will never be 'done' in the normal sense of most projects. As standards and new technologies are introduced by Canada's allies, Canada will have no choice but to continuously adjust its plans, and adopt new systems where it makes sense to do so. Indeed, according to one Australian officer with experience in Iraq, "if you are not interoperable, there is no point even showing up."[36] Consequently, while the IC2S will demand interoperability with allies to be effective, achieving this goal will be expensive, continuous, and complex.

[36] Name Withheld, Consultation C, Australian Lieutenant-Colonel, consultations with author February 2007.

CHAPTER 2 – RELEVANT CF DOCTRINE

The IC2S will provide a single backbone C2 System for use by all elements of the CF. This mandate presents one of the greatest challenges to the project, since despite the apparent efficiencies in a 'unified' force, there is often greater doctrinal alignment between the Canadian Navy and U.S. Navy for example, than there is between the Canadian Navy and Army – or Air Force. Thus, this chapter will discuss the issue of doctrine, and its important role in setting the framework for an effective IC2S. In order to accomplish this, the Chapter will begin with some basic definitions. Then, a brief discussion on inter-departmental/agency doctrine, or rather the lack of it, will frame the doctrinal picture under which IC2S is being developed. The paper will then cover the state of CF Joint doctrine and that of the individual services. Then, the doctrinal goals for the IC2S system will be briefly described. At the conclusion of this chapter, the reader will recognize that one of the greatest risks to the success of CF plans is incomplete doctrinal preparation.

2.1 GENERAL DOCTRINE

Doctrine forms an essential foundation upon which all military plans and capabilities should be based. According to the CF Manual on doctrine development, doctrine is the "fundamental principles by which the military forces guide their actions in support of objectives. It is authoritative but requires judgment in application."[37] The various influences on doctrine can be seen at Figure 3. Of note are the influences of technology, the threat, and changing concepts. Also noteworthy is that the term doctrine is generally used only by the military. At one level higher from Joint doctrine is

---

[37] Department of National Defence, A-AE-025-000/FP-*001 Canadian Forces Doctrine Development* (Ottawa: DND Canada, 2003), iii.

government policy. The CF Doctrine Manual explains that the CF can develop doctrine in the absence of specific government policy. However, when the government does issue a policy affecting doctrine, then the doctrine must be modified to comply.[38]

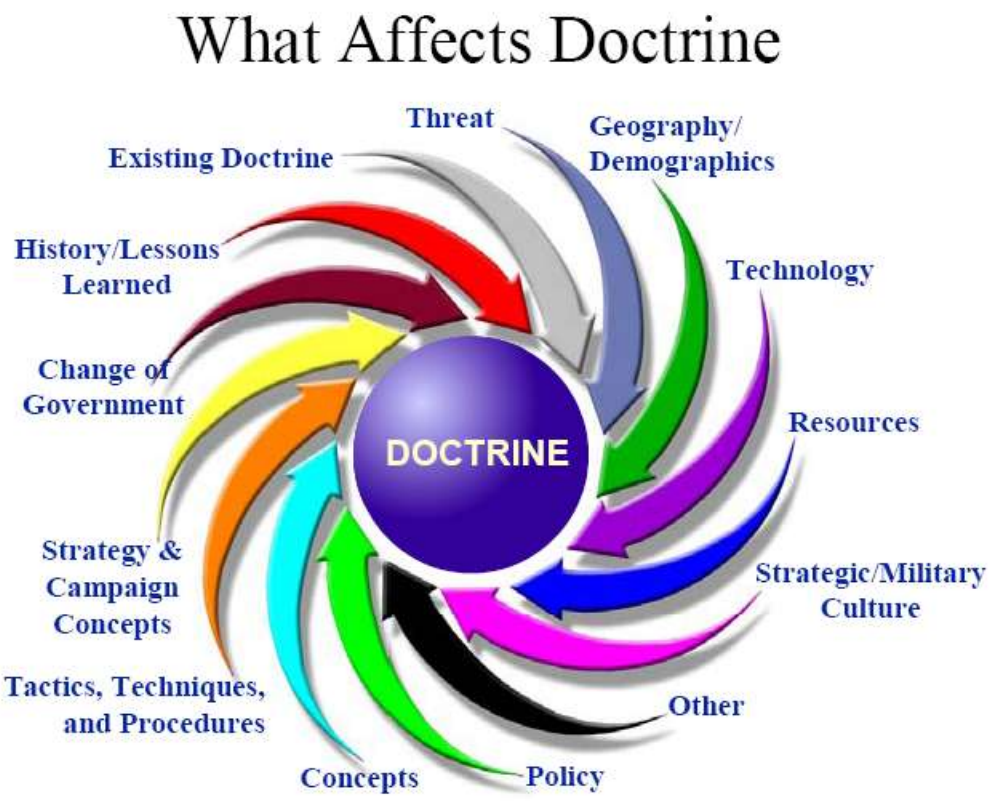

Figure 3 – What Affects Doctrine
Source: A-AE-025-000/FP-001

The first major challenge facing the IC2S project is the void between government policy, Canadian Forces Joint doctrine, and a 'doctrine equivalent' linking the Canadian Forces to the external actors upon which future military operations will depend. Interestingly, even complex evaluations of Network Enabled Operations conducted by Defence Research and Development Canada Sandy Babcock start their examination at

[38] A-AE-025-000/FP-001, ii.

the Joint level.[39] Nevertheless, the COE discussion in Chapter 2 highlights the fact that future operations will require more than just military means if they are to be successful. In a 'Whole of Government' environment, the CF will have to efficiently network with OGDs, International Governments, and perhaps even NGO's such as the Red Cross. Given this reality, one might expect that the Government of Canada is working on a comprehensive 'doctrine equivalent' for its Whole of Government Approach. The reality, as Canada's work in Afghanistan has made abundantly clear, is that little formal integration has been accomplished in the Command and Control of all Government of Canada operations at the Strategic and Operational level. This shortcoming is the principle risk to the IC2S project, since there is no framework driving departments like CIDA, Foreign Affairs, and the RCMP, for example, into a discussion with the CF over network integration to support a 3D+C or D.I.M.E. approach. Therefore, one of the foundations to a successful IC2S, the exchange of data with OGDs, has no formal doctrinal basis, and thus represents a significant risk to the project.

On an international basis, the situation is somewhat better. The CF has formally stated in their own doctrine that "CF doctrine, both joint and single-service, should be consistent with the doctrine of principle allies."[40] These allies include the United States, Britain, and Australia. Thus, the CF is routinely involved in doctrinal discussions and agreement with its principle allies through organizations such as NATO and ABCA, for example.[41] Thus, issues such as terminology, technology protocols, and standards are

---

[39] Babcock, 18.

[40] A-AE-025-000/FP-001, 1-7.

[41] NATO= North Atlantic Treaty Organization; ABCA= American, British, Canadian and Australian.

routinely worked to solution. This contrasts significantly with the current situation within the Government of Canada, where no such system of agreement exists. Thus, while national policy will sometimes guide the way, on what formal basis, for example, could the intelligence data-bases of CSIS and the RCMP be made available to the users of IC2S?

The next question facing the IC2S will be the weak foundation of CF Joint doctrine. At the time of writing, the CF had a single officer dedicated to writing this doctrine![42] Nevertheless, some of the more important aspects of Joint doctrine have been addressed. For example, manuals exist describing the process for writing CF doctrine, for the principles of leadership and command, and for Canadian Forces Operations. Despite these efforts there are huge gaps in CF Joint doctrine that will make the development of an IC2S a real challenge. Examples of these challenges will be described below.

For an IC2S, having a common doctrinal understanding of what constitutes Command and Control is critical to success. A Canadian Air Force Manual on Aerospace Command and Control highlights the fact that some endorse the concept of 'mission command,' while others endorse a philosophy of 'centralized control and decentralized execution' while still others embrace the notion of 'network centric' command philosophies.[43] On first glance, these appear as different constructs for Command and Control. However, despite these apparent differences, there is some

---

[42] Briefing to Joint Command and Staff Program 33. As of 15 November 2006, LCol J.G. Savard was the only officer in the CF assigned to writing Joint Doctrine.

[43] Department of National Defence, B-GA-400-000/FP-000 *Canadian Forces Aerospace Doctrine* (Ottawa: DND Canada, 2006), 6.

common ground. For example, there is doctrinal agreement that Command is defined as "the authority vested in an individual for the direction and control of military forces."[44] Moreover, whether an individual is a ship's Captain, an Air Force Aircraft Commander, or Army Unit Commander, it is generally true that Canadian leaders expect to be told what to do, not how to do it. Thus, the current Joint doctrine situation in the CF is somewhat schizophrenic.[45] There is common ground on basic definitions at the macro level; however, it is in the details where many challenges quickly become apparent.

Formal doctrinal expression varies considerably within the three different services. The Army possesses a large library of doctrinal publications that are well developed, and a comprehensive process for keeping these documents up-to-date. With the recent establishment of the Canadian Forces Aerospace Warfare Centre, the Air Force is now developing and expressing its own doctrinal concepts. Often, the Air Force has attempted to bring its own doctrine into relative alignment with the Army due to the latter's head start. So, for example, while the Army has formally expressed its Operational Functions as Command, Sense, Act, Shield and Sustain, the Air Force now has the terms Sense, Shape, Move, Sustain and Command within its doctrine.[46] Despite these lamentable efforts by both services, this approach reflects the fundamental

---

[44] Department of National Defence, B-GL-300-003/FP-000 *Command* (Ottawa: DND Canada, 1996), 1.

[45] Ross Pigeau, and Carol McCann, "Re-conceptualizing Command and Control." *Canadian Military Journal* (Spring 2002) [Journal on-line]; available from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc13/p519041.pdf; Internet; accessed 19 April 2007, 56.

[46] B-GA-400-000/FP-000, 37-47.

weakness of CF Doctrine, and is an inefficient way in which a comprehensive top down approach to doctrine development should occur.

If one examines the Canadian Navy, the real schisms in the CF Joint doctrine development process become apparent. For example, the Navy does not use the word doctrine in a formal sense at all. The terms Command, Sense, Act, Shield and Sustain, used the by the Army, are not formally recognized by the Canadian Navy. Instead, the Navy uses a different system which, from an Army and Air Force viewpoint, might be described as a mix of procedures, formal orders, and tactics. Known as Tactical Notes and Maritime Tactical Instructions, the Navy's approach to doctrine provides a system of formalized and approved common procedures that have been adopted by the fleet.[47]

Given the differences in both content and process in developing doctrine, it is not surprising that there are considerable variances between the services that will have a major impact on the IC2S. For example, with different doctrinal foundations, the Canadian Army and Navy use different tactical symbology, which is each unrecognizable to the other. Moreover, differences in language over the same terms also exist. For example, the Air Force may engage a target declared hostile, while the actual word hostile has a very different meaning to the Navy.[48] A failure to rectify these differences through a proper top down Joint approach to doctrine will create immense difficulties for the success of IC2S.

---

[47] Name Withheld, Consultation D, Naval Lieutenant-Commander, consultations with author February 2007.

[48] Consultation D.

2.2 DOCTRINE GOALS FOR IC2S

Although a review of the existing Joint CF doctrine would seem to indicate little focus on this important area of endeavor, the C4ISR Campaign Plan has nevertheless outlined some doctrinal goals for IC2S. Given some of the challenges outlined above, it is worth examining these goals. They include a desire for a more dynamic CF C2 doctrine based on the primacy of a knowledge centric approach to operations. Moreover, a goal is also to improve the planning for contingencies, and to learn and disseminate lessons learned from current operations.[49] If one examines these doctrinal goals, they all seem fairly straightforward, reasonable and sensible. However, given the problems outlined above concerning inter-governmental and Joint doctrine, one must ask whether these goals are feasible, achievable, or even the right priority.

The C4ISR campaign plan also recognizes the doctrinal realities of the COE. Yet, the existing documents are silent, or at least underemphasize, the risks associated with the lack of Canadian Joint doctrine, and the doctrinal complexities related to the external interactions that will be needed with non-DND actors. Thus, while the doctrinal goals outlined above may seem reasonable, it is suggested that they will not be achievable with the current CF approach to doctrine.

In conclusion, there are major doctrinal challenges to the successful implementation of the IC2S. These challenges begin with the fact that there are no formal mechanisms or doctrine in the military sense, to integrate the IC2S into the

---

[49] CF C4ISR Campaign Plan Interim Report, 26.

capabilities of the external actors upon which the success of the future system will depend. Internally, Joint doctrine remains very weak. Despite cooperation between the services and some attempts to align doctrine, the overarching Joint doctrine necessary to ensure common processes and language remains lacking. The personnel resources dedicated to solving the problems with intergovernmental and Joint doctrine remains totally inadequate, and present a high risk of failure to the IC2S.

CHAPTER 3 – CHALLENGES

This chapter will present some specific challenges that will occur within the context of the COE and doctrinal shortcomings outlined above. These challenges will present themselves despite the clear vision of the CF leadership, and despite the clarity of CF plans. Many of the lessons presented here have been learned the hard way by Canada's principle allies. If the CF is to succeed, it will have to surmount difficulties that even the most sophisticated nations are struggling to overcome. Nevertheless, the lessons learned by Canada's allies do represent an opportunity not to repeat past mistakes, and thus they are presented here for the benefit of future IC2S success.

The chapter will begin with an examination of the problems presented by people and processes. This is a universal issue that virtually all nations are dealing with. Then, the problems of establishing a common language and building the network from the bottom up will be presented. As already highlighted, a major component of the CF vision is establishing a COP, and this section will address some of the very real issues that the CF will face in meeting this goal. Then, some comments will be offered on the difficulties of networking systems. While this section will avoid too much technical detail, the joining of existing systems is often far from easy. The paper will then look at the experiences of allies using experimentation to build their systems, and the security challenges a system like IC2S will face. Finally, some comments on allied experiences and capabilities will be offered.

3.1 PEOPLE AND PROCESSES

This section will focus on the dual challenges of people and processes. To begin, people represent one area where current CF efforts may well lead to failure of the IC2S

project unless substantial improvements are made. These challenges include the training and qualifications of CF personnel, the number of personnel assigned, and issues related to the use of high technology equipment in a modern military force.[50]

3.1.1 Training and Qualifications

Over the last thirty years, the Canadian Forces has introduced numerous high technology capabilities that have strained individual and collective training systems. As an example, few are unaware of the giant technological leap that the CF-18 presented the Air Force when introduced. Similar examples exist within the Navy and Army. The question is, in the highly resource constrained environment of today, will the CF assign sufficient funding to address the key issue of personnel training?

Canada's principle allies have faced their own problems with it comes to training their personnel.[51] In a 2004 conference on Network Centric Warfare, one study group found that investments in the intellectual capital of a military organization are critical to the success of an integrated C2 system.[52] Moreover, in a British National Accounting Office report, it was highlighted that the British Ministry of Defence had to treble existing training facilities, which resulted in an increase of GBP 24 Million in costs, for a total of GBP 204 Million for the 25 year life of the Bowman communications system.[53]

---

[50] S.G. McIntyre, M. Gauvin and W Waruszynski. "Knowledge Management In The Military Context." *Canadian Military Journal*. (Spring 2003) [Journal on-line]; available from http://www.journal.dnd.ca/engraph/Vol4/no1/pdf/v4n1-p35-40_e.pdf; Internet; accessed 19 April 2007, 36.

[51] Australian Department of Defence, *Network Centric…, 35.*

[52] Lieutenant-Colonel Michael Ryan, "Finding Alligators: The Future of Network-Centric Warfare," *Australian Army Journal* Volume II, Number 2 (Autumn 2005), 107.

[53] Author Unspecified, "Bowman pulls in its horns," *Janes International Defence Review* (September 2006) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2006/idr10019.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B

Clearly, these are significant costs, and if the CF is to succeed with its IC2S, it will have to recognize the true funding requirements needed to support the training of personnel.

3.1.2 Assigning Personnel

A key requirement for an effective IC2S is to assign the necessary personnel, with the right training, to the task. Based on the recent past, the CF performance in this area is not encouraging. For example, in December 2006, the Project Director Staff for the IC2S project consisted of a single officer![54] The JIIFC Project reported that it was operating at 66% of the staff required.[55] Thus, inadequate staffing of C2 projects inevitably delays their introduction, and contributes to potential project failure.

The C4ISR Campaign Plan Interim Report argues that C4ISR is essentially a new capability, which will require additional personnel compared to current manning levels.[56] Ultimately, the CF has recognized that "people are the key to success or failure, as the processes and hardware are only tools that assist in achieving an effective Command Decision Support Capability."[57] This means that CF Transformation will have to recognize the Person Year (PY) demand of this capability compared to other priorities and make the necessary decisions on how far the CF can go with IC2S. Comparing available manpower with the requisite expertise may force an adjustment to the

---

80%5D%28+Bowman+%3CAND%3E+pulls+%3CAND%3E+its+%3CAND%3E+horns%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Bowman+%3CAND%3E+pulls+%3CAND%3E+its+%3CAND%3E+horns%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Bowman+%3CAND%3E+pulls+%3CAND%3E+its+%3CAND%3E+horns%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 2.

[54] Department of National Defence, *Integrated Command and Control System (IC2S) 2006 Year End Project Status* (Ottawa: DND Canada, DJCP 7-3, 22 December 2006), 5.

[55] JIIFC Strawman Briefing to CDS, Slide 9.

[56] C4ISR Campaign Plan Interim Report, 7.

[57] CF Command Decision Support Capability Principles and Goals, 11.

deliverables of the project, or perhaps more optimistically, to the timelines of the Target Integration Model.

3.1.3 The High Technology Force

Sufficiently trained experts who can deliver the IC2S capability are one thing; the ability of the CF to absorb and effectively employ the technology is another. According to Christopher Toomey, the US Army has learned that "digital skills are neither easily acquired or retained and require a steep learning curve for both soldiers and leaders."[58] These comments mirror both the author's own experience with TCCCS and the British experience with Bowman. Moreover, these challenges can be exacerbated by the rate at which new technologies are introduced into the forces. British soldiers have demonstrated the difficulty in service members adapting to the rapid changes that modern software and technology can achieve.[59] For further evidence of this, Lieutenant-Colonel David Schmidtchen, of the Australian Defence Forces, states that the ability of the ADF to "absorb, manage and integrate technological innovation will be the key step in making the transition to the network-enabled force."[60] Therefore, like the costs of actually introducing the technology, the CF must carefully measure and assess the impact that this technology will have on the effectiveness of the organization. If the new IC2S system

---

[58] Toomey, 3.

[59] Rupert Pengelley, "Bird in the hand: Bowman bridges the digital divide for British Army," *Janes International Defence Review* (September 2005) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2005/idr04296.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Bird+%3CAND%3E+in+%3CAND%3E+the+%3CAND%3E+hand%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Bird+%3CAND%3E+in+%3CAND%3E+the+%3CAND%3E+hand%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Bird+%3CAND%3E+in+%3CAND%3E+the+%3CAND%3E+hand%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 16.

[60] Alan Millet in Lieutenant-Colonel David Schmidtchen, "Network-Centric Warfare: An Idea in Good Currency," *Australian Army Journal* Volume II, Number 2 (Autumn 2005), 112.

requires extensive training time, the likelihood of failure in a resource constrained Canadian military will be very high indeed.

3.1.4 The Project Approval Process

Anyone who has ever experienced the Canadian Government's project approval process knows that it can be long, frustrating, and highly bureaucratic.[61] Small and under-resourced project staffs can make the process even more difficult. For the CF, demand always significantly exceeds the supply of available funding. Therefore, this reality has created an environment where a careful process of project prioritization and risk aversion has become the norm. Simply put, the CF can ill afford to waste its money, and therefore, no project is approved unless it has gone through multiple levels of scrutiny and careful examination by the CF and DND leadership.

There are now 138 projects, systems and initiatives related to C4ISR in the CF, all of which are undergoing the careful scrutiny outlined above.[62] Currently, projects within DND typically take a minimum of 7 years from initiation to completion. In some cases, this has been reduced to 18 months when the full process is followed. Projects needed in shorter timeframes typically use the Urgent Operational Requirement procedure.[63] Not surprisingly, the first VCDS Quarterly Report to the CDS on the IC2S project suggests, "the greatest challenges will be on the programmatic side, that is, aligning projects to deliver the required contribution to success; and the governance side, with 'encouraging'

---

[61] The comments in this section are the authors, and reflect experience as the Army staff officer advising the VCDS on all Army Capital Projects while employed in the Directorate of Force Planning and Program Coordination at NDHQ from August 2005 until July 2006.

[62] CF C4ISR Campaign Plan Interim Report, 38.

[63] CF C4ISR Command Guidance and Campaign Plan, 7.

the current system owners to support convergence."[64] Despite this rigorous process, it has been recently highlighted within the Chief of Force Development that "no one drives the boat from start to finish" when it comes to CF C2 projects.[65] Clearly then, there are major programmatic problems with the current CF project approval process when it relates to acquiring high technology.

The programmatic challenges faced by Canada mirror that experienced by Canada's principle ally - the United States. To illustrate, a report on C2 implementation challenges conducted by the United States National Research Council stated that "a key challenge to DOD and the services will continue to be to develop an appropriately responsive acquisition system that can procure, deploy, and exploit these commercial hardware and software capabilities in a timely and cost-effective way."[66] Thus, the Americans too are experiencing the same issues as Canada. If IC2S is to succeed, then a more streamlined project approval process seems necessary. Much of this needed change could be implemented internally within DND. However, discussions with Treasury Board by the senior leadership would also no doubt be required.

3.2 ESTABLISHING A COMMON LANGUAGE

The problems of differing language have already been described from a doctrinal viewpoint. However, there is also the issue of computer and technical languages that can be a major challenge in creating something like the IC2S. These languages and protocols are largely developed in two places. First, they are established by major principal allies

---

[64] VCDS Quarterly Report 30 November 2006, 2.

[65] Department of National Defence, *C4ISR CP Brief to CFOC* (Ottawa: LCol B.T. Pickard and LCol J.C.P. Jourdeuil, 27 Feb 2007), Slide 28.

[66] US NRC Report, 57.

such as the United States, and the related major alliances, like NATO and ABCA. Then, there is industry. Technologies such as TCP/IP and HTML have been developed for civilian applications, and for example, form the basic technology behind the Internet. These technologies have now migrated to the military, and are important for both national and international interoperability.

The problem for Canada is that the language of technology is constantly changing. The rules are made by major allies and industry, and thus, the CF will be involved in a continual process of evolution and modernization. IC2S will never reach Final Operating Capability because it will constantly have to evolve to adapt to new protocols, technology, and languages. This means that IC2S will never be perfect, and therefore, it will likely never provide 'near perfect' Blue Force situational awareness or any other information for that matter. The truth is the CF will succeed with some of its technologies related to IC2S, while other choices will inevitably fail, or become quickly obsolete.

3.3 BUILDING THE COP FROM THE BOTTOM UP

The principle technical challenge facing the IC2S is the requirement to provide a Common Operating Picture (COP). Understanding what actually constitutes the COP, is essential to understanding why achieving a useful COP will be so challenging. In Canadian doctrinal terms, the COP is

> a singular representation of operational information, based on common data and information shared by more than one command that can be tailored by users. The representation shows both temporal and spatial relationships, and assessed confidence value of the information. It facilitates collaborative planning, self synchronization and assists all echelons to achieve situational awareness.[67]

---

[67] Department of National Defence, B-GJ-005-300/FP-000 *Canadian Forces Operations* (Ottawa: DND Canada, 2005), 21-4.

Achieving this COP will depend upon the efficiency and utility of a wide variety of systems in use at the tactical level. In a technical sense, this will be the greatest challenge to IC2S, and this section will highlight some of the challenges that will be encountered in building the COP from the bottom up.

Within the aerospace and naval environments, the use of Tactical Data Links (TDLs) is widespread. The Air Force and Navy have made great strides in their abilities to exchange useful, relevant, and timely information. These networks, and their future successors, will inevitably form the backbone of the basic information flow into Operational and Strategic level components of the IC2S. They will also be crucial to the formulation of the Air and Naval components of the COP. Yet, as the users of these systems well know, they suffer from significant limitations, some of which will be highlighted below.

The most predominant existing Data Links include Link 11, Link 11B, Link 16, NATO Link 1, and Link 22.[68] The Canadian Navy and Air Force are longtime users of Link 11, while Link 16 is a newer capability whose full use is currently limited to the CF-18 fleet. When used with the Air Defence Systems Integrator, Link 16 can also be used between CF-18s, Canadian warships, and the Army's Air Defence Anti-Tank System. Link systems communicate using a variety of means, including secure land-line, satellite, and the UHF and HF bands. Using these latter two means, Link communications are often imperfect. For example, when using UHF, Line-of-Sight issues can be a major

---

[68] United States, Department of Defense, *Joint Data Network Operations* (Washington: Joint Staff, 2000), A-B-2.

limitation of the Link system.[69] Most importantly, a Link 16 network (the current widely deployed benchmark of the technology) "requires constant and dedicated attention by competent personnel to diagnose the network and fix, or recommend fixes to, problems as they occur."[70] Thus, while highly useful, Link systems do suffer from significant limitations that inhibit their ability to provide 'near perfect' information.

If one examines the Army, the ability of low-level tactical systems to provide the necessary reliability and completeness in their information to a higher IC2S is even more questionable. The leader in this field is unquestionably the U.S. Army. Its Force XXI Battle Command Brigade and Below (FBC2B) system provides reasonably reliable Blue Force information using the Raytheon Enhanced Position Location Reporting System (ELPRS) radio[71] and satellite communications. However, the system has proven less adept at providing timely information on the enemy, and unfortunately, US Army experience is that "containers tied to trucks are highly unlikely to sustain unbroken connectivity with leading echelons in fast-moving scenarios…"[72] Moreover, the fact that modern armies are routinely working in complex terrain, particularly urban terrain, and the fact that the lowest level that needs to feed the COP is a single soldier, one can

---

[69] *Ibid*., D1.

[70] *Ibid*., F1.

[71] Rupert Pengelley, "Network power: communications systems join up command levels," *Janes International Defence Review* (March 2007) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2007/idr10302.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Network+%3CAND%3E+power%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Network+%3CAND%3E+power%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Network+%3CAND%3E+power%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 2.

[72] *Ibid*., 2.

appreciate that building the COP from the lowest land component level has proven exceedingly complex and difficult.

Thus, it is not surprising that the IC2S project staff considers that the main challenges related to the COP will be "multiple and overlapping geospatial applications, data management and user expectations for capability."[73] The bottom line is that the tactical systems feeding the COP remain imperfect and prone to error and this includes forces that have been using mature Link systems. Thus, the desire of the CF for 'near-perfect' Blue Force situational awareness will remain largely unobtainable for some time to come.

3.4 NETWORKING THE SYSTEM OF SYSTEMS

With the challenges of building the COP from the bottom up now described, this section will address some of the challenges of bringing networks together. The specific focus will be on network discipline, non-compatible technologies, and bandwidth. Clearly, these are not the only complexities that can occur when bringing various network systems together. However, they are representative of some of the problems that Canada could encounter as it introduces IC2S.

A key component in having networks function effectively together is the ruthless adherence to common standards, protocols and language. While this may inhibit the introduction of newer and more capable technologies in some instances, it will allow for the greatest number of separate systems to work effectively together. This is the basis on which the successful Link 11 and 16 systems have been developed, and is essential if the widely disparate projects and systems that are being developed at any one time are to

---

[73] Department of National Defence, *Integrated Command and Control System…*, 3.

work towards a Joint solution. This requirement is mentioned so often throughout the documentation on C2, that it should be considered somewhat of a mantra. Therefore, systems that do not meet common and agreed standards should not be approved if networks are to function together effectively. In other words, new systems have to be "born joint."[74]

Unfortunately, the CF has not proven disciplined in the past on this issue. The number of possible vetoes affecting the DWAN has already been described. Moreover, on a Government of Canada basis, there is also a lack discipline from a standards perspective. Thus, if the CF is to effectively introduce IC2S, it will have to apply uncompromising standards to the various projects and Service leaders, who are normally the project sponsors for IC2S related capabilities, in order to ensure that projects remain aligned with Joint goals. If the OGD mandate of IC2S is also to be met, then Canada will have to improve its performance from a Government wide basis as well.

There are instances where the various technologies of a given network are inherently incompatible. For example, in 1998, the US Navy was forced to cancel the deployment of two of its Aegis Class cruisers when new computer upgrades associated with the Cooperative Engagement Capability (CEC) disrupted the ships existing Aegis combat systems.[75] The new CEC software, with over five million lines of computer

---

[74] United States, Department of Defense, Ms. Robin Quinlan, *Presentation - Family of Interoperable Operational Pictures (FOIC)* (Washington: Office of the Secretary of Defense, date unknown), Slide 5.

[75] Author Unspecified, "Software Problem Prevents Deployment of U.S. Navy's CEC," *Janes Defence Weekly* (July 1998) [Journal on-line]; available from http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw98/jdw02505.htm@current&Prod_Name=JDW&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Cooperative+%3CAND%3E+Engagement+%3CAND%3E+Capability%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Cooperative+%3CAND%3E+Engagement+%3

code, made the Aegis system "unable to perform it primary missions, including weapons cueing and monitoring potential air threats to the battle group."[76] Many of these problems were due to the use of Commercial-Off-The-Shelf display systems.[77] Thus, it is quite possible that important systems currently in use will have to be retired in favour of newer systems that are capable of integration into the new IC2S network. Having the institutional courage to affect these decisions in the face of potentially major opposition from various L1s will be a test of the CF leadership.

The final networking challenge that will be addressed is that of bandwidth. According to General Harry B. Raduege Jr, the Director of the Defense Information Systems Agency (DISA), "we can develop and implement all the net-centric services we want but if the back-bone is bandwidth constrained or inadequate in other ways then the benefits we gain from net-centric warfare will be limited."[78] Unfortunately, solving bandwidth issues can often involve very expensive solutions. Buying new High Capacity Data Radios or launching new communications satellites is costly. According to BGen Nordick, "as TCCCS and LFC2IS have demonstrated, new systems are so expensive that we must accept we will not be able to afford frequent wholesale replacement of entire C2

CAND%3E+Capability%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Cooperative+%3CAND%3E+Engagement+%3CAND%3E+Capability%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 67.

[76] *Ibid*., 7.

[77] *Ibid*., 7.

[78] John Williamson, "Bigger, better C4ISR systems underpin US warfighting efforts," *Janes International Defence Review* (August 2003) : [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2003/idr01622.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Bigger+%3CAND%3E++better%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Bigger+%3CAND%3E++better%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Bigger+%3CAND%3E++better%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 2.

fleets just to keep up with technology."[79] Thus, providing the backbone of an IC2S – bandwidth - requires a significant investment beyond the IC2S itself. A failure to invest in this backbone will result in an incomplete COP. For the CF to find the funding to ensure this within its highly constrained Strategic Capital Investment Plan will be one of the greatest risks to the success of the IC2S.

3.5 EXPERIMENTATION VERSUS ACTUAL EXPERIENCE

One of the strategies that have been employed by Canada's allies to mixed success has been the use of experimentation to develop and prove various network systems. In most cases, experimentation has been viewed as a means of reducing technical risk, schedule risks, and costs; however, as the experiences of Canada's closest allies will show, this is not necessarily always the case. Thus, this section will begin by looking at the cost and difficulties of maintaining an experimental force. Second, differences between the lab and the field will be examined. At the conclusion of this section, the reader will appreciate that while experimentation is useful, it is far from a panacea and it is very expensive. Despite these difficulties, it is worth doing as much as possible, and experimentation can definitely enhance the chances of success.

The United States and Britain have both, in the past, designated formation sized elements of their Army to support their digitization efforts. In the case of the United States, it was the 4th Infantry Division – an organization with more than 20,000 soldiers! Following the example of the U.S. Army, initial British plans had the 12th Mechanized Brigade being "ring fenced" as a trial organization for the Bowman System.[80] In the

---

[79] Brigadier-General G.W. Nordick, "Guest Editorial: Command and Control Aspects of Digitization," *The Army Doctrine and Training Bulletin* Volume 6, Number 1 (Spring 2003): 2.

[80] Pengelley, *Bird in the Hand…..,* 6.

event, because of operational demands, both armies had to abandon this process. Having this many soldiers and equipment unavailable for operational employment has proven too expensive even for these well funded militaries. Another example is the U.S. Navy. The designation of two Aegis Class cruisers for Cooperative Engagement Capability trials work, each valued at over $1 Billion and each with a crew of 360 sailors shows the type of human and financial investment required to support an active high technology trials environment outside the lab.[81]

Despite the costs and difficulties of the American and British trials, they have proven highly valuable in many respects. According to one British officer, "significant testing in the lab doesn't [sic] reflect accurately what happens in the field."[82] To illustrate, the British have been unable to establish a reliable working network with more than 120 Bowman High Capacity Data Radios, whereas a Brigade alone would typically require up to 240 such radios, and a Division up to 600.[83] Thus, the British have been able to learn important lessons related to digitized C2 that would have proven impossible if trials were restricted to the lab only. The evolutionary process for IC2S described in the C4ISR campaign plan should allow for at least some experimentation. However, if Canada is to achieve true success, then it will have to make the necessary investments in full scale experimentation to assure success.

---

[81] Author Unspecified, "The Ticonderoga Class (CG-47),"; available from http://navysite.de/cg/cg47class.htm; Internet; accessed 16 April 2007.

[82] Pegnelley, *Bird in the Hand…,* 18.

[83] Author Unspecified, *Bowman Pulls…,* 4.

3.6 SECURITY CHALLENGES

This next section of the paper will address the highly complex issue of security, which could easily be the subject of its own paper. According to Captain Xavier Rolin, of the French Army, "security will be the cornerstone of interoperability."[84] Thus, the intent for this section is to highlight only a few of the most important issues that could derail CF IC2S plans. These include some of the costs related to security, issues related to the Internet, and the 'need to share' concept. At the conclusion of this section, the reader will appreciate that security issues will be complex, and far from cheap.

Security of the IC2S will be expensive for several reasons. First, the desire for IC2S to interact with various OGDs and external actors will place significant security demands upon the system. Assuming they allow such access from a policy viewpoint, the data bases of CSIS and the RCMP for example, include sensitive information that has to be carefully protected from external scrutiny. To give an example, when the Netherlands equipped its new national crises center, up to 50% of the USD$ 14.5 Million cost was related directly to security, including encryption and shielding of equipment and rooms.[85] Thus, the entry fee for the IC2S to have the access to the sensitive information

---

[84] Xavier Rolin, "The RMA, C2 and Coalition Operations," *Australian Defence Force Journal*, number 144 (September/October 2000): 29.

[85] Joris Janssen Lok, "Netherlands equips national crisis centre," *Janes International Defence Review* (January 2007) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2007/idr10230.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Netherlands+%3CAND%3E+equips+%3CAND%3E+national%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Netherlands+%3CAND%3E+equips+%3CAND%3E+national%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Netherlands+%3CAND%3E+e

available from OGDs and external actors will be the security costs needed to protect this information.

Another security cost of the IC2S will be the fact that it is so widely distributed. Because up to 50,000 users will have access up to the Secret level, this could imply a greater demand on the security clearance procedures for far more personnel, most of whom currently use the unclassified DWAN. Moreover, the hard infrastructure required to support Secret level systems on the scale envisioned by IC2S simply does not exist at the current time, and will have to be built to support the system.

The next major issue related to security is that of the Internet. There are several issues of interest. First, the biggest source of information in the world today on any subject is the open sources of the Internet. Should CF personnel have access to this phenomenal source of information from their desk top? The answer, in theory, is clearly yes. Yet, "the use of the internet to connect C4I systems poses special vulnerabilities."[86] Nevertheless, the military and the IC2S project in particular, are in a bit of a dilemma. The quick and easy answer is to isolate the IC2S from the Internet. However, this solution will require the military to duplicate much of the functionality of the Internet as it has done with the DWAN Intranet – a poor copy of the Internet to be sure. Another solution is extensive firewalls to protect military systems from network attack. Whatever solution the IC2S project pursues, the Internet and its challenges will remain a dominating cloud hanging over IC2S efficiency and utility. Making the right choices on

---

quips+%3CAND%3E+national%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 1.

[86] US NRC Report, 140.

how to use the Internet while also protecting sensitive secret information will play a large part in the success or failure of IC2S.

The purists working in the world of integrated C2 Systems have coined a new term that articulates their vision of the future. Instead of thinking of information in terms of 'need to know' the new term is 'need to share.'[87] Indeed, the C4ISR Campaign Plan Interim Report states that many existing security policies are "stuck in the Iron Age…allowed to persist, [they] will severely constrain C4ISR transformation and convergence towards a network-enabled force."[88] Thus, it is a mantra within the modern world of C2 that information, particularly intelligence, needs to be more widely shared with users. Unfortunately, the C4ISR campaign plan makes little mention of some of the challenges this concept will experience. DND has both federal and departmentally mandated security and privacy obligations.[89] These obligations are mirrored in other departments, and will likely make the widespread sharing of information between departments in a 'need to share' climate very difficult to achieve.

A good example of the 'need to share' challenge is that between law enforcement and the intelligence communities. The latter will almost always seek to protect their sources and preserve the flow of information.[90] This is especially true as it relates to foreign intelligence, as the Mahar Arar case amply demonstrates. Law enforcement, on

---

[87] CF C4ISR Campaign Plan Interim Report, 5.

[88] *Ibid*., 21.

[89] CF C4ISR Campaign Plan Interim Report, 21.

[90] Erbetta, John, "Interoperability and Net-Centricity." *Military Technology* (May 2003) [Journal on-line]; available from http://proquest.umi.com/pqdweb?index=8&did=358330671&SrchMode=1&sid=1&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1176937041&clientId=1711; Internet; accessed 19 April 2007, 23.

the other hand, needs to deal with the reality that any information it receives may inevitably end up in a Court of Law, which is subject to disclosure rules. Thus, the goal of IC2S, which will seek this very same interdepartmental information, will be exceedingly difficult to achieve, particularly given the doctrinal shortcomings outlined in Chapter 2.

3.7 THE WORK OF ALLIES

This section will highlight some of the challenges and efforts of Canada's principle allies in the world of digital C2 systems. Because the scope of any examination could be huge if a tri-service approach was taken for each country, the examples given in this section are highly focused. Three allies will be examined, including the British, the United States, and the Australians. These three nations have been chosen due to their common cultural links to Canada, because they use many of the same technologies as Canada, and because their efforts in digital C2 are amongst the most advanced in the world. This discussion will highlight the fact that even these great nations are being considerably strained by their efforts at digitization. Nevertheless, there are lessons to be learned for Canada, and this section will bring out some of the most important.

3.7.1 The British

The British are involved in a wide variety of efforts that could be included in the general category of integrated command and control; however, this examination will focus on the Bowman System, which has Joint components. At $3.4 Billion (USD), the Bowman project's goal is to provide secure voice communications, messaging, local area sub-systems, user data terminals, automatic position locating and reporting capabilities,

battle management functions, system communication and cryptographic management.[91] Bowman includes the digitization of 22,000 vehicles, 133 naval vessels and about 70 aircraft.[92] On an individual platform basis, Bowman requirements can be extensive. For example, a Landing Platform Dock such as HMS *Bulkward* has 36 such radios between the ship and her embarked LCVPs and LCUs.[93] Thus, it would not be inaccurate to state that Bowman is the largest C2 program within the British military, and there are definitely some important lessons that can be learned by Canada from this project.

The British experience with the Bowman Project has elicited some colorful comparisons with early American Army digitization efforts, which were described as "giving birth to a bale of barb wire."[94] Despite their huge investment so far, the British remain far short of their goals, and today, are only "doing data to a degree."[95] Moreover, even now, the Bowman System only provides a "very limited capability"[96] for data exchange with other nations. For example, the Americans will depend upon their yet-to-be fielded Joint Tactical Radio System to talk to the British Bowman System, and only then, when using a VHF waveform.[97] Moreover, plans to integrate the Bowman System with the American Blue Force Tracker remain unfunded.[98]

---

[91] Pengelley, *Bird in the Hand…,* 2.

[92] *Ibid*., 2.

[93] *Ibid*., 12.

[94] *Ibid*., 1.

[95] *Ibid*., 11.

[96] Author Unspecified, *Bowman Pulls…,* 3.

[97] Pengelley,*Bird in the Hand…,*15.

[98] *Ibid*., 16.

A detailed examination of the project demonstrates some of the very high costs and technical challenges related to a project like Bowman. To illustrate, just to achieve connectivity with the Apache attack helicopter alone cost GBP 29 Million in addition to the costs outlined above.[99] Even with this investment, the capabilities of a Bowman equipped Apache will be extremely limited, and therefore, the vulnerability to an effective COP will be extensive. For example, with Bowman, the British Apache helicopter must be within 25 km line of sight from a vehicle equipped with the Apache Bowman Connectivity (ABC) node.[100] Not a very robust capability.

Finally, the British are the only other nation to have extensively used the American FBCB2[101] System (Blue Force Tracker), which they used during Operation Iraqi Freedom. They have written extensively about their experiences with the system, and have made some interesting observations. For example, they observed that the system provided a macro situational awareness over Blue Force units, particularly flanking units. As well, the system proved most useful at the Company level and above, and because it provided overall better situational awareness, it facilitated more rapid decision making.[102]

The British also reported that the FBCB2 system never achieved a credible Red Force picture during Operation Iraqi Freedom.[103] Thus, the British have learned some

---

[99] *Ibid*., 3.

[100] *Ibid*., 3.

[101] FBCB2= Force XXI, Battle Command, Brigade and Below

[102] Great Britain and the United States, Ministry of Defence and the Department of Defense, *A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom* (Washington: Office of Force Transformation, 2005), 5-2 to 5-4.

good lessons on the pitfalls of digital C2 Systems. Based on these experiences, the goals of IC2S are likely not going to be obtained for some considerable time. However, the British experience with FBCB2 does show that efforts to digitize C2 can be worthwhile and it can offer tangible benefits.

3.7.2 The United States

When it comes to digital and automated C2 Systems, the United States is by far the most advanced nation on earth. The four services of the United States military each possess a wide variety of systems to support all aspects of their command and control, although each of these systems is not necessarily interoperable with the others. This section will examine several major lessons learned by the United States, and how these lessons can influence the Canadian IC2S.

The United States' efforts in the domain of digital C2 systems have accelerated significantly in the period between the 1991 Gulf War and more recent operations. The most important lesson learned, particularly from a Canadian viewpoint, is the importance of bandwidth. For example, during Operation Iraqi Freedom the U.S. Military used 30 times more satellite bandwidth to support a force 45% smaller than that deployed during the first Gulf War.[104] As well, the bandwidth associated with the Secure Internet Protocol Router Network (SIPRNET) has been increased by 557% in the same period.[105] Thus, if Canada is to look to the United States for one important lesson for its IC2S, and the supporting systems, investments in bandwidth represent one of the greatest identifiable trends.

---

[103] *Ibid*., 6-8.

[104] Williamson, 2.

[105] *Ibid*., 2.

Another important American lesson is that the IC2S will have to have the flexibility to rapidly change to meet evolving situations and threats. Since September 11th, 2001, the United State's Global Command and Control System has been upgraded 22 times without going off line.[106] Since the IC2S will likely be linked or even use, GCCS technologies, it must be recognized that the IC2S will be a continually evolving capability. The TIM approach of the C4ISR Campaign Plan recognizes this reality, but commanders and funding suppliers like Treasury Board must understand that IC2S will never reach a Final Operating Capability where funding can be ceased.

The final important lesson from the United States is the fundamentally international nature of evolving C2 systems. An example of this is the Joint Automated Deep Operations Coordination System. Also used by the United Kingdom and Australia (soon), this system interfaces with a variety of existing digital systems including the US Global Command and Control System, Naval Fire Control System, and Advanced Field Artillery Data System.[107] The key lesson for the IC2S is that while none of these systems may provide a perfect answer to the CF requirement, interoperability between nations is often built upon functional systems, often operating at the service level. IC2S will have to be compatible with these systems, and conform to the language and standards requirements in order to function effectively with allies.

---

[106] *Ibid*., 1.

[107] Rupert Pengelley, "UK rethinks joint effects computing plan," *Janes International Defence Review* (October 2006) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2006/idr10059.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+UK+%3CAND%3E+rethinks+%3CAND%3E+joint+%3CAND%3E+effects%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+UK+%3CAND%3E+rethinks+%3CAND%3E+joint+%3CAND%3E+effects%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+UK+%3CAND%3E+rethinks+%3CAND%3E+joint+%3CAND%3E+effects%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 2.

Finally, despite American progress with C2 automation capabilities, their efforts have proven far from universally effective. An American committee examining C4I technology in the United States Armed Services articulated three principle challenges including interoperability, information systems security, and Department of Defense processes and culture.[108] Other shortcomings include Tactical Data Link deficiencies, coalition and system interoperability issues, and even problems of compatibility between services. [109] Based on the comments already offered in this paper, these areas of concern should be very familiar. Canada will face difficulties in these exact same areas despite the clarity of CF plans and vision. With limited resources, Canada will have to carefully track American progress in these areas and take advantage of the solutions when they become available.

3.7.3 The Australians

The Australian Defense Forces have many common cultural, military and political similarities to Canada. Thus, the situation in Australia, and any lessons they have learned could be very constructive in formulating Canadian plans. Therefore, this section of the paper will examine the Australian approach by looking at current capabilities, and the Australian approach to its future IC2S needs.

In terms of Strategic and Operational networks, Australian capabilities parallel those of Canada quite closely. The principle systems include the Defence Secure Net (DSN) and the Defence Restricted Net (DRN).[110] The former system is roughly

---

[108] US NRC Report, 3.

[109] Quinlan, Slide 21.

[110] All information contained within this section has been provided based on the advice of Consultation C, an Australian Defence Force Officer, during consultations with the author previously cited.

analogous to the Canadian DWAN system, while the latter system is similar to the Canadian TITAN system. Like the Canadian systems, these two networks largely use commercial off-the-shelf (COTS) equipment, and they are somewhat of a conglomeration of capabilities.

The DSN would typically be employed from the unit Commanding Officer level on upwards to the Strategic level. The Australians, like Canada, are also plugged into allied intelligence networks, and have recently gained at least limited access to the US SIPRNET. With these systems, a very limited COP is available to Australian commanders, though this would be presented in the same fashion currently used by Canada – i.e. text and power point slides etc.

Similar to the experiences of the Canadian, British, and American armies, the Australian Army has discovered that bandwidth, and data transmission at the tactical level are the most significant challenges to their conglomeration of existing tactical C2 systems. Thus, the reoccurring importance of bandwidth is the most important lessons the Australians have to teach Canada.

On the interagency level, the ADF emphasizes the use of Liaison Officers. There is no connectivity between the ADF and the Department of Foreign Affairs and Trade, for example, other than by e-mail. As well, there are no common data bases or other shared information on an inter-departmental level. Indeed, Australian plans do not envision any requirement for networking on an inter-departmental level. Arguably, the Australians may be taking a more pragmatic and realistic approach than Canada. As will be seen below, their objectives are relatively less ambitious.

The future plans of the ADF mirror, in some ways, many of the desires of Canada. According to Australian Chief of Army Lieutenant-General Peter Leahy, "the entire ADF will be networked throughout the battlespace with sensor-shooter links achieved in real time and the most appropriate fires will be brought to bear on the targets, irrespective of the service designated provider."[111] To achieve these goals, the Australians have created a project called the Battlespace Communications System (Land), which is a four phase project starting at the Brigade level in Phase 1, and going up to Joint capabilities in Phase 3. With a contract award only in December 2005 (to General Dynamics Canada – the contractor for the Canadian Iris and British Bowman Systems), the Australians are only now getting started on the same field as their allies.[112] No doubt, they will also experience many of the same frustrations and difficulties experienced by Canada and Britain.

Perhaps the greatest lesson Australia can teach Canada in formulating its plans for IC2S, are the dangers involved in some of the capabilities envisioned. The Australian Army has experienced some disturbing outcomes of the modern information age. For example, they have had instances of political leaders finding out about major events involving Australian forces (involving diplomatic personnel – ie 3D+C!) in Iraq, prior to senior ADF officers even knowing the full details of a given event. Another example, is that ADF officers report that their senior leaders have, on occasion, fallen into the trap of getting drawn down to the tactical level by, for example, watching live UAV video feeds.

---

[111] Lieutenant-General Peter Leahy, "Towards the Hardened and Networked Army," *Australian Army Journal* Volume II, number I (Winter 2004): 35.

[112] Pengelley, *Network Power*…, 4.

These experiences mirror similar Canadian experiences, and therefore, perhaps of all the lessons the ADF can teach the CF, the perils of modern technology are the most salient.

PART II

CHAPTER 4 – CONSULTATIONS ON REQUIREMENTS

4.1 BACKGROUND

Part 1 of this paper was about identifying why the success of IC2S was far from certain, despite clear vision, a comprehensive Campaign Plan and well articulated orders. In this second part of the paper, solutions and possibilities for overcoming at least some of these challenges will be offered. The intent of Chapter 4 has evolved since this paper was first conceived. Originally, results from the author's consultations with experienced members of the CF were aimed at narrowing down what the CF needed from its IC2S. However, the CF is clear on what it wants, and there exists a relatively good plan and clear vision for obtaining its goals. Nevertheless, the consultations undertaken in support of this paper have provided many useful suggestions on where the CF should focus its efforts to achieve success. Thus, this chapter will begin to offer some solutions by articulating the views of very experienced and knowledgeable CF personnel. [113]

4.2 RESULTS

The vast majority of those Officers and Non-Commissioned Officers providing advice in support of this paper agree that the CF should take immediate steps to acquire an IC2S. Most also agreed that the intended solution should take priority over service specific solutions. Because the consultations queried a wide variety of personnel, not just those involved in the world of C2, it may be concluded that support for an IC2S is quite

---

[113] The consultations described in this paper consisted of phone, e-mail and personal conversations by the author with serving CF and allied personnel with an interest or expertise in automated C2 Systems. Although the names of these personnel have been withheld to protect their anonymity, they represented a variety of MOCs from the ranks of CWO to LGen. The consultations were conducted in a quasi-survey format, though the sample size and question design means that the conclusions presented here have no statistical merit. Instead, responding to a series of standard questions, the results presented here are merely the opinions of some very experienced personnel, and should be viewed as such.

strong based on a small sample of experienced personnel. However, it is worth pointing out that many of the respondents placed qualifiers on this support. For example, one officer responded that "there is no evidence that communications from strategic down to the tactical level makes operations more effective. In fact I can easily make the argument that it would hinder the effectiveness of operations."[114] Moreover, several of those consulted expressed the fear that the objectives of IC2S may be too ambitious and that "the goal of connecting strategic to tactical would make the Joint C2 System cost prohibitive, with little to no benefit to operations."[115] Thus, there is recognition within the CF that there are shortcomings that need to be addressed, and that IC2S is a good idea generally. However, the comments above indicate some skepticism as to how far the system should go, and the fear of excessive costs is apparent.

When it came to the importance of working with allies, the author's consultations found that almost all those queried agreed or strongly agreed that it was important for the IC2S to be interoperable with key allies. From a domestic point of view, one officer highlighted the fact that the IC2S should be able to link into systems at NORAD, US NORTHCOM, and US Homeland Security elements.[116] Moreover, most of those consulted largely agreed that interoperability with key allies such as the United States, Britain and Australia should be the priority, which matches the plans of the C4ISR Campaign Plan. Thus, the vision of the CDS for interoperability with key allies is validated by the consultations conducted in support of this paper.

---

[114] Name Withheld, Consultation E, Air Force Signals Major, consultations with author February 2007.

[115] *Ibid*.

[116] Name Withheld, Consultation F, Air Force Lieutenant-Colonel Pilot, consultations with author February 2007.

Comments received by the author on the interoperability requirements of IC2S with OGDs were far more varied, but generally at the same level as support for interoperability with key allies. One officer highlighted the fact that the Government of Canada is in the process of developing a Secret Network for all government departments, however, "the reality is that this network will be very basic, and not robust…and [therefore] DND should not invest significant time and effort on the GoC secure network."[117] In contrast, one senior officer emphasized that "some effort should be given to CF C2 interoperability with Public Security and Emergency Preparedness Canada (PSEPC) and other key government departments since this area is much less advanced than interconnectivity with our allies."[118] Most of those consulted agreed that the OGDs that should link into IC2S include the RCMP, CSIS, Foreign Affairs Canada, the Coast Guard, and Border Security Agency as a minimum.[119] However, a significant number of those consulted indicated that the problems of integrating with other government departments may be best solved by the use of Liaison Officers, equipped with IC2S capabilities, rather than full electronic integration.[120] As described previously, this approach would match the current Australian view. Therefore, based on these comments and the approach of the Australians, the CF may want to pursue the OGD integration issue using suitably equipped liaison officers.

---

[117] Consultation E.

[118] Name Withheld, Consultation G, Army Brigadier-General, consultations with author February 2007.

[119] Consultation G.

[120] Name Withheld, Consultation H, Army Major, consultations with author February 2007.

In terms of the relative priority of an IC2S, the consultations produced interesting results. In response to the question of whether IC2S capabilities were so important they should be procured ahead of other defence priorities such as ships, aircraft and land systems, few officers and NCMs were on the extremes. Some agreed, some disagreed, and some had no strong opinions.

Despite this relative distribution in responses, there were some strong views on the subject of funding and relative priorities. For example, one senior officer pointed out that while the Canadian Forces has spent over $350 Million on the corporate enterprise resource planning system projects in one fiscal year, only $90 Million was allocated the Canadian Forces Command System.[121] A fellow senior officer stated that "new C2 models deserve parallel procurement, but not exclusive priority. Nothing in the current technology suggests disaster is imminent, thus connectivity over capability cannot be argued. C2 of nothing is therefore avoided."[122] An expert with the Director of Force Planning and Program Control, with long time experience in capital projects, stated that the CF should be spending about 15-20% of the available capital budget in the general area of C4ISR,[123] and an officer with extensive experience in a similar field stated that "there should be a cap on the maximum amount of funds expended on Joint C2 in proportion to other CF acquisitions"[124] Overall, several of those consulted emphasized that "there is no point in exerting effective command if there are no forces to

---

[121] Consultation G.

[122] Name Withheld, Consultation I, Navy Rear Admiral, consultations with author February 2007.

[123] Name Withheld, Consultation J, Civilian Procurement Expert and Retired Military Officer, consultations with author February 2007.

[124] Consultation E.

command."[125] Thus, based on these comments, at least some CF members clearly think that the CF should invest in IC2S like capabilities. However, it also clear that this investment cannot come at the expense of tactical level capabilities that accomplish the missions. The general recommendation that C2 funding should be about 15-20% of DND capital funding should serve as a guideline to keep expenditures under control.

Of those with experience as commanders on operations, most disagreed with the statement that they always had the necessary C2 systems to support their mission. This reinforces the view that improvements are necessary. One officer indicated that "a key weakness of existing systems is insufficient bandwidth to move graphic-intensive files along the Level II and Level III networks."[126] This view reinforces the experiences of the three allied armed forces covered in this paper. The Army Officers consulted see the primary challenges as being at the tactical level, perhaps most importantly with respect to fire support, data bases and intelligence.[127] Access to timely and relevant intelligence also comes to the fore frequently in the experiences of allied nations. Several of those consulted emphasized the importance of automated search tools that allow for the retrieval, evaluation and exploitation of all forms of information, including and especially, intelligence data.[128] Finally, the importance of an all-informed net, and the

---

[125] Name Withheld, Consultation K, Air Force Lieutenant-Colonel Strategic Planner, consultations with author February 2007.

[126] Consultation A.

[127] Name Withheld, Consultation L, Army Colonel, consultations with author February 2007.

[128] Consultation A.

ability to communicate on a synchronous and asynchronous basis was repeatedly emphasized during the author's consultations.[129]

The fear of an IC2S undermining CF Command Doctrine was consistently emphasized by many of those consulted. One CF General emphasized this danger by stating that "widespread networks promote skip echelon C2 whereby direction given from the strategic level to an individual on the ground, and this needs to be understood and direction given accordingly."[130] One Admiral stated that he "prefers the establishment of the authorities and rule sets to conduct operations, most of which are local or regional, as opposed to establishing a system to feed SA to the Centre or establish commonality across the organization."[131] Another officer with recent combat experience in Afghanistan emphasized that a major key deficiency in the current CF is the "inability to organize an integrated intelligence architecture that 'pushes' intelligence to the field commander."[132] Nor should any future C2 System erode "the empowering of the tactical commander, and trusting them to sort out tactical problems."[133] Indeed, the same officer emphasized that the tactical commander "needs to be able to draw upon higher intelligence, but does not require anything more from higher. He should already

---

[129] Consultation H.

[130] Consultation G.

[131] Consultation I.

[132] Name Withheld, Consultation M, Army Lieutenant-Colonel, consultations with author February 2007.

[133] *Ibid*.

be granted the resources he needs, and the authorization to use them without having to reach back for permission."[134] He went on to state that

> I am opposed to spending large amounts of money on strategic level C2 systems that do not provide any advantage to the small unit commander, but that to the contrary will probably impede him by giving the senior leadership in Ottawa visibility over the small unit action and hence the power to intervene. All efforts should be directed at pushing info and resources to the lower commander, not on providing the strategic HQ with more information about small tactical issues.[135]

Thus, for the architects of IC2S, one of the greatest risks of the system should be viewed as the undermining of CF Command Doctrine due to technical capabilities. Careful analysis should be undertaken about what information can and should be provided to each echelon if IC2S is to contribute, rather than detract from, CF C2 capabilities.

General comments also highlighted many small issues that would make the IC2S more effective if addressed. For example, any future capabilities must, to the maximum extent possible, use intuitive tools like those used by commercial systems such as Google Earth, Microsoft Products, common search engines, and Web-based systems currently found on the Internet. Many of those consulted emphasized that IC2S cannot make huge demands on the users to 'populate' the system.[136] Nor, can the training bill be too high if IC2S is to be successful.

Another aspect that became clear was the highly pragmatic wishes for the future capabilities of IC2S. For example, the major conclusion from these consultations was

---

[134] *Ibid*.

[135] *Ibid*.

[136] Name Withheld, Consultation N, Army Lieutenant-Colonel, consultations with author February 2007.

that simple communication between the levels and services is the key deliverable for IC2S. A senior officer stated that

> the ability to communicate amongst ourselves would go a long way to enabling a commander to do his job. I believe too much fuss is being made, at this point, over 'decision making' and 'decision making aids.' Communications will facilitate provision of information which will facilitate decision making.[137]

Thus, the consultations conducted in support of this paper highlighted many of the issues facing IC2S. While not of a scientific or statistically reliable nature, this feedback should serve as a focus point for IC2S project staff. Not all of the envisioned capabilities for IC2S are essential in the short term. The comments above may provide some guidance on what is important, and where the focus should lie. Efforts should be focused on improving simple communications within the CF, and in doing so, avoiding undermining proven principles of command.

---

[137] Name Withheld, Consultation N, Navy Captain, consultations with author February 2007.

CHAPTER 5 – THE POSSIBILITIES

5.1 GENERAL

This chapter is about the types of technologies that Canada could pursue that may support the CF vision for an IC2S. The technologies represented in this Chapter represent a path that may lead to an effective COP that goes from the tactical to the strategic level. The examples presented here are merely that – best practices. Every day, governments and industry come up with new solutions to problems that are currently stymieing CF goals. The challenge for the CF is to stay in step with its allies and industry trends in choosing which technologies to adopt, and to do so in a timely enough manner that the CF does not end up adopting yesterday's standard for technical integration. Thus, to accomplish this aim, this Chapter will include the NATO Secure Communications Interoperability Protocol (SCIP), the American experience with F-16 Block 30/Stryker combat vehicle integration, the U.S. Air Force's Battlefield Air Communications Node (BACN), and the Canadian Forces experience with the Air Defence Systems Integrator. At the conclusion of this chapter, the reader will appreciate that there is extensive work occurring with Canada's allies that can significantly contribute to the success of Canadian plans - if the right decisions can be made in a timely manner.

5.2 THE NATO SCIP EXAMPLE

The first example that will be presented demonstrates the benefits that can accrue from working closely with allies on issues of common languages and protocols. The NATO Secure Communications Interoperability Protocol (SCIP) is "a standardized

framework to allow end-to-end encryption over heterogeneous networks."[138] It is an example of the type of international work that goes on daily, from which Canada can benefit greatly. The system features a terminal configuration that provides the capability for both point to point and multi-party links, regardless of traffic type, including voice, video and data over a variety of means including Public Switched Telephone Networks, Integrated Service Digital Networks, the Public Land Mobile Network, HF Radio, Internet Protocol, and VHF tactical radio.[139] With this protocol, digital terminals manufactured in any country to the same standard will use the common Advanced Encryption Standard developed in Belgium, and all will be compatible.[140]

By linking into, or adopting the SCIP standard, or possibly other standards of a similar type, Canada can ensure that it will be able to interact closely with its principle allies. As previously described, often the United States will lead this effort. However, the Belgian encryption standard is a good example where the United States may not always offer the preferred solution. Thus, whatever system is chosen, using a common international standard such is SCIP is the only practical path forward to ensuring Canadian interoperability with allied nations.

---

[138] Rupert Pengelley, "NATO seeks a standard bearer for encryption in coalition operations," *Janes International Defence* Review (August 2006) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2006/idr04910.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+NATO+%3CAND%3E+seeks+%3CAND%3E+a+%3CAND%3E+standard+%3CAND%3E+bearer%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+NATO+%3CAND%3E+seeks+%3CAND%3E+a+%3CAND%3E+standard+%3CAND%3E+bearer%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+NATO+%3CAND%3E+seeks+%3CAND%3E+a+%3CAND%3E+standard+%3CAND%3E+bearer%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 2.

[139] *Ibid*., 3.

[140] *Ibid*., 4.

5.3 THE STRYKER/F-16C BLOCK 30 EXAMPLE

A key requirement for the COP is to provide timely and relevant information on the status of tactical and operational level forces to strategic leaders. However, equally important will be the capability to fuse information on a Joint level so that the various forces can communicate and work together. An interesting example of one of the technologies that may support this requirement is the integration capabilities of the U.S. Air National Guard operated F-16C Block 30, and the U.S. Army's Stryker Combat Vehicle. These two weapon systems demonstrate some of the significant potential of a common operating picture on the Joint level if the appropriate technologies can be merged. Using the Situational Awareness Data Link (SADL) of the F-16, in combination with the Enhanced Position Location Reporting System (EPLRS) radios in the Strykers, it is possible to exchange digital traffic, including most importantly, the location of every Stryker vehicle to supporting F-16s.[141] Moreover, the F-16/Stryker combination can cue each other to potential targets, and video from the targeting pods of the F-16s can be transmitted to the Stryker's.[142] Thus, the type of electronic interoperability envisioned by C2 purists is technically feasible if the tactical forces are appropriately equipped. If the

---

[141] Michael Sirak and Joshua Kucera, "US Air Force studies use of F-16 with army Strykers," *Janes Defence Weekly* (December 2004) [Journal on-line]; available from http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw2004/jdw09733.htm@current&Prod_Name=JDW&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+US+%3CAND%3E+Air+%3CAND%3E+Force+%3CAND%3E+studies%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+US+%3CAND%3E+Air+%3CAND%3E+Force+%3CAND%3E+studies%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+US+%3CAND%3E+Air+%3CAND%3E+Force+%3CAND%3E+studies%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 1.

[142] *Ibid*., 2.

CF can make the right decisions, this type of networking capability will have the potential to provide the raw data needed by the envisioned COP.

Unfortunately, it must be highlighted that the capabilities represented by the F-16/Stryker integration are not widely available throughout the U.S. Military. The F-16C Block 30 is the only variant of the F-16 family to use a tactical data link that is compatible with the EPLRS of the Stryker. The F-15E Strike Eagle, for example, uses the Link 16 system, and thus cannot integrate with the Stryker. This demonstrates the challenges of version control, and settling on a standard technical solution. Achieving this in the U.S. Military, with its aircraft operated by four military services, has resulted in a disparate collection of different types of data links – each with different advantages and capabilities. Thus, the CF will have to make its choices carefully, and will often be forced to choose between competing technologies.

5.4 BACN AND THE F-22 RAPTOR

One of the great possibilities for integrating the wide number of different tactical data links upon which the COP will depend are technologies that can be roughly described as electronic translators. In about the year 2010, a soldier operating on the ground will be able to send a text message using cell phone technology to the F-22A Raptor fighter bomber.[143] Unlike most of the more modern aircraft supporting Joint

---

[143] Stephen Trimble, "Network-Centric Warfare Part 1: Communication Gateways – Gateway to the Future," *Janes Defence Weekly* (January 2007) [Journal on-line]; available from http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw2007/jdw31553.htm@current&Prod_Name=JDW&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Network-centric+%3CAND%3E+Warfare+%3CAND%3E+Part+%3CAND%3E+1%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Network-centric+%3CAND%3E+Warfare+%3CAND%3E+Part+%3CAND%3E+1%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Network-

Forces, the F-22A is not currently equipped with the Link 11 or 16 Data Links. Instead, it is equipped with the low-probability-of-intercept Intra Flight Data Link, which allows the F-22A to only link with other F-22As.[144] To overcome these shortcomings, the U.S. Air Force plans to use the Battlefield Airborne Communications Node (BACN), built by Northrop Grumman. This system functions by "bridging the wide mix of incompatible radio signals in use today with an IP-based network overlaid."[145] The result is that different data links can communicate with each other using BACN.

Essentially, the BACN system receives messages from a wide variety of systems using different wave forms, translates the message into the needed format, and retransmits the information in the needed format to the intended receiver. Thus, aircraft like the F-16C Block 30 with a Situational Awareness Data Link, can communicate with the F-15, which is equipped with Link 16, using the BACN system.[146] Moreover, the BACN will allow communications between the A-10 Thunderbolt, with its Have-Quick radios and the SINGARS equipped AH-64D Apache.[147] The future of BACN is called the Common Link Integration Processing (CLIP). This will be a more robust version of BACN, and will bridge voice and data messages between Link-16, Link 11, Link 22, EPLRS and Joint Range Extension.[148] Clearly then, the type of technology that BACN and CLIP represents offers great possibilities for the CF to succeed in its plans for IC2S.

---

centric+%3CAND%3E+Warfare+%3CAND%3E+Part+%3CAND%3E+1%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 1.

[144] *Ibid*., 1.

[145] *Ibid*.,2.

[146] *Ibid*.,2.

[147] *Ibid*.,3.

[148] *Ibid*.,7.

Therefore, the CF should very closely track the development of translator type technologies, and where it makes sense to do so, move quickly to adopt these highly flexible tools. Dollar for dollar, investments in these types of technologies may well be the best money spent.

5.5 HMCS ALGONQUIN AND THE AIR DEFENCE SYSTEMS INTEGRATOR

It is a current reality that the CF is failing to exploit some of the tools it already has. Indeed, significant capabilities already reside within the CF; however, it will take a commitment of resources and command interest to maximize these capabilities. Should this be accomplished, the CF will be well on its way to achieving a COP, particularly with Maritime and Air elements, and particularly within the context of domestic operations.

In 2005 and 2006, the Canadian Navy conducted Exercise TRIDENT FURY in support of Anti-Air Warfare Controller Training.[149] Because of the limitations of the existing Combat Systems of the 280 Class ships, the Air Defence Systems Integrator (ADSI), built by Ultra Electronics of the United States, was procured. The purpose of procuring the ADSI System was to give the 280 class ships the ability to use the full capabilities of the Link 16 System, without requiring major and expensive modifications to the combat systems of the ships. The exercise included Canadian and American warships, U.S. Air Force and Navy aircraft, NORAD Regional and National Control Centers, the Canadian Army Air Defence Anti-Tank System, and Canadian CF-18s.

---

[149] The capabilities described in this section were described to the author during consultations previously cited by Consultation D, an experienced MARS Lieutenant-Commander with expertise with the Link and ADSI systems.

The ADSI makes use of the ships existing UHF links and Satellite Communications capabilities. The vision for the ADSI system for the exercise was to integrate and fuse all data inputs from up to 16 different data link inputs. In essence then, the ADSI gave full Link 16 capability to Link 11 equipped ships, and included data as well as voice capabilities.

With the ADSI system, HMCS Algonquin achieved a Common Operating Picture over multiple Areas of Operation, including activities conducted well beyond the 512 mile range of its own sensors and Link networks. This included the monitoring of CF-18 fighters conducting Close Air Support (CAS) missions in support of the Army over central British Columbia, while the Algonquin herself was hundreds of miles off the coast of Vancouver Island. A Chief Petty Officer described the capabilities being exercised as follows:

> NORAD North Bay picks up an Air Defence Identification Zone (ADIZ) violator during the 2010 Olympics. The contact is sent to HMCS Algonquin by Satellite Link 16 and backed up by chat. Algonquin picks up the target and classifies it off the West Coast of Vancouver Island and sends it back to 21 Radar Squadron on Vancouver Island. 42 Radar Squadron in Cold Lake receives the picture by Joint Range Extension Protocol B from North Bay (JREAP B – Link 16 via STU III) and briefs CF-18s on the ramp via UHF Link 16. From the cockpit, pilots can see the contact and are scrambled. With relay on Link 16 the CF 18s relay the contact to an ADATS on the lower mainland of BC. Joint tactical C2 is achieved. This Link 16 picture is processed by HMCS Algonquin via GCCS-M and forwarded to Joint Task Force Pacific and CANCOM – strategic C2 is achieved.[150]

The scenario described above is technically achievable today, and was the type of activity proven during Exercise TRIDENT FURY using the ADSI system. Clearly, this type of capability is what is envisioned for the COP of IC2S. Unfortunately, the reality since these exercises is not so bright. Canadian Navy efforts to entrench the capabilities

---

[150] Name Withheld, Consultation P, Navy Chief Warrant Officer – Expert on Link Systems, consultations with author February 2007.

described above have slowed due to a reluctance to expend funds on the old combat systems of ships like the Algonquin. Moreover, key oversight functions such as the Tactical Data Link Authority and the establishment, perhaps, of unique new supporting personnel, such as the American style Joint Interface Control Officer (JICO), who are needed to manage Link networks, has yet to occur. Without these essential changes, the CF is unlikely to be able to leverage even the technologies it currently owns to build the COP.

In conclusion, the types of technologies that have been described above are the types of investments that may offer a high payoff for the Canadian Forces. It is acknowledge that these and other 'solutions' may occasionally offer false promises of solving the many complex issues of C2. Nevertheless, occasionally new technologies emerge that can have a dramatic impact upon the effectiveness of CF operations. Thus, Canada needs the ability to react quickly when these technologies emerge before they themselves get surpassed by the next wave of inventions.

CHAPTER 6 – RECOMMENDATIONS FOR THE CF

In Chapter 5, it was highlighted that there are technologies that can support the CF desire for an IC2S, providing the right choices are made in a timely manner. The aim of this chapter is to consolidate some of the most important information presented in this paper, and to provide recommendations for the CF if it wants to succeed with IC2S. These recommendations are intended to address the macro issues. The detailed technical aspects of delivering a fully functional IC2S should be left to the experts. Thus, this chapter will comment on project management and processes, the functional approach, some general recommendations, some thoughts on funding, and the concept of evolution versus revolution. At the conclusion of this chapter, the layman will have a basic understanding of where the CF will have to go beyond its vision and its detailed plans if it is to succeed in delivering an effective IC2S.

6.1 PROJECT MANAGEMENT AND PROCESSES

The difficulties and challenges of government procurement practices in both Canada and with principle allies have been previously described. The aim of this section is to provide recommendations on how the project management process should evolve if IC2S is to be successfully fielded.

First, the CF and Government of Canada must evolve the procurement process to recognize the unique challenges represented by technologies such as IC2S. The reality, is that "in implementation, development/procurement cannot follow the traditional processes used in the past, as delivery will always be too little too late."[151] With an average project lifetime of seven years, the existing CF procurement process is doomed

---

[151] Name Withheld, Consultation Q, Civilian Expert on C2 Systems, consultations with author February 2007.

to provide obsolete technology too late for effective integration with rapidly evolving C2 technologies. This will require the CF to streamline its own internal processes, which are generally laborious, and risk adverse. It will also require the department to reach agreement with supporting Government of Canada Departments so that external processes are also streamlined.

The second recommendation on project management and processes is that the CF should adopt a culture of 'learning by doing.' As described by the ADF 'learn by doing' is an approach "that accepts that mistakes will be made in the development of networked forces."[152] The genesis of this approach is the American experience in developing atomic weapons, and is captured by the comments of US Brigadier General Leslie Groves, who stated at the time "nothing would be more fatal to [American atomic] success than to try to arrive at a perfect plan before taking any important step."[153] This approach has also being endorsed by Defence Research and Development Canada (DRDC) Scientist Sandy Babcock.[154] The issue with this approach is that a much greater tolerance of risk will have to be assumed than is currently the practice. A 'learn by doing' approach implies that DND efforts to field IC2S will not necessarily be efficient, and cost effective in all instances.[155] Some decisions will not bear fruit, and will be viewed as mistakes in retrospect. However, without this 'learn by doing' approach, the CF will not institutionally learn the lessons needed to successfully field an IC2S, and therefore, long term failure is more likely.

---

[152] Ryan, 103.

[153] Brigadier-General Leslie Groves in Ryan, 107

[154] Babcock, 44.

[155] Erbetta, 24.

6.2 THE FUNCTIONAL APPROACH

An approach that has proven quite successful in solving the many technical difficulties associated with the capabilities of an IC2S is a functional approach. This approach solves the challenges by identifying "communities of shared interest that need to be interoperable."[156] Common examples of these functional areas include Air Defence, Surface to Surface Fires/Deep Strike, Transportation and Logistics, Close Air Support, and Theatre Missile Defence.[157] A particularly effective way to drive these functional improvements from a Joint perspective is the use of major Joint exercises such as TRIDENT FURY – or by widely deploying rapidly procured capabilities proven on operations. Another approach is that of the U.S. Navy, where refits for USN ships are "now starting to be done on a battle group basis rather than on the more traditional class of ship basis."[158] Using the solutions that evolve from these functional requirements, the networking problems of the IC2S can be rectified over time.

6.3 GENERAL RECOMMENDATIONS

Within this section, some general recommendations that should be considered with respect to the IC2S are offered. They are in no particular order of importance, yet each has the potential to have a major impact on the success or failure of the future IC2S. Thus, to begin, the CF should select relatively stable technologies that are "achieving widespread adoption and are likely to enjoy longer term support."[159] As well, the CF

---

[156] Quinlan, Slide 10.

[157] US NRC Report, 70.

[158] J. LeRoy Pearce, *Presentation - The Revolution in Military Affairs* (Ottawa: DND Canada, 30 November 1998), 4.

[159] US NRC Report, 76.

should use well articulated commercial standards for the IC2S such as TCP/IP.[160] These two approaches will do much to reduce technical risk, and will therefore enhance the chances of success.

Teams designated to develop architecture for an IC2S must be kept as small as possible. Larger teams lead to compromises, which inevitably lead to "excessive complexity rather than a clear design philosophy."[161] To assist in this goal, the scope of the IC2S project should be narrowed and limited to the maximum extent possible for several reasons, including overall complexity and to keep the scale of the project commensurate with the pace of change in both missions and technologies.[162]

The CF should create a more robust capability to sponsor and manage Joint Projects such as IC2S. In other words, a structure that mirrors the staff horsepower of the Director(s) Air/Land/Maritime Requirements is required. This will assist the CF in being interoperable with itself, followed by, in priority, with the United States, ABCA, and then NATO.[163] Links to OGDs should be primarily through suitably equipped Liaison Officers, with the integration of data bases, where possible, with key enablers, particularly intelligence.

Most importantly, the CF must effectively use what it already has, like the CF-18 MIDS Link 16, the ADSI and Link 11 Systems. To do so, the CF must recognize that "interoperability, in a Joint sense will not reliably occur until the CF Data Link Authority

---

[160] US NRC Report, 90

[161] *Ibid*., 7.

[162] *Ibid*., 93.

[163] Nordick, 2.

can provide network direction, oversight, development and management."[164] Such an authority would provide "joint, tri-service, Data Link standards and directives."[165] Moreover, the supporting authority, structures and specially trained personnel must be put in place if these capabilities are to be exploited.

In terms of experimentation, the CF should pursue the dual tracks of lab experimentation and experimental units if success is to be fully achieved with IC2S, particularly those aspects related to the COP – and particularly land force units. To assist in this, for land forces, systems of systems complexity should be reduced to near zero below Brigade level.[166]

Finally, IC2S must recognize the fundamental tenants of CF leadership doctrine in the three services. The Army's 'Mission Command' philosophy "which is designed to achieve unity of effort at all levels and is dependent upon decentralization and empowerment,"[167] and its equivalents in the Navy and Air Force, cannot be ignored – even given technological capabilities. Thus, the CF should be "satisfied with less than perfect understanding of the situation and accept that you do not need to know everything, particularly as you go higher up the chain of command."[168] Pursuit of the

---

[164] Department of National Defence, *1 Canadian Air Division Multi-Purpose Information Distribution System Concept of Operations* (Ottawa: 1 Canadian Air Division A3 Fighter Systems, 3 July 2006), 1.

[165] *Ibid*., 1.

[166] Toomey, 6.

[167] Army CDR, 9.

[168] Giles Ebbutt, "Knowledge is power: armies refine their filtering of battlespace data," *Janes International Defence Review* (January 2007) [Journal on-line]; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2007/idr10240.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+knowledge+%3CAND%3E+is+%3CAND%3E+power%29+%3CIN%3E+body%29%2C+%2

'near perfect' COP is a chimera that is not necessary, almost certainly too expensive, and undermines the central themes of Canadian leadership practices.

6.4 SOME THOUGHTS ON FUNDING

If the Canadian Forces were to implement current plans for improved Command and Control capabilities without any change or rationalization, by 2112, the Government of Canada would have to commit approximately $8 Billion (Cdn) to fulfill these demands.[169] Given the financial realities facing the CF, clearly it would be imprudent to spend this kind of money when major capabilities such as land, sea and air systems face significant challenges over the same timeframe. In a recent CF review of its Information Technology (IT) related projects, it was recommended that numerous planned or existing projects be delayed or even cancelled. Should these recommendations be accepted, the CF could reduce the financial demands by up to $321 Million over the next five years.[170] Thus, a degree of rationalization could assist the CF in freeing up the necessary funding to support its IC2S initiatives. The question is, how much funding should the CF commit to its C2 capabilities?

In recommending an implementation strategy, the C4ISR Campaign Plan Interim Report uses terminology such as efficient, effective, economical, and fiscally responsible.[171] As this paper has attempted to illustrate, the nature of the technology itself, and the fact that Canada is so highly dependent upon external factors, makes the

---

8%5B100%5D+%28%5B100%5D%28+knowledge+%3CAND%3E+is+%3CAND%3E+power%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+knowledge+%3CAND%3E+is+%3CAND%3E+power%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007, 3.

[169] C4ISR Campaign Plan Interim Report, 6.

[170] Department of National Defence, *IM/IT Rationalization Tiger Team Projects Working Group: Final Report* (Ottawa: DND Canada, September 2006), 3.

[171] CF C4ISR Campaign Plan Interim Report, 22.

likelihood of the IC2S being efficient, (fully) effective, or economical and fiscally responsible very remote. Thus, the answer to the question of how much the CF should be spending is not totally clear. However, some basic guidelines could be useful.

Spending on C2 capabilities should be proportional, and in parallel with other priorities. Moreover, it is also recommended that a cap be established on funding so that costs do not get out of control. One suggestion was that this cap be about 15-20% of the overall capital program on a yearly basis. What is more important, however, is the concept that funding will have to be constant, on a year to year basis, and it will need to be accessible so that the CF can quickly take advantage of the opportunities that always arise in this high technology area. Indeed, American studies recommend that budgetary flexibility is required "to exploit unanticipated advances in C4I technology that have high payoff potential."[172] Thus, an actual dollar recommendation will not be made here in this paper. Instead, a new construct and way of thinking is what is needed.

6.5 EVOLUTION VERSUS REVOLUTION

The final recommendation of this paper, and one which has been alluded to throughout, is that the only path to successfully introducing the IC2S is an evolutionary one, rather than revolutionary. The CDS goal of successfully merging existing Secret level systems will almost certainly not be achieved in the very short time frame of only two years. Some key capabilities envisioned for IC2S, such as the COP, will take a long time to meet the vision of the CDS. There remain very difficult problems that today have proven insurmountable from a technological viewpoint. Thus, the CF will have to continue to evolve its capabilities to achieve its vision of a COP. There are no magic

---

[172] US NRC Report, 24.

answers to solving these problems, and even with unlimited funding, some issues will not be solved in the short term.

The C4ISR Campaign Plan has recognized this fundamental evolutionary nature of the technology in its Target Integration Model. What senior CF leaders must realize; however, is that a fundamental tenant of evolutionary acquisition "is acceptance of the 80% solution. Insistence on a 100% solution can radically increase costs and extensively delay system deployment…[and thus] it should be stipulated that an 80% solution is the goal of virtually all C4I acquisitions."[173] Given this, the vision of the IC2S is almost certainly overly ambitious. The Australian plan may be the more pragmatic, and thus achievable. In any case, while having a vision is a good thing, CF leaders should lead the institution in making pragmatic choices that select improved capabilities that remain imperfect.

[173] US NRC Report, 197.

CHAPTER 7 - CONCLUSIONS

This paper had two pragmatic goals. In Part I, the aim was to highlight the fact that despite a clear vision, a solid campaign plan, and well articulated orders from the highest levels, the current CF plans for the introduction of an IC2S capability remain inadequate. Chapter 1 outlined the current capabilities possessed by the CF. In this Chapter it was noted that the majority of CF personnel rely on the unclassified DWAN system, while far fewer service personnel have access to a wide variety of Secret level systems, almost all of which cannot communicate with the other systems in service. The vision of the CF for an IC2S, as expressed in the C4ISR Campaign Plan, and the current ongoing work related to IC2S was also covered in this first Chapter. Of note, the CF has invested considerable intellectual thought into what it wants from its IC2S and how to achieve these goals. The main product of this planning is the Target Integration Model, which recognizes a need for an evolutionary approach to the IC2S. Overall, it must be highlighted that the IC2S vision is comprehensive and ambitious. Finally, Chapter 1 also includes a review of the COE, with a focus on the requirement for the CF to interact with OGDs, NGO's and allies. Thus, the intent of Chapter 1 was to set the scene for the current situation as it relates to constructing the future IC2S.

In Chapter 2, the challenges facing IC2S as it relates to doctrine was covered. Because of the importance of external actors to the success of future CF missions, and IC2S, the lack of any doctrinal framework linking the CF, DND and OGDs was highlighted. Moreover, the great weakness that currently exists with current CF Joint Doctrine was also emphasized. Finally, the negative effect that this weak Joint doctrinal basis had on service specific doctrine and procedures was noted. The overall conclusion

of Chapter 2 is that IC2S is being conceived and built with a very weak doctrinal foundation, and that the CF should focus its efforts on resolving these weaknesses at both the inter-departmental and Joint levels.

In Chapter 3, the major weaknesses in current CF Plans for the introduction of an IC2S are introduced. These challenges begin with shortcomings in the general category of People and Processes. While the weaknesses of the current CF project approval process was highlighted, the major conclusion from this section is that the CF is not dedicating either enough, or sufficiently expert personnel to the problem of fielding an IC2S. This represents one of the greatest risks to future CF plans, and is the first area which must be addressed if IC2S plans are to succeed. Another challenge highlighted in Chapter 3 includes the issue of language. Ultimately, the idea "of total technical interoperability is a vision."[174] Achieving interoperability will always be a goal, rather than an accomplishment. Thus, this discussion builds upon the doctrinal discussions of Chapter 2, and highlights the challenges of different electronic languages working together.

Perhaps the major section of Chapter 3 is the one describing the technical difficulties of building the COP from the bottom up. This section highlights that many of the technologies upon which the CF vision for a COP depends remain imperfect and prone to a multitude of different errors. Thus, the CF will have to accept the fact that the COP will likely never be 'near perfect' although current capabilities can certainly be improved. Chapter 3 continues with discussions on the difficulties of networking different systems, the advantages and limitations of experimentation, and the security

---

[174] Erbetta, 24.

challenges DND will face in introducing IC2S. It then concludes with an examination of some of the challenges being experienced by Canada's principle allies, including the British, the United States, and Australia. From this discussion, it is more than evident that the challenges the CF will face in introducing an IC2S will be extensive and very expensive to overcome.

Chapter 4 represents the beginning of Part II of this paper, and was aimed at demonstrating that the goals for an IC2S can be achieved if the CF makes the right choices at the right times. The results of the author's consultation with a broad audience of CF Officers and Senior NCMs make it is clear that serving personnel support the goals of IC2S, though there are significant concerns related to the achievability of CF plans, and most important of all, the danger of the IC2S undermining the very doctrinal basis of Canadian command principles. The fear of being 'micro-managed' is palatable.

In Chapter 5, a variety of existing technological developments were examined in order to demonstrate how the CF can achieve its IC2S goals. What this chapter demonstrates, is that the goals of IC2S are largely achievable from a technical viewpoint. However, achieving these goals will require close collaboration with principle allies, and an evolutionary approach in which key technologies will have to be rapidly procured to achieve success.

In Chapter 6, a summary of recommendations that will assist the CF in achieving its goals for IC2S was presented. While these recommendations will not be repeated here, it is worth highlighting the most important. First, the CF must commit the necessary human and financial resources to IC2S if it is to have any chance of success. Second, new processes for project approval and implementation, or at least processes that

are faster, will have to be implemented. Third, the CF must do a better job of maximizing the capabilities it already has, such as the ADSI and Link 16 Systems, otherwise new investments will not pay-off. Finally, the CF must recognize that obtaining its goals for IC2S will take many years, and a constant flow of funding. There never will be an FOC, and thus, an evolutionary path will be necessary.

In conclusion, the CF hopes that by "adopting and prosecuting a coherent plan that encompasses technology, doctrine and organization via an integrated approach, [the CF] goals will be attained in an effective, efficient and economical manner."[175] This paper has demonstrated that this will not be enough. Some of the very real challenges facing Canada and her allies with respect to C2 have been highlighted. Overcoming these challenges will be a significant test for the CF. However, as this paper has shown, overall capabilities can be improved providing the CF can effectively select, and quickly field, the right technologies while ensuring good program management. Finally, while the CF has correctly deduced that "we must maintain a state of continual progress in our exploitation of technology"[176] the ability of the CF to use the technology it already possesses will be critical. After all, "sheer technological innovation…does not win wars. Instead, the interaction of technical change and organizational adaptation within realistic strategic assessment determines whether good ideas turn into real military capabilities."[177]

---

[175] C4ISR Campaign Plan Interim Report, 9.

[176] CF C4ISR Command Guidance and Campaign Plan, 20.

[177] Alan Millet in Schmidtchen, 118.

APPENDIX 1 - GLOSSARY

TERM	MEANING	USE
3D+C	Defence, Diplomacy, Development and Commerce	A widely used term that describes the different elements needed to address most of the problems of Foreign Affairs.
ABC	Apache Bowman Connectivity Node	The technology required by the British AH-64D Attack Helicopter to link into the British Army's Bowman Command and Control System
ADDN	Automated Defence Data Network	The legacy military message system used for classified and unclassified messages based on NATO standard message formats
AFCCIS	Air Force Command, Control, Information System	A secure system that basically mirrors unclassified capabilities of the DWAN for Air Force users.
BACN	Battlefield Air Communications Node	A "black box" that translates the wave forms of different tactical data links so that they can communicate with each other.
BOWMAN		The British Army's equivalent to the Canadian TCCCS/Iris System. Tactical radio based Command and Control System deployed on land, sea and air platforms.
C2	Command and Control	The Canadian Forces have not yet definitively selected the acronym that will be used when describing the concepts outlined in this paper. Thus, the very generic term C2, and occasionally terms such as C4ISR and IC2S will be used. Nevertheless, when these or other terms are used, they should be viewed as falling within the same generic category. Other synonymous terms that are in wide use include C2IS, which includes Information Systems; Command, Control, Communications and Computers (C4); C4I, which includes Intelligence; Integrated Command and Control System (IC2S); and C4ISR, which adds Surveillance and Reconnaissance to Intelligence.

Canada COM	Canada Command	The Canadian Forces Operational Level Headquarters responsible for Domestic and North American operations.
CEFCOM	Canadian Expeditionary Forces Command	The Canadian Forces Operational Level Headquarters responsible for all CF operations outside North America and Canada.
CLIP	Common Link Integration Processing	The more modern variant of the BACN capability. See above.
CNET	Classified Network	The backbone architecture of CF classified systems like TITAN. Current terminology is CSNI – Classified Infrastructure Secure Network
COE	Contemporary Operating Environment	A generic term used to describe the current operational environment. Usually used to differentiate current operations from the realities of the Cold War.
COMMAND VIEW		A system that provides CF commanders a rudimentary understanding of current operations. Includes a map display of the world that can be zoomed in and includes 'ticker tape' updates on CF Operations and a view of classified, but releasable situation reports.
COTS	Commercial Off the Shelf	When the Military purchases available systems off the commercial market that have civilian uses, but uses them for military roles. Rather than develop simple office tools, for example, the military buys COTS Microsoft Products.
DIME	Diplomatic, Information, Military, Economic	An acronym used to identify the 'levers of power' available to a government for the conduct of Foreign Affairs.
DWAN	Designated Wide Area Network	The most commonly deployed CF C2 System. Uses commercial hardware and software to provide unclassified computer support to the CF including an Intranet and MS Office tools. Some specialized military software is also available for specific unclassified

		roles.
EPLRS	Enhanced Position Location Reporting System	A tactical radio that provides voice and data capabilities with embedded Global Positioning System. This radio feeds the raw positional data needed by systems such as the Force XXI Battle Command Brigade and Below (Blue Force Tracker) System.
HTML	Hypertext Markup Language	Hypertext Markup Language is the authoring software language used on the Internet's World Wide Web. HTML is used for creating World Wide Web pages
IC2S	Integrated Command and Control System	A single system providing Secret level command and control capabilities that merges the capabilities of existing service specific systems into a single core architecture.
IRIS	The Canadian Army's Tactical Radio System.	Also more frequently referred to as TCCCS (pronounced 'tics') in Canadian Army Service
JIMP	Joint, Integrated, Multi-Agency, Public	Another term used to describe the requirements of the Contemporary Operating Environment for Foreign Affairs
LCSS	Land Command Support System	The Canadian Version of Blue Force Tracker, though it remains far from fully functional compared to the American version, and is based on the French Army "Athene" system.
LCU	Landing Craft Utility	A large conventional landing craft suitable for carrying vehicles and personnel.
LCVP	Landing Craft Vehicle and Personnel	A smaller landing craft that is often launched from the davits of amphibious ships that may not have the ability to flood down to launch LCU sized vessels.
LINK	Short for Tactical Data Link	Essentially a modem for the exchange of information, modern examples include Link 11, 16 and 22.
MCOIN	Maritime Command Operational Information Network	The Canadian Navy Secure System that basically duplicates the capabilities of the unsecure DWAN while also providing specialized naval applications.

MIDS	Multi-functional Information Distribution System	MIDS is the NATO name for the communication component of Link-16. An older MIDS is the JTIDS (Joint Tactical Information Distribution System).
MMHS	Military Message Handling System.	Updated capability of the ADDN.
MOTS	Military Off the Shelf	Software and Hardware not generally available to the public, but can be purchased from other governments.
NIPRNET	formerly called the Non-secure Internet Protocol Router Network	NIPRNET stands for Unclassified but Sensitive Internet Protocol Router Network. The NIPRNET is a network of Internet protocol routers owned by the Department of Defense (DOD). Created by the Defense Information Systems Agency (DISA), NIPRNET is used to exchange unclassified but sensitive information between "internal" users as well as providing users access to the Internet.
SADL	Situational Awareness Data Link	The specific data link fitted to the US Air National Guard F-16 Block 30 only. Similar in the basic idea of Link 16 and Link 11 – a modem like capability, but not compatible with these other systems.
SINGARS	Single Channel Ground and Airborne Radio System	A new family of VHF-FM radios designed to provide the primary means of command and control for Infantry, Armor, and Artillery units. The radios can transmit and receive voice and tactical data while operating in a frequency hopping mode.
SIPRNET	Secret Internet Protocol Router Network	The SIPRNET is a system of interconnected computer networks used by the U.S. Department of Defense to transmit classified information (up to and including information classified SECRET//NOFORN) by packet switching over the TCP/IP protocols in a completely secure environment. It also provides services such as hypertext documents and electronic mail.

TCCCS	Tactical Command, Control and Communications System	Pronounced 'tics' the Canadian Army's tactical radio system. Sometimes referred to as the Iris system, though usually only by signalers.
TCP/IP	Transmission Control Protocol/Internet Protocol	A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.
TITAN		A CF system that originated from the requirement for the National Defence Operations Centre to have a secure capability essentially duplicating the unclassified DWAN. The current standard Secret level system used at the Joint level.

BIBLIOGRAPHY

Books

Gompert, D.C., H. Pung, K.A. O'Brian and J. Peterson, *Stretching the Network – Using Transformed Forces in Demanding Contingencies Other Than War*. Santa Monica, CA: Rand Corporation, 2004.

Government of Canada Documents

Canada. Defence Research and Development Canada, Sandy Babcock. *DND/CF Network Enabled Operations Working Paper*. Toronto: Directorate of Scientific and Technical Policy, January 2006.

Canada. Department of National Defence. A-AE-025-000/FP-*001 Canadian Forces Doctrine Development*. Ottawa: DND Canada, 2003.

Canada. Department of National Defence. B-GA-400-000/FP-000 *Canadian Forces Aerospace Doctrine*. Ottawa: DND Canada, 2006.

Canada. Department of National Defence. B-GL-300-003/FP-000 *Command*. Ottawa: DND Canada, 1996.

Canada. Department of National Defence. B-GJ-005-300/FP-000 *Canadian Forces Operations*, Ottawa: DND Canada, 2005.

Canada. Department of National Defence. *Briefing to CDS/VCDS – Joint Information and Intelligence Fusion Capability Detachment Update: JIIFC Det Strawman to 2010*. Ottawa: DND Canada, 18 December 2006.

Canada. Department of National Defence. *C4ISR CP Brief to CFOC*. Ottawa: LCol B.T. Pickard and LCol J.C.P. Jourdeuil, 27 Feb 2007.

Canada. Department of National Defence. *Canadian Forces C4ISR Command Guidance and Campaign Plan*. Ottawa: Deputy Chief of Defence Staff, December 2003.

Canada. Department of National Defence. *Canadian Forces Command Decision Support Capability: Principles and Goals*. Ottawa: Director General Joint Force Development, September 2003.

Canada. Department of National Defence. *Canadian Forces C4ISR Campaign Plan – Interim Report*. Ottawa: Director Joint Force Capabilities, June 2003.

Canada. Department of National Defence. *Canadian Forces C4ISR Command Guidance and Campaign Plan*. Ottawa: Deputy Chief of Defence Staff, December 2003.

Canada. Department of National Defence. *Capability Development Record – Command*. Kingston: Director Army Doctrine, June 2006.

Canada. Department of National Defence. *Integrated Command and Control System: Interim Findings*. Ottawa: DND Canada, January 2007.

Canada. Department of National Defence. *Integrated Command and Control System (IC2S) 2006 Year End Project Status*. Ottawa: DND Canada, DJCP7-3, 22 December 2006.

Canada. Department of National Defence. *1 Canadian Air Division Multi-Purpose Information Distribution System Concept of Operations*. Ottawa: 1 Canadian Air Division A3 Fighter Systems, 3 July 2006.

Canada. Department of National Defence. *IM/IT Rationalization Tiger Team Projects Working Group: Final Report*. Ottawa: DND Canada, September 2006.

Hillier, General R.J. *CDS Directive – Command and Control Information System*. NDHQ Ottawa: file 1243-1 (CDS), 4 August 2006.

Natynczyk, Lieutenant-General W.J. *Quarterly Progress Report On The Implementation Of A CF Integrated Command and Control Information System*. NDHQ Ottawa: file 2700-1 (DJCP 6), 30 November 2006.

Natynczyk, Lieutenant-General W.J. *VCDS Direction –CF Integrated Command and Control Information System*. NDHQ Ottawa: file 2700-1 (CFD), 18 September 2006

Pearce, J.L. *Presentation - The Revolution in Military Affairs*. Ottawa: DND Canada, 30 November 1998.

Allied Government Documents

United States. National Research Council. *Realizing The Potential of C4I*. Washington: National Academy Press, 1999.

United States. Department of Defense. *Joint Data Network Operations*. Washington: Joint Staff, 2000.

United States. Department of Defense. Ms. Robin Quinlan. *Presentation - Family of Interoperable Operational Pictures (FOIC)*. Washington: Office of the Secretary of Defense, date unknown.

Great Britain and the United States. Ministry of Defence and the Department of Defense. *A Network-Centric Operations Case Study: US/UK Coalition Combat Operations*

during Operation Iraqi Freedom. Washington: Office of Force Transformation, 2005.

Journal Articles

Leahy, Lieutenant-General Peter."Towards the Hardened and Networked Army" *Australian Army Journal*. Volume II, number I (Winter 2004): 27-36.

Nordick, Brigadier-General G.W. "Guest Editorial: Command and Control Aspects of Digitization." *The Army Doctrine and Training Bulletin* Volume 6, Number 1 (Spring 2003): 1-3.

Rolin, Xavier. "The RMA, C2 and Coalition Operations," *Australian Defence Force Journal*. Number 144 (September/October 2000): 27-29.

Ryan, Lieutenant-Colonel Michael. "Finding Alligators: The Future of Network-Centric Warfare." *Australian Army Journal* Volume II, Number 2 (Autumn 2005): 101-110.

Schmidtchen, Lieutenant-Colonel David. "Network-Centric Warfare: An Idea in Good Currency." *Australian Army Journal* Volume II, Number 2 (Autumn 2005): 111-123.

Internet Sources

Australia, Department of Defence, Defence Science and Technology Organization, Leoni Warne, Irena Ali, Derek Bopping, Dennis Hart, and Celina Pascoe. *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*. Edinburgh: DSTO Information Sciences Laboratory, 2004; on line; available from http://www.dsto.defence.gov.au/publications/3430/DSTO-CR-0373.pdf; Internet; accessed 19 April 2007, 10.

Author Unspecified. "Bowman pulls in its horns." *Janes International Defence Review* (September 2006); Journal On-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2006/idr10019.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Bowman+%3CAND%3E+pulls+%3CAND%3E+its+%3CAND%3E+horns%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Bowman+%3CAND%3E+pulls+%3CAND%3E+its+%3CAND%3E+horns%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Bowman+%3CAND%3E+pulls+%3CAND%3E+its+%3CAND%3E+horns%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Author Unspecified. "The Ticonderoga Class (CG-47),"; available from http://navysite.de/cg/cg47class.htm; Internet; accessed 16 April 2007.

Author Unspecified. "Software Problem Prevents Deployment of U.S. Navy's CEC." *Janes Defence Weekly* (July 1998). Journal on-line; available from http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw98/jdw02505.htm@current&Prod_Name=JDW&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Cooperative+%3CAND%3E+Engagement+%3CAND%3E+Capability%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Cooperative+%3CAND%3E+Engagement+%3CAND%3E+Capability%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Cooperative+%3CAND%3E+Engagement+%3CAND%3E+Capability%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Ebbutt, Giles. "Knowledge is power: armies refine their filtering of battlespace data." *Janes International Defence Review* (January 2007). Journal on-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2007/idr10240.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+knowledge+%3CAND%3E+is+%3CAND%3E+power%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+knowledge+%3CAND%3E+is+%3CAND%3E+power%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+knowledge+%3CAND%3E+is+%3CAND%3E+power%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Erbetta, John. "Interoperability and Net-Centricity." *Military Technology*. (May 2003). Journal on-line; available from http://proquest.umi.com/pqdweb?index=8&did=358330671&SrchMode=1&sid=1&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1176937041&clientId=1711; Internet; accessed 19 April 2007.

Lok, Joris Janssen. "Netherlands equips national crisis centre." *Janes International Defence Review* (January 2007). Journal on-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2007/idr10230.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Netherlands+%3CAND%3E+equips+%3CAND%3E+national%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Netherlands+%3CAND%3E+equips+%3CAND%3E+national%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Netherlands+%3CAND%3E+equips+%3CAND%3E+national%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

McIntyre, S.G., M. Gauvin and W Waruszynski. "Knowledge Management in the Military Context." *Canadian Military Journal*. Spring 2003. Journal on-line; available from http://www.journal.dnd.ca/engraph/Vol4/no1/pdf/v4n1-p35-40_e.pdf; Internet; accessed 19 April 2007.

Pengelley, Rupert. "Bird in the hand: Bowman bridges the digital divide for British Army." *Janes International Defence Review* (September 2005). Journal on-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2005/idr04296.htm@current&Prod_Name=IDR&QueryTe

xt=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Bird+%3CAND%3E+in+%3CAND%3E+the+%3CAND%3E+hand%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Bird+%3CAND%3E+in+%3CAND%3E+the+%3CAND%3E+hand%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Bird+%3CAND%3E+in+%3CAND%3E+the+%3CAND%3E+hand%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Pengelley, Rupert. "NATO seeks a standard bearer for encryption in coalition operations." *Janes International Defence Review*. (August 2006). Journal on-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2006/idr04910.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+NATO+%3CAND%3E+seeks+%3CAND%3E+a+%3CAND%3E+standard+%3CAND%3E+bearer%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+NATO+%3CAND%3E+seeks+%3CAND%3E+a+%3CAND%3E+standard+%3CAND%3E+bearer%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+NATO+%3CAND%3E+seeks+%3CAND%3E+a+%3CAND%3E+standard+%3CAND%3E+bearer%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Pengelley, Rupert. "Network power: communications systems join up command levels." *Janes International Defence Review* (March 2007). Journal on-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2007/idr10302.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Network+%3CAND%3E+power%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Network+%3CAND%3E+power%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Network+%3CAND%3E+power%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Pengelley, Rupert. "UK rethinks joint effects computing plan." *Janes International Defence Review* (October 2006). Journal on-line; available from http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2006/idr10059.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+UK+%3CAND%3E+rethinks+%3CAND%3E+joint+%3CAND%3E+effects%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+UK+%3CAND%3E+rethinks+%3CAND%3E+joint+%3CAND%3E+effects%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+UK+%3CAND%3E+rethinks+%3CAND%3E+joint+%3CAND%3E+effects%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Pigeau, Ross and Carol McCann. "Reconceptualizing Command and Control." *Canadian Military Journal*. Spring 2002. Journal on-line; available from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc13/p519041.pdf; Internet; accessed 19 April 2007.

Sirak, Michael J. Kucera. "US Air Force studies use of F-16 with army Strykers." *Janes Defence Weekly*. (December 2004). Journal on-line; available from http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw2004/jdw09733.htm@current&Prod_Name=JDW&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+US+%3CAND%3E+Air+%3CAND%3E+Force+%3CAND%3E+studies%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+US+%3CAND%3E+Air+%3CAND%3E+Force+%3CAND%3E+studies%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+US+%3CAND%3E+Air+%3CAND%3E+Force+%3CAND%3E+studies%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Thomson, Michael H. and Barbara D. Adams. *Network Enabled Operations – DRDC Toronto No. CR-2005-162*. Toronto: Defence Research and Development Canada, May 2005; available from http://pubs.drdc-rddc.gc.ca/inbasket/CEBsupport.050513_1410.CR%202005-162%20final.pdf; Internet; accessed 19 April 2007.

Toomey, Christopher J. "Army Digitization: Making it Ready For Prime Time." *Parameters* 33, Number 4 (Winter 2003-2004). Journal on-line; available from http://www.carlisle.army.mil/usawc/Parameters/03winter/toomey.htm; Internet; accessed 18 April 2007.

Trimble, Stephen. "Network-Centric Warfare Part 1: Communication Gateways – Gateway to the Future." *Janes Defence Weekly* (January 2007). Journal on-line; available from http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw2007/jdw31553.htm@current&Prod_Name=JDW&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Network-centric+%3CAND%3E+Warfare+%3CAND%3E+Part+%3CAND%3E+1%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Network-centric+%3CAND%3E+Warfare+%3CAND%3E+Part+%3CAND%3E+1%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Network-centric+%3CAND%3E+Warfare+%3CAND%3E+Part+%3CAND%3E+1%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.

Williamson, John. "Bigger, better C4ISR systems underpin US warfighting efforts." *Janes International Defence Review* (August 2003). Journal on-line; available from

http://www4.janes.com/subscribe/idr/doc_view.jsp?K2DocKey=/content1/janesdata/mags/idr/history/idr2003/idr01622.htm@current&Prod_Name=IDR&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5D%28+Bigger+%3CAND%3E++better%29+%3CIN%3E+body%29%2C+%28%5B100%5D+%28%5B100%5D%28+Bigger+%3CAND%3E++better%29+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5D%28+Bigger+%3CAND%3E++better%29+%3CIN%3E+body%29%29%29%29; Internet; accessed 18 April 2007.