Research Essay

Communications and Information Systems

A Requirement for the Canadian Forces

Col P.J. McCabe

Advances Military Studies Course Number 1/Canadian Forces College

23 November, 1998

Introduction

Militaries throughout history have used communications and information dominance[1] to achieve victory on the battlefield. In discussing the evolution of Cyberwar, John Arquilla and David Ronfeldt comment on the effective use of information dominance by the Mongols in the twelfth and thirteenth centuries to achieve victory against forces from the finest armies of imperial China, Islam and Christendom.[2] Yet over the centuries, command staffs have grown in size. Moreover, the nature and the conduct of warfare have become even more complex. In consequence, there has been an increased demand for improved visualization of the battlespace[3] in an attempt to lift Clausewitz's "fog of war". As reported by John Miller, the recent wave of unprecedented change, brought on by the information revolution, has stimulated significant advances in Communications and Information Systems (CIS) to the point where reliable information

[1] Information dominance is defined as "the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary". Unites States, FM 100-6 Information Operations, (Washington, D.C.: Headquarters Department of the Army, 1996), Glossary 7.

[2] John Arquilla and David Ronfeldt, "Cyberwar is Coming," Comparative Strategy (Spring 1993): 148.

[3] Battlespace is defined as "components determined by the maximum capabilities of friendly and enemy forces to acquire and dominate each other by fires and maneuver in the electromagnetic spectrum". United States, FM 100-6 Information Operations, Glossary 1.

dominance is a reasonable expectation.[4] At the same time, the increased speed and processing power of these systems have led to instant battlespace visualization[5], significantly reducing the decision-action cycle time available to the military commander. To cope with increased speed and complexity of modern warfare, commanders at all levels are demanding access to robust and highly sophisticated CIS.

Since the end of the Cold War, Canada has witnessed a transition from a bipolar world involving two superpowers, to one with regions of instability that threaten international peace and security. It is anticipated that in the future, there will be a shift towards irregular operations or combined Operations Other Than War (OOTW) carried out by allied coalitions. For the Canadian Forces (CF) to participate in these types of operations in a credible manner, there will be a need for the CF to posses state-of-the-art CIS systems that are interoperable with our allies.

The aim of this essay is to demonstrate that in order to participate in coalition lead OOTW, the CF to must maintain a robust state-of-the-art CIS capability at the operational level. The CIS component of Information Operations (IO) will be explored to understand

[4] John Miller, "Information Warfare: Issues and Perspectives," Sun Tzu Art of War in Information Warfare (March 1995): 3.

[5] Battlespace visualization is defined as "the process whereby the commander develops a clear understanding of the current state with relation to the enemy and environment, envisions a desired end state that represents mission accomplishment, and then subsequently visualizes the sequence of activity that moves the commander's force from its current state to the end state". United States, FM 100-6 Information Operations, Glossary 1.

its applicability to the Canadian Forces. The nature of future Canadian military operations will be examined and the CIS requirements of Canadian commanders in combined operations with our allies will be assessed. Through an analysis of Canadian defence priorities, command requirements and current trends in technology, a compelling argument will be put forward for the CF to invest in a robust CIS infrastructure at the operational level.

Background

To exercise command in today's information age, military commanders at the strategic level are faced with operating in an expanding information domain termed the Global Information Environment (GIE). As defined by the Department of the Army, the GIE includes all individuals, organizations, or systems that collect, process and disseminate information to national and international audiences.[6] That area within the GIE that supports, enables or significantly influences military operations at the operational level is known as the Military Information Environment (MIE).[7] As advances in technology continue at an impressive rate, the MIE is becoming increasingly complex involving numerous technological challenges. Although many of the information processes and systems situated within MIE reside in the public domain, they have a direct impact on the outcome of military operations at the operational level. With

[6] United States, FM 100-6 Information Operations, 1-2.

[7] Ibid., 1-4.

the rapid expansion of global communications and ease of access to the Internet, the media, independent organizations and even individuals have become players within the MIE. The operational commander in warfare today, must be aware of and understand the MIE, and develop the culture and tools to achieve information dominance over an adversary.

The US Department of the Army defines IO as "continuous military operations within the MIE that enable, enhance, and protect the friendly forces ability to collect, process, and act on information to achieve an advantage across the full range of military operations: IO include interacting with the GIE and exploiting or denying an adversary's information and decision capabilities."[8] The CF Director of Army Doctrine staff view IO as a multidimensional combat function with a principal objective to "achieve superiority and relative advantage between the friendly commander's decision-action cycle and that of the enemy, and to use that advantage to enhance and enable other elements of combat power."[9] While it is evident from the preceding statements that there is a tendency to focus at the tactical level when discussing IO, it is important to note that critical activities take place at the operational level. It is at this level that commanders define and develop a campaign plan, establish centers of gravity and define the intent for IO within the campaign plan.

[8] Ibid., 2-3.

[9] Canada, B-GL-300-005/FP-000 Information Operations Draft Version 1.0, (Kingston, Canada: Director of Army Doctrine, 1998), 8.

In the Canadian context, IO is comprised of the following five interrelated components which have strategic, operational and tactical elements:[10]

Intelligence and Information the collection, use and dissemination of intelligence and relevant information which are fused to provide the commander with a complete view of the battlespace;

Communications and Information Systems (CIS) the communications and information systems and processes that allow the collection, processing, storage and dissemination of information relating to current and future operations;

Command and Control Warfare (C^2W) the integrated use of all military capabilities including electronic warfare, deception, psychological operations and operational security to deny information from the enemy, influence or degrade the adversary's Command and Control (C^2) capabilities and protecting our own from similar actions; [11]

Civilian Military Cooperation the act of interfacing with the critical civilian actors in the area of operations to collect information and influence and exploit relations among military forces, civil authorities and the civilian populace; and

[10] Ibid., 18-25.

[11] Command and control is defined "the exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; C^2 functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directing, coordinating and controlling forces and operations in the accomplishment of the mission". United States, FM 106 Information Operations, Glossary 2.

Public Affairs the act of monitoring public opinion and advising the commander on likely courses of action and the dissemination of factual information regarding the intent of the commander about military operations.

Norman Davis in his discussion of IO and the Marine Corps states that: "A significant lesson of the Gulf War was that the key to success on the modern battlefield is not just the possession of technologically superior weapons and delivery systems, but the ability to effectively control and integrate these tools on the battlefield."[12] To acquire the necessary battlespace visualization and exercise effective command at the operational level, commanders require access to systems that transform data into knowledge. When combined with a commander's judgement and intuition, this knowledge facilitates the commander understanding of the battlespace. It is within this complex and rapidly changing context that CIS has gained prominence. Effective implementation of CIS systems and technology holds the promise of information dominance, which can provide a significant advantage in future military operations.

The CIS is the glue that binds the components of IO together to form a cohesive system. It includes personnel, hardware and procedures necessary for the collection, processing, dissemination and display of information. The CIS provides the means by which raw data is transformed into well-organized knowledge facilitating the operational commander's understanding of the battlespace. It forms the backbone of the C^2 system,

[12] Norman C Davis, "The Marine Corps and Information Operations," Marine Corps Gazette (April 1997): 16.

enabling the commander to view and understand the battlespace, communicate operational intentions, control formations, and disseminate relevant and accurate information to all levels within the formation. The critical characteristics of the CIS are its flexibility and interoperability. [13] These features allow the commander to rapidly react to changes in priorities and to integrate effectively into a coalition command infrastructure.

To place this discussion of the CIS into context, it is necessary to examine the concept of a Revolution in Military Affairs (RMA) in order to predict the potential influence the employment CIS will have in future military operations. A basic understanding of the RMA is provided in the following definition put forward by the U.S. Department of Defense's Office of Net Assessment, "an RMA as a major change in the nature of warfare brought about by the innovative application of technologies which, combined with dramatic changes in military doctrine, and operational concepts, fundamentally alters the character and conduct of operations."[14] Two significant facts stand out in this definition: the RMA leads to major change in the nature of war; and advances in technologies alone do not bring about revolutionary change. As Andrew Krepinevich emphasizes, "while advances in technology typically underwrite a military

[13] United States, FM 106 Information Operations, 2-7 to 2-8.

[14] Earl H. Tilford, "The Revolution in Military Affairs: Prospects and Cautions," (Carlisle Barracks Pennsylvania: U.S. Army War College, 1995), 1.

revolution, they alone do not constitute a revolution.".[15] In his review of military revolutions, Krepinevich contends that there have been ten military revolutions from the so-called infantry revolution of the Hundred Years War, to the more recent nuclear revolution.[16] Each revolution has brought about significant changes in the conduct of conflict based on the integration of advanced technology with new processes or doctrine, executed by new military organizational structures. It should be noted that "new military organizational structures" have been included as a factor that contribute to a RMA. In summation, a RMA represents a significant or revolutionary change in the conduct of warfare brought about by the synergistic integration of advances in technology with changes in military doctrine, organizational structures and operational concepts. The synergy achieved through the integration of these concepts allows for an unprecedented change that would not have been possible through any one of the contributing elements acting alone. It is in this context that CIS will be assessed within the current RMA.

In his assessment of the current RMA, Michael Mazarr suggests that we are in fact in the midst of a RMA that stems from a decentralized information-based society, an independent world economy, and the dramatic effects of new civilian and military technologies.[17] More specifically, he states that information is at the core of the current

[15] Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest (Fall 1994): 30.

[16] Ibid., 31-36.

[17] Michael J. Mazarr, "The revolution in Military Affairs: A Framework For Defense Planning," (Carlisle Barracks Pennsylvania: U.S. Army War College, 1994), 3.

RMA. Considering the complexity and swift pace of modern warfare, he submits that a rapid exchange of information and reliable, real-time command and control are essential to success in battle.[18] Colin S Gray emphasizes this point in his assessment of the American RMA. [19] He holds that the RMA now under way is in the process of transforming the character of war by allowing the conduct of information warfare. In fact, he goes even further to suggest that this is an information-oriented RMA.[20] With advances in sensor technology, information warfare will soon yield the ability to quickly detect targets and precisely direct firepower simultaneously throughout the theatre of operations. From the preceding, it is clear that CIS development is situated in the center of the current RMA, and will be essential to effective command and control in the transformed information based battlespace of the future. As technology advances within the current RMA, CIS will be dramatically enhanced bringing significant capabilities to the operational level commander.

[18] Ibid., 9.

[19] Colin S. Gray, "The American Revolution in Military Affairs: An Interim Assessment," The Strategic and Combat Studies Institute, The Occasional Number 28 (1997): 10.

[20] Gray contends that the current RMA has been helped forward by the former Vice Chairman of the U.S. Joint Chiefs of Staff, Admiral William A Owens' leadership in fostering the information based transformation of warfare. Owen's trinitarian approach to the RMA includes a synergistic combination of intelligence, surveillance and reconnaissance (ISR) capabilities; advanced command, control, communications, computer and intelligence (C^4I) assets; and precision guided munitions (PGMs), working vitally together to achieve a transformation of the character of warfare. Ibid., 14.

Case For Action

Since the end of the Cold War, rising nationalist feelings and fundamentalist movements have lead to a significant increase in unrest and regional conflict throughout the world. In their study of the structured framework for the Military Technical Revolution, Michael Mazarr et al. state that Western defense planning has moved from an intense focus on a single global threat to analyzing and preparing for regional crisis and wars that involve a variety of potential aggressors and victims.[21] It is evident that there has been a transition from a bipolar world involving two superpowers to one with regions of instability that threaten international peace and security. The shift more towards coalition based OOTW witnessed in Bosnia, Somalia, Angola and Cambodia is anticipated to continue in the future. It is within this unpredictable environment, that Canada finds itself with a vital interest in ensuring global security to support Canada's political interests and economic future through its ability to trade freely with other nations.

In the 1994 Defence White Paper, the Canadian Government states that Canada is committed to remain an active participant in multilateral efforts to promote collective security.[22] Canada will continue to participate in multilateral operations anywhere in the

[21] Michael J. Mazarr, Jefrey Shaffer and Benjamin Ederington, Military Technical Revolution: A Structural Framework, (Washington, D.C.: The Center For Strategic and International Studies, 1993), 2.

[22] Canada, 1994 Defence White Paper, (Ottawa: Canada Communications Group, 1994), 12.

world under the auspices of the UN or in the defence of a NATO member state.[23] This reflects Canadians values and interests in particular: that Canadians deem their security to be indivisible from that of their allies; and that Canadians have a strong sense of responsibility to alleviate suffering and respond, where they can make a difference.

It is obvious that collective defence remains fundamental to Canada's security and that these cooperative defence arrangements serve Canada's interests extremely well. For a modest investment in the Canadian Forces, Canada gains valued stability in a very turbulent world. As noted in the White Paper, "the Government has concluded that the maintenance of a multi-purpose, combat-capable forces is in the national interest. It is only through the maintenance of such forces that Canada will be able to retain the necessary degree of flexibility and freedom of action when it comes to defence of its interests and the projection of its values abroad."[24] Through participation in UN operations Canada secures influence at the international level via the development of shared political and commercial interests. As a partner in the defence of North America, Canada influences the formulation of U.S. defence policy in those areas where Canada's defence interests are concerned.

The challenge for the Canadian Government is to meet these commitments at a time when there are limited resources to apply to the defence program. As suggested in

[23] Ibid., 38.

[24] Ibid., 13.

the White Paper, with reduced military expenditures in many countries, multilateral cooperation represents a sound method to pool national resources and achieve the greatest benefit.[25] In this manner, Canada will leverage the most benefit from a significantly reduced defence budget. What becomes clear from this reasoning is that, in the future, Canada's contribution to international security will be in the form of CF participation in multilateral or combined coalition operations.

Rapid advances in information systems resulting from the current RMA have thrust CIS into center stage in Western militaries where it is employed at the operational level in areas such as: logistics, operations, planning and intelligence functions. The complexity of today's battlespace, combined with a short duration decision-action cycle, demands that military commanders have access to a reliable C^2 system based on a robust CIS infrastructure. As stated by Stephan Blank in relating Soviet views on the Gulf War: "thus a new type of conventional war embracing land, sea, air, and space is upon us. … No longer will there be a front or a rear. Rather there will be targets and non-targets which can be precisely located. PGMs erase distinctions between tactical and strategic strikes and targets, often between offense and defense."[26] With a move towards more combined OOTW, effective CIS technology is essential for a smooth integration of "force packages" into the complex command and control arrangements of coalition forces. In addition, current reductions in militaries necessitates the introduction of the latest CIS technology and systems to maximize the potential of forces at the operational level.

It is evident, that for Canada to participate effectively in coalition OOTW, the CF must be able to integrate into a complex coalition C^2 structure to share operational information and receive direction. To accomplish this essential goal, Canada must continue to invest in CIS infrastructure, particularly in the area of command and control. If Canada lags behind, it runs a significant risk of loosing interoperability with its allies and thus the ability to participate in or influence combined operations. Davis makes this point very clearly in relation to the US Marine Corps where he states:

> "However the military is fundamentally a political instrument. Tactical actions are inextricably linked to strategic aims-and are increasingly capable of strategic effect. As future crises develop, national and theatre-level decision-makers will examine the potential military responses through the lens of IO/IW. Planners will use IO to seek to prevent the situation from deteriorating to the point where military forces must be committed in a combat role. If we cannot articulate how Marine Corps forces can contribute to such a theatre-level IO campaign, then we risk becoming marginalized in a narrow segment of the conflict spectrum as joint planners look to other forces that can articulate their relevance.".[27]

[27] Davis, "The Marine Corps and Information Operations," 19.

Unfortunately, as a result of recent budget reductions, there are early indicators of deficiencies in Canadian CIS capabilities that are already limiting CF interoperability. As an example, current compatibility limitations associated with the aging CF-188 aircraft tactical data link system will soon restrict Canadian participation in combined operations and exercises with our allies.[28] In the maritime patrol environment, the inability of the CP-140 aircraft acoustics system to receive data from sonobouys used by our allies, currently limits Canadian participation in combined operations and exercises.[29] Although work is progressing on the Joint Command and Control Information System (JC^{2}IS), full implementation at the strategic level is not anticipated until the year two thousand. Development will then proceed to achieve connectivity across all components at the operational level. As with other large projects of this nature, the future of the project is tied to adequate funding which is not certain. Additional reductions in the funding levels could therefore result in delays in the project or premature termination of the project without achieving the essential operational level connectivity. With these and other similar limitations in CIS infrastructure, Canada is at significant risk of loosing the ability to effectively participate in coalition exercises and OOTW. Considering the

[28] Tactical information and mission guidance is passed from area operations control centers to CF-188 aircraft in the form of encrypted digital transmissions. Without the ability to receive this information Canadian units will be unable to effectively participate in coalition operations. This information is based on the Author's first hand knowledge from current employment in 1 Canadian Air Division Headquarters.

[29] The sonobouy collects acoustic information related to maritime targets and transmits this information to the CP-140 aircraft. The newer sosnbouys utilized by our allies transmit data at frequencies that current CP-140 receivers are not capable of processing. This information is based on the Author's first hand knowledge from past employment at 14 Wing, Greenwood N.S.

indispensable training benefits of NATO exercises and the crucial leverage Canada achieves from UN and NATO operations, action should be taken to reverse this trend.

As reported in the 1994 Defence White Paper, the accumulated national debt combined with past budget deficits has limited the government's freedom of action in responding to the needs of Canadians .[30] For the CF this situation has resulted in significant reductions in defence funding and corresponding reductions in personnel levels. As articulated in the Land Force strategic Doctrine and Guidance:

> " Despite financial constraints, the Canadian government will continue to commit soldiers to overseas operations. Peace support missions are viewed by Canadian governments as foreign policy initiatives that have high domestic appeal and provide international recognition. These operations will be conducted in an environment that will include the expectation by the Canadian people and their elected representatives that the Army displays the highest moral values and restraint, follows strict rules of engagement and minimizes civilian casualties and damage to infrastructure. At the same time casualties to Canadian service personnel will be considered intolerable and Canadian operations will be subject to intense media scrutiny.".[31]

The CF must strive to achieve excellence in all operations with the precision application of force in a multi-faceted and multi-dimensional environment. In partnership with our

[30] Canada, 1994 Defence White Paper, 9.

[31] Canada, The Land Force Strategic Direction and Guidance, (Kingston: Director of Army Doctrine, 1998), Part I, Chapter 1, Section 4, Paragraph 3.

allies, Canada can move closer to achieving this goal through enhanced application of CIS to focus the employment of force, at the operational level, thus reducing the price of success and minimizing collateral damage.

In response to the potential increase in operational tempo and reduced resources, action has been initiated at all levels within the CF to re-engineer and improve processes to maximize the efficiency while retaining its military effectiveness. As witnessed in OP EXCEL (ADM(MAT)), FLIGH PLAN 97 (Air Command) and OP GENESIS (CF-188 support infrastructure), staffs at all levels are searching out new ways to achieve the mission with fewer resources. As a result, headquarters and units are demanding increased access to current CIS technology and systems for gains in efficiency. Despite best efforts and advances in many areas, additional funding cuts and personnel reductions have placed an even greater pressure on Canadian military commanders. The result is a focus on funding operations at the expense of capital equipment programs and infrastructure maintenance.[32] When Canada should be investing in CIS technology to gain efficiencies, funding for significant national infrastructure projects is being reduced and some programs are being delayed. This point is illustrated by the delays in the past two years in the Material Acquisition and Support Information System (MASIS) project which was initiated to update the CIS infrastructure that supports procurement and in service support of CF equipment.

[32] This statement is based on personal observation of the Author resulting from employment in Air Command Headquarters from 1992 to 1995 and employment in 1 Canadian Air Division Headquarters from 1996 until the present.

The impressive advances in technology and information systems have revolutionized private sector business with an unprecedented focus on information. In their discussion of cyberwar Arquilla and Ronfeldt make comment that information itself is a strategic resource with significant importance in the post-industrial era .[33] To meet the needs of a population spread throughout cities and isolated communities across a great geographical expanse, Canada, like many other countries, has invested heavily in a "high tech" infrastructure. The result is that within Canada the provision of public, business and finance services, communications and power distribution has become extremely vulnerable to the threats that exist in cyberspace. As James Adams commented to the Online News Summit '98, the critical infrastructure of modern society is at risk as a result of automation through the incorporation of advanced technology.[34] The telecommunications, transportation, electric power, finance and emergency services of the "wired nation" are dependent on a robust and secure cyberspace for their operation. He cites the loss of electrical power in Aukland, New Zealand and the Canadian ice storm in January 1998 as recent examples of what could happen as a result of a well planned cyber attack. In both cases, essential services were lost and many aspects of normal business were shut down.

[33] Arquilla, "Cyberwar is Coming," 143.

[34] James Adams, "Big Problem-Bad Solution: The Crisis in Critical Infrastructure and the Federal Solution," Online News Summit '98, 18 May 1998 2.

Canada must take action to protect its critical infrastructure, including strategic information, from attacks in cyberspace. In their discussion of information terrorism, Matthew Devost et al. present a strong case for the US military to play a key role in confronting and countering information terrorism in the US.[35] While the CF does not posses the detailed technical skills to resolve such a complex issue independently, it could add great value by taking a leadership role in this initiative and partnering with the private sector to develop the necessary capabilities. Considering the broad scope of this challenge, the CF may be the only institution with a national mandate and necessary infrastructure to take on such a task. The recent decision by the Government to appoint the CF as the lead agency in dealing with the Year 2000 computer problem, provides ready recognition of the ability of the CF to handle such an initiative. It makes sense to align the national domestic requirement in this area with the needs of the CF to develop a robust CIS infrastructure.

In summary, Canada's commitment to participate in multilateral coalition OOTW will continue to grow necessitating continued interoperability of C^2 systems with Canada's allies. To achieve the efficiencies dictated by force structure reductions and maintain a credible interoperability with its allies, Canada must continue to invest in CIS technology towards maintaining a robust state-of-the-art capability. This action will ensure the military maintains a much-needed capability to continue to accrue the benefits

[35] Matthew G. Devost, Brian K. Houghton and Neal A. Pollard. "Information Terrorism: Can You Trust Your Toaster," Institute for National and Strategic Studies, Sun Tzu Art in Information Warfare Web Page, "http://www.ndu.edu/inss/siws/ch3.html" 6-7.

derived from participation in UN and NATO coalition operations and provide a direct benefit to the national interests of Canada.

The Proposal

Canada should maintain a robust CIS capability at the operational level in a manner that allows the commander to exercise full command of assigned assets . This action would enable the CF to maintain full interoperability with allied forces while accruing the efficiencies offered by CIS technology. Moreover, a vision should be defined for CIS development to include a strategic plan that ensures the incorporation of innovative ideas and, where appropriate, development of advanced technology in partnership with private industry and in cooperation with our allies.

Limitations and Risks

Investing in CIS can be a two-edged sword as the additional capabilities resulting from the integration of advanced technology can expose the information and command processes at the operational level to increased risk from attack in cyberspace. As discussed in a RAND corporation research paper on this subject, "about 95 percent of military communications travel over the same phone networks used to fax a contract or talk with a friend in another state".[36] While this fact applies mostly at the strategic level,

[36] "Information Warfare: A Two-Edged Sword," RAND Research Review 19.2 (Fall 1995): 1.

similar vulnerabilities exist at the operational level due to a reliance on commercial satellites. This could result in significant risk for operational commanders. Gerald Segal follows up on this point in his look at how East Asian countries are dealing with the impact of the explosion of cyberspace and its associated crime throughout their society and government agencies.[37] He cites a number of examples of the damage caused by computer hackers who obtained secret government information through devious means and then posted it in the open media. Segal notes that: "An important problem faced by law enforcement authorities, even the most developed in the world, is the lack of sufficient expertise in dealing with criminal gangs."[38] It is critical to note that, at the operational level, the military is exposed to the same risks with no current means to defend against attack or influence by outside sources. The risk then, is that as the CF places more emphasis on advanced CIS technology, it becomes increasingly vulnerable to sabotage and attack from cyberspace.

Rapid advances in digital communications technology have had a significant impact on the CIS through the fusion of new sensors with high speed networks coupled with the impressive processing power of information systems. While there is great excitement regarding the advantages offered by the information revolution, it is this same rapid advance in technology and information system continues to drop rapidly, the life expectancy of CIS systems and technology continues to be reduced. The result is greater demand for investments in upgrades. In commenting on the wave of major technological advances, William Halal et al. state: " The four information-technology fields-computer hardware, computer software, communications, and information services-appear to lead the wave of innovation by about five years."[39] They go on to point-out that advances in information technology are driving a much larger technological revolution. To not invest in this critical area is to be quickly left behind as the technology revolution marches on yet, to remain current requires the allocation of significant resources to deal with the rapid advances.

The proliferation of CIS technology in the military environment and its impressive processing and data storage capabilities have lead to an overemphasis on the control aspect of C^2. Ross Pigeau and Carol McCann coined the term "Command and Control Schizophrenia (C^2S)" to describe the current imbalances existing at the command level. In addressing this subject they point out, "over-emphasis on Control has relegated the consideration of the human factors of C^2 to an ancillary and often post hoc status."[40] With the plethora of details available from CIS information systems, the emphasis on control has resulted in micro-managing the details at the expense of the big picture.

[39] William E. Halal, Michael D. Kull and Ann Leffmann, "Emerging Technologies: What's Ahead for 20001-2030," The Futurist (November/December 1997): 21.

[40] Ross Pigeau and Carol McCann, "Putting 'Command' Back into Command and Control: The Human Perspective," Command and Control Conference, Ottawa, 26 September 1995: C3.

Commanders, overtaxed with volumes of information have abdicated their responsibility of command for the safer more comfortable domain of the tactical details. In commenting on this aspect of command in war since the 1800s, Martin van Creveld states: “to cope with the flood of information, staff was piled upon staff, procedure upon procedure, machine upon machine. With each stage of growth of staffs, the problem of coordinating the staffs parts with each other, and the staff as a whole with the forces, was compounded.”[41] In our enthusiastic pursuit of technology we have forgotten common sense and developed advanced CIS systems that overwhelm commanders with a myriad of information “just because the technology is available”. The result has been systems that limit the role of the commander that now need to be optimized to reintroduce the human command element back in the loop.

Clearly, there are limitations and risks associated with the pursuit of CIS development within the CF. While limited in their nature, the issues raised can be addressed with the technology and skills which are currently available to the CF and industry. These issues must be recognized throughout all levels of command and appropriate action taken to address each adequately and thoroughly. To do otherwise would be to jeopardize the potential benefits that could result from a robust CIS infrastructure.

[41] Martin Van Creveld, Command in War, (Cambridge: Harvard University Press, 1985), 267.

Recipe for Success

As stated in the 1994 Defence White Paper: "We will continue to assess the relative costs and benefits of various capabilities in order to make trade-offs which, while difficult, will be essential if the Forces are to contribute to a broader range of Canadian objectives. …The Government's approach is to defence is to maintain the CF as a fundamental national resource which makes important contributions to a range of Canadian objectives."[42] From this and other statements in the White Paper, it is clear that Canada cannot, and should not, attempt to cover the entire military spectrum, but the CF should make a general contribution to a wide variety of domestic and international objectives. It is evident that the flexibility exists within the current defence guidance to focus on those defence capabilities that best meet Canada's interests. As stated by Krepinevich "even when countries will not be able to compete in the full spectrum of military capabilities, some of them, by specializing, will become formidable niche competitors."[43]

Considering the limited funding available to the Department of National Defence, the time has come for Canada to make difficult choices regarding which military capabilities are to be supported. The CF should reduce its focus to only those capabilities that will result in a balanced military, that is a flexible and agile force that can be

[42] Canada, 1994 Defence White Paper, 14.

[43] Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," 42.

deployed quickly. A robust, state-of-the-art CIS is a crucial to ensure CF can effectively integrate into any combined UN or NATO coalition operation, or respond to national domestic requirements. Therefore, CIS should be one of the capabilities retained and supported by the CF. A continued emphasis on CIS development and maintenance would place Canada in a position to make a credible contribution at the international level and gain much needed recognition, reinforcing her current status as a non-permanent member of the UN security Council

The CF should therefore take action to fully exploit CIS technology at the operational level be to provide commanders with relevant, reliable and accurate information at unprecedented speed. This initiative would allow them to achieve and maintain battlespace awareness at the operational level. Technologies should be acquired or developed, possibly in partnership with industry. This action would provide operational commanders with CIS tools that are interoperable with our allies to enable them to effectively integrate into the complex command and control relationships of coalition operations. Commanders would be able to more decisively focus their force on the opponent's centers of gravity, attacking their will to fight yet significantly reducing the cost of combat in terms of casualties and collateral damage. In commenting on the implications of IO, Donald Ryan highlights the potential for reduced violence as a result of the precise employment of force which should lead to significant reductions in human casualties and collateral damage.[44]

[44] Donald E. Ryan, "Implications of Information-Based Warfare," Joint Forces Quarterly (Autumn/Winter 1994): 114-116.

Essential within this initiative, is the need to consider the human dimension related to the introduction of complex technology and systems. All too often, common sense is put aside to make way for technological innovation, resulting in only partial value from the new systems. CIS systems should place the human back in the command loop and thus avoid the "Command and Control Schizophrenia (C^2S)" referred to by Pigeau and McCann. As stated in the discussion of the RMA, new technology should be carefully integrated with operational doctrine and military organizational structures to create a synergy to gain true leverage from the new systems. Systems should be designed with the commander's requirements in mind with a focus on reducing the workload so the commander can command more effectively. Action should be taken to reduce the potential for information paralysis, where the commander becomes overwhelmed with details to the point where he or she is not able to comprehend the larger picture. In this sense, emphasis should be placed on developing knowledge management tools that would assist operational commanders, and present them with only the relevant battlespace information. This would enable commanders to use the information from the CIS to increase their understanding of the battlespace that will lead to improved operational level decisions.

Office automation tools should be incorporated into support activities at all levels to maximize the effectiveness of staff to allow them to more rationally cope with the ever expanding set of responsibilities and tasks. Through wise investments in CIS technology, the military would gain significant effectiveness thus meeting the government's mandate of accomplishing the mission with fewer resources. An R&D program should be initiated in association with the private sector to develop the necessary tools and technology to protect Canadian military and domestic interests in cyberspace. Technological advances that fall out of a CIS R&D program would have a direct applicability in the Canadian private sector thereby offsetting the cost of development while meeting the need for a robust communications network that spans the Country. The skill sets and technology that result from this initiative should be transferable to the private sector to meet domestic requirements and provide the means to protect critical Canadian infrastructure.

Conclusions

In conclusion, a compelling case has been presented for the CF to continue to invest in the area of CIS to provide reliable communications and information processing capabilities at the operational level. It has been demonstrated that a robust, state-of-the-art CIS is essential to provide operational commanders the critical resources necessary to exercise effective command and gain control of the battlespace. In the final analysis, the maintenance of a state-of-the-art CIS would enable Canada to retain interoperability with her allies. As a result, the CF would be able to continue to participate in, and benefit from, UN and NATO coalition exercises and operations.

Annotated List of Works Cited

Adams, James. “Big Problem-Bad Solution: The Crisis in Critical Infrastructure and the Federal Solution.” Online News Summit ’98. 18 May 1998. The author presents his personal concerns regarding the vulnerability of Critical US Infrastructure to well planned cyber attack. He expresses his concerns regarding the lack of consultation with industry in dealing with this matter and his disappointment that the Department of Justice and the FBI have been placed in charge of dealing with the issue.

Allard, Kenneth. “Information Operations in Bosnia: A Preliminary Assessment.” American Intelligence Journal 17.3 (1997): 55-58. An excellent assessment of the role played by IO and the associated CIS technology in US operations in Bosnia. He concludes that while the technology in this area is impressive, the US military has a long way to go to implement it fully at the tactical level and he emphasizes the need for a stronger sense of the human factor.

Arquilla, John and David Ronfeldt. “Cyberwar is Coming.” Comparative Strategy 12.2 (1993): 141-156. A comprehensive look at the information revolution and its impact on modern day conflict. The concepts of netwar and cyberwar are explained in detail with current examples to bring them to life. The author provides an excellent review of the influence of information related factors in military history. Overall very good and informative reading.

Canada. Director of Army Doctrine. B-GL-300-005/FP-000 Information Operations Draft Version 1.0. Kingston: Director of Army Doctrine 5. A draft CF publication that puts the concepts provided in the equivalent US Army publication into Canadian context.

Canada. Director of Army Doctrine. The Land Force Strategic Direction and Guidance. Kingston: Director of the Army. A comprehensive publication covering all aspects of Canadian Land Forces Doctrine from a strategic perspective. This document provided excellent complement to the 1994 Defence White Paper in the area of the international strategic environment and offered valuable comments on Canadian domestic considerations.

Canada. Department of National Defence. 1994 Defence White Paper. Ottawa: Canada Communications Group, 1994. A thorough review of current Canadian interests and overall defence objectives. Excellent reading to gain a perspective into Canadian security concerns.

"Commanders Pull Intelligence in Information Warfare Strategy." Signal 48.12 (1994): 29-31. A brief article with a narrow focus on the need to manage the volumes of information flowing from today's CIS and the need to select the relevant intelligence information.

Davis, Norman C. “The Marine Corps and Information Operations.” Marine Corps Gazette 18.4 (1997): 16-22. A useful article, which espouses the value of the information revolution in the military, and the need for the Marine Corps to aggressively pursue a stronger focus on Information Operations. The author provide a good review of current status of IO initiatives in the three main services in the US military and makes a compelling argument for the Marine Corps to get more involved.

Devost, Matthew G., Brian K. Houghton and Neal A. Pollard. “Information Terrorism: Can You Trust Your Toaster.” Institute for National and Strategic Studies Sun Tzu Art in Information Warfare Web Page “http://www.ndu.edu/inss/siws/ch3.html”. The author provides a compelling view of the vulnerability of current commercial and military information infrastructure to sabotage and attack. He uses some excellent and plausible examples to make his point then suggests some possible solutions. Key to this article is the potential for the military to play an important role in this area.

Eggleton, Art. Address. The AFCEA Breakfast. Rideau Club, Ottawa. 28 May 1998. A good cursory review of the potential threats in the CIS environment with a look at what DND is doing to address the existing risks. Provides an important link between the military and civilian security requirements and makes the point that the military and private sector need to work together on this problem.

Goure, Dan. "Is There a Military-Technical Revolution in America's Future." The Washington Quarterly 16.4 (1993): 174-192. One of the better articles on the evolution of the MTR with an excellent analysis of the concept of an MTR. The author looks at current innovation in the US military and places it into context against the definition of an MTR. He concludes that while the US military is not in the midst of an information based MTR, all the ingredients are there. He points out that to gain the efficiencies necessitated by reductions the US military must take action to make the MTR a reality.

Gray, Colin S. "The American Revolution in Military Affairs: An Interim Assessment." The Strategic and Combat Studies Institute, The Occasional Number 28 (1997). This paper provides an in-depth assessment of the RMA in the context of current American initiatives. The author provides a number of valuable points of view which both support and question the existence of an RMA and the focus on information warfare within the RMA. The arguments are well thought out and proved very useful when reviewing this subject.

Halal, William E., Michael D. Kull and Ann Leffmann. "Emerging Technologies: What's Ahead for 20001-2030." The Futurist 31.4 (1997): 20-28. The authors provide a review of current trends in technology advances and provide predictions regarding the future. A good reference for identifying which technologies will impact our future the most as it provides a useful look at where we will be in the future.

"Information Warfare: A Two-Edged Sword." RAND Research Review 19.2 (1995). The article presents a brief look at the vulnerability of strategic information in the CIS environment and a light discussion of cyberwar issues. This article was of limited value in support of this essay.

Krepinevich, Andrew F. "Cavalry to Computer: The Pattern of Military Revolutions." The National Interest 37 (1994): 30-42. The author provides an overview of military revolutions over the centuries and their impact on the conduct of war. He takes a brief look at the current revolution and provides some insights into what the future holds.

Mazarr, Michael J. "The revolution in Military Affairs: A Framework For Defense Planning." Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 1994. Mazarr provides an very good overall assessment of the current RMA. He argues that the RMA is part of a larger sociopolitical transformation propelled by advances in technology. He offers a framework of four principles for defence planning to assist in dealing the ambiguities presented by the RMA.

Mazarr, Michael J., Jefrey Shaffer and Benjamin Ederington. Military Technical Revolution: A Structural Framework. Washington, DC: The Center For Strategic and International Studies, 1993. This report provides an excellent look at the concept of the MTR placing it within the strategic context of today's world environment. Comment is made on where the US military is today and what should be done to initiate a true MTR to maximize the opportunities being made available through technology advances. A very good reference to gain a strategic perspective in this area.

McConville, James E. "U.S. Army Information Operations: Concepts and Execution." Military Intelligence 23.1 (1997): 17-22. McConville provides a good review of the principles of IO placing them into context. This article is a good complement to the official US Army publication FM 100-6.

Miller, John. "Information Warfare: Issues and Perspectives." Sun Tzu Art of War in Information Warfare March 1995. One of the better articles on this subject. The Author provides a well-researched and comprehensive look at information warfare and the MTR. A very good reference for this essay with numerous valuable references.

Murray, Williamson. "Thinking About Revolutions in Military Affairs." Joint Forces Quarterly 16 (1997): 69-76. This article while not focused on the technology aspects of military revolutions provides a good background on the military aspects of revolutions in military affairs. This paper proved to be a good reference for this essay.

Pigeau, Ross and Carol McCann. "Putting 'Command' Back into Command and Control: The Human Perspective." Command and Control Conference. Ottawa, 26 September 1995: C1-C19. Pigeau and McCann provide a excellent review of this subject presenting a compelling case for dealing with C^2S and placing more focus on the human aspects of command. This was an excellent source document for this paper, which was of great assistance in developing the basic arguments.

Robinson, Clarence A. "Information Warfare Demands Battlespace Visualization Grasp." Signal 51.6 (1997): 17-20. This paper provides a thorough review of Information Warfare and its impact on operations on today's battlefield. A good reference to place the concepts of Information Warfare into context for the military commander. The author makes a strong case for improved knowledge management tools.

Ryan, Donald E. "Implications of Information-Based Warfare." Joint Forces Quarterly 6 (1994): 114-116. Ryan presents a brief look at the implications of Information Warfare and the benefits that can result. He looks at the potential to reduce conflict through a more informed application of force.

Segal, Gerald. "Asians in Cyberspace." Washington Quarterly 18.3 (1995): 5-16. This article provides an informative look at the growth and impact of cyberspace in the

East Asian countries. The author provides excellent examples of computer crime in East Asia and make relevant comment on the limitation facing law enforcement agencies around the world in this area.

Tilford, Earl H. "The Revolution in Military Affairs: Prospects and Cautions." Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 1995. A very good work that provides a comprehensive assessment of the current RMA. Tilford argues that RMAs are based on more than technology and that a true revolution depends on the convergence of political, social and technological factors.

Unites States. Department of the Army. FM 100-6 Information Operations. Washington, DC: Headquarters Department of the Army, 1996. This publication proved to be an excellent reference to gain an understanding of Information Operations and it's various components. It provides a thorough and logical explanation of IO concepts and their application in the Army.

Van Creveld, Martin. Command in War. Cambridge: Harvard University Press, 1985. While a comprehensive and authoritative work on command, chapter eight provided particular comment on the application of information systems in command. The author provides a realistic and critical look at the implementation of CIS technology and questions it's value to the commander. This book was an excellent reference to ensure a balanced perspective was presented.

Wynnyk, Paul F. Jointness: The Need for the Canadian Forces to Go Farther. Kingston: Royal Military College of Canada, 1997. An informative look at the development of joint doctrine in the CF in which a compelling argument is presented for the CF to go even further. This article was of limited value as a reference.